2017 IEEE International Symposium on Information Theory

Aachen, Germany | June 25 - 30, 2017

Book of Abstracts

ISIT 2017 AACHEN

www.isit2017.org

RWTH AACHEN UNIVERSITY

IEEE

IEEE INFORMATION THEORY SOCIETY

VDE ITG

FOCUS. PERSEVERE. BREAKTHROUGH.

Germany is on the brink of a new digital age. Whether in daily life or in the business world, modern technologies enable to network processes intelligently as well as to evaluate data quickly and efficiently. For many years, Huawei has been providing digital innovations that pave the way forward for German companies towards Industry 4.0. At the European Research Center in Munich, we are also contributing with breakthroughs to 5G, the next generation of mobile high speed telecommunication networks.
A better connected Germany.

HUAWEI

Welcome

The IEEE International Symposium on Information Theory (ISIT) will take place in the historic city of Aachen, Germany, from June 25 to 30, 2017. With 800 international experts, scientists and researchers expected, ISIT focuses on the processing, transmission, storage, and use of information. It specifically encompasses theoretical and certain applied aspects of coding, communications and communications networks, complexity and cryptography, detection and estimation, and learning.

The range of topics related to information theory includes, but is not limited to the following areas: Big Data Analytics, Coding for Communication and Storage, Coding Theory, Communication Theory, Complexity and Computation Theory, Compressed Sensing and Sparsity, Cryptography and Security, Detection and Estimation, Emerging Applications of IT, Information Theory and Statistics, Information Theory in Biology, Network Coding and Applications, Network Information Theory, Optical Communication, Pattern Recognition and Machine Learning, Physical Layer Security, Quantum Information and Coding Theory, Shannon Theory, Signal Processing, Source Coding and Data Compression, Wireless Communication and Networks.

The IEEE ISIT is a place for networking and a think tank for new ideas. By contributing to this conference you will be able to draw the attention of key players in this field from around the world. The range of use cases is broad. Network operators and developers are equally addressed. Companies and institutions which provide services for the “smart market” often use solutions based on Information Theory. We look forward to welcoming you to the world of Information Theory in Aachen!

Prof. Dr. Rudolf Mathar

RWTH Aachen University

Sponsors

Organizing Committee

General Co-Chairs
Rudolf Mathar
Gerhard Kramer

TPC Co-Chairs
Martin Bossert
Stephan ten Brink
Stephen Hanly
Sennur Ulukus

Finance Chair
Meik Dörpinghaus

Publications Chairs
Giuseppe Durisi
Christoph Studer

Tutorial Chairs
Eduard Jorswieck
Jörg Kliewer

Recent Results Chair
Anke Schmeink

Student Travel Grants
Bernhard Geiger

EDAS Administration
Gholamreza Alirezaei
Giuseppe Durisi

Local Arrangements
Christine Cox
Niklas Koep
Markus Rothe

Technical Program Committee

Salman Avestimehr
Sasha Barg
Andrew R. Barron
Gerhard Bauch
Matthieu Bloch
Holger Boche
Georg Böcherer
Helmut Bölcskei
Fredrik Brännström
Viveck Cadambe
Giuseppe Caire
Thomas Courtade
Marco Dalai
Nathasha Devroye
Suhas Diggavi
Alex Dimakis
Dariush Divsalar
Stark Draper
Tolga Duman
Michelle Effros
Abbas El Gamal
Salim El Rouayheb
Uri Erez
Elza Erkip
Meir Feder
Robert Fischer
Christina Fragouli
Michael Gastpar
Norbert Görtz
Pulkit Grover
Deniz Gündüz
Bruce Hajek
Tracey Ho
Camilla Hollanti
Tanya Ignatenko
Syed Jafar
Sid Jaggi
Tara Javidi
Thomas Johansson
Sarah Johnson
Eduard Jorswieck
Wei Kang
Kenta Kasai
Ashish Khisti
Young-Han Kim
Negar Kiyavash
Jörg Kliewer
Tobias Koch
Frank R. Kschischang
Volker Kühn
Vijay Kumar
Gitta Kutyniok
Amos Lapidoth
Gottfried Lechner
Michael Lentmaier
Yingbin Liang
Nan Liu
Gianluigi Liva
Angel Lozano
Arya Mazumdar
Muriel Médard
Olgica Milenkovic
Urbashi Mitra
Guido Montorsi
Stefan Moser
Mehul Motani
Pierre Moulin
Ralf Müller
Chandra Nair
Bobak Nazer
Lawrence Ong
Yasutada Oohama
Ayfer Özgür
Haim Permuter
Li Ping
H Vincent Poor
Maxim Raginsky
Lars Rasmussen
Stefano Rini
Anant Sahai
Lalitha Sankar
Anand Sarwate
Igal Sason
Jossy Sayir
Robert Schober
Christian Senger
Aydin Sezgin
Shlomo Shamai
Vladimir Sidorenko
Osvaldo Simeone
Mikael Skoglund
Changho Suh
Vincent Tan
Toshiyuki Tanaka
Ravi Tandon
Andrew Thangaraj
Antonia Tulino
Ertem Tuncel
Daniela Tuninetti
Himanshu Tyagi
Rüdiger Urbanke
Vinay Vaishampayan
Venu Veeravalli
Pramod Viswanath
Emanuele Viterbo
Aaron Wagner
Shun Watanabe
Tsachy Weissman
Rick Wesel
Michèle Wigger
Andreas Winter
Stefan Wolf
Gregory W. Wornell
Jing Yang
Roy Yates
Aylin Yener
Raymond Yeung
Wei Yu
Lizhong Zheng

Claude E. Shannon Award Lecture

Wednesday, June 28 Europa hall 8:30 - 9:30

The Spirit of Information Theory

David Tse, Stanford University, California, USA

Biography

David Tse received the B.A.Sc. degree in systems design engineering from University of Waterloo in 1989, and the M.S. and Ph.D. degrees in electrical engineering from Massachusetts Institute of Technology in 1991 and 1994 respectively. From 1994 to 1995, he was a postdoctoral member of technical staff at A.T. & T. Bell Laboratories. From 1995 to 2014, he was on the faculty of the University of California at Berkeley. He is currently a professor at Stanford University.

David Tse is the recipient of the 2017 Claude E. Shannon Award. Previously, he received a NSF CAREER award in 1998, the Erlang Prize from the INFORMS Applied Probability Society in 2000 and a Gilbreth Lectureship from the National Academy of Engineering in 2012. He received multiple best paper awards, including the Information Theory Society Paper Award in 2003, the IEEE Communications Society and Information Theory Society Joint Paper Awards in 2000, 2013 and 2015, the Signal Processing Society Best Paper Award in 2012 and the IEEE Communications Society Stephen O. Rice Prize in 2013. For his contributions to education, he received the Outstanding Teaching Award from the Department of Electrical Engineering and Computer Sciences at U.C. Berkeley in 2008 and the Frederick Emmons Terman Award from the American Society for Engineering Education in 2009. He is a coauthor, with Pramod Viswanath, of the text Fundamentals of Wireless Communication, which has been used in over 60 institutions around the world. He is the inventor of the proportional-fair scheduling algorithm used in all third and fourth-generation cellular systems.

Plenary Speakers

Monday, June 26 Europa hall 8:45 - 9:45

Reading and Hiding Data in Quantum Systems

Andreas Winter, Universitat Autònoma de Barcelona, Spain

Quantum data hiding, originally invented as a limitation on so-called local operations and classical communications (LOCC) in distinguishing globally orthogonal states, is actually a phenomenon arising generically in statistics whenever comparing a `strong' set of measurements (i.e., decision rules) with a `weak' one. The classical statistical analogue is secret sharing, in which two perfectly distinguishable multi-partite hypotheses appear to be indistinguishable when accessing only a marginal. The quantum versions are richer in that, e.g., LOCC allows for state tomography, so the states cannot become perfectly indistinguishable but only nearly so, and hence the question is one of efficiency. I will discuss two concrete examples and associated sets of problems.
1. Gaussian operations and classical computation (GOCC): GOCC cannot distinguish optimally even two coherent states of a single mode (Takeoka/Sasaki, 2008). We find states, each a mixture of multi-mode coherent states, which are almost perfectly distinguishable by suitable measurements, but when restricted to GOCC, i.e., linear optics and post-processing, the states appear almost identical. The construction is random and relies on coding arguments. Open questions include whether one can give a constructive version of the argument, and whether even thermal states can be used, and how efficient the hiding is.
2. Local operation and classical communication (LOCC): It is known that, asymptotically, log d bits can be hidden in a bipartite d x d-system (Hayden/Leung/Shor/Winter, 2004). We show that this is asymptotically optimal by using the calculus of min-entropies. In fact, we get bounds on the data hiding capacity of any preparation system; these are, however, not always tight. While it is known that data hiding by separable states is possible, i.e., the state preparation can be done by LOCC, it is open whether the optimal information efficiency of (asymptotically) log d bits can be achieved by separable states.

Biography
Andreas Winter received a Diploma degree in Mathematics from Freie Universität Berlin, Berlin, Germany, in 1997, and a Dr. math. degree from the Fakultät für Mathematik, Bielefeld University, Germany, in 1999. He was Research Associate at Bielefeld University, and from 2001 with the Department of Computer Science at University of Bristol, U.K. In 2003, still with University of Bristol, he was appointed Lecturer in Mathematics, and in 2006 Professor of Physics of Information. Since 2012 he is ICREA Research Professor with the Universitat Autònoma de Barcelona, Spain. He is the recipient of a Royal Society Wolfson Research Merit Award (2007), a Philip Leverhulme Prize (2009) and the Whitehead Prize of the London Mathematical Society (2012).
Andreas Winter's scientific interests revolve around quantum information theory and discrete mathematics, in particular quantum Shannon theory. He is the originator of several technical and conceptual innovations in that field, among them the discovery of state merging as a primitive and the meaning of negative information; the application of geometric measure concentration in quantum information and statistical mechanics; the development of a matrix tail bound à la Bernstein with numerous applications in information theory, signal processing and combinatorics; techniques towards strong converses and „pretty strong" converses in quantum Shannon theory; quantum entropy inequalities; and the development of zero-error quantum information theory, including an interpretation of the Lovász number as the zero-error capacity of a graph assisted by no-signalling correlations.

Tuesday, June 27 Europa hall 8:30 - 9:30

Biological Systems as Communication Networks

Urbashi Mitra, University of Southern California (USC), Los Angeles, USA

Significant progress has been made, of late, on fundamental problems across many areas of biology – in particular, biological interaction and signaling. Two important questions remain elusive. How do complex networks of simple organisms form in order to perform sophisticated tasks? What are the underlying signaling mechanisms that enable the formation and operation of such networks? Concepts and methods from information theory and communication theory offer some hope in providing abstractions and tools that can enable basic understanding of these two questions as well as determine fundamental limitations. The definition of communication in the biological context is vague and can be considered as „the transfer of information from one cell or molecule to another via chemical, mechanical, or electrical signals," or more broadly as „an activity by one organism that changes the behavior of another." Given the enormous diversity of organisms, there is an equally large number of communication systems that can be studied, and not all systems yield to a communication- or information-theoretic lens. To this end, we shall consider microbial ecosystems which contain a number of communication/information theoretic architectures. Microbial communities play a significant role in infection, bioremediation, plant growth promotion, human and animal digestion, the carbon cycle, cleaning water and microbial fuel cells. Two canonical multi-terminal structures are of importance: multi-hopped networks motivated by bacterial cables, and ad hoc multi-terminal networks as proxies for biofilms and quorum sensing. In this talk, we explore how a communication- and information-theoretic framework can be used to understand — and possibly design — biological systems.

Biography

Urbashi Mitra received the B.S. and the M.S. degrees from the University of California at Berkeley and her Ph.D. from Princeton University. She is currently a Dean's Professor of Electrical Engineering at the Department of Electrical Engineering at the University of Southern California (USC), Los Angeles. She is the inaugural Editor-in-Chief for the IEEE Transactions on Molecular, Biological and Multi-scale Communications. Dr. Mitra is a Distinguished Lecturer for the IEEE Communications Society for 2015-2017. She is a member of the IEEE Information Theory Society's Board of Governors (2002-2007, 2012-2017) and the IEEE Signal Processing Society's Technical Committee on Signal Processing for Communications and Networks (2012-2016). Dr. Mitra is a Fellow of the IEEE. She is the recipient of: a 2016 United Kingdom Royal Academy of Engineering, Distinguished Visiting Fellowship, a 2015 US Fulbright Scholar Award, a 2016-2017 Leverhulme Trust Visiting Professorship Fellowship, a 2015 Insight Magazine STEM Diversity Award, 2012 Globecom Signal Processing for Communications Symposium Best Paper Award, 2012 US National Academy of Engineering Lillian Gilbreth Lectureship, USC Center for Excellence in Research Fellowship (2010-2013), the 2009 DCOSS Applications and Systems Best Paper Award, Texas Instruments Visiting Professor (Fall 2002, Rice University), 2001 Okawa Foundation Award, 2000 OSU College of Engineering Lumley Award for Research, 1997 OSU College of Engineering MacQuigg Award for Teaching, and a 1996 National Science Foundation CAREER Award. She has been an Associate Editor for the following IEEE publications: Transactions on Signal Processing (2012--2015), Transactions on Information Theory (2007-2011), Journal of Oceanic Engineering (2006-2011), and Transactions on Communications (1996-2001). She has co-chaired: (technical program) 2014 IEEE International Symposium on Information Theory in Honolulu, HI, 2014 IEEE Information Theory Workshop in Hobart, Tasmania, IEEE 2012 International Conference on Signal Processing and Communications, Bangalore India, and the IEEE Communication Theory Symposium at ICC 2003 in Anchorage, AK; and was the general co-chair for the first ACM Workshop on Underwater Networks at Mobicom 2006, Los Angeles, CA. She served as co-Director of the Communication Sciences Institute at the University of Southern California from 2004-2007. Her research interests are in: wireless communications, communication and sensor networks, biological communication systems, detection and estimation and the interface of communication, sensing and control.

Thursday, June 29 Europa hall 8:30 - 9:30

The Flesh of Polar Codes

Emre Telatar, École polytechnique fédérale de Lausanne, Switzerland

Biography

I. Emre Telatar received the B.Sc. degree in electrical engineering from the Middle East Technical University, Ankara, Turkey, in 1986. He received the S.M. and Ph.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, in 1988 and 1992 respectively. In 1992, he joined the Communications Analysis Research Department at AT&T Bell Laboratories (later Lucent Technologies), Murray Hill, NJ. He has been at the EPFL since 2000.

Emre Telatar was the recipient of the IEEE Information Theory Society Paper Award in 2001. He was a program co-chair for the IEEE International Symposium on Information Theory in 2002, and associate editor for Shannon Theory for the IEEE Information Theory Transactions from 2001 to 2004. He was awarded the EPFL Agepoly teaching prize in 2005.

Emre Telatar‘s research interests are in communication and information theories.

Friday, June 30 Europa hall 8:30 - 9:30

Information Theory Out of its Box

Cédric Villani, University Claude Bernard, Lyon, France

Some examples of information theoretical tools doing great in various fields of mathematics - kinetic theory, mathematical physics, geometry.

Biography

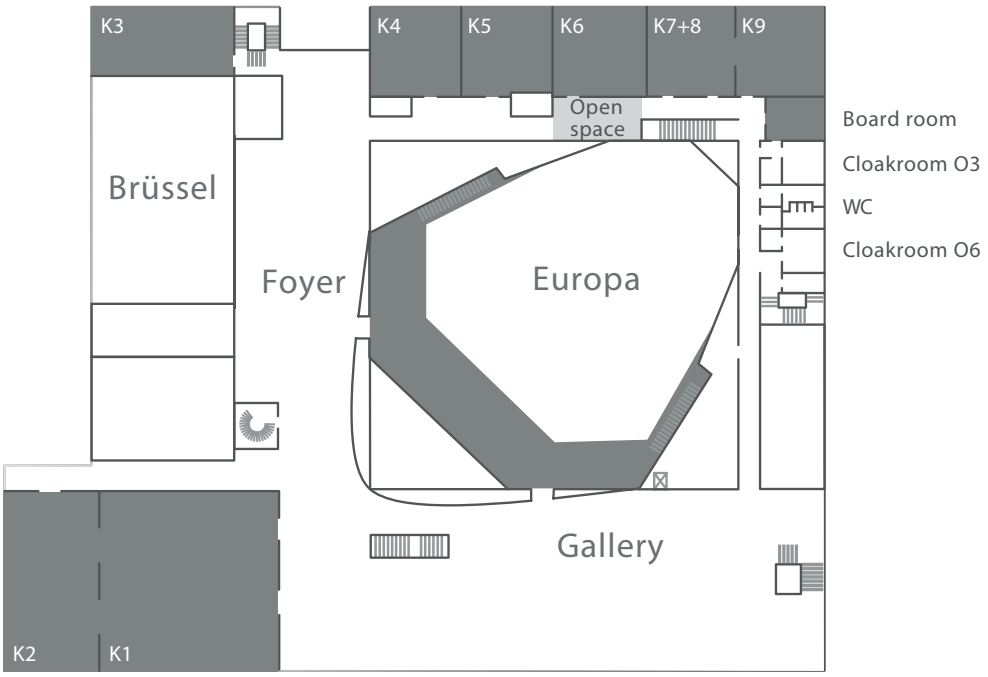
Cédric Villani‘s research interests are in kinetic theory (Boltzmann and Vlasov equations and their variants), and optimal transport and its applications.

Cédric Villani studied mathematics at École Normale Supérieure in Paris. In 1998, he defended his PhD on the mathematical theory of the Boltzmann equation. From 2000 to 2010, he was professor at École Normale Supérieure de Lyon, and now at the Université de Lyon. He occupied visiting professor positions in Atlanta, Berkeley and Princeton. Since 2009, he is the Director of Institut Henri Poincaré in Paris.

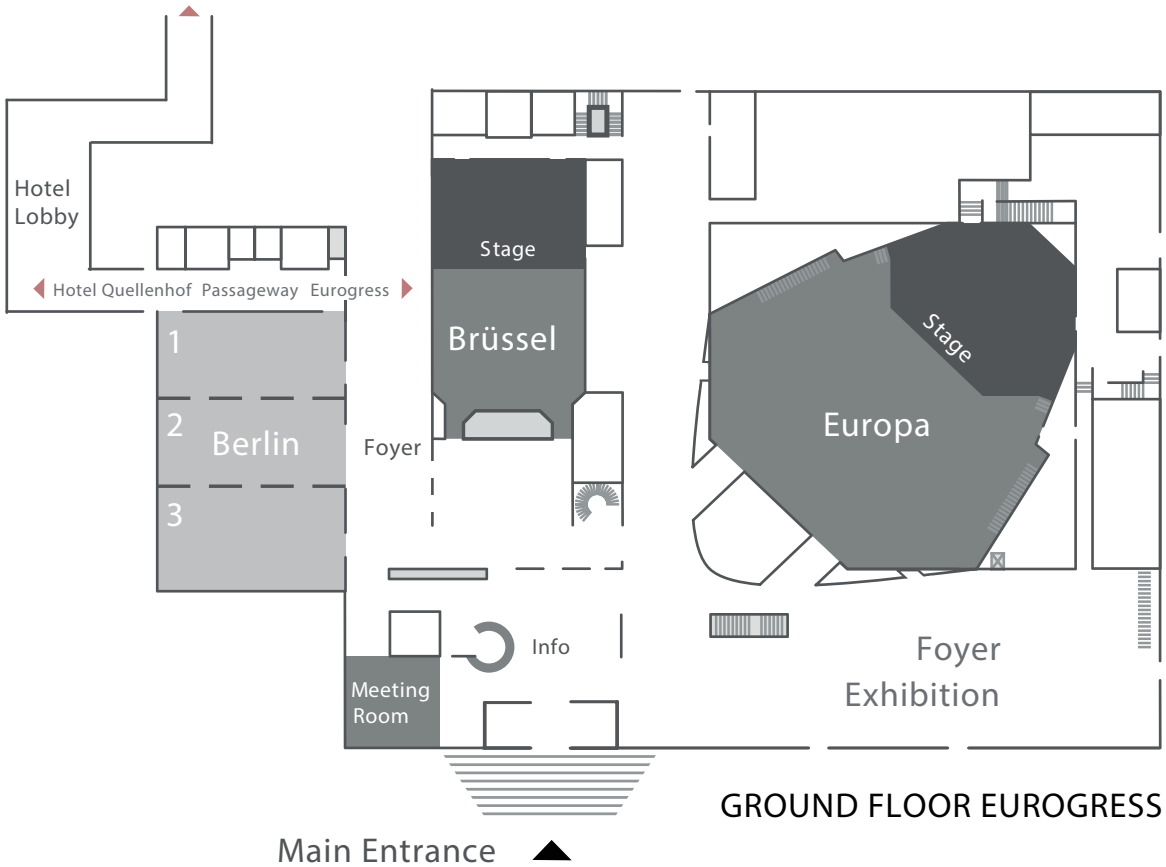
He received several national and international prizes for his research, in particular the Fields Medal, awarded at the 2010 International Congress of Mathematicians in Hyderabad (India), by the President of India. He is a chief editor of the Journal of Functional Analysis, and editor of Inventiones Mathematicae. He participates actively in the administration of science, through the Institut Henri Poincaré, but also by sitting on a number of panels and committees, including the higher council of research and the strategic council of Paris, and the High Level Group of Scientific Advisors at the European Commission. Since 2010 he has been involved in fostering mathematics in Africa, through programs by the Next Einstein Initiative and the World Bank.

He has been a member of the Paris Academy of Sciences since December 2013, and a member of the Pontifical Academy of Sciences (Roma, Italy) since 2016.

Venue Map



FIRST FLOOR EUROGRESS



GROUND FLOOR EUROGRESS

Technical Program

Monday, June 26 — 10:10-11:10

10:10	10:30	10:50
Mo1-1: Algebraic Coding Chair: Christian Senger		**Europa**
Constructions of Partial MDS Codes over Small Fields *Eitan Yaakobi, Ryan Gabrys, Mario Blaum, Paul Siegel*	Attaining Capacity with iterated (U|U+V) codes based on AG codes and Koetter-Vardy soft decoding *Jean-Pierre Tillich, Irene Márquez-Corbella*	An Algebraic-Combinatorial Proof Technique for the GM-MDS Conjecture *Anoosheh Heidarzadeh, Alex Sprintson*
Mo1-2: Convolutional Codes Chair: Michael Lentmaier		**Brussels**
On the Code Distance of a Woven Block Code Construction *Igor Zhilin, Alexey Kreshchuk, Victor V. Zyablov*	Generalized column distances for convolutional codes *Sara D. Cardell, Marcelo Firer, Diego Napp*	A Unified Ensemble of Concatenated Convolutional Codes *Saeedeh Moloudi, Michael Lentmaier, Alexandre Graell i Amat*
Mo1-3: Multiple Access 1 Chair: Aydin Sezgin		**K2**
Cooperative Binning for Semi-deterministic Channels with Non-causal State Information *Ido Gattegno, Haim Permuter, Shlomo (Shitz) Shamai, Ayfer Özgür*	A New Achievable Rate Region for Multiple-Access Channel with States *Mohsen Heidari Khoozani, Farhad Shirani, Sandeep Pradhan*	The Benefit of Encoder Cooperation in the Presence of State Information *Parham Noorzad, Michelle Effros, Michael Langberg*
Mo1-4: Entropy 1 Chair: Holger Boche		**K3**
A lower bound on the differential entropy for log-concave random variables with applications to rate-distortion theory *Arnaud Marsiglietti, Victoria Kostina*	H(X) vs. H(f(X)) *Ferdinando Cicalese, Luisa Gargano, Ugo Vaccaro*	Concavity of Entropy Power: Equivalent Formulations and Generalizations *Thomas Courtade*
Mo1-5: Optical Communications Chair: Frank Kschischang		**K4**
On Time-Bandwidth Product of Multi-Soliton Pulses *Alexander Span, Vahid Aref, Henning Buelow, Stephan ten Brink*	A Novel Demodulation Scheme for a Memoryless Optical Interference Channel *Kamran Keykhosravi, Erik Agrell*	Optical MISO IM/DD Channels: Optimality of Spatial Repetition Codes among DC-offset STBCs *Yerzhan Sapenov, Anas Chaaban, Zouheir Rezki, Mohamed-Slim Alouini*
Mo1-6: Precoding Chair: Jinyuan Chen		**K5**
Beamforming Codebook Compensation for Beam Squint with Channel Capacity Constraint *Mingming Cai, J. Nicholas Laneman, Bertrand Hochwald*	Asymptotics of Nonlinear LSE Precoders with Applications to Transmit Antenna Selection *Ali Bereyhi, Mohammad Ali Sedaghat, Ralf Müller*	MIMO IBC Beamforming with Combined Channel Estimate and Covariance CSIT *Wassim Tabikh, Dirk Slock, Yi Yuan-Wu*
Mo1-7: Quantization Chair: Ioannis Kontoyiannis		**K6**
How to Quantize n Outputs of a Binary Symmetric Channel to n-1 Bits? *Wasim Huleihel, Or Ordentlich*	Information-Distilling Quantizers *Bobak Nazer, Or Ordentlich, Yury Polyanskiy*	
Mo1-8: Rate Distortion Theory 1 Chair: Shigeaki Kuzuoka		**K7+8**
Distortion bounds for source broadcasting and asymmetric data transmission with bandwidth expansion *Shraga Bross, Hagai Zalach*	Rate-Distortion Region of a Gray-Wyner Problem with Side-Information *Meryem Benammar, Abdellatif Zaidi*	A Multiple Description CEO Problem with Log-Loss Distortion *Georg Pichler, Pablo Piantanida, Gerald Matz*
Mo1-9: Hypothesis Testing 1 Chair: Gregory Wornell		**K9**
Neyman-Pearson Test for Zero-Rate Multiterminal Hypothesis Testing *Shun Watanabe*	Using data-compressors for statistical analysis of problems on homogeneity testing and classification *Boris Ryabko, Andrey Guskov, Irina Selivanova*	First- and Second-Order Hypothesis Testing for Mixed Memoryless Sources with General Mixture *Te Sun Han, Ryo Nomura*
Mo1-A: Age of Information 1 Chair: Yin Sun		**Berlin 3**
Status updates through M/G/1/1 queues with HARQ *Elie Najm, Roy Yates, Emina Soljanin*	Information Freshness and Popularity in Mobile Caching *Clement Kam, Sastry Kompella, Gam Nguyen, Jeffrey Wieselthier, Anthony Ephremides*	Age-Optimal Constrained Cache Updating *Roy Yates, Philippe Ciblat, Aylin Yener, Michele Wigger*

Monday, June 26

11:30-12:50

11:30	11:50	12:10	12:30
Mo2-1: Coding Techniques 1 Chair: Jos Weber			**Europa**
PIR schemes with small download complexity and low storage requirements *Simon Blackburn, Tuvi Etzion, Maura Paterson*	Nearly Optimal Constructions of PIR and Batch Codes *Hilal Asi, Eitan Yaakobi*	Cyclone Codes *Christian Schindelhauer, Andreas Jakoby, Sven Köhler*	Approaching Capacity Using Incremental Redundancy without Feedback *Haobo Wang, Sudarsan Vasista Srinivasan Ranganathan, Richard Wesel*
Mo2-2: Locally Repairable Codes 1 Chair: Iwan Duursma			**Brussels**
Rate Optimal Binary Linear Locally Repairable Codes with Small Availability *Swanand Kadhe, Robert Calderbank*	On Optimal Ternary Locally Repairable Codes *Jie Hao, Shutao Xia, Bin Chen*	A Study on the Impact of Locality in the Decoding of Binary Cyclic Codes *Nikhil Krishnan Muralee Krishnan, Bhagyashree Puranik, P Vijay Kumar, Itzhak Tamo, Alexander Barg*	Locally Repairable Codes with the Optimum Average Information Locality *Mostafa Shahabinejad, Majid Khabbazian, Masoud Ardakani*
Mo2-3: Broadcast Channels 1 Chair: Chandra Nair			**K2**
Error Exponent of the Common-Message Broadcast Channel with Variable-Length Feedback *Lan Truong, Vincent Tan*	Exact Random Coding Exponents and Universal Decoders for the Degraded Broadcast Channel *Ran Averbuch, Neri Merhav*	Feedback Halves the Dispersion for Some Two-User Broadcast Channels with Common Message *Kasper Trillingsgaard, Wei Yang, Giuseppe Durisi, Petar Popovski*	A New Capacity-Approaching Protocol for General 1-to-K Broadcast Packet Erasure Channels with ACK/NACK *Chih-Hua Chang, Chih-Chun Wang*
Mo2-4: Feedback Chair: Gerhard Kramer			**K3**
On the Capacity of Burst Noise-Erasure Channels With and Without Feedback *Lin Song, Fady Alajaji, Tamas Linder*	The ARMA(k) Gaussian Feedback Capacity *Tao Liu, Guangyue Han*	An Optimal Coding Scheme for the BIBO Channel with a No-Repeated-Ones Input Constraint *Oron Sabag, Haim Permuter, Navin Kashyap*	
Mo2-5: Reconstruction Chair: Urbashi Mitra			**K4**
Compressed Sensing with Prior Information via Maximizing Correlation *Xu Zhang, Wei Cui, Yulong Liu*	Low Dimensional Atomic Norm Representations in Line Spectral Estimation *Maxime Ferreira Da Costa, Wei Dai*	Analysis of Approximate Message Passing with a Class of Non-Separable Denoisers *Yanting Ma, Cynthia Rush, Dror Baron*	Inexact Projected Gradients on Unions of Subspaces *Thomas Wiese, Lorenz Weiland, Wolfgang Utschick*
Mo2-6: Complexity Chair: Pulkit Grover			**K5**
Analysis and Enhancements of a Cognitive Based Complexity Measure *Dilshan De Silva, Nuwan Kodagoda, Saluka Kodituwakku, Amalka J. Pinidiyaarachchi*	Generic Cospark of a Matrix Can Be Computed in Polynomial Time *Sichen Zhong, Yue Zhao*	Enumeration of Boolean Functions of Sensitivity Three and Inheritance of Nondegeneracy *Kazuyuki Amano*	On the Complexity of Estimating Renyi Divergences *Maciej Skorski*
Mo2-7: ARQ Chair: Zouheir Rezki			**K6**
An Information Density Approach to Analyzing and Optimizing Incremental Redundancy with Feedback *Haobo Wang, Nathan Wong, Alexandar Baldauf, Christopher Bachelor, Sudarsan Vasista Srinivasan Ranganathan, Dariush Divsalar, Richard Wesel*	Outage Effective Capacity of Buffer-Aided Diamond Relay Systems Using HARQ-IR *Deli Qiao*	Constraints for coded tunnels across long latency bottlenecks with ARQ-based congestion control *Ulrich Speidel, Sven Puchinger, Martin Bossert*	Throughput of HARQ-IR with Finite Blocklength Codes and QoS Constraints *Yi Li, M. Cenk Gursoy, Senem Velipasalar*
Mo2-8: Quantum IT 1 Chair: Marco Dalai			**K7+8**
Polar Codes for Arbitrary Classical-Quantum Channels and Arbitrary cq-MACs *Rajai Nasser, Joseph Renes*	Sphere-Packing Bound for Symmetric Classical-Quantum Channels *Hao-Chung Cheng, Min-Hsiu Hsieh, Marco Tomamichel*	A meta-converse for private communication over quantum channels *Mark Wilde, Marco Tomamichel, Mario Berta*	Moderate Deviations for Classical-Quantum Channels *Hao-Chung Cheng, Min-Hsiu Hsieh*
Mo2-9: Source Coding 1 Chair: Lele Wang			**K9**
Entropy of Some General Plane Trees *Zbigniew Golebiewski, Abram Magner, Wojciech Szpankowski*	On Optimality and Redundancy of Side Information Version of SWLZ *Ayush Jain, Rakesh Bansal*	Two-Dimensional Source Coding by Means of Subblock Enumeration *Takahiro Ota, Hiroyoshi Morita*	
Mo2-A: Age of Information 2 Chair: Michele Wigger			**Berlin 3**
Timely Updates over an Erasure Channel *Roy Yates, Elie Najm, Emina Soljanin, Jing Zhong*	Remote Estimation of the Wiener Process over a Channel with Random Delay *Yin Sun, Yury Polyanskiy, Elif Uysal-Biyikoglu*	Age and Value of Information: Non-linear Age Case *Antzela Kosta, Nikolaos Pappas, Anthony Ephremides, Vangelis Angelakis*	Status Updates Over Unreliable Multiaccess Channels *Sanjit Kaul, Roy Yates*

Monday, June 26 14:40-16:20

14:40	15:00	15:20	15:40	16:00
Mo3-1: Reed-Solomon Codes Chair: Alexander Vardy				**Europa**
Twisted Reed-Solomon Codes *Peter Beelen, Sven Puchinger, Johan Rosenkilde*	Iterative Soft-Decision Decoding of Reed-Solomon Codes of Prime Lengths *Shu Lin, Khaled Abdel-Ghaffar, Juane Li, Keke Liu*	Optimal Repair Schemes for Some Families of Full-Length Reed-Solomon Codes *Hoang Dau, Olgica Milenkovic*	Repairing Reed-Solomon Codes With Two Erasures *Hoang Dau, Iwan Duursma, Han Mao Kiah, Olgica Milenkovic*	Decoding of Interleaved Reed-Solomon Codes Using Improved Power Decoding *Sven Puchinger, Johan Rosenkilde*
Mo3-2: LDPC Codes 1 Chair: Paul Siegel				**Brussels**
Average Spectra for Ensembles of LDPC Codes and Applications *Irina Bocharova, Boris Kudryashov, Vitaly Skachek, Yauhen Yakimenka*	Time-invariant LDPC convolutional codes *Dimitris Achlioptas, Hamed Hassani, Wei Liu, Ruediger Urbanke*	On LDPC Code Ensembles with Generalized Constraints *Yanfang Liu, Pablo M. Olmos, Tobias Koch*	Non-Uniformly Coupled LDPC Codes: Better Thresholds, Smaller Rate-loss, and Less Complexity *Laurent Schmalen, Vahid Aref, Fanny Jardel*	Reed-Solomon Based Non-binary Globally Coupled LDPC Codes: Correction of Random Errors and Bursts of Erasures *Juane Li, Keke Liu, Shu Lin, Khaled Abdel-Ghaffar*
Mo3-3: Caching 1 Chair: Osvaldo Simeone				**K2**
Characterizing the Rate-Memory Tradeoff in Cache Networks within a Factor of 2 *Qian Yu, Mohammad Ali Maddah-Ali, Salman Avestimehr*	A Computer-Aided Investigation on the Fundamental Limits of Caching *Chao Tian*	Capacity Scaling of Wireless Device-to-Device Caching Networks under the Physical Model *An Liu, Vincent Lau, Giuseppe Caire*	Wireless Coded Caching: A Topological Perspective *Jingjing Zhang, Petros Elia*	Multiplex Conductance and Gossip Based Information Spreading in Multiplex Networks *Yufan Huang, Huaiyu Dai*
Mo3-4: Channel Capacity 1 Chair: Min Li				**K3**
Capacity of Discrete-Time Wiener Phase Noise Channels to Within a Constant Gap *Luca Barletta, Stefano Rini*	Capacity Sensitivity in Additive Non-Gaussian Noise Channels *Malcolm Egan, Samir Perlaza, Vyacheslav Kungurtsev*	Communicating under Temperature and Energy Harvesting Constraints *Omur Ozel, Sennur Ulukus, Pulkit Grover*	On Additive Channels with Generalized Gaussian Noise *Alex Dytso, Ronit Bustin, H. Vincent Poor, Shlomo (Shitz) Shamai*	The Capacity of Injective Semi-Deterministic Two-Way Channels *Anas Chaaban, Lav Varshney, Mohamed-Slim Alouini*
Mo3-5: Detection and Estimation 1 Chair: Venugopal Veeravalli				**K4**
Sequential Estimation based on Conditional Cost *George Moustakides, Tony Yaacoub, Yajun Mei*	Fundamental limit of resolving two point sources limited by an arbitrary point spread function *Ronan Kerviche, Saikat Guha, Amit Ashok*	Denoising Linear Models with Permuted Data *Ashwin Pananjady, Martin Wainwright, Thomas Courtade*	Signal Recovery from Unlabeled Samples *Saeid Haghighatshoar, Giuseppe Caire*	Estimation of Sparsity via Simple Measurements *Abhishek Agarwal, Larkin Flodin, Arya Mazumdar*
Mo3-6: Wireless Networks 1 Chair: Andrea Goldsmith				**K5**
On Optimal Link Scheduling with Deadlines for Emptying a Wireless Network *Qing He, Di Yuan, Anthony Ephremides*	On the Coverage Probability of a Spatially Correlated Network *Chang-sik Choi, Jae Oh Woo, Jeffrey Andrews*	Efficiently Finding Simple Schedules in Gaussian Half-Duplex Relay Line Networks *Yahya Ezzeldin, Martina Cardone, Christina Fragouli, Daniela Tuninetti*	Exact Speed and Transmission Cost in a Simple One-Dimensional Wireless Delay-Tolerant Network *Dimitrios Cheliotis, Ioannis Kontoyiannis, Michail Loulakis, Stavros Toumpis*	Analysis of Breakdown Probability of Wireless Sensor Networks with Unreliable Relay Nodes *Takayuki Nozaki, Takafumi Nakano, Tadashi Wadayama*
Mo3-7: Communications 1 Chair: Nan Liu				**K6**
Optimal Frame Synchronization Over a Finite State Markov Channel *M Sundaram R, Arup Das, Devendra Jalihal, Venkatesh Ramaiyan*	Two-way Interference Channels with Jammers *Sidharth Jaggi, Michael Langberg*	Bit-Interleaved Coded Modulation for Phase Shift Keying on the Hypersphere *Christoph Rachinger, Ralf Müller, Johannes Huber*	Rigorous Dynamics of Expectation-Propagation-Based Signal Recovery from Unitarily Invariant Measurements *Keigo Takeuchi*	Geometrically uniform differential vector signaling schemes *Ezio Biglieri, Emanuele Viterbo*
Mo3-8: Compressed Sensing 1 Chair: Gerhard Wunder				**K7+8**
Statistical and computational phase transitions in spiked tensor estimation *Thibault Lesieur, Leo Miolane, Marc Lelarge, Florent Krzakala, Lenka Zdeborova*	Corrupted Sensing with Sub-gaussian Measurements *Jinchi Chen, Yulong Liu*	On the Phase Transition of Corrupted Sensing *Huan Zhang, Yulong Liu, Lei Hong*	On the Success Probability of the Box-Constrained Rounding and Babai Detectors *Jinming Wen, Xiao-Wen Chang, Chintha Tellambura*	A Characterization of Sampling Patterns for Low-Tucker-Rank Tensor Completion Problem *Morteza Ashraphijuo, Vaneet Aggarwal, Xiaodong Wang*
Mo3-9: MIMO 1 Chair: Christoph Studer				**K9**
Asymptotic Capacity Results for MIMO Wireless Optical Communication *Stefan Moser, Michail Mylonakis, Ligong Wang, Michele Wigger*	On Capacity of Noncoherent MIMO with Asymmetric Link Strengths *Joyson Sebastian, Ayan Sengupta, Suhas Diggavi*	On the Degrees-of-Freedom of the MIMO Three-Way Channel with Intermittent Connectivity *Anas Chaaban, Aydin Sezgin, Mohamed-Slim Alouini*	Outage Information Rate of Spatially Correlated Multi-Cluster Scattering MIMO Channels *Giorgio Taricco, Giuseppa Alfano*	A Generalized Zero-Forcing Precoder for Multiple Antenna Gaussian Broadcast Channels *Sha Hu, Fredrik Rusek*
Mo3-A: Age of Information 3 Chair: Elif Uysal-Biyikoglu				**Berlin 3**
Age of Information: Design and Analysis of Optimal Scheduling Algorithms *Yu-Pin Hsu, Eytan Modiano, Lingjie Duan*	Backlog-Adaptive Compression: Age of Information *Jing Zhong, Roy Yates, Emina Soljanin*	The Stationary Distribution of the Age of Information in FCFS Single-Server Queues *Yoshiaki Inoue, Hiroyuki Masuyama, Tetsuya Takine, Toshiyuki Tanaka*	Age-optimal Information Updates in Multihop Networks *Ahmed Bedewy, Yin Sun, Ness Shroff*	Communication over a Channel that Wears Out *Ting-Yi Wu, Lav Varshney, Vincent Tan*

Monday, June 26 16:40-18:20

16:40 17:00 17:20 17:40 18:00

Mo4-1: Coding Theory 1 Chair: Juergen Freudenberger — Europa

Non-linear Cyclic Codes that Attain the Gilbert-Varshamov Bound
Ishay Haviv, Michael Langberg, Moshe Schwartz, Eitan Yaakobi

Strong Functional Representation Lemma and Applications to Coding Theorems
Cheuk Ting Li, Abbas El Gamal

On the VC-Dimension of Binary Codes
Sihuang Hu, Nir Weinberger, Ofer Shayevitz

Duality of channels and codes
Joseph Renes

Polynomial Ring Transforms for Efficient XOR-based Erasure Coding
Jonathan Detchart, Jerome Lacan

Mo4-2: Coding for Storage Chair: Camilla Hollanti — Brussels

Secure RAID Schemes from EVENODD and STAR Codes
Wentao Huang, Jehoshua Bruck

Sector-disk codes with three global parities
Xiao Li, Iwan Duursma

Coding for Racetrack Memories
Yeow Meng Chee, Han Mao Kiah, Alexander Vardy, Van Khu Vu, Eitan Yaakobi

On the Tradeoff Region of Secure Exact-Repair Regenerating Codes
Shuo Shao, Tie Liu, Chao Tian, Cong Shen

Construction of Unrestricted-Rate Parallel Random Input-Output Code
Shan Lu, Hiroshi Kamabe, Jun Cheng, Akira Yamawaki

Mo4-3: Interference Channels 1 Chair: Daniela Tuninetti — K2

Two-way interference channel capacity: How to have the cake and eat it too
Changho Suh, Jaewoong Cho, David Tse

Capacity Region of the Symmetric Injective K-User Deterministic Interference Channel
Mehrdad Kiamari, Salman Avestimehr

State-Dependent Z-Interference Channel with Correlated States
Yunhao Sun, Yingbin Liang, Ruchen Duan, Shlomo (Shitz) Shamai

Novel Outer Bounds and Capacity Results for the Interference Channel with Conferencing Receivers
Reza K. Farsani, Amir K. Khandani

Approximate Capacity of a Class of Partially Connected Interference Channels
Muryong Kim, Yitao Chen, Sriram Vishwanath

Mo4-4: Shannon Inequalities Chair: Haim Permuter — K3

Wasserstein Stability of the Entropy Power Inequality for Log-Concave Random Vectors
Thomas Courtade, Max Fathi, Ashwin Pananjady

Two-Moment Inequalities for Renyi Entropy and Mutual Information
Galen Reeves

One-shot Multivariate Covering Lemmas via Weighted Sum and Concentration Inequalities
Mohammad Hossein Yassaee, Jingbo Liu, Sergio Verdú

A min-entropy power inequality for groups
Peng Xu, James Melbourne, Mokshay Madiman

A Minimal Set of Shannon-type Inequalities for Functional Dependence Structures
Satyajit Thakor, Terence Chan, Alex Grant

Mo4-5: Bounds 1 Chair: Martina Cardone — K4

Sum-set Inequalities from Aligned Image Sets: Instruments for Robust GDoF Bounds
Arash Gholami Davoodi, Syed Jafar

Scaling Exponent of Sparse Random Linear Codes over Binary Erasure Channels
Hessam Mahdavifar

A Frequency-Domain Approach to Tightening the Generalized Levenshtein Bound
Zilong Liu, Yong Liang Guan, Wai Ho Mow

Bounds for Cooperative Locality Using Generalized Hamming Weights
Khaled Abdel-Ghaffar, Jos Weber

Bounds on the Asymptotic Rate of Binary Constant Subblock-Composition Codes
Anshoo Tandon, Han Mao Kiah, Mehul Motani

Mo4-6: Multiterminal Source Coding Chair: Michelle Effros — K5

Distributed Cooperative Information Bottleneck
Matias Vera, Leonardo Rey Vega, Pablo Piantanida

A Unified Approach to Error Exponents for Multiterminal Source Coding Systems
Shigeaki Kuzuoka

Generalized Gaussian Multiterminal Source Coding and Probabilistic Graphical Models
Jun Chen, Farrokh Etezadi, Ashish Khisti

Two-Encoder Multiterminal Source Coding With Side Information Under Logarithmic Loss
Abdellatif Zaidi

Coding for Arbitrarily Varying Remote Sources
Amitalok Budkuley, Bikash Dey, Vinod Prabhakaran

Mo4-7: Security 1 Chair: Wei Kang — K6

On The Compound MIMO Wiretap Channel with Mean Feedback
Amr Abdelaziz, Ashraf Elbayoumy, Can Koksal, Hesham El Gamal

Multiple Access Wiretap Channel with Cribbing
Noha Helal, Aria Nosratinia

Wiretap channel capacity: Secrecy criteria, strong converse, and phase change
Eric Graves, Tan Wong

The Shannon Cipher System with a Guessing Eavesdropper
Lanqing Yu, Paul Cuff

Privacy-Aware Guessing Efficiency
Shahab Asoodeh, Mario Diaz, Fady Alajaji, Tamas Linder

Mo4-8: Privacy 1 Chair: Frans Willems — K7+8

Optimal Schemes for Discrete Distribution Estimation under Local Differential Privacy
Min Ye, Alexander Barg

Limits of Location Privacy under Anonymization and Obfuscation
Nazanin Takbiri, Amir Houmansadr, Dennis Goeckel, Hossein Pishro-Nik

Operational Definitions for Some Common Information Leakage Metrics
Ibrahim Issa, Aaron Wagner

Smart Meter Privacy Based on Adversarial Hypothesis Testing
Zuxing Li, Tobias Oechtering, Deniz Gündüz

Hypothesis Testing under Maximal Leakage Privacy Constraints
Jiachun Liao, Lalitha Sankar, Flavio Calmon, Vincent Tan

Mo4-9: Subspace and LDPC Codes Chair: Shu Lin — K9

Cyclic Subspace Codes and Sidon Spaces
Netanel Raviv, Itzhak Tamo

Grassmannian Codes from Multiple Families of Mutually Unbiased Bases
Olav Tirkkonen, Christopher Boyd, Roope Vehkalahti

Performance of ML Decoding for Ensembles of Binary and Nonbinary Regular LDPC Codes of Finite Lengths
Irina Bocharova, Boris Kudryashov, Vitaly Skachek

Interleaved Subspace Codes in Fountain Mode
Vladimir Sidorenko, Hannes Bartz, Antonia Wachter-Zeh

LT codes on Partial Erasure Channels
Carolyn Mayer, Christine Kelley

Mo4-A: Energy Harvesting 1 Chair: Yu-Pin Hsu — Berlin 3

Energy Harvesting Networks with General Utility Functions: Near Optimal Online Policies
Ahmed Arafa, Abdulrahman Baknina, Sennur Ulukus

On Achievable Rates of AWGN Energy-Harvesting Channels with Block Energy Arrival and Non-Vanishing Error Probabilities
Silas Fong, Vincent Tan, Ayfer Özgür

Optimal Transmission for Energy Harvesting Nodes under Battery Size and Usage Constraints
Jing Yang, Jingxian Wu

Single-User Channel with Data and Energy Arrivals: Online Policies
Abdulrahman Baknina, Sennur Ulukus

Tuesday, June 27 — 09:50-11:10

9:50	10:10	10:30	10:50
Tu1-1: Array Codes Chair: Joachim Rosenthal			**Europa**
Locality and Availability of Array Codes Constructed from Subspaces *Natalia Silberstein, Tuvi Etzion, Moshe Schwartz*	Efficient Lowest Density MDS Array Codes of Column Distance 4 *Zhijie Huang, Hong Jiang, Nong Xiao*	Triple-Fault-Tolerant Binary MDS Array Codes with Asymptotically Optimal Repair *Hanxu Hou, Patrick Pak-Ching Lee, Yunghsiang Han, Yuchong Hu*	Codes for Graph Erasures *Lev Yohananov, Eitan Yaakobi*
Tu1-2: Polar Codes 1 Chair: Ilya Dumer			**Brussels**
Fast Polarization for Non-Stationary Channels *Hessam Mahdavifar*	A Lower Bound on the Probability of Error of Polar Codes over BMS Channels *Boaz Shuval, Ido Tal*	On the Pointwise Threshold Behavior of the Binary Erasure Polarization Subchannels *Erik Ordentlich, Ron Roth*	Exploiting Source Redundancy to Improve the Rate of Polar Codes *Ying Wang, Krishna Narayanan, Anxiao Andrew Jiang*
Tu1-3: Multiple Access 2 Chair: Abbas El Gamal			**K2**
Outer Bounds for Gaussian Multiple Access Channels with State Known at One Encoder *Wei Yang, Yingbin Liang, Shlomo (Shitz) Shamai, H. Vincent Poor*	Homologous Codes for Multiple Access Channels *Pinar Sen, Young-Han Kim*	An Achievable Error Exponent for the Multiple Access Channel with Correlated Sources *Arezou Rezazadeh, Josep Font-Segura, Alfonso Martinez, Albert Guillén i Fàbregas*	A Broadcast Approach to Multiple Access Adapted to the Multiuser Channel *Samia Kazemi, Ali Tajer*
Tu1-4: Information Measures Chair: Thomas Courtade			**K3**
On the Information Dimension Rate of Stochastic Processes *Bernhard Geiger, Tobias Koch*	A Variational Characterization of Rényi Divergences *Venkat Anantharam*	A de Bruijn identity for discrete random variables *Oliver Johnson, Saikat Guha*	Direct Estimation of Information Divergence Using Nearest Neighbor Ratios *Morteza Noshad, Kevin Moon, Salimeh Yasaei Sekeh, Alfred Hero III*
Tu1-5: Joint Source-Channel Coding 1 Chair: Aaron Wagner			**K4**
Expurgated Joint Source-Channel Coding Bounds and Error Exponents *Jonathan Scarlett, Alfonso Martinez, Albert Guillén i Fàbregas*	Graph Information Ratio *Lele Wang, Ofer Shayevitz*	Second Order Analysis for Joint Source-Channel Coding with Markovian Source *Ryo Yaguchi, Masahito Hayashi*	On the Necessary Conditions for Transmitting Correlated Sources over a Multiple Access Channel *Basak Guler, Deniz Gündüz, Aylin Yener*
Tu1-6: Strong Converses Chair: Shun Watanabe			**K5**
Strong Converse for Content Identification with Lossy Recovery *Lin Zhou, Vincent Tan, Mehul Motani*	Strong Converse Theorems for Discrete Memoryless Networks with Tight Cut-Set Bound *Silas Fong, Vincent Tan*	Reverse hypercontractivity region for the binary erasure channel *Chandra Nair, Yan Nan Wang*	Beyond the Blowing-Up Lemma: Sharp Converses via Reverse Hypercontractivity *Jingbo Liu, Ramon van Handel, Sergio Verdú*
Tu1-7: Crypto 1 Chair: Matthieu Bloch			**K6**
An Information-theoretic Approach to Hardness Amplification *Ueli Maurer*	Witness-Hiding Proofs of Knowledge for Cable Locks *Chen-Da Liu Zhang, Ueli Maurer, Martin Raszyk, Daniel Tschudi*	Privacy Amplification of Distributed Encrypted Sources with Correlated Keys *Bagus Santoso, Yasutada Oohama*	
Tu1-8: Wireless Communication Chair: Yingbin Liang			**K7+8**
Can Full-Duplex More than Double the Capacity of Wireless Networks? *Serj Haddad, Ayfer Özgür, Emre Telatar*	Short-Message Communication and FIR System Identification using Huffman Sequences *Philipp Walk, Peter Jung, Babak Hassibi*	Novel Construction Methods of Quaternion Orthogonal Designs based on Complex Orthogonal Designs *Erum Mushtaq, Sajid Ali, Syed Ali Hassan*	
Tu1-9: Hypothesis Testing 2 Chair: Yanina Shkel			**K9**
Hypothesis Test for Upper Bound on the Size of Random Defective Set *Arkadii Dyachkov, Ilya Vorobyev, Nikita Polyanskii, Vladislav Shchukin*	Distributed Hypothesis Testing Over Noisy Channels *Sreejith Sreekumar, Deniz Gündüz*	Linear-Complexity Exponentially-Consistent Tests for Universal Outlying Sequence Detection *Yuheng Bu, Shaofeng Zou, Venugopal Veeravalli*	Active Hypothesis Testing on A Tree: Anomaly Detection under Hierarchical Observations *Chao Wang, Kobi Cohen, Qing Zhao*

Tuesday, June 27 — 11:30-12:50

11:30	11:50	12:10	12:30
Tu2-1: Coding Techniques 2 Chair: Alexander Barg			Europa
Fractional decoding: Error correction from partial information *Itzhak Tamo, Min Ye, Alexander Barg*	Performance of Optimal Data Shaping Codes *Yi Liu, Pengfei Huang, Paul Siegel*	Multilevel Code Construction for Compound Fading Channels *Antonio Campello, Ling Liu, Cong Ling*	Dense Gray Codes in Mixed Radices *Jessica Fan, Thomas Cormen*
Tu2-2: Locally Repairable Codes 2 Chair: Antonia Tulino			Brussels
Balanced and Sparse Tamo-Barg Codes *Wael Halbawi, Iwan Duursma, Hoang Dau, Babak Hassibi*	Bounds and Constructions of Codes with All-Symbol Locality and Availability *Stanislav Kruglik, Alexey Frolov*	Security for Minimum Storage Regenerating Codes and Locally Repairable Codes *Swanand Kadhe, Alex Sprintson*	
Tu2-3: Broadcast Channels 2 Chair: Vincent Tan			K2
The Arbitrarily Varying Degraded Broadcast Channel with Causal Side Information at the Encoder *Uzi Pereg, Yossef Steinberg*	Sub-optimality of superposition coding region for three receiver broadcast channel with two degraded message sets *Mehdi Yazdanpanah, Chandra Nair*	The Broadcast Channel with Degraded Message Sets and Unreliable Conference *Dor Itzhak, Yossef Steinberg*	On the Capacity Region of the K-User Discrete Memoryless Broadcast Channel with Two Degraded Messages *Mahesh Varanasi, Mohamed Salman*
Tu2-4: Channel Capacity 2 Chair: Amos Lapidoth			K3
The Optimal Exponent Function for the Additive White Gaussian Noise Channel at Rates above the Capacity *Yasutada Oohama*	A Generalized Ozarow-Wyner Capacity Bound with Applications *Alex Dytso, Mario Goldenbaum, H. Vincent Poor, Shlomo (Shitz) Shamai*	A Bound on the Shannon Capacity via a Linear Programming Variation *Sihuang Hu, Itzhak Tamo, Ofer Shayevitz*	On the Discreteness of Capacity-Achieving Distributions for the Censored Channel *Arash Behboodi, Gholamreza Alirezaei, Rudolf Mathar*
Tu2-5: Massive MIMO Chair: Christoph Studer			K4
Massive Device Connectivity with Massive MIMO *Liang Liu, Wei Yu*	On the MISO Channel with Feedback: Can Infinitely Massive Antennas Achieve Infinite Capacity? *Jinyuan Chen*	The BOX-LASSO with Application to GSSK Modulation in Massive MIMO Systems *Ismail Ben Atitallah, Christos Thrampoulidis, Abla Kammoun, Tareq Y. Al-Naffouri, Mohamed-Slim Alouini, Babak Hassibi*	Multi-Users Space-Time Modulation with QAM Division for Massive Uplink Communications *Jian-Kang Zhang, Zheng Dong*
Tu2-6: MIMO 2 Chair: Vasanthan Raghavan			K5
Generalized Degrees-of-Freedom of the 2-User Case MISO Broadcast Channel with Distributed CSIT *Antonio Bazco, Paul de Kerret, David Gesbert, Nicolas Gresset*	Spatially Correlated MIMO Broadcast Channel: Analysis of Overlapping Correlation Eigenspaces *Fan Zhang, Mohamed Fadel, Aria Nosratinia*	On the Achievable Rates of Decentralized Equalization in Massive MU-MIMO Systems *Charles Jeon, Kaipeng Li, Joseph Cavallaro, Christoph Studer*	V-BLAST in Lattice Reduction and Integer Forcing *Sebastian Stern, Robert Fischer*
Tu2-7: Energy Harvesting 2 Chair: Deniz Gündüz			K6
Energy-Based Adaptive Multiple Access in LPWAN IoT Systems with Energy Harvesting *Nicolò Michelusi, Marco Levorato*	Near Optimal Online Distortion Minimization for Energy Harvesting Nodes *Ahmed Arafa, Sennur Ulukus*	Scheduling Status Updates to Minimize Age of Information with an Energy Harvesting Sensor *Tan Bacinoglu, Elif Uysal-Biyikoglu*	Code Design for Binary Energy Harvesting Channel *Mehdi Dabirnia, Tolga Duman*
Tu2-8: Compressed Sensing 2 Chair: Tara Javidi			K7+8
A Greedy Blind Calibration Method for Compressed Sensing with Unknown Sensor Gains *Valerio Cambareri, Amirafshar Moshtaghpour, Laurent Jacques*	Information-theoretic bounds and phase transitions in clustering, sparse PCA, and submatrix localization *Jess Banks, Cristopher Moore, Roman Vershynin, Nicolas Verzelen, Jiaming Xu*	Almost Optimal Phaseless Compressed Sensing with Sublinear Decoding Time *Vasileios Nakos*	A Characterization of Sampling Patterns for Low-Rank Multi-View Data Completion Problem *Morteza Ashraphijuo, Xiaodong Wang, Vaneet Aggarwal*
Tu2-9: Source Coding 2 Chair: Ertem Tuncel			K9
Coding of Binary AIFV Code Trees *Kentaro Sumigawa, Hirosuke Yamamoto*	Universal lossy compression under logarithmic loss *Yanina Shkel, Maxim Raginsky, Sergio Verdú*	Towards Optimal Quantization of Neural Networks *Avhishek Chatterjee, Lav Varshney*	Stochastic Stability of Non-Markovian Processes and Adaptive Quantizers *Serdar Yüksel*

Tuesday, June 27 14:40-16:20

14:40	15:00	15:20	15:40	16:00
Tu3-1: Network Coding 1 Chair: Tuvi Etzion				**Europa**
Secrecy and Robustness for Active Attack in Secure Network Coding *Masahito Hayashi, Masaki Owari, Go Kato, Ning Cai*	Linear Network Coding for Two-Unicast-Z Networks: A Commutative Algebraic Perspective and Fundamental Limits *Mohammad Fahim, Viveck Cadambe*	Network-Coded Fronthaul Transmission for Cache-Aided C-RAN *Tian Ding, Xiaojun Yuan, Soung Chang Liew*	Optimal Secondary Access in Retransmission based Primary Networks via Chain Decoding *Nicolò Michelusi*	
Tu3-2: LDPC Codes 2 Chair: Khaled Abdel-Ghaffar				**Brussels**
Characterization and Efficient Exhaustive Search Algorithm for Elementary Trapping Sets of Irregular LDPC Codes *Yoones Hashemi Toroghi, Amir Banihashemi*	An Adaptive EMS Algorithm for Nonbinary LDPC Codes *Youngjun Hwang, Sunghye Cho, Kyeongcheol Yang*	A Two-Stage Decoding Algorithm for Short Nonbinary LDPC Codes with Near-ML Performance *Dixia Deng, Hengzhou Xu, Baoming Bai, Ji Zhang*	Design of Improved Quasi-Cyclic Protograph-Based Raptor-Like LDPC Codes for Short Block-Lengths *Sudarsan Vasista Srinivasan Ranganathan, Dariush Divsalar, Richard Wesel*	Finite-Length LDPC Codes on the q-ary Multi-Bit Channel *Rami Cohen, Yuval Cassuto*
Tu3-3: Caching 2 Chair: Bobak Nazer				**K2**
Online Edge Caching in Fog-Aided Wireless Networks *Seyyed Mohammadreza Azimi, Osvaldo Simeone, Avik Sengupta, Ravi Tandon*	Benefits of Cache Assignment on Degraded Broadcast Channels *Shirin Saeedi Bidokhti, Michele Wigger, Aylin Yener*	Rate-Memory Trade-off for the Two-User Broadcast Caching Network with Correlated Sources *Parisa Hassanzadeh, Antonia Tulino, Jaime Llorca, Elza Erkip*	On the Optimality of Separation between Caching and Delivery in General Cache Networks *Navid Naderializadeh, Mohammad Ali Maddah-Ali, Salman Avestimehr*	
Tu3-4: Second Order Chair: Giuseppe Durisi				**K3**
Dispersion of the Discrete Arbitrarily-Varying Channel with Limited Shared Randomness *Oliver Kosut, Joerg Kliewer*	On the calculation of the minimax-converse of the channel coding problem *Nir Elkayam, Meir Feder*	Exact Moderate Deviation Asymptotics in Streaming Data Transmission *Si-Hyeon Lee, Vincent Tan, Ashish Khisti*	Infinite Dispersion in Bursty Communication *Longguang Li, Aslan Tchamkerten*	Achievable Moderate Deviations Asymptotics for Streaming Slepian-Wolf Coding *Lin Zhou, Vincent Tan, Mehul Motani*
Tu3-5: Detection and Estimation 2 Chair: Jing Yang				**K4**
Demystifying Fixed k-Nearest Neighbor Information Estimators *Weihao Gao, Sewoong Oh, Pramod Viswanath*	Structure of optimal strategies for remote estimation over Gilbert-Elliott channel with feedback *Jhelum Chakravorty, Aditya Mahajan*	Sparse Gaussian Mixture Detection: Low Complexity, High Performance Tests via Quantization *Jonathan Ligo, George Moustakides, Venugopal Veeravalli*	Compressive Estimation of a Stochastic Process with Unknown Autocorrelation Function *Mahdi Barzegar Khalilsarai, Saeid Haghighatshoar, Giuseppe Caire, Gerhard Wunder*	Robust sequential change-point detection by convex optimization *Yang Cao, Yao Xie*
Tu3-6: Sequences 1 Chair: Prakash Narayan				**K5**
Perfect polyphase sequences from cubic polynomials *Min Kyu Song, Hong-Yeop Song*	Bayesian definition of random sequences with respect to conditional probabilities *Hayato Takahashi*	On the Correlation between Boolean Functions of Sequences of Random Variables *Farhad Shirani, Sandeep Pradhan*	The Hybrid k-Deck Problem: Reconstructing Sequences from Short and Long Traces *Ryan Gabrys, Olgica Milenkovic*	
Tu3-7: Communications 2 Chair: Tobias Koch				**K6**
Reliability of Universal Decoding Based on Vector–Quantized Codewords *Neri Merhav*	Sample Complexity of the Boolean Multireference Alignment Problem *Joao Pereira, Amit Singer, Emmanuel Abbe*	On the optimality of treating interference as noise in the 2 x M LD X-channel *Soheil Gherekhloo, Yasemin Karacora, Aydin Sezgin*	Interaction Information for Causal Inference: The Case of Directed Triangle *AmirEmad Ghassami, Negar Kiyavash*	Completely blind sensing of multi-band signals *Taehyung Lim, Massimo Franceschetti*
Tu3-8: Information Theory and Statistics 1 Chair: Pierre Moulin				**K7+8**
An Information-Theoretic Approach to Universal Feature Selection in High-Dimensional Inference *Shao-Lun Huang, Anuran Makur, Lizhong Zheng, Gregory Wornell*	Identifying Nonlinear 1-Step Causal Influences in Presence of Latent Variables *Saber Salehkaleybar, Jalal Etesami, Negar Kiyavash*	Closed-Form Moments of Finite-Dimension Non-central Wishart Matrices via Concentration of Spectral Measure *Xinmin Li, Ling Qiu*	Information-geometrical characterization of statistical models which are statistically equivalent to probability simplexes *Hiroshi Nagaoka*	Density Functional Estimators with k-Nearest Neighbor Bandwidths *Weihao Gao, Sewoong Oh, Pramod Viswanath*
Tu3-9: Machine Learning 1 Chair: Toshiyuki Tanaka				**K9**
Energy decay and conservation in deep convolutional neural networks *Philipp Grohs, Thomas Wiatowski, Helmut Bölcskei*	Neural Offset Min-Sum Decoding *Loren Lugosch, Warren Gross*	Learning-Based Epsilon Most Stringent Test for Gaussian Samples Classification *Lionel Fillatre, Igor Nikiforov*	Quickest Search and Learning over Multiple Sequences *Javad Heydari, Ali Tajer*	Minimax Lower Bounds for Ridge Combinations Including Neural Nets *Jason Klusowski, Andrew Barron*

Tuesday, June 27 — 16:40-18:20

16:40	17:00	17:20	17:40	18:00
Tu4-1: Coding Theory 2 Chair: Emina Soljanin				**Europa**
Pseudo-Wigner Matrices from Dual BCH Codes *Ilya Soloveychik, Yu Xiang, Vahid Tarokh*	On codes achieving zero error capacities in limited magnitude error channels *Bella Bose, Noha Elarief, Luca Tallini*	On the Capacities of Balanced Codes with Run-Length Constraints *Akiko Manada, Hiroyoshi Morita*	Geometric Orthogonal Codes Better than Optical Orthogonal Codes *Yeow Meng Chee, Han Mao Kiah, San Ling, Hengjia Wei*	The Augustin Center and The Sphere Packing Bound For Memoryless Channels *Baris Nakiboglu*
Tu4-2: Coding for Distributed Storage 1 Chair: Vitaly Skachek				**Brussels**
Secrecy Capacity of Minimum Storage Regenerating Codes *Ankit Singh Rawat*	Cooperative Data Exchange based on MDS codes *Su Li, Michael Gastpar*	Asymptotically Optimal Regenerating Codes Over Any Field *Netanel Raviv*	Private Information Retrieval in Distributed Storage Systems Using an Arbitrary Linear Code *Siddhartha Kumar, Eirik Rosnes, Alexandre Graell i Amat*	
Tu4-3: Interference Channels 2 Chair: Changho Suh				**K2**
Nash Region of the Linear Deterministic Interference Channel with Noisy Output Feedback *Victor Quintero, Samir Perlaza, Jean-Marie Gorce, H. Vincent Poor*	Characterization of Degrees of Freedom versus Receivers Backhaul Load in K-User Interference Channel *Borna Kananian, Mohammad Ali Maddah-Ali, Seyed Pooya Shariatpanahi, Babak Hossein Khalaj*	Discrete Modulation for Interference Mitigation *Mirza Uzair Baig, Anders Høst-Madsen, Aria Nosratinia*	Communicating Correlated Sources Over an Interference Channel *Arun Padakandla*	Topological Interference Management: Linear Cooperation is not useful for Wyner's Networks *Aly El Gamal*
Tu4-4: Entropy 2 Chair: Stefan Moser				**K3**
Urns and entropies revisited *František Matúš*	Metric and topological entropy bounds on state estimation for stochastic nonlinear systems *Christoph Kawan, Serdar Yüksel*	Playing Games with Bounded Entropy *Mehrdad Valizadeh, Amin Gohari*	Entropic Causality and Greedy Minimum Entropy Coupling *Murat Kocaoglu, Alexandros Dimakis, Sriram Vishwanath, Babak Hassibi*	On Structural Entropy of Uniform Random Intersection Graphs *Marcin Kardas, Zbigniew Golebiewski, Jakub Lemiesz, Krzysztof Majcher*
Tu4-5: Bounds 2 Chair: Viveck Cadambe				**K4**
Dependence Measures Bounding the Exploration Bias for General Measurements *Jiantao Jiao, Yanjun Han, Tsachy Weissman*	Binary Subblock Energy-Constrained Codes: Bounds on Code Size and Asymptotic Rate *Anshoo Tandon, Han Mao Kiah, Mehul Motani*	Sampled Graph-Signals: Iterative Recovery with an Analytic Error Bound *Norbert Goertz*	Multidimensional Semiconstrained Systems *Ohad Elishco, Tom Meyerovitch, Moshe Schwartz*	Variable-length codes for channels with memory and feedback: error-exponent lower bounds *Achilleas Anastasopoulos, Jui Wu*
Tu4-6: Sequences 2 Chair: Yossef Steinberg				**K5**
On Empirical Cumulant Generating Functions of Code Lengths for Individual Sequences *Neri Merhav*	Degree-(k + 1) Perfect Gaussian Integer Sequences of Period p^k *Ho-Hsuan Chang*	Reconstruction of Sequences over Non-Identical Channels *Michal Horovitz, Eitan Yaakobi*	Classification of a Sequence Family Using Plateaued Functions *Serdar Boztas, Ferruh Ozbudak, Eda Tekin*	
Tu4-7: Security 2 Chair: Arya Mazumdar				**K6**
Secret Key Agreement under Discussion Rate Constraints *Chung Chan, Manuj Mukherjee, Navin Kashyap, Qiaoqiao Zhou*	A Game Theoretic Treatment for Pair-wise Secret-Key Generation in Many-to-One Networks *Remi Chou, Aylin Yener*	Information-Theoretically Secure Key Generation and Management *Xin-Wen Wu, En-hui Yang*	Secret-Key Agreement with Public Discussion over Multi-Antenna Transmitters with Amplitude Constraints *Zouheir Rezki, Mohamed-Slim Alouini*	Robust and Secure Identification *Holger Boche, Christian Deppe*
Tu4-8: Quantum IT 2 Chair: Joseph Renes				**K7+8**
Moderate deviation analysis for classical communication over quantum channels *Christopher Chubb, Vincent Tan, Marco Tomamichel*	Quantum Information on Spectral Sets *Peter Harremoës*	Kolmogorov Amplification from Bell Correlation *Ämin Baumeler, Charles Alexandre Bédard, Gilles Brassard, Stefan Wolf*	Degradable states and one-way entanglement distillation *Felix Leditzky, Nilanjana Datta, Graeme Smith*	
Tu4-9: Compression 1 Chair: Faramarz Fekri				**K9**
Recovery of Vertex Orderings in Dynamic Graphs *Abram Magner, Ananth Grama, Jithin Sreedharan, Wojciech Szpankowski*	Variable-Length Lossy Compression Allowing Positive Overflow and Excess Distortion Probabilities *Shota Saito, Hideki Yagi, Toshiyasu Matsushima*	On Lossy Compression of Binary Matrices *Ronit Bustin, Ofer Shayevitz*	Universal Lossless Compression of Graphical Data *Payam Delgosha, Venkat Anantharam*	Compressing data on graphs with clusters *Amir Asadi, Emmanuel Abbe, Sergio Verdú*

Wednesday, June 28 09:50-11:10

9:50	10:10	10:30	10:50
We1-1: Iterative Decoding 1 Chair: Albert Guillén i Fàbregas			**Europa**
Vector Approximate Message Passing *Sundeep Rangan, Philip Schniter, Alyson Fletcher*	Generalized Approximate Message-Passing Decoder for Universal Sparse Superposition Codes *Erdem Biyik, Jean Barbier, Mohamad Dia*	Block Markov Superposition Transmission of BCH Codes with Iterative Hard-decision Decoding *Nina Lin, Suihua Cai, Xiao Ma*	Belief Propagation for Subgraph Detection with Imperfect Side-information *Arun Kadavankandy, Konstantin Avrachenkov, Laura Cottatellucci, Rajesh Sundaresan*
We1-2: Student Paper Awards Candidate Talks 1 Chair: Wei Yu			**Brussels**
Multiplexing Zero-Error and Rare-Error Communications over a Noisy Channel with Feedback *Tibor Keresztfalvi, Amos Lapidoth*	The Exact Rate-Memory Tradeoff for Caching with Uncoded Prefetching *Qian Yu, Mohammad Ali Maddah-Ali, Salman Avestimehr*	Greedy-Merge Degrading has Optimal Power-Law *Assaf Kartowsky, Ido Tal*	A Generic Transformation for Optimal Repair Bandwidth and Rebuilding Access in MDS Codes *Jie Li, Xiaohu Tang, Chao Tian*
We1-3: Coding for Storage and Streaming Chair: Ashish Khisti			**K2**
Multipermutation Ulam Sphere Analysis Toward Characterizing Maximal Code Size *Justin Kong, Manabu Hagiwara*	Multiplexed FEC for Multiple Streams with Different Playout Deadlines *Ahmed Badr, Devin Lui, Ashish Khisti, Wai-Tian Tan, Xiaoqing Zhu, John Apostolopoulos*	A Code Equivalence between Streaming Network Coding and Streaming Index Coding *Ming Fai Wong, Michelle Effros, Michael Langberg*	On the error probability of stochastic decision and stochastic decoding *Jun Muramatsu, Shigeki Miyake*
We1-4: Zero Error Capacity Chair: Alon Orlitsky			**K3**
The Birthday Problem and Zero-Error List Codes *Parham Noorzad, Michelle Effros, Michael Langberg, Victoria Kostina*	The Zero-Error Capacity of a Collision Channel With Successive Interference Cancellation *Yijin Zhang, Yi Chen, Yuan-Hsun Lo, Wing Shing Wong*	An improved bound on the zero-error list-decoding capacity of the 4/3 channel *Marco Dalai, Venkatesan Guruswami, Jaikumar Radhakrishnan*	
We1-5: Joint Source-Channel Coding 2 Chair: Sandeep Pradhan			**K4**
Dependence Balance in Multiple Access Channels with Correlated Sources *Amos Lapidoth, Shirin Saeedi Bidokhti, Michele Wigger*	On Minimum Energy for Robust Gaussian Joint Source-Channel Coding with a Distortion-Noise Profile *Erman Köken, Ertem Tuncel*	Communicating Correlated Sources Over a MAC *Arun Padakandla*	
We1-6: Spatial Coupling Chair: Laurent Schmalen			**K5**
Spatially Coupled LDLC: New Constructions *Svetlana Reznikov, Meir Feder*	A Protograph-Based Design of Quasi-Cyclic Spatially Coupled LDPC Codes *Li Chen, Shiyuan Mo, Daniel Costello, David Mitchell, Roxana Smarandache*	Complexity-Optimized Concatenated LDGM-Staircase Codes *Lei Zhang, Frank Kschischang*	A Novel Combinatorial Framework to Construct Spatially-Coupled Codes: Minimum Overlap Partitioning *Homa Esfahanizadeh, Ahmed Hareedy, Lara Dolecek*
We1-7: Security 3 Chair: Salim El Rouayheb			**K6**
Secure wireless communication under spatial and local Gaussian noise assumptions *Masahito Hayashi*	The Degraded Gaussian Multiple Access Wiretap Channel with Selfish Transmitters: A Coalitional Game Theory Perspective *Remi Chou, Aylin Yener*	MIMO Gaussian Wiretap Channels with Two Transmit Antennas: Optimal Precoding and Power Allocation *Mojtaba Vaezi, Wonjae Shin, H. Vincent Poor, Jungwoo Lee*	Computation of the Random Coding Secrecy Exponent for a Constant Composition Ensemble *Yutaka Jitsumatsu*
We1-8: Quantum IT 3 Chair: Min-Hsiu Hsieh			**K7+8**
Codes for Simultaneous Transmission of Quantum and Classical Information *Markus Grassl, Sirui Lu, Bei Zeng*	Belief propagation decoding of quantum channels by passing quantum messages *Joseph Renes*	Semidefinite programming converse bounds for classical communication over quantum channels *Xin Wang, Wei Xie, Runyao Duan*	On the Feasibility Conditions of Quantum State Discrimination *Chung-Chin Lu, Shiuan-Hao Kuo*
We1-9: Source Coding 3 Chair: Charalambos Charalambous			**K9**
An Information-Theoretic Analysis of Deduplication *Urs Niesen*	Extended Gray-Wyner System with Complementary Causal Side Information *Cheuk Ting Li, Abbas El Gamal*	Variable-Length Resolvability for General Sources *Hideki Yagi, Te Sun Han*	Universal Tree Source Coding Using Grammar-Based Compression *Markus Lohrey, Danny Hucke*

Wednesday, June 28 11:30-12:30

11:30	11:50	12:10
We2-1: Coding Techniques (Focus Session) Chair: Irina Bocharova		**Europa**
Multi-Block Interleaved Codes for Local and Global Read Access *Yuval Cassuto, Evyatar Hemo, Sven Puchinger, Martin Bossert*	Successive Cancellation Decoding of Single Parity-Check Product Codes *Mustafa Coşkun, Gianluigi Liva, Alexandre Graell i Amat, Michael Lentmaier*	Codes for Channels With Segmented Edits *Mahed Abroshan, Ramji Venkataramanan, Albert Guillén i Fàbregas*
We2-2: Student Paper Awards Candidate Talks 2 Chair: Elza Erkip		**Brussels**
A High-SNR Normal Approximation for Single-Antenna Rayleigh Block-Fading Channels *Alejandro Lancho, Tobias Koch, Giuseppe Durisi*	A Tight Rate Bound and a Matching Construction for Locally Recoverable Codes with Sequential Recovery From Any Number of Multiple Erasures *Balaji Srinivasan Babu, Ganesh Kini, P Vijay Kumar*	Feedback Capacity and Coding for the (0,k)-RLL Input-Constrained BEC *Ori Peled, Oron Sabag, Haim Permuter*
We2-3: Crypto (Focus Session) Chair: Natasa Zivic		**K2**
Efficiency Lower Bounds for Commit-and-Prove Constructions *Chen-Da Liu Zhang, Christian Badertscher, Sandro Coretti, Ueli Maurer*	Information Set Decoding with Soft Information and some cryptographic applications *Qian Guo, Thomas Johansson, Erik Mårtensson, Paul Stankovski*	Statistical Decoding *Thomas Debris-Alazard, Jean-Pierre Tillich*
We2-4: Security (Focus Session) Chair: Andrew Thangaraj		**K3**
Security of Helper Data Schemes for SRAM-PUF in Multiple Enrollment Scenarios *Lieneke Kusters, Tanya Ignatenko, Frans Willems, Roel Maes, Erik van der Sluis, Georgios. Selimis*	New Models for Interference and Broadcast Channels with Confidential Messages *Mohamed Nafea, Aylin Yener*	Secret Sharing with Optimal Decoding and Repair Bandwidth *Wentao Huang, Jehoshua Bruck*
We2-5: Network Information Theory (Focus Session) Chair: Anthony Ephremides		**K5**
Towards an Algebraic Network Information Theory: Simultaneous Joint Typicality Decoding *Sung Hoon Lim, Chen Feng, Adriano Pastore, Bobak Nazer, Michael Gastpar*	On the Sub-optimality of Single-letter Coding in Multi-terminal Communications *Farhad Shirani, Sandeep Pradhan*	Coordination with Clustered Common Randomness in a Three-Terminal Line Network *Ishaque Ashar Kadampot, Matthieu Bloch*
We2-P: Recent Results Posters Chair: Anke Schmeink		**Foyer Brussels**

Wednesday, June 28 12:45-13:45

We3-1: Awards Session Chair: Ruediger Urbanke — **Europa**

Wednesday, June 28 Afternoon

Social Events

Thursday, June 29 09:50-11:10

9:50	10:10	10:30	10:50
Th1-1: Lattice Codes 1 Chair: Stark Draper			**Europa**
Capacity Optimality of Lattice Codes in Common Message Gaussian Broadcast Channels with Coded Side Information *Lakshmi Natarajan, Yi Hong, Emanuele Viterbo*	On the Communication Cost of Determining an Approximate Nearest Lattice Point *Maiara Bollauf, Vinay Vaishampayan, Sueli Costa*	Communication Cost of Transforming a Nearest Plane Partition to the Voronoi Partition *Vinay Vaishampayan, Maiara Bollauf*	Compute-and-Forward over Block-Fading Channels Using Algebraic Lattices *Shanxiang Lyu, Antonio Campello, Cong Ling, Jean-Claude Belfiore*
Th1-2: Polar Codes 2 Chair: Ruediger Urbanke			**Brussels**
Construction of Polar Codes with Sublinear Complexity *Marco Mondelli, Hamed Hassani, Ruediger Urbanke*	On the Error Probability of Short Concatenated Polar and Cyclic Codes with Interleaving *Giacomo Ricciutelli, Marco Baldi, Franco Chiaraluce, Gianluigi Liva*	A Randomized Construction of Polar Subcodes *Peter Trifonov, Grigorii Trofimiuk*	On Design of CRC Codes for Polar Codes with Successive Cancellation List Decoding *Takumi Murata, Hideki Ochiai*
Th1-3: Broadcast Channels 3 Chair: Shlomo (Shitz) Shamai			**K2**
Block-fading Broadcast Channel with Hybrid CSIT and CSIR *Mohamed Fadel, Aria Nosratinia*	Application of Yamamoto-Itoh Coding Scheme to Discrete Memoryless Broadcast Channels *Hirosuke Yamamoto, Shintaro Hara*	Coding Across Heterogeneous Parallel Erasure Broadcast Channels is Useful *Sunghyun Kim, Soheil Mohajer, Changho Suh*	Rate Splitting and Superposition Coding for Concurrent Groupcasting over the Broadcast Channel: A General Framework *Henry Romero, Mahesh Varanasi*
Th1-4: Private Information Retrieval Chair: Michael Gastpar			**K3**
Private Information Retrieval from MDS Coded Data with Colluding Servers: Settling a Conjecture by Freij-Hollanti et al *Hua Sun, Syed Jafar*	Multi-Message Private Information Retrieval *Karim Banawan, Sennur Ulukus*	Robust Private Information Retrieval on Coded Data *Razane Tajeddine, Salim El Rouayheb*	Private Information Retrieval Schemes for Coded Data with Arbitrary Collusion Patterns *Razane Tajeddine, Oliver Gnilke, David Karpuk, Ragnar Freij-Hollanti, Camilla Hollanti, Salim El Rouayheb*
Th1-5: Rate Distortion Theory 2 Chair: Tsachy Weissman			**K4**
A Distortion Based Approach for Protecting Inferences *Chi-Yo Tsai, Gaurav Kumar Agarwal, Christina Fragouli, Suhas Diggavi*	Rate-Distortion Regions of Instances of Cascade Source Coding with Side Information *Chien-Yi Wang, Abdellatif Zaidi*	The Rate-Distortion Function for Successive Refinement of Abstract Sources *Victoria Kostina, Ertem Tuncel*	Rate-Distortion Tradeoffs under Kernel-Based Distortion Measures *Kazuho Watanabe*
Th1-6: Coding for Insertion and Deletion Channels 1 Chair: Joseph Jean Boutros			**K5**
Coding for the Permutation Channel with Insertions, Deletions, Substitutions, and Erasures *Mladen Kovačević, Vincent Tan*	Perfect Codes for Single Balanced Adjacent Deletions *Manabu Hagiwara*	Timing-Drift Channel Model and Marker-Based Error Correction Coding *Haruhiko Kaneko*	Limits to List Decoding of Insertions and Deletions *Antonia Wachter-Zeh*
Th1-7: Security 4 Chair: Lifeng Lai			**K6**
The Gelfand-Pinsker wiretap channel: Higher secrecy rates via a novel superposition code *Ziv Goldfeld, Paul Cuff, Haim Permuter*	The Gaussian Multiple Access Wiretap Channel when the Eavesdropper can Arbitrarily Jam *Remi Chou, Aylin Yener*	Secrecy Capacity of the First-Order Autoregressive Moving Average Gaussian Channel with Feedback *Chong Li, Yingbin Liang*	Asymptotic Converse Bound for Secret Key Capacity in Hidden Markov Model *Mohammad Reza Khalili Shoja, George Amariucai, Zhengdao Wang, Shuangqing Wei, Jing Deng*
Th1-8: Quantum IT 4 Chair: Stefan Wolf			**K7+8**
Compression for quantum population coding *Yuxiang Yang, Ge Bai, Giulio Chiribella, Masahito Hayashi*	Moderate Deviations for Quantum Hypothesis Testing and a Martingale Inequality *Hao-Chung Cheng, Min-Hsiu Hsieh*	Classical-Quantum Arbitrarily Varying Wiretap Channel: Secret Message Transmission under Jamming Attacks *Minglai Cai, Holger Boche, Christian Deppe, Janis Noetzel*	Quantum Markov Chains and Logarithmic Trace Inequalities *David Sutter, Mario Berta, Marco Tomamichel*
Th1-9: Source Coding 4 Chair: Yasutada Oohama			**K9**
Distributed Task Encoding *Annina Bracher, Amos Lapidoth, Christoph Pfister*	Performance Limits on the Classification of Kronecker-structured Models *Ishan Jindal, Matthew Nokleby*	The Redundancy Gains of Almost Lossless Universal Source Coding over Envelope Families *Jorge Silva, Pablo Piantanida*	Universal Sampling Rate Distortion *Vinay Praneeth Boda, Prakash Narayan*

Thursday, June 29

11:30-12:50

11:30	11:50	12:10	12:30
Th2-1: Coding Techniques 3 Chair: Vladimir Sidorenko			**Europa**
Cooling Codes: Thermal-Management Coding for High-Performance Interconnects *Tuvi Etzion, Alexander Vardy, Yeow Meng Chee, Han Mao Kiah*	Recursive Block Markov Superposition Transmission of Short Codes *Shancheng Zhao, Qin Huang, Xiao Ma, Baoming Bai*	Complete Characterization of the Solvability of PAPR Reduction for OFDM by Tone Reservation *Holger Boche, Ullrich Mönich, Ezra Tampubolon*	Construction of q-ary Constant Weight Sequences using a Knuth-like Approach *Elie Ngomseu Mambou, Theo Swart*
Th2-2: Locally Repairable Codes 3 Chair: P Vijay Kumar			**Brussels**
Bounds and Constructions for Linear Locally Repairable Codes over Binary Fields *Anyu Wang, Zhifang Zhang, Dongdai Lin*	Locally Repairable Codes with Multiple (r_i, δ_i)-Localities *Bin Chen, Shutao Xia, Jie Hao*	epsilon-MSR Codes with Small Subpacketization *Ankit Singh Rawat, Itzhak Tamo, Venkatesan Guruswami, Klim Efremenko*	An Explicit, Coupled-Layer Construction of a High-Rate MSR Code with Low Sub-Packetization Level, Small Field Size and $d < (n-1)$ *Birenjith Sasidharan, Myna Vajha, P Vijay Kumar*
Th2-3: Multicell and Cloud Radio Chair: Salman Avestimehr			**K2**
An Upper Bound on the Sum Capacity of the Downlink Multicell Processing with Finite Backhaul Capacity *Tianyu Yang, Nan Liu, Wei Kang, Shlomo (Shitz) Shamai*	Capacity Bounds on the Downlink of Symmetric, Multi-Relay, Single Receiver C-RAN Networks *Shirin Saeedi Bidokhti, Gerhard Kramer, Shlomo (Shitz) Shamai*	On the Capacity of Cloud Radio Access Networks *Shouvik Ganguly, Young-Han Kim*	On the Capacity of Cloud Radio Access Networks with Oblivious Relaying *Inaki Estella, Abdellatif Zaidi, Giuseppe Caire, Shlomo (Shitz) Shamai*
Th2-4: Channel Capacity 3 Chair: Muriel Médard			**K3**
Intrinsic Capacity *Shengtian Yang, Rui Xu, Jun Chen, Jian-Kang Zhang*	Gaussian Channels with Minimum Amplitude Constraints: When is Optimal Input Binary? *Zhengwei Ni, Mehul Motani*	On the Achievable Rate of Bandlimited Continuous-Time 1-Bit Quantized AWGN Channels *Sandra Bender, Meik Dörpinghaus, Gerhard Fettweis*	Single-Bit Quantization of Binary-Input, Continuous-Output Channels *Brian Kurkoski, Hideki Yagi*
Th2-5: Estimation 1 Chair: H. Vincent Poor			**K4**
Lower Bounds on Parameter Modulation-Estimation Under Bandwidth Constraints *Nir Weinberger, Neri Merhav*	Multi-Layer Generalized Linear Estimation *Andre Manoel, Florent Krzakala, Marc Mézard, Lenka Zdeborova*	Minimax Optimal Estimators for Additive Scalar Functionals of Discrete Distributions *Kazuto Fukuchi, Jun Sakuma*	I-MMSE relations in random linear estimation and a sub-extensive interpolation method *Jean Barbier, Nicolas Macris*
Th2-6: MIMO 3 Chair: Hamid Jafarkhani			**K5**
Multi-Antenna Coded Caching *Seyed Pooya Shariatpanahi, Giuseppe Caire, Babak Hossein Khalaj*	Optimally-Tuned Nonparametric Linear Equalization for Massive MU-MIMO Systems *Ramina Ghods, Charles Jeon, Gulnar Mirza, Arian Maleki, Christoph Studer*	Rate Bounds on 4-group fast decodable space-time code *Bharath Sethuraman*	
Th2-7: Security 5 Chair: Sidharth Jaggi			**K6**
Games on Linear Deterministic Channels with Eavesdroppers *Ruijie Xu, Hao Ge, Randall Berry*	A New Broadcast Wiretap Channel Model *Mohamed Nafea, Aylin Yener*	Secrecy-Reliability Tradeoff for Semi-Deterministic Wiretap Channels at Finite Blocklength *Wei Yang, Rafael Schaefer, H. Vincent Poor*	On Secure Asymmetric Multilevel Diversity Coding Systems *Congduan Li, Xuan Guang, Chee Wei Tan, Raymond W. Yeung*
Th2-8: Compressed Sensing 3 Chair: Tareq Y. Al-Naffouri			**K7+8**
Dynamical Functional Theory for Compressed Sensing *Burak Çakmak, Manfred Opper, Ole Winther, Bernard Fleury*	Compressed Sensing under Optimal Quantization *Alon Kipnis, Galen Reeves, Yonina Eldar, Andrea Goldsmith*	Noisy Tensor Completion for Tensors with a Sparse Canonical Polyadic Factor *Swayambhoo Jain, Alexander Gutierrez, Jarvis Haupt*	Compressed Sensing of Compressible Signals *Sajjad Beygi, Shirin Jalali, Arian Maleki, Urbashi Mitra*
Th2-9: Statistics 1 Chair: Andrew Barron			**K9**
Budget-Optimal Clustering via Crowdsourcing *Ravi Kiran Raman, Lav Varshney*	Universal Joint Image Clustering and Registration using Partition Information *Ravi Kiran Raman, Lav Varshney*	How to Find a Joint Probability Distribution of Minimum Entropy (almost) given the Marginals *Ferdinando Cicalese, Luisa Gargano, Ugo Vaccaro*	On the Fundamental Statistical Limit of Community Detection in Random Hypergraphs *Chung-Yi Lin, I Chien, I-Hsiang Wang*

Thursday, June 29 — 14:40-16:20

14:40 | 15:00 | 15:20 | 15:40 | 16:00

Th3-1: Coding Theory 3 — Chair: Antonia Wachter-Zeh — ⇒ Amsterdam ⇐

Multiset combinatorial batch codes
Hui Zhang, Eitan Yaakobi, Natalia Silberstein

Structured Spherical Codes With Asymptotically Optimal Distance Distributions
Robert Taylor, Lamine Mili, Amir Zaghloul

Weight Spectrum of Quasi-Perfect Binary Codes with Distance 4
Valentin Afanassiev, Alexander Davydov

Kronecker Product and Tiling of Permutation Arrays for Hamming Distances
Sergey Bereg, Luis Gerardo Mojica de la Vega, Linda Morales, I. Hal Sudborough

Performance of Spinal Codes with Sliding Window Decoding
Weiqiang Yang, Ying Li, Xiaopu Yu

Th3-2: Coding for Distributed Storage 2 — Chair: Joerg Kliewer — Brussels

Secure Regenerating Codes for Hybrid Cloud Storage Systems
Islam Samy, Gokhan Calis, O. Ozan Koyluoglu

Centralized Multi-Node Repair for Minimum Storage Regenerating Codes
Marwen Zorgui, Zhiying Wang

GDSP: A Graphical Perspective on the Distributed Storage Systems
Saeid Sahraei, Michael Gastpar

Distributed Storage Allocation for Multi-Class Data
Koosha Pourtahmasi Roshandeh, Moslem Noori, Masoud Ardakani, Chintha Tellambura

Th3-3: Relaying — Chair: Roy Yates — K2

The Capacity-distortion Function for Multihop Channels with State
Amir Salimi, Wenyi Zhang, Satish Vedantam, Urbashi Mitra

The Geometry of the Relay Channel
Xiugang Wu, Leighton Barnes, Ayfer Özgür

The CF-DF Approach for Relay Networks Based on Multiple Descriptions with the Shared Binning
Leila Ghabeli

Th3-4: Guessing — Chair: Neri Merhav — K3

Making Recommendations Bandwidth Aware
Linqi Song, Christina Fragouli

The Effect of Bias on the Guesswork of Hash Functions
Yair Yona, Suhas Diggavi

Guessing With Limited Memory
Wasim Huleihel, Salman Salamatian, Muriel Médard

Centralized vs Decentralized Multi-Agent Guesswork
Salman Salamatian, Ahmad Beirami, Asaf Cohen, Muriel Médard

Th3-5: Detection and Estimation 3 — Chair: Alfred Hero III — K4

Asymptotic Optimality of D-CuSum for Quickest Change Detection under Transient Dynamics
Shaofeng Zou, Georgios Fellouris, Venugopal Veeravalli

Sketched Covariance Testing: A Compression-Statistics Tradeoff
Gautam Dasarathy, Parikshit Shah, Richard Baraniuk

Error bounds for Bregman Denoising and Structured Natural Parameter Estimation
Amin Jalali, James Saunderson, Maryam Fazel, Babak Hassibi

On Random Sampling with Nodes Attraction: The Case of Gauss-Poisson Process
Flavio Zabini, Gianni Pasolini, Andrea Conti

Low-rank, Sparse and Line Constrained Estimation: Applications to Target Tracking and Convergence
Amr Elnakeeb, Urbashi Mitra

Th3-6: Multiple Access Feedback — Chair: Lalitha Sankar — K5

Two-User Downlink Non-Orthogonal Multiple Access with Limited Feedback
Xiaoyi Liu, Hamid Jafarkhani

Role of Feedback in Modulo-Sum Computation over Erasure Multiple-Access Channels
I-Hsiang Wang, Shih-Chun Lin, Yu-Chih Huang

On the Necessity of Structured Codes for Communications over MAC with Feedback
Mohsen Heidari Khoozani, Farhad Shirani, Sandeep Pradhan

On the Gaussian MAC with Stop-Feedback
Lan Truong, Vincent Tan

Th3-7: Communications 3 — Chair: Ralf Müller — K6

Probabilistic Shaping and Non-Binary Codes
Joseph Jean Boutros, Fanny Jardel, Cyril Measson

Successive Local and Successive Global Omniscience
Anoosheh Heidarzadeh, Alex Sprintson

Noncoherent Massive Space-Time Codes with PSK Modulation for Uplink Network Communications
Jian-Kang Zhang, Shuangzhi Li, Xiaomin Mu

FPLinQ: A Cooperative Spectrum Sharing Strategy for Device-to-Device Communications
Kaiming Shen, Wei Yu

On the Effective Rate of MISO/TAS Systems in Rayleigh Fading
Yazan Al-Badarneh, Costas Georghiades, Carlos Mejia

Th3-8: Compressed Sensing 4 — Chair: Bernard Henri Fleury — K7+8

Generalized Expectation Consistent Signal Recovery for Nonlinear Measurements
Hengtao He, Chao-Kai Wen, Shi Jin

Universality of the Elastic Net Error
Andrea Montanari, Phan Minh Nguyen

Using Mutual Information for Designing the Measurement Matrix in Phase Retrieval Problems
Nir Shlezinger, Ron Dabora, Yonina Eldar

Information Theoretic Limits for Linear Prediction with Graph-Structured Sparsity
Adarsh Barik, Jean Honorio, Mohit Tawarmalani

Improved Bounds for Universal One-bit Compressive Sensing
Jayadev Acharya, Arnab Bhattacharyya, Pritish Kamath

Th3-9: Signal Processing — Chair: Negar Kiyavash — K9

Principal Pivot Transforms on Radix-2 DFT-type Matrices
Sian-Jheng Lin, Amira Alloum, Tareq Y. Al-Naffouri

Adversarial Principal Component Analysis
Daniel Pimentel-Alarcon, Aritra Biswas, Claudia Solis-Lemus

Characterization of the stability range of the Hilbert transform with applications to spectral factorization
Holger Boche, Volker Pohl

Mellin-Transform-Based New Results of the Joint Statistics of Partial Products of Ordered Random Variables
Sung Sik Nam, Young-Chai Ko, Mohamed-Slim Alouini

Optimal Sensor Selection in the Presence of Noise and Interference
Afshin Abdi, Faramarz Fekri

Thursday, June 29 — 16:40-18:20

16:40	17:00	17:20	17:40	18:00
Th4-1: Network Coding 2 Chair: Ron Roth				⇒ **Amsterdam** ⇐
Circular-shift Linear Network Coding *Qifu Sun, Hanqi Tang, Zongpeng Li, Xiaolong Yang, Keping Long*	Coding for Networks of Compound Channels *Fariba Abbasi, Mayank Bakshi*	Distributed Decoding of Convolutional Network Error Correction Codes *Hengjie Yang, Wangmei Guo*	Multiuser Rate-Diverse Network-Coded Multiple Access *Haoyuan Pan, Lu Lu, Soung Chang Liew*	
Th4-2: Coded Computation Chair: Helmut Bölcskei				Brussels
Coded convolution for parallel and distributed computing within a deadline *Sanghamitra Dutta, Viveck Cadambe, Pulkit Grover*	Coded Computation over Heterogeneous Clusters *Amirhossein Reisizadeh, Saurav Prakash, Ramtin Pedarsani, Salman Avestimehr*	Coded Computation for Multicore Setups *Kangwook Lee, Ramtin Pedarsani, Dimitris Papailiopoulos, Kannan Ramchandran*	High-Dimensional Coded Matrix Multiplication *Kangwook Lee, Changho Suh, Kannan Ramchandran*	
Th4-3: Coded Caching 1 Chair: Giuseppe Caire				K2
Coded Caching with Partial Adaptive Matching *Jad Hachem, Nikhil Karamchandani, Sharayu Moharir, Suhas Diggavi*	Improved Converses and Gap-Results for Coded Caching *Chien-Yi Wang, Shirin Saeedi Bidokhti, Michele Wigger*	Coded Caching for Combination Networks with Cache-Aided Relays *Ahmed Zewail, Aylin Yener*	Asynchronous Coded Caching *Hooshang Ghasemi, Aditya Ramamoorthy*	Decentralized Coded Caching in Wireless Networks: Trade-off between Storage and Latency *Antonious Girgis, Ozgur Ercetin, Mohammed Nafie, Tamer ElBatt*
Th4-4: Shannon Theory and Molecular Chair: Olivier Leveque				K3
A Characterization of the Shannon Ordering of Communication Channels *Rajai Nasser*	On the Input-Degradedness and Input-Equivalence Between Channels *Rajai Nasser*	Models and information-theoretic bounds for nanopore sequencing *Wei Mao, Suhas Diggavi, Sreeram Kannan*	Less Noisy Domination by Symmetric Channels *Anuran Makur, Yury Polyanskiy*	Capacity of Molecular Channels with Imperfect Particle-Intensity Modulation and Detection *Nariman Farsad, Christopher Rose, Muriel Médard, Andrea Goldsmith*
Th4-5: Bounds 3 Chair: I-Hsiang Wang				K4
Information-theoretic Limits of Subspace Clustering *Kwangjun Ahn, Kangwook Lee, Changho Suh*	The Error Exponent of Sparse Regression Codes with AMP Decoding *Cynthia Rush, Ramji Venkataramanan*	Lower Bounds on the Number of Write Operations by Index-less Indexed Flash Code with Inversion Cells *Akira Yamawaki, Hiroshi Kamabe, Shan Lu*	Partial Data Extraction via Noisy Histogram Queries: Information Theoretic Bounds *Wei-Ning Chen, I-Hsiang Wang*	Asymptotics of the Error Probability in Quasi-Static Binary Symmetric Channels *Josep Font-Segura, Alfonso Martinez, Albert Guillén i Fàbregas*
Th4-6: Wireless Networks 2 Chair: Randall Berry				K5
Commitment in regulatory spectrum games: Examining the first-player advantage *Vidya Muthukumar, Anant Sahai*	Inferring Network Topology from Information Cascades *Feng Ji, Wenchang Tang, Wee Peng Tay, Edwin Chong*	Statistical beamforming for the large antenna broadcast channel *Vasanthan Raghavan, Junil Choi, David Love*	Efficient Resource Allocation in Mobile-edge Computation Offloading: Completion Time Minimization *Quy Hong Le, Hussein Al-Shatri, Anja Klein*	Scalable Spectrum Allocation for Large Networks Based on Sparse Optimization *Binnan Zhuang, Dongning Guo, Ermin Wei, Michael Honig*
Th4-7: Random Access Channels Chair: Robert Calderbank				K6
A perspective on massive random-access *Yury Polyanskiy*	Low Complexity Schemes for the Random Access Gaussian Channel *Or Ordentlich, Yury Polyanskiy*	Multi-Cell Aware Opportunistic Random Access *Huifa Lin, Won-Yong Shin*	Multi-Channel Random Access with Replications *Olga Galinina, Andrey Turlikov, Sergey Andreev, Yevgeni Koucheryavy*	
Th4-8: Index Coding 1 Chair: Lawrence Ong				K7+8
Private Broadcasting: an Index Coding Approach *Mohammed Karmoose, Linqi Song, Martina Cardone, Christina Fragouli*	Golden-Coded Index Coding *Yu-Chih Huang, Yi Hong, Emanuele Viterbo*	Generalized Index Coding Problem and Discrete Polymatroids *Anoop Thomas, B. Sundar Rajan*	A Pliable Index Coding Approach to Data Shuffling *Linqi Song, Christina Fragouli, Tianchu Zhao*	
Th4-9: Compression 2 Chair: Stefano Rini				K9
Fixed-Length-Parsing Universal Compression with Side Information *Yeohee Im, Sergio Verdú*	Coding Theorems for the Compress and Estimate Source Coding Problem *Alon Kipnis, Stefano Rini, Andrea Goldsmith*	Row-centric lossless compression of Markov images *Matthew Reyes, David Neuhoff*	A Practical Approach for Successive Omniscience *Ni Ding, Rodney Kennedy, Parastoo Sadeghi*	

Friday, June 30 09:50-11:10

9:50	10:10	10:30	10:50
Fr1-1: Lattice Codes 2 Chair: Robert Fischer			**Europa**
On the Universality of Lattice Codes for a Class of Ergodic Fading Channels *Ahmed Hindy, Aria Nosratinia*	Index Mapping for Bit-error Resilient Multiple Description Lattice Vector Quantizer *Sorina Dumitrescu, Yifang Chen, Jun Chen*	On Shaping Complex Lattice Constellations from Multi-level Constructions *Perathorn Pooksombat, J Harshan, Wittawat Kositwattanarerk*	On the Design of Multi-Dimensional Irregular Repeat-Accumulate Lattice Codes *Min Qiu, Lei Yang, Yixuan Xie, Jinhong Yuan*
Fr1-2: Polar Codes 3 Chair: Peter Trifonov			**Brussels**
Performance Bounds of Concatenated Polar Coding Schemes *Dina Goldin, David Burshtein*	Energy-Adaptive Polar Codes: Trading Off Reliability and Decoder Circuit Energy *Haewon Jeong, Christopher Blake, Pulkit Grover*	Polar codes with a stepped boundary *Ilya Dumer*	Permuted Successive Cancellation Decoding for Polar Codes *Sarit Buzaglo, Arman Fazeli, Veeresh Taranalli, Paul Siegel, Alexander Vardy*
Fr1-3: Multiple Access 3 Chair: Young-Han Kim			**K2**
On the Degrees of Freedom of Wide-Band Multi-Cell Multiple Access Channels With No CSIT *Yo-Seb Jeon, Namyoon Lee, Ravi Tandon*	Low-Density Code-Domain NOMA: Better Be Regular *Ori Shental, Benjamin Zaidel, Shlomo (Shitz) Shamai*	Capacity Region of a One-Bit Quantized Gaussian Multiple Access Channel *Borzoo Rassouli, Deniz Gündüz, Morteza Varasteh*	On OR Many-Access Channels *Wenyi Zhang, Lingyan Huang*
Fr1-4: Information Retrieval Chair: Eitan Yaakobi			**K3**
Improved Codes for List Decoding in the Levenshtein's channel and Information Retrieval *Tero Laihonen, Tuomo Lehtilä*	Binary, Shortened Projective Reed Muller Codes for Coded Private Information Retrieval *Myna Vajha, Vinayak Ramkumar, P Vijay Kumar*	Sparse Ternary Codes for similarity search have higher coding gain than dense binary codes *Sohrab Ferdowsi, Sviatoslav Voloshynovskiy, Dimche Kostadinov, Taras Holotyak*	PIR Array Codes with Optimal PIR Rates *Tuvi Etzion, Simon Blackburn*
Fr1-5: Information Dynamics Chair: Anant Sahai			**K4**
The Capacity of Unstable Dynamical Systems-Interaction of Control and Information Transmission *Ioannis Tzortzis, Charalambos Charalambous, Christos Kourtellaris, Sergey Loyka*	Optimal Quantizations of B-DMCs Maximizing α-Mutual Information with Monge Property *Yuta Sakai, Ken-ichi Iwata*	Information and estimation in Fokker-Planck channels *Andre Wibisono, Varun Jog, Po-Ling Loh*	Dynamical Systems, Ergodicity, and Posterior Matching *Todd Coleman*
Fr1-6: Coding for Insertion and Deletion Channels 2 Chair: Vahid Aref			**K5**
Asymptotically Optimal Sticky-Insertion-Correcting Codes with Efficient Encoding and Decoding *Hessam Mahdavifar, Alexander Vardy*	Permutation Codes Correcting a Single Burst Deletion II: Stable Deletions *Yeow Meng Chee, San Ling, Tuan Thanh Nguyen, Van Khu Vu, Hengjia Wei*	Guess & Check Codes for Deletions and Synchronization *Serge Kas Hanna, Salim El Rouayheb*	On Unique Decoding from Insertion Errors *Kayvon Mazooji*
Fr1-7: Security 6 Chair: Oliver Kosut			**K6**
Characterizing Optimal Security and Round-Complexity for Secure OR Evaluation *Amisha Jhanji, Hemanta Maji, Raphael Meyer*	Learning Adversary's Actions for Secret Communication *Mehrdad Tahmasbi, Matthieu Bloch, Aylin Yener*	On the Equivalency of Reliability and Security Metrics for Wireline Networks *Mohammad mahdi Mojahedian, Amin Gohari, Mohammad Reza Aref*	A code-based blind signature *Olivier Blazy, Philippe Gaborit, Julien Schrek, Nicolas Sendrier*
Fr1-8: Multiple Access Chair: Richard Wesel			**K7+8**
Asymptotic Analysis of Tone Reservation Method for the PAPR Reduction of CDMA Systems *Holger Boche, Ezra Tampubolon*	Spatial random multiple access with multiple departure *Serguei Foss, Andrey Turlikov, Maxim Grankin*	Coded Random Access Design for Constrained Outage *MohammadReza Ebrahimi, Farshad Lahouti, Victoria Kostina*	
Fr1-9: Channel Identification Chair: Kenta Kasai			**K9**
On Optimal Error Exponents in Noiseless Channel Identification *Marat Burnashev, Hirosuke Yamamoto*	Channel Resolvability Theorems for General Sources and Channels *Hideki Yagi*	Hierarchical Identification with Preprocessing *Minh Thanh Vu, Tobias Oechtering, Mikael Skoglund*	Mismatched Identification via Channels *Anelia Somekh-Baruch*

Friday, June 30 — 11:30-12:50

11:30	11:50	12:10	12:30
Fr2-1: Rank Metric Codes Chair: Sven Puchinger			Europa
On Decoding Rank-Metric Codes over Large Fields *Ron Roth*	Universal secure rank-metric coding schemes with optimal communication overheads *Umberto Martínez-Peñas*	MRD Rank Metric Convolutional Codes *Diego Napp, Raquel Pinto, Joachim Rosenthal, Paolo Vettori*	A decoding algorithm for Twisted Gabidulin codes *Tovohery Randrianarisoa, Joachim Rosenthal*
Fr2-2: Iterative Decoding 2 Chair: Yuval Cassuto			Brussels
An Iterative Soft-decision Decoding Algorithm for Reed-Solomon Codes *Huang Chang Lee, Jyun-Han Wu, Yeong-Luh Ueng, Chung-Hsuan Wang*	Decoding from Pooled Data: Phase Transitions of Message Passing *Ahmed El Alaoui, Aaditya Ramdas, Florent Krzakala, Lenka Zdeborova, Michael Jordan*	Topological Interference Management with Decoded Message Passing: A Polyhedral Approach *Xinping Yi, Giuseppe Caire*	
Fr2-3: Coded Caching 2 Chair: Petros Elia			K2
Decentralized Caching and Coded Delivery over Gaussian Broadcast Channels *Mohammad Mohammadi Amiri, Deniz Gündüz*	Low Subpacketization Schemes for Coded Caching *Li Tang, Aditya Ramamoorthy*	On Coded Caching in the Overloaded MISO Broadcast Channel *Enrico Piovano, Hamdi Joudeh, Bruno Clerckx*	Coded Caching with Linear Subpacketization is Possible using Ruzsa-Szeméredi Graphs *Karthikeyan Shanmugam, Antonia Tulino, Alexandros Dimakis*
Fr2-4: Channel Capacity 4 Chair: Hideki Yagi			K3
The Arbitrarily Varying Channel Under Constraints with Causal Side Information at the Encoder *Uzi Pereg, Yossef Steinberg*	Storage Capacity as an Information-Theoretic Analogue of Vertex Cover *Arya Mazumdar, Andrew McGregor, Sofya Vorotnikova*	Gaussian ISI Channels with Mismatch *Wasim Huleihel, Salman Salamatian, Neri Merhav, Muriel Médard*	Characterization of Super-Additivity and Discontinuity Behavior of the Capacity of Arbitrarily Varying Channels under List Decoding *Holger Boche, Rafael Schaefer, H. Vincent Poor*
Fr2-5: Communications 4 Chair: Remi Chou			K4
Optimal Covert Communications using Pulse-Position Modulation *Matthieu Bloch, Saikat Guha*	Covert Communication with Noncausal Channel-State Information at the Transmitter *Si-Hyeon Lee, Ligong Wang, Ashish Khisti, Gregory Wornell*	Strong Coordination of Signals and Actions over Noisy Channels *Giulia Cervia, Laura Luzzi, Mael Le Treust, Matthieu Bloch*	Strong Coordination over Noisy Channels: Is Separation Sufficient? *Sarah Obead, Badri Vellambi, Joerg Kliewer*
Fr2-6: Coding and Decoding Chair: Hessam Mahdavifar			K5
Universal Decoding Using a Noisy Codebook *Neri Merhav*	Variable-to-Fixed Length Homophonic Coding Suitable for Asymmetric Channel Coding *Junya Honda, Hirosuke Yamamoto*	Optimality of the recursive data exchange protocol *Himanshu Tyagi, Shun Watanabe*	Explicit Constructions of Finite-Length WOM Codes *Yeow Meng Chee, Han Mao Kiah, Alexander Vardy, Eitan Yaakobi*
Fr2-7: Privacy and Security Chair: Philippe Gaborit			K6
On Information-Theoretic Privacy with General Distortion Cost Functions *Kousha Kalantari, Lalitha Sankar, Oliver Kosut*	Impact of the Communication Channel on Information Theoretical Privacy *Mehmet Demir, Gunes Karabulut Kurt, Guido Dartmann, Volker Lücken, Gerd Ascheid*	Constructive Interference Based Secure Precoding *Muhammad Khandaker, Christos Masouros, Kai Kit Wong*	Secure and reliable connectivity in heterogeneous wireless sensor networks *Rashad Eletreby, Osman Yağan*
Fr2-8: Computation Chair: Anelia Somekh-Baruch			K7+8
Communication-Aware Computing for Edge Processing *Songze Li, Mohammad Ali Maddah-Ali, Salman Avestimehr*	Encoded Distributed Optimization *Can Karakus, Yifan Sun, Suhas Diggavi*	Fundamental Estimation Limits in Autoregressive Processes with Compressive Measurements *Milind Rao, Tara Javidi, Yonina Eldar, Andrea Goldsmith*	Minimizing Latency for Secure Distributed Computing *Rawad Bitar, Parimal Parag, Salim El Rouayheb*

Friday, June 30 14:40-16:20

14:40	15:00	15:20	15:40	16:00
Fr3-1: Codes and Graphs Chair: Norbert Goertz				Europa
On sparse graph coding for coherent and noncoherent demodulation *Charles-Ugo Piat-Durozoi, Charly Poulliat, Nathalie Thomas, Marie-Laure Boucheret, Guy Lesthievent*	The Number of Independent Sets In Hexagonal Graphs *Zhun Deng, Jie Ding, Kathryn Heal, Vahid Tarokh*	Density Evolution on a Class of Smeared Random Graphs *Kabir Chandrasekher, Orhan Ocal, Kannan Ramchandran*	Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs *Rashad Eletreby, Osman Yağan*	
Fr3-2: LDPC Codes 3 Chair: Boris Kudryashov				Brussels
Message Alignment for Discrete LDPC Decoders with Quadrature Amplitude Modulation *Jan Lewandowsky, Maximilian Stark, Gerhard Bauch*	Rate-Loss Reduction of SC-LDPC Codes by Optimizing Reliable Variable Nodes via Expected Graph Evolution *Heeyoul Kwak, Jaewha Kim, Jong-Seon No*	Compute-Forward Multiple Access (CFMA) with Nested LDPC Codes *Erixhen Sula, Jingge Zhu, Adriano Pastore, Sung Hoon Lim, Michael Gastpar*	Edge Spreading Design of High Rate Array-Based SC-LDPC Codes *David Mitchell, Eirik Rosnes*	LDPC Code Design for Correlated Sources using EXIT Charts *Mohamad. Khas, Hamid Saeedi, Reza Asvadi*
Fr3-3: Caching 3 Chair: Aditya Ramamoorthy				K2
Fundamental Limits of Distributed Caching in Multihop D2D Wireless Networks *Mingyue Ji, Rong-Rong Chen, Giuseppe Caire, Andreas Molisch*	Fundamental Limits on Latency in Transceiver Cache-Aided HetNets *Jaber Kakar, Soheil Gherekhloo, Aydin Sezgin*	Cache-Aided Cooperation with No CSIT *Eleftherios Lampiris, Jingjing Zhang, Petros Elia*		
Fr3-4: Entropy 3 Chair: Peter Harremoes				K3
Arimoto-Renyi Conditional Entropy and Bayesian Hypothesis Testing *Igal Sason, Sergio Verdú*	Rényi Entropy Rate of Hidden Markov Processes *Chengyu Wu, 'Easton' Li Xu, Guangyue Han*	Sharp Bounds on Arimoto's Conditional Rényi Entropies Between Two Distinct Orders *Yuta Sakai, Ken-ichi Iwata*	Minimax Rényi Redundancy *Semih Yagli, Yücel Altuğ, Sergio Verdú*	Infinity-Rényi entropy power inequalities *Peng Xu, James Melbourne, Mokshay Madiman*
Fr3-5: Machine Learning 2 Chair: Parimal Parag				K4
Noisy Inductive Matrix Completion Under Sparse Factor Models *Akshay Soni, Troy Chevalier, Swayambhoo Jain*	On the Problem of On-line Learning with Log-Loss *Yaniv Fogel, Meir Feder*	Multiclass MinMax Rank Aggregation *Pan Li, Olgica Milenkovic*	Adiabatic Persistent Contrastive Divergence Learning *Hyeryung Jang, Hyungwon Choi, Yung Yi, Jinwoo Shin*	Online Nonparametric Anomaly Detection based on Geometric Entropy Minimization *Yasin Yilmaz*
Fr3-6: Estimation 2 Chair: Laura Cottatellucci				K5
Spectral Initialization for Nonconvex Estimation: High-Dimensional Limit and Phase Transitions *Yue Lu, Gen Li*	Jackknife estimation for Markov processes with no mixing constraints *Kevin Oshiro, Changlong Wu, Narayana Prasad Santhanam*	Minimax Risk for Missing Mass Estimation *Nikhilesh Rajaraman, Andrew Thangaraj, Ananda Suresh*		
Fr3-7: Information Theory and Statistics 2 Chair: Himanshu Tyagi				K6
Ensemble Estimation of Mutual Information *Kevin Moon, Kumar Sricharan, Alfred Hero III*	Minimum Rates of Approximate Sufficient Statistics *Masahito Hayashi, Vincent Tan*	Information-theoretic characterizations of Markov random fields and subfields *Raymond W. Yeung, Ali Al-Bashabsheh, Chao Chen, Qi Chen, Pierre Moulin*	Conditional Central Limit Theorems for Gaussian Projections *Galen Reeves*	An Information Theoretic Analysis of Sequential Decision-Making *Meik Dörpinghaus, Édgar Roldán, Izaak Neri, Heinrich Meyr, Frank Jülicher*
Fr3-8: Index Coding 2 Chair: Guido Montorsi				K7+8
The Optimality of Partial Clique Covering for Index Coding *Xinping Yi, Giuseppe Caire*	On the Capacity for Distributed Index Coding *Yucheng Liu, Parastoo Sadeghi, Fatemeh Arbabjolfaei, Young-Han Kim*	Improved Bounds for Multi-Sender Index Coding *Min Li, Lawrence Ong, Sarah Johnson*	Uniprior Index Coding *Vijaya Kumar Mareedu, Prasad Krishnan*	Rate $\frac{1}{3}$ Index Coding: Forbidden and Feasible Configurations *Lalitha Vadlamani, Prasad Krishnan*
Fr3-9: Statistics 2 Chair: Raymond W. Yeung				K9
Divergence Scaling of Fixed-Length, Binary-Output, One-to-one Distribution Matching *Patrick Schulte, Bernhard Geiger*	Lower Bounds on the Minimax Risk for the Source Localization Problem *Praveen Venkatesh, Pulkit Grover*	On the Optimality of Some Group Testing Algorithms *Matthew Aldridge*	Measurement Dependent Noisy Search: The Gaussian Case *Anusha Lalitha, Nancy Ronquillo, Tara Javidi*	Scalable Multichannel Joint Sequential Change Detection and Isolation *Sourabh Banerjee, Georgios Fellouris*

Friday, June 30 16:40-18:00

16:40 17:00 17:20 17:40

Fr4-1: Coding Theory 4 Chair: Hans-Andrea Loeliger — Europa

A New Approach for Constructing and Decoding Maximum Rank Distance Codes
Hessam Mahdavifar

Individually-Secure Multi-Source Multicast
Alejandro Cohen, Asaf Cohen, Omer Gurewitz, Muriel Médard

Lattice coding for Rician fading channels from Hadamard rotations
Alex Karrila, Niko Väisänen, David Karpuk, Camilla Hollanti

Fr4-2: DNA and Coding Chair: Olgica Milenkovic — Brussels

Mutually Uncorrelated Codes for DNA Storage
Maya Levy, Eitan Yaakobi

Noise and Uncertainty in String-Duplication Systems
Siddharth Jain, Farzad Farnoud (Hassanzadeh), Moshe Schwartz, Jehoshua Bruck

Rank Modulation Codes for DNA Storage
Netanel Raviv, Moshe Schwartz, Eitan Yaakobi

Fundamental Limits of DNA Storage Systems
Reinhard Heckel, Ilan Shomorony, Kannan Ramchandran, David Tse

Fr4-3: Error Exponents Chair: Meir Feder — K2

Distributed Identity Testing with Zero-Rate Compression
Wenwen Zhao, Lifeng Lai

Exponential source/channel duality
Sergey Tridenski, Ram Zamir

Error Exponents for Sparse Communication
Lóránt Farkas, Tamás Kói, Imre Csiszár

Universal Random Access Error Exponents for Codebooks with Different Word-Lengths
Lóránt Farkas, Tamás Kói

Fr4-4: Bounds 4 Chair: Itzhak Tamo — K3

Bounds on the Rate and Minimum Distance of Codes with Availability
Balaji Srinivasan Babu, P Vijay Kumar

Improved existence bounds on IPP codes using the Clique Lovász Local Lemma
Cástor Aranda, Marcel Fernández

Explicit bounds on the length of optimal X-codes
Yu Tsunoda, Yuichiro Fujiwara

A convolution inequality for entropy over Z2
Varun Jog

Fr4-5: Shannon Theory and Applications Chair: Sergio Verdú — K4

Topological Structures on DMC spaces
Rajai Nasser

A Strong Data Processing Inequality for Thinning Poisson Processes and Some Applications
Ligong Wang

Continuity of Channel Parameters and Operations under Various DMC Topologies
Rajai Nasser

SCW Codes for Optimal CSI-Free Detection in Diffusive Molecular Communications
Vahid Jamali, Arman Ahmadzadeh, Nariman Farsad, Robert Schober

Fr4-6: Quantum IT 5 Chair: Masahito Hayashi — K5

Pretty good measures in quantum information theory
Raban Iten, Joseph Renes, David Sutter

Linear Programming Bounds for Entanglement-Assisted Quantum Codes
Ching-Yi Lai, Alexei Ashikhmin

Estimating the Information Rate of a Channel with Classical Input and Output and a Quantum State
Michael Cao, Pascal Vontobel

Fundamental limits of quantum-secure covert optical sensing
Boulat Bash, Christos Gagatsos, Animesh Datta, Saikat Guha

Fr4-7: Source Coding 5 Chair: Galen Reeves — K6

Source Coding with Distortion Profile Constraints
Pierre Moulin

Lower Bounds on Rate of Fixed-Length Source Codes under Average- and ϵ-Fidelity Constraints
Pierre Moulin

Enhanced MDL with Application to Atypicality
Elyas Sabeti, Anders Høst-Madsen

Distributed Coding of Multispectral Images
Maxim Goukhshtein, Petros Boufounos, Toshiaki Koike-Akino, Stark Draper

Abstracts

Mo1-1: Algebraic Coding

Monday, June 26, 10:10-11:10
Room: Europa
Chair: Christian Senger (University of Stuttgart, Germany)

Constructions of Partial MDS Codes over Small Fields (10:10)

Eitan Yaakobi (Technion, Israel); Ryan Gabrys (UIUC, USA); Mario Blaum (IBM Almaden Research Center & Universidad Complutense, Madrid, USA); Paul Siegel (University of California, San Diego, USA)

Partial MDS (PMDS) codes are a class of erasure-correcting array codes which combine local correction of the rows with global correction of the array. An $m \times n$ array code is called an $(r; s)$ PMDS code if each row belongs to an $[n, n-r, r+1]$ MDS code and the code can correct erasure patterns consisting of r erasures in each row together with s more erasures anywhere in the array. While a recent construction by Calis and Koyluoglu generates $(r; s)$ PMDS codes for all r and s, its field size is exponentially large. In this paper, a family of PMDS codes with field size $\mathcal{O}\left(\max\{m, n^{r+s}\}^s\right)$ is presented.

Attaining Capacity with iterated (U|U+V) codes based on AG codes and Koetter-Vardy soft decoding (10:30)

Jean-Pierre Tillich (INRIA, France); Irene Márquez-Corbella (University of La Laguna, Spain)

In this paper we show how to attain the capacity of discrete symmetric channels with polynomial time decoding complexity by considering iterated (U|U+V) constructions with algebraic geometry (AG) code components. These codes are decoded with a recursive computation of the a posteriori probabilities of the code symbols together with decoding the AG components with the Koetter-Vardy algorithm. We show that, when the number of levels of the iterated (U|U+V) construction tends to infinity, we attain the capacity of any discrete symmetric channel. Moreover the error probability decays quasi-exponentially with the codelength in the case of Reed-Solomon code constituents and exponentially with Tsfasman-Vladuts-Zink code constituents.

An Algebraic-Combinatorial Proof Technique for the GM-MDS Conjecture (10:50)

Anoosheh Heidarzadeh *(Texas A&M University, USA); Alex Sprintson (Texas A&M University, USA)*

This paper considers the problem of designing maximum distance separable (MDS) codes over small fields with constraints on the support of their generator matrices. For any given $m \times n$ binary matrix M, the *GM-MDS conjecture*, due to Dau *et al.*, states that if M satisfies the so-called MDS condition, then for any field $\mathbb{F}$ of size $q \geq n + m - 1$, there exists an $[n, m]_q$ MDS code whose generator matrix G, with entries in $\mathbb{F}$, fits M (i.e., M is the support matrix of G). Despite all the attempts by the coding theory community, this conjecture remains still open in general. It was shown, independently by Yan *et al.* and Dau *et al.*, that the GM-MDS conjecture holds if the following conjecture, referred to as the *TM-MDS conjecture*, holds: if M satisfies the MDS condition, then the determinant of a transformation matrix T, such that TV fits M, is not identically zero, where V is a Vandermonde matrix with distinct parameters. In this work, we generalize the TM-MDS conjecture, and present an algebraic-combinatorial approach based on polynomial-degree reduction for proving this conjecture. Our proof technique's strength is based primarily on reducing inherent combinatorics in the proof. We demonstrate the strength of our technique by proving the TM-MDS conjecture for the cases where the number of rows (m) of M is upper bounded by 5. For this class of special cases of M where the only additional constraint is on m, only cases with $m \leq 4$ were previously proven theoretically, and the previously used proof techniques are not applicable to cases with $m > 4$.

Mo1-2: Convolutional Codes

Monday, June 26, 10:10-11:10
Room: Brussels
Chair: Michael Lentmaier (Lund University, Sweden)

On the Code Distance of a Woven Block Code Construction (10:10)

Igor Zhilin *(Institute for Information Transmission Problems, Russia); Alexey Kreshchuk (Institute for Information Transmission Problems, Russia); Victor V. Zyablov (Institute for Information Transmission Problems (IITP) RAS, Russia)*

In this paper we propose a woven block code construction based on two convolutional outer codes and a single inner code. We proved lower and upper bounds on this construction's code distance. The lower bound is shown to be higher than the product of the free distances of inner and outer constituent codes. Since this construction uses well-developed convolutional constituent codes, we believe that it would be competitive to turbo codes in the future mobile communication systems.

Generalized column distances for convolutional codes (10:30)

Sara D. Cardell (University of Campinas, Brazil); Marcelo Firer (State University of Campinas - UNICAMP, Brazil); Diego Napp (University of Aveiro, Portugal)

In this work, we adapt the notion of generalized Hamming weight of block codes to introduce the novel concept of generalized column distances for convolutional codes. This can be considered an extension of the work done by J. Rosenthal and E. York on the generalized Hamming weights for free distance of convolutional codes. We also introduce the concept of Almost-MDP and Near- MDP convolutional code. The problem of constructing convolutional codes with design generalized column distance remains an interesting open problem that requires further research.

A Unified Ensemble of Concatenated Convolutional Codes (10:50)

Saeedeh Moloudi (Lund University, Sweden); Michael Lentmaier (Lund University, Sweden); Alexandre Graell i Amat (Chalmers University of Technology, Sweden)

We introduce a unified ensemble for turbo-like codes (TCs) that contains the four main classes of TCs: parallel concatenated codes, serially concatenated codes, hybrid concatenated codes, and braided convolutional codes. We show that for each of the original classes of TCs, it is possible to find an equivalent ensemble by proper selection of the design parameters in the unified ensemble. We also derive the density evolution (DE) equations for this ensemble over the binary erasure channel. The thresholds obtained from the DE indicate that the TC ensembles from the unified ensemble have similar asymptotic behavior to the original TC ensembles.

Mo1-3: Multiple Access 1

Monday, June 26, 10:10-11:10
Room: K2
Chair: Aydin Sezgin (RUB, Germany)

Cooperative Binning for Semi-deterministic Channels with Non-causal State Information (10:10)

Ido Gattegno (Ben-Gurion University, Israel); Haim Permuter (Ben-Gurion University, Israel); Shlomo (Shitz) Shamai (The Technion, Israel); Ayfer Özgür (Stanford University, USA)

The capacity of two semi-deterministic channels with the presence of non-causal channel state information (CSI) is characterized. The first channel is a state-dependent semi-deterministic relay channel. The CSI is available only at the transmitter and receiver, but not at the relay. The second channel is a state-dependent multiple access channel (MAC) with partial cribbing and CSI only at one transmitter and the receiver. In the semi-deterministic relay channel without states, the capacity can be achieved using partial-decode-forward scheme. The transmission is split to blocks; in each block, the relay decodes a part of the message and cooperation is established using those bits. When the channel depends on a state, the decoding procedure at the relay reduces the transmission rate. The cooperative-bin-forward is a coding scheme that establishes cooperation based on random bins. The deterministic output is mapped into bins, and the relay chooses the transmission sequence based the bin index. This scheme achieves the capacity when the CSI is available causally. In this work, we present a variation of the cooperative-bin-forward scheme that achieves capacity for non-causal CSI. The bin index of the deterministic output is selected by the transmitter, such that the relay's transmission is coordinated with the states. This coding scheme also applies for the MAC with partial cribbing and non-causal CSI at one transmitter and receiver. The capacity is achieved by the new variation of cooperative bin-forward. On top of that, we show an example in which the capacity with non-causal CSI is strictly greater than with causal CSI.

A New Achievable Rate Region for Multiple-Access Channel with States (10:30)

Mohsen Heidari Khoozani (University of Michigan, USA); Farhad Shirani (University of Michigan, USA); Sandeep Pradhan (University Michigan, USA)

The problem of reliable communication over the multiple-access channel (MAC) with states is investigated. We propose a new coding scheme for this problem which uses *quasi-group* codes (QGC). We derive a new computable single-letter characterization of the achievable rate region. As an example, we investigate the problem of *doubly-dirty* MAC with modulo-4 addition. It is shown that the sum rate $R_1 + R_2 = 1$ bits per channel use is achievable using the new scheme. Whereas, the natural extension of the Gel'fand-Pinsker scheme, sum-rates greater than 0.32 are not achievable.

The Benefit of Encoder Cooperation in the Presence of State Information (10:50)

Parham Noorzad (California Institute of Technology, USA); Michelle Effros (California Institute of Technology, USA); Michael Langberg (State University of New York at Buffalo, USA)

In many communication networks, the availability of channel state information at various nodes provides an opportunity for network nodes to work together, or cooperate. This work studies the benefit of cooperation in the multiple access channel with a cooperation facilitator, distributed state information at the encoders,

and full state information available at the decoder. Under various causality constraints, sufficient conditions are obtained such that encoder cooperation through the facilitator results in a gain in sum-capacity that has infinite slope in the information rate shared with the encoders. This result extends the prior work of the authors on cooperation in networks where none of the nodes have access to state information.

Mo1-4: Entropy 1

Monday, June 26, 10:10-11:10
Room: K3
Chair: Holger Boche (Technical University Munich, Germany)

A lower bound on the differential entropy for log-concave random variables with applications to rate-distortion theory (10:10)

Arnaud Marsiglietti *(California Institute of Technology, USA); Victoria Kostina (California Institute of Technology, USA)*

We derive a lower bound on the differential entropy for symmetric log-concave random variable X in terms of the p-th absolute moment of X, which shows that entropy and p-th absolute moment of a symmetric log-concave random variable are comparable. We apply our bound to study the rate distortion function under distortion measure $|x-\hat{x}|^r$ for sources that follow a log-concave probability distribution. In particular, we establish that the difference between the rate distortion function and the Shannon lower bound is at most $\log(\sqrt{2}e) \approx 1.9$ bits, independently of r and the target distortion d. For mean-square error distortion, the difference is at most $\log \sqrt{\pi e} \approx 1.55$ bits, regardless of d. Our results generalize to the case of vector X. Our proof technique leverages tools from convex geometry.

H(X) vs. H(f(X)) (10:30)

Ferdinando Cicalese (University of Verona, Italy); Luisa Gargano (University of Salerno, Italy); ***Ugo Vaccaro*** *(University of Salerno, USA)*

It is well known that the entropy H(X) of a finite random variable is always greater or equal to the entropy H(f(X)) of a function f of X, with equality if and only if the function f is one-to-one. In this paper, we give tights bounds on H(f(X)) when the function f is not one-to-one, and we illustrate a few scenarios where this matters. As an intermediate step towards our main result, we prove a lower bound on the entropy of a probability distribution, when only a bound on the ratio between the maximum and the minimum probability is known. Our lower bound improves previous results in the literature, and it is likely to find applications outside the scenario considered in this paper.

Concavity of Entropy Power: Equivalent Formulations and Generalizations (10:50)

Thomas Courtade (University of California, Berkeley, USA)

We investigate extensions of Costa's entropy power inequality (EPI). In particular, we show that Costa's EPI, when appropriately formulated, can be precisely generalized to non-Gaussian additive perturbations. This reveals fundamental links between the Gaussian logarithmic Sobolev inequality and the convolution inequalities for entropy and Fisher information. Various consequences including a reverse entropy power inequality and information-theoretic central limit theorems are discussed.

Mo1-5: Optical Communications

Monday, June 26, 10:10-11:10
Room: K4
Chair: Frank Kschischang (University of Toronto, Canada)

On Time-Bandwidth Product of Multi-Soliton Pulses (10:10)

Alexander Span *(University of Stuttgart, Germany); Vahid Aref (Nokia Bell Labs, Germany); Henning Buelow (Nokia Bell Labs, Germany); Stephan ten Brink (University of Stuttgart, Germany)*

Multi-soliton pulses are potential candidates for fiber optical transmissions where the information is modulated and recovered in the so-called nonlinear Fourier domain. While this is an elegant technique to account for the channel nonlinearity, the obtained spectral efficiency, so far, is not competitive with the classic Nyquist-based schemes. In this paper, we study the evolution of the time-bandwidth product of multi-solitons as they propagate along the optical fiber. For second and third order soliton pulses, we numerically optimize the pulse shapes to achieve the smallest time-bandwidth product when the phase of the spectral amplitudes is used for modulation. Moreover, we analytically estimate the pulse-duration and bandwidth of multi-solitons in some practically important cases. Those estimations enable us to approximate the time-bandwidth product for higher order solitons.

A Novel Demodulation Scheme for a Memoryless Optical Interference Channel (10:30)

Kamran Keykhosravi *(Chalmers University of Technology, Sweden); Erik Agrell (Chalmers University of Technology, Sweden)*

Matched filtering and sampling, which is known to be the optimal receiver for the linear additive white Gaussian noise channel, is in general suboptimal for a nonlinear medium. Nonetheless, it is commonly used in

fiber-optical communication systems with nonlinear distortion. In this paper, a novel demodulation scheme is proposed for a two-user memoryless interference channel, with a type of nonlinear crosstalk that occurs in wavelength-multiplexed optical transmission. We show by simulations that by using this demodulation scheme, unlike matched filtering and sampling, the symbol error rate decreases to zero in the high-power regime.

Optical MISO IM/DD Channels: Optimality of Spatial Repetition Codes among DC-offset STBCs (10:50)

Yerzhan Sapenov (KAUST & Nazarbayev University, Saudi Arabia); Anas Chaaban (King Abdullah University of Science and Technology, Saudi Arabia); Zouheir Rezki (University of Idaho, USA); Mohamed-Slim Alouini (King Abdullah University of Science and Technology (KAUST), Saudi Arabia)

In this paper, an optical wireless multiple-input single-output communication system employing intensity-modulation direct-detection is considered. Subject to a per transmit-aperture power constraint, the performance of direct current (DC) offset space-time block codes (STBC) is studied in terms of pairwise error probability (PEP). It is shown that among the class of DC-STBCs, the worst case PEP, i.e., the one corresponding to the minimum distance between two codewords, is minimized by repetition coding (RC) for any channel state. Therefore, it follows that among all DC-STBCs, RC is optimal in terms of worst case PEP under any turbulence statistics. This result agrees with previously published numerical results showing the superiority of RC in such systems. It also agrees with previously published analytical results on this topic under log- normal turbulence and further extends it to arbitrary turbulence statistics. Numerical results provided to verify this result also indicate that RC is not only optimal in terms of worst case PEP, but also in terms of average error probability.

Mo1-6: Precoding

Monday, June 26, 10:10-11:10
Room: K5
Chair: Jinyuan Chen (Louisiana Tech University, USA)

Beamforming Codebook Compensation for Beam Squint with Channel Capacity Constraint (10:10)

Mingming Cai (University of Notre Dame, USA); J. Nicholas Laneman (University of Notre Dame, USA); Bertrand Hochwald (Notre Dame University, USA)

Analog beamforming with phased arrays is a promising technique for 5G wireless communication in millimeter wave bands. A beam focuses on a small range of angles of arrival or departure and corresponds to a set of fixed phase shifts across frequency due to practical hardware constraints. In switched beamforming, a discrete codebook consisting of multiple beams is used to cover a larger angle range. However, for sufficiently large bandwidth, the gain provided by the phased array is frequency dependent even if the radiation pattern of the antenna elements is frequency independent. The effect is called beam squint. This paper shows that the beam squint reduces channel capacity of a uniform linear array (ULA). The beamforming codebook is designed to compensate for the beam squint by imposing a channel capacity constraint. For example, our codebook design algorithm can improve the channel capacity by 17.8% for a ULA with 64 antennas operating at bandwidth of 2.5 GHz and carrier frequency of 73 GHz. Analysis and numerical examples suggest that a denser codebook is required to compensate for the beam squint. Furthermore, the effect of beam squint is shown to increases as the growth of bandwidth, and the beam squint limits the bandwidth given the number of antennas in the array.

Asymptotics of Nonlinear LSE Precoders with Applications to Transmit Antenna Selection (10:30)

***Ali Bereyhi** (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany); Mohammad Ali Sedaghat (Friedrich Alexander University of Erlangen-Nürnberg, Germany); Ralf Müller (FAU Erlangen-Nürnberg, Germany)*

This paper studies the large-system performance of Least Square Error (LSE) precoders which minimize the input-output distortion over an arbitrary support subject to a general penalty function. The asymptotics are determined via the replica method in a general form which encloses the Replica Symmetric (RS) and Replica Symmetry Breaking (RSB) ansätze. As a result, the "marginal decoupling property" of LSE precoders for b-steps of RSB is derived. The generality of the studied setup enables us to address special cases in which the number of active transmit antennas are constrained. Our numerical investigations depict that the computationally efficient forms of LSE precoders based on "ℓ_1-norm" minimization perform close to the cases with "zero-norm" penalty function which have a considerable improvements compared to the random antenna selection. For the case with BPSK signals and restricted number of active antennas, the results show that RS fails to predict the performance while the RSB ansatz is consistent with theoretical bounds.

MIMO IBC Beamforming with Combined Channel Estimate and Covariance CSIT (10:50)

Wassim Tabikh (EURECOM, France); Dirk Slock (EURECOM, France); Yi Yuan-Wu (Orange Labs, France)

This work deals with beamforming for the MIMO Interfering Broadcast Channel (IBC), i.e. the Multi-Input

Multi-Output (MIMO) Multi-User Multi-Cell downlink (DL). The novel beamformers are here optimized for the Expected Weighted Sum Rate (EWSR) for the case of Partial Channel State Information at the Transmitters (CSIT). Gaussian (Posterior) partial CSIT can optimally combine channel estimate and channel covariance information. We introduce the first large system analysis for optimized beamformers with partial CSIT, here for the Massive MISO (MaMISO) case. In the case of Gaussian partial CSIT, the beamformers only depend on the means and covariances of the channels. The large system analysis furthermore allows to predict the EWSR performance on the basis of the channel statistics only.

Mo1-7: Quantization

Monday, June 26, 10:10-11:10
Room: K6
Chair: Ioannis Kontoyiannis (Athens UniversityEcon & Business, Greece)

How to Quantize n Outputs of a Binary Symmetric Channel to n-1 Bits? (10:10)

Wasim Huleihel (MIT, USA); Or Ordentlich (MIT, USA)

Suppose that Y^n is obtained by observing a uniform Bernoulli random vector X^n through a binary symmetric channel with crossover probability α. The "most informative Boolean function" conjecture postulates that the maximal mutual information between Y^n and any Boolean function $\mathrm{b}(X^n)$ is attained by a dictator function. In this paper, we consider the "complementary" case in which the Boolean function is replaced by $f:\{0,1\}^n \mapsto \{0,1\}^{n-1}$, namely, an $n-1$ bit quantizer, and show that $I(f(X^n);Y^n) \leq (n-1)\cdot(1-h(\alpha))$ for any such f. Thus, in this case, the optimal function is of the form $f(x^n)=(x_1,\ldots,x_{n-1})$.

Information-Distilling Quantizers (10:30)

Bobak Nazer (Boston University, USA); Or Ordentlich (MIT, USA); Yury Polyanskiy (MIT, USA)

Let X and Y be dependent random variables. We consider the problem of designing a scalar quantizer for Y to maximize the mutual information between its output and X, and study fundamental properties and bounds for this form of quantization. Our main focus is the regime of low $I(X;Y)$, where we show that for a binary X, there always exist an M-level quantizer attaining mutual information of $\Omega(-M\cdot I(X;Y)/\log(I(X;Y))$ and that there exists pairs of X,Y for which the mutual information attained by any M-level quantizer is $\mathcal{O}(-M\cdot I(X;Y)/\log(I(X;Y)))$.

Mo1-8: Rate Distortion Theory 1

Monday, June 26, 10:10-11:10
Room: K7+8
Chair: Shigeaki Kuzuoka (Wakayama University, Japan)

Distortion bounds for source broadcasting and asymmetric data transmission with bandwidth expansion (10:10)

Shraga Bross (Bar-Ilan University, Israel); Hagai Zalach (Bar-Ilan University, Israel)

We consider the broadcasting of a single Gaussian source over a two-user Gaussian broadcast channel with bandwidth expansion. In addition to the source broadcasting the encoder sends a message reliably to the "higher quality" user. Conditioned on the message rate, we derive an outer bound on the set of attainable mean-squared error distortion pairs at the two users which extends the Reznic-Feder-Zamir bound. Based on the outer bound and an inner bound that we derive we characterize the set of achievable energy-distortion exponents for this problem.

Rate-Distortion Region of a Gray-Wyner Problem with Side-Information (10:30)

Meryem Benammar (HUAWEI Technologies France, France); Abdellatif Zaidi (Université Paris-Est Marne La Vallée, France)

In this work, we establish a full single-letter characterization of the rate-distortion region of an instance of the Gray-Wyner model with side information at the decoders. In this model an encoder observes a pair of memoryless sources (S_1^n,S_2^n) and communicates with two receivers over a common error-free rate-limited link of capacity R_0, as well as two individual error-free rate-limited links of capacities R_1 and R_2. Both receivers reproduce the source component S_2^n losslessly; and Receiver 1 also reproduces the source component S_1^n lossily, to within some prescribed distortion level D_1. Also, Receiver 1 and Receiver 2 observe each a memoryless side information sequence, Y_1^n and Y_2^n, assumed to be arbitrarily correlated among them, and with the source pair (S_1^n,S_2^n).

A Multiple Description CEO Problem with Log-Loss Distortion (10:50)

Georg Pichler (Vienna University of Technology, Austria); Pablo Piantanida (CentraleSupélec-CNRS-Université Paris-Sud, France); Gerald Matz (Vienna University of Technology, Austria)

This paper investigates the Multiple Description (MD) Chief Executive Officer (CEO) problem under logarithmic-loss distortion. The setup extends previous

work of Courtade and Weissman (2014) by requiring the CEO to obtain a useful reconstruction also from a reduced set of descriptions. A single-letter characterization of the achievable region is derived under a suitable conditional independence assumption. Surprisingly, the resulting rate requirement is in general less than that required to ensure successful typicality decoding of the corresponding description.

Mo1-9: Hypothesis Testing 1

Monday, June 26, 10:10-11:10
Room: K9
Chair: Gregory Wornell (MIT, USA)

Neyman-Pearson Test for Zero-Rate Multiterminal Hypothesis Testing (10:10)

Shun Watanabe (Tokyo University of Agriculture and Technology, Japan)

The problem of zero-rate multiterminal hypothesis testing is revisited. A Neyman-Pearson-like test is proposed and its non-asymptotic performance is clarified; for short blocklength, it is numerically examined that the proposed test is superior to a previously known Hoeffding-like test proposed by Han-Kobayashi. For the large deviation regime, it is shown that our proposed test achieves the optimal trade-off between the type I and type II exponents shown by Han-Kobayashi. The information geometry method plays an important role in the analysis as well as the construction of the test.

Using data-compressors for statistical analysis of problems on homogeneity testing and classification (10:30)

Boris Ryabko (Institute of Computational Technologies of SB RAS & Novosibirsk State University, Russia); Andrey Guskov (The State Public Scientific Technological Library of SB RAS, Novosibirsk, Russia); Irina Selivanova (The State Public Scientific Technological Library of SB RAS, Novosibirsk, Russia)

Nowadays data compressors are applied to many problems of text analysis, but many such applications are developed outside of the framework of mathematical statistics. In this paper we overcome this obstacle and show how several methods of classical mathematical statistics can be developed based on applications of the data compressors.

First- and Second-Order Hypothesis Testing for Mixed Memoryless Sources with General Mixture (10:50)

Te Sun Han (University of Electro-Communications, Japan); ***Ryo Nomura*** *(Senshu University, Japan)*

The first- and second-order optimum achievable exponents in the simple hypothesis testing problem are investigated. The optimum achievable exponent for type II error probability, under constraints that the type I error probability is allowed asymptotically up to ε, is called the ε-optimum exponent. In this paper, we first give the second-order ε-exponent in the case where the null hypothesis and the alternative hypothesis are a mixed memoryless source and a stationary memoryless source, respectively. We next generalize this setting to the case where the alternative hypothesis is also a mixed memoryless source. We address the first-order ε-optimum exponent in this setting.

Mo1-A: Age of Information 1

Monday, June 26, 10:10-11:10
Room: Berlin 3
Chair: Yin Sun (the Ohio State University, USA)

Status updates through M/G/1/1 queues with HARQ (10:10)

Elie Najm (Ecole Polytechnique Fédérale de Lausanne, Switzerland); Roy Yates (Rutgers University, USA); Emina Soljanin (Rutgers University, USA)

We consider a system where randomly generated updates are to be transmitted to a monitor, but only a single update can be in the transmission service at a time. Therefore, the source has to prioritize between the two possible transmission policies: preempting the current update or discarding the new one. We consider Poisson arrivals and general service time, and refer to this system as the M/G/1/1 queue. We start by studying the average status update age and the optimal update arrival rate for these two schemes under general service time distribution. We then apply these results on two practical scenarios in which updates are sent through an erasure channel using (a) an infinite incremental redundancy (IIR) HARQ system and (b) a fixed redundancy (FR) HARQ system. We show that in both schemes the best strategy would be not to preempt. Moreover, we also prove that, from an age point of view, IIR is better than FR.

Information Freshness and Popularity in Mobile Caching (10:30)

Clement Kam (Naval Research Laboratory, USA); Sastry Kompella (Naval Research Laboratory, USA); Gam Nguyen (Naval Research Laboratory, USA); Jeffrey Wieselthier (Wieselthier Research, USA); Anthony Ephremides (University of Maryland, USA)

We propose a model for mobile caching in which the rate of requests for content is dependent on the *popularity* and the *freshness* of the information. We model popularity based on the history of requests and freshness based on the age of the content. We consider a discrete time (slotted) system in which new packets arrive at a limited capacity cache at discrete times. We prove that the optimal policy for choosing the set of packets to reside in a full cache when a packet arrives is to reject the one with the lowest request rate in that particular slot. Thus, there is no advantage to separately knowing the history of requests or the age of the content. Since the optimal policy depends on the profile of the request process, we also study the expected behavior of the request model. We provide a sufficient condition under which the change in the request rate goes to zero and provide some numerical examples that illustrate this behavior. We also consider a slight alteration to the model, in which only the recent history of requests is used for determining the request rate. In this case, we provide a sufficient condition for when the rate is equal to zero, which approximates the duration of requests for content.

Age-Optimal Constrained Cache Updating (10:50)

Roy Yates (Rutgers University, USA); Philippe Ciblat (Telecom ParisTech, France); Aylin Yener (Pennsylvania State University, USA); Michele Wigger (Telecom ParisTech, France)

We consider a system where a local cache maintains a collection of N dynamic content items that are randomly requested by local users. A capacity-constrained link to a remote network server limits the ability of the cache to hold the latest version of each item at all times, making it necessary to design an update policy. Using an age of information metric, we show under a relaxed problem formulation that an asymptotically optimal policy updates a cached item in proportion to the square root of the item's popularity. We then show experimentally that a physically realizable policy closely approximates the asymptotic optimal policy.

Mo2-1: Coding Techniques 1

Monday, June 26, 11:30-12:50
Room: Europa
Chair: Jos Weber (Delft University of Technology, The Netherlands)

PIR schemes with small download complexity and low storage requirements (11:30)

Simon Blackburn (Royal Holloway University of London, United Kingdom (Great Britain)); Tuvi Etzion (Technion-Israel Institute of Technology, Israel); Maura Paterson (Birkbeck, University of London, United Kingdom (Great Britain))

Shah, Rashmi and Ramchandran recently considered a model for Private Information Retrieval (PIR) where a user wishes to retrieve one of several R-bit messages from a set of n non-colluding servers. Their security model is information-theoretic. Their paper is the first to consider a model for PIR in which the database is not necessarily replicated, so allowing distributed storage techniques to be used. Shah et al. show that at least $R + 1$ bits must be downloaded from servers, and describe a scheme with linear total storage (in R) that downloads between $2R$ and $3R$ bits. For any positive ϵ, we provide a construction with the same storage property, that requires at most $(1 + \epsilon)R$ bits to be downloaded; moreover one variant of our scheme only requires each server to store a bounded number of bits (in the sense of being bounded by a function that is independent of R). We also provide variants of a scheme of Shah et al which downloads exactly $R + 1$ bits and has quadratic total storage. Finally, we simplify and generalise a lower bound due to Shah et al. on the download complexity a PIR scheme. In a natural model, we show that an n-server PIR scheme requires at least $nR/(n - 1)$ download bits in many cases, and provide a scheme that meets this bound.

Nearly Optimal Constructions of PIR and Batch Codes (11:50)

Hilal Asi (Technion - Israel Institute of Technology, Israel); Eitan Yaakobi (Technion, Israel)

In this work we study two families of codes with availability, namely private information retrieval (PIR) codes and batch codes. While the former requires that every information symbol has k mutually disjoint recovering sets, the latter asks this property for every multiset request of k information symbols. The main problem under this paradigm is to minimize the number of redundancy symbols. We denote this value by $r_P(n,k), r_B(n,k)$, for PIR, batch codes, respectively, where n is the number of information symbols. Previous results showed that for any constant k, $r_P(n,k) = \Theta(\sqrt{n})$ and $r_B(n,k) = \mathcal{O}(\sqrt{n}\log(n)$. In this work we study the asymptotic behavior of these codes

for non-constant k and specifically for $k = \Theta(n^\epsilon)$. We also study the largest value of k such that the rate of the codes approaches 1, and show that for all $\epsilon < 1$, $r_P(n, n^\epsilon) = o(n)$, while for batch codes, this property holds for all $\epsilon < 0.5$.

Cyclone Codes (12:10)

Christian Schindelhauer (University of Freiburg & Rechnernetze und Telematik an der Albert-Ludwigs-Universität Freiburg, Germany); Andreas Jakoby (Bauhaus-Universität Weimar, Germany); Sven Köhler (University of Freiburg, Germany)

We introduce Cyclone codes which are rateless erasure resilient codes. They combine Pair codes with Luby Transform (LT) codes by computing a code symbol from a random set of data symbols using bitwise XOR and cyclic shift operations. The number of data symbols is chosen according to the Robust Soliton distribution. XOR and cyclic shift operations establish a unitary commutative ring if data symbols have a length of p − 1 bits, for some prime number p. We consider the graph given by code symbols combining two data symbols. If n/2 such random pairs are given for n data symbols, then a giant component appears, which can be resolved in linear time. We can extend Cyclone codes to data symbols of arbitrary even length, provided the Goldbach conjecture holds. Applying results for this giant component, it follows that Cyclone codes have the same encoding and decoding time complexity as LT codes, while the overhead is upper-bounded by those of LT codes. Simulations indicate that Cyclone codes significantly decreases the overhead of extra coding symbols.

Approaching Capacity Using Incremental Redundancy without Feedback (12:30)

Haobo Wang *(University of California, Los Angeles, USA); Sudarsan Vasista Srinivasan Ranganathan (University of California, Los Angeles, USA); Richard Wesel (University of California, Los Angeles, USA)*

Variable-length codes with incremental redundancy controlled by feedback allow a system to approach capacity with short average blocklengths and thus relatively low-complexity decoders. This paper shows how to use those same variable-length codes with incremental redundancy to approach capacity without feedback. The general principle is to provide a common pool of redundancy that can be accessed by exactly the variable-length codes that need it. We provide example implementations using both regular and irregular low-density generator matrix (LDGM) codes to provide this common pool of redundancy, utilizing the inter-frame coding approach that Zeineddine and Mansour used to combat rate variation due to fading in broadcast transmissions. Obtaining the LDGM degree distributions requires a new design methodology involving differential evolution for a generalized peeling decoder. Monte-Carlo simulations using a 2dB binary-input additive white Gaussian noise channel confirm the feasibility of this new approach. For a frame error rate of 10^{-3}, the irregular LDGM code achieves 96% of the throughput of the corresponding feedback system.

Mo2-2: Locally Repairable Codes 1

Monday, June 26, 11:30-12:50
Room: Brussels
Chair: Iwan Duursma (University of Illinois at Urbana-Champaign, USA)

Rate Optimal Binary Linear Locally Repairable Codes with Small Availability (11:30)

Swanand Kadhe (Texas A&M University, USA); Robert Calderbank (Duke University, USA)

A locally repairable code with availability has the property that every code symbol can be recovered from multiple, disjoint subsets of other symbols of small size. In particular, a code symbol is said to have (r, t)-availability if it can be recovered from t disjoint subsets, each of size at most r. A code with availability is said to be 'rate optimal', if its rate is maximum among the class of codes with given locality, availability, and alphabet size. This paper focuses on rate-optimal binary, linear codes with small availability, and makes three contributions. First, it establishes tight upper bounds on the rate of binary linear codes with $(r, 2)$ and $(2, 3)$ availability. Second, it establishes a uniqueness result for binary rate-optimal codes, showing that for certain classes of binary linear codes with $(r, 2)$ and $(2, 3)$-availability, any rate-optimal code must be a direct sum of shorter rate-optimal codes. Finally, it derives properties of locally repairable codes associated with convex polyhedra, especially, focusing on the codes associated with the Platonic solids. It demonstrates that these codes are locally repairable with $t = 2$, and that the codes associated with (geometric) dual polyhedra are (coding theoretic) duals of each other.

On Optimal Ternary Locally Repairable Codes (11:50)

Jie Hao (Tsinghua University, P.R. China); Shutao Xia (Tsinghua University, P.R. China); Bin Chen (South China Normal University, P.R. China)

In an $[n, k, d]$ linear code, a code symbol is said to have locality r if it can be repaired by accessing at most r other code symbols. For an (n, k, r) *locally repairable code* (LRC), the minimum distance satisfies the well-known Singleton-like bound $d \leq n - k - \lceil k/r \rceil + 2$. In this paper, we study optimal ternary LRCs meeting this Singleton-like bound by employing a parity-check matrix approach. It is proved that there are only 8 classes of possible parameters with which optimal ternary LRCs exist. Moreover, we obtain explicit

constructions of optimal ternary LRCs for all these 8 classes of parameters, where the minimum distance could only be 2, 3, 4, 5 and 6.

A Study on the Impact of Locality in the Decoding of Binary Cyclic Codes (12:10)

Nikhil Krishnan Muralee Krishnan (Indian Institute of Science, India); Bhagyashree Puranik (Indian Institute of Science, India); P Vijay Kumar (Indian Institute of Science & University of Southern California, India); Itzhak Tamo (Tel Aviv University, Israel); Alexander Barg (University of Maryland, USA)

In this paper, we study the impact of locality on the decoding of binary cyclic codes under two approaches, namely ordered statistics decoding (OSD) and trellis decoding. Given a binary cyclic code having locality or availability, we suitably modify the OSD to obtain gains in terms of Signal-To-Noise ratio, for a given reliability and essentially the same level of decoder complexity. With regard to trellis decoding, we show that careful introduction of locality results in the creation of cyclic subcodes having lower maximum state complexity. We also present a simple upper-bounding technique on the state complexity profile, based on the zeros of the code. Finally, it is shown how the decoding speed can significantly be increased in the presence of locality, in the moderate-to-high SNR regime, by making use of a quick-look decoder that often returns the ML codeword.

Locally Repairable Codes with the Optimum Average Information Locality (12:30)

Mostafa Shahabinejad (University of Alberta, Canada); Majid Khabbazian (University of Alberta, Canada); Masoud Ardakani (University of Alberta, Canada)

Locally repairable codes (LRCs) have been proposed and used in practice as effective coding methods for distributed storage systems (DSSs). In a DSS, information block recovery is a critical task performed in the case of data node permanent failure or temporal unavailability. Temporal node unavailability accounts for 90% of all block recoveries triggered in DSS. Since parity blocks are not needed to be recovered during a temporal node unavailability, special attention should be given to reconstruction of information blocks when trying to minimize the average bandwidth needed for block recovery. Motivated by this, in this work, we study the average locality of information blocks. We obtain a lower bound on the average locality of information blocks of LRCs and design LRCs that achieve the bound. In addition to obtaining the optimal average locality for the information blocks, our codes achieve the optimal maximum locality for all the information blocks as well as some parity blocks (in some cases all the parity blocks).

Mo2-3: Broadcast Channels 1

Monday, June 26, 11:30-12:50
Room: K2
Chair: Chandra Nair (Chinese University of Hong Kong, Hong Kong)

Error Exponent of the Common-Message Broadcast Channel with Variable-Length Feedback (11:30)

Lan Truong (National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore)

We derive upper and lower bounds on the reliability function for the discrete memoryless broadcast channel with common message and variable-length feedback. We show that the bounds are tight when the broadcast channel is stochastically degraded. We adapt and supplement new ideas to Yamamoto and Itoh's two-phase coding scheme for the direct part and Burnashev's proof technique for the converse part.

Exact Random Coding Exponents and Universal Decoders for the Degraded Broadcast Channel (11:50)

Ran Averbuch (Technion, Israel); Neri Merhav (Technion, Israel)

This work contains two main contributions concerning the degraded broadcast channel. The first is an analysis of the exact random coding error exponents for both users, and the second is the derivation of universal decoders for both users. These universal decoders are certain variants of the maximum mutual information (MMI) universal decoder, and which achieve the corresponding random coding exponents. In addition, we introduce some lower bounds, which involve optimization over very few parameters, unlike the original, exact exponents, which involve minimizations over auxiliary probability distributions. Numerical results for the binary symmetric broadcast channel are given as well, which show improvements over previously derived error exponents for the same model.

Feedback Halves the Dispersion for Some Two-User Broadcast Channels with Common Message (12:10)

Kasper Trillingsgaard (Aalborg University, Denmark); Wei Yang (Princeton University, USA); Giuseppe Durisi (Chalmers University of Technology, Sweden); Petar Popovski (Aalborg University, Denmark)

We investigate the maximum coding rate achievable on a two-user broadcast channel for the case where a common-message is transmitted using fixed-blocklength codes with feedback. Specifically, we fo-

cus on a family of broadcast channels composed of two antisymmetric Z-channels. For this setup, we obtain matching upper and lower bounds on the dispersion term in the asymptotic expansion of the maximum coding rate. These bounds reveal that the dispersion is halved compared to the no-feedback case.

A New Capacity-Approaching Protocol for General 1-to-K Broadcast Packet Erasure Channels with ACK/NACK (12:30)

Chih-Hua Chang (Purdue University, USA); Chih-Chun Wang (Purdue University, USA)

The capacity region of 1-to-K broadcast packet erasure channels with ACK/NACK is known for some scenarios, e.g., $K \leq 3$, etc. However, existing achievability schemes either require knowing the target rate $\vec{R}$ in advance, and/or have a complicated description of the achievable rate region that is difficult prove whether it matches the capacity or not. This work proposes a new network coding protocol with the following unique set of features: (i) Its achievable rate region is identical to the capacity region for *all* the scenarios in which the capacity is known; (ii) Its achievable rate region is much more tractable that existing works and has been used to derive new capacity rate vectors; (iii) It employs *sequential encoding* that naturally handles dynamic packet arrivals; (iv) It automatically adapts to unknown packet arrival rates $\vec{R}$; (v) It is based on $GF(q)$ with $q > K$. Numerically, for $K = 4$, it admits an average control overhead 2–4% (assuming each packet has 1000 bytes), average encoding memory usage 48.5 packets, and average per-packet delay 94.8 time slots, when operating at 95% of the capacity.

Mo2-4: Feedback

Monday, June 26, 11:30-12:50
Room: K3
Chair: Gerhard Kramer (Technical University of Munich, Germany)

On the Capacity of Burst Noise-Erasure Channels With and Without Feedback (11:30)

Lin Song (Queen's University, Canada); Fady Alajaji (Queen's University, Canada); Tamas Linder (Queen's University, Canada)

A class of burst noise-erasure channels which incorporate both errors and erasures during transmission is studied. The channel, whose output is explicitly expressed in terms of its input and a stationary ergodic noise-erasure process, is shown to satisfy a so-called "quasi-symmetry" condition under certain invertibility conditions. As a result, it is proved that a uniformly distributed input process maximizes the channel's block mutual information, resulting in a closed-form formula for its non-feedback capacity in terms of the noise-erasure entropy rate and the entropy rate of an auxiliary erasure process. The feedback channel capacity is also characterized, showing that feedback does not increase capacity and generalizing prior related results.

The ARMA(k) Gaussian Feedback Capacity (11:50)

***Tao Liu** (The University of Hong Kong, Hong Kong); Guangyue Han (The University of Hong Kong, Hong Kong)*

Using Kim's variational formulation (with a slight yet important modification), we derive the ARMA(k) Gaussian feedback capacity, i.e., the feedback capacity of an additive channel where the noise is a k-th order autoregressive moving average Gaussian process. More specifically, the ARMA(k) Gaussian feedback capacity is expressed as a simple function of a solution to a system of polynomial equations, which proves to have only finitely many solutions for the cases k = 1,2 and possibly beyond.

An Optimal Coding Scheme for the BIBO Channel with a No-Repeated-Ones Input Constraint (12:10)

***Oron Sabag** (Ben-Gurion University, Israel); Haim Permuter (Ben-Gurion University, Israel); Navin Kashyap (Indian Institute of Science, India)*

A binary-input binary-output (BIBO) channel is investigated in the presence of feedback and input constraints. The feedback capacity and the optimal input distribution of this setting are presented for the case where the input sequence contains no consecutive ones. A simple coding scheme is designed based on the principle of posterior matching, which was introduced by Shayevitz and Feder for memoryless channels. The posterior matching scheme for our input-constrained setting is shown to achieve capacity using two new ideas: *message history*, which captures the memory embedded in the setting, and *message splitting*, which simplifies the scheme analysis. Additionally, in the special case of an S-channel, we give a very simple zero-error coding scheme that achieves capacity.

Mo2-5: Reconstruction

Monday, June 26, 11:30-12:50
Room: K4
Chair: Urbashi Mitra (University of Southern California, USA)

Compressed Sensing with Prior Information via Maximizing Correlation (11:30)

Xu Zhang *(Beijing Institute of Technology, P.R. China); Wei Cui (Beijing Institute of Technology, P.R. China); Yulong Liu (Beijing Institute of Technology, P.R. China)*

Compressed sensing (CS) with prior information concerns the problem of reconstructing a sparse signal with the aid of a similar signal which is known beforehand. We consider a new approach to integrate the prior information into CS via maximizing the correlation between the prior knowledge and the desired signal. We then present a geometric analysis for the proposed method under sub-gaussian measurements. Our results reveal that if the prior information is good enough, then the proposed approach can improve the performance of the standard CS. Simulations are provided to verify our results.

Low Dimensional Atomic Norm Representations in Line Spectral Estimation (11:50)

Maxime Ferreira Da Costa *(Imperial College London, United Kingdom (Great Britain)); Wei Dai (Imperial College, United Kingdom (Great Britain))*

The line spectral estimation problem consists in recovering the frequencies of a complex valued time signal that is assumed to be sparse in the spectral domain from its discrete observations. As opposed to discretization-based methods for inverse problems, line spectral estimation reconstructs signals whose spectral supports lie continuously in the Fourier domain. If recent advances have shown that atomic norm relaxation produces highly robust estimates in this context, the computational cost of this approach remains, however, the major flaw for its application to practical systems. In this work, we aim to bridge the complexity issue by studying the atomic norm minimization problem from low dimensional projection of the signal samples. We derive conditions on the subsampling matrix under which the partial atomic norm can be expressed by a low-dimensional semidefinite program. Moreover, we illustrate the tightness of this relaxation by showing that it is possible to recover the original signal in poly-logarithmic time for two specific sub-sampling patterns.

Analysis of Approximate Message Passing with a Class of Non-Separable Denoisers (12:10)

Yanting Ma (North Carolina State University, USA); Cynthia Rush (Columbia University, USA); Dror Baron (North Carolina State University, USA)

Approximate message passing (AMP) is a class of low-complexity scalable algorithms for solving high-dimensional linear regression tasks where one wishes to recover an unknown signal β_0 from noisy, linear measurements y = A β_0 + w. AMP has the attractive feature that its performance (for example, the mean squared error of its estimates) can be accurately tracked by a simple, scalar iteration referred to as state evolution when the unknown signal has independent and identically distributed (i.i.d.) entries. However, in many real-world applications, like image or audio signal reconstruction, the unknown signal contains dependencies between entries and so a coordinate-wise independence structure is not a good approximation for the prior of the unknown signal. In this paper we study the case where the unknown signal has dependent entries using a class of non-separable sliding-window denoisers and prove that a new form of state evolution still accurately predicts AMP performance in this scenario. This is an early step in understanding the role of non-separable denoisers within AMP, and will lead to a characterization of more general denoisers in problems including compressive image reconstruction.

Inexact Projected Gradients on Unions of Subspaces (12:30)

Thomas Wiese *(Technische Universität München, Germany); Lorenz Weiland (Technische Universität München, Germany); Wolfgang Utschick (Technische Universität München, Germany)*

We prove convergence of the projected gradient algorithm with inexact projections when applied to linear inverse problems with constraint sets that are unions of subspaces. Such an algorithm is useful for joint angle and delay estimation in MIMO radar, where classical estimators for angle estimation can be integrated into compressive sensing methods for range estimation.

Mo2-6: Complexity

Monday, June 26, 11:30-12:50
Room: K5
Chair: Pulkit Grover (Carnegie Mellon University, USA)

Analysis and Enhancements of a Cognitive Based Complexity Measure (11:30)

Dilshan De Silva *(Sri Lanka Institute of Information Technology, Sri Lanka); Nuwan Kodagoda (Sri Lanka Institute of Information Technology, Sri Lanka); Saluka Kodituwakku (University of Peradeniya, Sri Lanka); Amalka J. Pinidiyaarachchi (University of Peradeniya, Sri Lanka)*

As stated by Tom DeMacro, something that cannot be measured is uncontrollable. Thus, a number of metrics have been developed to measure the complexity associated with software by considering various aspects such as size, control flow and data flow between modules, cognitive informatics etc. Amongst these aspects, cognitive informatics is recognized as a promising aspect in measuring software complexity. Thus, majority of the complexity metrics that were proposed after the introduction of cognitive informatics have been proposed mainly based on the cognitive aspect. Amongst them, Chhillar and Bhasins' weighted composite complexity measure is one of the few metrics that had attempted to measure the complexity of a program by considering more than three or more complexity factors. After a thorough analysis, in a previous study, the authors identified that the weighted composite complexity measure could be further improved by considering more complexity factors. This paper extends the previous study to identify the most appropriate factors that could be considered by the weighted composite complexity measure. Using the opinions of the industry experts, the authors were able to discover that compound conditional statements, threads and recursion could also be considered by the weighted composite complexity measure. Accordingly, the weighted composite complexity measure was enhanced to capture the complexities that arise due to those factors. The paper also includes a demonstration of the complexity calculation method of the improved weighted composite complexity measure with the use of three sample java programs, which were written by incorporating the above mentioned factors. In addition, an application of the weighted composite complexity measure to the same programs are also given in the paper, to illustrate the changes in complexity values of the two measures.

Generic Cospark of a Matrix Can Be Computed in Polynomial Time (11:50)

Sichen Zhong (SUNY Stony Brook, USA); Yue Zhao (Stony Brook University, USA)

The cospark of a matrix is the cardinality of the sparsest vector in the column space of the matrix. Computing the cospark of a matrix is well known to be an NP hard problem. Given the sparsity pattern (i.e., the locations of the non-zero entries) of a matrix, if the non-zero entries are drawn from independently distributed continuous probability distributions, we prove that the cospark of the matrix equals, with probability one, to a particular number termed the generic cospark of the matrix. The generic cospark also equals to the maximum cospark of matrices consistent with the given sparsity pattern. We prove that the generic cospark of a matrix can be computed in polynomial time, and offer an algorithm that achieves this.

Enumeration of Boolean Functions of Sensitivity Three and Inheritance of Nondegeneracy (12:10)

Kazuyuki Amano (Gunma University, Japan)

The sensitivity of a Boolean function is the maximum, over all inputs, of the number of input bits which when flipped change the output of the function. We enumerate all Boolean functions of sensitivity at most three and investigate their properties with the aid of computers. The number of NPN equivalence classes of nondegenerate n-variable Boolean functions of sensitivity three is 7, 80, 4215, 190221, 65694, 8873, 848, 64 and 8 for $n = 3, 4, \ldots, 11$ and zero for $n \geq 12$. We verify that, over all these functions, the maximum of block sensitivity, certificate complexity, decision tree complexity and degree is 6, 6, 9 and 9, respectively. A key to making this enumeration possible is the fact that, for every nondegenerate Boolean function f, a subfunction $f|_{x_i=0}$ or $f|_{x_i=1}$ is nondegenerate for some variable x_i, which is recently shown by Lee, Lokam, Tsai and Yang [in Proc. of ISIT '15, pages 501-505]. We extend this result by showing that, the minimum number of nondegenerate subfunctions in $\{f|_{x_i=0}, f|_{x_i=1}\}_{1\leq i\leq n}$ is, in fact, four.

On the Complexity of Estimating Renyi Divergences (12:30)

Maciej Skorski (IST Austria, Austria)

This paper studies the complexity of estimating Rényi divergences of discrete distributions: p observed from samples and the baseline distribution q known *a priori*. Extending the results of Acharya et al. (SODA'15) on estimating Rènyi entropy, we present improved estimation techniques together with upper and lower bounds on the sample complexity. We show that, contrarily to estimating Rènyi entropy where a sublinear (in the alphabet size) number of samples suffices, the sample complexity is heavily dependent on *events occurring unlikely* in q, and is unbounded in general (no matter what an estimation technique is used). For any divergence of integer order bigger than 1, we provide upper and lower bounds on the number of samples dependent on probabilities of p and q (the lower bounds hold for non-integer orders as well). We conclude that the worst-case sample complexity is polynomial in the

alphabet size if and only if the probabilities of q are non-negligible. This gives theoretical insights into heuristics used in the applied literature to handle numerical instability, which occurs for small probabilities of q. Our result shows that they should be handled with care not only because of numerical issues, but also because of a blow up in the sample complexity.

Mo2-7: ARQ

Monday, June 26, 11:30-12:50
Room: K6
Chair: Zouheir Rezki (University of Idaho, USA)

An Information Density Approach to Analyzing and Optimizing Incremental Redundancy with Feedback (11:30)

Haobo Wang (University of California, Los Angeles, USA); ***Nathan Wong*** *(University of California, Los Angeles, USA); Alexandar Baldauf (University of California, Los Angeles, USA); Christopher Bachelor (University of California, Los Angeles, USA); Sudarsan Vasista Srinivasan Ranganathan (University of California, Los Angeles, USA); Dariush Divsalar (Jet Propulsion Laboratory, USA); Richard Wesel (University of California, Los Angeles, USA)*

This paper uses a case study of a tail-biting convolutional code (with successful decoding indicated by the reliability output Viterbi algorithm) to present an information density approach for analyzing and optimizing the throughput of systems using incremental redundancy controlled by feedback. Polyanskiy's normal approximation combined with a linear model for the information gap of a rate-compatible code family provides a simple and accurate characterization of the behavior of feedback systems employing practical codes, such as convolutional or low-density parity-check codes. Especially for short message lengths on the order of k < 50 message bits, the newly proposed model is more accurate than Vakilinia's model in which the rate of first successful decoding has a Gaussian probability density function.

Outage Effective Capacity of Buffer-Aided Diamond Relay Systems Using HARQ-IR (11:50)

Deli Qiao (East China Normal University, P.R. China)

In this paper, transmission over buffer-aided diamond relay systems under statistical quality of service (QoS) constraints is studied. The statistical QoS constraints are imposed as limitations on delay violation probabilities. In the absence of channel state information (CSI) at the transmitter, truncated hybrid automatic repeat request-incremental redundancy (HARQ-IR) is incorporated to make better use of the wireless channel and the resources for each communication link. The packets that cannot be successfully received upon the maximum number of transmissions will be removed from buffer, i.e., outage occurs. The *outage effective capacity* is defined as the maximum constant arrival rate to the source that can be supported by the *goodput* departure processes, i.e., the departure that can be successfully received by the receiver. The outage effective capacity for the buffer-aided diamond relay system is obtained for HARQ-IR incorporated transmission strategy under the *end-to-end* delay constraints. In comparison with the decode-and-forward (DF) protocol with perfect CSI at the transmitters, it is shown that HARQ-IR can achieve better performance when the delay constraints are stringent.

Constraints for coded tunnels across long latency bottlenecks with ARQ-based congestion control (12:10)

Ulrich Speidel (University of Auckland, New Zealand); Sven Puchinger (Ulm University, Germany); Martin Bossert (Ulm University, Germany)

This paper considers capacity and delay constraints for coded tunnels across an erasure channel which occurs on shared Internet satellite links. Such links are long latency bottlenecks with a limited capacity input queue which drops packets when it overflows. The latency delays ARQ ACK feedback to senders, making it difficult for them to tune their packet transmission rate. This can cause the input queue to oscillate between empty and overflow. Queue oscillation leaves the link underutilised during the empty phases and slows down large packet flows. Channel coding can in principle provide goodput improvement in this scenario by letting senders accelerate to higher packet rates before burst losses occur and by mitigating exponential backoff after losses. However, this is only possible if the codes preserve sufficient channel capacity for the improved goodput to expand into. We formulate capacity and delay constraints that such block codes must meet. Using loss data obtained on a purpose-built simulator network, we show that such coding is feasible in a practical scenario and that partial unit memory (PUM) codes are particularly suitable for this task. In this context, we propose a part-systematic encoding for PUM codes, which performs slightly better than non-systematic encoding.

Throughput of HARQ-IR with Finite Blocklength Codes and QoS Constraints (12:30)

Yi Li (Syracuse University, USA); M. Cenk Gursoy (Syracuse University, USA); Senem Velipasalar (Syracuse University, USA)

In this paper, throughput of hybrid automatic repeat request (HARQ) schemes with finite blocklength codes is studied for both constant-rate and ON-OFF discrete-time Markov arrivals under statistical queuing constraints and deadline limits. After analyzing the decoding error probability and outage probability, the dis-

tribution of transmission period is characterized, and the throughput expressions are obtained for both arrival models. Analytical results are verified via Monte Carlo simulations. In the numerical results, the impact of deadline constraints, fixed transmission rate, coding blocklength, and queuing constraints on the throughput is analyzed.

Mo2-8: Quantum IT 1

Monday, June 26, 11:30-12:50
Room: K7+8
Chair: Marco Dalai (University of Brescia, Italy)

Polar Codes for Arbitrary Classical-Quantum Channels and Arbitrary cq-MACs (11:30)

Rajai Nasser (École Polytechnique Fédérale de Lausanne, Switzerland); Joseph Renes (ETH Zurich, Switzerland)

We prove polarization theorems for arbitrary classical-quantum (cq) channels. The input alphabet is endowed with an arbitrary Abelian group operation and an Arıkan-style transformation is applied using this operation. It is shown that as the number of polarization steps becomes large, the synthetic cq-channels polarize to deterministic homomorphism channels that project their input to a quotient group of the input alphabet. This result is used to construct polar codes for arbitrary cq-channels and arbitrary classical-quantum multiple access channels (cq-MAC). The encoder can be implemented in $O(N \log N)$ operations, where N is the blocklength of the code. A quantum successive cancellation decoder for the constructed codes is proposed. It is shown that the probability of error of this decoder decays faster than 2^{-N^β} for any $\beta < \frac{1}{2}$.

Sphere-Packing Bound for Symmetric Classical-Quantum Channels (11:50)

Hao-Chung Cheng (National Taiwan University, Taiwan); Min-Hsiu Hsieh (University of Technology Sydney, Australia); Marco Tomamichel (University of Technology Sydney, Australia)

We provide a sphere-packing lower bound for the optimal error probability in finite blocklengths when coding over a symmetric classical-quantum channel. Our result shows that the pre-factor can be significantly improved from the order of the subexponential to the polynomial, The established pre-factor is arguably optimal because it matches the best known random coding upper bound in the classical case. Our approaches rely on a sharp concentration inequality in strong large deviation theory and crucial properties of the error-exponent function.

A meta-converse for private communication over quantum channels (12:10)

Mark Wilde (Louisiana State University, USA); Marco Tomamichel (University of Technology Sydney, Australia); Mario Berta (California Institute of Technology, USA)

We establish a converse bounds on the private transmission capabilities of a quantum channel. The main conceptual development builds firmly on the notion of a private state, which is a powerful, uniquely quantum method for simplifying the tripartite picture of privacy involving local operations and public classical communication to a bipartite picture of quantum privacy involving local operations and classical communication. This approach has previously led to some of the strongest upper bounds on secret key rates, including the squashed entanglement and the relative entropy of entanglement. Here we use this approach along with a 'privacy test' to establish a general meta-converse bound for private communication.

Moderate Deviations for Classical-Quantum Channels (12:30)

Hao-Chung Cheng (National Taiwan University, Taiwan); Min-Hsiu Hsieh (University of Technology Sydney, Australia)

We show that the reliable communication through a classical-quantum channel is possible when the transmission rate approaches the channel capacity sufficiently slowly. This scenario exists between the non-vanishing error probability regime, where the rate tends to capacity with a fixed error, and the small error probability regime, where the error vanishes given a rate below capacity. The proof employs a sharp concentration bound in strong large deviation theory, and the asymptotic expansions of the error-exponent functions.

Mo2-9: Source Coding 1

Monday, June 26, 11:30-12:50
Room: K9
Chair: Lele Wang (Stanford University, USA)

Entropy of Some General Plane Trees (11:30)

*Zbigniew Golebiewski (Wroclaw University of Science and Technology, Poland); **Abram Magner** (UIUC, USA); Wojciech Szpankowski (Purdue University, USA)*

We continue developing the information theory of advanced data structures. In our previous work, we introduced structural entropy of unlabeled graphs and designed lossless compression algorithms for *binary* trees (with structure-correlated vertex names). In this paper, we consider d-ary trees ($d \geq 2$) and trees with

unrestricted degree for which we compute the entropy (the first step to design optimal compression algorithms). It turns out that extending from binary trees to general trees is mathematically quite challenging and leads to new recurrences that find ample applications in the information theory of structures.

On Optimality and Redundancy of Side Information Version of SWLZ (11:50)

*Ayush Jain (Indian Institute of Technology Kanpur, India); **Rakesh Bansal** (Indian Institute of Technology Kanpur & India, India)*

In this work, we establish the pointwise optimality of side information version of SWLZ algorithm for stationary ergodic sources. We also obtain a pointwise upper bound on the redundancy rate of this side information version of SWLZ algorithm for a subclass of $\phi-$mixing sources, which includes Markov sources as a special case. This upper bound obtained differs only by a constant factor from the best bound that has been obtained on redundancy rate for the original SWLZ algorithm itself.

Two-Dimensional Source Coding by Means of Subblock Enumeration (12:10)

***Takahiro Ota** (Nagano Prefectural Institute of Technology, Japan); Hiroyoshi Morita (The University of Electro-Communications, Japan)*

A technique of lossless compression via substring enumeration (CSE) is a well-known lossless compression algorithm for a one-dimensional (1D) source. The CSE uses a probabilistic model built from the circular string of an input source for encoding the source. The CSE is applicable to two-dimensional (2D) sources such as images by dealing with a line of pixels of 2D source as a symbol of an extended alphabet. At the initial step of the CSE encoding process, we need to output number of occurrences of all symbols of the extended alphabet, so that the time complexity increases exponentially when the size of source becomes large. To reduce the time complexity, we propose a new CSE which can encode a 2D source in block-by-block instead of line-by-line. The proposed algorithm uses the flat torus of an input 2D source as a probabilistic model instead of the circular string of the source. Moreover, we prove the asymptotic optimality of the proposed algorithm for 2D general sources.

Mo2-A: Age of Information 2

Monday, June 26, 11:30-12:50
Room: Berlin 3
Chair: Michele Wigger (Telecom ParisTech, France)

Timely Updates over an Erasure Channel (11:30)

Roy Yates (Rutgers University, USA); Elie Najm (Ecole Polytechnique Fédérale de Lausanne, Switzerland); Emina Soljanin (Rutgers University, USA); Jing Zhong (Rutgers University, USA)

Using an age of information (AoI) metric, we examine the transmission of coded updates through a binary erasure channel to a monitor/receiver. We start by deriving the average status update age of an infinite incremental redundancy (IIR) system in which the transmission of a k-symbol update continues until k symbols are received. This system is then compared to a fixed redundancy (FR) system in which each update is transmitted as an n symbol packet and the packet is successfully received if and only if at least k symbols are received. If fewer than k symbols are received, the update is discarded. Unlike the IIR system, the FR system requires no feedback from the receiver. For a single monitor system, we show that tuning the redundancy to the symbol erasure rate enables the FR system to perform as well as the IIR system. As the number of monitors is increased, the FR system outperforms the IIR system that guarantees delivery of all updates to all monitors.

Remote Estimation of the Wiener Process over a Channel with Random Delay (11:50)

***Yin Sun** (the Ohio State University, USA); Yury Polyanskiy (MIT, USA); Elif Uysal-Biyikoglu (METU & Currently on leave at The Ohio State University, Turkey)*

In this paper, we consider a problem of sampling a Wiener process, with samples forwarded to a remote estimator via a channel that consists of a queue with random delay. The estimator reconstructs a real-time estimate of the signal from causally received samples. Motivated by recent research on age-of-information, we study the optimal sampling strategy that minimizes the mean square estimation error subject to a sampling frequency constraint. We prove that the optimal sampling strategy is a threshold policy, and find the optimal threshold. This threshold is determined by the sampling frequency constraint and how much the Wiener process varies during the channel delay. An interesting consequence is that even in the absence of the sampling frequency constraint, the optimal strategy is not zero-wait sampling in which a new sample is taken once the previous sample is delivered; rather, it is optimal to wait for a non-zero amount of time after the previous sample is delivered, and then take the

next sample. Further, if the sampling times are independent of the observed Wiener process, the optimal sampling problem reduces to an age-of-information optimization problem that has been recently solved. Our comparisons show that the estimation error of the optimal sampling policy is much smaller than those of age-optimal sampling, zero-wait sampling, and classic uniform sampling.

Age and Value of Information: Non-linear Age Case (12:10)

Antzela Kosta *(Linköping University, Sweden); Nikolaos Pappas (Linköping University, Sweden); Anthony Ephremides (University of Maryland, USA); Vangelis Angelakis (Linköping University, Sweden)*

We consider a real-time status update system consisting of a source-destination network. A stochastic process is observed at the source, and samples, so called status updates, are extracted at random time instances, and delivered to the destination. In this paper, we expand the concept of information ageing by introducing the Cost of Update Delay (CoUD) metric to characterize the cost of having stale information at the destination. We introduce the Value of Information of Update (VoIU) metric that captures the reduction of CoUD upon reception of an update. The importance of the VoIU metric lies on its tractability which enables an alternative performance criterion in status update systems.

Status Updates Over Unreliable Multiaccess Channels (12:30)

Sanjit Kaul (IIIT Delhi, India); Roy Yates (Rutgers University, USA)

Applications like environmental sensing, and health and activity sensing, are supported by networks of devices (nodes) that send periodic packet transmissions over the wireless channel to a sink node. We look at simple abstractions that capture the following commonalities of such networks (a) the nodes send periodically sensed information that is temporal and must be delivered in a timely manner, (b) they share a multiple access channel and (c) channels between the nodes and the sink are unreliable (packets may be received in error) and differ in quality. We consider scheduled access and slotted ALOHA-like random access. Under scheduled access, nodes take turns and get feedback on whether a transmitted packet was received successfully by the sink. During its turn, a node may transmit more than once to counter channel uncertainty. For slotted ALOHA-like access, each node attempts transmission in every slot with a certain probability. For these access mechanisms we derive the age of information (AoI), which is a timeliness metric, and arrive at conditions that optimize AoI at the sink. We also analyze the case of symmetric updating, in which updates from different nodes must have the same AoI. We show that ALOHA-like access, while simple, leads to AoI that is worse by a factor of about $2e$, in comparison to scheduled access.

Mo3-1: Reed-Solomon Codes

Monday, June 26, 14:40-16:20
Room: Europa
Chair: Alexander Vardy (University of California San Diego, USA)

Twisted Reed-Solomon Codes (14:40)

Peter Beelen (Technical University of Denmark, Denmark); ***Sven Puchinger*** *(Ulm University, Germany); Johan Rosenkilde (Technical University of Denmark, Denmark)*

We present a new general construction of MDS codes over a finite field $\mathbb{F}_q$. We describe two explicit subclasses which contain new MDS codes of length at least $q/2$ for all values of $q \geq 11$. Moreover, we show that most of the new codes are not equivalent to a Reed–Solomon code.

Iterative Soft-Decision Decoding of Reed-Solomon Codes of Prime Lengths (15:00)

Shu Lin (UC Davis, USA); Khaled Abdel-Ghaffar (University of California, USA); Juane Li (University of California at Davis, USA); Keke Liu (Broadcom, USA)

A novel scheme is presented for encoding and decoding of Reed-Solomon codes of prime lengths. Encoding is performed on a collection of codewords which are mapped through Galois Fourier transform into a codeword in a low-density parity-check code with a binary parity-check matrix for transmission. Using this matrix, a binary iterative soft-decision decoding algorithm is applied to jointly decode a collection of codewords in the Reed-Solomon code. By allowing information sharing among the received vectors corresponding to the codewords in the collection, the proposed decoding scheme achieves superior performance over algorithms decoding individual Reed-Solomon codewords including maximum likelihood decoding.

Optimal Repair Schemes for Some Families of Full-Length Reed-Solomon Codes (15:20)

Hoang Dau (University of Illinois at Urbana-Champaign, USA); Olgica Milenkovic (UIUC, USA)

Reed-Solomon codes have found many applications in practical storage systems, but were until recently considered unsuitable for distributed storage applications due to the widely-held belief that they have poor repair bandwidth. The work of Guruswami and Wootters (STOC'16) has shown that one can actually perform bandwidth-efficient linear repair with Reed-Solomon

codes: When the codes are over the field $\mathbb{F}_{q^t}$ and the number of parities $r \geq q^s$, where $(t-s)$ divides t, there exists a linear scheme that achieves a repair bandwidth of $(n-1)(t-s)\log_2 q$ bits. We extend this result by showing the existence of such a linear repair scheme for every $1 \leq s < t$. Moreover, our new schemes are optimal among all linear repair schemes for Reed-Solomon codes when $n = q^t$ and $r = q^s$. Additionally, we improve the lower bound on the repair bandwidth for Reed-Solomon codes, also established in the work of Guruswami and Wootters.

Repairing Reed-Solomon Codes With Two Erasures (15:40)

Hoang Dau (University of Illinois at Urbana-Champaign, USA); Iwan Duursma (University of Illinois at Urbana-Champaign, USA); Han Mao Kiah (Nanyang Technological University, Singapore); Olgica Milenkovic (UIUC, USA)

Despite their exceptional error-correcting properties, Reed-Solomon codes have been overlooked in distributed storage applications due to the common belief that they have poor repair bandwidth: A naive repair approach would require the whole file to be reconstructed in order to recover a single erased codeword symbol. In a recent work, Guruswami and Wootters (STOC'16) proposed a single-erasure repair method for Reed-Solomon codes that achieves the optimal repair bandwidth amongst all linear encoding schemes. We extend their trace collection technique to cope with two erasures.

Decoding of Interleaved Reed-Solomon Codes Using Improved Power Decoding (16:00)

Sven Puchinger *(Ulm University, Germany); Johan Rosenkilde (Technical University of Denmark, Denmark)*

We propose a new partial decoding algorithm for m-interleaved Reed–Solomon (IRS) codes that can decode, with high probability, a random error of relative weight $1 - R^{\frac{m}{m+1}}$ at all code rates R, in time polynomial in the code length n. For $m > 2$, this is an asymptotic improvement over the previous state-of-the-art for all rates, and the first improvement for $R > 1/3$ in the last 20 years. The method combines collaborative decoding of IRS codes with power decoding up to the Johnson radius.

Mo3-2: LDPC Codes 1

Monday, June 26, 14:40-16:20
Room: Brussels
Chair: Paul Siegel (University of California, San Diego, USA)

Average Spectra for Ensembles of LDPC Codes and Applications (14:40)

Irina Bocharova (St. Petersburg University of Information Technologies, Mechanics and Optics, Russia); Boris Kudryashov (St. Petersburg University of Information Technologies, Mechanics and Optics, Russia); Vitaly Skachek (University of Tartu, Estonia); Yauhen Yakimenka (University of Tartu, Estonia)

The exact values of finite length average weight distributions for both binary ensembles and binary images of nonbinary ensembles of regular LDPC codes are computed. The exact average stopping set distribution for the binary ensemble is also obtained. The computed spectra are applied in order to bound from above the average stopping redundancy of the ensemble of binary regular LDPC codes. The exponents both of the average weight distribution for the binary image of the ensemble of nonbinary regular LDPC codes and of the average stopping weight distribution for the binary regular LDPC codes are also presented.

Time-invariant LDPC convolutional codes (15:00)

Dimitris Achlioptas (University of california, USA); Hamed Hassani (ETH Zurich, Switzerland); Wei Liu (EPFL, Switzerland); Ruediger Urbanke (EPFL, Switzerland)

Spatially coupled codes have been shown to universally achieve the capacity for a large class of channels. Many variants of such codes have been introduced to date. We discuss a further such variant that is particularly simple and is determined by a very small number of parameters. More precisely, we consider time-invariant low-density convolutional codes with very large constraint lengths. We show via simulations that, despite their extreme simplicity, such codes still show the threshold saturation behavior known from the spatially coupled codes discussed in the literature. Further, we show how the typical minimum stopping set size is related to basic parameters of the code. Due to their simplicity and good performance, these codes might be attractive from an implementation perspective.

On LDPC Code Ensembles with Generalized Constraints (15:20)

Yanfang Liu (Universidad Carlos III de Madrid & Gregorio Marañón Health Research Institute, Spain); Pablo M. Olmos (Universidad Carlos III de Madrid & Gregorio Marañón Health Research Institute, Spain); Tobias Koch (Universidad Carlos III de Madrid & Gregorio Marañón Health Research Institute, Spain)

In this paper, we analyze the tradeoff between coding rate and asymptotic performance of a class of generalized low-density parity-check (GLDPC) codes constructed by including a certain fraction of generalized constraint (GC) nodes in the graph. The rate of the GLDPC ensemble is bounded using classical results on linear block codes, namely Hamming bound and Varshamov bound. We also study the impact of the decoding method used at GC nodes. To incorporate both bounded-distance (BD) and Maximum Likelihood (ML) decoding at GC nodes into our analysis without resorting on multi-edge type of degree distributions (DDs), we propose the probabilistic peeling decoder (P-PD) algorithm, which models the decoding step at every GC node as an instance of a Bernoulli random variable with a success probability that depends on the GC block code and its decoding algorithm. The P-PD asymptotic performance can be predicted using standard techniques for LDPC codes. Further, we propose a class of GLDPC ensembles for which the simulated P-PD performance numerically coincides with the actual performance of the GLPDC code. The methodology presented may serve as a reference for the design of coding systems based on spare graphs with generalized constraints

Non-Uniformly Coupled LDPC Codes: Better Thresholds, Smaller Rate-loss, and Less Complexity (15:40)

Laurent Schmalen *(Nokia Bell Labs, Germany); Vahid Aref (Nokia Bell Labs, Germany); Fanny Jardel (Nokia Bell Labs, Germany)*

We consider spatially coupled low-density parity-check codes with finite smoothing parameters. A finite smoothing parameter is important for designing practical codes that are decoded using low-complexity windowed decoders. By optimizing the amount of coupling between spatial positions, we show that we can construct codes with excellent thresholds and small rate loss, even with the lowest possible smoothing parameter and large variable node degrees, which are required for low error floors. We also establish that the decoding convergence speed is faster with non-uniformly coupled codes, which we verify by density evolution of windowed decoding with a finite number of iterations. We also show that by only slightly increasing the smoothing parameter, practical codes with potentially low error floors and thresholds close to capacity can be constructed. Finally, we give some indications on protograph designs.

Reed-Solomon Based Nonbinary Globally Coupled LDPC Codes: Correction of Random Errors and Bursts of Erasures (16:00)

Juane Li (University of California at Davis, USA); Keke Liu (Broadcom, USA); Shu Lin (UC Davis, USA); Khaled Abdel-Ghaffar (University of California, USA)

This paper presents a special type of nonbinary LDPC codes which are constructed based on Reed-Solomon codes. For a code of this type, its Tanner graph is composed of a set of disjoint and identical Tanner graphs, which are coupled together by a group of global check-nodes. Such a code is called a globally coupled LDPC code. This type of codes are capable of correcting random symbol errors, multiple phased bursts of erasures, and a single long burst of erasures.

Mo3-3: Caching 1

Monday, June 26, 14:40-16:20
Room: K2
Chair: Osvaldo Simeone (New Jersey Institute of Technology, USA)

Characterizing the Rate-Memory Tradeoff in Cache Networks within a Factor of 2 (14:40)

Qian Yu *(University of Southern California, USA); Mohammad Ali Maddah-Ali (Bell Labs, Alcatel Lucent, USA); Salman Avestimehr (University of Southern California, USA)*

We consider a basic caching system, where a single server with a database of N files (e.g. movies) is connected to a set of K users through a shared bottleneck link. Each user has a local cache memory with a size of M files. The system operates in two phases: a placement phase, where each cache memory is populated up to its size from the database, and a following delivery phase, where each user requests a file from the database, and the server is responsible for delivering the requested contents. The objective is to design the two phases to minimize the load (peak or average) of the bottleneck link. We characterize the rate-memory tradeoff of the above caching system within a factor of 2.00884 for both the peak rate and the average rate (under uniform file popularity), where the best proved characterization in the current literature gives a factor of 4 and 4.7 respectively. Moreover, in the practically important case, where the number of files (N) is large, we exactly characterize the tradeoff for systems with no more than 5 users, and characterize the tradeoff within a factor of 2 otherwise. We establish these results by developing novel information theoretic outer-bounds for the caching problem, which improves the state of the art and gives tight characterization in various cases.

A Computer-Aided Investigation on the Fundamental Limits of Caching (15:00)

Chao Tian (University of Tennessee Knoxville, USA)

We present our recent effort, in the context of the caching systems, in developing a computer-aided approach in the investigation of information systems. Yeung's linear programming (LP) outer bound of the entropy space is our starting point, however our effort goes significantly beyond using it to prove information inequalities. A symmetry-reduced linear program is used to identify the boundary of the memory-transmission-rate tradeoff for several simple cases, for which we can obtain a set of tight outer bounds. General hypotheses on the optimal tradeoff are formed from these computed data, which are then analytically proved. This leads to a complete characterization of the optimal tradeoff for caching systems with only two users, and a partial characterization for systems with only two files. Next, we show that by carefully analyzing the joint entropy structure of the outer bounds for certain cases, a novel code construction can be reverse-engineered, and unachievability of linear codes can be proved for some other cases. Finally, we show that strong outer bounds can be computed through strategically relaxing the LP, which allows us to compute outer bounds for larger problem cases, despite the seemingly impossible computation scale.

Capacity Scaling of Wireless Device-to-Device Caching Networks under the Physical Model (15:20)

An Liu (Hong Kong University of Science and Technology, Hong Kong); Vincent Lau (Hong Kong University of Science and Technology, Hong Kong); Giuseppe Caire (Technische Universität Berlin, Germany)

We study the capacity scaling law of a device-to-device (D2D) caching network where n nodes are placed on a regular grid of area n. Each node caches some (coded) bits from a content library and requests a file from the library independently according to the Zipf popularity distribution. We propose a cache-induced hierarchical cooperation scheme which achieves the optimal capacity scaling law under a commonly used "physical model". When the path loss exponent $\alpha < 3$, the capacity scaling law can be significantly better than the throughput scaling laws achieved by the existing state-of-the-art schemes. To the best of our knowledge, this is the first work that completely characterizes the capacity scaling law for wireless caching networks under the physical model.

Wireless Coded Caching: A Topological Perspective (15:40)

Jingjing Zhang (EURECOM, France); Petros Elia (EURECOM, France)

We explore the performance of coded caching in a SISO BC setting where some users have higher link capacities than others. Focusing on a binary and fixed topological model where strong links have a fixed normalized capacity 1, and where weak links have reduced normalized capacity $\tau < 1$, we identify — as a function of the cache size and τ — the optimal throughput performance, within a factor of at most 8. The transmission scheme that achieves this performance, employs a simple form of interference enhancement, and exploits the property that weak links attenuate interference, thus allowing for multicasting rates to remain high even when involving weak users. This approach ameliorates the negative effects of uneven topology in multicasting, now allowing all users to achieve the optimal performance associated to $\tau = 1$, even if τ is approximately as low as $\tau \leq 1 - (1 - w)^g$ where g is the coded-caching gain, and where w is the fraction of users that are weak. This leads to the interesting conclusion that for coded multicasting, the weak users need not bring down the performance of all users, but on the contrary to a certain extent, the strong users can lift the performance of the weak users without any penalties on their own performance. Furthermore for smaller ranges of τ, we also see that achieving the near-optimal performance comes with the advantage that the strong users do not suffer any additional delays compared to the case where $\tau = 1$.

Multiplex Conductance and Gossip Based Information Spreading in Multiplex Networks (16:00)

Yufan Huang (North Carolina State University, USA); ***Huaiyu Dai*** *(NC State University, USA)*

In this work, we study the information spreading time in multiplex networks, adopting the gossip (random-walk) based information spreading model. A new metric called multiplex conductance is defined based on the multiplex network structure and used to quantify the information spreading time in a general multiplex network in the idealized setting. Multiplex conductance is then evaluated for some interesting multiplex networks to facilitate understanding in this new area. Finally, the tradeoff between the information spreading efficiency improvement and the layer cost is examined to explain the user's social behavior and motivate effective multiplex network designs.

Mo3-4: Channel Capacity 1

Monday, June 26, 14:40-16:20
Room: K3
Chair: Min Li (The University of Newcastle, Australia)

Capacity of Discrete-Time Wiener Phase Noise Channels to Within a Constant Gap (14:40)

Luca Barletta (Politecnico di Milano, Italy); Stefano Rini (National Chiao Tung University, Taiwan)

The capacity of the discrete-time channel affected by both additive Gaussian noise and Wiener phase noise is studied. Novel inner and outer bounds are presented, which differ of at most 6.65 bits per channel use for all channel parameters. The capacity of this model can be subdivided in three regimes: (i) for large values of the frequency noise variance, the channel behaves similarly to a channel with circularly uniform iid phase noise; (ii) when the frequency noise variance is small, the effects of the additive noise dominate over those of the phase noise, while (iii) for intermediate values of the frequency noise variance, the transmission rate over the phase modulation channel has to be reduced due to the presence of phase noise.

Capacity Sensitivity in Additive Non-Gaussian Noise Channels (15:00)

Malcolm Egan (INRIA, France); Samir Perlaza (INRIA, France); Vyacheslav Kungurtsev (Czech Technical University in Prague, Czech Republic)

In this paper, a new framework based on the notion of *capacity sensitivity* is introduced to study the capacity of continuous memoryless point-to-point channels. The capacity sensitivity reflects how the capacity changes with small perturbations in any of the parameters describing the channel, even when the capacity is not available in closed-form. This includes perturbations of the cost constraints on the input distribution as well as on the channel distribution. The framework is based on continuity of the capacity, which is shown for a class of perturbations in the cost constraint and the channel distribution. The continuity then forms the foundation for obtaining bounds on the capacity sensitivity. As an illustration, the capacity sensitivity bound is applied to obtain scaling laws when the support of additive α-stable noise is truncated.

Communicating under Temperature and Energy Harvesting Constraints (15:20)

Omur Ozel (Carnegie Mellon University, USA); Sennur Ulukus (University of Maryland, USA); Pulkit Grover (Carnegie Mellon University, USA)

Temperature constraints arise naturally in communication scenarios where the act of data transmission causes heat dissipation in a temperature sensitive situation due to radiation. We address this problem in point to point communications over an additive white Gaussian noise channel in an information theoretic setting. In the specific scenario, transmitted code symbols cause heat dissipation as an input to a first order discrete time heat circuit and the output of this dynamical system, being the temperature, has to remain below a critical level T_c. Additionally, we allow the transmitter to use an energy harvesting device to power its transmission. We investigate channel capacity for various combinations of peak and average temperature, average power, and energy harvesting constraints on the transmitted code symbols.

On Additive Channels with Generalized Gaussian Noise (15:40)

Alex Dytso (Princeton University, USA); Ronit Bustin (Tel Aviv University, Israel); H. Vincent Poor (Princeton University, USA); Shlomo (Shitz) Shamai (The Technion, Israel)

The paper considers a problem of communication over an additive noise channel where the noise is distributed according to a Generalized Gaussian (GG) distribution. In the first part of the paper, a number of properties of the family of GG distributions are derived which are of independent interest. For example, considerable attention is given to the properties of the characteristic function of the GG distribution. In the second part of the paper, the capacity of an additive noise channel with GG noise is considered under p-th absolute moment constraints. It is shown that, even though Shannon's upper bound is achievable in some instances, in general such achievability is not possible. Moreover, it is shown that discrete inputs can achieve capacity within a constant gap or full degree of freedom for any p-th absolute moment constraint. Following the seminal work of Smith, the paper also gives a condition under which discrete inputs are exactly optimal.

The Capacity of Injective Semi-Deterministic Two-Way Channels (16:00)

Anas Chaaban (King Abdullah University of Science and Technology, Saudi Arabia); Lav Varshney (University of Illinois at Urbana-Champaign, USA); Mohamed-Slim Alouini (King Abdullah University of Science and Technology (KAUST), Saudi Arabia)

The capacity region of the class of injective semi-deterministic two-way channels (TWCs) is investigated in this paper. To characterize this capacity, two conditions under which Shannon's bounds on the capacity region of TWCs are tight are first given. Using those conditions, it is shown that the capacity of this class of TWCs is characterized by the rectangle formed by the one-way capacities. This proves that adaptation is not needed for this class. This class encompasses, among others, all memoryless additive channels with input-independent noise, and hence, adaptation is use-

less for all such channels. This also shows that there exist continuous additive TWCs not of the exponential family type for which adaptation is not necessary. An example of a Cauchy TWC is given, and its capacity is characterized in closed form under a logarithmic constraint. Finally, the impact of the dependence of the noise on the inputs is discussed, and it is shown that adaptation may still be useless in such cases.

Mo3-5: Detection and Estimation 1

Monday, June 26, 14:40-16:20
Room: K4
Chair: Venugopal Veeravalli (University of Illinois at Urbana-Champaign, USA)

Sequential Estimation based on Conditional Cost (14:40)

George Moustakides *(University of Patras, Greece); Tony Yaacoub (Georgia Institute of Technology, USA); Yajun Mei (Georgia Institute of Technology, USA)*

We consider the problem of parameter estimation under a sequential framework. Specifically we assume that an i.i.d. random process is observed sequentially with its common pdf having a random parameter that must be estimated. We are interested in designing a stopping time that will decide when is the best moment to stop sampling the process and an estimator that will use the acquired samples in order to provide the desired estimate. We follow a semi-Bayesian approach where we assign a cost which is a function of the estimate and the true parameter value and our goal is to minimize the average sample size guaranteeing at the same time that the average cost stays below some prescribed level. For our analysis we adopt a conditional average cost which leads to a considerable simplification in the sequential estimation problem, otherwise known to be analytically intractable. We apply our results to a number of examples and compare our method with the optimum fixed sample size but also with existing sequential schemes.

Fundamental limit of resolving two point sources limited by an arbitrary point spread function (15:00)

Ronan Kerviche (University of Arizona, USA); Saikat Guha (Raytheon BBN Technologies, USA); Amit Ashok (University of Arizona, USA)

Estimating the angular separation between two incoherently radiating monochromatic point sources is a canonical toy problem to quantify spatial resolution in imaging. In recent work, Tsang et al. showed, using a Fisher Information analysis, that Rayleigh's resolution limit is just an artifact of the conventional wisdom of intensity measurement in the image plane. They showed that the optimal sensitivity of estimating the angle is only a function of the total photons collected during the camera's integration time but entirely independent of the angular separation itself no matter how small it is, and found the information-optimal mode basis, intensity detection in which achieves the aforesaid performance. We extend the above analysis, which was done for a Gaussian point spread function (PSF) to a hard-aperture pupil proving the information optimality of image-plane sinc-Bessel modes, and generalize the result further to an arbitrary PSF. We obtain new counterintuitive insights on energy vs. information content in spatial modes, and extend the Fisher Information analysis to exact calculations of minimum mean squared error, both for Gaussian and hard aperture pupils.

Denoising Linear Models with Permuted Data (15:20)

Ashwin Pananjady (University of California, Berkeley, USA); Martin Wainwright (University of California, Berkeley, USA); Thomas Courtade (University of California, Berkeley, USA)

We consider the multivariate linear regression model with shuffled data and additive Gaussian noise, which arises in various correspondence estimation and matching problems. We focus on the denoising problem and characterize the minimax error rate up to logarithmic factors. We also analyze the performance of two versions of a computationally efficient estimator that are consistent for a large range of input parameters. Finally, we provide an exact algorithm for the noiseless problem and demonstrate its performance on an image point-cloud matching task. Our analysis also extends to datasets with outliers.

Signal Recovery from Unlabeled Samples (15:40)

Saeid Haghighatshoar (Technische Universität Berlin, Germany); Giuseppe Caire (Technische Universität Berlin, Germany)

In this paper, we study the recovery of a signal from a collection of unlabeled and possibly noisy measurements via a measurement matrix with random i.i.d. Gaussian components. We call the measurements unlabeled since their order is missing, namely, it is not known a priori which elements of the resulting measurements correspond to which row of the measurement matrix. We focus on the special case of ordered measurements, where only a subset of the measurements is kept and the order of the taken measurements is preserved. We identify a natural duality between this problem and the traditional Compressed Sensing, where we show that the unknown support (location of nonzero elements) of a sparse signal in Compressed Sensing corresponds in a natural way to the unknown location of the measurements kept in unlabeled sensing. While in Compressed Sensing it is possible to recover a sparse signal from an under-determined set of linear equations (less equations than the dimension

of the signal), successful recovery in unlabeled sensing requires taking more samples than the dimension of the signal. We develop a low-complexity alternating minimization algorithm to recover the initial signal from the set of its unlabeled samples. We also study the behavior of the proposed algorithm for different signal dimensions and number of measurements empirically via numerical simulations. The results are a reminiscent of the phase-transition similar to that occurring in Compressed Sensing.

Estimation of Sparsity via Simple Measurements (16:00)

Abhishek Agarwal (University of Minnesota-Twin Cities, USA); Larkin Flodin (University of Massachusetts Amherst, USA); Arya Mazumdar (University of Massachusetts Amherst, USA)

We consider several related problems of estimating the 'sparsity' or number of nonzero elements d in a length n vector $\mathbf{x}$ by observing only $\mathbf{b} = M \odot \mathbf{x}$, where M is a predesigned test matrix independent of $\mathbf{x}$, and the operation $\odot$ varies between problems. We aim to provide a Δ-approximation of sparsity for some constant Δ with a minimal number of measurements (rows of M). This framework generalizes multiple problems, such as estimation of sparsity in group testing and compressed sensing. We use techniques from coding theory as well as probabilistic methods to show that $O(D \log D \log n)$ rows are sufficient when the operation $\odot$ is logical OR (i.e., group testing), and nearly this many are necessary, where D is a known upper bound on d. When instead the operation $\odot$ is multiplication over $\mathbb{R}$ or a finite field, we show that respectively $\Theta(D)$ and $\Theta(D \log \frac{n}{D})$ measurements are necessary and sufficient.

Mo3-6: Wireless Networks 1

Monday, June 26, 14:40-16:20
Room: K5
Chair: Andrea Goldsmith (Stanford University, USA)

On Optimal Link Scheduling with Deadlines for Emptying a Wireless Network (14:40)

Qing He (Linköping University, Sweden); Di Yuan (Linköping University, Sweden); Anthony Ephremides (University of Maryland, USA)

We consider link scheduling in wireless networks for emptying the queues at the transmitters in minimum time, with time constraints, or deadlines, for one or multiple individual links. We formulate the minimum-time scheduling problem with deadlines (MTSD) mathematically and derive the optimal activation order of the link sets in a schedule solution. Theoretical results are obtained, showing that the MTSD can be treated as the conventional minimum-time scheduling problem by "absorbing" the deadline constraints into the rate region where the scheduling problem is defined. By this approach, optimality characterization and geometric interpretation for the MTSD are provided. Furthermore, we extend the results to the MTSD in a general form that accommodates an arbitrary rate region.

On the Coverage Probability of a Spatially Correlated Network (15:00)

***Chang-sik Choi** (The University of Texas at Austin, USA); Jae Oh Woo (The University of Texas at Austin, USA); Jeffrey Andrews (The University of Texas at Austin, USA)*

We propose a new cellular network model that captures both strong repulsion and randomness between base stations. The base station are modeled by superposition of a random shifted grid with intensity λg for the grid base stations and an independent Poisson point process with intensity λp for the random base stations. Assuming that the typical user is associated with the base station that provides the strongest average receive signal power, we derive the association probability of the typical user. In Rayleigh fading channels, the coverage probability of the typical user at the origin is derived.

Efficiently Finding Simple Schedules in Gaussian Half-Duplex Relay Line Networks (15:20)

***Yahya Ezzeldin** (University of California, Los Angeles, USA); Martina Cardone (University of Califonia, Los Angeles, USA); Christina Fragouli (UCLA, USA); Daniela Tuninetti (University of Illinois at Chicago, USA)*

The problem of operating a Gaussian Half-Duplex (HD) relay network optimally is challenging due to the exponential number of listen/transmit network states that need to be considered. Recent results have shown that, for the class of Gaussian HD networks with N relays, there always exists a simple schedule, i.e., with at most N +1 active states, that is sufficient for approximate (i.e., up to a constant gap) capacity characterization. This paper investigates how to efficiently find such a simple schedule over line networks. Towards this end, a polynomial-time algorithm is designed and proved to output a simple schedule that achieves the approximate capacity. The key ingredient of the algorithm is to leverage similarities between network states in HD and edge coloring in a graph. It is also shown that the algorithm allows to derive a closed-form expression for the approximate capacity of the Gaussian line network that can be evaluated distributively and in linear time.

Exact Speed and Transmission Cost in a Simple One-Dimensional Wireless Delay-Tolerant Network (15:40)

Dimitrios Cheliotis (University of Athens, Greece); Ioannis Kontoyiannis (Athens UniversityEcon & Business, Greece); Michail Loulakis (National Technical University of Athens, Greece); ***Stavros Toumpis*** *(Research Center - Athens University of Economics and Business, Greece)*

We study a simple one-dimensional, discrete-time network model that consists of two nodes moving on a discrete circle, changing their direction of movement randomly, and a single packet traveling in the clockwise direction, using combinations of transmissions between the two nodes (when they are co-located) and physical transports on their buffers. In this setting, we provide exact, explicit expressions for the long-term averages of the packet speed and the wireless transmission cost. Our work is a first step towards providing simple and exact results for more realistic wireless delay-tolerant network models.

Analysis of Breakdown Probability of Wireless Sensor Networks with Unreliable Relay Nodes (16:00)

Takayuki Nozaki (Yamaguchi University, Japan); Takafumi Nakano (Nagoya Institute of Technology, Japan); Tadashi Wadayama (Nagoya Institute of Technology, Japan)

In the present paper, we derive an upper bound of the average network breakdown probability of packet networks with unreliable relay nodes. We here assume that relay nodes get independently broken with a given node breakdown probability. A survivor graph is the induced subgraph obtained by removing the broken relay nodes and their connecting edges from the original graph. If the survivor network is disconnected, we consider a network breakdown happens. The primal contribution of the paper is to derive an upper bound of the average network breakdown probability, where the expectation is taken over a regular graph ensemble. The proof of the bound is based on a natural one-to-one correspondence between a regular graph and a regular bipartite graph, and also on enumeration of bipartite graphs satisfying certain conditions. This proof argument is inspired by the analysis of weight distribution for low-density parity-check codes. Compared with estimates of the average network breakdown probability obtained by computer experiments, it is observed that the upper bound provides the values which are not only upper bounds but also precise estimates of the network breakdown probability when the node breakdown probability is small.

Mo3-7: Communications 1

Monday, June 26, 14:40-16:20
Room: K6
Chair: Nan Liu (Southeast University, P.R. China)

Optimal Frame Synchronization Over a Finite State Markov Channel (14:40)

M Sundaram R (Indian Institute of Technology Madras, India); Arup Das (Indian Institute of Technology Madras, India); Devendra Jalihal (Indian Institute of Technology Madras, India); Venkatesh Ramaiyan (Indian Institute of Technology Madras, India)

We study a problem of sequential frame detection over a finite state Markov channel (FSMC). We consider an asynchronous framework, where a sync frame of length N symbols is transmitted uniformly over a large interval of known size A slots. In this setup, we study the scaling needed of the sync frame length N with the asynchronism interval length A for error-free frame synchronization. We study the problem when channel state information (CSI) is known at the transmitter and the receiver, and compute a synchronization threshold, $\bar{\alpha}$, that relates the average sync frame length $\bar{N}$ and A as $\bar{N} > \frac{\log_2(A)}{\bar{\alpha}}$ for asymptotic frame synchronization. Our discussion includes the description of a variable length and adaptive code word for FSMC that achieves the optimal delay performance.

Two-way Interference Channels with Jammers (15:00)

Sidharth Jaggi (Chinese University of Hong Kong, Hong Kong); Michael Langberg (State University of New York at Buffalo, USA)

Alice and Bob want to exchange information over an additive interference channel that also contains a malicious eavesdropper-jammer James who aims to disrupt this two-way communication. In the baseline model (motivated by wireless jamming scenarios), Alice and Bob transmit length-n q-ary encodings x_A and x_B respectively of their own messages. James observes the interference pattern $z = x_A + x_B$, and as a non-causal function of z and his knowledge of Alice and Bob's codebooks, chooses a jamming pattern s of power (Hamming weight) at most pn. Alice and Bob then both observe the interfered-jammed signal $x_A + x_B + s$, and aim to decode each others' messages despite the jamming pattern s. We demonstrate that in such a model, the fact of interference actually aids communication by allowing for communication to occur in each direction at a rate of $1 - H_q(p)$, i.e., the jammer can do no worse than act like "random noise". Interestingly, neither linear codes nor random codes (as "usually" defined) achieve this performance — we thus define and analyze a new class of "linearish" codes that do. We then extend our results to general

q-ary additive-error channels with asymmetric jamming patterns (with potentially different powers) to Alice and Bob, and also demonstrate how to simultaneously ensure information-theoretic secrecy of both Alice and Bob's messages from James.

Bit-Interleaved Coded Modulation for Phase Shift Keying on the Hypersphere (15:20)

Christoph Rachinger (University of Erlangen-Nuremberg, Germany); Ralf Müller (FAU Erlangen-Nürnberg, Germany); Johannes Huber (University of Erlangen-Nuremberg, Germany)

We analyze the performance of Bit-Interleaved Coded Modulation (BICM) for Multiple-Input Multiple-Output (MIMO) systems employing Phase Shift Keying on the Hypersphere (PSKH), an extension of Phase Shift Keying (PSK) to higher dimensions. Because the quality of BICM relies on the bit-mapping between coded bits and signal points, PSKH constellations with superior distance properties and capacities might have poor power efficiency. In this paper, we analyze these losses in power efficiency and propose a new method to generate PSKH constellations, i.e., spherical codes, together with a BICM optimized bit-mapping. It turns out that for one bit per real dimension, individual QPSK per antenna is optimal, whereas for other constellation sizes notable gains can be achieved.

Rigorous Dynamics of Expectation-Propagation-Based Signal Recovery from Unitarily Invariant Measurements (15:40)

Keigo Takeuchi (Toyohashi University of Technology, Japan)

This paper investigates sparse signal recovery based on expectation propagation (EP) from unitarily invariant measurements. A rigorous analysis is presented for the state evolution (SE) of an EP-based message-passing algorithm in the large system limit, where both input and output dimensions tend to infinity at an identical speed. The main result is the justification of an SE formula conjectured by Ma and Ping.

Geometrically uniform differential vector signaling schemes (16:00)

Ezio Biglieri (Universitat Pompeu Fabra, Barcelona, Spain); Emanuele Viterbo (Monash University, Australia)

Using a geometric approach, we examine the design and the performance of geometrically uniform line coding schemes transmitting b bits over $w = b + 1$ wires and obtained from a subset of a permutation modulation signal set.

Mo3-8: Compressed Sensing 1

Monday, June 26, 14:40-16:20
Room: K7+8
Chair: Gerhard Wunder (FU Berlin, Heisenberg Communications and Information Theory Group, Germany)

Statistical and computational phase transitions in spiked tensor estimation (14:40)

Thibault Lesieur (Institut de Physique Théorique CEA, France); Leo Miolane (INRIA and ENS, France); Marc Lelarge (INRIA and ENS, France); Florent Krzakala (Ecole Normale Superieure, France); Lenka Zdeborova (Institut de Physique Theorique IPhT, CEA Saclay and CNRS, France)

We consider tensor factorizations using a generative model and a Bayesian approach. We compute rigorously the mutual information, the Minimal Mean Square Error (MMSE), and unveil information-theoretic phase transitions. In addition, we study the performance of Approximate Message Passing (AMP) and show that it achieves the MMSE for a large set of parameters, and that factorization is algorithmically "easy" in a much wider region than previously believed. It exists, however, a "hard" region where AMP fails to reach the MMSE and we conjecture that no polynomial algorithm will improve on AMP.

Corrupted Sensing with Sub-gaussian Measurements (15:00)

Jinchi Chen *(Beijing Institute of Technology, P.R. China); Yulong Liu (Beijing Institute of Technology, P.R. China)*

This paper studies the problem of accurately recovering a structured signal from a small number of corrupted sub-gaussian measurements. We consider three different procedures to reconstruct signal and corruption when different kinds of prior knowledge are available. In each case, we provide conditions for stable signal recovery from structured corruption with added unstructured noise. The key ingredient in our analysis is an extended matrix deviation inequality for isotropic sub-gaussian matrices.

On the Phase Transition of Corrupted Sensing (15:20)

Huan Zhang *(Institute of Electronics, Chinese Academy of Sciences, P.R. China); Yulong Liu (Beijing Institute of Technology, P.R. China); Lei Hong (Institute of Electronics, Chinese Academy of Sciences, P.R. China)*

A sharp phase transition has been numerically observed when a constrained convex procedure is used to solve the corrupted sensing problem. In this paper,

we present a theoretical analysis for this phenomenon. Specifically, we establish the threshold below which this convex procedure fails to recover signals and there is corruption with high probability. We prove that a sharp phase transition occurs around the sum of the squares of spherical Gaussian widths of two tangent cones. Numerical experiments are provided to demonstrate the correctness and sharpness of our results.

On the Success Probability of the Box-Constrained Rounding and Babai Detectors (15:40)

Jinming Wen (University of Alberta, Canada); ***Xiao-Wen Chang*** *(McGill University, Canada); Chintha Tellambura (University of Alberta, Canada)*

In communications, one frequently needs to detect a parameter vector $\hat{\boldsymbol{x}}$ in a box from a linear model. The box-constrained rounding detector $\boldsymbol{x}^{\mathsf{BR}}$ and Babai detector $\boldsymbol{x}^{\mathsf{BB}}$ are often used to detect $\hat{\boldsymbol{x}}$ due to their high probability of correct detection, which is referred to as success probability, and their high efficiency of implimentation. It is generally believed that the success probability P^{BR} of $\boldsymbol{x}^{\mathsf{BR}}$ is not larger than the success probability P^{BB} of $\boldsymbol{x}^{\mathsf{BB}}$. In this paper, we first present formulas for P^{BR} and P^{BB} for two different situations: $\hat{\boldsymbol{x}}$ is deterministic and $\hat{\boldsymbol{x}}$ is uniformly distributed over the constraint box. Then, we give a simple example to show that P^{BR} may be strictly larger than P^{BB} if $\hat{\boldsymbol{x}}$ is deterministic, while we rigorously show that $P^{\mathsf{BR}} \leq P^{\mathsf{BB}}$ always holds if $\hat{\boldsymbol{x}}$ is uniformly distributed over the constraint box.

A Characterization of Sampling Patterns for Low-Tucker-Rank Tensor Completion Problem (16:00)

Morteza Ashraphijuo (Columbia University, USA); Vaneet Aggarwal (Purdue University, USA); Xiaodong Wang (Columbia University, USA)

In this paper, we characterize the deterministic conditions on the locations of the sampled entries, which are equivalent (necessary and sufficient) to finite completability of a low-rank tensor given some components of its Tucker rank. In order to derive this characterization, we propose an algebraic geometric analysis on the Tucker manifold, which allows us to incorporate multiple rank components in the proposed analysis in contrast with the conventional geometric approaches on the Grassmannian manifold. Then, using the developed tools for this analysis, we also derive a sufficient condition on the sampling pattern that ensures there exists only one completion for the sampled tensor (unique completability).

Mo3-9: MIMO 1

Monday, June 26, 14:40-16:20
Room: K9
Chair: Christoph Studer (Cornell University, USA)

Asymptotic Capacity Results for MIMO Wireless Optical Communication (14:40)

Stefan Moser (ETH Zurich & National Chiao Tung University (NCTU), Switzerland); Michail Mylonakis (ETH Zürich, Switzerland); Ligong Wang (ETIS & CNRS, France); Michele Wigger (Telecom ParisTech, France)

This paper provides several asymptotic capacity results for the multiple-input multiple-output free-space optical intensity channel in the regime of high signal-to-noise ratio (SNR). For the case where the channel matrix has full column rank, the asymptotic capacity is derived assuming a peak-power constraint on each transmit antenna, or an average-power constraint on the total power across all transmit antennas, or both. For multiple-input and single-output channels, the asymptotic high-SNR capacity is derived when either only the total average power is constrained, or only the per-antenna peak power is constrained, or both but with the average-power constraint being sufficiently loose.

On Capacity of Noncoherent MIMO with Asymmetric Link Strengths (15:00)

Joyson Sebastian (University of California, Los Angeles, USA); Ayan Sengupta (Stanford University, USA); Suhas Diggavi (University of California Los Angeles, USA)

We study the generalized degrees of freedom (gDoF) of the block-fading noncoherent MIMO channel with asymmetric distributions of link strengths, and a coherence time of T symbol durations. We first derive the optimal signaling structure for communication over this channel, which is distinct from that for the i.i.d MIMO setting. We prove that for T=1, the gDoF is zero for MIMO channels with arbitrary link strength distributions, extending the result for MIMO with i.i.d links. We then show that selecting the statistically best antenna is gDoF-optimal for both Multiple Input Single Output (MISO) and Single Input Multiple Output (SIMO) channels. We also derive the gDoF for the 2x2 MIMO channel with different exponents in the direct and cross links. In this setting, we show that it is always necessary to use both antennas to achieve the optimal gDoF, in contrast to the results for 2x2 MIMO with identical link distributions.

On the Degrees-of-Freedom of the MIMO Three-Way Channel with Intermittent Connectivity (15:20)

Anas Chaaban (King Abdullah University of Science and Technology, Saudi Arabia); Aydin Sezgin (RUB, Germany); Mohamed-Slim Alouini (King Abdullah University of Science and Technology (KAUST), Saudi Arabia)

The degrees-of-freedom (DoF) of the multi-antenna three-way channel (3WC) with an intermittent node is studied. Special attention is given to the impact of adaptation. A nonadaptive transmission scheme based on interference alignment, zero-forcing, and erasure-channel treatment is proposed, and its corresponding DoF region is derived. Then, it is shown that this scheme achieves the sum-DoF of the intermittent channel, in addition to the DoF region of the nonintermittent one. Thus, adaptation is not necessary from those perspectives. To the contrary, it is shown that adaptation is necessary for achieving the DoF region of the intermittent case. This is shown by deriving an outer bound for the intermittent channel with nonadaptive encoding, and giving a counterexample of an adaptive scheme which achieves DoF tuples outside this bound. This highlights the importance of cooperation in this intermittent network.

Outage Information Rate of Spatially Correlated Multi-Cluster Scattering MIMO Channels (15:40)

Giorgio Taricco (Politecnico di Torino, Italy); Giuseppa Alfano (Politecnico di Torino, Italy)

A one-sided spatially-correlated multi-cluster scattering Rayleigh MIMO channel is considered in this work and its outage probability is derived in an analytic form based on Meijer function determinants. First, the spatially-uncorrelated case is addressed and the Moment Generating Function (MGF) of the information rate is expressed in an analytic closed-form. The MGF is then used to obtain the outage probability. A few special cases are addressed to provide a confirmation of the analytic results. Next, the MGF in the one-sided spatially correlated case is derived with the constraint of distinct positive spatial eigenvalues. Numerical results are included to provide confirming evidence of the analytic results. These results are then used to assess the outage probability degradation due to spatial correlation in a selected example.

A Generalized Zero-Forcing Precoder for Multiple Antenna Gaussian Broadcast Channels (16:00)

Sha Hu (Lund University, Sweden); Fredrik Rusek (Lund University, Sweden)

In this paper, we consider precoder design for multiuser multiple-input-multiple-output (MIMO) Gaussian broadcast (BC) channels and propose a generalized zero-forcing (GZF) precoder based on successive dirty-paper coding (DPC), i.e., the GZF-DP precoder. The GZF-DP precoder is an extension of the GZF-DP precoder designed earlier for multi-input-single-output broadcast (MISO-BC) channels, and also a generalization of both the linear block-diagonalization ZF (BD-ZF) and the successive ZF with DPC (SZF-DPC) precoders. With the GZF-DP precoder, the depth of the inter-user interference after precoding (and before the DPC) can be specified at will by a parameter v, which provides a trade-off between the optimal rates and the DPC implementation-complexity. Utilizing DPC, the known noncausal inter-user interferences from the other (up to) v users are canceled through successive encoding. Within the class of GZF-DP, we analyze the optimal precoder designs both for sum-rate and minimum user-rate maximizations, which are solved in closed-forms in conjunction with water-filling algorithms depending on v. We show through numerical results that, the proposed GZF-DP precoder with a small v renders significant rate increments compared to the linear BD-ZF precoder, and is close to the SZF-DP preocder with a much less DPC complexity.

Mo3-A: Age of Information 3

Monday, June 26, 14:40-16:20
Room: Berlin 3
Chair: Elif Uysal-Biyikoglu (METU, Turkey)

Age of Information: Design and Analysis of Optimal Scheduling Algorithms (14:40)

Yu-Pin Hsu *(National Taipei University, Taiwan); Eytan Modiano (MIT, USA); Lingjie Duan (Singapore University of Technology and Design (SUTD), Singapore)*

Age of information is a newly proposed metric that captures delay from an application layer perspective. The age measures the amount of time that elapsed from the moment the mostly recently received update was generated until the present time. In this paper, we study an age minimization problem over a wireless broadcast network with many users, where only one user can be served at a time. We formulate a Markov decision process (MDP) to find dynamic transmission scheduling schemes, with the purpose of minimizing the long-run average age. While showing that an optimal scheduling algorithm for the MDP is a simple stationary switch-type, we propose a sequence of finite-state approximations for our infinite-state MDP and prove its convergence. We then propose both optimal off-line and on-line scheduling algorithms for the finite-approximate MDPs, depending on knowledge of time-varying arrivals.

Backlog-Adaptive Compression: Age of Information (15:00)

Jing Zhong *(Rutgers University, USA); Roy Yates (Rutgers University, USA); Emina Soljanin (Rutgers University, USA)*

The end-to-end delay of streaming source coding is characterized by an age of information (AoI) metric that measures the number of symbol periods the decoder output lags behind the encoder input. The source encoder receives input source symbols one per unit time and sequentially outputs binary codewords to a constant rate channel that transmits bits to the decoder. We examine a system in which knowledge of the busy/idle state at the channel interface enables the encoder to switch among codebooks with different source blocklengths based on the backlog of symbols at the encoder. We start by introducing two source sequence parsing policies and show that in each of them the blocklength process can be modeled by a Markov chain. We show by experiments that blocklength adjustment based on the channel interface state provides lower average age than codes with fixed blocklength. Aiming to avoid unnecessary frequent blocklength changes by the encoder backlog, we propose maximum blocklength control scheme at the encoder to further reduce the average age.

The Stationary Distribution of the Age of Information in FCFS Single-Server Queues (15:20)

Yoshiaki Inoue (Osaka University, Japan); Hiroyuki Masuyama (Kyoto University, Japan); Tetsuya Takine (Osaka University, Japan); Toshiyuki Tanaka (Kyoto University, Japan)

We consider the stationary distributions of the age of information (AoI) and the peak AoI in information update systems. We first derive an invariant relation among the distributions of the AoI, the peak AoI, and the system delay, which holds for a wide class of information update systems. Next, based on it, we obtain general formulas for the stationary distributions of the AoI and the peak AoI in the first-come first-served (FCFS) GI/GI/1 queue, as a general model of information update systems. Finally, we derive explicit formulas for the Laplace-Stieltjes transforms of the stationary distributions of the AoI and the peak AoI in FCFS M/GI/1 and GI/M/1 queues.

Age-optimal Information Updates in Multihop Networks (15:40)

Ahmed Bedewy (The Ohio State University, USA); Yin Sun (the Ohio State University, USA); Ness Shroff (The Ohio State University, USA)

The problem of reducing the age-of-information has been extensively studied in the single-hop networks. In this paper, we minimize the age-of-information in general multihop networks. If the packet transmission times over the network links are exponentially distributed, we prove that a preemptive Last Generated First Served (LGFS) policy results in smaller age processes at all nodes of the network (in a stochastic ordering sense) than any other causal policy. In addition, for arbitrary general distributions of packet transmission times, the non-preemptive LGFS policy is shown to minimize the age processes at all nodes of the network among all non-preemptive work-conserving policies (again in a stochastic ordering sense). It is surprising that such simple policies can achieve optimality of the joint distribution of the age processes at all nodes even under arbitrary network topologies, as well as arbitrary packet generation and arrival times. These optimality results not only hold for the age processes, but also for any non-decreasing functional of the age processes.

Communication over a Channel that Wears Out (16:00)

Ting-Yi Wu (University of Illinois at Champaign-Urbana, USA); Lav Varshney (University of Illinois at Urbana-Champaign, USA); Vincent Tan (National University of Singapore, Singapore)

This work investigates the limits of communication over a noisy channel that wears out, in the sense of signal-dependent catastrophic failure. In particular, we consider a channel that starts as a memoryless binary-input channel and when the number of transmitted ones causes a sufficient amount of damage, the channel ceases to convey signals. We restrict attention to constant composition codes. Since infinite blocklength codes will always wear out the channel for any finite threshold of failure and therefore convey no information, we analyze the performance of finite blocklength codes to determine the maximum expected transmission volume at a given level of average error probability. We show that this maximization problem has a recursive form and can be solved by dynamic programming. A discussion of damage state feedback in channels that wear out is also provided. Numerical results show that a sequence of block codes is preferred to a single block code for streaming sources.

Mo4-1: Coding Theory 1

Monday, June 26, 16:40-18:20
Room: Europa
Chair: Juergen Freudenberger (University of Applied Sciences, Konstanz, Germany)

Non-linear Cyclic Codes that Attain the Gilbert-Varshamov Bound (16:40)

Ishay Haviv (The Academic College of Tel Aviv-Yaffo, Israel); Michael Langberg (State University of New York at Buffalo, USA); Moshe Schwartz (Ben-Gurion University of the Negev, Israel); Eitan Yaakobi (Technion, Israel)

We prove that there exist non-linear binary cyclic codes that attain the Gilbert-Varshamov bound.

Strong Functional Representation Lemma and Applications to Coding Theorems (17:00)

Cheuk Ting Li *(Stanford University, USA); Abbas El Gamal (Stanford University, USA)*

This paper shows that for any random variables X and Y, it is possible to represent Y as a function of (X, Z) such that Z is independent of X and $I(X;Z|Y) \leq \log(I(X;Y)+1)+4$. We use this strong functional representation lemma (SFRL) to establish a tighter bound on the rate needed for one-shot exact channel simulation than was previously established by Harsha et. al., and to establish achievability results for one-shot variable-length lossy source coding and multiple description coding. We also show that the SFRL can be used to reduce the channel with state noncausally known at the encoder to a point-to-point channel, which provides a simple achievability proof of the Gelfand-Pinsker theorem. Finally we present an example in which the SFRL inequality is tight to within 5 bits.

On the VC-Dimension of Binary Codes (17:20)

Sihuang Hu (Tel Aviv University, Israel); ***Nir Weinberger*** *(Technion, Israel); Ofer Shayevitz (Tel Aviv University, Israel)*

We investigate the asymptotic rates of length-n binary codes with VC-dimension at most dn and minimum distance at least δn. Two upper bounds are obtained, one as a simple corollary of a result by Haussler and the other via a shortening approach combining Sauer–Shelah lemma and the linear programming bound. Two lower bounds are given using Gilbert–Varshamov type arguments over constant-weight and Markov-type sets.

Duality of channels and codes (17:40)

Joseph Renes (ETH Zurich, Switzerland)

For any given channel with classical inputs and possibly quantum outputs, a dual classical-input channel can be defined by embedding the original into a channel with quantum inputs and outputs. Here we give new uncertainty relations for a general class of entropies that lead to very close relationships between the original channel and its dual. Moreover, we show that channel duality can be combined with duality of linear codes, whereupon the uncertainty relations imply that the performance of a given code over a given channel is entirely characterized by the performance of the dual code on the dual channel. This has several applications. In the context of polar codes, it implies that the rates of polarization to ideal and useless channels must be identical. Duality also relates the tasks of channel coding and privacy amplification, implying that the finite blocklength performance of extractors and codes is precisely linked, and that optimal rate extractors can be transformed into capacity-achieving codes, and vice versa. Finally, duality also extends to the EXIT function of any channel and code. Here it implies that for any channel family, if the EXIT function for a fixed code has a sharp transition, then it must be such that the rate of the code equals the capacity at the transition. This may give a different route to proving a code family achieves capacity by establishing EXIT function transitions.

Polynomial Ring Transforms for Efficient XOR-based Erasure Coding (18:00)

Jonathan Detchart (University of Toulouse & ISAE, France); Jerome Lacan (University of Toulouse, France)

The complexity of software implementations of MDS erasure codes mainly depends on the efficiency of the finite field operations implementation. In this paper, we propose a method to reduce the complexity of the finite field multiplication by using simple transforms between a field and a ring to perform the multiplication in a ring. We show that moving to a ring reduces the complexity of the operations. Then, we show that this construction allows the use of simple scheduling to reduce the number of operations.

Mo4-2: Coding for Storage

Monday, June 26, 16:40-18:20
Room: Brussels
Chair: Camilla Hollanti (Aalto University, Finland)

Secure RAID Schemes from EVENODD and STAR Codes (16:40)

Wentao Huang (California Institute of Technology, USA); Jehoshua Bruck (California Institute of Technology, USA)

We study secure RAID, i.e., low-complexity schemes to store information in a distributed manner that is resilient to node failures and resistant to node eavesdrop-

ping. We describe a technique to shorten a previously developed secure EVENODD scheme, which can optimally tolerate 2 node failures and 2 eavesdropping nodes. The shortening technique allows us to obtain secure EVENODD schemes of arbitrary lengths, which is important for practical application. We also construct a new secure RAID scheme from the STAR code. The scheme can tolerate 3 node failures and 3 eavesdropping nodes with optimal encoding/decoding and random access complexity.

Sector-disk codes with three global parities (17:00)

Xiao Li *(University of Illinois at Urbana-Champaign, USA); Iwan Duursma (University of Illinois at Urbana-Champaign, USA)*

Codewords in array format find applications in disk storage where columns are stored on different disks in combination with parity checks across disks that protect data against disk failures. The addition of global parities protects against sector failures on any of the disks while keeping storage overhead low. We construct sector-disk array codes that tolerate any combination of two disk failures and three sector failures with minimal overhead. The construction is the first for codes of this type that does not rely on exhaustive search.

Coding for Racetrack Memories (17:20)

Yeow Meng Chee (Nanyang Technological University, Singapore); Han Mao Kiah (Nanyang Technological University, Singapore); Alexander Vardy (University of California San Diego, USA); Van Khu Vu (Nanyang Technological University, Singapore); Eitan Yaakobi (Technion, Israel)

Racetrack memory is a new technology which utilizes magnetic domains along a nanoscopic wire in order to obtain extremely high storage density. In racetrack memory, each magnetic domain can store a single bit of information, which can be sensed by a reading port (head). The memory has a tape-like structure which supports a shift operation that moves the domains to be read sequentially by the head. In order to increase the memory's speed, prior work studied how to minimize the latency of the shift operation, while the no less important reliability of this operation has received only a little attention. In this work we design codes which combat shift errors in racetrack memory, called position errors. Namely, shifting the domains is not an error-free operation and the domains may be over-shifted or are not shifted, which can be modeled as deletions and sticky insertions. While it is possible to use conventional deletion and insertion-correcting codes, we tackle this problem with the special structure of racetrack memory where the domains can be read by multiple heads. Each head outputs a noisy version of the stored data and the multiple outputs are combined in order to reconstruct the data. Under this paradigm, we will show that it is possible to correct, with at most a single bit of redundancy, d deletions with d+1 heads if the heads are well-separated. Similar results are provided for burst of deletions, sticky insertions and combinations of both deletions and sticky insertions.

On the Tradeoff Region of Secure Exact-Repair Regenerating Codes (17:40)

Shuo Shao (Texas A&M University, USA); Tie Liu (Texas A&M University, USA); Chao Tian (University of Tennessee Knoxville, USA); Cong Shen (University of Science and Technology of China, P.R. China)

We consider the (n, k, d, ℓ) secure exact-repair regenerating code problem, which generalizes the (n, k, d) exact-repair regenerating code problem with the additional constraint that the stored file needs to be kept information-theoretically secure against an eavesdropper, who can access the data transmitted to regenerate a total of ℓ different failed nodes. For all known results on this problem, the achievable tradeoff regions between the normalized storage capacity and repair bandwidth have a single corner point, achieved by a scheme proposed by Shah, Rashmi and Kumar (the SRK point). Since the achievable tradeoff regions of the exact-repair regenerating code problem without any secrecy constraints are known to have multiple corner points in general, these existing results suggest a phase-change-like behavior, i.e., enforcing a secrecy constraint ($\ell \geq 1$) immediately reduces the tradeoff region to one with a single corner point. In this work, we first show that when the secrecy parameter ℓ is sufficiently large, the SRK point is indeed the only corner point of the tradeoff region. However, when ℓ is small, we show that the tradeoff region can in fact have multiple corner points. In particular, we establish a precise characterization of the tradeoff region for the $(7, 6, 6, 1)$ problem, which has exactly two corner points. Thus, a smooth transition, instead of a phase-change-type of transition, should be expected as the secrecy constraint is gradually strengthened.

Construction of Unrestricted-Rate Parallel Random Input-Output Code (18:00)

Shan Lu (Gifu University, Japan); Hiroshi Kamabe (Gifu University, Japan); Jun Cheng (Doshisha University, Japan); Akira Yamawaki (Gifu University, Japan)

A coding scheme for two-page unrestricted-rate P-RIO code that each page may have different code rates is proposed. In the second page, the code for each messages consists of two complementary codewords. There are total of 2^{n-1} codes which are disjoint to guarantees uniquely-decodable for 2^{n-1} messages. In the first page, the code for each message consists of all weight-u vectors with their non-zero elements restricted to $(2u-1)$ same positions, where non-negative integer u is less than or equal to half of code length. Finding disjoint codes in the first page is equivalent to

construction of constant-weight codes, and the number of codes in the first page is the best-known number of codewords in constant-weight codes. Our coding scheme is constructive, and the code length is arbitrary. The sum rate of our proposed code are higher than that of previous work.

Mo4-3: Interference Channels 1

Monday, June 26, 16:40-18:20
Room: K2
Chair: Daniela Tuninetti (University of Illinois at Chicago, USA)

Two-way interference channel capacity: How to have the cake and eat it too (16:40)

Changho Suh (KAIST, Korea); Jaewoong Cho (KAIST, Korea); David Tse (Stanford University, USA)

Two-way communication is prevalent and its fundamental limits are first studied in the point-to-point setting by Shannon [1]. One natural extension is a two-way interference channel (IC) with four independent messages: two associated with each direction of communication. In this work, we explore a deterministic two-way IC which captures key properties of the wireless Gaussian channel. Our main contribution lies in the complete capacity region characterization of the two-way IC via a new achievable scheme. One surprising consequence of this result is that not only we can get an interaction gain over the one-way non-feedback capacities, we can sometimes get all the way to perfect feedback capacities in both directions simultaneously.

Capacity Region of the Symmetric Injective K-User Deterministic Interference Channel (17:00)

Mehrdad Kiamari (University of Southern California, USA); Salman Avestimehr (University of Southern California, USA)

We characterize the capacity region of the symmetric K-user Deterministic Interference Channel (DIC) for all channel parameters. The achievable rate region is derived by first projecting the achievable rate region of Han-Kobayashi (HK) scheme, which is in terms of common and private rates for each user, along the direction of aggregate rates for each user (i.e., the sum of common and private rates). We then show that the projected region is characterized by only the projection of those facets in the HK region for which the coefficient of common rate and private rate are the same for all users, hence simplifying the region. Furthermore, we derive a tight converse for each facet of the simplified achievable rate region.

State-Dependent Z-Interference Channel with Correlated States (17:20)

Yunhao Sun *(Syracuse University, USA); Yingbin Liang (Syracuse University, USA); Ruchen Duan (Samsung Semiconductor Inc., USA); Shlomo (Shitz) Shamai (The Technion, Israel)*

This paper investigates the Gaussian state-dependent Z-interference channel (Z-IC), in which two receivers are respectively corrupted by correlated states that are noncausally known to transmitters and unknown to receivers. Three interference regimes are studied, and the capacity region or sum capacity boundary is characterized either fully or partially under various channel parameters. The impact of correlation between states on state and interference cancelation as well as capacity achievability is demonstrated via numerical analysis.

Novel Outer Bounds and Capacity Results for the Interference Channel with Conferencing Receivers (17:40)

Reza K. Farsani (University of Waterloo, Canada); Amir K. Khandani (University of Waterloo, Canada)

Capacity bounds for the two-user interference channels with cooperative receivers via conferencing links of finite capacities are investigated. Capacity results known for these communication scenarios are limited to a very few special cases of the one-sided channels. One of the major challenges in analyzing such cooperative networks is how to establish efficient capacity outer bounds for them. In this paper, by applying new techniques, novel capacity outer bounds are established for the interference channels with conferencing receivers. Using the outer bounds, several new capacity results are proved for interesting channels with unidirectional cooperation in strong and mixed interference regimes. A fact is that a conferencing link (between receivers) may be utilized to provide one receiver with information about its corresponding signal or its non-corresponding signal (interference signal). As an interesting consequence, it is demonstrated that both strategies can be helpful to achieve capacity. Lastly, for the case of Gaussian interference channel with conferencing receivers, it is argued that our outer bound is strictly tighter than the previous one derived by Wang and Tse.

Approximate Capacity of a Class of Partially Connected Interference Channels (18:00)

Muryong Kim *(University of Texas at Austin, USA); Yitao Chen (University of Texas at Austin, USA); Sriram Vishwanath (University of Texas Austin, USA)*

We derive inner and outer bounds on the capacity region for a class of three-user partially connected interference channels. We focus on the impact of topology, interference alignment, and interplay between interference and noise. The representative channels we consider are the ones that have clear interference align-

ment gain. For these channels, Z-channel type outer bounds are tight to within a constant gap from capacity. We present near-optimal achievable schemes based on rate-splitting, lattice alignment, and successive decoding.

Mo4-4: Shannon Inequalities

Monday, June 26, 16:40-18:20
Room: K3
Chair: Haim Permuter (Ben-Gurion University, Israel)

Wasserstein Stability of the Entropy Power Inequality for Log-Concave Random Vectors (16:40)

Thomas Courtade (University of California, Berkeley, USA); Max Fathi (CNRS & Université Paul Sabatier, Institut de Mathématiques de Toulouse, France); Ashwin Pananjady (University of California, Berkeley, USA)

We establish quantitative stability results for the entropy power inequality (EPI) in arbitrary dimension. Specifically, we show that if uniformly log-concave densities nearly saturate the EPI, then they must be close to Gaussian densities in the quadratic Wasserstein distance. Further, if one of the densities is log-concave and the other is Gaussian, then the deficit in the EPI can be controlled in terms of the L^1-Wasserstein distance. As a counterpoint, an example shows that the EPI can be unstable with respect to the quadratic Wasserstein distance even if densities are uniformly log-concave on sets of measure arbitrarily close to one. The proofs are based on optimal transportation.

Two-Moment Inequalities for Renyi Entropy and Mutual Information (17:00)

Galen Reeves (Duke University, USA)

This paper explores some applications of a two-moment inequality for the integral of the r-th power of a function, where 0<r<1. The first contribution is an upper bound on the Renyi entropy of a random vector in terms of the two different moments. When one of the moments is equal to zero, these bounds recover previous results based on maximum entropy distributions under a single moment constraint. More generally, evaluation of the bound with two carefully chosen nonzero moments can lead to significant improvements with a modest increase in complexity. The second contribution is a method for upper bounding mutual information in terms of certain integrals with respect to the variance of the conditional density. The bounds have a number of useful properties arising from the connection with variance decompositions.

One-shot Multivariate Covering Lemmas via Weighted Sum and Concentration Inequalities (17:20)

Mohammad Hossein Yassaee (Princeton University, USA); Jingbo Liu (Princeton University, USA); Sergio Verdú (Princeton University, USA)

New one-shot bounds for multivariate covering are derived via a weighted sum technique and a one-sided concentration inequality which is stronger than the McDiarmid inequality.The new bounds are more compact and sharper than known bounds in the literature. In particular, the covering error can be shown to decay doubly exponential in the blocklength. Implications for the error exponent in broadcast channels are discussed.

A min-entropy power inequality for groups (17:40)

*Peng Xu (University of Delaware, USA); **James Melbourne** (University of Delaware, USA); Mokshay Madiman (University of Delaware, USA)*

We will develop a general notion of rearrangement for certain metric groups, and prove a Hardy-Littlewood type inequality. Combining this with a characterization of the extreme points of the set of probability measures with bounded densities with respect to a reference measure we will establish a general min-entropy inequality for convolutions. Special attention will be paid to the integers where a min-entropy power inequality will be conjectured and a partial result proved.

A Minimal Set of Shannon-type Inequalities for Functional Dependence Structures (18:00)

Satyajit Thakor (Indian Institute of Technology Mandi, India); Terence Chan (University of South Australia, Australia); Alex Grant (Myriota Pty Ltd, Australia)

The minimal set of Shannon-type inequalities (referred to as elemental inequalities), plays a central role in determining whether a given inequality is Shannon-type. Often, there arises a situation where one needs to check whether a given inequality is a constrained Shannon-type inequality. Another important application of elemental inequalities is to formulate and compute the Shannon outer bound for multi-source multi-sink network coding capacity. Under this formulation, it is the region of feasible source rates subject to the elemental inequalities and network coding constraints that is of interest. Hence it is of fundamental interest to identify the redundancies induced amongst elemental inequalities when given a set of functional dependence constraints. In this paper, we characterize a minimal set of Shannon-type inequalities when functional dependence constraints are present.

Mo4-5: Bounds 1

Monday, June 26, 16:40-18:20
Room: K4
Chair: Martina Cardone (University of Califonia, Los Angeles, USA)

Sum-set Inequalities from Aligned Image Sets: Instruments for Robust GDoF Bounds (16:40)

Arash Gholami Davoodi (University of California, Irvine, USA); ***Syed Jafar*** *(University of California Irvine, USA)*

We present sum-set inequalities specialized to the generalized degrees of freedom (GDoF) framework. These are information theoretic lower bounds on the entropy of bounded density linear combinations of discrete, power-limited dependent random variables in terms of the joint entropies of arbitrary linear combinations of new random variables that are obtained by power level partitioning of the original random variables. The bounds are useful instruments to obtain GDoF characterizations for wireless interference networks, especially with multiple antenna nodes, subject to arbitrary channel strength and channel uncertainty levels.

Scaling Exponent of Sparse Random Linear Codes over Binary Erasure Channels (17:00)

Hessam Mahdavifar (University of Michigan, USA)

The problem of analyzing the finite-length scaling behavior of sparse random linear codes is considered. Random linear codes with random generator matrices whose entries are picked according to i.i.d. Bernoulli distribution with parameter $q = o(1)$ are called *sparse*. The parameter q is referred to as the *sparsity* of the random linear code. We develop a methodology to show the optimality of the scaling exponent of uniform random linear codes, i.e., $q = 1/2$, with high probability. The results are then extended to sparse random linear codes with sparsity $q = \Theta(n^{-1/2})$, where n is the code block length. The encoding complexity of such sparse random linear codes is reduced from $O(n^2)$, in uniform random linear codes, to $O(n^{1/2})$. It is also conjectured that $q = \log n/n$ is the lowest sparsity of random linear codes with optimal scaling exponent. The connection of these results to an open problem regarding finding binary polar codes with optimal scaling exponent are also discussed. In particular, we point out that as the size of the polarization kernel increases it can be used as the generator matrix for a code with optimal scaling exponent, without the need to do further polarization.

A Frequency-Domain Approach to Tightening the Generalized Levenshtein Bound (17:20)

Zilong Liu (Nanyang Technological University, Singapore); Yong Liang Guan (Nanyang Technological University, Singapore); Wai Ho Mow (Hong Kong University of Science and Technology & HKUST, Hong Kong)

Generalized Levenshtein bound (GLB) is a lower bound on the maximum aperiodic correlation sum of quasi-complementary sequence set (QCSS) which refers to a set of two-dimensional matrices with low non-trivial aperiodic auto- and cross- correlation sums. GLB is an indefinite fractional quadratic function of a "simplex" weight vector $\mathbf{w}$ and three additional parameters associated with QCSS. We present a novel approach to analytically conduct fractional quadratic programming for the tightening of the GLB. Our key idea is to apply the frequency domain decomposition of the relevant circulant matrix (i.e., the numerator term of GLB) to convert the non-convex problem into a convex one. We derive a new weight vector which asymptotically leads to a tighter GLB (over the Welch bound) for all possible (K, M) cases, where K, M denote the set size, the number of channels, of QCSS, respectively.

Bounds for Cooperative Locality Using Generalized Hamming Weights (17:40)

Khaled Abdel-Ghaffar (University of California, USA); Jos Weber (Delft University of Technology, The Netherlands)

The Cadambe-Mazumdar bound gives a necessary condition for a code to have a certain locality in case of a single erasure in terms of length, dimension, and Hamming distance of the code and of certain shortened codes. The bound has been generalized by Rawat, Mazumdar, and Vishwanath to recover multiple erasures in a cooperative repair scenario. In this paper, the generalized Hamming weights of the code and its shortened codes, which include the Hamming distance as one component, are incorporated to obtain bounds on locality to recover a single erasure or multiple erasures cooperatively. The new bounds give sharper necessary conditions than existing bounds.

Bounds on the Asymptotic Rate of Binary Constant Subblock-Composition Codes (18:00)

Anshoo Tandon (National University of Singapore, Singapore); Han Mao Kiah (Nanyang Technological University, Singapore); Mehul Motani (National University of Singapore, Singapore)

The study of binary constant subblock-composition codes (CSCCs) has recently gained attention due to their application in diverse fields. These codes are a class of constrained codes where each codeword is partitioned into equal sized subblocks, and every subblock has the same fixed weight. We present novel

upper and lower bounds on the asymptotic rate for binary CSCCs, using the sphere-packing and Gilbert-Varshamov (GV) type bounds, respectively. For a fixed subblock length and small code distance, we show that the asymptotic rate for CSCCs is strictly lower than the corresponding rate for constant weight codes (CWCs). We also provide a correction to an earlier result by Chee et al. (2014) on the asymptotic CSCC rate.

Mo4-6: Multiterminal Source Coding

Monday, June 26, 16:40-18:20
Room: K5
Chair: Michelle Effros (California Institute of Technology, USA)

Distributed Cooperative Information Bottleneck (16:40)

Matias Vera (Universidad de Buenos Aires - Facultad de Ingeniería, Argentina); Leonardo Rey Vega (University of Buenos Aires, Facultad de Ingeniería & CONICET, Argentina); Pablo Piantanida (CentraleSupélec-CNRS-Université Paris-Sud, France)

This paper investigates a scenario where two distant nodes separately observe memoryless process, namely X_1 and X_2, and can cooperate through multiple exchanges of messages with the goal of enabling a third node to learn ”relevant information” (measured in terms of a multi-letter mutual information) about some hidden memoryless process Y, which is arbitrarily dependent on (X_1, X_2). These interactive exchanges yield an explicit cooperation that helps the third node to identify, from the distributed observations X_1 and X_2, useful features for the inference of Y. An inner and an outer bound to the rate-relevance region of this problem is derived. Optimal characterization of the rate-relevance region under two different conditions on the dependence structures of the involved variables is showed. Also two examples for Gaussian sources are studied.

A Unified Approach to Error Exponents for Multiterminal Source Coding Systems (17:00)

Shigeaki Kuzuoka (Wakayama University, Japan)

Two kinds of problems, (i) hypothesis testing with many-to-one compression and (ii) one-to-many lossy source coding with side-information at decoders, are investigated in a unified way. It is demonstrated that a simple key idea, which is developed by Iriyama for one-to-one source coding systems, can be applied to multiterminal source coding systems. In particular, general bounds on the error exponents of multiterminal hypothesis testing and one-to-many lossy source coding are given.

Generalized Gaussian Multiterminal Source Coding and Probabilistic Graphical Models (17:20)

Jun Chen (McMaster University, Canada); Farrokh Etezadi (University of Toronto, Canada); Ashish Khisti (University of Toronto, Canada)

The sum-rate-distortion function of generalized Gaussian multiterminal source coding is shown to coincide with that of joint encoding in the high-resolution regime if and only if the source-encoder bipartite graph and the undirected graphical model (also known as Gaussian Markov network or Gaussian Markov random field) of the source distribution satisfy a certain condition.

Two-Encoder Multiterminal Source Coding With Side Information Under Logarithmic Loss (17:40)

Abdellatif Zaidi (Université Paris-Est Marne La Vallée, France)

In this work, we study the problem of two-encoder multiterminal source coding with side information under logarithmic loss distortion measure. We establish a single-letter characterization of the rate-distortion region of this model in the discrete memoryless case. The proof of the converse relies heavily on that of Courtade-Weissman rate-distortion region of the classic two-encoder multiterminal distributed source coding without side information; and extends it to the case in which the decoder has access to a side information stream that is statistically dependent on the sources that need to be compressed. We also apply our result to the so-called Information Bottleneck Method and establish the optimal tradeoff between complexity and accuracy of the prediction in this setting.

Coding for Arbitrarily Varying Remote Sources (18:00)

Amitalok Budkuley (The Chinese University of Hong Kong, Hong Kong); Bikash Dey (Indian Institute of Technology Bombay, India); Vinod Prabhakaran (Tata Institute of Fundamental Research, India)

We study a lossy source coding problem for a memoryless remote source. The source data is broadcast over an arbitrarily varying channel (AVC) controlled by an adversary. One output of the AVC is received as input at the encoder, and another output is received as side information at the decoder. The adversary is assumed to know the source data non-causally, and can employ randomized jamming strategies arbitrarily correlated to the source data. The decoder reconstructs the source data from the encoded message and the side information. We determine the adversarial rate distortion function for the source under randomized coding. Interestingly, even with vector jamming strategies allowed, it is seen that the adversary cannot affect the rate any worse than when restricted to memoryless strategies.

Mo4-7: Security 1

Monday, June 26, 16:40-18:20
Room: K6
Chair: Wei Kang (Southeast University, P.R. China)

On The Compound MIMO Wiretap Channel with Mean Feedback (16:40)

Amr Abdelaziz (The Ohio State University & Military Technical College, USA); Ashraf Elbayoumy (Military Technical College, Egypt); Can Koksal (The Ohio State University, USA); Hesham El Gamal (Ohio State University, USA)

Compound MIMO wiretap channel with double sided uncertainty is considered under channel mean information model. In mean information model, channel variations are centered around its mean value which is fed back to the transmitter. We show that the worst case main channel is anti-parallel to the channel mean information resulting in an overall unit rank channel. Further, the worst eavesdropper channel is shown to be isotropic around its mean information. Accordingly, we provide the capacity achieving beamforming direction. We show that the saddle point property holds under mean information model and, thus, compound secrecy capacity equals to the worst case capacity over the class of uncertainty. Moreover, capacity achieving beamforming direction is found to require matrix inversion, thus, we derive null steering (NS) beamforming as an alternative sub-optimal solution that precludes the necessity of matrix inversion. NS beamformer is the beamforming direction orthogonal to the eavesdropper mean channel that maintains the maximum possible gain in the direction mean main channel. Extensive computer simulation reveals that NS beamforming performs very close to the optimal solution. It also verifies that, NS beamforming outperforms both maximum ratio transmission (MRT) and zero forcing (ZF) beamforming approaches over the entire SNR range. Finally, an equivalence relation with MIMO wiretap channel in Rician fading environment is established.

Multiple Access Wiretap Channel with Cribbing (17:00)

Noha Helal (University of Texas at Dallas, USA); Aria Nosratinia (University of Texas, Dallas, USA)

This paper introduces the discrete memoryless multiple access wiretap channel with noiseless cribbing, where the cribbing may be either causal or strictly causal. We derive lower bounds for secrecy rates for both causal and strictly causal cribbing under either a decode-forward or partial-decode-forward strategy. Our results recover the achievable rate regions of the MAC wiretap and MAC with cribbing, and demonstrate improvement of secrecy rate due to cribbing. An outer bound is presented for this channel under causal cribbing, which also serves as an outer bound for strictly causal case.

Wiretap channel capacity: Secrecy criteria, strong converse, and phase change (17:20)

Eric Graves (Army Research Lab, USA); Tan Wong (University of Florida, USA)

This paper employs equal-image-size source partitioning techniques to derive the capacities of the general discrete memoryless wiretap channel (DM-WTC) under four different secrecy criteria. These criteria respectively specify requirements on the expected values and tail probabilities of the differences, in absolute value and in exponent, between the joint probability of the secret message and the eavesdropper's observation and the corresponding probability if they were independent. Some of these criteria reduce back to the standard leakage and variation distance constraints that have been previously considered in the literature. The capacities under these secrecy criteria are found to be different when non-vanishing error and secrecy tolerances are allowed. Based on these new results, we are able to conclude that the strong converse property generally holds for the DM-WTC only under the two secrecy criteria based on constraining the tail probabilities. Under the secrecy criteria based on the expected values, an interesting phase change phenomenon is observed as the tolerance values vary.

The Shannon Cipher System with a Guessing Eavesdropper (17:40)

Lanqing Yu (Princeton University, USA); Paul Cuff (Princeton University, USA)

We consider a Shannon cipher system in which distortion is allowed at the legitimate receiver. The secrecy metric used is the exponent of the probability that the reconstruction of the source sequence by the eavesdropper is within a distortion level. A single-letter characterization is provided when the message rate is large enough. Under the optimal code, the eavesdropper can do no better than either making a reconstruction blindly or guessing the key first and then reconstructing based on the sequence reconstructed by the legitimate receiver.

Privacy-Aware Guessing Efficiency (18:00)

Shahab Asoodeh (Queen's University, Canada); Mario Diaz (Queen's University, Canada); Fady Alajaji (Queen's University, Canada); Tamas Linder (Queen's University, Canada)

We investigate the problem of guessing a discrete random variable Y under a privacy constraint dictated by another correlated discrete random variable X, where both guessing efficiency and privacy are assessed in terms of the probability of correct guessing. We

define $\tilde{h}(P_{XY}, \varepsilon)$ as the maximum probability of correctly guessing Y given an auxiliary random variable Z, where the maximization is taken over all $P_{Z|Y}$ ensuring that the probability of correctly guessing X given Z does not exceed ε. We show that the map $\varepsilon \mapsto \tilde{h}(P_{XY}, \varepsilon)$ is strictly increasing, concave, and piecewise linear, which allows us to derive a closed form expression for $\tilde{h}(P_{XY}, \varepsilon)$ when X and Y are connected via a binary-input binary-output channel. For $\{(X_i, Y_i)\}_{i=1}^n$ being pairs of independent and identically distributed binary random vectors, we similarly define $\underline{h}_n(P_{X^nY^n}, \varepsilon)$ under the assumption that Z^n is also a binary vector. Then we obtain a closed form expression for $\underline{h}_n(P_{X^nY^n}, \varepsilon)$ for sufficiently large, but nontrivial values of ε.

Mo4-8: Privacy 1

Monday, June 26, 16:40-18:20
Room: K7+8
Chair: Frans Willems (Technical University Eindhoven, The Netherlands)

Optimal Schemes for Discrete Distribution Estimation under Local Differential Privacy (16:40)

Min Ye (UMD, USA); Alexander Barg (University of Maryland, USA)

We consider the minimax estimation problem of a discrete distribution with support size k under privacy constraints. A privatization scheme is applied to each raw sample independently, and we need to estimate the distribution of the raw samples from the privatized samples. A positive number ϵ measures the privacy level of a privatization scheme. For a given ϵ, we want to find the optimal privatization scheme which minimizes the expected estimation loss for the worst-case distribution. Two schemes in the literature provide order optimal performance in the high-privacy regime when ϵ is very close to 0, and in the low-privacy regime when $e^\epsilon \approx k$, respectively. In this paper, we propose a new family of schemes which substantially improve the performance of the existing schemes in the medium privacy regime when $1 \ll e^\epsilon \ll k$. More concretely, we prove that when $3.8 < \epsilon < \ln(k/9)$, our schemes reduce the expected estimation loss by 50% under ℓ_2^2 metric and 30% under ℓ_1 metric over the existing schemes. We also prove a tight lower bound for the whole region $e^\epsilon \ll k$, which implies that our schemes are order optimal in this regime.

Limits of Location Privacy under Anonymization and Obfuscation (17:00)

*Nazanin Takbiri (University of Massachusetts Amherst, USA); Amir Houmansadr (University of Massachusetts Amherst, USA); Dennis Goeckel (University of Massachusetts, USA); **Hossein Pishro-Nik** (University of Massachusetts, Amherst, USA)*

The prevalence of mobile devices and location-based services (LBS) has generated great concerns regarding the LBS users' privacy, which can be compromised by statistical analysis of their movement patterns. A number of algorithms have been proposed to protect the privacy of users in such systems, but the fundamental underpinnings of such remain unexplored. Recently, the concept of perfect location privacy was introduced and its achievability was studied for anonymization-based LBS systems, where user identifiers are permuted at regular intervals to prevent identification based on statistical analysis of long time sequences. In this paper, we significantly extend that investigation by incorporating the other major tool commonly employed to obtain location privacy: obfuscation, where user locations are purposely obscured to protect their privacy. Since anonymization and obfuscation reduce user utility in LBS systems, we investigate how location privacy varies with the degree to which each of these two methods is employed. We provide: (1) achievability results for the case where the location of each user is governed by an i.i.d. process; (2) converse results for the i.i.d. case as well as the more general Markov Chain model. We show that, as the number of users in the network grows, the obfuscation-anonymization plane can be divided into two regions: in the first region, all users have perfect location privacy; and, in the second region, no user has location privacy.

Operational Definitions for Some Common Information Leakage Metrics (17:20)

Ibrahim Issa (Cornell University, USA); Aaron Wagner (Cornell University, USA)

Maximal leakage from a random variable X to a random variable Y is defined as the multiplicative increase, upon observing Y, of the probability of correctly guessing a randomized function of X, maximized over all such functions [1]. Herein, this *guessing* framework is used to give operational definitions to common information leakage metrics, including Shannon capacity, maximal correlation, and local differential privacy. Shannon capacity is shown to capture the multiplicative increase of the probability of correct guessing over the restricted set of functions of X that can be *reliably* reconstructed from Y, hence *underestimating* leakage. Maximal correlation is shown to capture the multiplicative change in the *variance* of functions of X, rather than the guessing probability. Local differential privacy is shown to capture the multiplicative increase of the guessing probability of functions of X, maximized over *realizations*

of Y and over distributions P_X. Moreover, maximizing over realizations of Y for a fixed P_X is shown to yield a valid leakage measure, which is equal to the maximum information rate.

Smart Meter Privacy Based on Adversarial Hypothesis Testing (17:40)

Zuxing Li *(KTH Royal Institute of Technology & Communication Theory Lab., Sweden); Tobias Oechtering (KTH Royal Institute of Technology & School of Electrical Engineering, EE, Sweden); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain))*

Privacy-preserving energy management is studied in the presence of a renewable energy source. It is assumed that the energy demand/supply from the energy provider is tracked by a smart meter. The resulting privacy leakage is measured through the probabilities of error in a binary hypothesis test, which tries to detect the consumer behavior based on the meter readings. An optimal privacy-preserving energy management policy maximizes the minimal Type II probability of error subject to a constraint on the Type I probability of error. When the privacy-preserving energy management policy is based on all the available information of energy demands, energy supplies, and hypothesis, the asymptotic exponential decay rate of the maximum minimal Type II probability of error is characterized by a divergence rate expression. Two special privacy-preserving energy management policies, the memoryless hypothesis-aware policy and the hypothesis-unaware policy with memory, are then considered and their performances are compared. Further, it is shown that the energy supply alphabet can be constrained to the energy demand alphabet without loss of optimality for the evaluation of a single-letter-divergence privacy-preserving guarantee.

Hypothesis Testing under Maximal Leakage Privacy Constraints (18:00)

Jiachun Liao (Arizona State University, USA); Lalitha Sankar (Arizona State University, USA); Flavio Calmon (IBM, USA); Vincent Tan (National University of Singapore, Singapore)

The problem of publishing privacy-guaranteed data for hypothesis testing is studied using the maximal leakage (ML) as a metric for privacy and the type-II error exponent as the utility metric. The optimal mechanism (random mapping) that maximizes utility for a bounded leakage guarantee is determined for the entire leakage range for binary datasets. For non-binary datasets, approximations in the high privacy and high utility regimes are developed. The results show that, for any desired leakage level, maximizing utility forces the ML privacy mechanism to reveal partial to complete knowledge about a subset of the source alphabet. The results developed on maximizing a convex function over a polytope may also of an independent interest.

Mo4-9: Subspace and LDPC Codes

Monday, June 26, 16:40-18:20
Room: K9
Chair: Shu Lin (UC Davis, USA)

Cyclic Subspace Codes and Sidon Spaces (16:40)

Netanel Raviv (Technion & Tel-Aviv University, Israel); Itzhak Tamo (Tel Aviv University, Israel)

The interest in subspace codes has increased in recent years due to their application in error correction for random network coding. In order to study their properties and find good constructions, the notion of cyclic subspace codes was introduced by using the extension field structure of the ambient space. However, to this date there exists no general construction with a polynomial relation between k, the dimension of the codewords, and n, the dimension of the entire space. Independently of the study of cyclic subspace codes, *Sidon spaces* were recently introduced by Bachoc et al. as a tool for the study of certain multiplicative properties of subspaces over finite fields. In this paper it is shown that Sidon spaces are necessary and sufficient for obtaining a full-orbit cyclic subspace code with minimum distance $2k-2$. By presenting several constructions of Sidon spaces, full-orbit cyclic subspace codes are obtained, in which n is *quadratic* in k. The constructions are based on a variety of tools; namely, Sidon sets, that are sets of integers in which all pairwise sums are distinct, irreducible polynomials, and linearized polynomials. Further, the existence of a Sidon space in which n is *linear* in k is shown, alongside the fact that any Sidon space induces a Sidon set.

Grassmannian Codes from Multiple Families of Mutually Unbiased Bases (17:00)

Olav Tirkkonen (Aalto University, Finland); Christopher Boyd (Aalto University, Finland); Roope Vehkalahti (Aalto University, Finland)

We explore the underlying algebraic structure of Mutually Unbiased Bases (MUBs), and their application to code design. Columns in MUBs have inner products with absolute values less or equal to $1/\sqrt{N}$. MUBs provide a systematic way of generating optimal codebooks for various coding and precoding applications. A maximal set of MUBs (MaxMUBs) in $N = 2^m$ dimensions, with $m \in \mathbb{Z}$, can produce codebooks of QPSK lines with good distance properties and alphabets which limit processing complexity. We expand the construction by identifying that in $N = 2^m$ dimensions there exists $N^(m-1)/2$ families of MUB, each with N matrices. Inner products of columns of these matrices are less or equal to $1/\sqrt{2}$. Considering Grassmannian line codebooks that can be generated from these matrices, we

conjecture that Grassmannian codebooks of maximum cardinality for minimum chordal distance $1/\sqrt{2}$ can be constructed when entries are constrained to be normalized fourth roots of unity. Then decoding or encoding these codebooks can be performed without multiplications, and with a number of additions that scales linearly with the number of codewords, irrespective of the dimension.

Performance of ML Decoding for Ensembles of Binary and Nonbinary Regular LDPC Codes of Finite Lengths (17:20)

Irina Bocharova (St. Petersburg University of Information Technologies, Mechanics and Optics, Russia); Boris Kudryashov (St. Petersburg University of Information Technologies, Mechanics and Optics, Russia); Vitaly Skachek (University of Tartu, Estonia)

The Gallager ensembles of binary regular LDPC codes and binary images of nonbinary regular LDPC codes are studied. Recurrent procedure for computing average spectra for these two ensembles is presented. By using the existing bounding techniques, estimates on the error probability of the maximum-likelihood (ML) decoding over an AWGN channel with BPSK signaling for short codes from different ensembles of LDPC codes are obtained. The numerical results show performance of the ML decoding for different code ensembles. Conclusions drawn based on the average code spectra are then verified by near-ML decoding simulations for both randomly selected and the best known short codes. The asymptotic ML decoding thresholds for AWGN and BS channels are calculated. As expected, codes with the ML decoding performance superior to that of the average code in the ensemble, are easy to find. However, it follows from the presented results that the ML decoding performance should not be used as a target for searching for good iteratively decodable codes.

Interleaved Subspace Codes in Fountain Mode (17:40)

Vladimir Sidorenko (Technical University of Munich, Germany); Hannes Bartz (Technical University of Munich, Germany); Antonia Wachter-Zeh (Technical University of Munich (TUM), Germany)

We consider subspace codes obtained by lifting L-interleaved [n,k] Gabidulin codes. When used in networks with random linear coding, these codes are able to correct with high probability gamma packet insertions and delta packet deletions if gamma/L + delta < n-k. We propose to use these subspace codes in the so called fountain mode. In this case we do not need to correct deletions and are able to correct with high probability a large number L(n-k) of packet insertions. We present a simplified decoder correcting insertions only.

LT codes on Partial Erasure Channels (18:00)

***Carolyn Mayer** (University of Nebraska-Lincoln, USA); Christine Kelley (University of Nebraska - Lincoln, USA)*

LT codes are a class of rateless codes designed for data dissemination on erasure channels. In this paper, we present a decoder for LT codes on partial erasure channels, which were recently introduced for multi-level read storage channel applications. We compare the efficiency of LT codes on these channels to those on the QEC.

Mo4-A: Energy Harvesting 1

Monday, June 26, 16:40-18:20
Room: Berlin 3
Chair: Yu-Pin Hsu (National Taipei University, Taiwan)

Energy Harvesting Networks with General Utility Functions: Near Optimal Online Policies (16:40)

Ahmed Arafa (University of Maryland College Park, USA); Abdulrahman Baknina (University of Maryland, USA); Sennur Ulukus (University of Maryland, USA)

We consider online scheduling policies for single-user energy harvesting communication systems, where the goal is to characterize online policies that maximize the long term average utility, for some general concave and monotonically increasing utility function. In our setting, the transmitter relies on energy harvested from nature to send its messages to the receiver, and is equipped with a finite-sized battery to store its energy. Energy packets are independent and identically distributed (i.i.d.) over time slots, and are revealed causally to the transmitter. Only the average arrival rate is known a priori. We first characterize the optimal solution for the case of Bernoulli arrivals. Then, for general i.i.d. arrivals, we first show that fixed fraction policies [Shaviv-Ozgur] are within a constant multiplicative gap from the optimal solution for all energy arrivals and battery sizes. We then derive a set of sufficient conditions on the utility function to guarantee that fixed fraction policies are within a constant additive gap as well from the optimal solution.

On Achievable Rates of AWGN Energy-Harvesting Channels with Block Energy Arrival and Non-Vanishing Error Probabilities (17:00)

***Silas Fong** (National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore); Ayfer Özgür (Stanford University, USA)*

This paper investigates the achievable rates of an additive white Gaussian noise (AWGN) energy-harvesting (EH) channel with an infinite battery under the assumption that the error probabilities do not vanish as the blocklength increases. The EH process is character-

ized by a sequence of blocks of harvested energy. The harvested energy remains constant within a block while the harvested energy across different blocks is characterized by a sequence of independent and identically distributed (i.i.d.) random variables. The blocks have length L, which can be interpreted as the coherence time of the energy arrival process. If L is a constant or grows sublinearly in the blocklength n, we fully characterize the first-order coding rate. In addition, we obtain lower and upper bounds on the second-order coding rate, which are proportional to $-\sqrt{\frac{L}{n}}$ for any fixed error probability <1/2. If L grows linearly in n, we obtain lower and upper bounds on the first-order coding rate, which coincide whenever the EH random variable is continuous. Our results suggest that correlation in the energy-arrival process decreases the effective blocklength by a factor of L.

Optimal Transmission for Energy Harvesting Nodes under Battery Size and Usage Constraints (17:20)

Jing Yang (The Pennsylvania State University, USA); Jingxian Wu (University of Arkansas, USA)

In this paper, we study the optimal energy management policy of an energy harvesting transmitter by taking both battery degradation and finite battery constraints into consideration. We consider a scenario where the sensor is able to harvest energy from the ambient environment and use it to power its transmission. The harvested energy can be used for transmission immediately without entering the equipped battery, or charged into the battery and discharged later for transmission. When the battery is charged or discharged, a cost will be incurred to account for its impact on battery degradation. We impose a long-term average cost constraint on the battery, which is translated to the average number of charge/discharge operations per unit time. At the same time, we assume the capacity of the battery is finite, and the total amount of energy stored in the battery cannot exceed its capacity. Our objective is to develop an online energy management policy to maximize the long-term average throughput of the transmitter under both the battery usage constraint and finite battery constraint. We propose an energy-aware adaptive transmission policy, which is a modified version of the optimal policy for the infinite battery case. Our analysis indicates that the energy-aware adaptive transmission policy is asymptotically optimal when the battery size is sufficiently large. Simulation results corroborate the theoretical analysis.

Single-User Channel with Data and Energy Arrivals: Online Policies (17:40)

Abdulrahman Baknina (University of Maryland, USA); Sennur Ulukus (University of Maryland, USA)

We consider a single-user channel in which the transmitter is equipped with finite-sized data and energy buffers. The transmitter receives energy and data packets randomly and intermittently over time and stores them in the finite-sized buffers. The arrival amounts are known only causally as they happen. We study the online power allocation problem, in which the transmitter relies only on the causal arrival (energy and data) information. We focus on the special case when the energy and data arrivals are fully-correlated. We first study the case when the arrivals are Bernoulli. For this case, we determine the optimal policy. Inspired by this policy and in order to study the case of general fully-correlated arrivals, we propose a structured policy and bound its performance by a multiplicative gap from the optimal. We then show that this policy is optimal when the energy arrivals dominate the data arrivals, and is within a constant additive gap from the optimal policy when the data arrivals dominate the energy arrivals.

Tu1-1: Array Codes

Tuesday, June 27, 09:50-11:10
Room: Europa
Chair: Joachim Rosenthal (University of Zurich, Switzerland)

Locality and Availability of Array Codes Constructed from Subspaces (09:50)

Natalia Silberstein (Yahoo! Labs, Israel); Tuvi Etzion (Technion-Israel Institute of Technology, Israel); Moshe Schwartz (Ben-Gurion University of the Negev, Israel)

Ever-increasing amounts of data are created and processed in internet-scale companies such as Google, Facebook, and Amazon. The efficient storage of such copious amounts of data has thus become a fundamental and acute problem in modern computing. No single machine can possibly satisfy such immense storage demands. Therefore, distributed storage systems (DSS), which rely on tens of thousands of storage nodes, are the only viable solution. Such systems are broadly used in all modern internet-scale systems. However, the design of a DSS poses a number of crucial challenges, markedly different from single-user storage systems. Such systems must be able to reconstruct the data efficiently, to overcome failure of servers, to correct errors, etc. Lots of research was done in the last few years to answer these challenges and the research is increasing in parallel to the increasing amount of stored data. The main goal of this paper is to consider codes which have two of the most important features of distributed storage systems, namely, locality and availability. Our codes are array codes which are based on subspaces of a linear space over a finite field. We present several constructions of such codes which are q-analog to some of the known block codes. Some of these codes possess independent intellectual merit. We examine the locality and avail-

ability of the constructed codes. In particular we distinguish between two types of locality and availability, node vs. symbol, locality and availability. To our knowledge this is the first time that such a distinction is given in the literature.

Efficient Lowest Density MDS Array Codes of Column Distance 4 (10:10)

Zhijie Huang *(Sun Yat-Sen University, P.R. China); Hong Jiang (University of Texas at Arlington, USA); Nong Xiao (Sun Yat-Sen University, P.R. China)*

The extremely strict code length constraint is the main drawback of lowest density, maximum-distance separable (MDS) array codes of distance greater than 3. To break away from the status quo, we proposed in [6] a family of lowest density MDS array codes of (column) distance 4, called XI-Code. Compared with the previous alternatives, XI-Code has lower encoding and decoding complexities, and much looser constraint on the code length, thus is much more practical. In this paper, we present a new family of lowest density MDS array codes of (column) distance 4, called RΛ-Code, which is derived from XI-Code, and outperforms the latter substantially in terms of encoding complexity, decoding complexity, and memory consumption during encoding/decoding. The inherent connection between RΛ-Code and XI-Code and how the former is derived from the latter may provide inspiration for the readers to derive new codes from other existing codes in a similar way.

Triple-Fault-Tolerant Binary MDS Array Codes with Asymptotically Optimal Repair (10:30)

Hanxu Hou (Dongguan University of Technology, P.R. China); Patrick Pak-Ching Lee (The Chinese University of Hong Kong, Hong Kong); Yunghsiang Han (Dongguan University of Technology, P.R. China); Yuchong Hu (Huazhong University of Science and Technology, P.R. China)

Binary maximum distance separable (MDS) array codes are a special class of erasure codes for distributed storage that not only provide fault tolerance with minimum storage redundancy, but also achieve low computational complexity. They are constructed by encoding k information columns into r parity columns, in which each element in a column is a bit, such that any k out of the $k+r$ columns suffice to recover all information bits. In addition to providing fault tolerance, it is critical to improve repair performance. Specifically, if a single column fails, our goal is to minimize the repair bandwidth by downloading the least amount of bits from d non-failed columns, where $k \leq d \leq k+r-1$. However, existing binary MDS codes that achieve high data rates (i.e., $k/(k+r) > 1/2$) and minimum repair bandwidth only support double fault tolerance (i.e., $r = 2$), which is insufficient for failure-prone distributed storage environments in practice. This paper fills the void by proposing an explicit construction of triple-fault-tolerant (i.e., $r = 3$) binary MDS array codes that achieve asymptotically minimum repair bandwidth for $d = k + 1$.

Codes for Graph Erasures (10:50)

Lev Yohananov (Technion - Israel Institute of Technology, Israel); Eitan Yaakobi (Technion, Israel)

Motivated by systems where the information is represented by a graph, such as neural networks, associative memories, and distributed systems, we present in this work a new class of codes, called codes over graphs. Under this paradigm, the information is stored on the edges of an undirected graph, and a code over graphs is a set of graphs. A node failure is the event where all edges in the neighborhood of the failed node have been erased. We say that a code over graphs can tolerate ρ node failures if it can correct the erased edges of any ρ failed nodes in the graph. While the construction of such codes can be easily accomplished by MDS codes, their field size has to be at least $\mathcal{O}(n^2)$, when n is the number of nodes in the graph. In this work we present several constructions of codes over graphs with smaller field size. In particular, we present optimal codes over graphs correcting two node failures over the binary field, when the number of nodes in the graph is a prime number. We also present a construction of codes over graphs correcting ρ node failures for all ρ over a field of size at least $(n+1)/2-1$, and show how to improve this construction for optimal codes when $\rho = 2, 3$.

Tu1-2: Polar Codes 1

Tuesday, June 27, 09:50-11:10
Room: Brussels
Chair: Ilya Dumer (University of California at Riverside, USA)

Fast Polarization for Non-Stationary Channels (09:50)

Hessam Mahdavifar (University of Michigan, USA)

We consider the problem of polar coding for transmission over a non-stationary sequence of independent binary-input memoryless symmetric (BMS) channels $\{W_i\}_{i=1}^{\infty}$, where the i-th encoded bit is transmitted over W_i. We show, for the first time, a polar coding scheme that achieves the average symmetric capacity

$$\overline{I}(\{W_i\}_{i=1}^{\infty}) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} I(W_i),$$

assuming that the limit exists. The polar coding scheme is constructed using Arıkan's channel polarization transformation in combination with certain permutations at each polarization level and certain skipped operations. This guarantees a fast polarization process

that results in polar coding schemes with block lengths upper bounded by a polynomial of $1/\epsilon$, where ϵ is the gap to the average capacity. More specifically, given an arbitrary sequence of BMS channels $\{W_i\}_{i=1}^N$ and P_e, where $0 < P_e < 1$, we construct a polar code of length N and rate R guaranteeing a block error probability of at most P_e for transmission over $\{W_i\}_{i=1}^N$ such that

$$N \leq \frac{\kappa}{(\overline{I}_N - R)^\mu}$$

where μ is a constant, κ is a constant depending on P_e and μ, and $\overline{I}_N$ is the average of the symmetric capacities $I(W_i)$, for $i = 1, 2, , \ldots, N$. We further show a numerical upper bound on μ that is: $\mu \leq 10.78$. The encoding and decoding complexities of the constructed polar code preserves $O(N \log N)$ complexity of Arıkan's polar codes.

A Lower Bound on the Probability of Error of Polar Codes over BMS Channels (10:10)

Boaz Shuval *(Technion, Israel); Ido Tal (Technion, Israel)*

Consider a polar code designed for some binary memoryless symmetric channel. We develop a lower bound on the probability of error of this polar code under successive-cancellation decoding. The bound exploits the correlation between the various codeword bits and improves upon existing lower bounds.

On the Pointwise Threshold Behavior of the Binary Erasure Polarization Subchannels (10:30)

Erik Ordentlich (Yahoo, Inc., USA); Ron Roth (Technion, Israel)

It is shown that when Arikan's n-level polarization transformation is applied to the binary erasure channel, each of the resulting individual 2^n subchannels has a sharp threshold, for sufficiently large n.

Exploiting Source Redundancy to Improve the Rate of Polar Codes (10:50)

Ying Wang (Texas A&M University, USA); Krishna Narayanan (Texas A&M University, USA); Anxiao Andrew Jiang (Texas A&M University, USA)

We consider a joint source-channel decoding (JSCD) problem where the source encoder leaves residual redundancy in the source. We first model the redundancy in the source encoder output as the output of a side information channel at the channel decoder, and show that this improves random error exponent. Then, we consider the use of polar codes in this framework when the source redundancy is modeled using a sequence of t-erasure correcting block codes. For this model, the rate of polar codes can be improved by unfreezing some of originally frozen bits and that the improvement in rate depends on the distribution of frozen bits within a codeword. We present a proof for the convergence of that distribution, as well as the convergence of the maximum rate improvement. The significant performance improvement and improved rate provide strong evidences that polar code is a good candidate to exploit the benefit of source redundancy in the JSCD scheme.

Tu1-3: Multiple Access 2

Tuesday, June 27, 09:50-11:10
Room: K2
Chair: Abbas El Gamal (Stanford University, USA)

Outer Bounds for Gaussian Multiple Access Channels with State Known at One Encoder (09:50)

Wei Yang (Princeton University, USA); Yingbin Liang (Syracuse University, USA); Shlomo (Shitz) Shamai (The Technion, Israel); H. Vincent Poor (Princeton University, USA)

This paper studies a two-user state-dependent Gaussian multiple-access channel with state noncausally known at one encoder. Two new outer bounds on the capacity region are derived, which improve uniformly over the best known (genie-aided) outer bound. The two corner points of the capacity region as well as the sum rate capacity are established, and it is shown that a single-letter solution is adequate to achieve both the corner points and the sum rate capacity. Furthermore, the full capacity region is characterized in situations in which the sum rate capacity is equal to the capacity of the helper problem. The proof relies on the optimal-transportation idea of Polyanskiy and Wu (which was used previously to establish an outer bound on the capacity region of the interference channel) and on a generalization of the worst-case Gaussian noise result to the case in which the input and the noise are dependent.

Homologous Codes for Multiple Access Channels (10:10)

Pinar Sen (UCSD, USA); Young-Han Kim (UCSD, USA)

Building on recent development by Padakandla and Pradhan, and by Lim, Feng, Pastore, Nazer, and Gastpar, this paper studies structured coding as a complete replacement for random coding in network information theory. The roles of two techniques used in nested coset coding to generate nonuniform codewords, namely, shaping and channel transformation, are clarified and illustrated via the simple example of the two-sender multiple access channel. While individually deficient, the optimal combination of shaping and channel transformation is shown to achieve the same performance as traditional random codes for this channel model, which opens up new possibilities of utilizing nested coset codes with the same generator matrix for

a broader class of applications.

An Achievable Error Exponent for the Multiple Access Channel with Correlated Sources (10:30)

Arezou Rezazadeh (Universitat Pompeu Fabra, Spain); Josep Font-Segura (Universitat Pompeu Fabra, Spain); Alfonso Martinez (Universitat Pompeu Fabra, Spain); Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra & University of Cambridge, Spain)

This paper derives an achievable random-coding error exponent for joint source-channel coding over a multiple access channel with correlated sources. The codebooks are generated by drawing codewords from a multi-letter distribution that depends on the composition of the source message.

A Broadcast Approach to Multiple Access Adapted to the Multiuser Channel (10:50)

Samia Kazemi (Rensselaer Polytechnic Institute, USA); Ali Tajer (Rensselaer Polytechnic Institute, USA)

A broadcast strategy for multiple access communication over slowly fading channels is introduced, in which the channel state information is known to only the receiver. In this strategy, the transmitters split their information streams into multiple independent coded information layers, each adapted to a specific actual channel realization. The major distinction between the proposed strategy and the existing ones is that in the existing approaches, each transmitter adapts its transmission strategy only to the fading process of its direct channel to the receiver, hence directly adopting a single-user strategy previously designed for the single-user channels. However, the contribution of each user to a network-wide measure (e.g., sum-rate capacity) depends not only on the user's direct channel to the receiver, but also on the qualities of other channels. Driven by this premise, this paper proposes an alternative broadcast strategy in which the transmitters adapt their transmissions to the combined states resulting from both users' channels. This leads to generating a larger number of information layers by each transmitter and adopting a different decoding strategy by the receiver. An achievable rate region that captures the trade-off among the rates of different information is established and is shown to subsume the existing known regions.

Tu1-4: Information Measures

Tuesday, June 27, 09:50-11:10
Room: K3
Chair: Thomas Courtade (University of California, Berkeley, USA)

On the Information Dimension Rate of Stochastic Processes (09:50)

Bernhard Geiger (Technical University of Munich, Germany); Tobias Koch (Universidad Carlos III de Madrid & Gregorio Marañón Health Research Institute, Spain)

Jalali and Poor ("Universal compressed sensing," arXiv:1406.7807v3, Jan. 2016) have recently proposed a generalization of Rényi's information dimension to stationary stochastic processes by defining the information dimension of the stochastic process as the information dimension of k samples divided by k in the limit as $k \to \infty$. This paper proposes an alternative definition of information dimension as the entropy rate of the uniformly-quantized stochastic process divided by minus the logarithm of the quantizer step size $1/m$ in the limit as $m \to \infty$. It is demonstrated that both definitions are equivalent for stochastic processes that are ψ^*-mixing, but that they may differ in general. In particular, it is shown that for Gaussian processes with essentially-bounded power spectral density (PSD), the proposed information dimension equals the Lebesgue measure of the PSD's support. This is in stark contrast to the information dimension proposed by Jalali and Poor, which is 1 if the process's PSD is positive on a set of positive Lebesgue measure, irrespective of its support size.

A Variational Characterization of Rényi Divergences (10:10)

Venkat Anantharam (University of California at Berkeley, USA)

We present a variational characterization of the Rényi divergences between any two probability distributions on an arbitrary measurable space, in terms of relative entropies. This yields as a corollary a recently developed variational formula, due to Atar, Chowdhary and Dupuis, for exponential integrals of bounded measurable functions in terms of Rényi divergences. We also develop a similar variational characterization of the Rényi divergence rates between two stationary finite state Markov chains in terms of relative entropy rates. This leads to an analog of the variational formula of Atar, Chowdary and Dupuis in the framework of stationary finite state Markov chains.

A de Bruijn identity for discrete random variables (10:30)

Oliver Johnson (University of Bristol, United Kingdom (Great Britain)); Saikat Guha (Raytheon BBN Technologies, USA)

We discuss properties of the ”beamsplitter addition” operation, which provides a non-standard scaled convolution of random variables supported on the non-negative integers. We give a simple expression for the action of beamsplitter addition using generating functions. We use this to give a self-contained and purely classical proof of a heat equation and de Bruijn identity, satisfied when one of the variables is geometric.

Direct Estimation of Information Divergence Using Nearest Neighbor Ratios (10:50)

Morteza Noshad (University of Michigan, USA); Kevin Moon (Yale University, USA); Salimeh Yasaei Sekeh (University of Michigan, Ann Arbor, USA); Alfred Hero III (University of Michigan, USA)

We propose a direct estimation method for Renyi and f-divergence measures based on a new graph theoretical interpretation. Suppose that we are given two sample sets X and Y, respectively with N and M samples, where $\eta := M/N$ is a constant value. Considering the k-nearest neighbor (k-NN) graph of Y in the joint data set (X, Y), we show that the average powered ratio of the number of X points to the number of Y points among all k-NN points is proportional to Renyi divergence of X and Y densities. A similar method can also be used to estimate f-divergence measures. We derive bias and variance rates, and show that for the class of γ-Holder smooth functions, the estimator achieves the MSE rate of $N^{-2\gamma/(\gamma+d)}$. Furthermore, by using a weighted ensemble estimation technique, for density functions with continuous and bounded derivatives of up to the order d, and some extra conditions at the support set boundary, we derive an ensemble estimator that achieves the parametric MSE rate of $O(1/N)$. Our estimators are more computationally tractable than other competing estimators, which makes them appealing in many practical applications.

Tu1-5: Joint Source-Channel Coding 1

Tuesday, June 27, 09:50-11:10
Room: K4
Chair: Aaron Wagner (Cornell University, USA)

Expurgated Joint Source-Channel Coding Bounds and Error Exponents (09:50)

Jonathan Scarlett (EPFL, Switzerland); Alfonso Martinez (Universitat Pompeu Fabra, Spain); Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra & University of Cambridge, Spain)

This paper studies expurgated random-coding bounds and exponents for joint source-channel coding (JSCC). We extend Gallager's expurgation techniques for channel coding to the JSCC setting, and derive a non-asymptotic bound that recovers two exponents derived by Csiszár using the method of types. Our approach has the notable advantage of being directly applicable to channels with continuous alphabets.

Graph Information Ratio (10:10)

Lele Wang (Stanford University & Tel Aviv University, USA); Ofer Shayevitz (Tel Aviv University, Israel)

We introduce the notion of information ratio $\mathrm{Ir}(H/G)$ between two (simple, undirected) graphs G and H, which characterizes the maximal number of source symbols per channel use that can be reliably sent over a channel with confusion graph H, where reliability is measured w.r.t. a source confusion graph G. Many different results are provided, including in particular lower and upper bounds on $\mathrm{Ir}(H/G)$ in terms of various graph properties, inequalities and identities for behavior under strong product and disjoint union, relations to graph cores, and notions of graph criticality. Informally speaking, $\mathrm{Ir}(H/G)$ can be interpreted as a measure of similarity between G and H. We make this notion precise by introducing the concept of information equivalence between graphs, a more quantitative version of homomorphic equivalence. We then describe a natural partial ordering over the space of information equivalence classes, and endow it with a suitable metric structure that is contractive under the strong product. Various examples and intuitions are discussed.

Second Order Analysis for Joint Source-Channel Coding with Markovian Source (10:30)

Ryo Yaguchi (Nagoya University, Japan); Masahito Hayashi (Nagoya University, Japan)

We derive the second order rates of joint source-channel coding, whose source obeys the ergodic Markov process by introducing new distribution family, switched Gaussian convolution distribution, when the

channel is a discrete memoryless. We also compare the joint source-channel scheme with the separation scheme.

On the Necessary Conditions for Transmitting Correlated Sources over a Multiple Access Channel (10:50)

Basak Guler (The Pennsylvania State University, USA); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain)); Aylin Yener (Pennsylvania State University, USA)

We study the lossy communication of correlated sources over a multiple access channel (MAC). In particular, we provide a new set of necessary conditions for the achievability of a distortion pair over a given channel. The necessary conditions are then specialized to the case of bivariate Gaussian sources and doubly symmetric binary sources over a Gaussian multiple access channel. Our results indicate that the new necessary conditions provide the tightest conditions to date in certain cases.

Tu1-6: Strong Converses

Tuesday, June 27, 09:50-11:10
Room: K5
Chair: Shun Watanabe (Tokyo University of Agriculture and Technology, Japan)

Strong Converse for Content Identification with Lossy Recovery (09:50)

Lin Zhou *(National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore); Mehul Motani (National University of Singapore, Singapore)*

In this paper, we revisit the content identification problem with lossy recovery (Tuncel and Gündüz, 2014) and establish the exponential strong converse theorem for the problem. Further, we derive an upper bound on the joint excess-distortion and error exponent for the problem.

Strong Converse Theorems for Discrete Memoryless Networks with Tight Cut-Set Bound (10:10)

Silas Fong *(National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore)*

This paper considers a multimessage network where each node may send a message to any other node in the network. Under the discrete memoryless model, we prove the strong converse theorem for any network with tight cut-set bound, i.e., whose cut-set bound is achievable. Our result implies that for any network with tight cut-set bound and any fixed rate vector that resides outside the capacity region, the average error probabilities of any sequence of length-n codes operated at the rate vector must tend to 1 as n grows. The proof is based on the method of types. The proof techniques are inspired by the work of Csiszar and Korner in 1982 which fully characterized the reliability function of any discrete memoryless channel (DMC) with feedback for rates above capacity. Our proof techniques can be extended to the Gaussian case.

Reverse hypercontractivity region for the binary erasure channel (10:30)

Chandra Nair (Chinese University of Hong Kong, Hong Kong); Yan Nan Wang (The Chinese University of Hong Kong, Hong Kong)

In this paper, we obtain the reverse hypercontractive region for the pair of variables (X, Y) where X is a uniformly distributed binary random variable and Y (a ternary random variable) is obtained by passing X through a symmetric binary erasure channel (BEC), for a non-trivial range of parameters. The technique used builds on two result results: $a)$ characterization of reverse hypercontractivity using information measures, and $b)$ computation of the forward hypercontractive region for the BEC.

Beyond the Blowing-Up Lemma: Sharp Converses via Reverse Hypercontractivity (10:50)

Jingbo Liu (Princeton University, USA); Ramon van Handel (Princeton University, USA); Sergio Verdú (Princeton University, USA)

This paper proposes a general method for establishing non-asymptotic converses in network information theory via reverse hypercontractivity of Markov semigroups. In contrast to the blowing-up lemma, the proposed approach is applicable to non-discrete settings, and yields the optimal order of the second-order term in the rate expansion (square root of the blocklength) in the regime of non-vanishing error probability.

Tu1-7: Crypto 1

Tuesday, June 27, 09:50-11:10
Room: K6
Chair: Matthieu Bloch (Georgia Institute of Technology, USA)

An Information-theoretic Approach to Hardness Amplification (09:50)

Ueli Maurer (ETH Zurich, Switzerland)

Consider two independent games of chance, G and H, which can be won with probability at most β and γ, respectively. Then it can be shown that the game consisting of winning both G *and* H can be won with

probability at most $\beta\gamma$. If the bounds on the winning probability are only due to the computational hardness of the problems and the computational complexity constraints of the game solver algorithm, then the analogous statement is not trivial but indeed holds in an approximate sense under certain conditions. This paper provides a general information-theoretic treatment of this result, showing that it is an abstract statement that is independent of complexity-theoretic considerations and exhibiting explicitly the requirement that a given game instance must be clonable. The core of the proof is a lemma on multi-argument conditional probability distributions. The amplification statement can be generalized to an arbitrary number of independent games, making the winning probability exponentially small in the number of such games.

Witness-Hiding Proofs of Knowledge for Cable Locks (10:10)

Chen-Da Liu Zhang (ETH Zurich, Switzerland); Ueli Maurer (ETH Zurich, Switzerland); Martin Raszyk (ETH Zurich, Switzerland); Daniel Tschudi (ETH Zurich, Switzerland)

We consider the general setting where users need to provide a secret code c to a verifying entity V in order to obtain access to a resource. More generally, the right to access the resource could, for example, be granted if one knows one of two codes c1 and c2. For privacy reasons, a party P may want to hide which of the two codes it knows and only prove that it knows at least one of them. For example, if the knowledge of a code corresponds to membership in a certain society, one may want to hide which society one belongs to. In cryptography, such a proof is called a witness-hiding proof of knowledge. How can P prove such a statement to V? This paper is concerned with witness-hiding proofs of knowledge using simple mechanical tools. Specifically, we consider cable (or bicycle) locks, where the codes of the locks correspond to the secret codes. The above example of proving knowledge of either c1 or c2 in a witness-hiding fashion can be achieved simply as follows. When given the two locks closed and unlinked (by V), P presents the configuration of the two locks interlocked, which can be generated if and only if P knows at least one of the codes. In the most general case with n codes c1,...,cn, the access right is characterized by a so-called knowledge structure G, a subset of the power set of 1,...,n. Access is granted if a user knows the codes corresponding to any of the subsets of G. We present lock-based protocols for witness-hiding proofs of knowledge for any such monotone knowledge structure, and investigate the efficiency (i.e., in particular, the number of lock configurations that P must present) in several settings such as the availability of solid rings or the availability of multiple locks for a given code. The topic of this paper is similar in spirit to other works, such as the picture hanging puzzles by Demaine et al., which explore connections between topology and real-world applications, where the motivation arises also, or even primarily, from mathematical curiosity.

Privacy Amplification of Distributed Encrypted Sources with Correlated Keys (10:30)

Bagus Santoso *(University of Electro-Communications, Japan); Yasutada Oohama (University of Electro-Communications, Japan)*

In this paper, we consider a system where multiple sources are encrypted in separated nodes and sent through their respective public communication channels into a joint sink node. We are interested at the problem on protecting the security of an already existing system such above, which is found out to have correlated encryption keys. Specifically, we focus on finding a solution which does not require the modification of either the source data or the keys, since physically modifying terminals or key generators of an existing system in real world is not always feasible. We propose a solution under a security model where an eavesdropper obtains all ciphertexts, i.e., encrypted sources, by accessing available public communication channels. Our main technique is to use encoders of certain linear codes to encode the ciphertexts before sending them to public communication channels. We show that if the rates of linear codes are within a certain rate region: (1) the success probability of any eavesdropper to extract the original sources from the encoded ciphertexts without the keys is negligible, while (2) one who has legitimate keys is able to retrieve the original source data with negligible error probability.

Tu1-8: Wireless Communication

Tuesday, June 27, 09:50-11:10
Room: K7+8
Chair: Yingbin Liang (Syracuse University, USA)

Can Full-Duplex More than Double the Capacity of Wireless Networks? (09:50)

Serj Haddad (EPFL, Switzerland); Ayfer Özgür (Stanford University, USA); Emre Telatar (EPFL, Switzerland)

Usually, wireless radios are half-duplex, i.e. they can not transmit and receive at the same time over the same frequency band. However, building on self-interference cancellation techniques, full-duplex radios have emerged as a viable paradigm over the recent years. In this paper, we ask the following question: how much can full-duplex increase the capacity of wireless networks? Intuitively, one may expect that full-duplex radios can at most double the capacity of wireless networks, since they enable nodes to transmit and receive at the same time. In this paper, we show that the capacity gain can indeed be larger than a fac-

tor of 2; in particular, we construct a specific instance of a wireless relay network where the capacity with full-duplex radios is triple the capacity of the network when the relays are half-duplex. We also propose a universal schedule for half-duplex networks composed of independent, memoryless, point-to-point channels which achieves at least a fraction of 1/4 of the corresponding full-duplex capacity. This means that for wireless networks composed of point-to-point channels full-duplex capability at the relays cannot more than quadruple the capacity of network.

Short-Message Communication and FIR System Identification using Huffman Sequences (10:10)

Philipp Walk *(California Institute of Technology, USA); Peter Jung (TU-Berlin, Communications and Information Theory Group & Fraunhofer HHI - Heinrich Hertz Institute, Germany); Babak Hassibi (California Institute of Technology, USA)*

Providing short-message communication and simultaneous channel estimation for sporadic and fast fading scenarios is a challenge for future wireless networks. In this work we propose a novel blind communication and deconvolution scheme by using Huffman sequences, which allows to solve three important tasks at once: (i) determination of the transmit power (ii) identification of the instantaneous discrete-time FIR channel if the channel delay is less than $L/2$ and (iii) simultaneously communicating $L-1$ bits of information. Our signal reconstruction uses a recent semi-definite program that can recover two unknown signals from their auto-correlations and cross-correlations. This convex algorithm shows numerical stability and operates fully deterministic without any further channel assumptions.

Novel Construction Methods of Quaternion Orthogonal Designs based on Complex Orthogonal Designs (10:30)

Erum Mushtaq (National University of Sciences and Technology (NUST), Pakistan); ***Sajid Ali*** *(National University of Sciences and Technology, Pakistan); Syed Ali Hassan (National University of Sciences and Technology, Pakistan)*

Quaternion orthogonal designs (QODs) are considered the foundation of orthogonal space time polarization block codes (OSTPBCs). OSTPBCs benefit from orthogonal polarizations and orthogonal space and time block coding simultaneously to enhance the capacity of wireless communication systems. To exploit these advantages of OSTPBCs, this paper explores two generalized construction techniques of QODs, where the first one is based on symmetric-paired designs while the second technique maps the complex orthogonal designs (CODs) to QODs directly. With these schemes, QODs for any number of transmit antennas can be constructed. Moreover, a low-complexity maximum-likelihood (ML) decoder for the proposed construction techniques has been presented that provides optimal decoupled decoding with phenomenal complexity reduction. Simulation results show that the diversity order of the first QOD construction is higher than the second design given the number of transmit antennas are same.

Tu1-9: Hypothesis Testing 2

Tuesday, June 27, 09:50-11:10
Room: K9
Chair: Yanina Shkel (UIUC and Princeton University, USA)

Hypothesis Test for Upper Bound on the Size of Random Defective Set (09:50)

Arkadii Dyachkov (Moscow State University, Russia); Ilya Vorobyev (Moscow State University, Russia); Nikita Polyanskii (Huawei Technologies Co. & Institute for Information Transmission Problems, Russia); Vladislav Shchukin (Moscow State University, Russia)

Let $1 \leq s < t$, $N \geq 1$ be fixed integers and a complex electronic circuit of size t is said to be an s-active, $s \ll t$, and can work as a system block if not more than s elements of the circuit are defective. Otherwise, the circuit is said to be an s-defective and should be replaced by a similar s-active circuit. Suppose that there exists a possibility to run N non-adaptive group tests to check the s-activity of the circuit. As usual, we say that a (disjunctive) group test yields the positive response if the group contains at least one defective element. In this paper, we will interpret the unknown set of defective elements as a random set and discuss upper bounds on the error probability of the hypothesis test for the null hypothesis $\{H_0 : \text{the circuit is s-active}\}$ verse the alternative hypothesis $\{H_1 : \text{the circuit is s-defective}\}$. Along with the conventional decoding algorithm based on the known random set of positive responses and disjunctive s-codes, we consider a T-weight decision rule, which is based on the simple comparison of a fixed threshold T, $1 \leq T < N$, with the known random number of positive responses p, $0 \leq p \leq N$.

Distributed Hypothesis Testing Over Noisy Channels (10:10)

Sreejith Sreekumar (Imperial College London, United Kingdom (Great Britain)); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain))

A distributed binary hypothesis testing problem, in which multiple observers transmit their observations to a detector over noisy channels, is studied. Given its own side information, the goal of the detector is to decide between two hypotheses for the joint distribution of the data. Single-letter upper and lower bounds on the optimal type 2 error exponent (T2-EE), when the type 1 error probability vanishes with the block-length

are obtained. These bounds coincide and characterize the optimal T2-EE when only a single helper is involved. Our result shows that the optimal T2-EE depends on the marginal distributions of the data and the channels rather than their joint distribution. However, an operational separation between HT and channel coding does not hold, and the optimal T2-EE is achieved by generating channel inputs correlated with observed data.

Linear-Complexity Exponentially-Consistent Tests for Universal Outlying Sequence Detection (10:30)

Yuheng Bu (University of Illinois at Urbana Champaign, USA); Shaofeng Zou (University of Illinois at Urbana Champaign, USA); Venugopal Veeravalli (University of Illinois at Urbana-Champaign, USA)

We study a universal outlying sequence detection problem, in which there are M sequences of samples out of which a small subset of outliers need to be detected. A sequence is considered as an outlier if the observations therein are generated by a distribution different from those generating the observations in the majority of the sequences. In the universal setting, the goal is to identify all the outliers without any knowledge about the underlying generating distributions. In prior work, this problem was studied as a universal hypothesis testing problem, and a generalized likelihood (GL) test was constructed and its asymptotic performance characterized. In this paper, we propose a different class of tests for this problem based on distribution clustering. Such tests are shown to be exponentially consistent and their time complexity is linear in the total number of sequences, in contrast with the GL test, which has time complexity that is exponential in the number of outliers. Furthermore, our tests based on clustering are applicable to more general scenarios. For example, when both the typical and outlier distributions form clusters, the clustering based test is exponentially consistent, but the GL test is not even applicable.

Active Hypothesis Testing on A Tree: Anomaly Detection under Hierarchical Observations (10:50)

Chao Wang (Cornell University, USA); ***Kobi Cohen*** *(Ben-Gurion University of the Negev, Israel); Qing Zhao (Cornell University, USA)*

The problem of detecting a few anomalous processes among a large number of M processes is considered. At each time, aggregated observations can be taken from a chosen subset of processes, where the chosen subset conforms to a given binary tree structure. The random observations are i.i.d. over time with a general distribution that may depend on the size of the chosen subset and the number of anomalous processes in the subset. The objective is a sequential search strategy that minimizes the sample complexity (i.e., the expected number of observations which represents detection delay) subject to a reliability constraint. A sequential test that results in a biased random walk on the tree is developed and is shown to be asymptotically optimal in terms of detection accuracy. Furthermore, it achieves the optimal logarithmic-order sample complexity in M provided that the Kullback-Liebler divergence between aggregated observations in the presence and the absence of anomalous processes are bounded away from zero at all levels of the tree structure as M approaches infinity. Sufficient conditions on the decaying rate of the aggregated observations to pure noise under which a sublinear scaling in M is preserved are also identified for the Bernoulli case.

Tu2-1: Coding Techniques 2

Tuesday, June 27, 11:30-12:50
Room: Europa
Chair: Alexander Barg (University of Maryland, USA)

Fractional decoding: Error correction from partial information (11:30)

Itzhak Tamo (Tel Aviv University, Israel); Min Ye (UMD, USA); Alexander Barg (University of Maryland, USA)

We consider error correction by maximum distance separable (MDS) codes based on a part of the received codeword. Our problem is motivated by applications in distributed storage. While efficiently correcting erasures by MDS storage codes (the "repair problem") has been widely studied in recent literature, the problem of correcting errors in a similar setting seems to represent a new question in coding theory. Suppose that k data symbols are encoded using an (n, k) MDS code, and some of the codeword coordinates are located on faulty storage nodes that introduce errors. We want to recover the original data from the corrupted codeword under the constraint that the decoder can download only an α proportion of the codeword (*fractional decoding*). For any (n, k) code we show that the number of correctable errors under this constraint is bounded above by $\lfloor (n - k/\alpha)/2 \rfloor$. Moreover, we present two families of MDS array codes which achieves this bound with equality under a simple decoding procedure. The decoder downloads an α proportion of each of the codeword's coordinates, and provides a much larger decoding radius compared to the naive approach of reading some αn coordinates of the codeword. One of the code families is formed of Reed-Solomon (RS) codes with well-chosen evaluation points, while the other is based on folded RS codes. Finally, we show that folded RS codes also have the optimal list decoding radius under the fractional decoding constraint.

Performance of Optimal Data Shaping Codes (11:50)

Yi Liu (University of California, San Diego, USA); Pengfei Huang (University of California, San Diego, USA); Paul Siegel (University of California, San Diego, USA)

Data shaping is a coding technique that has been proposed to increase the lifetime of flash memory devices. Several data shaping codes have been described in recent work, including endurance codes and direct shaping codes for structured data. In this paper, we study information-theoretic properties of a general class of data shaping codes and prove a separation theorem stating that optimal data shaping can be achieved by the concatenation of optimal lossless compression with optimal endurance coding. We also determine the expansion factor that minimizes the total wear cost. Finally, we analyze the performance of direct shaping codes and establish a condition for their optimality.

Multilevel Code Construction for Compound Fading Channels (12:10)

Antonio Campello (Imperial College London, United Kingdom (Great Britain)); Ling Liu (Department of Electrical and Electronic Engineering Imperial College London, United Kingdom (Great Britain)); Cong Ling (Imperial College London, United Kingdom (Great Britain))

We consider explicit constructions of multi-level lattice codes that universally approach the capacity of the compound block-fading channel. Specifically, building on algebraic partitions of lattices, we show how to construct codes with negligible probability of error for any channel realization and normalized log-density approaching the Poltyrev limit. Capacity analyses and numerical results on the achievable rates for each partition level are provided. The proposed codes have several enjoyable properties such as constructiveness and good decoding complexity, as compared to random one-level codes. Numerical results for finite-dimensional multi-level lattices based on polar codes are exhibited.

Dense Gray Codes in Mixed Radices (12:30)

***Jessica Fan** (Dartmouth College, USA); Thomas Cormen (Dartmouth College, USA)*

The standard binary reflected Gray code produces a permutation of the sequence of integers <0,1,...,n-1>, where n is a power of 2, such that the binary representation of each integer in the permuted sequence differs from the binary representation of the preceding integer in exactly one bit. In an earlier paper, we presented two methods to compute binary dense Gray codes, which extend the possible values of n to the set of all positive integers while preserving both the Gray code property—only one bit changes between each pair of consecutive integers—and the denseness property—the sequence contains exactly the n integers 0 to n-1. This paper generalizes our method for binary dense Gray codes to arbitrary radices that may be either a single fixed radix for all digits or mixed radices, so that each digit may have a different radix. That is, we show how to produce a permutation of <0,1,...,n-1> represented in any set of radices, such that the representation of each number differs from the representation of the preceding number in exactly one digit, and the values of these digits differ by exactly 1. We provide a simple formula for this permutation, which we can use to quickly compute a Hamiltonian path for a dynamic array of n nodes, where the nodes are added and deleted in order along the k dimensions of a grid network.

Tu2-2: Locally Repairable Codes 2

Tuesday, June 27, 11:30-12:50
Room: Brussels
Chair: Antonia Tulino (Bell Labs, USA)

Balanced and Sparse Tamo-Barg Codes (11:30)

*Wael Halbawi (California Institute of Technology, USA); **Iwan Duursma** (University of Illinois at Urbana-Champaign, USA); Hoang Dau (University of Illinois at Urbana-Champaign, USA); Babak Hassibi (California Institute of Technology, USA)*

We construct balanced and sparse generator matrices for Tamo and Barg's Locally Recoverable Codes (LRCs). More specifically, for length n, dimension k and locality r cyclic Tamo–Barg code, we show how to deterministically construct a generator matrix where the number of nonzeros in any two columns differs by at most one, and where the weight of every row is $d+r-1$, where d is the minimum distance of the code. Since LRCs are designed mainly for distributed storage systems, the results presented here provide a computationally balanced and efficient encoding scheme for these codes. The balanced property ensures the computational effort exerted is the essentially the same for any server, whilst the sparse property ensures that this effort is minimal. The work presented in this paper extends a similar result for Reed–Solomon (RS) codes, where it is now known that any cyclic RS code possesses a generator matrix that is balanced as described, but is sparsest, meaning that each row has d nonzeros.

Bounds and Constructions of Codes with All-Symbol Locality and Availability (11:50)

Stanislav Kruglik *(Moscow Institute of Physics and Technology & Skolkovo Institute of Science and Technology, Russia); Alexey Frolov (Skolkovo Institute of Science and Technology & IITP RAS, Russia)*

We investigate the distance properties of linear locally recoverable codes (LRC codes) with all-symbol locality and availability. New upper and lower bounds on the minimum distance of such codes are derived. The upper bound is based on the shortening method and improves existing shortening bounds. To reduce the gap in between upper and lower bounds we do not restrict the alphabet size and propose explicit constructions of codes with locality and availability via rank-metric codes. The first construction relies on expander graphs and is better in low rate region, the second construction utilizes LRC codes developed by Wang et al. as inner codes and better in high rate region.

Security for Minimum Storage Regenerating Codes and Locally Repairable Codes (12:10)

Swanand Kadhe (Texas A&M University, USA); Alex Sprintson (Texas A&M University, USA)

We consider the problem of designing 'repair efficient' distributed storage systems, which are information-theoretically secure against a passive eavesdropper that can gain access to a limited number of storage nodes. We present a framework that enables design of a broad range of secure storage codes through a joint construction of inner and outer codes. As case studies, we focus on two specific families of storage codes: (i) minimum storage regenerating (MSR) codes, and (ii) maximally recoverable (MR) codes, which are a class of locally repairable codes (LRCs). The main idea of this framework is to utilize the existing constructions of storage codes to jointly design an outer coset code and inner storage code. Finally, we present a construction of an outer coset code over small field size to secure locally repairable codes presented by Tamo and Barg for the special case of an eavesdropper that can observe any subset of nodes of maximum possible size.

Tu2-3: Broadcast Channels 2

Tuesday, June 27, 11:30-12:50
Room: K2
Chair: Vincent Tan (National University of Singapore, Singapore)

The Arbitrarily Varying Degraded Broadcast Channel with Causal Side Information at the Encoder (11:30)

Uzi Pereg (Technion, Israel); Yossef Steinberg (Technion, Israel)

In this work, we study the arbitrarily varying degraded broadcast channel (AVDBC), when state information is available at the transmitter in a causal manner. We establish inner and outer bounds on both the random code capacity region and the deterministic code capacity region. The capacity region is then determined for a class of channels satisfying a condition on the mutual informations between the strategy variables and the channel outputs. As an example, we show that the condition holds for the arbitrarily varying binary symmetric broadcast channel, and we find the corresponding capacity region.

Sub-optimality of superposition coding region for three receiver broadcast channel with two degraded message sets (11:50)

Mehdi Yazdanpanah (The Chinese University of Hong Kong, Hong Kong); Chandra Nair (Chinese University of Hong Kong, Hong Kong)

In this article, we resolve open problem 8.2 in Network Information Theory Book by El Gamal and Kim. We show that superposition coding is sub-optimal for a three receiver broadcast channel with two message sets (M_0, M_1) where two of the three receivers need to decode messages (M_0, M_1) while the remaining one just needs to decode the message M_0.

The Broadcast Channel with Degraded Message Sets and Unreliable Conference (12:10)

Dor Itzhak (Technion, Israel); Yossef Steinberg (Technion, Israel)

As demonstrated in many recent studies, cooperation between users can greatly improve the performance of communication systems. Most of the works in the literature present models where all the users are aware of the resources available for cooperation. However, the scenario where cooperation links are sometimes unavailable or that some users cannot be updated whether the cooperation links are present or not, is more realistic in today's dynamic ad-hoc communication systems. In such a case we need coding schemes that exploit the cooperation links if they are present,

and can still operate if cooperation is not possible. In this work we study the general broadcast channel model with degraded message sets and cooperation links that may be absent, and derive it's capacity region under such uncertainty conditions.

On the Capacity Region of the K-User Discrete Memoryless Broadcast Channel with Two Degraded Messages (12:30)

Mahesh Varanasi (University of Colorado, USA); Mohamed Salman (University of Colorado Boulder, USA)

The K-user discrete memoryless (DM) broadcast channel (BC) with two degraded messages, with one common message to be decoded by all receivers and a private message by a subset of receivers, is studied. The receivers that must decode both messages are referred to as private receivers and the remaining ones that must decode only the common message as common receivers. We obtain two main results. The first main result establishes the capacity region of two classes of DM BCs characterized by the associated sets of pair-wise relationships between and among the common and private receivers, each described by the well-known more capable and less noisy conditions. For both these classes, the capacity region is achieved by superposition coding and joint decoding so that the main contribution herein lies in the proofs of the converses. When specialized to the two previously well-studied cases of a single private receiver and a single common receiver, the two aforementioned classes are respectively as large as or larger than those for which capacity was previously obtained. The second main result is a new inner bound in closed form for arbitrary K and a general subset of private receivers that involves rate splitting, superposition coding, and indirect decoding and we state its capacity optimality for a new class of four-receiver DM BCs.

Tu2-4: Channel Capacity 2

Tuesday, June 27, 11:30-12:50
Room: K3
Chair: Amos Lapidoth (ETHZ, Switzerland)

The Optimal Exponent Function for the Additive White Gaussian Noise Channel at Rates above the Capacity (11:30)

Yasutada Oohama (University of Electro-Communications, Japan)

We consider the additive white Gaussian noise channels. We prove that the error probability of decoding tends to one exponentially for rates above the capacity and derive the optimal exponent function. We shall demonstrate that the information spectrum approach is quite useful for investigating this problem.

A Generalized Ozarow-Wyner Capacity Bound with Applications (11:50)

*Alex Dytso (Princeton University, USA); **Mario Goldenbaum** (Princeton University, USA); H. Vincent Poor (Princeton University, USA); Shlomo (Shitz) Shamai (The Technion, Israel)*

In this paper, a generalized Ozarow-Wyner capacity bound is presented that holds for arbitrary noise channels. The bound is then used to approximate the capacity of a large class of additive noise channels that are subject to a p-th moment input constraint, where p is some positive real number, as well as to the Cauchy noise channel with a logarithmic moment constraint. For both channel models the gap to the capacity is precisely specified.

A Bound on the Shannon Capacity via a Linear Programming Variation (12:10)

Sihuang Hu (Tel Aviv University, Israel); Itzhak Tamo (Tel Aviv University, Israel); Ofer Shayevitz (Tel Aviv University, Israel)

We prove an upper bound on the Shannon capacity of a graph via a linear programming variation. We also show that our bound can be better than Lovasz theta number and Haemers minimum rank bound.

On the Discreteness of Capacity-Achieving Distributions for the Censored Channel (12:30)

***Arash Behboodi** (RWTH Aachen University, Germany); Gholamreza Alirezaei (RWTH Aachen University, Germany); Rudolf Mathar (RWTH Aachen University, Germany)*

The censored channel is one of the fundamental channels in information theory, which belongs to the class of non-linear channels. It is modeled by cascading an additive noise channel with a clipping operator. This paper is concerned with the information theoretic capacity of this channel. A necessary and sufficient condition for optimality of the input distribution is derived and it is shown that the capacity-achieving input distribution for the amplitude-limited censored channel has only a finite number of mass points. This result holds for a large class of noise distributions including additive Gaussian noise.

Tu2-5: Massive MIMO

Tuesday, June 27, 11:30-12:50
Room: K4
Chair: Christoph Studer (Cornell University, USA)

Massive Device Connectivity with Massive MIMO (11:30)

Liang Liu (University of Toronto, Canada); Wei Yu (University of Toronto, Canada)

This paper studies a single-cell uplink massive device communication scenario in which a large number of single antenna devices are connected to the base station (BS), but user traffic is sporadic so that at a given coherence interval, only a subset of users are active. For such a system, active user detection and channel estimation are key issues. To accommodate such a large number of active users, this paper studies the asymptotic regime where the BS is equipped with a large number of antennas. A grant-free two-phase access scheme is adopted where user activity detection and channel estimation are performed in the first phase, and data is transmitted in the second phase. Our main contributions are as follows. First, this paper shows that despite the non-orthogonality of pilot sequences (which is necessary for accommodating a large number of potential devices), in the asymptotic massive multiple-input multiple-output (MIMO) regime, both the missed detection and false alarm probabilities can be made to go to zero by utilizing compressed sensing techniques that exploit sparsity in user activities. Further, this paper shows that despite the guaranteed success in user activity detection, the non-orthogonality of pilot sequences nevertheless can cause significant channel estimation error, thus the overall achievable transmission rate in the massive MIMO regime is mostly limited by channel estimation rather than device activity detection performance. This paper quantifies the cost due to non-orthogonal pilots for massive connectivity and further identifies the optimal pilot length in this setting.

On the MISO Channel with Feedback: Can Infinitely Massive Antennas Achieve Infinite Capacity? (11:50)

Jinyuan Chen (Louisiana Tech University, USA)

We consider communication over a multiple-input single-output (MISO) block fading channel in the presence of an independent noiseless feedback link. We assume that the transmitter and receiver have no prior knowledge of the channel state realizations, but the transmitter and receiver can acquire the channel state information (CSIT/CSIR) via downlink training and feedback. For this channel, we show that increasing the number of transmit antennas to infinity will not achieve an infinite capacity, for a finite channel coherence and a finite input constraint on the second or fourth moment. This insight follows from our new capacity bounds that hold for any linear and nonlinear coding strategies, and any channel training schemes. In addition to the channel capacity bounds, we also provide a characterization on the beamforming gain that is also known as array gain or power gain, at the regime with large number of antennas.

The BOX-LASSO with Application to GSSK Modulation in Massive MIMO Systems (12:10)

Ismail Ben Atitallah (KAUST, Saudi Arabia); Christos Thrampoulidis (MIT, USA); Abla Kammoun (Kaust, Saudi Arabia); Tareq Y. Al-Naffouri (King Abdullah University of Science and Technology, USA); Mohamed-Slim Alouini (King Abdullah University of Science and Technology (KAUST), Saudi Arabia); Babak Hassibi (California Institute of Technology, USA)

The BOX-LASSO is a variant of the popular LASSO that includes an additional box-constraint. We propose its use as a decoder in modern Multiple Input Multiple Output (MIMO) communication systems with modulation methods such as the Generalized Space Shift Keying (GSSK) modulation, which produce constellation vectors that are inherently sparse and have elements that belong to finite alphabets. In that direction, we prove novel explicit asymptotic characterizations of the squared-error and of the per-element error rate of the BOX-LASSO, under iid Gaussian measurements. In particular, the theoretical predictions can be used to quantify the improved performance of the BOX-LASSO, when compared to the previously used standard LASSO. We include simulation results that validate both these premises and our theoretical predictions.

Multi-Users Space-Time Modulation with QAM Division for Massive Uplink Communications (12:30)

Jian-Kang Zhang (McMaster University, Canada); Zheng Dong (McMaster University, Canada)

In this paper, we consider the design of multi-users space-time modulation (MUSTM) for an uplink MIMO system with one base station equipped with the massive number of antennas and N single-antenna users, where it is assumed that only large scale channel coefficients are available at both the transmitter and the receiver. For such a system, a novel concept called uniquely factorable (UF) MUSTM is introduced. Then, using our recently developed framework on uniquely decomposable constellation group with energy-efficient quadrature amplitude modulation (QAM), and properly and timely assigning each subconstellation to each user at each time slot, we develop a machinery method for systematically designing a family of invertible UF-MUSTM with flexible data rates in order to assure the reliable estimation of the transmit-

ted signal as well as of the channel for the massive MIMO system. In addition, a simple cross-correlation receiver is proposed to efficiently and effectively detect such UF-MUSTM. Its pair-wise error probability (PEP) is derived, showing that our proposed invertible UF-MUSRM enables full receiver diversity. Furthermore, the optimal closed-form power allocation and the optimal user constellation assignment are found to maximize the worst-case coding gain under a peak power constraint on each user and each time slot.

Tu2-6: MIMO 2

Tuesday, June 27, 11:30-12:50
Room: K5
Chair: Vasanthan Raghavan (Qualcomm, Inc., USA)

Generalized Degrees-of-Freedom of the 2-User Case MISO Broadcast Channel with Distributed CSIT (11:30)

Antonio Bazco *(EURECOM & Mitsubitshi Electric Research Centre Europe, France); Paul de Kerret (EURECOM, France); David Gesbert (Eurecom Institute, France); Nicolas Gresset (Mitsubishi Electric Research Centre Europe, France)*

This work analyses the Generalized Degrees-of-Freedom (GDoF) of the 2-User Multiple-Input Single-Output (MISO) Broadcast Channel (BC) in the so-called Distributed CSIT regime, with application to decentralized wireless networks. This regime differs from the classical limited CSIT one in that the CSIT is not just noisy but also imperfectly shared across the transmitters (TXs). Hence, each TX precodes data on the basis of local CSIT and statistical quality information at other TXs. We derive the GDoF result and obtain the surprising outcome that by specific accounting of the pathloss information, it becomes possible for the decentralized precoded network to reach the same performance as a genie-aided centralized network where the central node has obtained the estimates of both TXs. The key idea allowing this surprising robustness is to let the TXs have asymmetrical roles such that the most informed TX is able to balance the lower CSIT quality at the other TX.

Spatially Correlated MIMO Broadcast Channel: Analysis of Overlapping Correlation Eigenspaces (11:50)

Fan Zhang (University of Texas at Dallas, USA); Mohamed Fadel (University of Texas at Dallas, USA); Aria Nosratinia (University of Texas, Dallas, USA)

Antenna correlation is prevalent in higher frequencies as well as in massive MIMO, thus the study of *correlated* MIMO broadcast channels is becoming a subject of increasing interest. This paper explores the fundamental limits of such systems, focusing on cases where correlation eigenspaces are neither independent nor identical, so that known beam-space division techniques do not directly apply. We begin by introducing a simple but novel tight outer bound on the degrees of freedom (DoF) of noncoherent point-to-point MIMO channels under transmit antenna correlation. We then analyze the performance of a two-user MIMO broadcast channel when one correlation eigenspace is a subspace of the other. We extend the result to K-user MIMO broadcast channel. Our results show that it is possible to exploit the differences between the correlation structure of transmit antennas towards different receivers to extract DoF gains out of the system. The extent of these gains are highlighted via several examples.

On the Achievable Rates of Decentralized Equalization in Massive MU-MIMO Systems (12:10)

Charles Jeon (Cornell University, USA); Kaipeng Li (Rice University, USA); Joseph Cavallaro (Rice University, USA); Christoph Studer (Cornell University, USA)

Massive multi-user (MU) multiple-input multiple-output (MIMO) promises significant gains in spectral efficiency compared to traditional, small-scale MIMO technology. Linear equalization algorithms, such as zero forcing (ZF) or minimum mean-square error (MMSE)-based methods, typically rely on centralized processing at the base station (BS), which results in (i) excessively high interconnect and chip input/output data rates, and (ii) high computational complexity. In this paper, we investigate the achievable rates of decentralized equalization that mitigates both of these issues. We consider two distinct BS architectures that partition the antenna array into clusters, each associated with independent radio-frequency chains and signal processing hardware, and the results of each cluster are fused in a feedforward network. For both architectures, we consider ZF, MMSE, and a novel, non-linear equalization algorithm that builds upon approximate message passing (AMP), and we theoretically analyze the achievable rates of these methods. Our results demonstrate that decentralized equalization with our AMP-based methods incurs no or only a negligible loss in terms of achievable rates compared to that of centralized solutions.

V-BLAST in Lattice Reduction and Integer Forcing (12:30)

Sebastian Stern *(Ulm University, Germany); Robert Fischer (Ulm University, Germany)*

Lattice-reduction-aided decision-feedback equalization (LRA DFE) and successive integer forcing are MIMO detection schemes which combine the equalization in a suited basis with the principle of successive interference cancellation (SIC). To this end, the reduction algorithm not only has to find a suited basis, but

it should also provide an optimized detection order for SIC: the V-BLAST ordering, known to be optimal for conventional DFE. How these two tasks can be solved jointly has so far remained unclear in the literature. In this paper, we describe how the Lenstra-Lenstra-Lovasz (LLL) reduction has to be adapted to achieve this aim. Moreover, we propose a weakened variant of the Hermite-Korkine-Zolotareff (HKZ) reduction that optimally solves both tasks jointly. Results obtained from numerical simulations complement the theoretical derivations.

Tu2-7: Energy Harvesting 2

Tuesday, June 27, 11:30-12:50
Room: K6
Chair: Deniz Gündüz (Imperial College London, United Kingdom (Great Britain))

Energy-Based Adaptive Multiple Access in LPWAN IoT Systems with Energy Harvesting (11:30)

Nicolò Michelusi (Purdue University, USA); Marco Levorato (University of California, Irvine, USA)

This paper develops a control framework for a network of energy harvesting nodes connected to a Base Station (BS) over a multiple access channel. The objective is to adapt their transmission strategy to the state of the network, including the energy available to the individual nodes. In order to reduce the complexity of control, an optimization framework is proposed where energy storage dynamics are replaced by dynamic average power constraints induced by the time correlated energy supply, thus enabling lightweight and flexible network control. Specifically, the BS adapts the packet transmission probability of the ”active” nodes (those currently under a favorable energy harvesting state) so as to maximize the average long-term throughput, under these dynamic average power constraints. The resulting policy takes the form of the packet transmission probability as a function of the energy harvesting state and number of active nodes. The structure of the throughput-optimal genie-aided policy, in which the number of active nodes is known non-causally at the BS, is proved. Inspired by the genie-aided policy, a Bayesian estimation approach is presented to address the case where the BS estimates the number of active nodes based on the observed network transmission pattern. It is shown that the proposed scheme outperforms by 20% a scheme in which the nodes operate based on local state information only, and performs well even when energy storage dynamics are taken into account.

Near Optimal Online Distortion Minimization for Energy Harvesting Nodes (11:50)

Ahmed Arafa (University of Maryland College Park, USA); Sennur Ulukus (University of Maryland, USA)

We consider online scheduling for an energy harvesting communication system where a sensor node collects samples from a Gaussian source and sends them to a destination node over a Gaussian channel. The sensor is equipped with a finite-sized battery that is recharged by an independent and identically distributed (i.i.d.) energy harvesting process over time. The goal is to minimize the long term average distortion of the source samples received at the destination. We study two problems: the first is when sampling is cost-free, and the second is when there is a sampling cost incurred whenever samples are collected. We show that fixed fraction policies [Shaviv-Ozgur], in which a fixed fraction of the battery state is consumed in each time slot, are near-optimal in the sense that they achieve a long term average distortion that lies within a constant additive gap from the optimal solution for all energy arrivals and battery sizes. For the problem with sampling costs, the transmission policy is bursty; the sensor can collect samples and transmit for only a portion of the time.

Scheduling Status Updates to Minimize Age of Information with an Energy Harvesting Sensor (12:10)

Tan Bacinoglu (METU, Turkey); Elif Uysal-Biyikoglu (METU, Turkey)

Age of Information is a measure of the freshness of status updates in monitoring applications and update-based systems. We study a real-time sensing scenario with a sensor which is restricted by time-varying energy constraints and battery limitations. The sensor sends updates over a packet erasure channel with no feedback. The problem of finding an age- optimal threshold policy, with the transmission threshold being a function of the energy state and the estimated current age, is formulated. The average age is analyzed for the unit battery scenario under a memoryless energy arrival process. Somewhat surprizingly, for any finite arrival rate of energy, there is a positive age threshold for transmission, which corresponding to transmitting lower than the rate of energy arrivals. A lower bound on the average age is obtained for general battery size.

Code Design for Binary Energy Harvesting Channel (12:30)

Mehdi Dabirnia (Bilkent University, Turkey); Tolga Duman (Bilkent University, Turkey)

We consider a binary energy harvesting communication system with a finite battery transmitter over a noisy channel, and design explicit and implementable codes based on concatenation of a nonlinear trellis code

(NLTC) with an outer low density parity check (LDPC) code. We propose two different decoding methods where the simplified one ignores the memory in the battery state while the more sophisticated one utilizes the memory. Numerical results demonstrate that the designed codes outperform other reference schemes. The results also show the superiority of the improved decoding approach over the naive solution.

Tu2-8: Compressed Sensing 2

Tuesday, June 27, 11:30-12:50
Room: K7+8
Chair: Tara Javidi (UCSD, USA)

A Greedy Blind Calibration Method for Compressed Sensing with Unknown Sensor Gains (11:30)

Valerio Cambareri (Université Catholique de Louvain, Belgium); ***Amirafshar Moshtaghpour*** *(Université Catholique de Louvain, Belgium); Laurent Jacques (University of Louvain, Belgium)*

The realisation of sensing modalities based on the principles of compressed sensing is often hindered by discrepancies between the mathematical model of its sensing operator, which is necessary during signal recovery, and its actual physical implementation, which can amply differ from the assumed model. In this paper we tackle the bilinear inverse problem of recovering a sparse input signal and some unknown, unstructured multiplicative factors affecting the sensors that capture each compressive measurement. Our methodology relies on collecting a few snapshots under new draws of the sensing operator, and applying a greedy algorithm based on projected gradient descent and the principles of iterative hard thresholding. We explore empirically the sample complexity requirements of this algorithm by testing its phase transition, and show in a practically relevant instance of this problem for compressive imaging that the exact solution can be obtained with only a few snapshots.

Information-theoretic bounds and phase transitions in clustering, sparse PCA, and submatrix localization (11:50)

Jess Banks (University of California-Berkeley, USA); Cristopher Moore (Santa Fe Institute, Algeria); Roman Vershynin (University of Michigan, USA); Nicolas Verzelen (INRA, USA); Jiaming Xu (Purdue University, USA)

We study the problem of detecting a structured, low-rank signal matrix corrupted with additive Gaussian noise. This includes clustering in a Gaussian mixture model, sparse PCA, and submatrix localization. Each of these problems is conjectured to exhibit a sharp information-theoretic threshold, below which the signal is too weak for any algorithm to detect. We derive upper and lower bounds on these thresholds by applying the first and second moment methods to the likelihood ratio between these "planted models" and null models where the signal matrix is zero. For sparse PCA and submatrix localization, we determine this threshold exactly in the limit where the number of blocks is large or the signal matrix is very sparse; for the clustering problem, our bounds differ by a factor of $\sqrt{2}$ when the number of clusters is large. Moreover, our upper bounds show that for each of these problems there is a significant regime where reliable detection is information-theoretically possible but where known algorithms such as PCA fail completely, since the spectrum of the observed matrix is uninformative. This regime is analogous to the conjectured 'hard but detectable' regime for community detection in sparse graphs.

Almost Optimal Phaseless Compressed Sensing with Sublinear Decoding Time (12:10)

Vasileios Nakos (Harvard University, USA)

In the problem of compressive phase retrieval, one wants to recover an approximately k-sparse signal $x \in \mathbb{C}^n$, given the magnitudes of the entries of Φx, where $\Phi \in \mathbb{C}^{m \times n}$. This problem has received a fair amount of attention, with sublinear time algorithms appearing in several publications. In this paper we further investigate the direction of sublinear decoding for real signals by giving a recovery scheme under the ℓ_2/ℓ_2 guarantee, with almost optimal, $\mathcal{O}(k \log n)$, number of measurements. Our result outperforms all previous work in the number of measurements, while it also achieves a stronger error guarantee and a smaller failure probability. Moreover, we give a very simple deterministic scheme that recovers all k-sparse vectors in $\mathcal{O}(k^3)$ time, using $4k - 1$ measurements.

A Characterization of Sampling Patterns for Low-Rank Multi-View Data Completion Problem (12:30)

Morteza Ashraphijuo (Columbia University, USA); Xiaodong Wang (Columbia University, USA); Vaneet Aggarwal (Purdue University, USA)

In this paper, we consider the problem of completing a sampled matrix $\mathbf{U} = [\mathbf{U}_1|\mathbf{U}_2]$ given the ranks of $\mathbf{U}$, $\mathbf{U}_1$, and $\mathbf{U}_2$ which is known as the multi-view data completion problem. We characterize the deterministic conditions on the locations of the sampled entries that is equivalent (necessary and sufficient) to finite completability of the sampled matrix. To this end, in contrast with the existing analysis on Grassmannian manifold for a single-view matrix, i.e., conventional matrix completion, we propose a geometric analysis on the manifold structure for multi-view data to incorporate more than one rank constraint. Then, using the proposed geometric analysis, we propose sufficient conditions on the sampling pattern, under which

there exists only one completion (unique completability) given the three rank constraints.

Tu2-9: Source Coding 2

Tuesday, June 27, 11:30-12:50
Room: K9
Chair: Ertem Tuncel (UC Riverside, USA)

Coding of Binary AIFV Code Trees (11:30)

Kentaro Sumigawa (The University of Tokyo, Japan); Hirosuke Yamamoto (The University of Tokyo, Japan)

Binary AIFV codes, which can attain better compression rate than Huffman codes, uses two code trees that may have incomplete internal nodes, and source symbols are assigned to some internal nodes in addition to leaves. Although the code trees of Huffman codes, which are full binary trees, are well studied, the AIFV code trees have not yet studied in detail. In this paper, we show that there exists a bijection between binary AIFV code trees and Schröder paths, and give two coding schemes to represent Schröder paths. The first one is a fixed length coding scheme, which has O(n^2) time-complexity. The second one is a variable length coding scheme using a simple AIFV code. The latter attains O(n) time-complexity, but the coding rate has loss less than 4.1% of the optimal coding rate.

Universal lossy compression under logarithmic loss (11:50)

Yanina Shkel (UIUC and Princeton University, USA); Maxim Raginsky (University of Illinois at Urbana-Champaign, USA); Sergio Verdú (Princeton University, USA)

Universal lossy source coding with the logarithmic loss distortion criterion is studied. Bounds on the non-asymptotic fundamental limit of fixed-length universal coding with respect to a family of distributions are derived. These bounds generalize the well-known minimax bounds for universal lossless source coding. The asymptotic behavior of the resulting optimization problem is studied for a family of iid sources with a finite alphabet size, and is characterized up to a constant. The redundancy of memoryless sources behaves like $\frac{k}{2}\log n$, where n is the blocklength and k is the number of degrees of freedom in the parameter space. The impact of the coding rate is on the constant term: higher compression rate effectively reduces the volume of the parameter uncertainty set.

Towards Optimal Quantization of Neural Networks (12:10)

Avhishek Chatterjee (University of Illinois at Urbana-Champaign, USA); Lav Varshney (University of Illinois at Urbana-Champaign, USA)

Due to the unprecedented success of deep neural networks in inference tasks like speech and image recognition, there has been increasing interest in using them in mobile and in-sensor applications.As most current deep neural networks are very large in size, a major challenge lies in storing the network in devices with limited memory. Consequently there is growing interest in compressing deep networks by quantizing synaptic weights, but most prior work is heuristic and lacking theoretical foundations. Here we develop an approach to quantizing deep networks using functional high-rate quantization theory. Under certain technical conditions, this approach leads to an optimal quantizer that is computed using the celebrated backpropagation algorithm. In all other cases, a heuristic quantizer with certain regularization guarantees can be computed.

Stochastic Stability of Non-Markovian Processes and Adaptive Quantizers (12:30)

Serdar Yüksel (Queen's University, Canada)

In many applications, the common assumption that a driving noise process affecting a system is independent or Markovian may not be realistic, but the noise process may be assumed to be stationary. To study such problems, this paper investigates stochastic stability properties of a class of non-Markovian processes, where the existence of a stationary measure, asymptotic mean stationarity and ergodicity conditions are studied. Applications in adaptive quantization and stochastic networked control are presented.

Tu3-1: Network Coding 1

Tuesday, June 27, 14:40-16:20
Room: Europa
Chair: Tuvi Etzion (Technion-Israel Institute of Technology, Israel)

Secrecy and Robustness for Active Attack in Secure Network Coding (14:40)

Masahito Hayashi (Nagoya University, Japan); Masaki Owari (Shizuoka University, Japan); Go Kato (NTT Corporation, Japan); Ning Cai (Xidian University, P.R. China)

In the network coding, we discuss the effect by sequential error injection to information leakage. We show that there is no improvement when the network is composed of linear operations. However, when the network contains non-linear operations, we find a coun-

terexample to improve Eve's obtained information. Further, we discuss the asymptotic rate in the linear network under the secrecy and robustness conditions.

Linear Network Coding for Two-Unicast-Z Networks: A Commutative Algebraic Perspective and Fundamental Limits (15:00)

Mohammad Fahim (The Pennsylvania State University, USA); Viveck Cadambe (Pennsylvania State University, USA)

We consider a two-unicast-Z network over a directed acyclic graph of unit capacitated edges; the two-unicast-Z network is a special case of two-unicast networks where one of the destinations has apriori side information of the unwanted (interfering) message. In this paper, we settle open questions on the limits of network coding for two-unicast- Z networks by showing that the generalized network sharing bound is not tight, vector linear codes outperform scalar linear codes, and non-linear codes outperform linear codes in general. We also develop a commutative algebraic approach to deriving linear network coding achievability results, and demonstrate our approach by providing an alternate proof to the previous result of Wang et. al. regarding feasibility of rate (1, 1) in the network.

Network-Coded Fronthaul Transmission for Cache-Aided C-RAN (15:20)

Tian Ding *(The Chinese University of Hong Kong, Hong Kong); Xiaojun Yuan (University of Electronic Science and Technology of China, P.R. China); Soung Chang Liew (The Chinese University of Hong Kong, Hong Kong)*

In this paper, we study the cache-aided cloud radio access network (C-RAN) with wireless fronthaul, where multiple cache-enabled users are served by multiple cache-enabled transmitters that are connected to a cloud processor through a wireless fronthaul link. We put forth a caching-and-delivery scheme that combines network-coded fronthaul transmission with cache- aided interference management. By broadcasting network-coded messages, the cloud processor provides additional information of the requested files to the transmitters, so as to reduce the edge delivery time. Based on our scheme, an achievable normalized delivery time (NDT) is derived with respect to the cache sizes and the fronthaul capacity.

Optimal Secondary Access in Retransmission based Primary Networks via Chain Decoding (15:40)

Nicolò Michelusi (Purdue University, USA)

This paper investigates the design of secondary access policies which exploit the temporal redundancy of the retransmission protocol employed by primary users (PU) to improve the spectral efficiency of wireless networks. Secondary users (SU) perform selective retransmissions in order to optimize the potential of interference cancellation by buffering the corrupted signals at the SU receiver, and then decoding them via the successive application of chain decoding [1]. The structure of the optimal SU access policy is investigated, so as to maximize the SU throughput under a constraint on the maximum interference caused to the PU. The optimal policy and its performance are found in closed form. It is shown that the optimal policy reflects an optimal randomization among three modes of operation of the SU: 1) The SU remains idle over the entire retransmission interval of the PU, to avoid interfering with the PU; 2) The SU transmits only after decoding the PU packet to leverage interference cancellation; 3) The SU always transmits over the entire retransmission interval of the PU, so as to leverage the chain decoding potential. It is shown numerically that chain decoding attains a throughput gain of 15% with respect to a state-of-the art scheme where the SU does not perform selective retransmissions.

Tu3-2: LDPC Codes 2

Tuesday, June 27, 14:40-16:20
Room: Brussels
Chair: Khaled Abdel-Ghaffar (University of California, USA)

Characterization and Efficient Exhaustive Search Algorithm for Elementary Trapping Sets of Irregular LDPC Codes (14:40)

Yoones Hashemi Toroghi *(Carleton University, Canada); Amir Banihashemi (Carleton University, Canada)*

In this paper, we propose a characterization of elementary trapping sets (ETSs) for irregular low-density parity-check (LDPC) codes. These sets are known to be the main culprits in the error floor region of such codes. The proposed characterization is based on a hierarchical graphical representation of ETSs, starting from simple cycles of the graph, or from single variable nodes, and involves three simple expansion techniques: degree-one tree (dot), $path$ and $lollipop$, thus, the terminology *dpl characterization*. The proposed dpl characterization corresponds to an efficient search algorithm, that, for a given irregular LDPC code, can find all the instances of (a, b) ETSs with size a and with the number of unsatisfied check nodes b, within any range of interest $a \leq a_{max}$ and $b \leq b_{max}$, exhaustively. Simulation results are presented to show the versatility of the search algorithm, and to demonstrate that, compared to the literature, significant improvement in search speed can be obtained.

An Adaptive EMS Algorithm for Nonbinary LDPC Codes (15:00)

Youngjun Hwang (Samsung Electronics Company, Ltd., Korea); Sunghye Cho (Pohang University of Science and Technology (POSTECH), Korea); Kyeongcheol Yang (Pohang University of Science and Technology (POSTECH), Korea)

The extended min-sum (EMS) algorithm for decoding low-density parity-check codes over the finite field with q elements significantly reduces decoding complexity by truncating each message of length q into a message of effective length n_m. The number of effectively dominant components in each truncated message may gradually decrease with the number of decoding iterations. Based on this observation, we propose a novel adaptive EMS algorithm, called a two-length EMS (TL-EMS) algorithm. It chooses one of two candidate values as the effective message length n_m for each message by reflecting the concept called *message separation*. Numerical results show that it can significantly reduce the computational complexity with little performance degradation.

A Two-Stage Decoding Algorithm for Short Nonbinary LDPC Codes with Near-ML Performance (15:20)

Dixia Deng (Xidian University, P.R. China); Hengzhou Xu (Zhoukou Normal University, P.R. China); Baoming Bai (Xidian University, P.R. China); Ji Zhang (Xidian University, P.R. China)

This paper proposes a two-stage decoding algorithm (called BP-LED) for short nonbinary low-density parity-check (LDPC) codes. It consists of the classical belief propagation (BP) decoder and a list erasures decoder (LED). Simulation results show that, for the (16, 8) LDPC code over GF(256) in the CCSDS standard, our proposed BP-LED algorithm can achieve a coding gain of 0.6 dB with respect to the FFT-QSPA. By choosing the parameters suitable for the proposed algorithm, it has a negligible performance loss with low decoding complexity compared with the BP-MRB (most reliable basis) algorithm.

Design of Improved Quasi-Cyclic Protograph-Based Raptor-Like LDPC Codes for Short Block-Lengths (15:40)

Sudarsan Vasista Srinivasan Ranganathan (University of California, Los Angeles, USA); Dariush Divsalar (Jet Propulsion Laboratory, USA); Richard Wesel (University of California, Los Angeles, USA)

Protograph-based Raptor-like low-density parity-check codes (PBRL codes) are a recently proposed family of easily encodable and decodable rate-compatible LDPC (RC-LDPC) codes. These codes have an excellent iterative decoding threshold and performance across all design rates. PBRL codes designed thus far, for both long and short block-lengths, have been based on optimizing the iterative decoding threshold of the protograph of the RC code family at various design rates. In this work, we propose a design method to obtain better quasi-cyclic (QC) RC-LDPC codes with PBRL structure for short block-lengths (of a few hundred bits). We achieve this by maximizing an upper bound on the minimum distance of any QC-LDPC code that can be obtained from the protograph of a PBRL ensemble. The obtained codes outperform the original PBRL codes at short block-lengths by significantly improving the error floor behavior at all design rates. Furthermore, we identify a reduction in complexity of the design procedure, facilitated by the general structure of a PBRL ensemble.

Finite-Length LDPC Codes on the q-ary Multi-Bit Channel (16:00)

***Rami Cohen** (Technion - Israel Institute of Technology, Israel); Yuval Cassuto (Technion, Israel)*

In this paper, we address the finite-length decoding performance of LDPC codes over the q-ary multi-bit channel (QMBC). The QMBC is defined over the full q-ary symbols, while addressing the differences in reliability between the bits composing the symbol. We show that unlike the binary erasure channel, the QMBC iterative decoder does not necessarily halt at stopping sets. Instead, its performance depends on the edge-label configuration of the LDPC code graph. We characterize good edge-label configurations, and propose an edge-labeling algorithm for improved iterative-decoding performance. We then provide finite-length maximum-likelihood decoding analysis for both the standard nonbinary random ensemble and LDPC ensembles. Finally, simulations are presented to demonstrate the advantages of the proposed edge-labeling algorithm.

Tu3-3: Caching 2

Tuesday, June 27, 14:40-16:20
Room: K2
Chair: Bobak Nazer (Boston University, USA)

Online Edge Caching in Fog-Aided Wireless Networks (14:40)

Seyyed Mohammadreza Azimi (New Jersey Institute of Technology, USA); Osvaldo Simeone (New Jersey Institute of Technology, USA); Avik Sengupta (Intel Corporation, USA); Ravi Tandon (University of Arizona, USA)

In a Fog Radio Access Network (F-RAN) architecture, edge nodes (ENs), such as base stations, are equipped with limited-capacity caches, as well as with fronthaul links that can support given transmission rates from a cloud processor. Existing information-theoretic analyses of content delivery in F-RANs have

focused on offline caching with separate content placement and delivery phases. In contrast, this work considers an online caching set-up, in which the set of popular files is time-varying and both cache replenishment and content delivery can take place in each time slot. The analysis is centered on the characterization of the long-term Normalized Delivery Time (NDT), which captures the temporal dependence of the coding latencies accrued across multiple time slots in the high signal to noise ratio regime. Online caching and delivery schemes based on reactive and proactive caching are investigated, and their performance is compared to optimal offline caching schemes both analytically and via numerical results.

Benefits of Cache Assignment on Degraded Broadcast Channels (15:00)

Shirin Saeedi Bidokhti (Stanford University, USA); Michele Wigger (Telecom ParisTech, France); Aylin Yener (Pennsylvania State University, USA)

Degraded K-receiver broadcast channels (BC) are studied when receivers have cache memories. Lower and upper bounds are derived on the capacity-memory tradeoff, i.e., on the largest rate that can be achieved over the BC as a function of the receivers' cache sizes. The lower bounds are achieved by two new coding schemes that benefit from non-uniform cache assignment. In some special cases lower and upper bounds coincide. The paper also provides lower and upper bounds on the global capacity-memory tradeoff of degraded BCs, i.e., on the largest capacity-memory tradeoff that can be attained by optimizing the receivers cache-assignment subject to a total cache memory budget. The bounds coincide when the total cache memory budget is sufficiently small or sufficiently large, with thresholds depending on the BC statistics. For small total cache budget M, it is optimal to assign all the cache memory to the weakest receiver. In this regime, the global capacity-memory tradeoff grows as M/D, where D denotes the total number of files in the system. For large total cache budget, it is optimal to assign a positive cache memory to every receiver, where weaker receivers are assigned larger cache memories than stronger receivers. When the total cache budget M exceeds a threshold, then the global capacity memory tradeoff grows as 1/K*M/D. A uniform cache-assignment policy is suboptimal.

Rate-Memory Trade-off for the Two-User Broadcast Caching Network with Correlated Sources (15:20)

Parisa Hassanzadeh (New York University, USA); Antonia Tulino (Bell Laboratories & Università degli studi di Napoli, USA); Jaime Llorca (Nokia Bell Labs, USA); Elza Erkip (New York University, USA)

This paper studies the fundamental limits of caching in a network with two receivers and two files generated by a two-component discrete memoryless source with arbitrary joint distribution. Each receiver is equipped with a cache of equal capacity, and the requested files are delivered over a shared error- free broadcast link. First, a lower bound on the optimal peak rate-memory trade-off is provided. Then, in order to leverage the correlation among the library files to alleviate the load over the shared link, a two-step correlation-aware cache-aided coded multicast (CACM) scheme is proposed. The first step uses Gray-Wyner source coding to represent the library via one common and two private descriptions, such that a second correlation-unaware multiple-request CACM step can exploit the additional coded multicast opportunities that arise. It is shown that the rate achieved by the proposed two-step scheme matches the lower bound for a significant memory regime and it is within half of the conditional entropy for all other memory values.

On the Optimality of Separation between Caching and Delivery in General Cache Networks (15:40)

Navid Naderializadeh (University of Southern California, USA); Mohammad Ali Maddah-Ali (Bell Labs, Alcatel Lucent, USA); Salman Avestimehr (University of Southern California, USA)

We consider a system, containing a library of multiple files and a general memoryless communication network through which a server is connected to multiple users, each equipped with a local isolated cache of certain size that can be used to store part of the library. Each user will ask for one of the files in the library, which needs to be delivered by the server through the intermediate communication network. The objective is to design the cache placement (without prior knowledge of users' future requests) and the delivery phase in order to minimize the (normalized) delivery delay. We assume that the delivery phase consists of two steps: (1) generation of a set of multicast messages at the server, one for each subset of users, and (2) delivery of the multicast messages to the users. In this setting, we show that there exists a universal scheme for cache placement and multicast message generation, which is independent of the underlying communication network between the server and the users, and achieves the optimal delivery delay to within a constant factor for all memoryless networks. We prove this result, even though the capacity region of the underlying communication network is not known, even approximately. This result shows that in the aforementioned setting, a separation between caching and multicast message generation on one hand, and delivering the multicast messages to the users on the other hand is approximately optimal. This result has the important practical implication that the prefetching can be done independent of network structure in the upcoming delivery phase.

Tu3-4: Second Order

Tuesday, June 27, 14:40-16:20
Room: K3
Chair: Giuseppe Durisi (Chalmers University of Technology, Sweden)

Dispersion of the Discrete Arbitrarily-Varying Channel with Limited Shared Randomness (14:40)

Oliver Kosut (Arizona State University, USA); Joerg Kliewer (New Jersey Institute of Technology, USA)

The second-order behavior of the discrete memoryless arbitrarily-varying channel is considered in the fixed error regime when the encoder and decoder share randomness that is independent from the adversarial choice of state. The dispersion (coefficient of the second-order term) is exactly characterized for most channels of interest when infinite shared randomness is allowed, and it is shown that precisely the same dispersion is achievable with only O(log n) bits of shared randomness. We also show that the dispersion is identical to that of the non-adversarial channel induced by the adversary simply choosing an i.i.d. state sequence according to the correct distribution. Further, we present some remarks on the connection to the compound channel, as well as on cost constraints for input and state sequences.

On the calculation of the minimax-converse of the channel coding problem (15:00)

Nir Elkayam (Tel Aviv University, Israel); Meir Feder (Tel-Aviv University, Israel)

A minimax-converse has been suggested for the general channel coding problem. This converse comes in two flavors. The first flavor is generally used for the analysis of the coding problem with non-vanishing error probability and provides an upper bound on the rate given the error probability. The second flavor fixes the rate and provides a lower bound on the error probability. Both converses are given as a min-max optimization problem of an appropriate binary hypothesis testing problem. The minimax solution can also be used in conjunction with random coding to achieve "optimal" coding performance. In this paper we study the properties of the second form, i.e., when the rate is fixed. Necessary and sufficient conditions on the saddle point solution are proved. Moreover, an algorithm for the computation of the saddle point, and hence the bound, is developed. In the DMC case, the algorithm runs in a polynomial time.

Exact Moderate Deviation Asymptotics in Streaming Data Transmission (15:20)

Si-Hyeon Lee (POSTECH, Korea); Vincent Tan (National University of Singapore, Singapore); Ashish Khisti (University of Toronto, Canada)

In this paper, a streaming transmission setup is considered where an encoder observes a new message in the beginning of each block and a decoder sequentially decodes each message after a delay of T blocks. In this streaming setup, the fundamental interplay between the coding rate, the error probability, and the blocklength in the moderate deviations regime is studied. For output symmetric channels, the moderate deviations constant is shown to improve over the block coding or non-streaming setup by exactly a factor of T for a certain range of moderate deviations scalings. For the converse proof, a more powerful decoder to which some extra information is fedforward is assumed. The error probability is bounded first for an auxiliary channel and this result is translated back to the original channel by using a newly developed change-of-measure lemma, where the speed of decay of the remainder term in the exponent is carefully characterized.

Infinite Dispersion in Bursty Communication (15:40)

Longguang Li (Telecom ParisTech, France); Aslan Tchamkerten (Telecom ParisTech, France)

This paper establishes finite-length tradeoffs between detection delay, output sampling rate, and communication rate for bursty communication. These tradeoffs imply regimes where the rate gap to capacity is captured by the inverse of the sampling rate rather than the usual dispersion.

Achievable Moderate Deviations Asymptotics for Streaming Slepian-Wolf Coding (16:00)

Lin Zhou *(National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore); Mehul Motani (National University of Singapore, Singapore)*

Motivated by streaming multi-view video coding, we consider the problem of blockwise streaming compression of a pair of correlated sources, which we term streaming Slepian-Wolf coding. We study the moderate deviations regime in which the rate pairs of a sequence of codes converges, along a straight line, to various points on the boundary of the Slepian-Wolf region at a speed slower than the inverse square root of the blocklength n, while the error probability decays subexponentially fast in n. Our main result focuses on directions of approaches to corner points of the Slepian-Wolf region. It states that for each correlated source and all corner points, there exists a non-empty subset of directions of approaches such that the moderate deviations constant (the constant of proportionality

for the subexponential decay of the error probability) is enhanced (over the non-streaming case) by at least a factor of T, the block delay of decoding symbol pairs. Further, we specialize our main result to the setting of lossless streaming source coding.

Tu3-5: Detection and Estimation 2

Tuesday, June 27, 14:40-16:20
Room: K4
Chair: Jing Yang (The Pennsylvania State University, USA)

Demystifying Fixed k-Nearest Neighbor Information Estimators (14:40)

Weihao Gao (University Of Illinois at Urbana-Champaign, USA); Sewoong Oh (University of Illinois at Urbana-Champaign, USA); Pramod Viswanath (University of Illinois, Urbana-Champaign, USA)

Estimating mutual information from i.i.d. samples drawn from an unknown joint density function is a basic statistical problem of broad interest with multitudinous applications. The most popular estimator is one proposed by Kraskov and Stogbauer and Grassberger (KSG) in 2004, and is nonparametric and based on the distances of each sample to its k-th nearest neighboring sample, where k is a fixed small integer. Despite its widespread use (part of scientific software packages), theoretical properties of this estimator have been largely unexplored. In this paper we demonstrate that the estimator is consistent and also identify an upper bound on the rate of convergence of the ℓ_2 error as a function of number of samples. We argue that the performance benefits of the KSG estimator stems from a curious "correlation boosting" effect and build on this intuition to modify the KSG estimator in novel ways to construct a superior estimator. As a byproduct of our investigations, we obtain nearly tight rates of convergence of the ℓ_2 error of the well known fixed k nearest neighbor estimator of differential entropy by Kozachenko and Leonenko.

Structure of optimal strategies for remote estimation over Gilbert-Elliott channel with feedback (15:00)

Jhelum Chakravorty (McGill University, Canada); Aditya Mahajan (McGill University, Canada)

We investigate remote estimation over a Gilbert- Elliot channel with feedback. The channel is modelled as an ON/OFF channel, where the state of the channel evolves as a Markov chain. The channel state is observed by the receiver and fed back to the transmitter with one unit delay. In addition, the transmitter gets ACK/NACK feedback for successful/unsuccessful transmission. Using ideas from team theory, we establish the structure of optimal transmission and estimation strategies and identify a dynamic program to determine optimal strategies with that structure. We then consider first-order autoregressive sources where the noise process has unimodal and symmetric distribution. Using ideas from majorization theory, we show that the optimal transmission strategy has a threshold structure and the optimal estimation strategy is Kalman-filter like.

Sparse Gaussian Mixture Detection: Low Complexity, High Performance Tests via Quantization (15:20)

Jonathan Ligo *(University of Illinois at Urbana-Champaign, USA); George Moustakides (University of Patras, Greece); Venugopal Veeravalli (University of Illinois at Urbana-Champaign, USA)*

We study the problem of testing between a sparse signal in noise, modeled as a mixture distribution, versus pure noise, with a Gaussian signal and noise of same variance, but differing means as the mixture proportion tends to zero. We construct a simple new adaptive test based on quantizing data with sample size-dependent quantizers and prove its consistency. The proposed test has almost linear time complexity and sub-linear space complexity, which is better than existing tests, and in particular, the celebrated Higher Criticism test. Moreover, our numerical results show that the proposed test is competitive with commonly used tests even with a small number of quantizer levels.

Compressive Estimation of a Stochastic Process with Unknown Autocorrelation Function (15:40)

Mahdi Barzegar Khalilsarai (Technische Universität Berlin, Germany); Saeid Haghighatshoar (Technische Universität Berlin, Germany); Giuseppe Caire (Technische Universität Berlin, Germany); Gerhard Wunder (FU Berlin, Heisenberg Communications and Information Theory Group, Germany)

In this paper, we study the prediction of a circularly symmetric zero-mean stationary Gaussian process from a window of observations consisting of finitely many samples. This is a prevalent problem in a wide range of applications in communication theory and signal processing. Due to the stationarity, when the autocorrelation function or equivalently the power spectral density (PSD) of the process is available, the Minimum Mean Squared Error (MMSE) predictor is readily obtained. In particular, it is given by a linear operator that depends on autocorrelation of the process as well as the noise power in the observed samples. The prediction becomes, however, quite challenging when the PSD of the process is unknown. In this paper, we propose a blind predictor that does not require the a priori knowledge of the PSD of the process and compare its performance with that of an MMSE predictor that has the full knowledge of the the PSD of the process. To design such a blind predictor, we use the random spectral representation of a stationary Gaus-

sian process. We apply the well-known atomic-norm minimization technique to the observed samples to obtain a discrete quantization of the underlying random spectrum, which we use to predict the process. Our simulation results show that this estimator has a good performance comparable with that of the MMSE estimator.

Robust sequential change-point detection by convex optimization (16:00)

*Yang Cao (Georgia Institute of Technology, USA); **Yao Xie** (Georgia Institute of Technology, USA)*

We address the computational challenge of finding the robust sequential change-point detection procedures when the pre- and post-change distributions are not completely specified. Earlier works (Veeravalli, Basar, Poor 1994) and (Unnikrishnan, Veeravalli, Meyn 2011) establish the general conditions for robust procedures which include finding a pair of least favorable distributions (LFDs). However, in the multi-dimensional setting, it is hard to find such LFDs computationally. We present a method based on convex optimization to that address this issue when the distributions are Gaussian with unknown parameters from pre-specified uncertainty sets. We also establish theoretical properties of our robust procedures, and numerical examples demonstrate their good performance.

Tu3-6: Sequences 1

Tuesday, June 27, 14:40-16:20
Room: K5
Chair: Prakash Narayan (University of Maryland, USA)

Perfect polyphase sequences from cubic polynomials (14:40)

Min Kyu Song (Yonsei University, Korea); Hong-Yeop Song (Yonsei University, Korea)

In this paper, we propose a new construction of perfect p^k-ary sequences of period p^k, where p is an odd prime and $k \geq 2$ is a positive integer, based on cubic polynomials over the integers modulo p^k. We show that, for some appropriate parameters, it generates perfect polyphase sequences which are not the generalized chirp-like sequences constructed by Popovic in 1992.

Bayesian definition of random sequences with respect to conditional probabilities (15:00)

Hayato Takahashi (Random Data Laboratory, Japan)

We review the recent progress on the definition of randomness with respect to conditional probabilities and a generalization of van Lambalgen theorem (Takahashi 2006, 2008, 2009, 2011). In addition we generalize Kjos Hanssen theorem (2010) when the consistency of the posterior distributions holds. Finally we propose a definition of random sequences with respect to conditional probabilities as the section of Martin-Löf random set at the random parameters and argue the validity of the definition from the Bayesian statistical point of view.

On the Correlation between Boolean Functions of Sequences of Random Variables (15:20)

Farhad Shirani (University of Michigan, USA); Sandeep Pradhan (University Michigan, USA)

In this paper, we establish a new inequality tying together the effective length and the maximum correlation between the outputs of an arbitrary pair of Boolean functions which operate on two sequences of correlated random variables. We derive a new upper-bound on the correlation between the outputs of these functions. The upper-bound is useful in various disciplines which deal with common-information. We build upon Witsenhausen's bound on maximum-correlation. The previous upper-bound did not take the effective length of the Boolean functions into account. One possible application of the new bound is to characterize the communication-cooperation tradeoff in multi-terminal communications. In this problem, there are lower-bounds on the effective length of the Boolean functions due to the rate-distortion constraints in the problem, as well as lower bounds on the output correlation at different nodes due to the multi-terminal nature of the problem.

The Hybrid k-Deck Problem: Reconstructing Sequences from Short and Long Traces (15:40)

Ryan Gabrys (UIUC, USA); Olgica Milenkovic (UIUC, USA)

We introduce a new variant of the k-deck problem, which in its traditional formulation asks for determining the smallest k that allows one to reconstruct any binary sequence of length n from the multiset of its k-length subsequences. In our version of the problem, termed the hybrid k-deck problem, one is given a certain number of special subsequences of the sequence of length n - t, t > 0, and the question of interest is to determine the smallest value of k such that the k-deck, along with the subsequences, allows for reconstructing the original sequence in an error-free manner. We first consider the case that one is given a single subsequence of the sequence of length n - t, obtained by deleting zeros only, and seek the value of k that allows for hybrid reconstruction. We prove that in this case, $k \in [\log t + 2, \min\{t+1, O(\sqrt{n \cdot (1+\log t)})\}]$. We then proceed to extend the single-subsequence setup to the case where one is given M subsequences of length n-t obtained by deleting zeroes only. In this case, we first aggregate the asymmetric traces, and then invoke the single-trace results. The analysis and problem at hand are motivated by nanopore sequencing problems for

DNA-based data storage.

Tu3-7: Communications 2

Tuesday, June 27, 14:40-16:20
Room: K6
Chair: Tobias Koch (Universidad Carlos III de Madrid, Spain)

Reliability of Universal Decoding Based on Vector–Quantized Codewords (14:40)

Neri Merhav (Technion, Israel)

Motivated by applications of biometric identification and content identification systems, we consider the problem of random coding for channels, where each codeword undergoes vector quantization, and where the decoder bases its decision only on the compressed codewords and the channel output, which is in turn, the channel's response to the transmission of an original codeword, before compression. For memoryless sources and memoryless channels with finite alphabets, we propose a new universal decoder and analyze its error exponent, which improves on an earlier result by Dasarathy and Draper (2011), who used the classic maximum mutual information (MMI) universal decoder. We show that our universal decoder provides the same error exponent as that of the optimal, maximum likelihood (ML) decoder, at least as long as all single-letter transition probabilities of the channel are positive.

Sample Complexity of the Boolean Multireference Alignment Problem (15:00)

Joao Pereira *(Princeton University, USA); Amit Singer (Princeton University, USA); Emmanuel Abbe (Princeton University, USA)*

The Boolean multireference alignment problem consists in recovering a Boolean signal from multiple shifted and noisy observations. In this paper we obtain an expression for the error exponent of the maximum A posteriori decoder. This expression is used to characterize the number of measurements needed for signal recovery in the low SNR regime, in terms of higher order autocorrelations of the signal. The characterization is explicit for various signal dimensions, such as prime and even dimensions.

On the optimality of treating interference as noise in the 2 x M LD X-channel (15:20)

Soheil Gherekhloo (RUB, Germany); Yasemin Karacora (Ruhr Universität Bochum, USA); Aydin Sezgin (RUB, Germany)

The optimality of the simple scheme of treating interference as noise (TIN) is studied in this paper for the 2 × M linear deterministic (LD) X-channel. A new capacity upper bound is derived. In the considered scheme (denoted as 2-IC-TIN), the setup is reduced to a 2-user interference channel while the receivers employ TIN. It is shown that as long as 2-IC-TIN is optimal in a M × 2 X-channel, it is also capacity-optimal in the 2 × M X-channel which is generated by changing the role of transmitters and receivers. The result of this paper expands the capacity optimal regime of TIN for the 2 × M LD X-channel compared to the state of the art.

Interaction Information for Causal Inference: The Case of Directed Triangle (15:40)

AmirEmad Ghassami (University of Illinois at Urbana-Champaign, USA); Negar Kiyavash (University of Illinois at Urbana-Champaign, USA)

Interaction information is one of the multivariate generalizations of mutual information, which expresses the amount of information shared among a set of variables, beyond the information shared in any proper subset of those variables. Unlike (conditional) mutual information, which is always non-negative, interaction information can be negative. We utilize this property to find the direction of causal influences among variables in a triangle topology under some mild assumptions.

Completely blind sensing of multi-band signals (16:00)

Taehyung Lim (UC San Diego, USA); Massimo Franceschetti (University of California at San Diego, USA)

A solution for the completely blind sensing problem of determining the minimum number of measurements sufficient to recover multi-band signals without any spectral information beside an upper bound on the measure of the whole support set in the frequency domain is presented. A scaling law for the number of measurements sufficient for reconstruction is provided, as well as a tight converse bound. Results show that a factor of two in the measurement rate is the price pay for blindness, compared to reconstruction with full spectral knowledge. The minimum number of measurements is also related to the fractal (Minkowski-Bouligand) dimension of a discrete approximating set, defined in terms of the Kolmogorov ϵ-entropy. A comparison with analogous results in compressed sensing is illustrated, where the relevant dimensionality notion in a stochastic setting is the information (Rényi) dimension, defined in terms of the Shannon entropy.

Tu3-8: Information Theory and Statistics 1

Tuesday, June 27, 14:40-16:20
Room: K7+8
Chair: Pierre Moulin (University of Illinois at Urbana-Champaign, USA)

An Information-Theoretic Approach to Universal Feature Selection in High-Dimensional Inference (14:40)

Shao-Lun Huang (Tsinghua-Berkeley Shenzhen Institute, P.R. China); Anuran Makur (Massachusetts Institute of Technology, USA); Lizhong Zheng (Massachusetts Institute of Technology, USA); Gregory Wornell (MIT, USA)

We develop an information theoretic framework for addressing feature selection in applications where the inference task is not specified in advance and the data is from a large alphabet. We introduce a natural notion of universality for such problems, and show that locally optimal solutions are straightforward to obtain, admit natural interpretations via information geometry, have computationally efficient implementations, and represent a practically useful learning methodology. Our development also reveals the key role of Hirschfeld-Gebelein-Renyi maximal correlation and the alternating conditional expectations (ACE) algorithm in such problems.

Identifying Nonlinear 1-Step Causal Influences in Presence of Latent Variables (15:00)

Saber Salehkaleybar (University of Illinois at Urbana-Champaign, USA); Jalal Etesami (University of Illinois at Urbana-Champaign, USA); Negar Kiyavash (University of Illinois at Urbana-Champaign, USA)

We propose an approach for learning the causal structure in stochastic dynamical systems with a 1-step functional dependency in the presence of latent variables. We propose an information-theoretic approach that allows us to recover the causal relations among the observed variables as long as the latent variables evolve without exogenous noise. We further propose an efficient learning method based on linear regression for the special sub-case when the dynamics are restricted to be linear. We validate the performance of our approach via numerical simulations.

Closed-Form Moments of Finite-Dimension Non-central Wishart Matrices via Concentration of Spectral Measure (15:20)

***Xinmin Li** (University of Science and Technology of China, P.R. China); Ling Qiu (University of Science and Technology of China, P.R. China)*

In this paper, we derive a closed-form expression for the moments of finite-dimension non-central Wishart matrices. Such question has become an extensively researched topic in wireless communication and signal processing. The capacity analysis of massive MIMO system is established in the finite dimension regime via the concentration of spectral measure of random matrix. Two kinds of the significant probability measures are used to characterize the spectral distributions of random matrix. The closed-form expressions of capacity can provide a valuable insight instead of Mente-Carlo simulation. In addition, the exact convergence probabilities in these two measures are obtained

Information-geometrical characterization of statistical models which are statistically equivalent to probability simplexes (15:40)

Hiroshi Nagaoka (University of Electro-Communications, Japan)

The probability simplex is the set of all probability distributions on a finite set and is the most fundamental object in the finite probability theory. In this paper we give a characterization of statistical models on finite sets which are statistically equivalent to probability simplexes in terms of $\check{e}alpha$-families including exponential families and mixture families. The subject has a close relation to some fundamental aspects of information geometry such as $\check{e}alpha$-connections and autoparallelity.

Density Functional Estimators with k-Nearest Neighbor Bandwidths (16:00)

Weihao Gao (University Of Illinois at Urbana-Champaign, USA); Sewoong Oh (University of Illinois at Urbana-Champaign, USA); Pramod Viswanath (University of Illinois, Urbana-Champaign, USA)

Estimating expected polynomials of density functions from samples is a basic problem with numerous applications in statistics and information theory. Although kernel density estimators are widely used in practice for such functional estimation problems, practitioners are left on their own to choose an appropriate bandwidth for each application in hand. Further, kernel density estimators suffer from boundary biases, which are prevalent in real world data with lower dimensional structures. We propose using the fixed-k nearest neighbor distances for the bandwidth, which adaptively adjusts to local geometry. Further, we propose a novel estimator based on local likelihood density estimators, that mitigates the boundary biases. Although such a choice

of fixed-k nearest neighbor distances to bandwidths results in inconsistent estimators, we provide a simple debiasing scheme that precomputes the asymptotic bias and divides off this term. With this novel correction, we show consistency of this debiased estimator. We provide numerical experiments suggesting that it improves upon competing state-of-the-art methods.

Tu3-9: Machine Learning 1

Tuesday, June 27, 14:40-16:20
Room: K9
Chair: Toshiyuki Tanaka (Kyoto University, Japan)

Energy decay and conservation in deep convolutional neural networks (14:40)

Philipp Grohs (University of Vienna, Austria); Thomas Wiatowski (ETH Zurich, Switzerland); Helmut Bölcskei (ETH Zurich, Switzerland)

Many practical machine learning tasks employ very deep convolutional neural networks. Such large depths pose formidable computational challenges in training and operating the network. It is therefore important to understand how many layers are actually needed to have most of the input signal's features be contained in the feature vector generated by the network. This question can be formalized by asking how quickly the energy contained in the feature maps decays across layers. In addition, it is desirable that none of the input signal's features be "lost" in the feature extraction network or, more formally, we want energy conservation in the sense of the energy contained in the feature vector being proportional to that of the corresponding input signal. This paper establishes conditions for energy conservation for a wide class of deep convolutional neural networks and characterizes corresponding feature map energy decay rates. Specifically, we consider general scattering networks, and find that under mild analyticity and high-pass conditions on the filters (which encompass, inter alia, various constructions of Weyl-Heisenberg filters, wavelets, ridgelets, (α)-curvelets, and shearlets) the feature map energy decays at least polynomially. For broad families of wavelets and Weyl-Heisenberg filters, the guaranteed decay rate is shown to be exponential. Our results yield handy estimates of the number of layers needed to have at least $((1-\varepsilon)\cdot 100)\%$ of the input signal energy be contained in the feature vector.

Neural Offset Min-Sum Decoding (15:00)

Loren Lugosch *(McGill University, Canada); Warren Gross (McGill University, Canada)*

Recently, it was shown that if multiplicative weights are assigned to the edges of a Tanner graph used in belief propagation decoding, it is possible to use deep learning techniques to find values for the weights which improve the error-correction performance of the decoder. Unfortunately, this approach requires many multiplications, which are generally expensive operations. In this paper, we suggest a more hardware-friendly approach in which offset min-sum decoding is augmented with learnable offset parameters. Our method uses no multiplications and has a parameter count less than half that of the multiplicative algorithm. This both speeds up training and provides a feasible path to hardware architectures. After describing our method, we compare the performance of the two neural decoding algorithms and show that our method achieves error-correction performance within 0.1 dB of the multiplicative approach and as much as 1 dB better than traditional belief propagation for the codes under consideration.

Learning-Based Epsilon Most Stringent Test for Gaussian Samples Classification (15:20)

Lionel Fillatre *(Université Côte d'Azur, France); Igor Nikiforov (Université de Technologie de Troyes, UTT/ICD/LM2S & UMR 6281, CNRS, France)*

This paper studies the problem of classifying some Gaussian samples into one of two parametric probabilistic models, also called sources, when the parameter and the a priori probability of each source are unknown. Each source is governed by an univariate normal distribution whose mean is unknown. A training sequence is available for each source in order to compensate the lack of prior information. An almost optimal most stringent test is proposed to solve this classification problem subject to a constrained false alarm probability. This learning-based test minimizes its maximum shortcoming with respect to the most powerful test which knows exactly the parameters of the sources. It also guarantees a prescribed false alarm probability whatever the size of the training sequences. The threshold, the probability of false alarm and the probability of correct detection are calculated analytically.

Quickest Search and Learning over Multiple Sequences (15:40)

Javad Heydari (Rensselaer Polytechnic Institute, USA); Ali Tajer (Rensselaer Polytechnic Institute, USA)

Consider a set of random sequences, each consisting of independent and identically distributed random variables. Each sequence is generated according to one of the two possible distributions F_0 or F_1 with prior probabilities $(1-\epsilon)$ and ϵ, respectively. The objective is to design a sequential decision-making procedure that identifies a sequence generated according to F_1 with the fewest number of measurements. Earlier analyses of this search problem have demonstrated that the optimal design of the sequential rules strongly hinge on the known value of ϵ. Such information, however, might not be available in certain applications, espe-

cially in anomaly detection where the anomalous sequences occur with unpredicted patterns. Motivated by this premise, this paper designs a sequential inference mechanism that forms two coupled decisions for identifying a sequence of interest, and also learning the value of ϵ. The paper devises three strategies that place different levels of emphasis on each of these inference goals.

Minimax Lower Bounds for Ridge Combinations Including Neural Nets (16:00)

Jason Klusowski (Yale University, USA); Andrew Barron (Yale University, USA)

Estimation of functions of d variables is considered using ridge combinations of the form $\sum_{k=1}^{m} c_{1,k}\phi(\sum_{j=1}^{d} c_{0,j,k}x_j - b_k)$ where the activation function ϕ is a function with bounded value and derivative. These include single-hidden layer neural networks, polynomials, and sinusoidal models. From a sample of size n of possibly noisy values at random sites $X \in B = [-1,1]^d$, the minimax mean square error is examined for functions in the closure of the ℓ_1 hull of ridge functions with activation ϕ. It is shown to be of order d/n to a fractional power (when d is of smaller order than n), and to be of order $(\log d)/n$ to a fractional power (when d is of larger order than n). Dependence on constraints v_0 and v_1 on the ℓ_1 norms of inner parameter c_0 and outer parameter c_1, respectively, is also examined. Also, lower and upper bounds on the fractional power are given. The heart of the analysis is development of information-theoretic packing numbers for these classes of functions.

Tu4-1: Coding Theory 2

Tuesday, June 27, 16:40-18:20
Room: Europa
Chair: Emina Soljanin (Rutgers University, USA)

Pseudo-Wigner Matrices from Dual BCH Codes (16:40)

Ilya Soloveychik (Harvard University, USA); Yu Xiang (Harvard University, USA); Vahid Tarokh (Harvard University, USA)

We consider the problem of generating pseudo-random matrices based on the similarity of their spectra to Wigner's semicircular law. We introduce r-independent pseudo-Wigner ensembles and prove closeness of their spectra to the semicircular density in Kolmogorov distance. We give an explicit construction of a family of N by N pseudo-Wigner ensembles using dual BCH codes and show that the Kolmogorov complexity of the constructed matrices is of the order of log(N). Finally, we provide numerical simulations verifying our theoretical results.

On codes achieving zero error capacities in limited magnitude error channels (17:00)

Bella Bose (Oregon State University, USA); Noha Elarief (Hewlett Packard, Corvallis, OR., USA); Luca Tallini (Università di Teramo, Italy)

Shannon in his 1956 seminal paper introduced the concept of the zero error capacity, C_0, of a noisy channel. This is defined as the least upper bound of rates at which it is possible to transmit information with zero probability of error. At present not many codes are known to achieve the zero error capacity. In this paper, some codes which achieve zero error capacities in limited magnitude error channels are described. The code lengths of these zero error capacity achieving codes can be of any finite length $n = 1, 2, \ldots$, in contrast to the long lengths required for the known regular capacity achieving codes such as turbo codes, LDPC codes and polar codes. Both non-systematic and systematic codes are described.

On the Capacities of Balanced Codes with Run-Length Constraints (17:20)

Akiko Manada (The University of Electro-Communications, Japan); Hiroyoshi Morita (The University of Electro-Communications, Japan)

A balanced code is a set of words over $\{a, b\}$ such that the number of a's and the number of b's in a word are equal, and many applications using balanced codes have been proposed so far. Recently, not only the original balanced code, but also balanced codes with some other constraints have been studied mainly for an application of data storage media. However, contrary to other typical sets of words satisfying some constraints, the capacities of such balanced codes have not been well studied up to this moment. In this paper, we focus on balanced codes satisfying various run-length constraints and analyze their capacities. More precisely, we exhibit lower bounds on the capacities, or present the explicit capacities for certain cases.

Geometric Orthogonal Codes Better than Optical Orthogonal Codes (17:40)

Yeow Meng Chee (Nanyang Technological University, Singapore); Han Mao Kiah (Nanyang Technological University, Singapore); San Ling (NTU, Singapore); Hengjia Wei (Nanyang Technological University, Singapore)

The class of geometric orthogonal codes (GOCs) were introduced by Doty and Winslow (2016) for more robust macrobonding in DNA origami. They observed that GOCs are closely related to optical orthogonal codes (OOCs). It is possible for GOCs to have size greater than OOCs of corresponding parameters due to slightly more relaxed constraints on correlations. However, the existence of GOCs exceeding the size of optimal OOCs of corresponding parameters have

never been demonstrated. This paper gives the first infinite family of GOCs of size greater than optimal OOCs.

The Augustin Center and The Sphere Packing Bound For Memoryless Channels (18:00)

Baris Nakiboglu *(None, Turkey)*

For any channel with a convex constraint set and finite Augustin capacity, the existence of a unique Augustin center and the associated Erven-Harremoes bound are established. Augustin-Legendre capacity, center, and radius are introduced and proved to be equal to the corresponding Renyi-Gallager entities. Sphere packing bounds with polynomial prefactors are derived for codes on two families of channels: (possibly non-stationary) memoryless channels with multiple additive cost constraints and stationary memoryless channels with convex constraints on the empirical distribution of the input codewords.

Tu4-2: Coding for Distributed Storage 1

Tuesday, June 27, 16:40-18:20
Room: Brussels
Chair: Vitaly Skachek (University of Tartu, Estonia)

Secrecy Capacity of Minimum Storage Regenerating Codes (16:40)

Ankit Singh Rawat (Massachusetts Institute of Technology, USA)

This paper revisits the problem of designing secure minimum storage regenerating (MSR) codes for distributed storage systems (DSS). A secure MSR code ensures that a DSS does not reveal the stored information to a passive eavesdropper. The eavesdropper is assumed to have access to the content stored on ℓ_1 number of storage nodes in the system and the data downloaded during the bandwidth efficient repair of an additional ℓ_2 number of storage nodes. This paper combines the Gabidulin codes based precoding [Rawat et al.] and a new construction of MSR codes (without security requirements) by Ye and Barg in order to obtain secure MSR codes. Such optimal secure MSR codes were previously known only in the setting where the eavesdropper was allowed to observe the repair of ℓ_2 nodes among a specific subset of k nodes [Rawat et al., Goparaju et al.]. The secure coding scheme presented in this paper allows the eavesdropper to observe repair of any ℓ_2 out of n nodes in the system and characterizes the secrecy capacity of linear repairable MSR codes.

Cooperative Data Exchange based on MDS codes (17:00)

Su Li (EPFL, Switzerland); Michael Gastpar (EPFL & University of California, Berkeley, Switzerland)

The coded cooperative data exchange problem is studied for the fully connected network. In this problem, each node initially only possesses a subset of the K packets making up the file. Nodes make broadcast transmissions that are received by all other nodes. The goal is for each node to recover the full file. In this paper, we present a polynomial-time deterministic algorithm to compute the optimal (i.e., minimal) number of required broadcast transmissions and to determine the precise transmissions to be made by the nodes. A particular feature of our approach is that each of the K-d transmissions is a linear combination of exactly d+1 packets, and we show how to optimally choose the value of d. We also show how the coefficients of these linear combinations can be chosen by leveraging a connection to Maximum Distance Separable (MDS) codes.

Asymptotically Optimal Regenerating Codes Over Any Field (17:20)

Netanel Raviv (Technion & Tel-Aviv University, Israel)

The study of regenerating codes has advanced tremendously in recent years. However, most known constructions require large field size, and hence may be hard to implement in practice. In this paper, by using notions from the theory of extension fields and matrix analysis, two explicit constructions of regenerating codes are obtained. These codes approach the cut-set bound as the reconstruction degree increases, and may be realized over any given field if the file size is large enough. Since distributed storage systems are the main purpose of regenerating codes, this file size restriction is trivially satisfied in most conceivable scenarios. The first construction attains the cut-set bound at the MBR point asymptotically for all parameters, whereas the second one attains the cut-set bound at the MSR point asymptotically for low-rate parameters.

Private Information Retrieval in Distributed Storage Systems Using an Arbitrary Linear Code (17:40)

Siddhartha Kumar (University of Bergen & Simula Research Laboratory, Norway); Eirik Rosnes (University of Bergen, Norway); Alexandre Graell i Amat (Chalmers University of Technology, Sweden)

We propose an information-theoretic private information retrieval (PIR) scheme for distributed storage systems where data is stored using a linear systematic code of rate R > 1/2. The proposed scheme generalizes the PIR scheme for data stored using maximum distance separable codes recently proposed by Tajeddine and El Rouayheb for the scenario of a single spy

node. We further propose an algorithm to optimize the communication price of privacy (cPoP) using the structure of the underlying linear code. As an example, we apply the proposed algorithm to several distributed storage codes, showing that the cPoP can be significantly reduced by exploiting the structure of the distributed storage code.

Tu4-3: Interference Channels 2

Tuesday, June 27, 16:40-18:20
Room: K2
Chair: Changho Suh (KAIST, Korea)

Nash Region of the Linear Deterministic Interference Channel with Noisy Output Feedback (16:40)

Victor Quintero (INRIA, France); Samir Perlaza (INRIA, France); Jean-Marie Gorce (INSA-Lyon & CITI, Inria, France); H. Vincent Poor (Princeton University, USA)

In this paper, the η-Nash equilibrium (η-NE) region of the two-user linear deterministic interference channel with noisy channel-output feedback is characterized for all $\eta > 0$ arbitrarily small. The η-NE region, a subset of the capacity region, contains the set of all achievable information rate pairs that are stable in the sense of an η-NE. More specifically, given an η-NE coding scheme, there does not exist an alternative coding scheme for either transmitter-receiver pair that increases the individual rate by more than η bits per channel use. Existing results such as the η-NE region of the linear deterministic IC without feedback and with perfect output feedback are obtained as particular cases of the result presented in this paper.

Characterization of Degrees of Freedom versus Receivers Backhaul Load in K-User Interference Channel (17:00)

Borna Kananian (Sharif University of Technology & Hong Kong University of Science and Technology, Iran); Mohammad Ali Maddah-Ali (Bell Labs, Alcatel Lucent, USA); Seyed Pooya Shariatpanahi (Institute for Research in Fundamental Sciences (IPM), Iran); Babak Hossein Khalaj (Sharif University of Technology, Iran)

We consider a K-user Interference Channel where each transmitter is interested in conveying a message to its corresponding receiver. In addition, we assume a fully connected noiseless backhaul network through which receivers can collaborate and help each other recover their desired messages. In this paper, we fully characterize the trade-off between the rate in wireless link (per user) in terms of degrees of freedom (DoF) versus backhaul load (per user) for large values of K. In particular, we characterize the optimal trade-off for all values of K, where K is an even number. For odd values of K, we characterize the trade-off within a gap of 2(K-1)/K(K+1), which goes to zero as K increases. For achievability we use time-sharing between two corner points: (i) using interference alignment for the case where backhaul load is zero, and (ii) collecting a quantized version of all the received signals at one of the receivers to jointly decode the messages, for the case where DoF of one per user is desired. For the converse, we develop a new outer-bound based on the results from two-user multiple antenna interference channel with limited backhaul cooperation. Recently, it was shown that for the case of three-user interference channel, the optimal trade-off is achieved by some sort of alignment in the backhaul messaging, known as Cooperation Alignment. Our result shows that unlike the gain of interference alignment, the gain of cooperation alignment does not scale with the number of users K.

Discrete Modulation for Interference Mitigation (17:20)

Mirza Uzair Baig (University of Hawaii, USA); Anders Høst-Madsen (University of Hawaii, USA); Aria Nosratinia (University of Texas, Dallas, USA)

This paper analyzes the performance of discrete input distributions (coded modulation) in certain 3 user interference channels. This approach is motivated in part by the necessity of using coded modulation in practical systems, and in part by the potential of discrete distributions for interference alignment as well as the demonstrated importance of discrete input distributions for transmission over the 2×2 interference channel when treating interference as noise. The contribution of this work includes the establishment of achievable rates subject to discrete (PAM) modulations. In the process, new bounds involving the minimum distance of the sum of discrete modulations have been developed that are useful for facilitating further work in this area.

Communicating Correlated Sources Over an Interference Channel (17:40)

Arun Padakandla (Purdue University, USA)

A new coding technique, based on *fixed block-length* codes, is proposed for the problem of communicating a pair of correlated sources over a $2-$user interference channel. Its performance is analyzed to derive a new set of sufficient conditions. The latter is proven to be strictly less binding than the current known best, which is due to Liu and Chen [Dec, 2011]. Our findings are inspired by Dueck's example [Mar, 1981].

Topological Interference Management: Linear Cooperation is not useful for Wyner's Networks (18:00)

Aly El Gamal (Purdue University, USA)

In this work, we study the value of cooperative trans-

mission in wireless networks if no channel state information is available at the transmitters (no CSIT). Our focus is on large locally connected networks, where each transmitter is connected to the receiver that has the same index as well as L succeeding receivers. The cases of L=1 and L=2 represent Wyner's asymmetric and symmetric network models, respectively. The considered rate criterion is the per user Degrees of Freedom (puDoF) as the number of transmitter-receiver pairs goes to infinity. For the case when L=1, it was shown in previous work that linear cooperation schemes do not increases the puDoF value, and that the optimal scheme relies on assigning each message to a single transmitter and using orthogonal access (TDMA). Here, we extend this conclusion to the case where L=2, by proving optimality of TDMA in this case as well. We conclude by discussing whether increasing the value of L can create a value for linear cooperation schemes from a DoF perspective.

Tu4-4: Entropy 2

Tuesday, June 27, 16:40-18:20
Room: K3
Chair: Stefan Moser (ETH Zurich, Switzerland)

Urns and entropies revisited (16:40)

Františ ek Matúš *(Academy of Sciences of the Czech Republic & Institute of Information Theory and Automation, Czech Republic)*

An urn containing colored balls is sampled sequentially without replacement. New lower and upper bounds on the conditional and unconditional mutual information, and multiinformation are presented. They estimate dependence between drawings in terms of the colored ball configuration. Asymptotics are worked out when the number of balls increases and the proportion of the balls of each color stabilizes. Inequalities by Stam and by Diaconis and Freedman are compared and improved. Distances between the sampling with and without replacement, and between the multinomial and multivariate hypergeometric distributions are discussed.

Metric and topological entropy bounds on state estimation for stochastic non-linear systems (17:00)

Christoph Kawan (University of Passau, Germany); Serdar Yüksel (Queen's University, Canada)

This paper studies state estimation over noisy channels for stochastic non-linear systems. We consider three estimation objectives, a strong and a weak form of almost sure stability of the estimation error as well as quadratic stability in expectation. For all three objectives, we derive lower bounds on the smallest channel capacity C_0 above which the objective can be achieved with an arbitrarily small error. Lower bounds are obtained via a dynamical systems (through a novel construction of a dynamical system), an information-theoretic and a random dynamical systems approach. The first two approaches show that for a large class of systems, such as additive noise systems, $C_0 = \infty$, i.e., the estimation objectives cannot be achieved via channels of finite capacity. The random dynamical systems approach is shown to be operationally non-adequate for the problem, since it yields finite lower bounds C_0 under mild assumptions. Finally, we prove that a memoryless noisy channel in general constitutes no obstruction to asymptotic almost sure state estimation with arbitrarily small errors, when there is no noise in the system.

Playing Games with Bounded Entropy (17:20)

Mehrdad Valizadeh (Sharif University of Technology, Iran); Amin Gohari (Sharif University of Technology, Iran)

We study a two-player zero-sum game in which one of the players is restricted to mixed strategies with limited randomness. More precisely, we consider the maximum payoff that the maximizer (Alice) can secure with limited randomness h. This problem finds an operational interpretation in the context of repeated games with non-ideal sources of randomness. The computational aspects of this problem has not received much attention in the game theory literature. We begin by observing the equivalence of this problem with entropy minimization problems in other scientific contexts. Next, we provide two explicit lower bounds on the entropy-payoff tradeoff curve. To do this, we provide and utilize new results for the set of distribution that guarantee a certain payoff for Alice (mixed strategies corresponding to a security level for Alice). In particular, we study how this set of distribution shrinks as we increase the security level. While the use of total variation distance is common in game theory, our derivation indicates the suitability of utilizing the Renyi-divergence of order two.

Entropic Causality and Greedy Minimum Entropy Coupling (17:40)

Murat Kocaoglu (The University of Texas at Austin, USA); Alexandros Dimakis (University of Texas at Austin, USA); Sriram Vishwanath (University of Texas Austin, USA); Babak Hassibi (California Institute of Technology, USA)

We study the problem of identifying the causal relationship between two discrete random variables from observational data. We recently proposed a novel framework called entropic causality that works in a very general functional model but makes the assumption that the unobserved exogenous variable has small entropy in the true causal direction. This framework requires the solution of a minimum entropy coupling problem: Given marginal distributions of m discrete

random variables, each on n states, find the joint distribution with minimum entropy, that respects the given marginals. This corresponds to minimizing a concave function of n^m variables over a convex polytope defined by nm linear constraints, called a transportation polytope. Unfortunately, it was recently shown that this minimum entropy coupling problem is NP-hard, even for 2 variables with n states. Even representing points (joint distributions) over this space can require exponential complexity (in n, m) if done naively. In our recent work we introduced an efficient greedy algorithm to find an approximate solution for this problem. In this paper we analyze this algorithm and establish two results: that our algorithm always finds a local minimum and also is within an additive approximation error from the unknown global optimum.

On Structural Entropy of Uniform Random Intersection Graphs (18:00)

Marcin Kardas (Wrocław University of Technology, Poland); Zbigniew Golebiewski (Wroclaw University of Technology, Poland); ***Jakub Lemiesz*** *(Wroclaw University of Science and Technology, Poland); Krzysztof Majcher (TU Wroclaw, Poland)*

Recently, the need for efficient representations of data conveyed by graphical structures has emerged in many different contexts. While compressing such data one must consider two types of information. The first type is the information carried by the labels embedded in the structure. The second type is the information conveyed by the structure itself. In this extended abstract we address the latter type, namely we study the information carried by the structure of Uniform Random Intersection Graphs (URIGs). Random Intersection Graphs emerge in many scenarios, e.g., they correspond to the topology of many social networks and secure wireless networks, and they are induced in the clusterization process. We analyze algebraic properties of an automorphism group of the underlying structure of URIGs and derive a precise asymptotic formula for their structural entropy for various values of model parameters.

Tu4-5: Bounds 2

Tuesday, June 27, 16:40-18:20
Room: K4
Chair: Viveck Cadambe (Pennsylvania State University, USA)

Dependence Measures Bounding the Exploration Bias for General Measurements (16:40)

Jiantao Jiao (Stanford University, USA); Yanjun Han (Stanford University, USA); Tsachy Weissman (Stanford University, USA)

We propose a framework to analyze and quantify the bias in adaptive data analysis. It generalizes that proposed by Russo and Zou'15, applying to all measurements whose moment generating function exists, and to all measurements with a finite p-norm. We introduce a new class of dependence measures which retain key properties of mutual information while more effectively quantifying the exploration bias for heavy tailed distributions. We provide examples of cases where our bounds are nearly tight in situations where the original framework of Russo and Zou'15 does not apply.

Binary Subblock Energy-Constrained Codes: Bounds on Code Size and Asymptotic Rate (17:00)

Anshoo Tandon (National University of Singapore, Singapore); Han Mao Kiah (Nanyang Technological University, Singapore); Mehul Motani (National University of Singapore, Singapore)

The subblock energy-constrained codes (SECCs) have recently been shown to be suitable candidates for simultaneous energy and information transfer, where bounds on SECC capacity were presented for communication over noisy channels. In this paper, we study binary SECCs with given error correction capability, by considering codes with a certain minimum distance. Binary SECCs are a class of constrained codes where each codeword is partitioned into equal sized subblocks, and every subblock has weight exceeding a given threshold. We present several upper and lower bounds on the optimal SECC code size, and also derive the asymptotic Gilbert-Varshamov (GV) and sphere-packing bounds for SECCs. A related class of codes are the heavy weight codes (HWCs) where the weight of each codeword exceeds a given threshold. We show that for a fixed subblock length, the asymptotic rate for SECCs is strictly lower than the corresponding rate for HWCs when the relative distance of the code is small. The rate gap between HWCs and SECCs denotes the penalty due to imposition of weight constraint per subblock, relative to the codeword based weight constraint.

Sampled Graph-Signals: Iterative Recovery with an Analytic Error Bound (17:20)

Norbert Goertz *(Vienna University of Technology (TU Wien), Austria)*

Recovery of graph signals from a limited number of sampled components is investigated. An iterative graph-signal recovery algorithm is motivated and derived, including an analytic upper bound for the reconstruction error.

Multidimensional Semiconstrained Systems (17:40)

Ohad Elishco (Ben-Gurion University of the Negev, Israel); Tom Meyerovitch (Ben-Gurion University of the Negev, Israel); Moshe Schwartz (Ben-Gurion University of the Negev, Israel)

We generalize the notion of independence entropy to the study of semiconstrained systems. Using it, we obtain a new lower bound on the capacity of multidimensional semiconstrained systems. We show the new bound improves upon the best-known bound in a case study of $(0, k, p)$- RLL semiconstrained systems.

Variable-length codes for channels with memory and feedback: error-exponent lower bounds (18:00)

Achilleas Anastasopoulos (University of Michigan, USA); Jui Wu (University of Michigan, USA)

The reliability function of memoryless channels with noiseless feedback and variable-length coding has been found to be a linear function of the average rate in the classic work of Burnashev. In this work we consider unifilar channels with noiseless feedback and study specific transmission schemes, the performance of which provides lower bounds for the channel reliability function. In unifilar channels the channel state evolves in a deterministic fashion based on the previous state, input, and output, and is known to the transmitter but is unknown to the receiver. We consider a two-stage transmission scheme. In the first stage, both transmitter and receiver summarize their common information in an M-dimensional vector with elements in the state space of the unifilar channel and an M-dimensional probability mass function, with M being the number of messages. The second stage, which is entered when one of the messages is sufficiently reliable, is resolving a binary hypothesis testing problem. The analysis assumes the presence of some common randomness shared by the transmitter and receiver, and is based on the study of the log-likelihood ratio of the transmitted message posterior belief, and in particular on the study of its multi-step drift. Simulation results confirm that the bounds are tight compared to the upper bounds derived in a companion paper.

Tu4-6: Sequences 2

Tuesday, June 27, 16:40-18:20
Room: K5
Chair: Yossef Steinberg (Technion, Israel)

On Empirical Cumulant Generating Functions of Code Lengths for Individual Sequences (16:40)

Neri Merhav (Technion, Israel)

We consider the problem of lossless compression of individual sequences using finite-state (FS) machines, from the perspective of the best achievable empirical cumulant generating function (CGF) of the code length, i.e., the normalized logarithm of the empirical average of the exponentiated code length. Since the probabilistic CGF is minimized in terms of the Renyi entropy of the source, one of the motivations of this study is to derive an individual-sequence analogue of the Rényi entropy, in the same way that the FS compressibility is the individual-sequence counterpart of the Shannon entropy. We consider the CGF of the code-length both from the perspective of fixed-to-variable (F-V) length coding and the perspective of variable-to-variable (V-V) length coding, where the latter turns out to yield a better result, that coincides with the FS compressibility. We also extend our results to compression with side information, available at both the encoder and decoder. In this case, the V-V version no longer coincides with the FS compressibility, but results in a different complexity measure.

Degree-$(k+1)$ Perfect Gaussian Integer Sequences of Period p^k (17:00)

Ho-Hsuan Chang (I-Shou University, Taiwan)

This paper presents a method for constructing degree-$(k+1)$ perfect Gaussian integer sequence (PGIS) of period $N = p^k$, where p is a prime number. The study begins with the partitioning of set Z_N into $k+1$ subsets and exploration of their properties and theorems. The base sequences can be defined and the associated $k+1$ degree PGIS is constructed based on the partitioning of Z_N. The k constraint equations that govern the $k+1$ different sequence coefficients to match the criteria for a sequence to be perfect are nonlinear equations, which makes the construction of higher degree PGISs especially challenging. A new method of transforming k nonlinear constraint equations into $2k2$ linear equations with $2k2$ variables is presented. It is then easy to derive a unique solution, from which the construction of degree-$(k+1)$ PGISs becomes straightforward. Both degree-5 and degree7 PGIS examples are provided for demonstration.

Reconstruction of Sequences over Non-Identical Channels (17:20)

Michal Horovitz (Technion - Israel Institute of Technology, Israel); Eitan Yaakobi (Technion, Israel)

Motivated by the error behavior in DNA storage channels, in this work we extend the previously studied sequence reconstruction problem by Levenshtein. The reconstruction problem studies the model in which the information is read through multiple noisy channels, and the decoder, which receives all channel estimations, is required to decode the information. For the combinatorial setup, the assumption is that all the channels can cause at most some t errors. However, since the channels do not necessarily have the same behavior, we generalize this model and assume that the channels are not identical and thus may cause a different maximum number of errors. For example, we assume that there are N channels, that can cause at most t_1 or t_2 errors, where $t_1 < t_2$, and the number of channels with at most t_1 errors is at most $\lceil pN \rceil$, for some fixed $0 < p < 1$. If the information codeword belongs to a code with minimum distance d, the problem is then to find the minimum number of channels N that guarantees successful decoding in the worst case.

Classification of a Sequence Family Using Plateaued Functions (17:40)

Serdar Boztas (RMIT University, Australia); Ferruh Ozbudak (Middle East Technical University, Turkey); Eda Tekin (Karabuk University, Turkey)

The design of CDMA sequence families using quadratic functions dates back to Gold sequences from the 1960s. Since then there have been a number of different such designs with good correlation properties, some optimal and some nearoptimal, and the term ”Gold-like” is usually used to denote such sequences. In this paper we use the concept of plateaued functions in order to classify such sequence families and present some examples in this direction which depend on the characteristic p and degree n of the Galois field Fpn used to define the sequences.

Tu4-7: Security 2

Tuesday, June 27, 16:40-18:20
Room: K6
Chair: Arya Mazumdar (University of Massachusetts Amherst, USA)

Secret Key Agreement under Discussion Rate Constraints (16:40)

Chung Chan (The Chinese University of Hong Kong, Hong Kong); Manuj Mukherjee (Indian Institute of Science, India); Navin Kashyap (Indian Institute of Science, India); Qiaoqiao Zhou (The Chinese University of Hong Kong, Hong Kong)

For the multiterminal secret key agreement problem, new single-letter lower bounds are obtained regarding the public discussion rate required to achieve any given secret key rate below the capacity. The results apply to general source model without helpers or wiretapper’s side information but can be strengthened for hypergraphical sources. In particular, for the pairwise independent network, the results give rise to a complete characterization of the maximum secret key rate under a constraint on the total discussion rate.

A Game Theoretic Treatment for Pair-wise Secret-Key Generation in Many-to-One Networks (17:00)

Remi Chou (Pennsylvania State University, USA); Aylin Yener (Pennsylvania State University, USA)

We consider secret-key generation between several agents and a base station that observe independent and identically distributed (i.i.d.) realizations of correlated random variables. Each agent wishes to generate the longest possible individual key with the base station by means of public communication. All keys must be jointly kept secret from all external entities. We do not require them to be kept secret among the agents. In this many-to-one secret-key generation setting, it can be shown that the agents can take advantage of a collective protocol to increase the sum-rate of all the generated keys. However, when each agent is only interested in maximizing its own secret-key rate, agents may be unwilling to participate in a collective protocol. Furthermore, when such a collective protocol is employed, how to fairly allocate individual key rates arises as a valid issue. We study this tension between cooperation and self-interest with a game-theoretic treatment. We establish that cooperation is in the best interest of all agents and that there exists individual secret-key rate allocations that incentivize the agents to follow the protocol. Additionally, we propose an explicit and low-complexity coding scheme based on polar codes and hash functions that achieves such allocations.

Information-Theoretically Secure Key Generation and Management (17:20)

Xin-Wen Wu (Griffith University, Australia); En-hui Yang (University of Waterloo, Canada)

In this paper, we address the problems of key generation and management for enabling one-key-for-one-file secure encryption, where every file is encrypted by using an independent random key, which is highly desired in long-term protection of data stored on public clouds and other applications. A new concept dubbed information-theoretical ϵ-security is introduced to measure the security of a keystore (i.e., a set of random keys, k_i, $1 \leq i \leq \Lambda$, each having length of l bits) which are generated from a random string of L bits, called the keystore seed. An efficient keystore generation scheme is presented, and the resulting keystore $\Psi = \{k_i : 1 \leq i \leq \Lambda\}$ is shown to be information-theoretically ϵ-secure with small ϵ. Specifically, they satisfy the following properties: (1) $\Lambda \gg L$ is sufficiently large to realize one-key-for-one-file encryption for applications with a large number of files; (2) for any key index i, the key k_i is uniformly distributed over the key space $\{0,1\}^l$ and hence statistically independent of i if i is chosen randomly; (3) for any two independent $i, j, 1 \leq i, j \leq \Lambda$, the probability that $k_i = k_j$ is very small and less than $(1-\epsilon) \times 2^{-l} + \epsilon$; and (4) for any two independent key indices i and j, knowing i, j, and k_i does not reduce the amount of uncertainty about k_j significantly, i.e., the conditional Shannon entropy $H(k_j|i,j,k_i)$ is at least as large as $(1-\epsilon)H(k_j|j)$. These security properties along with easy generation of each key k_i from the keystore seed and the key index i remove most challenges in distributing and managing a large number of random keys.

Secret-Key Agreement with Public Discussion over Multi-Antenna Transmitters with Amplitude Constraints (17:40)

Zouheir Rezki *(University of Idaho, USA); Mohamed-Slim Alouini (King Abdullah University of Science and Technology (KAUST), Saudi Arabia)*

We consider secret-key agreement with public discussion over a multiple-input single output (MISO) Gaussian channel with an amplitude constraint. We prove that the capacity is achieved by a discrete input, i.e., an input whose support is sparse. The proof follows from the concavity of the conditional mutual information in terms of the input distribution and hence the KKT condition provides a necessary and sufficient condition for optimality. Then, a contradiction argument that rules out the non-sparsity of any optimal input's support is utilized. The latter approach is essential to apply the identity theorem in multidimensional setting as $\mathbb{R}^n$ is not an open subset $\mathbb{C}^n$.

Robust and Secure Identification (18:00)

Holger Boche (Technical University Munich, Germany); Christian Deppe (University of Bielefeld, Germany)

We determine the identification capacity of compound channels with and without wiretapper. It turned out, that the secure capacity formula fulfill a dichotomy theorem. It is positive if its secure capacity is positive and equals the transmission capacity of the channel. Otherwise the capacity is zero. We analyze the (dis-)continuity and (super-)additivity of the capacities, which we determined. Alon gave in a conjecture about maximal violation for the additivity for capacity functions. We show that this maximal violation holds for the secure identification capacity. This is the first example of a capacity function, which has this behavior.

Tu4-8: Quantum IT 2

Tuesday, June 27, 16:40-18:20
Room: K7+8
Chair: Joseph Renes (ETH Zurich, Switzerland)

Moderate deviation analysis for classical communication over quantum channels (16:40)

Christopher Chubb *(The University of Sydney, Australia); Vincent Tan (National University of Singapore, Singapore); Marco Tomamichel (University of Technology Sydney, Australia)*

We analyse families of codes for classical data transmission over quantum channels that have both a vanishing probability of error and a code rate approaching capacity as the code length increases. To characterise the fundamental tradeoff between decoding error, code rate and code length for such codes we introduce a quantum generalisation of the moderate deviation analysis proposed by Altug and Wagner as well as Polyanskiy and Verdu. We derive such a tradeoff for classical-quantum (as well as image-additive) channels in terms of the channel capacity and the channel dispersion, giving further evidence that the latter quantity characterises the necessary backoff from capacity when transmitting finite blocks of classical data. To derive these results we also study asymmetric binary quantum hypothesis testing in the moderate deviations regime. Due to the central importance of the latter task, we expect that our techniques will find further applications in the analysis of other quantum information processing tasks.

Quantum Information on Spectral Sets (17:00)

Peter Harremoës (Niels Brock, Copenhagen Business College, Denmark)

For convex optimization problems Bregman diver-

gences appear as regret functions. Such regret functions can be defined on any convex set, but if a sufficiency condition is added the regret function must be proportional to information divergence and the convex set must be spectral. Spectral set are sets where different orthogonal decompositions of a state into pure states have unique mixing coefficients. Only on such spectral sets it is possible to define well behaved information theoretic quantities like entropy and divergence. It is only possible to perform measurements in a reversible way if the state space is spectral. The most important spectral sets can be represented as positive elements of Jordan algebras with trace 1. This means that Jordan algebras provide a natural framework for studying quantum information.

Kolmogorov Amplification from Bell Correlation (17:20)

Ämin Baumeler (Università della Svizzera Italiana, Switzerland); Charles Alexandre Bédard (Université de Montréal, Canada); Gilles Brassard (Université de Montréal & Canadian Institute for Advanced Research, Canada); Stefan Wolf (USI Lugano, Switzerland)

It was first observed by John Bell that quantum theory predicts correlations between measurement outcomes that lie beyond the explanatory power of local hidden variable theories. These correlations have traditionally been studied extensively in the probabilistic framework. A drawback of this perspective is that one is then forced to use in a single argument the outcomes of mutually-exclusive measurements. One of us has initiated an alternative approach, invoking only data at hand, in order to circumvent this issue. In this factual view, which is based on Kolmogorov complexity, we introduce mechanisms such as complexity amplification. We establish that this functionality is realizable, just as its probabilistic counterpart, hereby underlining that Bell correlations are a precious information-processing resource.

Degradable states and one-way entanglement distillation (17:40)

Felix Leditzky (University of Colorado Boulder, USA); Nilanjana Datta (Cambridge, United Kingdom (Great Britain)); Graeme Smith (University of Colorado Boulder, USA)

We derive an upper bound on the one-way distillable entanglement of bipartite quantum states. To this end, we revisit the notion of degradable, conjugate degradable, and antidegradable bipartite quantum states [Smith et al., IEEE Trans. on Inf. Th. 54.9 (2008), pp. 4208-4217]. We prove that for degradable and conjugate degradable states the one-way distillable entanglement is equal to the coherent information, and thus given by a single-letter formula. Furthermore, it is well-known that the one-way distillable entanglement of antidegradable states is zero. We use these results to derive an upper bound for arbitrary bipartite quantum states, which is based on a convex decomposition of a bipartite state into degradable and antidegradable states. This upper bound is always at least as good an upper bound as the entanglement of formation. Applying our bound to the qubit depolarizing channel, we obtain an upper bound on its quantum capacity that is strictly better than previously known bounds in the high noise regime. We also transfer the concept of approximate degradability [Sutter et al., arXiv:1412.0980 [quant-ph]] to quantum states and show that this yields another easily computable upper bound on the one-way distillable entanglement. Moreover, both methods of obtaining upper bounds on the one-way distillable entanglement can be combined into a generalized one.

Tu4-9: Compression 1

Tuesday, June 27, 16:40-18:20
Room: K9
Chair: Faramarz Fekri (Georgia Institute of Technology, USA)

Recovery of Vertex Orderings in Dynamic Graphs (16:40)

***Abram Magner** (UIUC, USA); Ananth Grama (Purdue University, USA); Jithin Sreedharan (Purdue University, USA); Wojciech Szpankowski (Purdue University, USA)*

Many networks in the real world are dynamic in nature: nodes enter, exit, and make and break connections with one another as time passes. Several random graph models of these networks are such that nodes have well-defined arrival times. It is natural to ask if, for a given random graph model, we can recover the arrival order of nodes, given information about the structure of the graph. In this work, we give a rigorous formulation of the problem in a statistical learning framework and tie its feasibility, for a broad class of models, to several sets of permutations associated with the symmetries of the random graph model and graphs generated by it. Moreover, we show how the same quantities are fundamental to the study of the information content of graph structures. We then apply our general results to the special cases of the Erdős-Rényi and preferential attachment models to derive strong inapproximability results.

Variable-Length Lossy Compression Allowing Positive Overflow and Excess Distortion Probabilities (17:00)

Shota Saito (Waseda University, Japan); Hideki Yagi (University of Electro-Communications, Japan); Toshiyasu Matsushima (Waseda University, Japan)

This paper investigates the problem of variable-length

lossy source coding. We deal with the case where both the excess distortion probability and the overflow probability of codeword length are less than or equal to positive constants. The infimum of the thresholds on the overflow probability is characterized by a smooth max entropy-based quantity. Both non-asymptotic and asymptotic cases are analyzed. To show the achievability results, we do not utilize the random coding argument but give an explicit code construction.

On Lossy Compression of Binary Matrices (17:20)

Ronit Bustin (Tel Aviv University, Israel); Ofer Shayevitz (Tel Aviv University, Israel)

We consider lossy compression of random binary matrices under distortion constraints that strive to preserve the structure of the matrix. Specifically, we assume that matrix elements are statistically independent (but not necessarily identically distributed), and that the worst case row/column average distortion is to be controlled. We discuss a natural notion of matrix types termed (R;C)-type, and provide various results concerning its probability and cardinality, as well as a "Sanov-type" result, in the spirit of the method-of-types. We then derive bounds on the associated matrix rate distortion function via a suitable matrix version of the covering lemma.

Universal Lossless Compression of Graphical Data (17:40)

Payam Delgosha (University of California, Berkeley, USA); Venkat Anantharam (University of California at Berkeley, USA)

Consider a data source comprised of a graph with marks on its edges and vertices. Examples of such data sources are social networks, biological data, web graphs, etc. Our goal is to design schemes that can efficiently compress such data without making assumptions about its stochastic properties, i.e. universal compression. To make sense of this, we employ the framework of local weak convergence, also called the objective method, which formalizes the notion of stationary stochastic processes indexed by graphs. We generalize a recently developed notion of entropy for such processes, due to Bordenave and Caputo, to the case of marked graphs, and use it to evaluate the efficiency of a compression scheme. The lossless compression scheme we propose in this paper is then proved to be universally optimal. It is also capable of performing local data queries in the compressed form.

Compressing data on graphs with clusters (18:00)

Amir Asadi (Princeton University, USA); ***Emmanuel Abbe*** *(Princeton University, USA); Sergio Verdú (Princeton University, USA)*

This paper investigates the fundamental limits for compressing data on graphs, exploiting dependencies due to community structures in the graph. The source model, referred to as the data block model (DBM), is a mixture of discrete memoryless sources determined by the community structure of a stochastic block model (SBM). The main result gives the optimal expected length of a lossless compressor when the community signal is strong enough, a condition on the edge probabilities and the data distributions, which can take place below the exact recovery threshold of the SBM. This is derived in part by obtaining the threshold for exact recovery in SBMs with strong side information, a result of independent interest, which extends the CH-divergence threshold. Finally we discuss compressing data with almost exact recovery algorithms.

We1-1: Iterative Decoding 1

Wednesday, June 28, 09:50-11:10
Room: Europa
Chair: Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra, Spain)

Vector Approximate Message Passing (09:50)

Sundeep Rangan (New York University, USA); Philip Schniter (The Ohio State University, USA); Alyson Fletcher (University of California, Los Angeles, USA)

The standard linear regression (SLR) problem is to recover a vector x0 from noisy linear observations y = Ax0 +w. The approximate message passing (AMP) algorithm recently proposed by Donoho, Maleki, and Montanari is a computationally efficient iterative approach to SLR that has a remarkable property: for large i.i.d. sub-Gaussian matrices A, its per- iteration behavior is rigorously characterized by a scalar state-evolution whose fixed points, when unique, are Bayes optimal. AMP, however, is fragile in that even small deviations from the i.i.d. sub-Gaussian model can cause the algorithm to diverge. This paper considers a "vector AMP" (VAMP) algorithm and shows that VAMP has a rigorous scalar state-evolution that holds under a much broader class of large random matrices A: those that are right-rotationally invariant. After performing an initial singular value decomposition (SVD) of A, the per-iteration complexity of VAMP is similar to that of AMP. In addition, the fixed points of VAMP's state evolution are consistent with the replica prediction of the minimum mean-squared error recently derived by Tulino, Caire, Verdú, and Shamai.

Generalized Approximate Message-Passing Decoder for Universal Sparse Superposition Codes (10:10)

Erdem Biyik (Bilkent University, Turkey); Jean Barbier (EPFL, Switzerland); Mohamad Dia (EPFL, Switzerland)

Sparse superposition (SS) codes were originally proposed as a capacity-achieving communication scheme over the additive white Gaussian noise channel (AWGNC) [1]. Very recently, it was discovered that these codes are universal, in the sense that they achieve capacity over any memoryless channel under generalized approximate message-passing (GAMP) decoding [2], although this decoder has never been stated for SS codes. In this contribution we introduce the GAMP decoder for SS codes, we confirm empirically the universality of this communication scheme through its study on various channels and we provide the main analysis tools: state evolution and potential. We also compare the performance of GAMP with the Bayes-optimal MMSE decoder. We empirically illustrate that despite the presence of a phase transition preventing GAMP to reach the optimal performance, spatial coupling allows to boost the performance that eventually tends to capacity in a proper limit. We also prove that, in contrast with the AWGNC case, SS codes for binary input channels have a vanishing error floor in the limit of large codewords. Moreover, the performance of Hadamard-based encoders is assessed for practical implementations.

Block Markov Superposition Transmission of BCH Codes with Iterative Hard-decision Decoding (10:30)

Nina Lin (Sun Yat-sen University, P.R. China); Suihua Cai (Sun Yat-sen University, P.R. China); Xiao Ma (Sun Yat-sen University, P.R. China)

This paper is concerned with block Markov superposition transmission of BCH (BMST-BCH) codes. Compared with other BMST codes, BMST-BCH codes can achieve a lower error floor with an encoding memory of two, which is critical to reduce both delay and implementation complexity. To further reduce the implementation complexity, we propose a hard-decision sliding-window decoding algorithm, in which only binary and/or erasure messages are processed and exchanged between nodes. A fast simulation approach is proposed, with the help of the genie-aided lower bound and the density evolution analysis, to evaluate the performance of BMST-BCH codes at the BER of 10^{-15}. BMST-BCH codes are constructed with overheads ranging from 15% to 25%, exhibiting performances comparable to staircase codes with similar latencies. The proposed construction is more flexible to trade off latency against performance, and may find applications in optical transport networks as an attractive candidate.

Belief Propagation for Subgraph Detection with Imperfect Side-information (10:50)

Arun Kadavankandy (Inria, EURECOM, France); Konstantin Avrachenkov (INRIA Sophia Antipolis, France); Laura Cottatellucci (EURECOM, France); Rajesh Sundaresan (Indian Institute of Science, India)

We propose a local message passing algorithm based on Belief Propagation (BP) to detect a small hidden Erdos-Renyi (ER) subgraph embedded in a larger sparse ER random graph in the presence of side-information. We consider side-information in the form of revealed subgraph nodes called cues, some of which may be erroneous. Namely, the revealed nodes may not all belong to the subgraph, and it is not known to the algorithm a priori which cues are correct and which are incorrect. We show that asymptotically as the graph size tends to infinity, the expected fraction of misclassified nodes approaches zero for any positive value of a parameter λ, which represents the effective Signal-to-Noise Ratio of the detection problem. Previous works on subgraph detection using BP without side-information showed that BP fails to recover the subgraph when $\lambda < 1/e$. Our results thus demonstrate the substantial gains in having even a small amount of side-information.

We1-2: Student Paper Awards Candidate Talks 1

Wednesday, June 28, 09:50-11:10
Room: Brussels
Chair: Wei Yu (University of Toronto, Canada)

Multiplexing Zero-Error and Rare-Error Communications over a Noisy Channel with Feedback (09:50)

Tibor Keresztfalvi (ETH Zurich, Switzerland); Amos Lapidoth (ETHZ, Switzerland)

Two independent data streams—the ”zero-error stream” and the ”rare-error stream”—are to be transmitted over a noisy discrete memoryless channel with feedback. Errors are tolerated only in the rare-error stream, provided that their probability tends to zero. Clearly the rate of the error-free stream cannot exceed the channel’s zero-error feedback capacity, and the sum of the streams’ rates cannot exceed the channel’s Shannon capacity. Using a suitable coding scheme, these necessary conditions are shown to characterize all the achievable rate pairs. Planning for the worst—as is needed to achieve zero- error communication—and planning for the true channel—as is needed to communicate near the Shannon limit—are thus not incompatible.

The Exact Rate-Memory Tradeoff for Caching with Uncoded Prefetching (10:10)

Qian Yu *(University of Southern California, USA); Mohammad Ali Maddah-Ali (Bell Labs, Alcatel Lucent, USA); Salman Avestimehr (University of Southern California, USA)*

We consider a cache network, where a single server is connected to multiple users via a shared bottleneck link. The server has a set of files, which can be cached by each user in a prefetching phase. In a following delivery phase, each user requests a file and the server needs to deliver users' demands as efficiently as possible by taking into account their cache contents. We focus on an important and commonly used class of prefetching schemes, where the caches are filled with uncoded data. We provide the exact characterization of rate-memory tradeoff for this problem, by deriving the both the minimum average rate (for a uniform file popularity) and the minimum peak-rate required on the bottleneck link for a given cache size available at each user. We propose a novel caching scheme, which strictly improves the state of the art by exploiting commonality among users' demands. We then demonstrate the exact optimality of our proposed scheme through a matching converse, by dividing the set of all demands into types, and showing that the placement phase in the proposed caching scheme is universally optimal for all types. Using these techniques, we can also fully characterize the rate-memory tradeoff for a decentralized setting, in which users fill out their cache content without any coordination.

Greedy-Merge Degrading has Optimal Power-Law (10:30)

Assaf Kartowsky (Technion, Israel); Ido Tal (Technion, Israel)

Consider a channel with a given input distribution. Our aim is to degrade it to a channel with at most L output letters. One such degradation method is the so called ”greedy-merge” algorithm. We derive an upper bound on the reduction in mutual information between input and output. For fixed input alphabet size and variable L, the upper bound is within a constant factor of an algorithm-independent lower bound. Thus, we establish that greedy-merge is optimal in the power-law sense.

A Generic Transformation for Optimal Repair Bandwidth and Rebuilding Access in MDS Codes (10:50)

Jie Li *(Southwest Jiaotong University, P.R. China); Xiaohu Tang (SWJTU, P.R. China); Chao Tian (University of Tennessee Knoxville, USA)*

We propose a generic transformation on maximum distance separable (MDS) codes, which can convert any non-binary (k+r,k) MDS code into another (k+r,k) MDS code with the following properties: 1) An arbitrarily chosen r nodes will have the optimal repair bandwidth and the optimal rebuilding access, 2) the repair bandwidth and rebuilding access efficiencies of all other nodes are maintained as in the code before the transformation, 3) it uses the same finite field as the code before the transformation, and 4) the sub-packetization is increased only by a factor of r. As two immediate applications of this powerful transformation, we show that 1) any non-binary MDS code with optimal repair bandwidth, or optimal rebuilding access, for only systematic nodes can be converted into an MDS code with the corresponding repair optimality for all nodes; and 2) any non-binary scalar MDS code can be converted to an MDS code with optimal repair bandwidth and rebuilding access for all nodes, or to an MDS code with optimal rebuilding access for all systematic nodes and moreover with the optimal sub-packetization, by applying the transformation multiple times.

We1-3: Coding for Storage and Streaming

Wednesday, June 28, 09:50-11:10
Room: K2
Chair: Ashish Khisti (University of Toronto, Canada)

Multipermutation Ulam Sphere Analysis Toward Characterizing Maximal Code Size (09:50)

Justin Kong *(Chiba University, Japan); Manabu Hagiwara (Chiba University, Japan)*

Permutation codes, in the form of rank modulation, have shown promise for applications such as flash memory. One of the metrics recently suggested as appropriate for rank modulation is the Ulam metric, which measures the minimum translocation distance between permutations. Multipermutation codes have also been proposed as a generalization of permutation codes that would improve code size (and consequently the code rate). In this paper we analyze the Ulam metric in the context of multipermutations, noting some similarities and differences between the Ulam metric in the context of permutations. We also consider sphere sizes for multipermutations under the Ulam metric and resulting bounds on code size.

Multiplexed FEC for Multiple Streams with Different Playout Deadlines (10:10)

Ahmed Badr (University of Toronto, Canada); Devin Lui (University of Toronto, Canada); Ashish Khisti (University of Toronto, Canada); Wai-Tian Tan (Cisco Systems, USA); Xiaoqing Zhu (Cisco Systems, USA); John Apostolopoulos (Cisco Systems, USA)

We study a setting where two source streams with different decoding deadlines must be transmitted over a

burst erasure channel. The source streams are multiplexed into a single stream of channel-packets at the encoder. The decoder must recover the source-packets within each stream sequentially, by their corresponding deadlines. We consider the burst-erasure channel model and characterize the capacity region for a certain range of system parameters. We show that the operation of the system can be dividing into three different regimes based on the relative values of decoding deadlines. We propose a coding scheme for each case. On the achievability side, we show that jointly coding across the two streams in a judicious manner can outperform the baseline scheme where we apply a single-stream code to each of the streams separately. On the converse side we develop information theoretic outer bounds on the capacity region. Interestingly we find that the capacity region exhibits a "corner point" where we can transmit the urgent stream at a positive rate, yet attain a sum-rate equal to the capacity of the non-urgent stream.

A Code Equivalence between Streaming Network Coding and Streaming Index Coding (10:30)

Ming Fai Wong (California Institute of Technology, USA); Michelle Effros (California Institute of Technology, USA); Michael Langberg (State University of New York at Buffalo, USA)

We consider a delay-constrained streaming model for communications and show that under this model, network coding and index coding problems are code equivalent. That is, any streaming network coding instance can be efficiently mapped to a corresponding acyclic streaming index coding instance such that an index code for the latter can be efficiently transformed into a network code for former. This reduction holds even for network coding instances that contain cycles, thereby proving the first known reduction from cyclic to finite acyclic network coding networks.

On the error probability of stochastic decision and stochastic decoding (10:50)

Jun Muramatsu (NTT Corporation, Japan); Shigeki Miyake (NTT, Japan)

This paper investigates the error probability of a stochastic decision and the way in which it differs from the error probability of an optimal decision, i.e., the maximum a posteriori decision. This paper calls attention to the fact that the error probability of a stochastic decision with the a posteriori distribution is at most twice the error probability of the maximum a posteriori decision. It is shown that, by generating an independent identically distributed random sequence subject to the a posteriori distribution and making a decision that maximizes the a posteriori probability over the sequence, the error probability approaches exponentially the error probability of the maximum a posteriori decision as the sequence length increases. Using these ideas as a basis, we can construct stochastic decoders for source/channel codes.

We1-4: Zero Error Capacity

Wednesday, June 28, 09:50-11:10
Room: K3
Chair: Alon Orlitsky (University of California, San Diego, USA)

The Birthday Problem and Zero-Error List Codes (09:50)

Parham Noorzad (California Institute of Technology, USA); Michelle Effros (California Institute of Technology, USA); Michael Langberg (State University of New York at Buffalo, USA); Victoria Kostina (California Institute of Technology, USA)

As an attempt to bridge the gap between classical information theory and the combinatorial world of zero-error information theory, this paper studies the performance of randomly generated codebooks over discrete memoryless channels under a zero-error constraint. This study allows the application of tools from one area to the other. Furthermore, it leads to an information-theoretic formulation of the birthday problem, which is concerned with the probability that in a given population, a fixed number of people have the same birthday. Due to the lack of a closed-form expression for this probability when the distribution of birthdays is not uniform, the resulting computation is not feasible in some applications; the information-theoretic formulation, however, can be analyzed for all distributions.

The Zero-Error Capacity of a Collision Channel With Successive Interference Cancellation (10:10)

Yijin Zhang *(Nanjing University of Science and Technology, P.R. China); Yi Chen (The Chinese University of Hong Kong, Shenzhen, Hong Kong); Yuan-Hsun Lo (Xiamen University, P.R. China); Wing Shing Wong (The Chinese University of Hong Kong, P.R. China)*

The collision channel without feedback (CCw/oFB) model depicts a scenario in which multiple users share a communication channel with random relative time offsets among their clocks. This paper considers an extension of this model, which allows the receiver to use successive interference cancellation (SIC) to iteratively cancel the interference caused by those collided packets that have been decoded by the receiver. We derive the zero-error capacity region of this channel in the slot-synchronous case, and present a zero-error capacity achieving scheme by joint protocol sequences and channel coding design. It is shown that the negative impact on the zero-error capacity due to a lack of time synchronization can be removed by SIC

An improved bound on the zero-error list-decoding capacity of the 4/3 channel (10:30)

Marco Dalai (University of Brescia, Italy); Venkatesan Guruswami (Carnegie Mellon University, USA); Jaikumar Radhakrishnan (TIFR, Mumbai, India)

We prove a new, improved upper bound on the size of codes $C \subseteq \{1,2,3,4\}^n$ with the property that every four distinct codewords in C have a coordinate where they all differ. Specifically, we show that such a code has size at most $2^{6n/19+o(n)}$, or equivalently has rate bounded by $6/19 \leq 0.3158$ (measured in bits). This improves the previous best upper bound of 0.3512 due to (Arikan 1994), which in turn improved the 0.375 bound that followed from general bounds for perfect hashing due to (Fredman and Komlós, 1984) and (Körner and Marton, 1988). The context for this problem is two-fold: zero-error list decoding capacity, where such codes give a way to communicate with no error on the "4/3 channel" when list-of-3 decoding is employed, and perfect hashing, where such codes give a perfect hash family of size n mapping C to $\{1,2,3,4\}$.

We1-5: Joint Source-Channel Coding 2

Wednesday, June 28, 09:50-11:10
Room: K4
Chair: Sandeep Pradhan (University Michigan, USA)

Dependence Balance in Multiple Access Channels with Correlated Sources (09:50)

Amos Lapidoth (ETHZ, Switzerland); Shirin Saeedi Bidokhti (Stanford University, USA); Michele Wigger (Telecom ParisTech, France)

A necessary condition is established for the lossy transmission of correlated sources over memoryless multiple access channels (MAC). It is used to derive lower bounds on the symmetric distortions that are achievable over Gaussian and binary adder MACs. When specialized to symmetric Gaussian MACs and Gaussian sources, the new lower bound recovers Lapidoth and Tinguely's max-correlation lower bound (2010) for matched source and channel bandwidths, and it improves on it for bandwidth mismatch factors below one. An analogous condition is also derived for MACs with correlated sources and feedback.

On Minimum Energy for Robust Gaussian Joint Source-Channel Coding with a Distortion-Noise Profile (10:10)

Erman Köken (UC Riverside, USA); Ertem Tuncel (UC Riverside, USA)

Minimum energy required to achieve a distortion-noise profile, i.e., a function indicating the maximum allowed distortion value for each noise level, is studied for robust transmission of Gaussian sources over Gaussian channels. It is shown that for the inversely linear profile, uncoded transmission is optimal. On the other hand, it turns out that exponential profiles are not achievable with finite energy. Finally, using a family of lower bounds and a proposed coding scheme, the minimum energy behavior for the square-law profile is understood up to a multiplicative constant.

Communicating Correlated Sources Over a MAC (10:30)

Arun Padakandla (Purdue University, USA)

The problem of characterizing sufficient conditions for communicating correlated sources over a MAC is considered. The technique of inducing source correlation onto channel inputs - due to Cover, El Gamal and Salehi [Nov, 1980] - is enhanced by the use of *fixed B-L coding*. The performance of the proposed coding technique is characterized via single-letter expressions to derive a new set of sufficient conditions. The latter conditions are contained within those characterized in [Cover, El Gamal, Salehi], and are proven to be strictly less binding than those of the latter for certain examples.

We1-6: Spatial Coupling

Wednesday, June 28, 09:50-11:10
Room: K5
Chair: Laurent Schmalen (Nokia Bell Labs, Germany)

Spatially Coupled LDLC: New Constructions (09:50)

Svetlana Reznikov (Tel-Aviv University, Israel); Meir Feder (Tel-Aviv University, Israel)

Low Density Lattice Code (LDLC) uses a lattice with a sparse inverse matrix, which allows a linear complexity decoding. Spatially Coupled Low Density Lattice Code (SC-LDLC) is built by coupling some LDLCs and has a smaller Symbol Error Rate (SER) than the LDLC scheme for every tested block length n. In this paper, some new constructions of the spatially coupled low density lattice codes are introduced.

A Protograph-Based Design of Quasi-Cyclic Spatially Coupled LDPC Codes (10:10)

Li Chen (Sun Yat-sen University, P.R. China); Shiyuan Mo (Sun Yat-sen University, P.R. China); Daniel Costello (University of Notre Dame, USA); David Mitchell (New Mexico State University, USA); Roxana Smarandache (University of Notre Dame, USA)

Spatially coupled (SC) low-density parity-check (LDPC) codes can achieve capacity approaching per-

formance with low message recovery latency when using sliding window (SW) decoding. An SC-LDPC code constructed from a protograph can be generated by first *coupling* a chain of block protographs and then *lifting* the coupled protograph using permutation matrices. This paper introduces a systematic design of SC-LDPC codes to eliminate 4-cycles in the coupled protograph. Using a quasi-cyclic (QC) lifting, we obtain QC-SC-LDPC codes of girth at least eight. Coupling a chain of block protographs implies *spreading* edges from one protograph to the others. Our protograph-based design can be viewed as guiding the edge spreading and also the graph-lifting process. Simulation results show the design results in improved decoding performance, particularly in the error floor, compared to random designs.

Complexity-Optimized Concatenated LDGM-Staircase Codes (10:30)

Lei Zhang *(University of Toronto, Canada); Frank Kschischang (University of Toronto, Canada)*

A concatenated soft-decision channel coding scheme consisting of an inner LDGM code and an outer staircase code is proposed. The soft-decision LDGM code is used for error reduction while the majority of bit errors are corrected by the low complexity hard-decision staircase code. Decoding complexity of the concatenated code is quantified by a score based on the number of edges in the LDGM code Tanner graph, the number of decoding iterations, and the number of staircase code decoding operations. The inner LDGM ensemble is designed by solving an optimization problem, which minimizes the product of the average node degree and an estimate of the required number of decoding iterations. A search procedure is used to find the inner and outer code pair with lowest complexity. The design procedure results in a Pareto-frontier characterization of the trade-off between net coding-gain and complexity for the concatenated code. Simulations of code designs at rate 5/6 show that the proposed scheme achieves net coding-gains equivalent to existing soft-decision codes, with up to 57% reduction in complexity.

A Novel Combinatorial Framework to Construct Spatially-Coupled Codes: Minimum Overlap Partitioning (10:50)

Homa Esfahanizadeh (University of California, Los Angeles, USA); Ahmed Hareedy (University of California, Los Angeles (UCLA), USA); ***Lara Dolecek*** *(UCLA, USA)*

Spatially-coupled (SC) codes are a family of graph-based codes that have attracted significant attention thanks to their capacity approaching performance. An SC code is constructed by partitioning an underlying block code into a number of components, and coupling these copies together. In this paper, we introduce a new partitioning scheme, namely minimum overlap partitioning, that outperforms previous methods. We also present a general approach for the enumeration of problematic objects in the error-floor area that can be applied to any circulant-based SC code and to a variety of partitioning schemes. Our results show that, compared to the decoupled block code, an SC code constructed by the minimum overlap partitioning has more than 1.5 and 3 orders of magnitude performance improvement for the memory 1 and 2, respectively. Additionally, it outperforms the existing method of partitioning via cutting vectors by at least half an order of magnitude; this performance advantage becomes more pronounced with increasing the memory.

We1-7: Security 3

Wednesday, June 28, 09:50-11:10
Room: K6
Chair: Salim El Rouayheb (Illinois Institute of Technology, USA)

Secure wireless communication under spatial and local Gaussian noise assumptions (09:50)

Masahito Hayashi (Nagoya University, Japan)

We consider wireless communication between Alice and Bob when the intermediate space between Alice and Bob is controlled by Eve. That is, our model divides the channel noise into two parts, the noise generated during the transmission and the noise generated in the detector. Eve is allowed to control the former, but is not allowed to do the latter. While the latter is assumed to be a Gaussian random variable, the former is not assumed to be a Gaussian random variable. In this situation, using backward reconciliation and the random sampling, we propose a protocol to generate secure keys between Alice and Bob under the assumption that Eve's detector has a Gaussian noise and Eve is out of Alice's neighborhood. In our protocol, the security criteria are quantitatively guaranteed even with finite block-length code based on the evaluation of error of the estimation of channel.

The Degraded Gaussian Multiple Access Wiretap Channel with Selfish Transmitters: A Coalitional Game Theory Perspective (10:10)

Remi Chou (Pennsylvania State University, USA); Aylin Yener (Pennsylvania State University, USA)

We study the degraded Gaussian multiple access wiretap channel with selfish transmitters, i.e., they are each solely interested in maximizing their individual secrecy rate. The question then arises as to whether selfish transmitters can increase their individual secrecy rate by participating in a collective protocol, instead of operating on their own. If yes, is there a protocol that satisfy all the participating transmitters, in the sense that no transmitter has an incentive to deviate from the

protocol? We answer these questions in the positive utilizing coalitional game theory. In particular, we show that cooperation is in the best interest of all transmitters and that there exist protocols that incentivize all transmitters to participate. Furthermore, we determine a unique, fair, and stable achievable secrecy rate allocation.

MIMO Gaussian Wiretap Channels with Two Transmit Antennas: Optimal Precoding and Power Allocation (10:30)

Mojtaba Vaezi (Princeton University, USA); Wonjae Shin (Seoul National University, Korea); H. Vincent Poor (Princeton University, USA); Jungwoo Lee (Seoul National University, Korea)

A Gaussian multiple-input multiple-output wiretap channel in which the eavesdropper and legitimate receiver are equipped with arbitrary numbers of antennas and the transmitter has two antennas is studied in this paper. It is shown that the secrecy capacity of this channel can be achieved by linear precoding. The optimal precoding and power allocation scheme achieving the secrecy capacity are developed subsequently, and the secrecy capacity is compared with the generalized singular value decomposition (GSVD)-based precoding, which is the best previously proposed precoding for this problem. Numerical results demonstrate that substantial gain can be obtained in secrecy rate between the proposed and GSVD-based precoding.

Computation of the Random Coding Secrecy Exponent for a Constant Composition Ensemble (10:50)

Yutaka Jitsumatsu (Kyushu University, Japan)

Recently, Parizi, Telatar, and Merhav [1] determined the exact random coding secrecy exponents for a wiretap channel. In this study, we focus on the computation of such secrecy exponents. To obtain the exact random coding secrecy exponent for a constant composition random coding ensemble, optimization with respect to two stochastic matrices must be performed. Parizi et al. suggested that inner optimization is a convex optimization problem and therefore can be solved efficiently and that the outer optimization is not guaranteed to have convex structure and is solved by an exhaustive search. In this paper, we develop an efficient computation of the exact random coding secrecy exponent.

We1-8: Quantum IT 3

Wednesday, June 28, 09:50-11:10
Room: K7+8
Chair: Min-Hsiu Hsieh (University of Technology Sydney, Australia)

Codes for Simultaneous Transmission of Quantum and Classical Information (09:50)

Markus Grassl (Max-Plank-Institut für die Physik des Lichts, Germany); ***Sirui Lu*** *(Tsinghua University, P.R. China); Bei Zeng (University of Guelph, Canada)*

We consider the characterization as well as the construction of quantum codes that allow to transmit both quantum and classical information, which we refer to as 'hybrid codes'. We construct hybrid codes $[[n, k : m, d]]_q$ with length n and distance d, that simultaneously transmit k qudits and m symbols from a classical alphabet of size q. Many good codes such as $[[7, 1 : 1, 3]]_2$, $[[9, 2 : 2, 3]]_2$, $[[10, 3 : 2, 3]]_2$, $[[11, 4 : 2, 3]]_2$, $[[11, 1 : 2, 4]]_2$, $[[13, 1 : 4, 4]]_2$, $[[13, 1 : 1, 5]]_2$, $[[14, 1 : 2, 5]]_2$, $[[15, 1 : 3, 5]]_2$, $[[19, 9 : 1, 4]]_2$, $[[20, 9 : 2, 4]]_2$, $[[21, 9 : 3, 4]]_2$, $[[22, 9 : 4, 4]]_2$. All these codes have better parameters than hybrid codes obtained from the best known stabilizer quantum code.

Belief propagation decoding of quantum channels by passing quantum messages (10:10)

Joseph Renes (ETH Zurich, Switzerland)

We construct a belief propagation algorithm which passes quantum messages on the factor graph and is capable of decoding the classical-quantum channel with pure state outputs. This gives explicit decoding circuits whose number of gates is quadratic in the code length. We show that the decoder can be modified to work with polar codes for the pure state channel and as part of a decoder for transmitting quantum information over the amplitude damping channel. These yield the first explicit capacity-achieving decoders for non-Pauli channels.

Semidefinite programming converse bounds for classical communication over quantum channels (10:30)

Xin Wang (University of Technology Sydney, Australia); Wei Xie (University of Technology Sydney, Australia); Runyao Duan (University of Technology Sydney, Australia)

We study the classical communication over quantum channels when assisted by no-signalling (NS) and PPT-preserving (PPT) codes. We first show that both the optimal success probability of a given transmission rate and one-shot ϵ-error capacity can be formalized as semidefinite programs (SDPs) when assisted by NS and PPT codes. Based on this, we derive SDP fi-

nite blocklength converse bounds for general quantum channels, which also reduce to the converse bound of Polyanskiy, Poor, and Verdu for classical channels. Furthermore, we derive an SDP strong converse bound for the classical capacity of a general quantum channel: for any code with a rate exceeding this bound, the optimal success probability vanishes exponentially fast as the number of channel uses increases. In particular, applying our efficiently computable bound, we derive improved upper bounds to the classical capacity of the amplitude damping channels and also establish the strong converse property for a new class of quantum channels.

On the Feasibility Conditions of Quantum State Discrimination (10:50)

Chung-Chin Lu *(National Tsing Hua University, Taiwan); Shiuan-Hao Kuo (Silicon Motion, Inc., Taiwan)*

In this paper, we consider the quantum unambiguous discrimination problem of a set of linearly independent pure states. With a constructive procedure, we establish a necessary and sufficient condition for feasible POVM measurements for unambiguous quantum state discrimination. We develop methods to calculate the optimal discrimination efficiencies for minimizing the inconclusive probability and the optimal discrimination efficiencies for the minimax criterion. Finally, we prove a necessary and sufficient condition to have a feasible POVM measurement which achieves the minimum inconclusive probability criterion and the minimax criterion simultaneously and show that geometrically uniform states with equal a priori probabilities meet this condition.

We1-9: Source Coding 3

Wednesday, June 28, 09:50-11:10
Room: K9
Chair: Charalambos Charalambous (University of Cyprus, Cyprus)

An Information-Theoretic Analysis of Deduplication (09:50)

Urs Niesen (Qualcomm Research, USA)

Deduplication finds and removes long-range data duplicates. It is commonly used in cloud and enterprise server settings and has been successfully applied to primary, backup, and archival storage. Despite its practical importance as a source-coding technique, its analysis from the point of view of information theory is missing. This paper provides such an information-theoretic analysis of data deduplication. It introduces a new source model adapted to the deduplication setting. It formalizes both fixed and variable-length deduplication schemes, and it introduces a novel, multi-chunk deduplication scheme. It then provides an analysis of these three deduplication variants, emphasizing the importance of boundary synchronization between source blocks and deduplication chunks. The proposed multi-chunk deduplication scheme is shown to be order optimal under fairly mild assumptions.

Extended Gray-Wyner System with Complementary Causal Side Information (10:10)

Cheuk Ting Li *(Stanford University, USA); Abbas El Gamal (Stanford University, USA)*

We establish the rate region of an extended Gray-Wyner system for 2-DMS (X, Y) with two additional decoders having complementary causal side information. This extension is interesting because in addition to the operationally significant extreme points of the Gray-Wyner rate region, which include Wyner's common information, Gács-Körner common information and information bottleneck, the rate region for the extended system also includes the Körner graph entropy, the privacy funnel and excess functional information, as well as three new quantities of potential interest, as extreme points. To simplify the investigation of the 5-dimensional rate region of the extended Gray-Wyner system, we establish an equivalence of this region to a 3-dimensional mutual information region that consists of the set of all triples of the form $(I(X;U),\, I(Y;U),\, I(X,Y;U))$ for some $p_{U|X,Y}$. We further show that projections of this mutual information region yield the rate regions for many settings involving a 2-DMS, including lossless source coding with causal side information, distributed channel synthesis, and lossless source coding with a helper.

Variable-Length Resolvability for General Sources (10:30)

Hideki Yagi (University of Electro-Communications, Japan); Te Sun Han (University of Electro-Communications, Japan)

We introduce the problem of variable-length source resolvability, where a given target probability distribution is approximated by encoding variable-length uniform random numbers, and the asymptotically minimum average length rate of the uniform random numbers, called the (variable-length) resolvability, is investigated. We first analyze the variable-length resolvability with the variational distance as an approximation measure. We then extend the analysis to the case under the divergence as an approximation measure. When the asymptotically exact approximation is required, it is shown that the resolvability under the two kinds of approximation measures coincides. We also analyze the second-order variable-length resolvability.

Universal Tree Source Coding Using Grammar-Based Compression (10:50)

Markus Lohrey (University of Siegen, Germany); ***Danny Hucke*** *(University of Siegen, Germany)*

We apply so-called tree straight-line programs to the problem of universal source coding for binary trees. We derive an upper bound on the maximal pointwise redundancy (or worst-case redundancy) that improve previous bounds on the average case redundancy obtained by Zhang, Yang, and Kieffer using directed acyclic graphs. Using this, we obtain universal codes for new classes of tree sources.

We2-1: Coding Techniques (Focus Session)

Wednesday, June 28, 11:30-12:30
Room: Europa
Chair: Irina Bocharova (St. Petersburg University of Information Technologies, Mechanics and Optics, Russia)

Multi-Block Interleaved Codes for Local and Global Read Access (11:30)

Yuval Cassuto (Technion, Israel); Evyatar Hemo (Technion - Institute of Technology, Israel); Sven Puchinger (Ulm University, Germany); Martin Bossert (Ulm University, Germany)

We define multi-block interleaved codes as codes that allow reading information from either a small sub-block or from a larger full block. The former offers faster access, while the latter provides better reliability. We specify the correction capability of the sub-block code through its gap t from optimal minimum distance, and look to have full-block minimum distance that grows with the parameter t. We construct two families of such codes when the number of sub-blocks is 3. The codes match the distance properties of known integrated-interleaving codes, but with the added feature of mapping the same number of information symbols to each sub-block. As such, they are the first codes that provide read access in multiple size granularities and correction capabilities.

Successive Cancellation Decoding of Single Parity-Check Product Codes (11:50)

Mustafa Coşkun (Technische Universität München, Germany); Gianluigi Liva (DLR - German Aerospace Center, Germany); Alexandre Graell i Amat (Chalmers University of Technology, Sweden); Michael Lentmaier (Lund University, Sweden)

We introduce successive cancellation (SC) decoding of product codes (PCs) with single parity-check (SPC) component codes by using recursive formulas. We analyze the error probability of SPC-PCs over the binary erasure channel under SC decoding. A bridge with the analysis of PCs introduced by Elias in 1954 is also established. Furthermore, bounds on the block error probability under SC decoding are provided, and compared to the bounds under the original decoding algorithm proposed by Elias. It is shown that SC decoding of SPC-PCs achieves a lower block error probability than Elias' decoding.

Codes for Channels With Segmented Edits (12:10)

Mahed Abroshan (University of Cambridge, United Kingdom (Great Britain)); Ramji Venkataramanan (University of Cambridge, United Kingdom (Great Britain)); Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra & University of Cambridge, Spain)

We consider insertion and deletion channels with the additional assumption that the channel input sequence is implicitly divided into segments such that at most one edit can occur within a segment. We further assume that there are no segment markers in the received sequence. We propose code constructions for the segmented deletion, segmented insertion, and segmented insertion-deletion channels based on subsets of VT codes chosen with pre-determined prefixes and/or suffixes. The proposed codes are zero-error, can be decoded segment-by-segment, and their rate scaling as the segment length increases is the same as that of the maximal code.

We2-2: Student Paper Awards Candidate Talks 2

Wednesday, June 28, 11:30-12:30
Room: Brussels
Chair: Elza Erkip (New York University, USA)

A High-SNR Normal Approximation for Single-Antenna Rayleigh Block-Fading Channels (11:30)

Alejandro Lancho *(Universidad Carlos III de Madrid & Gregorio Marañón Health Research Institute, Spain); Tobias Koch (Universidad Carlos III de Madrid & Gregorio Marañón Health Research Institute, Spain); Giuseppe Durisi (Chalmers University of Technology, Sweden)*

This paper concerns the maximal achievable rate at which data can be transmitted over a non-coherent, single-antenna, Rayleigh block-fading channel using an error-correcting code of a given blocklength with a block-error probability not exceeding a given value. In particular, a high-SNR normal approximation of the maximal achievable rate is presented that becomes accurate as the signal-to-noise ratio (SNR) and the number of coherence intervals L over which we code tend to infinity. Numerical analyses suggest that the

approximation is accurate already at SNR values of 15 dB.

A Tight Rate Bound and a Matching Construction for Locally Recoverable Codes with Sequential Recovery From Any Number of Multiple Erasures (11:50)

Balaji Srinivasan Babu *(IISc, India); Ganesh Kini (Indian Institute of Science, India); P Vijay Kumar (Indian Institute of Science & University of Southern California, India)*

An $[n, k]$ code $\mathcal{C}$ is said to be locally recoverable in the presence of a single erasure, and with locality parameter r, if each of the n code symbols of $\mathcal{C}$ can be recovered by accessing at most r other code symbols. An $[n, k]$ code is said to be a locally recoverable code with sequential recovery from t erasures, if for any set of $s \leq t$ erasures, there is an s-step sequential recovery process, in which at each step, a single erased symbol is recovered by accessing at most r other code symbols. This is equivalent to the requirement that for any set of $s \leq t$ erasures, the dual code contain a codeword whose support contains the coordinate of precisely one of the s erased symbols. In this paper, a tight upper bound on the rate of such a code, for any value of number of erasures t and any value $r \geq 3$, of the locality parameter is derived. This bound proves an earlier conjecture due to Song, Cai and Yuen. While the bound is valid irrespective of the field over which the code is defined, a matching construction of *binary* codes that are rate-optimal is also provided, again for any value of t and any value $r \geq 3$.

Feedback Capacity and Coding for the (0,k)-RLL Input-Constrained BEC (12:10)

Ori Peled *(Ben-Gurion University, Israel); Oron Sabag (Ben-Gurion University, Israel); Haim Permuter (Ben-Gurion University, Israel)*

The input-constrained binary erasure channel (BEC) with strictly causal feedback is studied. The channel input sequence must satisfy the $(0, k)$-runlength limited (RLL) constraint, i.e., no more than k consecutive zeros are allowed. The feedback capacity of this channel is derived for all $k \geq 1$,

$$C_{(0,k)}^{\mathrm{fb}}(\varepsilon) = \max \frac{\overline{\varepsilon} H_2(\delta_0) + \sum_{i=1}^{k-1} \left(\overline{\varepsilon}^{i+1} H_2(\delta_i) \prod_{m=0}^{i-1} \delta_m \right)}{1 + \sum_{i=0}^{k-1} \left(\overline{\varepsilon}^{i+1} \prod_{m=0}^{i} \delta_m \right)},$$

where ε is the erasure probability, $\overline{\varepsilon} = 1 - \varepsilon$, $H_2(\cdot)$ is the binary entropy function and the maximization is only over δ_{k-1}, while the other parameters $\delta_0, \ldots, \delta_{k-2}$ are simple functions of δ_{k-1}. A simple coding scheme is constructed for all k, establishing that the feedback capacity can be achieved using variable length zero-error coding. In addition, it is shown that non-causal knowledge of the erasures at the encoder does not increase the feedback capacity.

We2-3: Crypto (Focus Session)

Wednesday, June 28, 11:30-12:30
Room: K2
Chair: Natasa Zivic (University of Siegen, Germany)

Efficiency Lower Bounds for Commit-and-Prove Constructions (11:30)

Chen-Da Liu Zhang (ETH Zurich, Switzerland); Christian Badertscher (ETH Zurich, Switzerland); Sandro Coretti (New York University, USA); Ueli Maurer (ETH Zurich, Switzerland)

Commitment schemes that come along with zero-knowledge proofs for relations among committed values are known as commit-and-prove functionalities or notarized envelopes. An important role in this context take equality proofs among commitments. They appear in various contexts of multi-party computation, circuit satisfiability or inclusion proofs. Using commit-and-prove functionalities for equality, we investigate black-box constructions of commit-and-prove functionalities for more complex relations. We are interested in the relationship between the soundness of such protocols and the number of additional commitments a protocol creates during a run. In particular, for the natural and quite general class of 3-round public-coin zero-knowledge protocols, it turns out that implementing an inequality proof, or any of the relations NAND, NOR, or XOR, essentially requires at least $2n$ additional commitments in order to achieve a soundness of 2^{-n}. For concreteness, we revisit a protocol for inequality that exactly matches this bound.

Information Set Decoding with Soft Information and some cryptographic applications (11:50)

Qian Guo (Lund University & Lund University, Sweden); Thomas Johansson (Lund University, Sweden); Erik Mårtensson (Lund University, Sweden); Paul Stankovski (Lund University, Sweden)

The class of information set decoding algorithms is the best known way of decoding general codes, i.e. codes that admit no special structure, in the Hamming metric. Stern's algorithm is the origin of the most efficient algorithms in this class. In this paper we consider the same decoding problem but for a channel with soft information. We give a version of Stern's algorithm for a channel with soft information that includes some novel steps of ordering vectors in lists, based on reliability values. We then demonstrate how this new algorithm can be used in a few cryptographic applications, including a very efficient attack on a recently proposed McEliece-type cryptosystem.

Statistical Decoding (12:10)

Thomas Debris-Alazard (Inria Paris, France); Jean-Pierre Tillich (INRIA, France)

The security of code-based cryptography relies primarily on the hardness of generic decoding with linear codes. The best generic decoding algorithms are all improvements of an old algorithm due to Prange: they are known under the name of information set decoding techniques (ISD). A while ago a generic decoding algorithm which does not belong to this family was proposed: statistical decoding. It is a randomized algorithm that requires the computation of a large set of parity-check equations of moderate weight. We solve here several open problems related to this decoding algorithm. We give in particular the asymptotic complexity of this algorithm, give a rather efficient way of computing the parity-check equations needed for it inspired by ISD techniques and give a lower bound on its complexity showing that when it comes to decoding on the Gilbert-Varshamov bound it can never be better than Prange's algorithm.

We2-4: Security (Focus Session)

Wednesday, June 28, 11:30-12:30
Room: K3
Chair: Andrew Thangaraj (IIT Madras, India)

Security of Helper Data Schemes for SRAM-PUF in Multiple Enrollment Scenarios (11:30)

Lieneke Kusters (Eindhoven University of Technology, The Netherlands); Tanya Ignatenko (Eindhoven University of Technology, The Netherlands); Frans Willems (Technical University Eindhoven, The Netherlands); Roel Maes (Intrinsic-ID, The Netherlands); Erik van der Sluis (Intrinsic-ID, The Netherlands); Georgios. Selimis (Intrinsic-ID, The Netherlands)

Fuzzy commitment and syndrome-based schemes are two well-known helper data schemes used to bind and generate, respectively, a secret key to/from SRAM-PUF observations. To allow the decoder to reconstruct this secret key from a new (verification) observation of an SRAM-PUF, an encoder has to generate so-called helper data. This helper data is a function of an SRAM-PUF enrollment observation and, in case of fuzzy commitment, the secret key. The helper data is assumed to be public and thus must leak no information about the secret key. It is known that in the unbiased case both schemes can achieve secrecy capacity equal to the mutual information between enrollment and verification SRAM-PUF observations at negligible secrecy leakage, when a secret key is created for a single SRAM-PUF enrollment observation. We study here the situation when multiple SRAM-PUF observations are used to create different secret keys. First, we introduce a symmetry property for multiple SRAM-PUF observations. For such symmetric SRAM-PUFs, we show that, in both helper data schemes, the helper data corresponding to multiple SRAM-PUF observations provide no information about any of the secret keys.

New Models for Interference and Broadcast Channels with Confidential Messages (11:50)

Mohamed Nafea *(The Pennsylvania State University, USA); Aylin Yener (Pennsylvania State University, USA)*

A new model for the interference channel with confidential messages (IC-CM) is introduced, where each receiver, besides his noisy observations, is provided with a fixed-length subset, of his choosing, of noiseless observations for the transmitted codewords of both users, making confidential communication more challenging than the previous such model. In addition, in the same spirit, a broadcast channel with confidential messages (BC-CM), where the receivers noiselessly tap into subsets of their choice of the transmitted codeword, is considered. Achievable strong secrecy rate regions for both models are derived. In both models, the size of the subset quantifies a secure rate trade-off between the two receivers. The case of the new BC-CM model with one receiver's noisy observations are degraded with respect to the other receiver, and only the degraded receiver is provided with the subset of noiseless observations, is highlighted. In this case, the receiver with the degraded noisy observations has a positive rate after a certain threshold of his noiseless observations, i.e., with the aid of these symbols.

Secret Sharing with Optimal Decoding and Repair Bandwidth (12:10)

Wentao Huang (California Institute of Technology, USA); Jehoshua Bruck (California Institute of Technology, USA)

This paper studies the communication efficiency of threshold secret sharing schemes. We construct a family of Shamir's schemes with asymptotically optimal decoding bandwidth for arbitrary parameters. We also construct a family of secret sharing schemes with both optimal decoding and optimal repair bandwidth for arbitrary parameters. The construction leads to a family of regenerating codes allowing centralized repair of multiple node failures with small sub-packetization.

We2-5: Network Information Theory (Focus Session)

Wednesday, June 28, 11:30-12:30
Room: K5
Chair: Anthony Ephremides (University of Maryland, USA)

Towards an Algebraic Network Information Theory: Simultaneous Joint Typicality Decoding (11:30)

Sung Hoon Lim (Korea Institute of Ocean Science and Technology, Korea); Chen Feng (University of British Columbia, Canada); Adriano Pastore (Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain); Bobak Nazer (Boston University, USA); Michael Gastpar (EPFL & University of California, Berkeley, Switzerland)

Recent work has employed joint typicality encoding and decoding of nested linear code ensembles to generalize the compute–forward strategy to discrete memoryless multiple-access channels (MACs). An appealing feature of these nested linear code ensembles is that the coding strategies and error probability bounds are conceptually similar to classical techniques for random i.i.d. code ensembles. In this paper, we consider the problem of recovering K linearly independent combinations over a K-user MAC, i.e., recovering the messages in their entirety via nested linear codes. While the MAC rate region is well-understood for random i.i.d. code ensembles, new techniques are needed to handle the statistical dependencies between competing codeword K-tuples that occur in nested linear code ensembles. This is an important step towards characterizing the general case of recovering $L \leq K$ linear combinations.

On the Sub-optimality of Single-letter Coding in Multi-terminal Communications (11:50)

Farhad Shirani (University of Michigan, USA); Sandeep Pradhan (University Michigan, USA)

We investigate binary block-codes (BBC). A BBC is defined as a vector of Boolean functions. We consider BBCs which are generated randomly, and using single-letter distributions. We characterize the vector of dependency spectrums of these BBCs. We use this vector to upper-bound the correlation between the outputs of two distributed BBCs. Finally, the upper-bound is used to show that the large blocklength single-letter coding schemes in the literature are sub-optimal in some multiterminal communication settings.

Coordination with Clustered Common Randomness in a Three-Terminal Line Network (12:10)

*Ishaque Ashar Kadampot (Georgia Institute of Technology, USA); **Matthieu Bloch** (Georgia Institute of Technology, USA)*

To achieve strong coordination in a network, nodes benefit from access to a source of common randomness. Most studies pertaining to strong coordination assume the existence of a source of common randomness accessible to all nodes in the network. This assumption, however, is not practical in a decentralized network. We analyze the problem of strong coordination in a three-terminal line network with common randomness available only at the first two nodes and assume that the actions of the first node are specified by an external agent. We use coding schemes developed for channel resolvability codes to characterize the strong coordination capacity region when the intermediate node is operating in a functional mode. A comparison of our coordination capacity region with a case in which all nodes have access to a common randomness shows that we have to increase the communication rate between the second and the third nodes to achieve the same coordination distribution.

Th1-1: Lattice Codes 1

Thursday, June 29, 09:50-11:10
Room: Europa
Chair: Stark Draper (University of Toronto, Canada)

Capacity Optimality of Lattice Codes in Common Message Gaussian Broadcast Channels with Coded Side Information (09:50)

Lakshmi Natarajan (Indian Institute of Technology Hyderabad, India); Yi Hong (Monash University, Australia); Emanuele Viterbo (Monash University, Australia)

Lattices possess elegant mathematical properties which have been previously used in the literature to show that structured codes can be efficient in a variety of communication scenarios. We consider the family of single-transmitter multiple-receiver Gaussian channels where the source transmits a set of common messages to all the receivers (multicast scenario), and each receiver has 'coded side information', i.e., prior information in the form of linear combinations of the messages. This channel model is motivated by applications to multi-terminal networks where the nodes may have access to coded versions of the messages from previous signal hops or through orthogonal channels. The capacity of this channel is known and follows from the work of Tuncel (2006), which is based on random coding arguments. In this paper, following the approach introduced by Erez and Zamir, we show that lattice codes are capacity-optimal for this family of

channels. The structured coding scheme proposed in this paper is derived from Construction A lattices designed over prime fields, and utilizes 'algebraic binning' at the decoders to expurgate the channel code and obtain good lattice subcodes, for every possible set of linear combinations available as side information.

On the Communication Cost of Determining an Approximate Nearest Lattice Point (10:10)

Maiara Bollauf *(University of Campinas, Brazil); Vinay Vaishampayan (City Univerity of New York, USA); Sueli Costa (University of Campinas-UNICAMP (Brazil), Brazil)*

We consider the closest lattice point problem in a distributed network setting and study the communication cost and the error probability for computing an approximate nearest lattice point, using the nearest-plane algorithm, due to Babai. Two distinct communication models, centralized and interactive, are considered. The importance of proper basis selection is addressed. Assuming a reduced basis for a two-dimensional lattice, we determine the approximation error of the nearest plane algorithm. The communication cost for determining the Babai point, or equivalently, for constructing the rectangular nearest-plane partition, is calculated in the interactive setting. For the centralized model, an algorithm is presented for reducing the communication cost of the nearest plane algorithm in an arbitrary number of dimensions.

Communication Cost of Transforming a Nearest Plane Partition to the Voronoi Partition (10:30)

Vinay Vaishampayan *(City Univerity of New York, USA); Maiara Bollauf (University of Campinas, Brazil)*

We consider the problem of distributed computation of the nearest lattice point for a two dimensional lattice. An interactive model of communication is considered. We address the problem of reconfiguring a specific rectangular partition, a nearest plane, or Babai, partition, into the Voronoi partition. Expressions are derived for the error probability as a function of the total number of communicated bits. With an infinite number of allowed communication rounds, the average cost of achieving zero error probability is shown to be finite. For the interactive model, with a single round of communication, expressions are obtained for the error probability as a function of the bits exchanged. We observe that the error exponent depends on the lattice.

Compute-and-Forward over Block-Fading Channels Using Algebraic Lattices (10:50)

Shanxiang Lyu (Imperial College London, United Kingdom (Great Britain)); Antonio Campello (Imperial College London, United Kingdom (Great Britain)); Cong Ling (Imperial College London, United Kingdom (Great Britain)); Jean-Claude Belfiore (Telecom Paristech & Huawei Technologies, France)

Previous approaches to compute-and-forward (C&F) are mostly based on quantizing channel coefficients to integers. In this work, we investigate the C&F strategy over block fading channels using Construction A over rings, so as to allow better quantization for the channels. Advantages in decoding error probabilities and computation rates are demonstrated, and the construction is shown to outperform the C&F strategy over the integers $\mathbb{Z}$.

Th1-2: Polar Codes 2

Thursday, June 29, 09:50-11:10
Room: Brussels
Chair: Ruediger Urbanke (EPFL, Switzerland)

Construction of Polar Codes with Sublinear Complexity (09:50)

Marco Mondelli (Stanford University, USA); Hamed Hassani (ETH Zurich, Switzerland); Ruediger Urbanke (EPFL, Switzerland)

Consider the problem of constructing a polar code of block length N for the transmission over a given channel W. Typically this requires to compute the reliability of all the N synthetic channels and then to include those that are sufficiently reliable. However, we know from [1], [2] that there is a partial order among the synthetic channels. Hence, it is natural to ask whether we can exploit it to reduce the computational burden of the construction problem. We show that, if we take advantage of the partial order [1], [2], we can construct a polar code by computing the reliability of roughly $N/\log^{3/2} N$ synthetic channels. Such a set of synthetic channels is universal, in the sense that it allows one to construct polar codes for any W, and it can be identified by solving a maximum matching problem on a bipartite graph. Our proof technique consists of reducing the construction problem to the problem of computing the maximum cardinality of an antichain for a suitable partially ordered set. As such, this method is general and it can be used to further improve the complexity of the construction problem in case a new partial order on the synthetic channels of polar codes is discovered.

On the Error Probability of Short Concatenated Polar and Cyclic Codes with Interleaving (10:10)

Giacomo Ricciutelli (Università Politecnica delle Marche, Italy); Marco Baldi (Università Politecnica delle Marche, Italy); Franco Chiaraluce (Università Politecnica delle Marche, Italy); Gianluigi Liva (DLR - German Aerospace Center, Germany)

In this paper, the analysis of the performance of the concatenation of a (short) polar code with an outer binary linear block code is addressed from a distance spectrum viewpoint. The analysis targets the case where an outer cyclic code is employed together with an inner systematic polar code. A concatenated code ensemble is introduced placing an interleaver at the input of the polar encoder. The introduced ensemble allows deriving bounds on the achievable error rates under maximum likelihood decoding, by applying the union bound to the (expurgated) average weight enumerators. The analysis suggests the need of careful optimization of the outer code, at least in the short block length regime, to attain low error floors.

A Randomized Construction of Polar Subcodes (10:30)

Peter Trifonov *(Saint-Petersburg State Polytechnic University, Russia); Grigorii Trofimiuk (Peter the Great St. Petersburg Polytechnic University, Russia)*

A method for construction of polar subcodes is presented, which aims on minimization of the number of low-weight codewords in the obtained codes, as well as on improved performance under list or sequential decoding with small list size. Simulation results are provided, which show that the obtained codes outperform LDPC and turbo codes.

On Design of CRC Codes for Polar Codes with Successive Cancellation List Decoding (10:50)

Takumi Murata (Yokohama National University, Japan); Hideki Ochiai (Yokohama National University, Japan)

Concatenation of polar codes with cyclic redundancy check (CRC) codes, together with successive cancellation list (SCL) decoding, is known to be an effective approach that can significantly enhance the performance of the original polar codes. Most of the studies on the concatenation of CRC and polar codes, however, pay little attention to the structure of CRC codes themselves, even though the longer CRC may lead to loss in terms of information rate. In this work, we investigate the effect of CRC length on the CRC-concatenated polar code performance by developing an analytical bound for the frame error rate (FER) after the CRC-assisted list decoding. As a result, we reveal that there is a trade-off between the CRC length and FER performance, and for a given target FER, there is the minimum length of CRC that satisfies the FER constraint in high signal-to-noise ratio (SNR). The validity of our analytical framework is confirmed by extensive simulation over an additive white Gaussian noise (AWGN) channel. The results thus offer a useful guideline when designing CRC codes for polar codes with SCL decoding.

Th1-3: Broadcast Channels 3

Thursday, June 29, 09:50-11:10
Room: K2
Chair: Shlomo (Shitz) Shamai (The Technion, Israel)

Block-fading Broadcast Channel with Hybrid CSIT and CSIR (09:50)

Mohamed Fadel (University of Texas at Dallas, USA); Aria Nosratinia (University of Texas, Dallas, USA)

The broadcast channel under delayed, mixed, hybrid, or no CSIT is a subject of much interest but has been studied only under i.i.d. fading and perfect CSIR for all users. Models that go beyond i.i.d. fading and perfect CSIR are of practical importance since users may experience unequal fading block-length (coherence time) and unequal CSIR availability due to different mobility and scattering environment. This paper studies a two-user MISO broadcast channel with hybrid CSIR, where one static user (with slower fading) has CSIR and one dynamic user (with faster fading) does not have free CSIR. Under this hybrid CSIR condition, the paper studies the degrees of freedom under various CSIT scenarios: no, delayed, and hybrid CSIT. For no CSIT, we provide an outer bound that meets the achievable degrees of freedom region when the coherence times of the users are the same. For both delayed and hybrid CSIT, the achievable regions partially meet their corresponding outer bounds, and furthermore the corresponding gaps decrease with the dynamic user coherence time.

Application of Yamamoto-Itoh Coding Scheme to Discrete Memoryless Broadcast Channels (10:10)

Hirosuke Yamamoto (The University of Tokyo, Japan); Shintaro Hara (The University of Tokyo, Japan)

The Yamamoto-Itoh (YI) scheme is a simple two phase coding scheme for discrete memoryless channels with noiseless feedback, which can attain the so-called Burnashev error-exponent. In this paper, we show how we can apply the YI scheme to discrete memoryless broadcast channels, and derive the achievable error-exponents region of the YI scheme for given coding rates.;

Coding Across Heterogeneous Parallel Erasure Broadcast Channels is Useful (10:30)

Sunghyun Kim (ETRI, Korea); Soheil Mohajer (University of Minnesota, USA); Changho Suh (KAIST, Korea)

Motivated by recent efforts to harness millimeter-wave (mmWave) bands, known to have high outage probabilities, we explore a K-user parallel packet-erasure broadcast channel that consists of orthogonal subchannels prone to packet-erasures. Our main result is two-fold. First, in the homogeneous channel where all subchannels have the same erasure probability, we show that the separation principle holds, i.e., coding across subchannels provides no gain. Second, in the heterogeneous channel where the subchannels have different erasure probabilities, we devise a scheme that employs coding across subchannels and show that the principle fails to hold, i.e., coding across subchannels provides a gain. Inspired by this finding, we demonstrate our scheme to be effective in harnessing the mmWave bands. Compared to the current approach in the 4G systems which allocates subchannels to users exclusively, we show that our scheme offers a huge gain. We find the gain to be significant in scenarios where the erasure probabilities are largely different, and importantly to increase with the growth of K. Our result calls for joint coding schemes in future wireless systems to meet growing mobile data demands.

Rate Splitting and Superposition Coding for Concurrent Groupcasting over the Broadcast Channel: A General Framework (10:50)

Henry Romero (MIT Lincoln Laboratory, USA); Mahesh Varanasi (University of Colorado, USA)

A general inner bound is given for the discrete memoryless broadcast channel with an arbitrary number of users and general message sets, a setting that accounts for the most general form of concurrent groupcasting, with up to exponentially many messages intended for any set of subsets of receivers. Achievability is based on superposition coding and rate-splitting, where each receiver jointly decodes both its desired messages as well as the partial interference assigned to it via rate-splitting. The proof of achievability builds on the techniques for the description and analysis of superposition coding recently developed by the authors for the multiple access channel with general messages.

Th1-4: Private Information Retrieval

Thursday, June 29, 09:50-11:10
Room: K3
Chair: Michael Gastpar (EPFL, Switzerland)

Private Information Retrieval from MDS Coded Data with Colluding Servers: Settling a Conjecture by Freij-Hollanti et al (09:50)

Hua Sun (University of California, Irvine, USA); Syed Jafar (University of California Irvine, USA)

A (K,N,T,Kc) instance of the MDS-TPIR problem is comprised of K messages and N distributed servers. Each message is separately encoded through a (Kc,N) MDS storage code. A user wishes to retrieve one message, as efficiently as possible, while revealing no information about the desired message index to any colluding set of up to T servers. The fundamental limit on the efficiency of retrieval, i.e., the capacity of MDS-TPIR is known only at the extremes where either T or Kc belongs to 1,N. The focus of this work is a recent conjecture by Freij-Hollanti, Gnilke, Hollanti and Karpuk which offers a general capacity expression for MDS-TPIR. We prove that the conjecture is false by presenting as a counterexample a PIR scheme for the setting (K,N,T,Kc) = (2,4,2,2), which achieves the rate 3/5, exceeding the conjectured capacity, 4/7.

Multi-Message Private Information Retrieval (10:10)

Karim Banawan (University of Maryland, USA); Sennur Ulukus (University of Maryland, USA)

We consider the problem of multi-message private information retrieval (MPIR) from N non-communicating replicated databases. In MPIR, the user is interested in retrieving P messages out of M stored messages without leaking the identity of the retrieved messages. The information-theoretic sum capacity of MPIR C_s^P is the maximum number of desired message symbols that can be retrieved privately per downloaded symbol. For the case $P \geq \frac{M}{2}$, we determine the exact sum capacity of MPIR as $C_s^P = \frac{1}{1+\frac{M-P}{PN}}$. For $P \leq \frac{M}{2}$, we develop lower and upper bounds for all M, P, N. These bounds match if the number of messages M is an integer multiple of the number of desired messages P, in which case, $C_s^P = \frac{1-\frac{1}{N}}{1-(\frac{1}{N})^{M/P}}$. Our results indicate that joint retrieval of desired messages is more efficient than successive use of single-message retrieval schemes.

Robust Private Information Retrieval on Coded Data (10:30)

Razane Tajeddine *(Illinois Institute of Technology, USA); Salim El Rouayheb (Illinois Institute of Technology, USA)*

We consider the problem of designing PIR scheme

on coded data when certain nodes are unresponsive. We provide the construction of ν-robust PIR schemes that can tolerate up to ν unresponsive nodes. These schemes are adaptive and universally optimal in the sense of achieving (asymptotically) optimal download cost for any number of unresponsive nodes up to ν.

Private Information Retrieval Schemes for Coded Data with Arbitrary Collusion Patterns (10:50)

Razane Tajeddine (Illinois Institute of Technology, USA); Oliver Gnilke (Aalto University, Finland); David Karpuk (Aalto University, Finland); Ragnar Freij-Hollanti (Aalto University, Finland); ***Camilla Hollanti*** *(Aalto University, Finland); Salim El Rouayheb (Illinois Institute of Technology, USA)*

In Private Information Retrieval (PIR), one wants to download a file from a database without revealing to the database which file is being downloaded. Much attention has been paid to the case of the database being encoded across several servers, subsets of which can collude to attempt to deduce the requested file. With the goal of studying the achievable PIR rates in realistic scenarios, we generalize results for coded data from the case of all subsets of servers of size t colluding, to arbitrary subsets of the servers. We investigate the effectiveness of previous strategies in this new scenario, and present new results in the case where the servers are partitioned into disjoint colluding groups.

Th1-5: Rate Distortion Theory 2

Thursday, June 29, 09:50-11:10
Room: K4
Chair: Tsachy Weissman (Stanford University, USA)

A Distortion Based Approach for Protecting Inferences (09:50)

Chi-Yo Tsai (UCLA, USA); Gaurav Kumar Agarwal (University of California Los Angeles, USA); Christina Fragouli (UCLA, USA); Suhas Diggavi (University of California Los Angeles, USA)

Eavesdropping attacks in inference systems aim to learn not the raw data, but the system inferences to predict and manipulate system actions. We argue that conventional entropy measures can be ambiguous on the adversary's estimation abilities, and adopt instead a distortion based framework. We show that requiring perfect distortion-based security is more frugal than requiring perfect entropy- based secrecy even for block length 1 codes, offering in some cases unbounded gains. Within this framework, we design algorithms that enable to efficiently use shared randomness, and show that each shared random key is exponentially useful in security.

Rate-Distortion Regions of Instances of Cascade Source Coding with Side Information (10:10)

Chien-Yi Wang (Télécom ParisTech, France); Abdellatif Zaidi (Université Paris-Est Marne La Vallée, France)

In this work, we study a three-terminal cascade source coding problem with side information Y_1 known to the source encoder and the first user, and side information Y_2 known only to the second user. Each user wants to reconstruct some desired function of the source, lossily, to within some fidelity level. We establish single-letter characterization of the rate-distortion region of this model in some important special cases, including when the reconstruction is lossless at the first user. We then establish a connection among the studied model and the so-called side information-scalable source coding problem (i.e., Heegard-Berger problem with side information and successive refinement) to infer single-letter characterization of the rate-distortion region of some instances of the latter problem. In contrast with most previous related works, the results of this paper hold irrespective of the ordering among the source and side information sequences, which are then arbitrarily correlated.

The Rate-Distortion Function for Successive Refinement of Abstract Sources (10:30)

Victoria Kostina (California Institute of Technology, USA); Ertem Tuncel (UC Riverside, USA)

In successive refinement of information, the decoder refines its representation of the source progressively as it receives more encoded bits. The rate-distortion region of successive refinement describes the minimum rates required to attain the target distortions at each decoding stage. In this paper, we derive a parametric characterization of the rate-distortion region for successive refinement of abstract sources. Our characterization extends Csiszár's result to successive refinement, and generalizes a result by Tuncel and Rose, applicable for finite alphabet sources, to abstract sources. The new characterization leads to a family of outer bounds to the rate-distortion region. It also enables new nonasymptotic converse bounds.

Rate-Distortion Tradeoffs under Kernel-Based Distortion Measures (10:50)

Kazuho Watanabe *(Toyohashi University of Technology, Japan)*

Kernel methods have been used for turning linear learning algorithms into nonlinear ones. These nonlinear algorithms measures distances between data points by the distance in the kernel-induced feature space. In lossy data compression, the optimal tradeoff between the number of quantized points and the incurred distortion is characterized by the rate-distortion function. However, the rate-distortion functions associated with

distortion measures involving kernel feature mapping have yet to be analysed. We consider two reconstruction schemes, reconstruction in input space and reconstruction in feature space, and provide bounds to the rate-distortion functions for these schemes. Comparison of the derived bounds to the quantizer performance obtained by the kernel K-means method suggests that the rate-distortion bounds for input space and feature space reconstructions are informative at low and high distortion levels, respectively.

Th1-6: Coding for Insertion and Deletion Channels 1

Thursday, June 29, 09:50-11:10
Room: K5
Chair: Joseph Jean Boutros (Texas A&M University, USA)

Coding for the Permutation Channel with Insertions, Deletions, Substitutions, and Erasures (09:50)

Mladen Kovačević *(National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore)*

This paper is motivated by the error-control problem in communication channels in which the transmitted sequences are subjected to random permutations, in addition to being impaired with insertions, deletions, substitutions, and erasures of symbols. Bounds on the size of optimal codes in this setting are derived, and their asymptotic behavior examined in the fixed-minimum-distance regime. A family of codes correcting these types of errors is described and is shown to be asymptotically optimal for some sets of parameters. The corresponding error-detection problem is also analyzed.

Perfect Codes for Single Balanced Adjacent Deletions (10:10)

Manabu Hagiwara (Chiba University, Japan)

Two classes of perfect codes for single balanced adjacent deletions are provided. These classes are inspired by Levenshtein's work on binary perfect codes for single standard deletion. One of the classes is defined via the inversion number and the other is defined via Levenshtein codes. The first half of this paper is devoted to the proof of perfectness and the other is devoted to discussion on the other properties of the provided codes.

Timing-Drift Channel Model and Marker-Based Error Correction Coding (10:30)

Haruhiko Kaneko *(Tokyo Institute of Technology, Japan)*

Several types of insertion/deletion/substitution error correction codings have been proposed for channels with imperfect synchronization. Most of the conventional coding schemes assume insertion/deletion errors of bit granularity, while in some applications, e.g. bit patterned media recording, insertion/deletion errors occur as a result of accumulation of small synchronization errors. This paper considers a fractional insertion/deletion error channel in which a fraction of bit (i.e., $1/\nu$-bit) is inserted and deleted, and describes application of conventional marker-based IDS error correction coding to the channel. Also simulation results show bit error rates of the marker-based coding.

Limits to List Decoding of Insertions and Deletions (10:50)

Antonia Wachter-Zeh (Technical University of Munich (TUM), Germany)

List decoding of insertions and deletions in the Levenshtein metric is considered. In this paper, a Johnson-like upper bound on the maximum list size when decoding in the Levenshtein metric is derived. This bound depends only on the length and minimum Levenshtein distance of the code, the length of the received word, and the alphabet size. It shows that polynomial-time list decoding beyond half the Levenshtein distance is possible for many parameters. For example, list decod- ing of two insertions/deletions with the well-known Varshamov- Tenengolts (VT) codes is feasible. Further, we also show a lower bound on list decoding VT codes and an efficient list decoding algorithm for two insertions/deletions with VT codes.

Th1-7: Security 4

Thursday, June 29, 09:50-11:10
Room: K6
Chair: Lifeng Lai (University of California, Davis, USA)

The Gelfand-Pinsker wiretap channel: Higher secrecy rates via a novel superposition code (09:50)

Ziv Goldfeld (Ben Gurion University, Israel); Paul Cuff (Princeton University, USA); Haim Permuter (Ben-Gurion University, Israel)

We study the state-dependent (SD) wiretap channel (WTC) with non-causal channel state information (CSI) at the encoder. This model subsumes all other instances of CSI availability as special cases, and calls for an efficient utilization of the state sequence both for reliability and security purposes. A lower bound on the secrecy-capacity, that improves upon the previously

best known result by Chen and Han Vinck, is derived based on a novel superposition coding scheme. The improvement over the Chen and Han Vinck result is strict for some SD-WTCs. Specializing the lower bound to the case where CSI is also available to the decoder reveals that it is at least as good as the achievable formula by Chia and El-Gamal, which is already known to outperform the adaptation of the Chen and Han Vinck code to the encoder and decoder CSI scenario. The results are derived under the strict semantic-security metric that requires negligible information leakage for all message distributions. The proof of achievability relies on a stronger version of the soft-covering lemma for superposition codes.

The Gaussian Multiple Access Wiretap Channel when the Eavesdropper can Arbitrarily Jam (10:10)

Remi Chou (Pennsylvania State University, USA); Aylin Yener (Pennsylvania State University, USA)

We study the Gaussian multiple access channel in presence of an adversary, who is simultaneously able to eavesdrop and jam, i.e., an active wiretapper. We assume that the adversary has a power constraint, which she can utilize to have any arbitrary jamming strategy. The multiple access channel between the legitimate transmitters and the receiver thus becomes arbitrarily varying. We derive inner and outer bounds on the secrecy rate region of our model. In the case of a degraded channel, we characterize the optimal secrecy sum-rate, and within 0.5 bits per channel use the optimal individual rate constraints. As a special case, we obtain the secrecy capacity of the point-to-point Gaussian wiretap channel when the eavesdropper is able to arbitrarily jam.

Secrecy Capacity of the First-Order Autoregressive Moving Average Gaussian Channel with Feedback (10:30)

Chong Li (Qualcomm R&D, USA); Yingbin Liang (Syracuse University, USA)

In this paper, we consider the first-order autoregressive moving average Gaussian channel with perfect causal feedback where an eavesdropper receives noisy observations of the channel inputs and outputs. We show that the secrecy capacity is equal to the feedback capacity without the presence of eavesdropper. Furthermore, we explicitly construct the secrecy capacity-achieving feedback code, which is deterministic and simple to implement.

Asymptotic Converse Bound for Secret Key Capacity in Hidden Markov Model (10:50)

Mohammad Reza Khalili Shoja (Iowa State University, USA); George Amariucai (Iowa State University, USA); Zhengdao Wang (Iowa State University, USA); Shuangqing Wei (Louisiana State University, USA); Jing Deng (University of North Carolina at Greensboro, USA)

Secret key establishment from common randomness has been traditionally investigated under certain limiting assumptions, of which the most ubiquitous appears to be that the information available to all parties comes in the form of independent and identically distributed (i.i.d.) samples of some correlated random variables. Unfortunately, models employing the i.i.d assumption are often not accurate representations of real scenarios. A more capable model would represent the available information as correlated hidden Markov models (HMMs), based on the same underlying Markov chain. Such a model accurately reflects the scenario where all parties have access to imperfect observations of the same source random process, exhibiting a certain time dependency. In this paper, we derive a computationally-efficient asymptotic converse bound for the secret key capacity of the correlated-HMM scenario. The main obstacle, not only for our model, but also for other non-i.i.d cases, is the computational complexity. We address this by converting the initial bound to a product of Markov random matrices, and using recent results regarding its convergence to a Lyapunov exponent. The methods developed in the paper are easily extensible to derive a secret-key capacity lower bound.

Th1-8: Quantum IT 4

Thursday, June 29, 09:50-11:10
Room: K7+8
Chair: Stefan Wolf (USI Lugano, Switzerland)

Compression for quantum population coding (09:50)

Yuxiang Yang (The University of Hong Kong, Hong Kong); Ge Bai (The University of Hong Kong, Hong Kong); Giulio Chiribella (The University of Hong Kong, Hong Kong); Masahito Hayashi (Nagoya University, Japan)

We study the compression of arbitrary parametric families of n identically prepared finite-dimensional quantum states, in a setting that can be regarded as a quantum analogue of population coding. For a family with f free parameters, we propose an asymptotically faithful protocol that requires a memory of overall size (f/2)log n. Our construction uses a quantum version of local asymptotic normality and, as an intermediate step, solves the problem of the optimal compres-

sion of n identically prepared displaced thermal states. Our protocol achieves the ultimate bound predicted by quantum Shannon theory. In addition, we explore the minimum requirement for quantum memory: On the one hand, the amount of quantum memory used by our protocol can be made arbitrarily small compared to the overall memory cost; on the other hand, any protocol using only classical memory cannot be faithful.

Moderate Deviations for Quantum Hypothesis Testing and a Martingale Inequality (10:10)

Hao-Chung Cheng (National Taiwan University, Taiwan); Min-Hsiu Hsieh (University of Technology Sydney, Australia)

We study the asymptotic behavior of the type-I error in quantum hypothesis testing when the exponent of the type-II error approaches the quantum relative entropy sufficiently slowly. Our result shows that the moderate deviation principle holds for the testing problem if the quantum relative variance is positive. Our proof strategy employs strong large deviation theory and a martingale inequality.

Classical-Quantum Arbitrarily Varying Wiretap Channel: Secret Message Transmission under Jamming Attacks (10:30)

Minglai Cai *(Technische Universität München, Germany); Holger Boche (Technical University Munich, Germany); Christian Deppe (University of Bielefeld, Germany); Janis Noetzel (Technische Universität Dresden, Germany)*

We analyze arbitrarily varying classical-quantum wiretap channels. These channels are subject to two attacks at the same time: one passive (eavesdropping), and one active (jamming). We progress on previous works by introducing a reduced class of allowed codes that fulfills a more stringent secrecy requirement than earlier definitions. In addition, we prove that non-symmetrizability of the legal link is sufficient for equality of the deterministic and the common randomness assisted secrecy capacities. At last, we focus on analytic properties of both secrecy capacities: We completely characterize their discontinuity points, and their super-activation properties.

Quantum Markov Chains and Logarithmic Trace Inequalities (10:50)

David Sutter (ETH Zurich, Switzerland); Mario Berta (California Institute of Technology, USA); Marco Tomamichel (University of Technology Sydney, Australia)

A Markov chain is a tripartite quantum state ρ_{ABC} where there exists a recovery map $R_{B\to BC}$ such that $\rho_{ABC} = R_{B\to BC}(\rho_{AB})$. More generally, an approximate Markov chain ρ_{ABC} is a state whose distance to the closest recovered state $R_{B\to BC}(\rho_{AB})$ is small. Recently it has been shown that this distance can be bounded from above by the conditional mutual information $I(A:C|B)_\rho$ of the state. We improve on this connection by deriving the first bound that is tight in the commutative case and features an explicit and universal recovery map. The key tool in our proof is a multivariate extension of the Golden-Thompson inequality, which allows us to extend logarithmic trace inequalities from two to arbitrarily many matrices.

Th1-9: Source Coding 4

Thursday, June 29, 09:50-11:10
Room: K9
Chair: Yasutada Oohama (University of Electro-Communications, Japan)

Distributed Task Encoding (09:50)

Annina Bracher (Swiss Re, Switzerland); Amos Lapidoth (ETHZ, Switzerland); ***Christoph Pfister*** *(ETH Zurich, Switzerland)*

The rate region of the task-encoding problem for two correlated sources is characterized using a novel parametric family of dependence measures. The converse uses a new expression for the ρ-th moment of the list size, which is derived using the relative α-entropy.

Performance Limits on the Classification of Kronecker-structured Models (10:10)

Ishan Jindal (Wayne State University, USA); Matthew Nokleby (Wayne State University, USA)

Kronecker-structured (K-S) models recently have been proposed for the efficient representation, processing, and classification of multidimensional signals such as images and video. Because they are tailored to the multi-dimensional structure of the target images, K-S models show improved performance in compression and reconstruction over more general (union of) subspace models. In this paper, we study the classification performance of Kronecker-structured models in two asymptotic regimes. First, we study the diversity order, the slope of the error probability as the signal noise power goes to zero. We derive an exact expression for the diversity order as a function of the signal and subspace dimensions of a K-S model. Next, we study the classification capacity, the maximum rate at which the number of classes can grow as the signal dimension goes to infinity. We derive upper and lower bounds on the prelog factor of the classification capacity. Finally, we evaluate the empirical classification performance of K-S models, showing that they agree with the diversity order analysis.

The Redundancy Gains of Almost Lossless Universal Source Coding over Envelope Families (10:30)

Jorge Silva (University of Chile, Chile); Pablo Piantanida (CentraleSupélec-CNRS-Université Paris-Sud, France)

The problem of almost lossless universal coding is revisited in this work. We study uniform rate of convergence for distortion and redundancy over a family of envelope distributions. In particular, we show that an almost lossless coding scheme offers faster rate of convergence for the (minimax) redundancy compared with the well-known information radius developed for the lossless case at the expense of tolerating a non-zero distortion that vanishes to zero as the block-length grows. Our results show that even when lossless universality is feasible, an almost lossless scheme can still offer different regimes on the rates of convergence of the redundancy versus the distortion.

Universal Sampling Rate Distortion (10:50)

Vinay Praneeth Boda (University of Maryland, College Park, USA); Prakash Narayan (University of Maryland, USA)

We examine the coordinated and universal rate-efficient sampling of a subset of correlated discrete memoryless sources followed by lossy compression of the sampled sources. The goal is to reconstruct a predesignated subset of sources within a specified level of distortion. The combined sampling mechanism and rate distortion code are universal in that they are devised to perform robustly without exact knowledge of the underlying probability distribution of the sources. Single-letter characterizations are provided for a universal sampling rate distortion function for fixed-set and independent random sampling.

Th2-1: Coding Techniques 3

Thursday, June 29, 11:30-12:50
Room: Europa
Chair: Vladimir Sidorenko (Technical University of Munich, Germany)

Cooling Codes: Thermal-Management Coding for High-Performance Interconnects (11:30)

*Tuvi Etzion (Technion-Israel Institute of Technology, Israel); Alexander Vardy (University of California San Diego, USA); Yeow Meng Chee (Nanyang Technological University, Singapore); **Han Mao Kiah** (Nanyang Technological University, Singapore)*

High temperatures have dramatic negative effects on interconnect performance. Numerous techniques have been proposed to reduce the power dissipation of on-chip buses but they fall short of fully addressing the thermal challenges posed by high-performance interconnects. We introduce new efficient coding schemes that directly control the peak temperature of a bus by effectively cooling its hottest wires. This is achieved by avoiding state transitions on the hottest wires for as long as necessary until their temperature drops off. At the same time, we reduce the average power consumption by ensuring that the total number of state transitions on all the wires is bounded. Our solutions call for redundancy: we use $n > k$ wires to encode a given k-bit bus. Therefore, it is important to determine the minimum possible number of wires n needed to encode k bits while satisfying the desired properties. We provide full analysis in each case, and show that the number of additional wires required to cool the t hottest wires is negligible when k is large. Moreover, the resulting encoders and decoders are fully practical. They do not require significant computational overhead and can be implemented without sacrificing a large circuit area.

Recursive Block Markov Superposition Transmission of Short Codes (11:50)

Shancheng Zhao (Jinan University, P.R. China); Qin Huang (Beihang University, Beijing, P.R. China); Xiao Ma (Sun Yat-sen University, P.R. China); Baoming Bai (Xidian University, P.R. China)

Extensive studies have demonstrated the effectiveness of constructing capacity-approaching codes by block Markov superposition transmission (BMST). However, to achieve high performance, BMST codes typically require large encoding memories and large decoding window sizes, which result in increased decoding complexity and decoding latency. To address this issue, we introduce the recursive BMST (rBMST), in which block-oriented feedback convolutional code is used instead of the block-oriented feedforward convolutional code. We propose to use a modified extrinsic information transfer (EXIT) chart analysis to study the convergence behavior of rBMST codes. On one hand, rBMST code shares most merits of BMST code, including near-capacity performance, low-complexity encoding, and flexible construction. On the other hand, compared with BMST code, rBMST code requires a smaller encoding memory, hence a lower decoding complexity, to approach the capacity. In particular, analytical results show that, rBMST code ensemble with encoding memory three reveals a lower error-floor than the BMST code ensemble with encoding memory twelve.

Complete Characterization of the Solvability of PAPR Reduction for OFDM by Tone Reservation (12:10)

Holger Boche (Technical University Munich, Germany); Ullrich Mönich (Technische Universität München, Germany); Ezra Tampubolon (Technische Universität München, Germany)

In this paper we analyze the peak-to-average power ratio (PAPR) reduction by tone reservation for orthogonal frequency division multiplexing (OFDM) schemes. In addition to the strong solvability of the PAPR reduction problem, where the PAPR has to be bounded by some constant, we consider a weaker form of solvability, where only the boundedness of the peak value of the signal is required. We show that for OFDM both forms of solvability are equivalent. Further, we show that in the case where the PAPR problem is not solvable, the set of input signals that lead to an unbounded OFDM signal is a residual set. As a consequence, if the upper density of the carriers, used for information transmission, is positive, the set of input signals that lead to a bounded OFDM signal is a meager set.

Construction of q-ary Constant Weight Sequences using a Knuth-like Approach (12:30)

Elie Ngomseu Mambou *(University of Johannesburg, South Africa); Theo Swart (University of Johannesburg, South Africa)*

We present an encoding and decoding scheme for constant weight sequences, that is, given an information sequence, the construction results in a sequence of specific weight within a certain range. The scheme uses a prefix design that is based on Gray codes. Furthermore, by adding redundant symbols we extend the range of weight values for output sequences, which is useful for some applications.

Th2-2: Locally Repairable Codes 3

Thursday, June 29, 11:30-12:50
Room: Brussels
Chair: P Vijay Kumar (Indian Institute of Science, India)

Bounds and Constructions for Linear Locally Repairable Codes over Binary Fields (11:30)

Anyu Wang (Institute of Information Engineering, Chinese Academy of Sciences, P.R. China); Zhifang Zhang (Academy of Mathematics and Systems Science, Chinese Academy of Sciences, P.R. China); Dongdai Lin (Institute of Information Engineering, Chinese Academy of Sciences, P.R. China)

For binary $[n, k, d]$ linear locally repairable codes (LRCs), two new upper bounds on k are derived. The first one applies to LRCs with disjoint local repair groups, for general values of n, d and locality r, containing some previously known bounds as special cases. The second one is based on solving an optimization problem and applies to LRCs with arbitrary structure of local repair groups. Particularly, an explicit bound is derived from the second bound when $d \geq 5$. A specific comparison shows this explicit bound outperforms the Cadambe-Mazumdar bound for $5 \leq d \leq 8$ and large values of n. Moreover, a construction of binary linear LRCs with $d \geq 6$ attaining our second bound is provided.

Locally Repairable Codes with Multiple (r_i, δ_i)-Localities (11:50)

Bin Chen (South China Normal University, P.R. China); Shutao Xia (Tsinghua University, P.R. China); Jie Hao (Tsinghua University, P.R. China)

In distributed storage systems, locally repairable codes (LRCs) are introduced to realize low disk I/O and repair cost. In order to tolerate multiple node failures, the LRCs with (r, δ)-*locality* are further proposed. Since hot data is not uncommon in a distributed storage system, both Zeh *et al.* and Kadhe *et al.* focus on the LRCs with *multiple localities or unequal localities* (ML-LRCs) recently, which said that the localities among the code symbols can be different. ML-LRCs are attractive and useful in reducing repair cost for hot data. In this paper, we generalize the ML-LRCs to the (r, δ)-locality case of multiple node failures, and define an LRC with multiple $(r_i, \delta_i)_{i\in[s]}$ localities ($s \geq 2$), where $r_1 \leq r_2 \leq \cdots \leq r_s$ and $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_s \geq 2$. Such codes ensure that some hot data could be repaired more quickly and have better failure-tolerance in certain cases because of relatively smaller r_i and larger δ_i. Then, we derive a Singleton-like upper bound on the minimum distance for the proposed LRCs by employing the regenerating-set technique. Finally, we obtain a class of explicit and structured constructions of optimal ML-LRCs, and further extend them to the cases of multiple $(r_i, \delta)_{i\in[s]}$ localities.

epsilon-MSR Codes with Small Sub-packetization (12:10)

Ankit Singh Rawat (Massachusetts Institute of Technology, USA); Itzhak Tamo (Tel Aviv University, Israel); Venkatesan Guruswami (Carnegie Mellon University, USA); Klim Efremenko (Tel Aviv University, Israel)

Minimum storage regenerating (MSR) codes form a special class of maximum distance separable (MDS) codes by providing mechanisms for exact regeneration of a single code block in their codewords by downloading the minimum amount of information from the remaining code blocks. As a result, the MSR codes find application to distributed storage systems to enable node repairs with the optimal repair bandwidth. How-

ever, the construction of exact-repairable MSR codes requires working with a large sub-packetization level, which restricts the employment of these codes in practice. This paper explores exact-repairable MDS codes that significantly reduce the required sub-packetization level by achieving slightly sub-optimal repair bandwidth as compared to the MSR codes. This paper presents a general approach to combine an MSR code with large sub-packetization level with a code with large enough minimum distance to construct exact-repairable MDS codes with small sub-packetization level and near-optimal repair bandwidth. For a given number of parity blocks, the codes constructed using this approach have their sub-packetization level scaling logarithmically with the code length. In addition, the obtained codes require field size linear in the code length and ensure load balancing among the intact code blocks in terms of the information downloaded from these blocks during a node repair.

An Explicit, Coupled-Layer Construction of a High-Rate MSR Code with Low Sub-Packetization Level, Small Field Size and $d < (n-1)$ (12:30)

Birenjith Sasidharan (Indian Institute of Science, India); Myna Vajha (Indian Institute of Science, India); P Vijay Kumar (Indian Institute of Science & University of Southern California, India)

This paper presents an explicit construction for an $((n = 2qt, k = 2q(t-1), d = n-(q+1)), (\alpha = q(2q)^{t-1}, \beta = \frac{\alpha}{q}))$ regenerating code over a field $\mathbb{F}_Q$ operating at the Minimum Storage Regeneration (MSR) point. The MSR code can be constructed to have rate k/n as close to 1 as desired, sub-packetization level $\alpha \leq r^{\frac{n}{r}}$ for $r = (n-k)$, field size Q no larger than n and where all code symbols can be repaired with the same minimum data download. This is the first-known construction of such an MSR code for $d < (n-1)$.

Th2-3: Multicell and Cloud Radio

Thursday, June 29, 11:30-12:50
Room: K2
Chair: Salman Avestimehr (University of Southern California, USA)

An Upper Bound on the Sum Capacity of the Downlink Multicell Processing with Finite Backhaul Capacity (11:30)

Tianyu Yang (Southeast University, P.R. China); Nan Liu (Southeast University, P.R. China); Wei Kang (Southeast University, P.R. China); Shlomo (Shitz) Shamai (The Technion, Israel)

In this paper, we study upper bounds on the sum capacity of the downlink multicell processing model with finite backhaul capacity for the simple case of 2 base stations and 2 mobile users. It is modeled as a two-user multiple access diamond channel. It consists of a first hop from the central processor to the base stations via orthogonal links of finite capacity, and the second hop from the base stations to the mobile users via a Gaussian interference channel. The converse is derived using the converse tools of the multiple access diamond channel and that of the Gaussian MIMO broadcast channel. Through numerical results, it is shown that our upper bound improves upon the existing upper bound greatly in the medium backhaul capacity range, and as a result, the gap between the upper bounds and the sum rate of the time-sharing of the known achievable schemes is significantly reduced.

Capacity Bounds on the Downlink of Symmetric, Multi-Relay, Single Receiver C-RAN Networks (11:50)

Shirin Saeedi Bidokhti (Stanford University, USA); Gerhard Kramer (Technical University of Munich, Germany); Shlomo (Shitz) Shamai (The Technion, Israel)

The downlink of symmetric Cloud Radio Access Networks (C-RAN) with multiple relays and a single receiver is studied. Lower and upper bounds are derived on the capacity. The lower bound is achieved by Marton's coding which facilitates dependence among the multiple-access channel inputs. The upper bound uses Ozarow's technique to augment the system with an auxiliary random variable. The bounds are studied over scalar Gaussian C-RANs and are shown to meet and characterize the capacity for interesting regimes of operation.

On the Capacity of Cloud Radio Access Networks (12:10)

Shouvik Ganguly (University of California, San Diego, USA); Young-Han Kim (UCSD, USA)

Uplink and downlink cloud radio access networks are modeled as two-hop K-user L-relay networks, whereby small base-stations act as relays and are connected to a central processor via orthogonal links of finite capacity. Simplified versions of noisy network coding and distributed decode-forward are used to establish inner bounds on the capacity region for uplink and downlink communications, respectively. Through a careful analysis, the uplink inner bound is shown to achieve the cutset bound on the capacity region universally within O(log L) bits per user. The downlink inner bound achieves the cutset bound with a slightly looser gap of O(log(KL)). These tight per-user gap results are extended to the situations in which the nodes have multiple antennas.

On the Capacity of Cloud Radio Access Networks with Oblivious Relaying (12:30)

Inaki Estella (Huawei Technologies Co., Ltd., France); Abdellatif Zaidi (Université Paris-Est Marne La Vallée, France); Giuseppe Caire (Technische Universität Berlin, Germany); Shlomo (Shitz) Shamai (The Technion, Israel)

We study the transmission over a network in which users send information to a remote destination through relay nodes that are connected to the destination via finite-capacity error-free links, i.e., a cloud radio access network. The relays are constrained to operate without knowledge of the users codebooks, i.e., they perform oblivious processing – The destination, or central processor, however, is informed about the users' codebooks. We establish a single-letter characterization of the capacity region of this model for a class of discrete memoryless channels in which the outputs at the relay nodes are independent given the users' inputs. We show that both relaying à-la Cover-El Gamal, i.e., compress-and-forward with joint decompression and decoding, and "noisy network coding", are optimal. The proof of the converse part establishes, and utilizes, connections with the Chief Executive Officer (CEO) source coding problem under logarithmic loss distortion measure. Extensions to general discrete memoryless channels are also investigated. In this case, we establish inner and outer bounds on the capacity region. For memoryless Gaussian channels within the studied class of channels, we characterize the capacity under Gaussian channel inputs.

Th2-4: Channel Capacity 3

Thursday, June 29, 11:30-12:50
Room: K3
Chair: Muriel Médard (MIT, USA)

Intrinsic Capacity (11:30)

Shengtian Yang (Zhejiang Gongshang University, P.R. China); Rui Xu (McMaster University, Canada); Jun Chen (McMaster University, Canada); Jian-Kang Zhang (McMaster University, Canada)

Every channel can be expressed as a convex combination of deterministic channels with each deterministic channel corresponding to one particular intrinsic state. Such convex combinations are in general not unique, each giving rise to a specific intrinsic-state distribution. In this paper we study the maximum and the minimum capacities of a channel when the realization of its intrinsic state is causally available at the encoder and/or the decoder. Several conclusive results are obtained for binary-input channels and binary-output channels. Byproducts of our investigation include a generalization of the Birkhoff-von Neumann theorem and a condition on the uselessness of causal state information at the encoder.

Gaussian Channels with Minimum Amplitude Constraints: When is Optimal Input Binary? (11:50)

Zhengwei Ni (National University of Singapore, Singapore); Mehul Motani (National University of Singapore, Singapore)

In this paper, we consider a scalar Gaussian Channel with minimum amplitude constraint, and investigate when the capacity-achieving input is binary. First, we study the case that the input satisfies both minimum and peak amplitude constraints and find that the optimal input is discrete. Then, for a given minimum amplitude, we find sufficient conditions that the peak amplitude constraint must satisfy such that the optimal input is binary and when it is not binary. Similarly, for a given peak amplitude, we find sufficient conditions that the minimum amplitude constraint must satisfy such that the optimal input is binary and when it is not binary. Finally, we find that when the input satisfies minimum amplitude and average power constraints, the optimal input is not binary, regardless of whether there is also a peak amplitude constraint.

On the Achievable Rate of Bandlimited Continuous-Time 1-Bit Quantized AWGN Channels (12:10)

Sandra Bender (TU Dresden, Germany); Meik Dörpinghaus (TU Dresden, Germany); Gerhard Fettweis (Technische Universität Dresden, Germany)

We consider a continuous-time bandlimited additive white Gaussian noise channel with 1-bit output quantization. On such a channel the information is carried by the temporal distances of the zero-crossings of the transmit signal. The set of input signals is constrained by the bandwidth of the channel and an average power constraint. Under a set of assumptions, we derive a lower bound on the capacity by lower-bounding the achievable rate for a given set of waveforms with exponentially distributed zero-crossing distances. We focus on the behaviour in the high signal-to-noise ratio regime and characterize the achievable rate depending on the available bandwidth and the signal-to-noise ratio.

Single-Bit Quantization of Binary-Input, Continuous-Output Channels (12:30)

Brian Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan); Hideki Yagi (University of Electro-Communications, Japan)

A binary-input, memoryless channel with a continuous-valued output quantized to one bit is considered. For arbitrary noise models, conditions on an optimal quantizer, in the sense of maximizing mutual information between the channel input and the quantizer output, are given. This result is obtained by considering the

"backward" channel and applying Burshtein et al.'s theorem on optimal classification. In this backward channel, there exists an optimal quantizer for which the quantizer preimage is convex. It is possible no optimal forward quantizer is convex, but by working with the backward channel, this optimal quantizer may be found.

Th2-5: Estimation 1

Thursday, June 29, 11:30-12:50
Room: K4
Chair: H. Vincent Poor (Princeton University, USA)

Lower Bounds on Parameter Modulation-Estimation Under Bandwidth Constraints (11:30)

Nir Weinberger *(Technion, Israel); Neri Merhav (Technion, Israel)*

The problem of modulating the value of a parameter onto a band-limited signal to be transmitted over a continuous-time, additive white Gaussian noise (AWGN) channel, and estimating this parameter at the receiver, is considered. The performance is measured by the mean power-α error (MPαE), which is defined as the worst-case αth order moment of the absolute estimation error. The optimal exponential decay rate of the MPαE as a function of the transmission time, is investigated. Two upper (converse) bounds on the MPαE exponent are derived, on the basis of known bounds for the AWGN channel of inputs with unlimited bandwidth. The bounds are computed for typical values of the error moment and the signal-to-noise ratio (SNR), and the SNR asymptotics of the different bounds are analyzed. The new bounds are compared to known converse and achievability bounds, which were derived from channel coding considerations.

Multi-Layer Generalized Linear Estimation (11:50)

Andre Manoel (Neurospin, CEA, Université Paris-Saclay, France); Florent Krzakala (Ecole Normale Superieure, France); Marc Mézard (École Normale Supérieure, France); Lenka Zdeborova (Institut de Physique Theorique IPhT, CEA Saclay and CNRS, France)

We consider the problem of reconstructing a signal from multi-layered (possibly) non-linear measurements. Using standard but non-rigorous methods from statistical physics we present the Multi-Layer Approximate Message Passing (ML-AMP) algorithm for computing marginal probabilities of the corresponding estimation problem and derive the associated state evolution equations to analyze its performance. We also give the expression of the asymptotic free energy and the minimal information-theoretically achievable reconstruction error. Finally, we present some applications of this measurement model for compressed sensing and perceptron learning with structured matrices/patterns, and for a simple model of estimation of latent variables in an auto-encoder.

Minimax Optimal Estimators for Additive Scalar Functionals of Discrete Distributions (12:10)

Kazuto Fukuchi *(University of Tsukuba & Graduate School of Systems and Information Engineering, Japan); Jun Sakuma (University of Tsukuba, Japan)*

In this paper, we consider estimators for an *additive functional* of ϕ, which is defined as $\theta(P;\phi) = \sum_{i=1}^{k} \phi(p_i)$, from n i.i.d. random samples drawn from a discrete distribution $P = (p_1, ..., p_k)$ with alphabet size k. We propose a minimax optimal estimator for the estimation problem of the additive functional. We reveal that the minimax optimal rate is characterized by the *divergence speed* of the fourth derivative of ϕ if the divergence speed is high. As a result, we show there is no consistent estimator if the divergence speed of the fourth derivative of ϕ is larger than p^{-4}. Furthermore, if the divergence speed of the fourth derivative of ϕ is $p^{4-\alpha}$ for $\alpha \in (0, 1)$, the minimax optimal rate is obtained within a universal multiplicative constant as $\frac{k^2}{(n \ln n)^{2\alpha}} + \frac{k^{2-2\alpha}}{n}$.

I-MMSE relations in random linear estimation and a sub-extensive interpolation method (12:30)

Jean Barbier (EPFL, Switzerland); Nicolas Macris (EPFL, Switzerland)

Consider random linear estimation with Gaussian measurement matrices and noise. One can compute infinitesimal variations of the mutual information under infinitesimal variations of the signal-to-noise ratio or of the measurement rate. We discuss how each variation is related to the minimum mean-square error and deduce that the two variations are directly connected through a very simple identity. The main technical ingredient is a new interpolation method called "sub-extensive interpolation method". We use it to provide a new proof of an I-MMSE relation recently found by Reeves and Pfister [1] when the measurement rate is varied. Our proof makes it clear that this relation is intimately related to another I-MMSE relation also recently proved in [2]. One can directly verify that the identity relating the two types of variation of mutual information is indeed consistent with the one letter replica symmetric formula for the mutual information, first derived by Tanaka [3] for binary signals, and recently proved in more generality in [1,2,4,5] (by independent methods). However our proof is independent of any knowledge of Tanaka's formula.

Th2-6: MIMO 3

Thursday, June 29, 11:30-12:50
Room: K5
Chair: Hamid Jafarkhani (University of California, Irvine, USA)

Multi-Antenna Coded Caching (11:30)

Seyed Pooya Shariatpanahi (Institute for Research in Fundamental Sciences (IPM), Iran); Giuseppe Caire (Technische Universität Berlin, Germany); Babak Hossein Khalaj (Sharif University of Technology, Iran)

In this paper we consider a single-cell downlink scenario where a multiple-antenna base station delivers contents to multiple cache-enabled user terminals. Based on the multicasting opportunities provided by the so-called Coded Caching technique, we investigate three delivery approaches. Our baseline scheme employs the coded caching technique on top of max-min fair multicasting. The second one consists of a joint design of Zero-Forcing (ZF) and coded caching, where the coded chunks are formed in the signal domain (complex field). The third scheme is similar to the second one with the difference that the coded chunks are formed in the data domain (finite field). We derive closed-form rate expressions where our results suggest that the latter two schemes surpass the first one in terms of Degrees of Freedom (DoF). However, at the intermediate SNR regime forming coded chunks in the signal domain results in power loss, and will deteriorate throughput of the second scheme. The main message of our paper is that the schemes performing well in terms of DoF may not be directly appropriate for intermediate SNR regimes, and modified schemes should be employed.

Optimally-Tuned Nonparametric Linear Equalization for Massive MU-MIMO Systems (11:50)

Ramina Ghods (Cornell University, USA); Charles Jeon (Cornell University, USA); Gulnar Mirza (Cornell University, USA); Arian Maleki (Columbia University, USA); Christoph Studer (Cornell University, USA)

This paper deals with linear equalization in massive multi-user multiple-input multiple-output (MU-MIMO) wireless systems. We first provide simple conditions on the antenna configuration for which the well-known linear minimum mean-square error (L-MMSE) equalizer provides near-optimal spectral efficiency, and we analyze its performance in the presence of parameter mismatches in the signal and/or noise powers. We then propose a novel, optimally-tuned NOnParametric Equalizer (NOPE) for massive MU-MIMO systems, which avoids knowledge of the transmit signal and noise powers altogether. We show that NOPE achieves the same performance as that of the L-MMSE equalizer in the large-antenna limit, and we demonstrate its efficacy in realistic, finite-dimensional systems. From a practical perspective, NOPE is computationally efficient and avoids dedicated training that is typically required for parameter estimation.

Rate Bounds on 4-group fast decodable space-time code (12:10)

Bharath Sethuraman (California State University, Northridge, USA)

It is known that the maximum number of groups into which space-time codes from division algebras can be partitioned so that the resulting vectorized representations, for any channel matrix, break off into pairwise orthogonal subsets, is four. Such partitions are key to fast decodability of codes. In this paper we study the rate of such 4-group fast decodable codes, and show that if the codes arise from $n \times n$ matrices, then the maximum data rate, measured in number of real symbols per transmitted matrix, is $2n$. We give examples of codes that meet this bound.

Th2-7: Security 5

Thursday, June 29, 11:30-12:50
Room: K6
Chair: Sidharth Jaggi (Chinese University of Hong Kong, Hong Kong)

Games on Linear Deterministic Channels with Eavesdroppers (11:30)

Ruijie Xu (Northwestern University, USA); Hao Ge (Northwestern University, USA); Randall Berry (Northwestern University, USA)

We consider adding secrecy constraints to a model of information theoretic games introduced in earlier works. In these games, each user autonomously selects their encoding and decoding strategy with the objective of maximizing their own secure rate in the presence of a single eavesdropper. We study the Nash equilibrium regions for such games when the users are communicating over linear deterministic models of a multiple access channel and an interference channel. In particular, we show that for interference channels, the presence of an eavesdropper results in significantly different equilibrium properties than when an eavesdropper is not present.

A New Broadcast Wiretap Channel Model (11:50)

Mohamed Nafea *(The Pennsylvania State University, USA); Aylin Yener (Pennsylvania State University, USA)*

A new broadcast wiretap channel (B-WTC) with a wiretapper who noiselessly taps into a fixed-length subset of the transmitted symbols of her choice, and observes

the remainder through a noisy channel, is studied. An achievable strong secrecy rate region which extends Marton's inner bound to the proposed setting, is derived. Strong secrecy capacity regions for two classes of the new B-WTC, namely the new B-WTC with deterministic receivers, and the new B-WTC with degraded receivers and more noisy wiretapper, are identified. These results extend the recently proposed new wiretap channel model to the broadcast setting.

Secrecy-Reliability Tradeoff for Semi-Deterministic Wiretap Channels at Finite Blocklength (12:10)

Wei Yang (Princeton University, USA); Rafael Schaefer (Technische Universität Berlin, Germany); H. Vincent Poor (Princeton University, USA)

This paper studies the maximum secrecy rate for a semi-deterministic wiretap channel, in which the channel between the transmitter and legitimate receiver is deterministic, while that between the transmitter and the eavesdropper is a discrete memoryless channel. For a given decoding error probability and information leakage (measured by the variational distance), the optimal second-order secrecy rate is derived. Unlike the secrecy capacity, the second-order secrecy rate characterizes the optimal tradeoff between secrecy and reliability at finite blocklength.

On Secure Asymmetric Multilevel Diversity Coding Systems (12:30)

Congduan Li (City University of Hong Kong, Hong Kong); Xuan Guang (The Chinese University of Hong Kong, P.R. China); Chee Wei Tan (City University of Hong Kong, Hong Kong); Raymond W. Yeung (The Chinese University of Hong Kong, Hong Kong)

Whether superposition (source separation) is optimal for the asymmetric multilevel diversity coding systems (AMDCS) with perfect secrecy is answered in this paper by studying a non-trivial example. Threshold perfect secrecy is added to the AMDCS model. The eavesdropper may have access to any one but not more than one subset of the channels but can get nothing about the sources, as long as the size of the subset is not above the security level. The secure AMDCS (S-AMDCS) with five sources, four encoders and security level two is solved and it is shown that linear codes are optimal for this instance. However, in contrast with the secure symmetric multilevel diversity coding systems (S-SMDCS), superposition is shown to be not optimal for S-AMDCS in general from this counterexample.

Th2-8: Compressed Sensing 3

Thursday, June 29, 11:30-12:50
Room: K7+8
Chair: Tareq Y. Al-Naffouri (King Abdullah University of Science and Technology, USA)

Dynamical Functional Theory for Compressed Sensing (11:30)

Burak Çakmak *(Aalborg University, Denmark); Manfred Opper (KI / TU Berlin, Germany); Ole Winther (Technical University of Denmark, Denmark); Bernard Fleury (Aalborg University, Denmark)*

We introduce a theoretical approach for designing generalizations of the approximate message passing (AMP) algorithm for compressed sensing which are valid for large observation matrices that are drawn from an invariant random matrix ensemble. By construction, the fixed points of the algorithm obey the Thouless-Anderson-Palmer (TAP) equations corresponding to the ensemble. Using a dynamical functional approach we are able to derive an effective stochastic process for the marginal statistics of a single component of the dynamics. This allows us to design memory terms in the algorithm in such a way that the resulting fields become Gaussian random variables allowing for an explicit analysis. The asymptotic statistics of these fields are consistent with those obtained for the replica ansatz of the compressed sensing problem.

Compressed Sensing under Optimal Quantization (11:50)

Alon Kipnis (Stanford University, USA); Galen Reeves (Duke University, USA); Yonina Eldar (Technion-Israel Institute of Technology, Israel); Andrea Goldsmith (Stanford University, USA)

We consider the problem of recovering a sparse vector from a quantized or a lossy compressed version of its noisy random linear projections. We characterize the minimal distortion in this recovery as a function of the sampling ratio, the sparsity rate, the noise intensity and the total number of bits in the quantized representation. We first derive a singe-letter expression that can be seen as the indirect distortion-rate function of the sparse source observed through a Gaussian channel whose signal-to-noise ratio is derived from these parameters. Under the replica symmetry postulation, we prove that there exists a quantization scheme that attains this expression in the asymptotic regime of large system dimensions. In addition, we prove a converse demonstrating that the MMSE in estimating any fixed sub-block of the source from the quantized measurements at a fixed number of bits does not exceed this expression as the system dimensions go to infinity. Thus, under these conditions, the expression we derive describes the excess distortion incurred in encoding the

source vector from its noisy random linear projections in lieu of the full source information.

Noisy Tensor Completion for Tensors with a Sparse Canonical Polyadic Factor (12:10)

Swayambhoo Jain (University of Minnesota, USA); Alexander Gutierrez (University of Minnesota, USA); Jarvis Haupt (University of Minnesota, USA)

In this paper we study the problem of noisy tensor completion for tensors that admit a canonical polyadic or CANDECOMP/PARAFAC (CP) decomposition with one of the factors being sparse. We present general theoretical error bounds for an estimate obtained by using a complexity-regularized maximum likelihood principle and then instantiate these bounds for the case of additive white Gaussian noise. We also provide an ADMM-type algorithm for solving the complexity-regularized maximum likelihood problem and validate the theoretical finding via experiments on synthetic data set.

Compressed Sensing of Compressible Signals (12:30)

Sajjad Beygi (University of Southern California, USA); Shirin Jalali (Bell Labs, USA); Arian Maleki (Columbia University, USA); Urbashi Mitra (University of Southern California, USA)

A novel low-complexity robust-to-noise iterative algorithm named compression-based gradient descent (C-GD) algorithm is proposed. C-GD is a generic compressed sensing recovery algorithm, that at its core, employs compression codes, such as JPEG2000 and MPEG4. Through using compression codes, C-GD strongly generalizes the scope of structures used by compressed sensing recovery algorithms beyond sparsity or low-rankness. The squared error of the proposed method and its associated convergence is characterized and predicts the strong performance of C-GD. Numerical results suggest that C-GD, when combined with state-of-the-art compression codes, either outperforms or performs comparably to modern compressed sensing recovery methods.

Th2-9: Statistics 1

Thursday, June 29, 11:30-12:50
Room: K9
Chair: Andrew Barron (Yale University, USA)

Budget-Optimal Clustering via Crowdsourcing (11:30)

Ravi Kiran Raman (University of Illinois at Urbana-Champaign, USA); Lav Varshney (University of Illinois at Urbana-Champaign, USA)

This paper defines and studies the problem of universal clustering using responses of crowd workers, without knowledge of worker reliability or task difficulty. We model stochastic worker response distributions by incorporating traits of memory for similar objects and traits of distance among differing objects. We are particularly interested in two limiting worker types—temporary and long-term workers, without and with memory respectively. We first define clustering algorithms for these limiting cases and then integrate them into an algorithm for the unified worker model. We prove asymptotic consistency of the algorithms and establish sufficient conditions on the sample complexity of the algorithm. Converse arguments establish necessary conditions on sample complexity, proving that the defined algorithms are asymptotically order-optimal in cost.

Universal Joint Image Clustering and Registration using Partition Information (11:50)

Ravi Kiran Raman (University of Illinois at Urbana-Champaign, USA); Lav Varshney (University of Illinois at Urbana-Champaign, USA)

The problem of joint clustering and registration of images is studied in a universal setting. We define universal joint clustering and registration algorithms using multivariate information functionals. We first study the problem of registering two images using maximum mutual information and prove its asymptotic optimality. We then show the shortcomings of pairwise registration in multi-image registration, and design an asymptotically optimal algorithm based on multiinformation. Finally, we define a novel multivariate information functional to perform joint clustering and registration of images, and prove consistency of the algorithm.

How to Find a Joint Probability Distribution of Minimum Entropy (almost) given the Marginals (12:10)

***Ferdinando Cicalese** (University of Verona, Italy); Luisa Gargano (University of Salerno, Italy); Ugo Vaccaro (University of Salerno, USA)*

Given two discrete random variables X and Y, with probability distributions $p = (p_1, ..., p_n)$ and $q =$

$(q_1, ..., q_m)$, respectively, denote by $C(p, q)$ the set of all joint distributions of X and Y (couplings) of p and q, that is, the set of all bivariate probability distributions that have p and q as marginals. In this paper, we study the problem of finding the joint probability distribution in $C(p, q)$ of minimum entropy (equivalently, the joint probability distribution that maximizes the mutual information between X and Y), and we discuss several situations where the need for this kind of optimization naturally arises. Since the optimization problem is known to be NP-hard, we give an efficient algorithm to find a joint probability distribution in $C(p, q)$ with entropy exceeding the minimum possible by at most 1, thus providing an approximation algorithm with additive approximation factor of 1. We also discuss some related consequences of our findings.

On the Fundamental Statistical Limit of Community Detection in Random Hypergraphs (12:30)

Chung-Yi Lin (National Taiwan University, Taiwan); I Chien (National Taiwan University, Taiwan); I-Hsiang Wang (National Taiwan University, Taiwan)

The problem of community detection in random hyper graphs is considered. We extend the Stochastic Block Model (SBM) from graphs to hypergraphs with d-uniform hyperedges, which we term ”d-wise hyper stochastic block model” (d-hSBM), and consider a homogeneous and approximately equal-sized K community case. For d=3, we fully characterize the exponentially decaying rate of the minimax risk in recovering the underlying communities, where the loss function is the mis-match ratio between the true community assignment and the recovered one. It turns out that the rate function is a weighted combination of several divergence terms, each of which is the Renyi divergence of order 1/2 between two Bernoulli distributions. The Bernoulli distributions involved in the characterization of the rate function are those governing the random instantiation of hyperedges in d-hSBM. The lower bound is set by finding a smaller parameter space where we can analyze the risk, while the upper bound is achieved with the Maximum Likelihood estimator. The technical contribution is to show that upper bound has the same decaying rate as the lower bound, which involves careful bounding of the various probabilities of errors. Finally, we relate the minimax risk to the recovery criterion under the Bayesian framework and derive a threshold condition for exact recovery.

Th3-1: Coding Theory 3

Thursday, June 29, 14:40-16:20
Room: Amsterdam
Chair: Antonia Wachter-Zeh (Technical University of Munich (TUM), Germany)

Multiset combinatorial batch codes (14:40)

Hui Zhang (Technion - Israel Institute of Technology, Israel); Eitan Yaakobi (Technion, Israel); Natalia Silberstein (Yahoo! Labs, Israel)

Batch codes, first introduced by Ishai, Kushilevitz, Ostrovsky, and Sahai, mimic a distributed storage of a set of n data items on m servers, in such a way that any batch of k data items can be retrieved by reading at most some t symbols from each server. *Combinatorial batch codes*, are replication-based batch codes in which each server stores a subset of the data items. In this paper, we propose a generalization of combinatorial batch codes, called *multiset combinatorial batch codes* (*MCBC*), in which n data items are stored in m servers, such that any multiset request of k items, where any item is requested at most r times, can be retrieved by reading at most t items from each server. The setup of this new family of codes is motivated by recent work on codes which enable high availability and parallel reads in distributed storage systems. The main problem under this paradigm is to minimize the number of items stored in the servers, given the values of n, m, k, r, t, which is denoted by $N(n, k, m, t; r)$. We first give a necessary and sufficient condition for the existence of MCBCs. Then, we present several bounds on $N(n, k, m, t; r)$ and constructions of MCBCs. In particular, we determine the value of $N(n, k, m, 1; r)$ for any $n \geq \left\lfloor \frac{k-1}{r} \right\rfloor \binom{m}{k-1} - (m-k+1)A(m, 4, k-2)$, where $A(m, 4, k-2)$ is the maximum size of a binary constant weight code of length m, distance four and weight $k-2$. We also determine the exact value of $N(n, k, m, 1; r)$ when $r \in \{k, k-1\}$ or $k = m$.

Structured Spherical Codes With Asymptotically Optimal Distance Distributions (15:00)

Robert Taylor (Virginia Tech, USA); Lamine Mili (Virginia Tech, USA); Amir Zaghloul (US Army Research Laboratory & Virginia Tech, USA)

We introduce a new geometric construction of cyclic group codes in odd-dimensional spaces formed by intersecting even-dimensional constant curvature curves with hyperplanes of one less dimension. This allows us to recast the cyclic group code as a uniform sampling of a constant curvature curve whereby the design of the constant curvature curve controls code performance. Using a tool from knot theory known as the circumradius function, we derive properties of cyclic group codes from properties of the constant curvature curve passing through every point of the spherical code. By

relating the distribution of the squared circumradius function of the connecting curve to the distribution of the pairwise distances of the cyclic group code, we show that the distance spectrum of cyclic group codes achieves optimality in the sense of matching the random spherical code distance distribution bound as the block length grows large.

Weight Spectrum of Quasi-Perfect Binary Codes with Distance 4 (15:20)

Valentin Afanassiev *(Intitute Problems of Information Transmission, Russia); Alexander Davydov (Institute for Information Transmission Problem, Russia)*

We consider the weight spectrum of a class of quasi-perfect binary linear codes with code distance 4. For example, extended Hamming code and Panchenko code are the known members of this class. Also, it is known that in many cases Panchenko code has the minimal number of weight 4 codewords. We give exact recursive formulas for the weight spectrum of quasi-perfect codes and their dual codes. As an example of application of the weight spectrum we derive a lower estimate for the conditional probability of correction of erasure patterns of high weights (equal to or greater than code distance).

Kronecker Product and Tiling of Permutation Arrays for Hamming Distances (15:40)

Sergey Bereg (University of Texas at Dallas, USA); Luis Gerardo Mojica de la Vega (University of Texas at Dallas, USA); Linda Morales (University of Texas at Dallas, USA); I. Hal Sudborough (University of Texas at Dallas, USA)

We give improved lower bounds for M(n,d), for various positive integers d and n with d<n, where M(n,d) is the largest number of permutations on n symbols with pairwise Hamming distance at least d. Permutation arrays are used for constructing error correcting permutation codes, which have been proposed for power-line communications. We describe two techniques, which use Kronecker products and a ”tiling” operation. Our techniques improve the size of permutation arrays, and improve lower bounds on M(n,d), for infinitely many n and d, d<n.

Performance of Spinal Codes with Sliding Window Decoding (16:00)

Weiqiang Yang (Xidian University, P.R. China); Ying Li (University of Xidian, P.R. China); Xiaopu Yu (Xidian University, P.R. China)

In this paper, we focus on the finite-length performance of spinal codes with a sliding window decoder over binary erasure channel. An expression of the error probability of spinal codes is derived. Particularly, we also derive an expression of the error probability of spinal codes with some known tail bits, which can improve the error-control performance. Moreover, easier-to-compute upper and lower bounds on the error probability are also provided. Simulation results show that the error-control performance can be improved by introducing known tail bits and the performance becomes better with the increase of the maximum window length. Finally, the derived bounds can well evaluate the error performance of spinal codes.

Th3-2: Coding for Distributed Storage 2

Thursday, June 29, 14:40-16:20
Room: Brussels
Chair: Joerg Kliewer (New Jersey Institute of Technology, USA)

Secure Regenerating Codes for Hybrid Cloud Storage Systems (14:40)

Islam Samy *(University of Arizona, USA); Gokhan Calis (University of Arizona, USA); O. Ozan Koyluoglu (University of California, Berkeley, USA)*

We study the scenario of hybrid cloud storage where the client utilizes both an off-site and a local storage. The former is a distributed storage system (DSS) with the presence of an eavesdropper that has access to the content stored in and downloaded to some subset of nodes. The latter (local) storage is utilized to store a secret key to secure the stored file against the eavesdropper. We introduce two possibilities to utilize local storage (secret key) in enhancing the DSS. First, the key can be used to increase the maximum file size stored in the DSS. We propose an upper bound for this scenario and show constructions achieving it. Second, the key can be used to decrease the number of contacted nodes required to reconstruct the file at the client. We extend the product matrix (PM) framework and construct codes that enables efficient data access. Our analysis includes both minimum repair bandwidth regenerating (MBR) and minimum storage regenerating (MSR) codes.

Centralized Multi-Node Repair for Minimum Storage Regenerating Codes (15:00)

Marwen Zorgui (University of California, Irvine, USA); Zhiying Wang (UC Irvine, USA)

In distributed storage, erasure codes are widely used to provide data reliability, where every codeword symbol corresponds to one storage node. The network traffic cost during the repair of node failures, called repair bandwidth, is an important metric in code design. In particular, minimum storage regenerating (MSR) codes are maximum distance separable (MDS) codes that have optimal repair bandwidth. In this paper, we gen-

eralize the problem to minimum storage multi-node regenerating (MSMR) codes, which are MDS codes with optimal repair bandwidth for e node failures. We describe a general framework for converting MSR codes to MSMR codes. The repair strategy for e failures is similar to that for single failure, however certain extra requirements need to be satisfied by the repairing functions for single failure. Then we apply this framework to product-matrix codes and interference alignment codes.

GDSP: A Graphical Perspective on the Distributed Storage Systems (15:20)

Saeid Sahraei (EPFL, Switzerland); Michael Gastpar (EPFL & University of California, Berkeley, Switzerland)

The classical distributed storage problem can be modeled by a k-uniform *complete* hyper-graph where vertices represent servers and hyper-edges represent users. Hence each hyper-edge should be able to recover the full file using only the memories of the vertices associated with it. This paper considers the generalization of this problem to *arbitrary* hyper-graphs and to the case of multiple files, where each user is only interested in one, a problem we will refer to as the graphical distributed storage problem (GDSP). Specifically, we make progress in the analysis of minimum-storage codes for two main subproblems of the GDSP which extend the classical model in two independent directions: the case of an arbitrary graph with multiple files, and the case of an arbitrary hyper-graph with a single file.

Distributed Storage Allocation for Multi-Class Data (15:40)

Koosha Pourtahmasi Roshandeh (University of Alberta, Canada); Moslem Noori (University of Alberta, Canada); Masoud Ardakani (University of Alberta, Canada); Chintha Tellambura (University of Alberta, Canada)

Distributed storage systems (DSSs) provide a scalable solution for reliably storing massive amounts of data coming from various sources. Heterogeneity of these data sources often means different data classes (types) exist in a DSS, each needing a different level of quality of service (QoS). As a result, efficient data storage and retrieval processes that satisfy various QoS requirements are needed. This paper studies storage allocation, meaning how the data of different classes is spread over storage nodes, for a multi-class DSS. More specifically, assuming a probabilistic access to the storage nodes, we aim at maximizing the weighted sum of the probability of successful data recovery of data classes. Solving this optimization problem for a general setup is intractable. Thus, we find the optimal storage allocation when the data of each class is spread minimally over the nodes, i.e. minimal spreading allocation (MSA). Then, by comparing the performance of the optimal MSA with the performance upper bound, we show that the optimal MSA is indeed the optimal storage allocation in many practical cases. Numerical examples are also presented for better illustration of the results.

Th3-3: Relaying

Thursday, June 29, 14:40-16:20
Room: K2
Chair: Roy Yates (Rutgers University, USA)

The Capacity-distortion Function for Multihop Channels with State (14:40)

Amir Salimi (University of Southern California, USA); Wenyi Zhang (University of Science and Technology of China, P.R. China); Satish Vedantam (University of Southern California, USA); Urbashi Mitra (University of Southern California, USA)

We consider a joint communication and channel estimation problem over a multi-hop relay network with discrete-memoryless channel states. The state information on each link is not available either for the senders or the receivers. Each receiver in the network needs to construct an estimation of channel states with certain fidelity constraint, as well as helping the destination to decode the message reliably. First, we study a two-hop network where channel states on each hop are independent. We then show that a decode-and-Forward strategy, in conjunction with a compress-and-forward strategy achieves the entire capacity-distortion region. We also prove an achievable rate when the channel states are correlated. We extend the result to a multi-hop network, where each node is intended to reconstruct channel state information from L previous links.

The Geometry of the Relay Channel (15:00)

Xiugang Wu (Stanford University, USA); Leighton Barnes (Stanford University, USA); Ayfer Özgür (Stanford University, USA)

Consider a memoryless relay channel, where the channel from the relay to the destination is an isolated bit pipe of capacity C_0. Let $C(C_0)$ denote the capacity of this channel as a function of C_0. What is the critical value of C_0 such that $C(C_0)$ first equals $C(\infty)$? This is a long-standing open problem posed by Cover and named "The Capacity of the Relay Channel," in *Open Problems in Communication and Computation*, Springer-Verlag, 1987. In our recent work, we answered this question in the case when the channels from the source to the relay and destination are symmetric, which is the original assumption imposed by Cover, and when these channels are Gaussian. We showed that $C(C_0)$ can not equal to $C(\infty)$ unless

$C_0 = \infty$, regardless of the SNR of the Gaussian channels, while the cut-set bound would suggest that $C(\infty)$ can be achieved at finite C_0. In this paper, we show that our techniques for solving Cover's problem can be naturally extended to the general Gaussian case, where the channels from the source to the relay and destination may be asymmetric, and prove an upper bound on the capacity $C(C_0)$ of a general Gaussian relay channel for any C_0. This upper bound immediately implies that our previous conclusion, i.e. $C(C_0)$ can not equal to $C(\infty)$ unless $C_0 = \infty$, also holds in the asymmetric case. Our approach is geometric and relies on a strengthening of the isoperimetric inequality on the sphere by using the Riesz rearrangement inequality.

The CF-DF Approach for Relay Networks Based on Multiple Descriptions with the Shared Binning (15:20)

Leila Ghabeli *(Department of Electrical Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran, Iran)*

Decode-and-forward (DF) and compress-and-forward (CF) are well-known strategies to transmit information over the relay channel. There are several methods which generalize these strategies to relay networks, among them, the unified CF-DF strategy is one with relatively good performance and less complexity. In this method the nodes are divided into two groups: DF relay nodes and CF relay nodes, where the DF relay nodes fully utilize the help of the CF relay nodes. Here we present a modified CF-DF approach in which the CF relay nodes form multiple description coding. This method let different DF relay nodes and the destination receive the relay observation at different quality levels. In comparison with similar approaches, here the key point is that we use the shared binning for all descriptions at a CF relay node. This strategy reduces the complexity of the obtained achievable rate and yielding the better performance at the same time. Simulation results for Gaussian relay networks show that our proposed achievable rate includes the previously proposed ones.

Th3-4: Guessing

Thursday, June 29, 14:40-16:20
Room: K3
Chair: Neri Merhav (Technion, Israel)

Making Recommendations Bandwidth Aware (14:40)

Linqi Song (University of California, Los Angeles, USA); Christina Fragouli (UCLA, USA)

This paper asks how much we can gain in terms of bandwidth and user satisfaction, if recommender systems became bandwidth aware and took into account not only the user preferences, but also the fact that they may need to serve these users under bandwidth constraints, as is the case over wireless networks. We formulate this as a new problem in the context of index coding: we relax the index coding requirements to capture scenaria where each client has preferences associated with messages. The client is satisfied to receive any message she does not already have, with a satisfaction proportional to her preference for that message. We consistently find, over a number of scenaria we sample, that although the optimization problems are in general NP-hard, significant bandwidth savings are possible even when restricted to polynomial time algorithms.

The Effect of Bias on the Guesswork of Hash Functions (15:00)

Yair Yona (University of California Los Angeles, USA); Suhas Diggavi (University of California Los Angeles, USA)

In this work we analyze the average guesswork for the problem of hashed passwords cracking (i.e., finding a password that has the same hash value as the actual password). We focus on the following two cases: Averaging over all strategies of guessing passwords one by one for any hash function that has effective distribution (i.e., the fraction of mappings to any bin) which is i.i.d. Bernoulli(p), and averaging over all hash functions whose effective distribution is i.i.d. Bernoulli(p) for any strategy of guessing passwords one by one. We analyze the average guesswork under both online and offline attacks by deriving upper and lower bounds on the average guesswork as a function of the bins to which passwords are mapped, along with the most likely average guesswork, that is, the average guesswork of the most likely set of bins. Furthermore, we provide a *concentration* result that shows that the probability mass function of the guesswork is concentrated around its mean value. These results give quantifiable bounds for the effect of bias as well as the number of users on the average guesswork of a hash function, and show that increasing the number of users has a far worse effect than bias in terms of the average guesswork.

Guessing With Limited Memory (15:20)

Wasim Huleihel (MIT, USA); Salman Salamatian (Massachusetts Institute of Technology, USA); Muriel Médard (MIT, USA)

Suppose that we wish to guess the realization x of a discrete random variable X taking values in a finite set, by asking sequential questions of the form "Is X equal to x?", exhausting the elements of X until the answer is "Yes" [1,2]. If the distribution of X is known to the guesser, and the guesser has memory of his previous queries then the best strategy is to guess in decreas-

ing order of probabilities. In this paper, we consider the problem of a *memoryless* guesser, namely, each new guess is independent of the previous guesses. We consider also the scenario of a guesser with a bounded number of guesses. For both cases we derive the optimal guessing strategies, and show new connections to Rényi entropy.

Centralized vs Decentralized Multi-Agent Guesswork (15:40)

Salman Salamatian *(Massachusetts Institute of Technology, USA); Ahmad Beirami (MIT, USA); Asaf Cohen (Ben-Gurion University of the Negev, Israel); Muriel Médard (MIT, USA)*

We study a notion of guesswork, where multiple agents intend to launch a coordinated brute-force attack to find a single binary secret string, and each agent has access to side information generated through either a BEC or a BSC. The average number of trials required to find the secret string grows exponentially with the length of the string, and the rate of the growth is called the guesswork exponent. We compute the guesswork exponent for several multi-agent attacks, and show that a multi-agent attack reduces the guesswork exponent compared to a single agent, even when the agents do not exchange information to coordinate their attack, and try to individually guess the secret string using a predetermined scheme in a decentralized fashion. Further, we show that the guesswork exponent of two agents who do coordinate their attack is strictly smaller than that of any finite number of agents individually performing decentralized guesswork.

Th3-5: Detection and Estimation 3

Thursday, June 29, 14:40-16:20
Room: K4
Chair: Alfred Hero III (University of Michigan, USA)

Asymptotic Optimality of D-CuSum for Quickest Change Detection under Transient Dynamics (14:40)

Shaofeng Zou (University of Illinois at Urbana Champaign, USA); Georgios Fellouris (University of Illinois at Urbana-Champaign, USA); Venugopal Veeravalli (University of Illinois at Urbana-Champaign, USA)

The problem of quickest change detection (QCD) under transient dynamics is studied, in which the change from the initial distribution to the final persistent distribution does not happen instantaneously, but after a series of cascading transient phases. It is assumed that the durations of the transient phases are deterministic but unknown. The goal is to detect the change as quickly as possible subject to a constraint on the average run length to false alarm. The dynamic CuSum (D-CuSum) algorithm is investigated, which is based on reformulating the QCD problem into a dynamic composite hypothesis testing problem, and has a recursion that facilitates implementation. We show that this algorithm is adaptive to the unknown change point, as well as the unknown transient duration. And under mild conditions of the pre-change and post-change distributions, its asymptotic optimality is demonstrated for all possible asymptotic regimes as the transient duration and the average run length to false alarm go to infinity.

Sketched Covariance Testing: A Compression-Statistics Tradeoff (15:00)

Gautam Dasarathy (Rice University, USA); Parikshit Shah (Yahoo Research, USA, USA); Richard Baraniuk (Rice University, USA)

Hypothesis testing of covariance matrices is an important problem in multivariate analysis. Given n data samples and a covariance matrix Σ0, the goal is to determine whether or not the data is consistent with this matrix. In this paper we introduce a framework that we call Sketched Covariance Testing, where the data is provided after being compressed by multiplying by a ”sketching” matrix A. We propose a statistical test in this setting and quantify an achievable sample complexity as a function of the amount of compression. Our result reveals an intriguing tradeoff between the compression ratio and the statistical information required for reliable hypothesis testing; the sample complexity increases as the fourth power of amount of compression.

Error bounds for Bregman Denoising and Structured Natural Parameter Estimation (15:20)

Amin Jalali (Wisconsin Institute for Discovery, USA); James Saunderson (University of Washington, USA); Maryam Fazel (Univiversity of Washington, USA); Babak Hassibi (California Institute of Technology, USA)

We analyze an estimator based on the Bregman divergence for recovery of structured models from additive noise. The estimator can be seen as a regularized maximum likelihood estimator for an exponential family where the natural parameter is assumed to be structured. For all such Bregman denoising estimators, we provide an error bound for a natural associated error measure. Our error bound makes it possible to analyze a wide range of estimators, such as those in proximal denoising and inverse covariance matrix estimation, in a unified manner. In the case of proximal denoising, we exactly recover the existing tight normalized mean squared error bounds. In sparse precision matrix estimation, our bounds provide optimal scaling with interpretable constants in terms of the associated error measure. Lastly, we give a numerical example for the multivariate Gaussian distribution to showcase the Bregman denoiser and the bound.

On Random Sampling with Nodes Attraction: The Case of Gauss-Poisson Process (15:40)

Flavio Zabini (University of Bologna, Italy); Gianni Pasolini (University of Bologna, Italy); Andrea Conti (ENDIF University of Ferrara, WiLAB University of Bologna, Italy)

The deployment of sensing nodes is crucial for applications relying on the reconstruction of spatial fields. Theoretical analysis usually assumes that nodes are distributed according to a homogeneous Poisson point process (PPP), in which nodes positions are stochastically independent. However, realistic scenarios for crowd sourcing and Internet of Things call for clustered layouts of sensing nodes, for which homogeneous PPP is not appropriate. This paper analyzes sampling and reconstruction of finite-energy signals in Rd, with samples gathered in space according to a Gauss-Poisson point process (G-PPP), which has been recently proposed to model node spatial distribution with attraction (as in clustering). In particular, it is shown that attraction between nodes modeled by G-PPP reduces the reconstruction accuracy with respect the case of homogeneous PPP with the same intensity. This represents the opposite case of the repulsion effect, which was investigated in a previous work relying on Ginibre point process sampling.

Low-rank, Sparse and Line Constrained Estimation: Applications to Target Tracking and Convergence (16:00)

Amr Elnakeeb (University of Southern California, USA); Urbashi Mitra (University of Southern California, USA)

In this paper, the incorporation of a line constraint is considered for structured estimation. In particular, multiple forms of structure on matrices are extended from low-rank and sparsity. The line constraint is introduced via a rotation that yields a secondary low rank condition. The proposed method is applied to single object tracking in video wherein the trajectory can be parameterized as a line. The optimization is solved via the Augmented Lagrange Multiplier method. Measurable performance improvement is observed over previous background subtraction methods that do not exploit the line structure. An aggregated error is proven to converge to zero and a boundedness analysis is conducted which suggests that the iterative algorithm is convergent.

Th3-6: Multiple Access Feedback

Thursday, June 29, 14:40-16:20
Room: K5
Chair: Lalitha Sankar (Arizona State University, USA)

Two-User Downlink Non-Orthogonal Multiple Access with Limited Feedback (14:40)

Xiaoyi Liu (University of California, Irvine, USA); Hamid Jafarkhani (University of California, Irvine, USA)

In this paper, we analyze downlink non-orthogonal multiple access (NOMA) networks with limited feedback. Our goal is to derive appropriate transmission rates for rate adaptation and minimize outage probability of minimum rate for the constant-rate data service, based on distributed channel feedback information from two receivers. We propose an efficient quantizer with variable-length encoding that approaches the best performance of the case where perfect channel state information is available everywhere. We prove that in the typical application with two receivers, the losses in the minimum rate and outage probability decay at least exponentially with the minimum feedback rate. Furthermore, we analyze the diversity gain and provide a sufficient condition for the quantizer to achieve the maximum diversity order.

Role of Feedback in Modulo-Sum Computation over Erasure Multiple-Access Channels (15:00)

I-Hsiang Wang (National Taiwan University, Taiwan); Shih-Chun Lin (National Taiwan University of Science and Technology, Taiwan); Yu-Chih Huang (National Taipei University, Taiwan)

The problem of computing the modulo-sum of messages over a finite-field erasure multiple access channel (MAC) is studied, and the role of feedback for function computation is explored. Our main contribution is two-fold. First, a new outer bound on the non-feedback computation capacity is proved, which strictly improves the state of the art by Khisti, Hern, and Narayanan. The new outer bound answers a previously unsettled question in the affirmative: delayed state feedback strictly increases computation capacity for the two-user erasure MAC universally. The proof leverages the subset entropy inequality by Madiman and Tetali. Second, focusing on the family of linear coding schemes with hybrid-ARQ-type retransmissions, we develop the optimal computation rate with delayed state feedback. For the considered family of schemes, it is always sub-optimal to compute modulo-sum by decoding all messages first. This is in contrast to the non-feedback case by Khisti et al. where sometimes the aforementioned ”decode- all” strategy can reach the best known achievable rates.

On the Necessity of Structured Codes for Communications over MAC with Feedback (15:20)

Mohsen Heidari Khoozani (University of Michigan, USA); Farhad Shirani (University of Michigan, USA); Sandeep Pradhan (University Michigan, USA)

The problem of three-user multiple-access channel (MAC) with noiseless feedback is investigated. A new coding strategy is presented. The coding scheme builds upon the natural extension of the Cover-Leung (CL) scheme [1]; and uses quasi-linear codes. A new single-letter achievable rate region is derived. The new achievable region strictly contains the CL region. This is shown through an example. In this example, the coding scheme achieves optimality in terms of transmission rates. It is shown that any optimality achieving scheme for this example must have a specific algebraic structure. Particularly, the codebooks must be closed under binary addition.

On the Gaussian MAC with Stop-Feedback (15:40)

Lan Truong (National University of Singapore, Singapore); Vincent Tan (National University of Singapore, Singapore)

We characterize the information theoretic limits of the Gaussian multiple access channel (MAC) when variable-length stop-feedback is available at the encoder and a non-vanishing error probability is permitted. Due to the continuous nature of the channel and the presence of expected power constraints, we need to develop new achievability and converse techniques. Due to the multi-terminal nature of the channel model, we are faced with the need to bound the asymptotic behavior of the expected value of the maximum of several stopping times. We do so by leveraging tools from renewal theory developed by Gut, Lai and Siegmund.

Th3-7: Communications 3

Thursday, June 29, 14:40-16:20
Room: K6
Chair: Ralf Müller (FAU Erlangen-Nürnberg, Germany)

Probabilistic Shaping and Non-Binary Codes (14:40)

Joseph Jean Boutros (Texas A&M University, USA); ***Fanny Jardel*** *(Nokia Bell Labs, Germany); Cyril Measson (Nokia & Qualcomm, EPFL, France)*

We generalize probabilistic amplitude shaping (PAS) with binary codes [1] to the case of non-binary codes defined over prime finite fields. Firstly, we introduce probabilistic shaping via time sharing where shaping applies to information symbols only. Then, we design circular quadrature amplitude modulations (CQAM) that allow to directly generalize PAS to prime finite fields with full shaping. [1] G. Böcherer, F. Steiner, and P. Schulte, "Bandwidth efficient and rate-matched Low-Density Parity-Check coded modulation," IEEE Trans. Commun., vol. 63, no. 12, pp. 4651-4665, Dec. 2015.

Successive Local and Successive Global Omniscience (15:00)

Anoosheh Heidarzadeh *(Texas A&M University, USA); Alex Sprintson (Texas A&M University, USA)*

This paper considers two generalizations of the cooperative data exchange problem, referred to as the *successive local omniscience* (SLO) and the *successive global omniscience* (SGO). The users are divided into ℓ nested sub-groups. Each user initially knows a subset of packets in a ground set X of size k, and all users wish to learn all packets in X. The users exchange their packets by broadcasting coded or uncoded packets. In SLO or SGO, in the lth ($1 \leq l \leq \ell$) round of transmissions, the lth smallest sub-group of users need to learn all packets they collectively hold or all packets in X, respectively. The problem is to find the minimum sum-rate (i.e., the total transmission rate by all users) for each round, subject to minimizing the sum-rate for the previous round. To solve this problem, we use a linear-programming approach. For the cases in which the packets are randomly distributed among users, we construct a system of linear equations whose solution characterizes the minimum sum-rate for each round with high probability as k tends to infinity. Moreover, for the special case of two nested groups, we derive closed-form expressions, which hold with high probability as k tends to infinity, for the minimum sum-rate for each round.

Noncoherent Massive Space-Time Codes with PSK Modulation for Uplink Network Communications (15:20)

Jian-Kang Zhang (McMaster University, Canada); Shuangzhi Li (Zhengzhou University, P.R. China); Xiaomin Mu (Zhengzhou University, P.R. China)

We consider a multi-user massive MIMO uplink system in which there are multiple users with each having a single antenna and one base station (BS) with a large number of antennas. It is assumed that each user and BS have neither small scale nor large scale channel state information. For such a noncoherent system, we systematically design a series of absolutely additively uniquely decomposable constellation pairs (AAUDCPs) using the phase-shift keying (PSK) constellations such that when any linear combination of two PSK constellation points with positive weighting coefficients is received, each individual PSK signal can be uniquely decoded. With this, a novel noncoherent massive space-time block code with PSK modulation is developed for the system. In a noise-free case, we prove that when the number of antenna at BS grows

to infinite, the transmitted symbols and uplink channel can be uniquely determined if the channel coherence time is at least equal to the number of users. In a noisy case, a robust Euclidean distance receiver is developed for efficiently and effectively estimating both the channel coefficients and the transmitted signals.

FPLinQ: A Cooperative Spectrum Sharing Strategy for Device-to-Device Communications (15:40)

Kaiming Shen (University of Toronto, Canada); Wei Yu (University of Toronto, Canada)

Interference management is a fundamental problem for the device-to-device (D2D) network, in which transmitter and receiver pairs may be arbitrarily located geographically with full frequency reuse, so active links may severely interfere with each other. This paper devises a new optimization strategy called FPLinQ that coordinates link scheduling decisions together with power control among the interfering links throughout the network. Scheduling and power optimization for the interference channel are challenging combinatorial and nonconvex optimization problems. This paper proposes a fractional programming (FP) approach that derives a problem reformulation whereby the optimization variables are determined analytically in each iterative step. As compared to the existing works of FlashLinQ, ITLinQ and ITLinQ+, a merit of the proposed strategy is that it does not require tuning of design parameters. FPLinQ shows significant performance advantage as compared to the benchmarks in maximizing system throughput in a typical D2D network.

On the Effective Rate of MISO/TAS Systems in Rayleigh Fading (16:00)

Yazan Al-Badarneh (Texas A&M University, USA); Costas Georghiades (Texas A&M University, USA); Carlos Mejia (Texas A&M University, USA)

The effective rate is an important metric that takes delay quality of service (QoS) requirements into consideration while analyzing the performance of wireless systems. In this paper we analyze the effective rate of multiple-input single-output (MISO) systems with transmit antenna selection (TAS) subject to Rayleigh fading. Specifically, we derive a closed-form expression for the effective rate of MISO/ TAS systems. We also derive closed form expressions for the effective rate in asymptotically high and low signal-to-noise ratio (SNR) regimes. Furthermore, we analyze the effective rate of MISO/ TAS systems with large of number of transmit antennas and derive an asymptotic closed-form expression for it.

Th3-8: Compressed Sensing 4

Thursday, June 29, 14:40-16:20
Room: K7+8
Chair: Bernard Fleury (Aalborg University, Denmark)

Generalized Expectation Consistent Signal Recovery for Nonlinear Measurements (14:40)

Hengtao He *(Southeast University, P.R. China); Chao-Kai Wen (National Sun Yat-sen University, Taiwan); Shi Jin (Southeast University, P.R. China)*

In this paper, we propose a generalized expectation consistent signal recovery algorithm to estimate the signal $\mathbf{x}$ from the nonlinear measurements of a linear transform output $\mathbf{z} = \mathbf{A}\mathbf{x}$. This estimation problem has been encountered in many applications, such as communications with front-end impairments, compressed sensing, and phase retrieval. The proposed algorithm extends the prior art called generalized turbo signal recovery from a partial discrete Fourier transform matrix $\mathbf{A}$ to a class of general matrices. Numerical results show the excellent agreement of the proposed algorithm with the theoretical Bayesian-optimal estimator derived using the replica method.

Universality of the Elastic Net Error (15:00)

Andrea Montanari (Stanford University, USA); ***Phan Minh Nguyen*** *(Stanford University, USA)*

We consider the problem of reconstructing a vector $\boldsymbol{x}_0 \in \mathbb{R}^n$ from noisy linear observations $\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x}_0 + \boldsymbol{w}$, where $\boldsymbol{A} \in \mathbb{R}^{m\times n}$ is a known operator and $\boldsymbol{w}$ is a noise vector, using the elastic net method. Assuming that $\boldsymbol{A}$ is random with independent and identically distributed entries, and under suitable moment conditions, we prove the following universality result. In the high-dimensional asymptotics $n \to \infty$ and $\frac{m}{n} \to \delta > 0$, the normalized error of the elastic net minimizer converges in probability to a limit, that does not depend on the exact distribution that the entries are drawn from. We also provide an explicit formula for the limit.

Using Mutual Information for Designing the Measurement Matrix in Phase Retrieval Problems (15:20)

Nir Shlezinger (Ben Gurion University, Israel); ***Ron Dabora*** *(Ben-Gurion University, Israel); Yonina Eldar (Technion-Israel Institute of Technology, Israel)*

In the phase retrieval problem, the observations consist of the magnitude of a linear transformation of the signal of interest (SOI) with additive noise, where the linear transformation is typically referred to as measurement matrix. The objective is then to reconstruct the SOI from the observations up to an inherent phase ambiguity. Many works on phase retrieval assume

that the measurement matrix is a random Gaussian matrix, which in the noiseless scenario with sufficiently many measurements guarantees uniqueness of the mapping between the SOI and the observations. However, in many applications, e.g., optical imaging, the measurement matrix corresponds to the underlying physical setup, and is therefore a deterministic matrix with structure constraints. In this work we study the design of deterministic measurement matrices, aimed at maximizing the mutual information between the SOI and the observations. We characterize necessary conditions for the optimal measurement matrix, and propose a practical design method for measurement matrices corresponding to masked Fourier measurements. Simulation tests of the proposed method show that it achieves the same performance as random Gaussian matrices for various phase recovery algorithms.

Information Theoretic Limits for Linear Prediction with Graph-Structured Sparsity (15:40)

Adarsh Barik (Purdue University, USA); Jean Honorio (Purdue University, USA); Mohit Tawarmalani (Purdue University, USA)

We analyze the necessary number of samples for sparse vector recovery in a noisy linear prediction setup. This model includes problems such as linear regression and classification. We focus on structured graph models. In particular, we prove that sufficient number of samples for the weighted graph model proposed by Hegde and others is also necessary. We use the Fano's inequality on well constructed ensembles as our main tool in establishing information theoretic lower bounds.

Improved Bounds for Universal One-bit Compressive Sensing (16:00)

Jayadev Acharya (Cornell University, USA); Arnab Bhattacharyya (Indian Institute of Science, India); ***Pritish Kamath*** *(Massachusetts Institute of Technology, USA)*

Unlike compressive sensing where the measurement outputs are assumed to be real-valued and have infinite precision, in "one-bit compressive sensing", measurements are quantized to one bit, their signs. In this work, our contributions are as follows: 1. We show how to recover the support of sparse high-dimensional vectors in the 1-bit compressive sensing framework with an asymptotically near-optimal number of measurements. We do this by showing an equivalence between the task of support recovery using 1-bit compressive sensing and a well-studied combinatorial object known as Union Free Families. 2. We also improve the bounds on the number of measurements for approximately recovering vectors from 1-bit compressive sensing measurements. All our results are about universal measurements, namely the measurement schemes that work simultaneously for all sparse vectors. Our improved bounds naturally lead the way to suggest several interesting open problems.

Th3-9: Signal Processing

Thursday, June 29, 14:40-16:20
Room: K9
Chair: Negar Kiyavash (University of Illinois at Urbana-Champaign, USA)

Principal Pivot Transforms on Radix-2 DFT-type Matrices (14:40)

Sian-Jheng Lin *(University of Science and Technology of China, P.R. China); Amira Alloum (Nokia Bell Labs, France); Tareq Y. Al-Naffouri (King Abdullah University of Science and Technology, USA)*

In this paper, we discuss the principal pivot transforms (PPT) on a family of matrices, called the radix-2 DFT-type matrices. Given a transformation matrix, the PPT of the matrix is a transformation matrix with exchanging some entries between the input array and the output array. The radix-2 DFT-type matrices form a classification of matrices such that the transformations by the matrices can be calculated via radix-2 butterflies. A number of well-known matrices, such as radix-2 DFT matrices and Hadamard matrices, belong to this classification. In this paper, the sufficient conditions for the PPTs on radix-2 DFT-type matrices are given, such that their transformations can also be computed in $O(n \lg n)$. Then based on the results above, an encoding algorithm for systematic Reed-Solomon (RS) codes in $O(n \lg n)$ field operations is presented.

Adversarial Principal Component Analysis (15:00)

Daniel Pimentel-Alarcon (University of Wisconsin-Madison, USA); Aritra Biswas (University of Wisconsin-Madison, USA); Claudia Solis-Lemus (University of Wisconsin-Madison, USA)

This paper studies the following question: where should an adversary place an outlier of a given magnitude in order to maximize the error of the subspace estimated by PCA? We give the exact location of this "worst" possible outlier, and the exact expression of the maximum possible error. Equivalently, we determine the information-theoretic bounds on how much an outlier can "tilt" a subspace in its direction. This in turn provides universal (worst-case) error bounds for PCA under arbitrary noisy settings. Our results also have several implications on adaptive PCA, online PCA, and rank-one updates. We illustrate our results with a subspace tracking experiment.

Characterization of the stability range of the Hilbert transform with applications to spectral factorization (15:20)

Holger Boche (Technical University Munich, Germany); Volker Pohl (Technische Universität München, Germany)

The Hilbert transform plays an important role in many different applications. Especially in the area of detection and estimation it is closely related to the calculation of the spectral factorization. Generally, it is not possible to calculate the Hilbert transform in closed form. Therefore approximation methods are applied. This paper studies the stability of a general class of approximation algorithms for the Hilbert transform which contains all traditional numerical integration methods. To this end, the paper introduces a scale of signal spaces with finite energy in which a factor $(\log n)^\beta$ measures the concentration of the signal energy in its Fourier coefficients c_n. It will be shown that if the energy concentration is two weak, i.e. if $0 \leq \beta \leq 1$, then every approximation method diverges. Conversely, if the energy concentration is sufficiently good, i.e. if $\beta > 1$, convergent approximation methods do exist and we give a natural characterization of all convergent methods.

Mellin-Transform-Based New Results of the Joint Statistics of Partial Products of Ordered Random Variables (15:40)

Sung Sik Nam (Korea University, Korea); Young-Chai Ko (Korea University, Korea); Mohamed-Slim Alouini (King Abdullah University of Science and Technology (KAUST), Saudi Arabia)

Order statistics find applications in various areas including communications and signal processing. In this paper, we introduce new results of the joint statistics of partial products of ordered random variables (RVs) based on a Mellin-transform-based unified analytical framework. With the proposed approach, we can systematically derive the joint statistics of any partial products of ordered statistics, in terms of the Mellin transform and the probability density function (PDF). Our Mellin-transform-based approach can apply when all the K-ordered RVs are involved even for more complicated cases, when only the Ks (Ks <K) best RVs are also considered. In addition, the closed-form expressions for the exponential RV special case are presented. As an application example, these results can apply to the performance analysis of various wireless communication systems over fading channels.

Optimal Sensor Selection in the Presence of Noise and Interference (16:00)

Afshin Abdi (Georgia Institute of Technology, USA); Faramarz Fekri (Georgia Institute of Technology, USA)

The sensor selection problem arises in many applications ranging from sensor networks for event detection to determining concentrations of bio-markers for disease detection. In this paper, we assume that in addition to noise, there exist interference signals (which can be correlated with the desired signals) corrupting the measurements. We consider two different criteria to measure the performance of the selected sensors; average error and minimax analysis. For each case, the cost function is defined over the reconstruction algorithm (or matrix in the linear case), which in turn, explicitly determines the selected sensors. Therefore, minimizing the cost function with some sparsity constraints on the reconstruction algorithm results in the best subset of sensors and as to how we recover the desired signals from the selected measurements. In this paper, we consider the problem for the linear measurement system in various settings and derive the optimization problems. Finally, we propose various methods to solve these problems, and show the effectiveness of the proposed algorithms through simulations.

Th4-1: Network Coding 2

Thursday, June 29, 16:40-18:20
Room: Amsterdam
Chair: Ron Roth (Technion, Israel)

Circular-shift Linear Network Coding (16:40)

Qifu Sun (University of Science and Technology Beijing, P.R. China); Hanqi Tang (University of Science and Technology Beijing, P.R. China); Zongpeng Li (University of Calgary, Canada); Xiaolong Yang (University of Science & Technology Beijing, P.R. China); Keping Long (University of Science and Technology Beijing, P.R. China)

We study a class of linear network coding (LNC) schemes, called *circular-shift* LNC, whose encoding operations at intermediate nodes consist of only circular-shifts and bit-wise addition (XOR). Departing from existing literature, we systematically formulate circular-shift LNC as a special type of vector LNC, where the local encoding kernels of an L-dimensional circular-shift linear code of degree δ are summation of at most δ cyclic-permutation matrices of size L. Under this framework, an intrinsic connection between scalar LNC and circular-shift LNC is established. In consequence, for some block lengths L, an $(L-1, L)$-fractional circular-shift linear solution of arbitrary degree δ can be efficiently constructed on a multicast network. With different δ, the constructed solution has an interesting encoding-decoding complexity tradeoff, and when $\delta = (L-1)/2$, it requires fewer binary operations for both encoding and decoding processes compared with scalar LNC. While the constructed $(L-1, L)$-fractional solution has one-bit redundancy per edge transmission, we show that this is inevitable, and that circular-shift LNC is insufficient to achieve the

exact capacity of multicast networks.

Coding for Networks of Compound Channels (17:00)

Fariba Abbasi (Sharif Institute of Technology, Iran); Mayank Bakshi (The Chinese University of Hong Kong, Hong Kong)

In this paper, we consider networks where every edge is a compound channel whose transition probability is determined by a global network state. We examine the setting where each edge corresponds to a Binary Symmetric Channel, and the sum of the transition probabilities for all edges satisfies an overall global upper bound. We first consider networks with exactly one source and one sink. For such networks, we show that capacity is given by the smallest min-cut among all permitted networks. We show that routing along with end-to-end error correction is optimal for such networks. Next, we consider networks with one source and multiple sinks with multicast demands. We give upper and lower bounds on the capacity of such networks. The coding strategy that leads to our lower bound is intriguing – it involves both end-to-end error correction across the network as well as link-by-link error correction.

Distributed Decoding of Convolutional Network Error Correction Codes (17:20)

***Hengjie Yang** (Xidian University, P.R. China); Wangmei Guo (Xidian University, P.R. China)*

The decoding problem is addressed in this paper for the scenario that convolutional codes are employed at the source node of the network with linear or convolutional network coding for error correction. Since network errors may disperse or neutralize due to network coding, decoding cannot be done at sink nodes merely based on the minimum Hamming distance between the received and sent sequence. Source decoding is proposed in previous work by multiplying the inverse of the network transfer matrix, where the inverse is hard to compute and sometimes the result is noncausal. Starting from the Maximum A Posteriori (MAP) decoding criterion, we find that it is equivalent to the minimum error weight under our model. Inspired by classical Viterbi algorithm, we propose a Viterbi-like decoding algorithm based on the minimum error weight of combined error vectors, which can be carried out directly at sink nodes and can correct any network errors within the capability of convolutional network error correction codes (CNECC). We then study the distributed decoding of CNECC and give a sufficient condition that is able to realize such a decoding process with the proposed algorithm.

Multiuser Rate-Diverse Network-Coded Multiple Access (17:40)

***Haoyuan Pan** (The Chinese University of Hong Kong, Hong Kong); Lu Lu (The Chinese University of Hong Kong, Hong Kong); Soung Chang Liew (The Chinese University of Hong Kong, Hong Kong)*

This paper presents the first Network-Coded Multiple Access (NCMA) system with multiple users adopting different signal modulations, referred to as rate-diverse NCMA. A distinguishing feature of NCMA is the joint use of physical-layer network coding (PNC) and multiuser decoding (MUD) to boost throughput of multi-packet reception systems. In previous NCMA systems, users adopt the same modulation regardless of their individual channel conditions. This leads to suboptimal throughput for many practical scenarios, especially when different users have widely varying channel conditions. A rate-diverse NCMA system allows different users to use modulations that are commensurate with their channel conditions. A key challenge is the design of PNC mapping and decoding mechanisms in NCMA when different users adopt different modulations. While there have been past work on non-channel-coded rate-diverse PNC, this paper is the first attempt to design channel-coded rate-diverse PNC to ensure the reliability of the overall NCMA system. Specifically, we put forth a symbol-splitting channel coding and modulation design so that PNC/NCMA can work over different modulations. We implemented our rate-diverse NCMA system on software-defined radios. Experimental results show that the throughput of rate-diverse NCMA can outperform the state-of-the-art rate-homogeneous NCMA by 80%. Overall, the introduction of rate diversity significantly boosts the NCMA system throughput in practical scenarios.

Th4-2: Coded Computation

Thursday, June 29, 16:40-18:20
Room: Brussels
Chair: Helmut Bölcskei (ETH Zurich, Switzerland)

Coded convolution for parallel and distributed computing within a deadline (16:40)

Sanghamitra Dutta (Carnegie Mellon University, USA); Viveck Cadambe (Pennsylvania State University, USA); Pulkit Grover (Carnegie Mellon University, USA)

We consider the problem of computing the convolution of two long vectors using parallel processors in the presence of “stragglers”. Stragglers refer to the small fraction of faulty or slow processors that delays the entire computation in time-critical distributed systems. We first show that splitting the vectors into smaller pieces and using a linear code to encode these pieces provides improved resilience against stragglers than

replication-based schemes under a simple, worst-case straggler analysis. We then demonstrate that under commonly used models of computation time, coding can dramatically improve the probability of finishing the computation within a target "deadline" time. As opposed to the more commonly used technique of expected computation time analysis, we quantify the exponents of the probability of failure in the limit of large deadlines. Our exponent metric captures the probability of failing to finish before a specified deadline time, i.e. , the behavior of the "tail". Moreover, our technique also allows for simple closed form expressions for more general models of computation time, e.g. shifted Weibull models instead of only shifted exponentials. Thus, through this problem of coded convolution, we establish the utility of a novel asymptotic failure exponent analysis for distributed systems.

Coded Computation over Heterogeneous Clusters (17:00)

Amirhossein Reisizadeh (University of California, Santa Barbara, USA); Saurav Prakash (University of Southern California, USA); Ramtin Pedarsani (University of California, Santa Barbara, USA); Salman Avestimehr (University of Southern California, USA)

In large-scale distributed computing clusters, such as Amazon EC2, there are several types of "system noise" that can result in major degradation of performance: system failures, bottlenecks due to limited communication bandwidth, latency due to straggler nodes, etc. On the other hand, these systems enjoy abundance of redundancy – a vast number of computing nodes and large storage capacity. There have been recent results that demonstrate the impact of coding for efficient utilization of computation and storage redundancy to alleviate the effect of stragglers and communication bottlenecks in homogeneous clusters. In this paper, we focus on general heterogeneous distributed computing clusters consisting of a variety of computing machines with different capabilities. We propose a coding framework for speeding up distributed computing in heterogeneous clusters with straggling servers by trading redundancy for reducing the latency of computation. In particular, we propose Heterogeneous Coded Matrix Multiplication (HCMM) algorithm for performing distributed matrix multiplication over heterogeneous clusters that is provably asymptotically optimal. Moreover, if the number of worker nodes in the cluster is n, we show that HCMM is $\Theta(\log n)$ times faster than any uncoded scheme. We further provide numerical results demonstrating significant speedups of up to 49% and 34% for HCMM in comparison to the "uncoded" and "homogeneous coded" schemes, respectively.

Coded Computation for Multicore Setups (17:20)

Kangwook Lee (KAIST, Korea); Ramtin Pedarsani (University of California, Santa Barbara, USA); Dimitris Papailiopoulos (UW-Madison, USA); Kannan Ramchandran (University of California at Berkeley, USA)

Consider a distributed computing setup consisting of a mater node and n worker nodes, each equipped with p cores, and a function $f(x) = g(f_1(x), f_2(x), .., f_k(x))$, where each f_i can be computed independently of the rest. Assuming that the worker computational times have exponential tails, what is the minimum possible time for computing f? Can we use coding theory principles to speed up this distributed computation? Unlike the case where the local functions are linear (recently studied in [1]), in the non-linear case, it is not clear if traditional codes can provide any gains due to the high density of the parities. To resolve this problem, we propose the use of codes with sparse generator matrices for assigning local functions to different cores, and provide design guidelines for optimal constructions that minimize the runtime. We show that our coding solution offers (up to a constant factor) optimal performance, and has a provable unbounded gap compared to any uncoded schemes.

High-Dimensional Coded Matrix Multiplication (17:40)

Kangwook Lee (KAIST, Korea); Changho Suh (KAIST, Korea); Kannan Ramchandran (University of California at Berkeley, USA)

Coded computation is a framework for providing redundancy in distributed computing systems to make them robust to slower nodes, or stragglers. In [1], the authors propose a coded computation scheme based on maximum distance separable (MDS) codes for computing the product of two matrices, and this scheme is suitable for the case where one of the matrices is small enough to fit into a single compute node. In this work, we study coded computation involving large matrix multiplication where both matrices are large, and propose a new coded computation scheme, which we call product-coded matrix multiplication. Our analysis reveals interesting insights into which schemes perform best in which regimes. When the number of backup workers scales sub-linearly in the size of the product, the product-coded scheme achieves the best run-time performance. On the other hand, when the number of backup workers scales linearly in the size of the product, the MDS-coded scheme achieves the fundamental limit on the run-time performance. Further, we propose a novel application of low-density-parity-check (LDPC) codes to achieve linear-time decoding complexity, thus allowing our proposed solutions to scale gracefully.

Th4-3: Coded Caching 1

Thursday, June 29, 16:40-18:20
Room: K2
Chair: Giuseppe Caire (Technische Universität Berlin, Germany)

Coded Caching with Partial Adaptive Matching (16:40)

Jad Hachem (University of California, Los Angeles, USA); Nikhil Karamchandani (Indian Institute of Technology Bombay, India); Sharayu Moharir (Indian Institute of Technology Bombay, India); Suhas Diggavi (University of California Los Angeles, USA)

We study the coded caching problem when we are allowed to match users to caches based on their requested files. We focus on the case where caches are divided into clusters and each user can be assigned to a unique cache from a specific cluster. We show that neither the coded delivery strategy (approximately optimal when the user-cache assignment is pre-fixed) nor the uncoded replication strategy (approximately optimal when all caches belong to a single cluster) is sufficient for all memory regimes. We propose a hybrid solution that combines ideas from both schemes and that performs strictly better than both. Finally, we show that this hybrid strategy is approximately optimal in most memory regimes.

Improved Converses and Gap-Results for Coded Caching (17:00)

Chien-Yi Wang (Télécom ParisTech, France); Shirin Saeedi Bidokhti (Stanford University, USA); Michele Wigger (Telecom ParisTech, France)

Improved lower bounds on the worst-case and the average-case rate-memory tradeoffs for the Maddah-Ali&Niesen coded-caching scenario are presented. For any number of users and files and for arbitrary cache sizes, the multiplicative gap between the exact rate-memory tradeoff and the new lower bound is less than 2.315 in the worst-case scenario and less than 2.507 in the average-case scenario.

Coded Caching for Combination Networks with Cache-Aided Relays (17:20)

Ahmed Zewail (Pennsylvania State University, USA); Aylin Yener (Pennsylvania State University, USA)

We study a two-hop cache-aided network, where a layer of relay nodes connects a server and a set of end users, i.e., a combination network. We consider the case where both the relay nodes and the end users have caching capabilities. We provide upper and lower bounds which are applicable to any combination network, noting that previous work had focused on models where the relays do not have caches as well as schemes that were suitable for a special class of combination networks. Utilizing maximum distance separable (MDS) codes, we jointly optimize the placement and the delivery phases, demonstrating the impact of cache memories in alleviating the delivery load over the two hop communications. Moreover, we show how cooperation between the relay nodes and the end users can effectively replace the server during the delivery phase whenever the total memory at each end user and its connected relay nodes is sufficient to store the database.

Asynchronous Coded Caching (17:40)

Hooshang Ghasemi (Iowa State University, USA); Aditya Ramamoorthy (Iowa State University, USA)

Coded caching is a technique that promises huge reductions in network traffic in content-delivery networks. However, the original formulation and several subsequent contributions in the area, assume that the file requests from the users are synchronized, i.e., they arrive at the server at the same time. In this work we formulate and study the coded caching problem when the file requests from the users arrive at different times. We assume that each user also has a prescribed deadline by which they want their request to be completed. In the offline case, we assume that the server knows the arrival times before starting transmission and in the online case, the user requests are revealed to the server over time. We present a LP formulation for the offline case that minimizes the overall rate subject to constraint that each user meets his/her deadline. While the online case is much harder, we demonstrate that in the case when the server wishes to minimize the overall completion time, the online solution can be as good as the offline solution. Our simulation results indicate that in the presence of mild asynchronism, much of the benefit of coded caching can still be leveraged.

Decentralized Coded Caching in Wireless Networks: Trade-off between Storage and Latency (18:00)

Antonious Girgis *(Nile University, Egypt); Ozgur Ercetin (Sabanci University, Turkey); Mohammed Nafie (Cairo University & Nile University, Egypt); Tamer ElBatt (Faculty of Engineering, Cairo University & WINC, Nile University, Egypt)*

This paper studies the decentralized coded caching for a Fog Radio Access Network (F-RAN), whereby two edge-nodes (ENs) connected to a cloud server via fronthaul links with limited capacity are serving the requests of K_r users. We consider all ENs and users are equipped with caches. A decentralized content placement is proposed to independently store contents at each network node during the off-peak hours. After that, we design a coded delivery scheme in order to deliver the user demands during the peak-hours under

the objective of minimizing the normalized delivery time (NDT), which refers to the worst case delivery latency. An information-theoretic lower bound on the minimum NDT is derived for arbitrary number of ENs and users. We evaluate numerically the performance of the decentralized scheme. Additionally, we prove the approximate optimality of the decentralized scheme for a special case when the caches are only available at the ENs.

Th4-4: Shannon Theory and Molecular

Thursday, June 29, 16:40-18:20
Room: K3
Chair: Olivier Lévêque (EPFL, Switzerland)

A Characterization of the Shannon Ordering of Communication Channels (16:40)

Rajai Nasser (École Polytechnique Fédérale de Lausanne, Switzerland)

The ordering of communication channels was first introduced by Shannon. In this paper, we aim to find a characterization of the Shannon ordering. We show that W' contains W if and only if W is the skew-composition of W' with a convex-product channel. This fact is used to derive a characterization of the Shannon ordering that is similar to the Blackwell-Sherman-Stein theorem. Two channels are said to be Shannon-equivalent if each one is contained in the other. We investigate the topologies that can be constructed on the space of Shannon-equivalent channels. We introduce the strong topology and the BRM metric on this space. Finally, we study the continuity of a few channel parameters and operations under the strong topology.

On the Input-Degradedness and Input-Equivalence Between Channels (17:00)

Rajai Nasser (École Polytechnique Fédérale de Lausanne, Switzerland)

A channel W is said to be input-degraded from another channel W' if W can be simulated from W' by randomization at the input. We provide a necessary and sufficient condition for a channel to be input-degraded from another one. We show that any decoder that is good for W' is also good for W. We provide two characterizations for input-degradedness, one of which is similar to the Blackwell-Sherman-Stein theorem. We say that two channels are input-equivalent if they are input-degraded from each other. We study the topologies that can be constructed on the space of input-equivalent channels, and we investigate their properties. Moreover, we study the continuity of several channel parameters and operations under these topologies.

Models and information-theoretic bounds for nanopore sequencing (17:20)

Wei Mao (University of California Los Angeles, USA); Suhas Diggavi (University of California Los Angeles, USA); Sreeram Kannan (University of Washington Seattle, USA)

Nanopore sequencing is an emerging new technology for sequencing DNA, which can read long fragments of DNA (50,000 bases) unlike most current sequencers which can only read hundreds of bases. While nanopore sequencers can acquire long reads, the high error rates ($\approx$ 30%) pose a technical challenge. In a nanopore sequencer, a DNA is migrated through a nanopore and current variations are measured. The DNA sequence is inferred from this observed current pattern using an algorithm called a *base-caller*. In this paper, we propose a mathematical model for the “channel” from the input DNA sequence to the observed current, and calculate bounds on the information extraction capacity of the nanopore sequencer. This model incorporates impairments like inter-symbol interference, deletions, as well as random response. The practical application of such information bounds is two-fold: (1) benchmarking present base-calling algorithms, and (2) offering an optimization objective for designing better nanopore sequencers.

Less Noisy Domination by Symmetric Channels (17:40)

Anuran Makur (Massachusetts Institute of Technology, USA); Yury Polyanskiy (MIT, USA)

Consider the family of all q-ary symmetric channels (q-SCs) with capacities decreasing from log(q) to 0. This paper addresses the following question: what is the member of this family with the smallest capacity that dominates a given channel V in the ”less noisy” preorder sense. When the q-SCs are replaced by q-ary erasure channels, this question is known as the ”strong data processing inequality.” We provide several equivalent characterizations of the less noisy preorder in terms of chi-squared-divergence, Loewner (PSD) partial order, and spectral radius. We then illustrate a simple criterion for domination by a q-SC based on degradation, and mention special improvements for the case where V is an additive noise channel over an Abelian group of order q. Finally, as an application, we discuss how logarithmic Sobolev inequalities for q-SCs, which are well-studied, can be transported to an arbitrary channel V.

Capacity of Molecular Channels with Imperfect Particle-Intensity Modulation and Detection (18:00)

Nariman Farsad (Stanford University, USA); Christopher Rose (Brown University, USA); Muriel Médard (MIT, USA); Andrea Goldsmith (Stanford University, USA)

This work introduces the particle-intensity channel (PIC) as a model for molecular communication systems and characterizes the properties of the optimal input distribution and the capacity limits for this system. In the PIC, the transmitter encodes information, in symbols of a given duration, based on the number of particles released, and the receiver detects and decodes the message based on the number of particles detected during the symbol interval. In this channel, the transmitter may be unable to control precisely the number of particles released, and the receiver may not detect all the particles that arrive. We demonstrate that the optimal input distribution for this channel always has mass points at zero and the maximum number of particles that can be released. We then consider diffusive particle transport, derive the capacity expression when the input distribution is binary, and show conditions under which the binary input is capacity-achieving. In particular, we demonstrate that when the transmitter cannot generate particles at a high rate, the optimal input distribution is binary.

Th4-5: Bounds 3

Thursday, June 29, 16:40-18:20
Room: K4
Chair: I-Hsiang Wang (National Taiwan University, Taiwan)

Information-theoretic Limits of Subspace Clustering (16:40)

***Kwangjun Ahn** (KAIST, Korea); Kangwook Lee (KAIST, Korea); Changho Suh (KAIST, Korea)*

Subspace clustering is a celebrated problem that comes up in a variety of applications such as motion segmentation and face clustering. The goal of the problem is to find clusters in different subspaces from similarity measurements across data points. While the algorithmic aspect of this problem has been extensively studied in the literature, the information-theoretic limit on the number of similarities required for reliable clustering has been unknown. In this paper, we translate the problem into an instance of community recovery in hypergraphs, and characterize the sharp threshold on the limit required for exact subspace clustering. Moreover, we present a computationally efficient algorithm that achieves the fundamental limit.

The Error Exponent of Sparse Regression Codes with AMP Decoding (17:00)

Cynthia Rush (Columbia University, USA); Ramji Venkataramanan (University of Cambridge, United Kingdom (Great Britain))

Sparse regression codes (SPARCs) are a recent class of codes for reliable communication over the AWGN channel at rates approaching the channel capacity. Approximate message passing (AMP) decoding, a computationally efficient technique for decoding SPARCs, has been proven to be asymptotically capacity-achieving for the AWGN channel. In this paper, we refine the asymptotic results by deriving a large deviations bound on the probability of AMP decoding error. This bound shows that for an appropriate choice of code parameters and any fixed rate smaller than the AWGN capacity, the probability of decoding error decays exponentially in $n/(\log n)^{2T}$, where T is the number of AMP iterations required for successful decoding. The number of iterations T is proportional to the inverse of the logarithm of the ratio of channel capacity to rate. For the above choice of code parameters, the complexity of the AMP decoder scales as a low-order polynomial in the block length n.

Lower Bounds on the Number of Write Operations by Index-less Indexed Flash Code with Inversion Cells (17:20)

Akira Yamawaki (Gifu University, Japan); Hiroshi Kamabe (Gifu University, Japan); Shan Lu (Gifu University, Japan)

Index-less indexed flash code (ILIFC) is a coding scheme for flash memories in which one bit of a data sequence is stored in a slice consisting of several cells but the index of the bit is stored implicitly. Although several modified ILIFC schemes have been proposed, in this study we consider an ILIFC with inversion cells (I-ILIFC). The I-ILIFC reduces the total number of cell level changes at each write request. Computer simulation is used to show that the I-ILIFC improves the average performance of ILIFC in many cases. This paper presents our derivation of the lower bound on the number of write operations by I-ILIFC. Additionally, we consider another lower bound thereon and show that the threshold of the code length that determines whether the I-ILIFC improves the worst-case performance of the ILIFC is smaller than that in the first lower bound. Lastly, we analyze the asymptotic performance of the I-ILIFC in the worst case.

Partial Data Extraction via Noisy Histogram Queries: Information Theoretic Bounds (17:40)

Wei-Ning Chen (National Taiwan University, Taiwan); I-Hsiang Wang (National Taiwan University, Taiwan)

The problem of extracting data via noisy histogram queries is investigated. A data set is a collection of

items, and each item carries a piece of categorical data taking values in a finite alphabet. Data analysts are allowed to query the data set by specifying a subset and then obtain the histogram of the queried subset. The histogram released by the curator, however, is perturbed by some noise with magnitude δ_n. The reconstruction is successful if the Hamming distance between the reconstructed data set and the actual data set is less than a tolerance parameter k_n. In this work, we prove several sharp upper and lower bounds on the minimum query complexity T_n^* for successful reconstruction, which depends on the noise level δ_n and the tolerance level k_n. We first show that if the noise-tolerance condition $\delta_n = O(kn^(1/2))$ is satisfied, the minimum query complexity $T_n = \Theta(n/logn)$, where the achievability is based on random sampling and the converse is based on counting and packing arguments. On the other hand, if $\delta_n = \Omega(kn^(1+\epsilon)/2)$ for some $\epsilon > 0$, we prove that $T_n = \omega(n^p)$ for any positive integer p. In words, no querying methods with Poly(n) query complexity can successfully reconstruct the data set in that regime. This impossibility result is established by a novel combinatorial lower bound on T_n (converse).

Asymptotics of the Error Probability in Quasi-Static Binary Symmetric Channels (18:00)

Josep Font-Segura (Universitat Pompeu Fabra, Spain); Alfonso Martinez (Universitat Pompeu Fabra, Spain); Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra & University of Cambridge, Spain)

This paper provides an asymptotic expansion of the error probability, as the codeword length n goes to infinity, in quasi-static binary symmetric channels. After the leading term, namely the outage probability, the following two terms are found to be proportional to (log n)/n and 1/n respectively. Explicit characterizations of the respective coefficients are given. The resulting expansion gives an accurate approximation to the random-coding union for even small codeword lengths.

Th4-6: Wireless Networks 2

Thursday, June 29, 16:40-18:20
Room: K5
Chair: Randall Berry (Northwestern University, USA)

Commitment in regulatory spectrum games: Examining the first-player advantage (16:40)

Vidya Muthukumar (UC Berkeley, USA); Anant Sahai (UC Berkeley, USA)

Recent advances in dynamic spectrum sharing have led to renewed focus on the structure of regulatory games between a primary, incumbent user and a secondary, opportunistic user of a spectrum band. The primary user has to decide to what extent it invokes the services of the regulator, and the secondary user has to decide how to operate in the spectrum band. This paper builds on a mathematical model for light-handed regulation using “spectrum jails” to show that the order of play and amount of commitment matters. A primary that can commit to its strategy before the game is able to reduce its equilibrium cost, even when the secondary best responds to the committed strategy. We compare the ensuing Stackelberg game with the simultaneous primary-secondary game. We also introduce a new concept of *partial* commitment by which the primary can only commit to a range of strategies using a finite number of bits. We show explicitly that the more the primary commits to, the more it benefits, and that Stackelberg commitment can be understood as a limit of infinite “commitment bits”.

Inferring Network Topology from Information Cascades (17:00)

Feng Ji *(Nanyang Technological University, Singapore); Wenchang Tang (Nanyang Technological University, Singapore); Wee Peng Tay (Nanyang Technological University, Singapore); Edwin Chong (Colorado State University, USA)*

We study the problem of inferring the graph structure of a network using knowledge of information cascades in the network. Unlike previous studies, which assume knowledge of the distributions of information diffusion across edges in the network, we only require that diffusion along different edges in the network be independent together with limited information on their distributions (e.g., just the means). We introduce the concept of a separating vertex set for a graph, which is a set of vertices in which for any two given distinct vertices of the graph, one can find a vertex whose distance to them are different. We show that a necessary condition for reconstructing a tree perfectly using distance information between pairs of vertices is given by the size of an observed separating vertex set. We then propose an algorithm to recover the tree structure using infection times, whose differences have means corresponding to the distance between two vertices. To improve the accuracy, we propose the concept of redundant vertices, which allows us to perform averaging to better estimate the distance between two vertices. Though the theory is developed mainly for trees, we demonstrate how the algorithm can be extended heuristically to general graphs. Simulation results suggest that our proposed algorithm performs better than some current state-of-the-art network reconstruction methods.

Statistical beamforming for the large antenna broadcast channel (17:20)

Vasanthan Raghavan *(Qualcomm, Inc., USA); Junil Choi (POSTECH, Korea); David Love (Purdue University, USA)*

This paper studies the broadcast channel with M antennas at the base-station and M single antenna users. Most of the works in the literature assume perfect channel state information at both ends of each link. In this work, we assume that these links are spatially correlated and only the long-term statistical information corresponding to the covariance matrices of the links are available at both ends. We are interested in the design of beamforming vectors for data transmission to the M users to maximize the ergodic sum-rate obtained by treating interference as noise. In the simpler M = 2 setting, prior work has shown the optimality of a generalized eigenvector beamformer structure for this problem. However, these results are not easily extendable to the general M user setting. We overcome these difficulties by first establishing a tractable approximation for the ergodic sum-rate in terms of the beamforming vectors and covariance matrices that is surprisingly asymptotically tight in M. We then cast the sum-rate approximation maximization problem as a manifold optimization and illustrate the optimality of the generalized eigenvector structure in the general M user setting.

Efficient Resource Allocation in Mobile-edge Computation Offloading: Completion Time Minimization (17:40)

Quy Hong Le (Technische Universitaet Darmstadt, Germany); Hussein Al-Shatri (TU Darmstadt, Germany); Anja Klein (TU Darmstadt, Germany)

Mobile-edge computation offloading (MECO) is a promising solution for enhancing the capabilities of mobile devices. For an optimal usage of the offloading, a joint consideration of radio resources and computation resources is important, especially in multiuser scenarios where the resources must be shared between multiple users. We consider a multi-user MECO system with a base station equipped with a single cloudlet server. Each user can offload its entire task or part of its task. We consider parallel sharing of the cloudlet, where each user is allocated a certain fraction of the total computation power. The objective is to minimize the completion time of users' tasks. Two different access schemes for the radio channel are considered: Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA). For each access scheme, we formulate the corresponding joint optimization problem and propose efficient algorithms to solve it. Both algorithms use the bisection-search method, where each step requires solving a feasibility problem. For TDMA, the feasibility problem has a closed-form solution. Numerical results show that the performance of offloading is higher than of local computing. In particular, MECO with FDMA outperforms MECO with TDMA, but with a small margin.

Scalable Spectrum Allocation for Large Networks Based on Sparse Optimization (18:00)

Binnan Zhuang (Samsung Semiconductor, Inc., USA); Dongning Guo (Northwestern University, USA); Ermin Wei (Northwestern University, USA); Michael Honig (Northwestern University, USA)

Joint allocation of spectrum and user association is considered for a large cellular network. The objective is to optimize a network utility function such as average delay given traffic statistics collected over a slow timescale. A key challenge is scalability: given n Access Points (APs), there are $O(2^n)$ ways in which the APs can share the spectrum. The number of variables is reduced from $O(2^n)$ to $O(nk)$, where k is the number of users, by optimizing over local overlapping neighborhoods, defined by interference conditions, and by exploiting the existence of sparse solutions in which the spectrum is divided into $k+1$ segments. We reformulate the problem by optimizing the assignment of subsets of active APs to those segments. An ℓ_0 constraint enforces a one-to-one mapping of subsets to spectrum, and an iterative (reweighted ℓ_1) algorithm is used to find an approximate solution. Numerical results for a network with 100 APs serving several hundred users show the proposed method achieves a substantial increase in total throughput relative to benchmark schemes.

Th4-7: Random Access Channels

Thursday, June 29, 16:40-18:20
Room: K6
Chair: Robert Calderbank (Duke University, USA)

A perspective on massive random-access (16:40)

Yury Polyanskiy (MIT, USA)

This paper discusses the contemporary problem of providing multiple-access (MAC) to massive number of uncoordinated users. First, we define a random-access code for K_a-user Gaussian MAC to be a collection of norm-constrained vectors such that the noisy sum of any K_a of them can be decoded with a given (suitably defined) probability of error. An achievability bound for existence of such codes is proposed and compared against popular practical solutions: ALOHA, coded slotted ALOHA, CDMA, and treating interference as noise. It is found out that as the number of users increases existing solutions become vastly energy-inefficient. Second, we discuss the asymptotic (in blocklength) problem of coding for a K-user Gaussian MAC when K is proportional to blocklength and each user's payload is fixed. It is discovered that the energy-per-bit vs. spectral efficiency exhibits a rather

curious tradeoff in this case.

Low Complexity Schemes for the Random Access Gaussian Channel (17:00)

Or Ordentlich (MIT, USA); Yury Polyanskiy (MIT, USA)

We consider an uncoordinated Gaussian multiple access channel with a relatively large number of active users within each block. A low complexity coding scheme is proposed, which is based on a combination of compute-and-forward and coding for a binary adder channel. For a wide regime of parameters of practical interest, the energy-per-bit required by each user in the proposed scheme is significantly smaller than that required by popular solutions such as slotted-ALOHA and treating interference as noise.

Multi-Cell Aware Opportunistic Random Access (17:20)

Huifa Lin (Dankook University, Korea); Won-Yong Shin (Dankook University, Korea)

We propose a decentralized multi-cell aware opportunistic random access (MA-ORA) protocol that almost achieves the optimal throughput scaling in a K-cell random access network with one access point (AP) and N users in each cell. Under our MA-ORA protocol, users opportunistically transmit with a predefined physical layer data rate in a decentralized manner if the desired signal power to the serving AP is sufficiently large and the generating interference power to other APs is sufficiently small. It is proved that the aggregate throughput scales as $\frac{K}{e}(1-\epsilon)\log(\mathsf{SNR}\log N)$ in a high signal-to-noise ratio (SNR) regime if N scales faster than $\mathsf{SNR}^{\frac{K-1}{1-\delta}}$ for small constants $\epsilon, \delta > 0$. Our analytical result is validated by computer simulations.

Multi-Channel Random Access with Replications (17:40)

Olga Galinina (Tampere University of Technology, Finland); Andrey Turlikov (Saint-Petersburg State University of Aerospace Instrumentation, Russia); Sergey Andreev (Tampere University of Technology, Finland); Yevgeni Koucheryavy (Tampere University of Technology, Finland)

This paper considers a class of multi-channel random access algorithms, where contending devices may send multiple copies (replicas) of their messages to the central base station. We first develop a hypothetical algorithm that delivers a lower estimate for the access delay performance within this class. Further, we propose a feasible access control algorithm achieving low access delay by sending multiple message replicas, which potentially approaches the hypothetical case. The resulting performance is readily approximated by a simple lower bound, which is derived for a large number of channels.

Th4-8: Index Coding 1

Thursday, June 29, 16:40-18:20
Room: K7+8
Chair: Lawrence Ong (The University of Newcastle, Australia)

Private Broadcasting: an Index Coding Approach (16:40)

*Mohammed Karmoose (UCLA, USA); Linqi Song (University of California, Los Angeles, USA); **Martina Cardone** (University of Califonia, Los Angeles, USA); Christina Fragouli (UCLA, USA)*

Using a broadcast channel to transmit clients' data requests may impose privacy risks. In this paper, we tackle such privacy concerns in the index coding framework. We show how a curious client can infer some information about the requests and side information of other clients by learning the encoding matrix used by the server. We propose an information-theoretic metric to measure the level of privacy and show how encoding matrices can be designed to achieve specific privacy guarantees. We then consider a special scenario for which we design a transmission scheme and derive the achieved levels of privacy in closed-form. We also derive upper bounds and we compare them to the levels of privacy achieved by our scheme, highlighting that an inherent trade-off exists between protecting privacy of the request and of the side information of the clients.

Golden-Coded Index Coding (17:00)

Yu-Chih Huang (National Taipei University, Taiwan); Yi Hong (Monash University, Australia); Emanuele Viterbo (Monash University, Australia)

We study the problem of constructing good space-time codes for broadcasting K independent messages over a MIMO network to L users, where each user demands all the messages and already has a subset of messages as side information. As a first attempt, we consider the 2x2 case and propose golden-coded index coding by partitioning the golden codes into K subcodes, one for each message. The proposed scheme is shown to have the property that for any side information configuration, the minimum determinant of the code increases exponentially with the amount of information contained in the side information.

Generalized Index Coding Problem and Discrete Polymatroids (17:20)

*Anoop Thomas (Indian Institute of Science, India); **B. Sundar Rajan** (Indian Institute of Science, India)*

The index coding problem has been generalized re-

cently to accommodate receivers which demand functions of messages and which possess functions of messages. The connections between index coding and matroid theory have been well studied in the recent past. Index coding solutions were first connected to multi linear representation of matroids. For vector linear index codes discrete polymatroids which can be viewed as a generalization of the matroids was used. It was shown that a vector linear solution to an index coding problem exists if and only if there exists a representable discrete polymatroid satisfying certain conditions. In this work we explore the connections between generalized index coding and discrete polymatroids. The conditions that needs to be satisfied by a representable discrete polymatroid for a generalized index coding problem to have a vector linear solution is established. From a discrete polymatroid we construct an index coding problem with coded side information and show that if the index coding problem has a certain optimal length solution then the discrete polymatroid satisfies certain properties. Furthermore, from a matroid we construct a similar generalized index coding problem and show that it has a binary scalar linear solution of optimal length if and only if the matroid is binary representable.

A Pliable Index Coding Approach to Data Shuffling (17:40)

Linqi Song (University of California, Los Angeles, USA); Christina Fragouli (UCLA, USA); Tianchu Zhao (Tsinghua University, P.R. China)

A promising research area that has recently emerged, is on how to use index coding to improve the communication efficiency in distributed computing systems, especially for data shuffling in iterative computations. In this paper, we posit that pliable index coding can offer a more efficient framework for data shuffling, as it can better leverage the many possible shuffling choices to reduce the number of transmissions. We theoretically analyze pliable index coding under data shuffling constraints, and design an hierarchical data-shuffling scheme that uses pliable index coding as a component. We find benefits up to $O(ns/m)$ over index coding, where ns/m is the average number of workers caching a message, and m, n, and s are the numbers of messages, workers, and cache size, respectively.

Th4-9: Compression 2

Thursday, June 29, 16:40-18:20
Room: K9
Chair: Stefano Rini (National Chiao Tung University, Taiwan)

Fixed-Length-Parsing Universal Compression with Side Information (16:40)

***Yeohee Im** (Princeton University, USA); Sergio Verdú (Princeton University, USA)*

This paper presents a fixed-length-parsing universal compression algorithm for settings where compressor and decompressor share the same side information. We prove the optimality of the algorithm for any stationary processes. Furthermore, strategies to modify the algorithm are suggested in order to lower the data compression rate.

Coding Theorems for the Compress and Estimate Source Coding Problem (17:00)

Alon Kipnis (Stanford University, USA); Stefano Rini (National Chiao Tung University, Taiwan); Andrea Goldsmith (Stanford University, USA)

We consider the remote source coding setting in which a source realization is estimated from a lossy compressed sequence of noisy observations. Unlike in the optimal remote source coding problem, however, the encoder is bound to use good codes with respect to the observation sequence, i.e., codes that are optimal for the lossy reconstruction of the observation, rather than the remote source. This encoding strategy is denoted as the compress-and-estimate (CE) scheme. For the case of an i.i.d source observed through a memoryless channel, we show that the distortion in the CE scheme is characterized by a single-letter expression, referred to as the CE distortion-rate function (CE-DRF). In particular, we show that the CE-DRF can be attained by estimating the source from the output of a remote encoder employing any sequence of good codes with respect to the observation sequence. In addition, we show that the limiting distortion in estimating any finite sub-block of the source realization from the output of a remote encoder employing good codes, averaged over all sub-blocks, is also bounded by the CE-DRF.

Row-centric lossless compression of Markov images (17:20)

Matthew Reyes (University of Michigan, USA); David Neuhoff (University of Michigan, USA)

Motivated by the question of whether the recently introduced Reduced Cutset Coding (RCC) offers rate-complexity performance benefits over conventional context-based conditional coding for sources with two-

dimensional Markov structure, this paper compares several row-centric coding strategies that vary in the amount of conditioning as well as whether a model or an empirical table is used in the encoding of blocks of rows. The conclusion is that, at least for sources exhibiting low-order correlations, 1-sided model-based conditional coding is superior to the method of RCC for a given constraint on complexity, and conventional context-based conditional coding is nearly as good as the 1-sided model-based coding.

A Practical Approach for Successive Omniscience (17:40)

Ni Ding (The Australian National University, Australia); Rodney Kennedy (The Australian National University, Australia); Parastoo Sadeghi (The Australian National University, Australia)

The system that we study in this paper contains a set of users that observe a discrete memoryless multiple source and communicate via noise-free channels with the aim of attaining omniscience, the state that all users recover the entire multiple source. We adopt the concept of successive omniscience (SO), i.e., letting the local omniscience in some user subset be attained before the global omniscience in the entire system, and consider the problem of how to efficiently attain omniscience in a successive manner. Based on the existing results on SO, we propose a CompSetSO algorithm for determining a complimentary set, a user subset in which the local omniscience can be attained first without increasing the sum-rate, the total number of communications, for the global omniscience. We also derive a sufficient condition for a user subset to be complimentary so that running the CompSetSO algorithm only requires a lower bound, instead of the exact value, of the minimum sum-rate for attaining global omniscience. The CompSetSO algorithm returns a complimentary user subset in polynomial time. We show by example how to recursively apply the CompSetSO algorithm so that the global omniscience can be attained by multi-stages of SO.

Fr1-1: Lattice Codes 2

Friday, June 30, 09:50-11:10
Room: Europa
Chair: Robert Fischer (Ulm University, Germany)

On the Universality of Lattice Codes for a Class of Ergodic Fading Channels (09:50)

Ahmed Hindy (University of Texas at Dallas, USA); ***Aria Nosratinia*** *(University of Texas, Dallas, USA)*

One of the main challenges of communication in the absence of transmitter channel knowledge is codebook universality, i.e., the existence of a single codebook that guarantees a given rate for all channel states. We address this problem for a class of ergodic fading multiple-input multiple-output (MIMO) channels, whose fading distribution is not necessarily isotropic. It is shown that a universal codebook drawn from a nested lattice code achieves the ergodic capacity to within a constant gap. Interestingly, the gap vanishes in some scenarios.

Index Mapping for Bit-error Resilient Multiple Description Lattice Vector Quantizer (10:10)

Sorina Dumitrescu (McMaster University, Canada); Yifang Chen (McMaster UNiversity, Canada); Jun Chen (McMaster University, Canada)

This work addresses the construction of bit-error resilient multiple description lattice vector quantizers (MDLVQ) by proposing the design of a structured mapping γ of side lattice points to binary indexes. We assume that the first description is correct while the second description may carry bit errors. To design the mapping γ the set of side lattice points is first partitioned into Voronoi regions of an appropriate coarse lattice. Next a good channel code C is selected, each Voronoi region is assigned a coset of this channel code and the side lattice points within each Voronoi region are mapped to binary sequences in the corresponding coset. We derive a lower bound on the error correction performance of the mapping γ in terms of the performance of the code C and we show that, as the rate of the MDLVQ grows to ∞, the mapping γ becomes as good as the code C. Simulation results show the significant superiority of the proposed mapping versus random mappings.

On Shaping Complex Lattice Constellations from Multi-level Constructions (10:30)

Perathorn Pooksombat (Mahidol University, Thailand); J Harshan (Advanced Digital Sciences Center, Singapore); Wittawat Kositwattanarerk (Mahidol University, Thailand)

Construction of lattices is known to have a strong connection to the study of classical linear codes over $\mathbb{F}_2$; one such celebrated construction is that of Barnes-Wall (BW) lattices over $\mathbb{Z}[i]$, with $i = \sqrt{-1}$, wherein a set of nested Reed-Muller codes when weighed over powers of the base $1 + i$ results in the famous *multi-level construction* of BW lattices. Although such a construction facilitates simple encoding and decoding of information bits, the resulting set of codewords needs to be mapped onto their representatives in order to reduce the average energy of the lattice code. Drawing inspiration from the case of BW lattices, in this work, we address a general question of how to arrive at representatives of the codewords of a lattice code over $\mathbb{Z}[\theta]$, where θ is a quadratic integer, that is generated via a multi-level construction over linear codes over $\mathbb{F}_q$, for $q \neq 2$. In particular, we introduce a novel shaping function $\tau : \mathbb{Z}[\theta] \longmapsto \mathbb{Z}[\theta]$ on the components of lattice code-

words, and prove that the natural constellation of lattices from multi-level constructions can be rearranged into a multi-dimensional cubic- or parallelepiped-shape under such a map. We show that our mapping results in a reduction of upto 29.82% in average energy of lattice constellations. Our proposed mapping has applications in communications, particularly in encoding and decoding of lattice codes from multi-level constructions over q-ary linear codes for $q > 2$.

On the Design of Multi-Dimensional Irregular Repeat-Accumulate Lattice Codes (10:50)

Min Qiu *(University of New South Wales, Australia); Lei Yang (University of New South Wales, Australia); Yixuan Xie (University of New South Wales, Australia); Jinhong Yuan (University of New South Wales, Australia)*

We propose and design the lattice codes with finite lattice constellations based on multi-dimensional (more than two dimensions) lattice partitions. The codes are constructed from non-binary irregular repeat-accumulate (IRA) codes. Most notably, we propose a novel encoding structure to ensure that the decoder's messages exhibit permutation-invariance and symmetry properties. With these two properties, the densities of the messages in our iterative decoder can be well modeled by Gaussian distributions described by a single parameter. Under the Gaussian approximation, extrinsic information transfer charts for our multi-dimensional IRA lattice codes are developed and used for analysing the convergence behaviour and optimising the decoding threshold. Simulation results show that our proposed lattice codes outperform the previously designed lattice codes with two-dimensional lattice partitions.

Fr1-2: Polar Codes 3

Friday, June 30, 09:50-11:10
Room: Brussels
Chair: Peter Trifonov (Saint-Petersburg State Polytechnic University, Russia)

Performance Bounds of Concatenated Polar Coding Schemes (09:50)

Dina Goldin (Tel Aviv University, Israel); David Burshtein (Tel Aviv University, Israel)

A concatenated coding scheme using a polarization transformation followed by outer sub-codes is analyzed. Achievable error exponents and upper bounds on the error rate are derived. The first bound is obtained using outer codes which are typical linear codes from the ensemble of parity check matrices whose elements are chosen independently and uniformly. As a byproduct of this bound, it determines the required rate split of the total rate to the rates of the outer codes. A lower bound on the error exponent that holds for all BMS channels with a given capacity is then derived. Improved bounds and approximations for small block-length codes are also obtained. The bounds are compared to actual simulation results from the literature.

Energy-Adaptive Polar Codes: Trading Off Reliability and Decoder Circuit Energy (10:10)

Haewon Jeong *(Carnegie Mellon University, USA); Christopher Blake (University of Toronto, USA); Pulkit Grover (Carnegie Mellon University, USA)*

It is now well known that using a long and complicated error correcting code (ECC) designed for the worst-case error probability requirement wastes excessive total system energy (transmit + circuit energy) when the error probability requirement is much higher than the worst case. We propose a novel adaptive polar coding strategy that adjusts the decoder circuit to consume minimal decoding circuit energy at each given target error requirement. By combining Thompson's VLSI theory and scaling analysis of polar codes, we provide upper bounds on energy, area, and time complexity of polar decoding circuits in terms of target block error probability. The upper bounds are derived from an explicit construction of decoder circuit based on mesh-network structure. Comparison of the upper bounds for non-adaptive polar coding and our proposed adaptive polar coding showed that the adaptive coding strategy has a scaling-sense gain in decoding energy with little circuit area overhead when there is a large gap between the worst-case and typical target error rate requirements.

Polar codes with a stepped boundary (10:30)

Ilya Dumer *(University of California at Riverside, USA)*

We design polar codes of blocklength $n \to \infty$ and code rate $R \to 1$ that achieve the vanishing output error rates on the binary symmetric channels with transition error probability $p \to 0$. These codes have a substantially smaller redundancy order $(1 - R)n$ than do other known high-rate codes, such as Reed-Muller (RM) or BCH codes. The construction is explicit and has complexity of order $n \log n$. We also design asymptotically optimal low-rate codes that achieve the vanishing output error rates if $p \to 1/2$.

Permuted Successive Cancellation Decoding for Polar Codes (10:50)

Sarit Buzaglo (UCSD, USA); Arman Fazeli (University of California, San Diego, USA); Veeresh Taranalli (University of California, San Diego, USA); ***Paul Siegel*** *(University of California, San Diego, USA); Alexander Vardy (University of California San Diego, USA)*

Defined through a certain 2×2 matrix called *Arikan's kernel*, polar codes are known to achieve the symmetric capacity of binary-input discrete memoryless channels under the *successive cancellation* (SC) decoder. Yet, for short block-lengths, polar codes fail to deliver a compelling performance under the low complexity SC decoding scheme. Recent studies provide evidence for improved performance when Arikan's kernel is replaced with larger kernels that have smaller *scaling exponents*. However, for $\ell \times \ell$ kernels the time complexity of the SC decoding increases by a factor of 2^{ℓ}. In this paper we study a special type of kernels called *permuted kernels*. The advantage of these kernels is that the SC decoder for the corresponding polar codes can be viewed as a permuted version of the SC decoder for the conventional polar codes that are defined through Arikan's kernel. This *permuted successive cancellation* (PSC) decoder outputs its decisions on the input bits according to a permuted order of their indices. We introduce an efficient PSC decoding algorithm and show simulations for two 16×16 permuted kernels that have better scaling exponents than Arikan's kernel.

Fr1-3: Multiple Access 3

Friday, June 30, 09:50-11:10
Room: K2
Chair: Young-Han Kim (UCSD, USA)

On the Degrees of Freedom of Wide-Band Multi-Cell Multiple Access Channels With No CSIT (09:50)

Yo-Seb Jeon (POSTECH, Korea); Namyoon Lee (POSTECH, Korea); Ravi Tandon (University of Arizona, USA)

This paper considers a K-cell multiple access channel with inter-symbol interference (ISI). The primary finding of this paper is that, without instantaneous channel state information at a transmitter, the interference-free sum degrees of freedom of K is asymptotically achievable when the number of users per cell is sufficiently large, and also when the number of channel-impulse-response taps of desired links is greater than that of interfering links. This achievability is shown by a blind interference management method that exploits the relativity in delay spreads between desired and interfering links.

Low-Density Code-Domain NOMA: Better Be Regular (10:10)

Ori Shental (Bell Labs, USA); Benjamin Zaidel (Bar-Ilan University, Israel); Shlomo (Shitz) Shamai (The Technion, Israel)

A closed-form analytical expression is derived for the limiting empirical squared singular value density of a channel transfer matrix corresponding to sparse low-density code-domain (LDCD) non-orthogonal multiple-access (NOMA) with regular random user-resource allocation. The derivation relies on associating the channel transfer matrix with the adjacency matrix of a large semiregular bipartite graph. For a simple repetition-based sparse spreading scheme, the result directly follows from a rigorous analysis of spectral measures of infinite graphs. Turning to random (sparse) binary spreading, we harness the cavity method from statistical physics, and show that the limiting spectral density coincides in both cases. This result is then used to compute the normalized input-output mutual information of the underlying vector channel in the large-system limit. The latter may be interpreted as the achievable total throughput per dimension with optimum processing in a corresponding multiple-access channel setting or, alternatively, in a fully-symmetric broadcast channel setting with full decoding capabilities at each receiver. Surprisingly, the total throughput of regular LDCD-NOMA is found to be not only superior to that achieved with irregular user-resource allocation, but also to the total throughput of dense randomly-spread NOMA, for which optimum processing is computationally intractable. In contrast, the superior performance of regular LDCD-NOMA can be potentially achieved with a feasible message-passing algorithm. This observation may advocate employing regular, rather than irregular, LDCD-NOMA in 5G cellular physical layer design.

Capacity Region of a One-Bit Quantized Gaussian Multiple Access Channel (10:30)

Borzoo Rassouli (Imperial College London, United Kingdom (Great Britain)); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain)); Morteza Varasteh (Imperial College, United Kingdom (Great Britain))

The capacity region of a two-transmitter Gaussian multiple access channel (MAC) under average input power constraints is studied, when the receiver employs a zero-threshold one-bit analog-to-digital converter (ADC). It is proved that the input distributions that achieve the boundary points of the capacity region are discrete. Based on the position of a boundary point, upper bounds on the number of the mass points of the corresponding distributions are derived. Finally, a conjecture on the sufficiency of K mass points in a point-to-point real AWGN with a K-bin ADC front end (no matter symmetric or asymmetric) is settled.

On OR Many-Access Channels (10:50)

Wenyi Zhang (University of Science and Technology of China, P.R. China); Lingyan Huang (University of Science and Technology of China, P.R. China)

OR multi-access channel is a simple model where the channel output is the Boolean OR among the Boolean

channel inputs. We revisit this model, showing that employing Bloom filter, a randomized data structure, as channel inputs achieves its capacity region with joint decoding and the symmetric sum rate of $\ln 2$ bits per channel use without joint decoding. We then proceed to the "many-access" regime where the number of potential users grows without bound, treating both activity recognition and message transmission problems, establishing scaling laws which are optimal within a constant factor, based on Bloom filter channel inputs.

Fr1-4: Information Retrieval

Friday, June 30, 09:50-11:10
Room: K3
Chair: Eitan Yaakobi (Technion, Israel)

Improved Codes for List Decoding in the Levenshtein's channel and Information Retrieval (09:50)

Tero Laihonen *(University of Turku, Finland); Tuomo Lehtilä (University of Turku, Finland)*

In this paper, we consider t-revealing codes in the binary Hamming space. Let C be a code and denote by $I_t(C;x)$ the set of elements of C which are within (Hamming) distance t from a word x. A code C is called t-revealing if the majority voting on the coordinates of the words in $I_t(C;\boldsymbol{x})$ gives unambiguously $\boldsymbol{x}$. These codes have applications, for instance, to the list decoding problem of the Levenshtein's channel model, which is relevant for recent advanced storage technologies, and to the information retrieval problem of the Yaakobi-Bruck model of associative memories. We give t-revealing codes which improve some of the key parameters for these applications compared to earlier code constructions, namely, the length of the output list of the decoder and the maximal number of input clues needed for information retrieval.

Binary, Shortened Projective Reed Muller Codes for Coded Private Information Retrieval (10:10)

Myna Vajha (Indian Institute of Science, India); Vinayak Ramkumar (Indian Institute of Science, India); P Vijay Kumar (Indian Institute of Science & University of Southern California, India)

The notion of a Private Information Retrieval (PIR) code was recently introduced by Fazeli, Vardy and Yaakobi who showed that this class of codes permit PIR at reduced levels of storage overhead in comparison with replicated-server PIR. In the present paper, the construction of an (n,k) τ-server binary, linear PIR code having parameters $n=\sum_{i=0}^{\ell}\binom{m}{i}$, $k=\binom{m}{\ell}$ and $\tau=2^{\ell}$ is presented. These codes are obtained through homogeneous-polynomial evaluation and correspond to the binary, Projective Reed Muller (PRM) code. The construction can be extended to yield PIR codes for any τ of the form 2^{ℓ}, $2^{\ell}-1$ and any value of k, through a combination of single-symbol puncturing and shortening of the PRM code. Each of these code constructions above, have smaller storage overhead in comparison with other PIR codes appearing in the literature. For the particular case of $\tau=3,4$, we show that the codes constructed here are optimal, systematic PIR codes by providing an improved lower bound on the block length $n(k,\tau)$ of a systematic PIR code. It follows from a result by Vardy and Yaakobi, that these codes also yield optimal, systematic primitive multiset $(n,k,\tau)_B$ batch codes for $\tau=3,4$. The PIR code constructions presented here also yield upper bounds on the generalized Hamming weights of binary PRM codes.

Sparse Ternary Codes for similarity search have higher coding gain than dense binary codes (10:30)

Sohrab Ferdowsi *(University of Geneva, Switzerland); Sviatoslav Voloshynovskiy (University of Geneva, Switzerland); Dimche Kostadinov (University of Geneva, Switzerland); Taras Holotyak (University of Geneva, Switzerland)*

This paper addresses the problem of Approximate Nearest Neighbor (ANN) search in pattern recognition where feature vectors in a database are encoded as compact codes in order to speed-up the similarity search in large-scale databases. Considering the ANN problem from an information-theoretic perspective, we interpret it as an encoding, which maps the original feature vectors to a less entropic sparse representation while requiring them to be as informative as possible. We then define the coding gain for ANN search using information-theoretic measures. We next show that the classical approach to this problem, which consists of binarization of the projected vectors is sub-optimal. Instead, a properly designed ternary encoding achieves higher coding gains and lower complexity.

PIR Array Codes with Optimal PIR Rates (10:50)

Tuvi Etzion *(Technion-Israel Institute of Technology, Israel); Simon Blackburn (Royal Holloway University of London, United Kingdom (Great Britain))*

There has been much recent interest in Private information Retrieval (PIR) in models where a database is stored across several servers using coding techniques from distributed storage, rather than being simply replicated. In particular, a recent breakthrough result of Fazelli, Vardy and Yaakobi introduces the notion of a PIR code and a PIR array code, and uses this notion to produce efficient protocols. In this paper we are interested in designing PIR array codes. We consider the case when we have m servers, with each server storing a fraction $(1/s)$ of the bits of the database; here s is a fixed rational number with $s>1$. We study the

maximum PIR rate of a PIR array code with the k-PIR property (which enables a k-server PIR protocol to be emulated on the m servers), where the PIR rate is defined to be k/m. We present upper bounds on the achievable rate, some constructions, and ideas how to obtain PIR array codes with the highest possible PIR rate. In particular, we present constructions that asymptotically meet our upper bounds, and the exact largest PIR rate is obtained when $1 < s \leq 2$.

Fr1-5: Information Dynamics

Friday, June 30, 09:50-11:10
Room: K4
Chair: Anant Sahai (UC Berkeley, USA)

The Capacity of Unstable Dynamical Systems-Interaction of Control and Information Transmission (09:50)

Ioannis Tzortzis (University of Cyprus, Cyprus); Charalambos Charalambous (University of Cyprus, Cyprus); Christos Kourtellaris (University of Cyprus, Cyprus); Sergey Loyka (University of Ottawa, Canada)

The extremum problem of maximizing directed information from inputs to outputs of dynamical systems, not necessarily stationary or ergodic, which may correspond to unstable control systems or unstable communication channels, over conditional distributions with feedback, subject to an average cost constraint of total power $\kappa \in [0, \infty)$ is investigated. It is shown that optimal conditional distributions, which for communication channels correspond to channel input distributions, and for control systems correspond to randomized control strategies, have a dual role, to simultaneously control the output process and to encode information. The dual role is due to the interaction of control and information transmission; it states that encoders in communication channels operate as encoders-controllers, while controllers in control systems operate as a controllers-encoders. Through the analysis of Gaussian linear control systems with randomized strategies, which are equivalent to Additive Gaussian Noise channels, *Stable or Unstable*, with arbitrary memory on past outputs, with an average constraint of quadratic form, it is shown that unstable dynamical systems have *Control-Coding Capacity* which is operational, precisely as in Shannon's operational definition. However, the control-coding capacity is zero, unless the power κ allocated to the system, exceeds a threshold κ_{min}, where κ_{min} is the minimum cost of ensuring asymptotic stability and ergodicity. The excess power $\kappa - \kappa_{min}$ is turned into an achievable rate of information transmission over the dynamical system.

Optimal Quantizations of B-DMCs Maximizing α-Mutual Information with Monge Property (10:10)

***Yuta Sakai** (University of Fukui, Japan); Ken-ichi Iwata (University of Fukui, Japan)*

This study examines quantizations for outputs of binary-input discrete memoryless channels (B-DMCs) by concatenating its output with another DMC, so-called a quantizer. As an objective function of channel quantizations, we employ the α-mutual information of a B-DMC, which connects to more powerful coding theorem than the ordinary mutual information. Showing a Monge property of the α-mutual information, we propose an optimal quantizer design algorithm for given B-DMC in polynomial time complexity with respect to the output alphabet size and the quantized level. Since the proposed method employs the SMAWK algorithm due to the Monge property, our algorithm is faster than a naive dynamic programming.

Information and estimation in Fokker-Planck channels (10:30)

Andre Wibisono (University of Wisconsin-Madison, USA); Varun Jog (University of Wisconsin - Madison, USA); Po-Ling Loh (University of Wisconsin-Madison, USA)

We study the relationship between information- and estimation-theoretic quantities in time-evolving systems. We focus on the Fokker-Planck channel defined by a general stochastic differential equation, and show that the time derivatives of entropy, KL divergence, and mutual information are characterized by estimation-theoretic quantities involving an appropriate generalization of the Fisher information. Our results vastly extend De Bruijn's identity and the classical I-MMSE relation.

Dynamical Systems, Ergodicity, and Posterior Matching (10:50)

Todd Coleman (UCSD, USA)

The Posterior Matching (PM) scheme is a mutual information maximizing scheme for efficiently communicating a message point in a continuum over a noisy channel, by utilizing the feedback after each channel use. It was originally developed when the message point was on a subset of the real line, and more recently we have generalized the framework to arbitrary dimensions. We consider a wide class of encoder dynamical systems and demonstrate a necessary condition for reliability, the measurability of the message point with respect to the infinite sequence of observations, to involve invertibility of a dynamical system. This justifies the use of optimal transport theory to construct diffeomorphism based encoders that allow for this. Next, we show that the ergodicity of the aforementioned dynamical system state variable is a necessary and sufficient condition for posterior matching to be reliable. Lastly, we show

a surprising "all or nothing" result: this same condition is necessary and sufficient to achieve capacity.

Fr1-6: Coding for Insertion and Deletion Channels 2

Friday, June 30, 09:50-11:10
Room: K5
Chair: Vahid Aref (Nokia Bell Labs, Germany)

Asymptotically Optimal Sticky-Insertion-Correcting Codes with Efficient Encoding and Decoding (09:50)

Hessam Mahdavifar (University of Michigan, USA); Alexander Vardy (University of California San Diego, USA)

The problem of constructing sticky-insertion-correcting codes with efficient encoding and decoding is considered. An (n, M, r) sticky-insertion-correcting code consists of M codewords of length n such that any pattern of up to r sticky insertions can be corrected. We utilize BCH codes and their analogous in the Lee space to construct explicit and systematic codes that are immune to up to r sticky insertions. It is shown that the ratio of the number of constructed redundancy bits in the construction to a certain upper bound approaches one as the block length grows large, which implies the optimality of the construction.

Permutation Codes Correcting a Single Burst Deletion II: Stable Deletions (10:10)

Yeow Meng Chee (Nanyang Technological University, Singapore); San Ling (NTU, Singapore); Tuan Thanh Nguyen (Nanyang Technological University, Singapore); Van Khu Vu (Nanyang Technological University, Singapore); Hengjia Wei (Nanyang Technological University, Singapore)

We construct permutation codes capable of correcting bursts of stable deletions. For correcting a single burst of exactly s stable deletions, our code has size $\frac{sn!}{((2s)!n)^2}$, while the upper bound is $\frac{n!}{s!(n-s+1)}$.We also construct permutation codes for the cases of single burst of up to s stable deletions, and up to b bursts of at most s stable deletions each.

Guess & Check Codes for Deletions and Synchronization (10:30)

Serge Kas Hanna *(Illinois Institute of Technology, USA); Salim El Rouayheb (Illinois Institute of Technology, USA)*

We consider the problem of constructing codes that can correct δ deletions occurring in an arbitrary binary string of length n bits. Varshamov-Tenengolts (VT) codes can correct all possible single deletions $(\delta = 1)$ with an asymptotically optimal redundancy. Finding similar codes for $\delta \geq 2$ deletions is an open problem. We propose a new family of codes, that we call Guess & Check (GC) codes, that can correct, with high probability, a constant number of deletions δ occurring at uniformly random positions within an arbitrary string. The GC codes are based on MDS codes and have an asymptotically optimal redundancy that is $\Theta(\delta \log n)$. We provide deterministic polynomial time encoding and decoding schemes for these codes. We also describe the applications of GC codes to file synchronization.

On Unique Decoding from Insertion Errors (10:50)

Kayvon Mazooji *(UCLA, USA)*

For any code, the set of received words generated by insertion errors is infinitely large. We prove that infinitely many of these words are uniquely decodable. We proceed to analyze how often unique decoding from insertions occurs for arbitrary codes. These questions are relevant because insertion errors frequently occur in synchronization and DNA, a medium which is beginning to be used for long term data storage. For a codeword c of length n, we are interested in two particular measures. The first is the probability of uniquely decoding when t insertions occur, if each distinct length $n+t$ received word is output with equal probability. The second is the probability of uniquely decoding when t sequential insertions occur, and each insertion position and element are selected uniformly at random. This paper attempts to better understand the behavior of the measures for arbitrary codewords, placing a particular emphasis on limiting behavior as t or n increases. Our most substantial contribution is the derivation of upper bounds on both measures, which are mathematically related to Levenshtein's reconstruction problem.

Fr1-7: Security 6

Friday, June 30, 09:50-11:10
Room: K6
Chair: Oliver Kosut (Arizona State University, USA)

Characterizing Optimal Security and Round-Complexity for Secure OR Evaluation (09:50)

Amisha Jhanji (Purdue University, USA); Hemanta Maji (Purdue University, USA); ***Raphael Meyer*** *(Purdue University, USA)*

Secure multi-party computation allows mutually distrusting parties to compute securely over their private data. However, even in the semi-honest two-party setting, most interesting functions cannot be computed securely in the information-theoretic plain model. Intuitively, the objective of accurately evaluating the output of such functions is inherently inimical to the privacy concerns of the parties. Securely evaluating OR of

the input bits of two parties is the simplest example, and this result captures the essence of the hardness in securely evaluating most functions. This work studies the interplay between accuracy and privacy of secure 2-party function evaluation in the information-theoretic plain model. We provide an optimal accuracy versus privacy tradeoff for computing OR(x,y), where x and y are, respectively, the private input bits of Alice and Bob. In particular, we construct a round-optimal two-party protocol for OR that has maximum semi-honest security in the information-theoretic plain model. Prior results exhibit only weak tradeoffs that are far from the optimal. We generalize our techniques to obtain a tight accuracy-versus-privacy tradeoff characterization for a stronger notion of security, namely differentially-private semi-honest security. The technical heart of our result is a new technique to derive inequalities for distributions of transcripts generated by protocols. This approach reduces the domain of the optimization problem from an unbounded number of transcripts to a constant size while preserving the optimal solution to the original problem. We believe that these techniques for analyzing protocols in the information-theoretic plain model will be of independent interest.

Learning Adversary's Actions for Secret Communication (10:10)

Mehrdad Tahmasbi (Georgia Institute of Technology, USA); ***Matthieu Bloch*** *(Georgia Institute of Technology, USA); Aylin Yener (Pennsylvania State University, USA)*

We analyze the problem of secure communication over a wiretap channel with an active adversary, in which the legitimate transmitter has the opportunity to sense and learn the adversary's actions. Specifically, the adversary has the ability to switch between two channels and to observe the corresponding output at every channel use; the encoder, however, has *causal* access to a degraded and noisy version of the attacker's observations. We develop a joint learning/transmission coding scheme that allows the legitimate users to exploit their ability to learn to adapt to the adversary's actions. For some channel models, we show that the achievable rates, which we define precisely, are arbitrarily close to those obtained *with hindsight* if the transmitter had known the actions ahead of time. This suggests that there is much to exploit and gain in physical-layer security by monitoring the environment.

On the Equivalency of Reliability and Security Metrics for Wireline Networks (10:30)

Mohammad mahdi Mojahedian (Sharif University of Technology, Iran); Amin Gohari (Sharif University of Technology, Iran); Mohammad Reza Aref (Sharif University of Tech., Iran)

In this paper, we show the equivalency of weak and strong secrecy conditions for a large class of secure network coding problems. When we restrict to linear operations, we show the equivalency of "perfect secrecy with zero-error constraint" and "weak secrecy with ϵ-error constraint".

A code-based blind signature (10:50)

Olivier Blazy (University of Limoges, France); ***Philippe Gaborit*** *(Universite de Limoges, France); Julien Schrek (Limoges University, France); Nicolas Sendrier (INRIA, France)*

In this paper we give the first blind signature protocol for code-based cryptography. Our approach is different from the classical original RSA based blind signature scheme, it is done in the spirit of the Fischlin approach [7] which is based on proofs of knowledge. To achieve our goal we consider a new tool for zero-knowledge (ZK) proofs, the Concatenated Stern ZK protocol, which permits to obtain an authentication protocol for concatenated matrices. A signature is then obtained from the usual Fiat-Shamir heuristic. We describe our blind signature protocol for cryptography based on Hamming metric and show how it can be extended to rank based cryptography. The security of our blind protocol is based on the security of a trapdoor function for the syndrome decoding problem: the CFS signature scheme for Hamming distance and on the more recent RankSign protocol for rank metric. We give proofs in the random oracle model (ROM) for our blind signature scheme, which rely on the Syndrome Decoding problem. The parameters we obtain for our protocol are practical for rank metric (200kBytes) for the signature length and 15kBytes for public key size) and a little less practical for Hamming distance.

Fr1-8: Multiple Access

Friday, June 30, 09:50-11:10
Room: K7+8
Chair: Richard Wesel (University of California, Los Angeles, USA)

Asymptotic Analysis of Tone Reservation Method for the PAPR Reduction of CDMA Systems (09:50)

Holger Boche (Technical University Munich, Germany); ***Ezra Tampubolon*** *(Technische Universität München, Germany)*

The high peak value of the transmission signal of wireless communication systems lead to wasteful energy consumption and degradation of several transmission performances. We continue the theoretical contributions made in [1], [2] towards the understanding of tone reservation method for orthogonal transmission schemes. There it was shown that the combinatorial object called arithmetic progression plays an important role in setting limitations for the applicability of the tone reservation method for OFDM system. In this work,

we introduce the combinatorial object called perfect Walsh sum (PWS), playing a similar role for CDMA systems as arithmetic progression for OFDM systems. We show that for a given $m, n \in \mathbb{N}$ and $\delta \in (0,1)$, every subset $\mathcal{I}$ of the set $[N]$ of the first $N = 2^n$ numbers, which fulfills $|\mathcal{I}|/N \geq \delta$ and $|\mathcal{I}| \geq 2(2/\delta)^{2^m-1}$, contains a PWS of size 2^m. Consequences of the latter are results analogous to the famous Szemerédi Theorem on arithmetic progressions, Conlon-Gower's Theorem on probabilistic construction of "sparse" sets containing an arithmetic progression, and even a solution of Erdős' conjecture on arithmetic progressions. Those results give in particular an insight into the asymptotic behaviour of tone reservation method for CDMA systems.

Spatial random multiple access with multiple departure (10:10)

Serguei Foss (Heriot-Watt University, United Kingdom (Great Britain)); Andrey Turlikov (Saint-Petersburg State University of Aerospace Instrumentation, Russia); Maxim Grankin (Saint Petersburg State University of Aerospace Instrumentation & Quantenna Communications, Russia)

We introduce a new model of spatial random multiple access systems with a non-standard departure policy: all arriving messages are distributed uniformly on a finite sphere in the space, and when a successful transmission of a single message occurs, the transmitted message leaves the system together with all its neighbours within a ball of a given radius centred at the message's location. We consider three classes of protocols: centralised protocols and decentralised protocols with either ternary or binary feedback; and analyse their stability. Further, we discuss some asymptotic properties of stable protocols

Coded Random Access Design for Constrained Outage (10:30)

MohammadReza Ebrahimi (University of Tehran, Iran); Farshad Lahouti (Caltech Institute of Techlonogy, USA); Victoria Kostina (California Institute of Technology, USA)

The emergence of networks of many devices in the context of cyber-physical systems motivates novel solutions for communication over random access channels. Currently deployed random access protocols attempt to avoid collisions, and target the performance of a scheduled multiple access system (a strategy known to be only suboptimal from the information-theoretic perspective). In contrast, in this paper, we allow collisions among the transmissions of different users. We consider code design for random access channels with erasures in which the number of users in each frame is unknown at the transmitters but known at the receiver, and we present a two-layer coding architecture for joint contention resolution and erasure correction.For random LDPC codes based on this scheme, the density evolution is asymptotically analyzed, which enables optimized code design for maximized throughput with constrained outage. The results demonstrate that the proposed low-complexity scheme approaches the outage capacity of the random access channel with erasures when the average number of active users is small.

Fr1-9: Channel Identification

Friday, June 30, 09:50-11:10
Room: K9
Chair: Kenta Kasai (Tokyo Institute of Technology, Japan)

On Optimal Error Exponents in Noiseless Channel Identification (09:50)

Marat Burnashev (Institute for Information Transmission Problems, Russian Academy of Sciences, Russia); Hirosuke Yamamoto (The University of Tokyo, Japan)

Recently Yamamoto and Ueda proposed multiple object identification (MOID) codes to identify multiple objects via a channel at once, which is an extension of identification (ID) codes. They gave the explicit construction of MOID codes and derived the achievable triplet of coding rate R, the error exponents E_1 and E_2 of type I and type II decoding error probabilities. However, they did not treat the converse problem of the coding theorem. In this paper, we consider the coding rate of multiple objects R_K in addition to R, E_1, and E_2, and derive a condition that (R, R_K, E_1, E_2) must satisfy for any MOID codes of noiseless channels.

Channel Resolvability Theorems for General Sources and Channels (10:10)

Hideki Yagi (University of Electro-Communications, Japan)

In the problem of channel resolvability, where a given output probability distribution via a channel is approximated by transforming the uniform random numbers, characterizing the asymptotically minimum rate of the size of the random numbers, called the channel resolvability, has been open. In this paper, we derive a general formula for the channel resolvability for a given general source and channel pair. We also investigate the channel resolvability in an optimistic sense. It is demonstrated that the derived general formulas recapture a single-letter formula for the stationary memoryless source and channel. The established formulas reduce to an alternative form of sup-spectral entropy rates which often appear in the information spectrum methods when the channel is the identity mapping.

Hierarchical Identification with Pre-processing (10:30)

Minh Thanh Vu (KTH Royal Institute of Technology, Sweden); Tobias Oechtering (KTH Royal Institute of Technology, Sweden); Mikael Skoglund (KTH Royal Institute of Technology, Sweden)

We study a two-stage identification problem with pre-processing to enable efficient data retrieval and reconstruction. The first stage outputs a list of compatible users to the second stage which uses it to return the exact user identity with a corresponding reconstruction sequence. The rate- distortion region is characterized. A connection to a two observer identification problem is also studied.

Mismatched Identification via Channels (10:50)

Anelia Somekh-Baruch (Bar-Ilan University, Israel)

The problem of identification via channels concerns a decoder that needs to provide a reliable answer to the question of whether or not a specific message (unknown in advance) was transmitted. The achievability result of Ahlswede and Dueck who introduced this problem, relied on a *universal* identification decoder. This decoder assigns a channel output vector y^n to a decision region $\mathcal{D}_m$ if the empirical mutual information between y^n and an input vector that could have been transmitted given message m exceeds a certain threshold. We study a generalized class of identification decoders that determine the decision regions by comparing a type-dependent "metric" to a threshold. We introduce the notion of identification capacity with respect to a given decoding metric as the supremum of achievable normalized iterated logarithm of the number of messages that can be identified reliably using these metrics. We characterize achievable identification rates and error exponents using a type-dependent metric. In the case of an additive metric we show that the random coding achievable rate for classical mismatched decoding is an achievable identification rate.

Fr2-1: Rank Metric Codes

Friday, June 30, 11:30-12:50
Room: Europa
Chair: Sven Puchinger (Ulm University, Germany)

On Decoding Rank-Metric Codes over Large Fields (11:30)

Ron Roth (Technion, Israel)

A decoding algorithm is presented for rank-metric array codes that are based on diagonal interleaving of MDS codes. W.r.t. this metric, such array codes are known to be optimal when the underlying field is algebraically closed. It is also shown that for any list decoding radius that is smaller than the minimum rank distance, the list size can be bounded from above by an expression that is independent of the field.

Universal secure rank-metric coding schemes with optimal communication overheads (11:50)

Umberto Martínez-Peñas (Aalborg University, Denmark)

We study the problem of reducing the communication overhead from a wire-tap channel or storage system where data is encoded as a matrix, when more columns (or their linear combinations) are available. We present its applications to universal secure linear network coding and secure distributed storage with crisscross erasures. Our main contribution is a method to transform coding schemes based on linear rank-metric codes, with certain properties, to schemes with lower communication overheads. By applying this method to pairs of Gabidulin codes, we obtain coding schemes with optimal information rate with respect to their security and rank error correction capability, and with universally optimal communication overheads, when $n \leq m$, being n and m the number of columns and number of rows, respectively. Moreover, our method can be applied to other families of maximum rank distance codes when $n > m$. The downside of the method is generally expanding the packet length, but some practical instances come at no cost.

MRD Rank Metric Convolutional Codes (12:10)

Diego Napp (University of Aveiro, Portugal); Raquel Pinto (University of Aveiro, Portugal); Joachim Rosenthal (University of Zurich, Switzerland); Paolo Vettori (University of Aveiro, Portugal)

So far, in the area of Random Linear Network Coding, attention has been given to the so-called one-shot network coding, meaning that the network is used just once to propagate the information. In contrast, one can use the network more than once to spread redundancy over different shots. In this paper, we propose rank metric convolutional codes for this purpose. The framework we present is slightly more general than the one which can be found in the literature. We introduce a rank distance, which is suitable for convolutional codes, and derive a new Singleton-like upper bound. Codes achieving this bound are called Maximum Rank Distance (MRD) convolutional codes. Finally, we prove that this bound is optimal by showing a concrete construction of a family of MRD convolutional codes.

A decoding algorithm for Twisted Gabidulin codes (12:30)

Tovohery Randrianarisoa (University of Zurich, Switzerland); Joachim Rosenthal (University of Zurich, Switzerland)

In this work, we modify the decoding algorithm for sub-

space codes by Kötter and Kschischang to get a decoding algorithm for (generalized) twisted Gabidulin codes. The decoding algorithm we present applies to cases where the code is linear over the base field $\mathbb{F}_q$ but not linear over $\mathbb{F}_{q^n}$.

Fr2-2: Iterative Decoding 2

Friday, June 30, 11:30-12:50
Room: Brussels
Chair: Yuval Cassuto (Technion, Israel)

An Iterative Soft-decision Decoding Algorithm for Reed-Solomon Codes (11:30)

Huang Chang Lee (Chang Gung University, Taiwan); Jyun-Han Wu (National Tsing Hua University, Taiwan); Yeong-Luh Ueng (National Tsing Hua University, Taiwan); Chung-Hsuan Wang (National Chiao Tung University, Taiwan)

This paper proposes an iterative soft-decision decoding algorithm for Reed-Solomon (RS) codes. The proposed decoding algorithm combines the concepts of adapting the parity-check matrix and informed dynamic scheduling decoding. The parity-check matrix is rearranged before each iteration, where the systematic part is mapped to the least reliable bits, consequently reducing their influence on the other bits. Using dynamic scheduling, the more important decoding messages are updated to these least reliable bits, meaning that the majority of the error bits with low reliability can be corrected. When the proposed integrated decoding is applied to (255, 239) RS code, the difference between its frame error rate performance (FER) and the maximum-likelihood (ML) bound can be reduced to 0.8 dB, and a gain of about 0.1 dB is achieved compared to all the previously recorded soft-decision decoding for RS codes.

Decoding from Pooled Data: Phase Transitions of Message Passing (11:50)

Ahmed El Alaoui (UC Berkeley, USA); Aaditya Ramdas (University of California, Berkeley, USA); Florent Krzakala (Ecole Normale Superieure, France); Lenka Zdeborova (Institut de Physique Theorique IPhT, CEA Saclay and CNRS, France); Michael Jordan (UC Berkeley, USA)

We consider the problem of decoding a discrete signal of categorical variables from the observation of several histograms of pooled subsets of it. We present an Approximate Message Passing (AMP) algorithm for recovering the signal in the *random dense* setting where each observed histogram involves a random subset of size proportional to n of entries. We characterize the performance of the algorithm in the asymptotic regime where the number of observations m tends to infinity proportionally to n, by deriving the corresponding State Evolution (SE) equations and studying their dynamics. We initiate the analysis of the multi-dimensional SE dynamics by proving their convergence to a fixed point, along with some further properties of the iterates. The analysis reveals sharp phase transition phenomena where the behavior of AMP changes from exact recovery to weak correlation with the signal as m/n crosses a threshold. We derive formulae for the threshold in some special cases and show that they accurately match experimental behavior.

Topological Interference Management with Decoded Message Passing: A Polyhedral Approach (12:10)

Xinping Yi (Technische Universität Berlin, Germany); Giuseppe Caire (Technische Universität Berlin, Germany)

We consider the topological interference management problem with decoded message passing (TIM-MP) using a polyhedral approach. The TIM-MP problem studies partially-connected interference networks with no channel state information except for the network topology (i.e., connectivity graph) at the transmitters, while the decoded messages at the receivers can be routed to other receivers via backhaul links to help cancel interference. With the aid of polyhedral combinatorics, we identify the structural properties of certain classes of network topologies where orthogonal access achieves the optimal degrees-of-freedom (DoF) region in the information-theoretic sense. We are also able to prove the linear optimality of orthogonal access in terms of symmetric DoF for the networks up to four users with all possible network topologies (218 instances).

Fr2-3: Coded Caching 2

Friday, June 30, 11:30-12:50
Room: K2
Chair: Petros Elia (EURECOM, France)

Decentralized Caching and Coded Delivery over Gaussian Broadcast Channels (11:30)

Mohammad Mohammadi Amiri (Imperial College London, United Kingdom (Great Britain)); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain))

A cache-aided K-user Gaussian broadcast channel (BC) is considered. The transmitter has a library of N equal-rate files, from which each user demands one. The impact of the equal-capacity receiver cache memories on the minimum required transmit power to satisfy all user demands is studied. Decentralized caching with uniformly random demands is considered, and both the minimum average power (averaged over all demand combinations) and the minimum peak power (minimum power required to satisfy the worst-case

demand combination) are studied. Upper and lower bounds are presented on the minimum required average and peak transmit power as a function of the cache capacity, assuming uncoded cache placement. The gaps between the upper and lower bounds on both the minimum peak and average power values are shown to be relatively small through numerical results, particularly for large cache capacities.

Low Subpacketization Schemes for Coded Caching (11:50)

Li Tang (Iowa State University, USA); Aditya Ramamoorthy (Iowa State University, USA)

Coded caching is a technique that generalizes conventional caching and promises significant reductions in traffic over caching networks. However, the basic coded caching scheme requires that each file hosted in the server be partitioned into a large number (called the subpacketization level) of non-overlapping subfiles. From a practical perspective, this is problematic as it means that prior schemes are only applicable when the size of the files is extremely large. In this work, we propose coded caching schemes based on combinatorial structures called resolvable designs. These structures can be obtained in a natural manner from linear block codes whose generator matrices possess certain rank properties. We demonstrate that several schemes with subpacketization levels that are exponentially smaller than the basic scheme can be obtained.

On Coded Caching in the Overloaded MISO Broadcast Channel (12:10)

Enrico Piovano *(Imperial College London, United Kingdom (Great Britain)); Hamdi Joudeh (Imperial College London, United Kingdom (Great Britain)); Bruno Clerckx (Imperial College London, United Kingdom (Great Britain))*

This work investigates the interplay of coded caching and spatial multiplexing in an overloaded Multiple-Input-Single-Output (MISO) Broadcast Channel (BC), i.e. a system where the number of users is greater than the number of transmitting antennas. On one hand, coded-caching uses the aggregate global cache memory of the users to create multicasting opportunities. On the other hand, the multiple antennas at the transmitter leverages the available CSIT to transmit multiple streams simultaneously. In this paper, we introduce a novel scheme which combines both the gain derived from coded caching and spatial multiplexing and outperforms existing schemes in terms of delivery time and CSIT requirement.

Coded Caching with Linear Subpacketization is Possible using Ruzsa-Szeméredi Graphs (12:30)

Karthikeyan Shanmugam (IBM Research, T. J Watson Center, USA); Antonia Tulino (Bell Laboratories & Università degli studi di Napoli, USA); Alexandros Dimakis (University of Texas at Austin, USA)

Coded caching is a problem where encoded broadcasts are used to satisfy users requesting popular files and having caching capabilities. Recent work by Maddah-Ali and Niesen showed that it is possible to satisfy a scaling number of users with only a constant number of broadcast transmissions by exploiting coding and caching. Unfortunately, all previous schemes required the splitting of files into an exponential number of packets before the significant coding gains of caching appeared. The question of what can be achieved with polynomial subpacketization (in the number of users) has been a central open problem in this area. We resolve this problem and present the first coded caching scheme with polynomial (in fact, linear) subpacketization. We obtain a number of transmissions that is not constant, but can be any polynomial in the number of users with an exponent arbitrarily close to zero. Our central technical tool is a novel connection between Ruzsa-Szeméredi graphs and coded caching.

Fr2-4: Channel Capacity 4

Friday, June 30, 11:30-12:50
Room: K3
Chair: Hideki Yagi (University of Electro-Communications, Japan)

The Arbitrarily Varying Channel Under Constraints with Causal Side Information at the Encoder (11:30)

Uzi Pereg (Technion, Israel); Yossef Steinberg (Technion, Israel)

We study the arbitrarily varying channel (AVC) with input and state constraints, when the encoder has state information in a causal manner. Lower and upper bounds on the random code capacity are developed. A lower bound on the deterministic code capacity is established in the case of a message-averaged input constraint. In the setting where a state constraint is imposed on the jammer, while the user is under no constraints, the random code bounds coincide, and the random code capacity is determined. Furthermore, for this scenario, a generalized non-symmetrizability condition is stated, under which the deterministic code capacity coincides with the random code capacity.

Storage Capacity as an Information-Theoretic Analogue of Vertex Cover (11:50)

Arya Mazumdar (University of Massachusetts Amherst, USA); Andrew McGregor (University of Massachusetts, Amherst, USA); Sofya Vorotnikova (University of Massachusetts, USA)

Motivated by applications in distributed storage, the storage capacity of a graph was recently defined to be the maximum amount of information that can be stored across the vertices of a graph such that the information at any vertex can be recovered from the information stored at the neighboring vertices. Computing the storage capacity is a fundamental problem in network coding and is related, or equivalent, to some well-studied problems such as index coding with side information and generalized guessing games. In this paper, we consider storage capacity as a natural information-theoretic analogue of the minimum vertex cover of a graph. Indeed, while it was known that storage capacity is upper bounded by minimum vertex cover, we show that by treating it as such we can get a $3/2$ approximation for planar graphs, and a $4/3$ approximation for triangle-free planar graphs. Since the storage capacity is intimately related to the index coding rate, we get a 1.923 approximation of index coding for planar graphs and $3/2$ approximation for triangle-free planar graphs. Previously only a trivial 4 approximation of the index coding rate was known for planar graphs. We then develop a general method of "gadget covering" to upper bound the storage capacity in terms of the average of a set of vertex covers. This method is intuitive and leads to the exact characterization of storage capacity for various families of graphs, such as cycles with chords. Finally, we generalize the storage capacity notion to include recovery from partial failures in distributed storage. We show tight upper and lower bounds on this partial recovery capacity that scales nicely with the fraction of failure in a vertex.

Gaussian ISI Channels with Mismatch (12:10)

Wasim Huleihel (MIT, USA); Salman Salamatian (Massachusetts Institute of Technology, USA); Neri Merhav (Technion, Israel); Muriel Médard (MIT, USA)

This paper considers the problem of channel coding over Gaussian intersymbol interference (ISI) channels with a given (possibly suboptimal) metric decoding rule. Specifically, it is assumed that the mismatched decoder has incorrect knowledge of the ISI coefficients (or, the impulse response function). The mismatch capacity is the highest achievable rate for a given decoding rule. Unfortunately, existing lower bounds to the mismatch capacity for multi-letter channels and decoding metrics (or, channels and decoding metrics with memory), as in our model, are presented only in the form of multi-letter expressions, and thus cannot be calculated in practice. Consequently, they provide little insight on the mismatch problem. In this paper, we derive a computable single-letter lower bound to the mismatch capacity, and discuss some implications of our results.

Characterization of Super-Additivity and Discontinuity Behavior of the Capacity of Arbitrarily Varying Channels under List Decoding (12:30)

*Holger Boche (Technical University Munich, Germany); **Rafael Schaefer** (Technische Universität Berlin, Germany); H. Vincent Poor (Princeton University, USA)*

The arbitrarily varying channel (AVC) models communication over a channel that varies in an arbitrary and unknown manner from channel use to channel use. This paper considers the AVC under list decoding and studies the corresponding list capacity. In particular, the list capacity function is shown to be discontinuous and the corresponding discontinuity points are characterized for all possible list sizes. For orthogonal AVCs it is then shown that the list capacity is super-additive, implying that joint encoding and decoding for two orthogonal AVCs can yield a larger list capacity than independent processing of both channels. This discrepancy is shown to be arbitrary large.

Fr2-5: Communications 4

Friday, June 30, 11:30-12:50
Room: K4
Chair: Remi Chou (Pennsylvania State University, USA)

Optimal Covert Communications using Pulse-Position Modulation (11:30)

Matthieu Bloch (Georgia Institute of Technology, USA); Saikat Guha (Raytheon BBN Technologies, USA)

This paper shows the optimality of Pulse-Position Modulation (PPM) for covert communications over discrete-memoryless channels. Specifically, the concatenation of an m-ary outer code of length O(m) and an inner code consisting of PPM of order m achieves the information-theoretic limits of covert communications. This suggests alternative code constructions for covert communications, in which the sparsity of the PPM symbols ensures covertness and an appropriate choice of the blocklength results in the square root law.

Covert Communication with Noncausal Channel-State Information at the Transmitter (11:50)

Si-Hyeon Lee (POSTECH, Korea); Ligong Wang (ETIS & CNRS, France); Ashish Khisti (University of Toronto, Canada); Gregory Wornell (MIT, USA)

We consider the problem of covert communication over a state-dependent channel, where the transmit-

ter has noncausal knowledge of the channel states. Here, “covert” means that the probability that a warden on the channel can detect the communication must be small. In contrast with traditional models without noncausal channel-state information at the transmitter, we show that covert communication can be possible with positive rate. We derive closed-form formulas for the maximum achievable covert communication rate (“covert capacity”) in this setting for discrete memoryless channels as well as additive white Gaussian noise channels. We also derive lower bounds on the rate of the secret key that is needed for the transmitter and the receiver to achieve the covert capacity.

Strong Coordination of Signals and Actions over Noisy Channels (12:10)

Giulia Cervia (ETIS/ ENSEA, University Cergy-Pontoise, CNRS, France); Laura Luzzi (ENSEA & CNRS, Université de Cergy-Pontoise, France); Mael Le Treust (ETIS / ENSEA, Université Cergy-Pontoise, CNRS, France); Matthieu Bloch (Georgia Institute of Technology, USA)

We develop a random binning scheme for strong coordination in a network of two nodes separated by a noisy channel, in which the input and output signals have to be coordinated with the source and its reconstruction. In the case of non-causal encoding and decoding, we propose a joint source-channel coding scheme and develop inner and outer bounds for the strong coordination region. While the set of achievable target distributions is the same as for empirical coordination, we show that a positive rate of common randomness is required for strong coordination.

Strong Coordination over Noisy Channels: Is Separation Sufficient? (12:30)

Sarah Obead (New Jersey Institute of Technology, USA); Badri Vellambi (New Jersey Institute of Technology, USA); Joerg Kliewer (New Jersey Institute of Technology, USA)

We study the problem of strong coordination in which agents X and Y communicate over a noisy communication channel to ensure that their actions follow a behavior specified by a joint probability distribution. We propose two novel coding schemes for this noisy coordination scenario and derive inner bounds for the respective strong capacity region. The first scheme is a joint coordination-channel coding scheme that utilizes the randomness provided by the communication channel to reduce the local randomness required in generating the action sequence at Node Y. The second scheme exploits separate coordination and channel coding where local randomness is extracted from the channel after decoding. Finally we present a example in which the joint scheme is able to outperform the separate case in terms of coordination rate.

Fr2-6: Coding and Decoding

Friday, June 30, 11:30-12:50
Room: K5
Chair: Hessam Mahdavifar (University of Michigan, USA)

Universal Decoding Using a Noisy Codebook (11:30)

Neri Merhav (Technion, Israel)

We consider the topic of universal decoding with a decoder that does not have direct access to the codebook, but only to noisy versions of the various randomly generated codewords, a problem motivated by biometrical identification systems. Both the source that generates the original (clean) codewords, and the channel that corrupts them in generating the noisy codewords, as well as the main channel for communicating the messages, are all modeled by non-unifilar, finite-state systems (hidden Markov models). As in previous works on universal decoding, here too, the average error probability of our proposed universal decoder is shown to be as small as that of the optimal maximum likelihood (ML) decoder, up to a multiplicative factor that is a sub-exponential function of the block length. It therefore has the same error exponent, whenever the ML decoder has a positive error exponent. The universal decoding metric is based on Lempel-Ziv (LZ) incremental parsing of each noisy codeword jointly with the given channel output vector, but this metric is somewhat different from the one proposed in earlier works on universal decoding for finite-state channels, by Ziv (1985) and by Lapidoth and Ziv (1998). The reason for the difference is that here, unlike in those earlier works, the probability distribution that governs the (noisy) codewords is, in general, not uniform across its support. This non-uniformity of the codeword distribution also makes our derivation more challenging. Another reason for the more challenging analysis is the fact that the effective induced channel between the noisy codeword of the transmitted message and the main channel output is not a finite-state channel in general.

Variable-to-Fixed Length Homophonic Coding Suitable for Asymmetric Channel Coding (11:50)

Junya Honda (The University of Tokyo, Japan); Hirosuke Yamamoto (The University of Tokyo, Japan)

In the communication through asymmetric channels the capacity-achieving input distribution is not uniform in general. Homophonic coding is a framework to invertibly convert a (usually uniform) message into a sequence with some target distribution, and is a promising candidate to generate codewords with the target nonuniform distribution for asymmetric channels. In particular, a Variable-to-Fixed length (VF) homophonic

code is suitable as a component of channel codes to avoid decoding error propagation. However, the existing VF homophonic code requires to know the maximum relative gap of probabilities between two adjacent sequences beforehand, which is unrealistic for long block codes. In this paper we propose a new VF homophonic code without such requirement by allowing one-symbol decoding delay. We evaluate this code theoretically and experimentally to verify its asymptotic optimality.

Optimality of the recursive data exchange protocol (12:10)

Himanshu Tyagi (Indian Institute of Science, India); Shun Watanabe (Tokyo University of Agriculture and Technology, Japan)

Multiple parties observe correlated data generated independent and identically (in time) from a known joint distribution. Parties communicate with each other interactively to enable each party to recover the data observed by all the other parties and attain omniscience. We characterize the asymptotic growth of the number of bits of interactive communication required by the parties to attain omniscience up to the second-order term. For the converse, we provide a single-shot lower bound for the required number of bits of communication, which yields the asymptotic result as a special case. It is shown that the knowledge of the distribution can be used to modify the recently proposed recursive universal data exchange protocol to render it optimal up to the second-order term. As a corollary, we provide a precise characterization of the reduction in communication for omniscience due to interaction.

Explicit Constructions of Finite-Length WOM Codes (12:30)

Yeow Meng Chee (Nanyang Technological University, Singapore); Han Mao Kiah (Nanyang Technological University, Singapore); Alexander Vardy (University of California San Diego, USA); Eitan Yaakobi (Technion, Israel)

Write-once memory (WOM) is a storage device consisting of binary cells which can only increase their levels. A t-write WOM code is a coding scheme which allows to write t times to the WOM without decreasing the levels of the cells. The sum-rate of a WOM code is the ratio between the total number of bits written to the memory and the number of cells. It is known that the maximum sum-rate of a t-write WOM code is $\log(t+1)$. This is also an achievable upper bound both by information theory arguments and explicit WOM code constructions. While existing constructions of WOM codes were targeted to increase the sum-rate, we consider here two more figures of merit in evaluating the constructions. The first one is the complexity of the encoding and decoding maps of the code. The second one is called the convergence rate, and is defined to be the minimum code length $n(\epsilon)$ in order to reach ϵ close to a point in the capacity region. One of our main results in the paper is a specific capacity achieving construction for two-write WOM codes which has polynomial complexity and relatively short block length to be ϵ close to the capacity. Using these two-write WOM codes, we obtain three-write WOM codes that approach sum-rate 1.809 with relatively short block lengths. Finally, we provide another construction of three-write WOM that achieves sum-rate 1.71 by using only 100 cells.

Fr2-7: Privacy and Security

Friday, June 30, 11:30-12:50
Room: K6
Chair: Philippe Gaborit (Universite de Limoges, France)

On Information-Theoretic Privacy with General Distortion Cost Functions (11:30)

Kousha Kalantari (Arizona State University, USA); Lalitha Sankar (Arizona State University, USA); Oliver Kosut (Arizona State University, USA)

The privacy-utility tradeoff problem is formulated as determining the privacy mechanism (random mapping) that minimizes the mutual information (a metric for privacy leakage) between the private features of the original dataset and a released version. The minimization is subject to a constraint on the average distortion cost defined as a function f evaluated for every distortion d between the public features and the released version of dataset. The asymptotic optimal leakage is derived both for general and stationary memoryless privacy mechanisms. It is shown that for convex cost functions there is no asymptotic loss in using stationary memoryless mechanisms. Of independent interest are the proof techniques developed here for arbitrary cost functions.

Impact of the Communication Channel on Information Theoretical Privacy (11:50)

***Mehmet Demir** (Boğaziçi University, Turkey); Gunes Karabulut Kurt (Istanbul Technical University, Turkey); Guido Dartmann (University of Applied Sciences Trier, Germany); Volker Lücken (RWTH Aachen University & Chair for Integrated Signal Processing Systems, Germany); Gerd Ascheid (RWTH Aachen University, Germany)*

As private information of individuals become more accessible, data privacy evolved to be an important aspect of communication technologies. Among existing privacy definitions, the utility privacy trade-off model is suitable for the assessment of privacy due to its relation with information theory and rate distortion theory. In this paper, the effects of the wireless channel errors

are studied with respect to the utility privacy trade-off in a wireless communication network. First, the transmission error probability is embedded to the existing trade-off definitions. Then, it is shown via numerical examples, in which binary and normally distributed sources satisfy the updated rate distortion equivocation and equivocation distortion functions.

Constructive Interference Based Secure Precoding (12:10)

Muhammad Khandaker (University College London, United Kingdom (Great Britain)); Christos Masouros (University College London, United Kingdom (Great Britain)); Kai Kit Wong (University College London, United Kingdom (Great Britain))

Recent advances in interference exploitation showed that exploiting knowledge of interference constructively can improve the receive signal-to-interference and noise ratio (SINR) at the destination. This paper exploits this concept to design artificial noise (AN) beamformers constructive to the intended receiver (IR) yet keeping AN disruptive to possible eavesdroppers (Eves). A multiple-input single-output (MISO) wiretap channel with multiple eavesdroppers scenario has been investigated taking both perfect and imperfect channel information into consideration. The main objective is to improve the receive SINR at the IR through exploitation of AN power in an attempt to minimize the total transmit power, while confusing the Eves.

Secure and reliable connectivity in heterogeneous wireless sensor networks (12:30)

Rashad Eletreby (Carnegie Mellon University, USA); ***Osman Yağan*** *(Carnegie Mellon University & CyLab, USA)*

We consider a wireless sensor network secured by the heterogeneous random key predistribution scheme and investigate its reliability against both link and node failures. The heterogeneous random key predistribution scheme is a lightweight security mechanism proposed to secure sensor networks that include nodes with varying levels of resources, features, or connectivity requirements; e.g., regular nodes vs. cluster heads. To capture the reliability of the network against both link and node failure, we consider the case when each link fails independently with probability $1-\alpha$ and present conditions (in the form of zero-one laws) on how to scale the parameters of the resulting network so that it is k-connected with high probability, i.e., the network remains connected even if any $k1$ nodes fail or leave the network. Collectively, we obtain a network that is reliable against the probabilistic failure of each link and against the failure of any $k1$ nodes. We present numerical results to support these conditions in the finite-node regime.

Fr2-8: Computation

Friday, June 30, 11:30-12:50
Room: K7+8
Chair: Anelia Somekh-Baruch (Bar-Ilan University, Israel)

Communication-Aware Computing for Edge Processing (11:30)

Songze Li (University of Southern California, USA); Mohammad Ali Maddah-Ali (Bell Labs, Alcatel Lucent, USA); Salman Avestimehr (University of Southern California, USA)

We consider a mobile edge computing problem, in which mobile users offload their computation tasks to computing nodes (e.g., base stations) at the network edge. The edge nodes compute the requested functions and communicate the computed results to the users via wireless links. For this problem, we propose a Universal Coded Edge Computing (UCEC) scheme for linear functions to simultaneously minimize the load of computation at the edge nodes, and maximize the physical-layer communication efficiency towards the mobile users. In the proposed UCEC scheme, edge nodes create coded inputs of the users, from which they compute coded output results. Then, the edge nodes utilize the computed coded results to create communication messages that zero-force all the interference signals over the air at each user. Specifically, the proposed scheme is universal since the coded computations performed at the edge nodes are oblivious of the channel states during the communication process from the edge nodes to the users.

Encoded Distributed Optimization (11:50)

Can Karakus (University of California, Los Angeles, USA); Yifan Sun (Technicolor Corporation, USA); Suhas Diggavi (University of California Los Angeles, USA)

Today, many real-world machine learning and data analytics problems are of a scale that requires distributed optimization; unlike in centralized computing, these systems are vulnerable to network and node failures. Recently, coding-theoretic ideas have been applied to mitigate node failures in such distributed computing networks. Relaxing the exact recovery requirement of such techniques, we propose a novel approach for adding redundancy in large-scale convex optimization problems, making solvers more robust against sudden and persistent node failures and loss of data. This is done by linearly encoding the data variables; all other aspects the computation operate as usual. We show that under moderate amounts of redundancy, it is possible to recover a close approximation to the solution under node failures. In particular, we show that encoding with (equiangular) tight frames result

in bounded objective error, and obtain an explicit error bound for a specific construction that uses Paley graphs. We also demonstrate the performance of the proposed technique for three specific machine learning problems, (two using real world datasets) namely ridge regression, binary support vector machine, and low-rank approximation.

Fundamental Estimation Limits in Autoregressive Processes with Compressive Measurements (12:10)

Milind Rao (Stanford University, USA); Tara Javidi (UCSD, USA); Yonina Eldar (Technion-Israel Institute of Technology, Israel); Andrea Goldsmith (Stanford University, USA)

We consider the problem of estimating the parameters of a vector autoregressive (VAR) process from low-dimensional random projections of the observations. This setting covers the cases where we make compressive measurements of the observations or have limits in the data acquisition process associated with the measurement system and are only able to subsample. We first present fundamental bounds for the convergence of any estimator for the covariance or state-transition matrices with and without considering structural constraints of sparsity and low-rankness. We then construct an estimator for these matrices or the parameters of the VAR process and show that it is optimal in an order sense.

Minimizing Latency for Secure Distributed Computing (12:30)

Rawad Bitar (Illinois Institute of Technology, USA); Parimal Parag (Indian Institute of Science, India); Salim El Rouayheb (Illinois Institute of Technology, USA)

We consider the setting of a master server who possesses confidential data (genomic, medical data, etc.) and wants to run intensive computations on it, as part of a machine learning algorithm for example. The master wants to distribute these computations to untrusted workers who have volunteered or are incentivized to help with this task. However, the data must be kept private (in an information theoretic sense) and not revealed to the individual workers. The workers may be busy, or even unresponsive, and will take a random time to finish the task assigned to them. We are interested in reducing the aggregate delay experienced by the master. We focus on linear computations as an essential operation in many iterative algorithms. A known solution is to use a linear secret sharing scheme to divide the data into secret shares on which the workers can compute. We propose to use instead new secure codes, called Staircase codes, introduced previously by two of the authors. We study the delay induced by Staircase codes which is always less than that of secret sharing. The reason is that secret sharing schemes need to wait for the responses of a fixed fraction of the workers, whereas Staircase codes offer more flexibility in this respect. For instance, for codes with rate $R = 1/2$ Staircase code can lead to up to 40% reduction in delay compared to secret sharing.

Fr3-1: Codes and Graphs

Friday, June 30, 14:40-16:20
Room: Europa
Chair: Norbert Goertz (Vienna University of Technology (TU Wien), Austria)

On sparse graph coding for coherent and noncoherent demodulation (14:40)

Charles-Ugo Piat-Durozoi (INPT/IRIT, France); Charly Poulliat (INP - ENSEEIHT Toulouse, France); Nathalie Thomas (University of Toulouse, France); Marie-Laure Boucheret (University of Toulouse IRIT Enseeiht, France); Guy Lesthievent (CNES, France)

In this paper, we consider a bit-interleaved coded modulation scheme (BICM) composed of an error correcting code serially concatenated with a M-ary non linear modulation. We first compare demodulation strategies for both the coherent and the non coherent cases. Then, we perform an asymptotic analysis and try to show that the design of coding schemes performing well for both the coherent and the non coherent regimes should be done carefully when considering sparse graph based codes such as low-density parity-check (LDPC) codes. It will be shown that optimized coding schemes for the non coherent setting can perform fairly well when using coherent demodulation, while on the contrary, optimized coding schemes for the coherent setting may lead to ”non stable” coding schemes in the non coherent setting.

The Number of Independent Sets In Hexagonal Graphs (15:00)

Zhun Deng (Harvard University & Work, USA); Jie Ding (Harvard University, USA); Kathryn Heal (Harvard University, USA); Vahid Tarokh (Harvard University, USA)

We derive the tightest known bounds on η, the growth rate of the logarithm of the number of independent sets on a hexagonal lattice. To obtain these bounds, we generalize a method proposed by Calkin and Wilf. Their original strategy cannot immediately be used to derive bounds for η, due to the difference in symmetry between square and hexagonal lattices, so we propose a modified method and an algorithm to derive rigorous bounds on η. In particular, we prove that 1.546440708536001 ≤ η ≤ 1.5513, which improves upon the best known bounds of 1.5463 ≤ η ≤ 1.5527 given by Nagy and Zeger. Our lower bound matches the numerical estimate of Baxter up to 9 digits after

the decimal point, and our upper bound can be further improved by following our method.

Density Evolution on a Class of Smeared Random Graphs (15:20)

Kabir Chandrasekher (University of California, Berkeley, USA); Orhan Ocal (University of California, Berkeley, USA); Kannan Ramchandran (University of California at Berkeley, USA)

We introduce a new ensemble of random bipartite graphs, which we term the 'smearing ensemble', where each left node is connected to some number of consecutive right nodes. Such graphs arise naturally in recovering sparse wavelet coefficients when signal acquisition is in the Fourier domain, such as in magnetic resonance imaging (MRI). Graphs from this ensemble exhibit small, structured cycles with high probability, rendering current techniques for determining iterative decoding thresholds inapplicable. In this paper, we develop a theoretical platform to analyze and evaluate the power of smearing-based structure. Despite the existence of these small cycles, we derive exact density evolution recurrences for iterative decoding on graphs with smear-length two. Furthermore, we give lower bounds on the performance of a much larger class from the smearing ensemble, and provide numerical experiments showing tight agreement between empirical thresholds and those determined by our bounds. We additionally detail a system architecture to recover sparse wavelet representations in the MRI setting, giving explicit oversampling thresholds for the one-stage Haar wavelet.

Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs (15:40)

Rashad Eletreby (Carnegie Mellon University, USA); ***Osman Yağan*** *(Carnegie Mellon University & CyLab, USA)*

We study the connectivity of a random graph formed by the intersection of an inhomogeneous random key graph with an inhomogeneous Erdős-Rényi graph. The former graph is naturally induced by a heterogeneous random key predistribution scheme introduced for securing wireless sensor network communications. In this scheme, nodes are divided into r classes according to a probability distribution $\mu = \mu_1, ..., \mu_r$, and a class-i sensor is assigned K_i cryptographic keys that are selected uniformly at random from a common pool of P keys. The latter graph represents a heterogeneous on/off channel model, where the wireless channel between a class-i node and a class-j node is on (resp. off) with probability α_{ij} (resp. $1\alpha_{ij}$) independently from others. We present conditions on how to scale the parameters of the intersection model so that it is connected with high probability as the number of nodes gets large. The result is given in the form of a zero-one law and supported by a numerical study in the finite-node regime.

Fr3-2: LDPC Codes 3

Friday, June 30, 14:40-16:20
Room: Brussels
Chair: Boris Kudryashov (St. Petersburg University of Information Technologies, Mechanics and Optics, Russia)

Message Alignment for Discrete LDPC Decoders with Quadrature Amplitude Modulation (14:40)

Jan Lewandowsky *(Hamburg University of Technology, Germany); Maximilian Stark (Hamburg University of Technology, Germany); Gerhard Bauch (Hamburg University of Technology, Germany)*

Recent works describe the design of discrete decoders for low-density parity-check codes by application of mutual information maximizing clustering algorithms in discrete density evolution. In the resulting discrete message passing decoders only integers are exchanged and node operations become simple lookup operations. Earlier works only describe discrete decoders for binary modulation schemes. This paper presents a new technique called message alignment which enables to design discrete decoders for higher-order modulation schemes. First, we design a channel output quantizer for quadrature amplitude modulation with the Information Bottleneck method. The quantizer attempts to preserve the relevant information on the modulation symbols. Afterwards, we illustrate that the assignment of several bits to one modulation symbol does not allow straightforward decoder design with the available discrete density evolution technique. The proposed message alignment solves this problem. The resulting discrete decoder is compared with state-of-the-art decoders using bit error rate simulations.

Rate-Loss Reduction of SC-LDPC Codes by Optimizing Reliable Variable Nodes via Expected Graph Evolution (15:00)

Heeyoul Kwak *(Seoul National University, Korea); Jaewha Kim (Seoul National University, Korea); Jong-Seon No (Seoul National University, Korea)*

The outstanding decoding performance of spatially-coupled low-density parity-check (SC-LDPC) codes comes from wave-like propagation of reliable messages. The reliable messages are triggered by shortened (known) variable nodes in some consecutive reliable positions. However, at the cost of the improvement, shortened variable nodes cause rate-loss of SC-LDPC codes. To reduce the rate-loss, additional variable nodes (so called reliable variable nodes) can be added to the reliable positions instead of shortened variable nodes. Density evolution (DE) is an efficient

method to design degree distribution of the reliable variable nodes. However, degree distributions obtained by DE show degraded performance in finite-length code performance. In this paper, we generalize the expected graph evolution and use the analysis tool in optimizing degree distribution which shows the minimum rate-loss without finite-length performance degradation. From the well designed degree distribution, rate-loss reduction by 60% can be achieved without finite-length performance degradation.

Compute-Forward Multiple Access (CFMA) with Nested LDPC Codes (15:20)

Erixhen Sula (École Polytechnique Fédérale de Lausanne, Switzerland); Jingge Zhu (UC Berkeley, USA); Adriano Pastore (Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain); Sung Hoon Lim (Korea Institute of Ocean Science and Technology, Korea); Michael Gastpar (EPFL & University of California, Berkeley, Switzerland)

Inspired by the compute-and-forward scheme from Nazer and Gastpar, a novel multiple-access scheme introduced by Zhu and Gastpar makes use of nested lattice codes and sequential decoding of linear combinations of codewords to recover the individual messages. This strategy, coined *compute-forward multiple access* (CFMA), provably achieves points on the dominant face of the multiple-access capacity region while circumventing the need of time sharing or rate splitting. For a two-user multiple-access channel (MAC), we propose a practical procedure to design suitable codes from off-the-shelf LDPC codes and present a sequential belief propagation decoder with complexity comparable with that of point-to-point decoders. We demonstrate the potential of our strategy by comparing several numerical evaluations with theoretical limits.

Edge Spreading Design of High Rate Array-Based SC-LDPC Codes (15:40)

David Mitchell (New Mexico State University, USA); Eirik Rosnes (University of Bergen, Norway)

Absorbing sets (ASs) are combinatorially defined objects existing in the Tanner graph of a low-density parity-check (LDPC) code that have been shown to cause failures in the iterative message-passing decoder when transmission occurs over the additive white Gaussian noise channel. In this paper, we propose an edge spreading approach to construct high rate array-based spatially-coupled LDPC codes by jointly optimizing the AS spectrum and the minimum distance. By considering general edge spreadings and by considering a larger memory, we show that strictly better codes can be constructed, both in terms of achievable minimum distance for small-to-moderate block lengths and in terms of the number of small ASs.

LDPC Code Design for Correlated Sources using EXIT Charts (16:00)

Mohamad. Khas (Tarbiat Modares University, Iran); Hamid Saeedi (Tarbiat Modares University, Iran); Reza Asvadi (Shahid Beheshti University, Iran)

This paper is concerned with the design of capacity approaching ensembles of Low-Density Parity-Check (LDPC) codes for correlated sources. We consider correlated binary sources where the data is encoded independently at each source through a systematic LDPC encoder and sent over two independent Gaussian channels. At the receiver, a joint iterative decoder consisting of two component LDPC decoders is considered where the encoded bits at the output of each component decoder are used at the other decoder as the a priori information. We first provide asymptotic performance analysis using the concept of extrinsic information transfer (EXIT) charts. Compared to the conventional EXIT charts devised to analyze LDPC codes for point to point communication, the proposed EXIT charts have been completely modified to able to accommodate the systematic nature of the codes as well as the iterative behavior between the two component decoders. Then the developed modified EXIT charts are deployed to design ensembles for different levels of correlation. Our results show that as the average degree of the designed ensembles grow, the thresholds corresponding to the designed ensembles approach the capacity. In particular, for ensembles with average degree of around 9, the gap to capacity is reduced to about 0.2 dB.

Fr3-3: Caching 3

Friday, June 30, 14:40-16:20
Room: K2
Chair: Aditya Ramamoorthy (Iowa State University, USA)

Fundamental Limits of Distributed Caching in Multihop D2D Wireless Networks (14:40)

Mingyue Ji (University of Utah, USA); Rong-Rong Chen (University of Utah, USA); Giuseppe Caire (Technische Universität Berlin, Germany); Andreas Molisch (University of Southern California, USA)

We consider a wireless Device-to-Device (D2D) caching network, where users make arbitrary requests from a library of files and have pre-fetched (cached) information on their devices, subject to a per-node storage capacity constraint. The network is assumed to obey the “protocol model”, widely considered in the wireless network literature. Unlike other related works, which either restrict the communication to single-hop, or assume entire file caching, here we consider both multi-hop transmission and fully general caching strategies, including file subpacketization. We propose a

caching strategy based on deterministic assignment of MDS-coded packets of the library files, and a coded multicast delivery strategy where the users send linearly coded messages to each other in order to collectively satisfy their demands. We show that our approach can achieve the information theoretic outer bound within a multiplicative constant factor in practical parameter regimes.

Fundamental Limits on Latency in Transceiver Cache-Aided HetNets (15:00)

Jaber Kakar (Ruhr-Universitaet Bochum, Germany); Soheil Gherekhloo (RUB, Germany); Aydin Sezgin (RUB, Germany)

Stringent mobile usage characteristics force wireless networks to undergo a paradigm shift from conventional connection-centric to content-centric deployment. With respect to 5G, caching and heterogenous networks (HetNet) are key technologies that will facilitate the evolution of highly content-centric networks by facilitating unified quality of service in terms of low-latency communication. In this paper, we study the impact of transceiver caching on the latency for a HetNet consisting of a single user, a receiver and one cache-assisted transceiver. We define an information-theoretic metric, the delivery time per bit (DTB), that captures the delivery latency. We establish coinciding lower and upper bounds on the DTB as a function of cache size and wireless channel parameters; thus, enabling a complete characterization of the DTB optimality of the network under study. As a result, we identify cache beneficial and non-beneficial channel regimes.

Cache-Aided Cooperation with No CSIT (15:20)

Eleftherios Lampiris (EURECOM, France); Jingjing Zhang (EURECOM, France); Petros Elia (EURECOM, France)

This work explores cache-aided interference management in the absence of channel state information at the transmitters (CSIT), focusing on the setting with K transmitter/receiver pairs endowed with caches, where each receiver k is connected to transmitter k via a direct link with normalized capacity 1, and to any other transmitter via a cross link with normalized capacity $\tau \leq 1$. In this setting, we explore how a combination of pre-caching at transmitters and receivers, together with interference enhancement techniques, can a) partially counter the lack of CSIT, and b) render the network self-sufficient, in the sense that the transmitters need not receive additional data after pre-caching. Toward this we present new schemes that blindly harness topology and transmitter-and-receiver caching, to create separate streams, each serving many receivers at a time. Key to our approach is a combination of three impactful techniques, Rate-splitting, Interference Enhancement and Coded Caching.

Fr3-4: Entropy 3

Friday, June 30, 14:40-16:20
Room: K3
Chair: Peter Harremoës (Niels Brock, Copenhagen Business College, Denmark)

Arimoto-Renyi Conditional Entropy and Bayesian Hypothesis Testing (14:40)

Igal Sason (Technion - Israel Institute of Technology, Israel); Sergio Verdú (Princeton University, USA)

This paper gives upper and lower bounds on the minimum error probability of Bayesian M-ary hypothesis testing in terms of the Arimoto-Renyi conditional entropy of an arbitrary order α. The improved tightness of these bounds over their specialized versions with the Shannon conditional entropy ($\alpha = 1$) is demonstrated. In particular, in the case where M is finite, we show how to generalize Fano's inequality under both the conventional and list-decision settings. As a counterpart to the generalized Fano's inequality, allowing M to be infinite, a lower bound on the Arimoto-Renyi conditional entropy is derived as a function of the minimum error probability. Explicit upper and lower bounds on the minimum error probability are obtained as a function of the Arimoto-Renyi conditional entropy.

Rényi Entropy Rate of Hidden Markov Processes (15:00)

Chengyu Wu *(The University of Hong Kong, Hong Kong); 'Easton' Li Xu (Texas A&M University, USA); Guangyue Han (The University of Hong Kong, Hong Kong)*

In this paper, we focus our attention on the Rényi entropy rate of hidden Markov processes under certain positivity assumptions. The existence of the Rényi entropy rate for such processes is established. Furthermore, we show that, with some extra "fast-forgetting" assumptions, the Rényi entropy rate of the approximating Markov processes exponentially converges to that of the original hidden Markov process, as the Markov order goes to infinity.

Sharp Bounds on Arimoto's Conditional Rényi Entropies Between Two Distinct Orders (15:20)

Yuta Sakai *(University of Fukui, Japan); Ken-ichi Iwata (University of Fukui, Japan)*

This study examines sharp bounds on Arimoto's conditional Rényi entropy of order β with a fixed another one of distinct order $\alpha \neq \beta$. Arimoto inspired the relation between the Rényi entropy and the ℓ_r-norm of probability distributions, and he introduced a conditional version of the Rényi entropy. From this perspective, we analyze the ℓ_r-norms of particular distributions.

As results, we identify specific probability distributions whose achieve our sharp bounds on the conditional Rényi entropy. The sharp bounds derived in this study can be applicable to other information measures, e.g., the minimum average probability of error, the Bhattacharyya parameter, Gallager's reliability function E_0, and Sibson's α-mutual information, whose are strictly monotone functions of the conditional Rényi entropy.

Minimax Rényi Redundancy (15:40)

Semih Yagli (Princeton University, USA); Yücel Altuğ (Princeton University, USA); Sergio Verdú (Princeton University, USA)

The redundancy for universal lossless compression in Campbell's setting is characterized as a minimax Rényi divergence, which is shown to be equal to the maximal α-mutual information via a generalized redundancy-capacity theorem. Special attention is placed on the analysis of the asymptotics of minimax Rényi divergence, which is determined up to a term vanishing in blocklength.

Infinity-Rényi entropy power inequalities (16:00)

*Peng Xu (University of Delaware, USA); **James Melbourne** (University of Delaware, USA); Mokshay Madiman (University of Delaware, USA)*

An optimal ∞-Rényi entropy power inequality is derived for d-dimensional random vectors. In fact, the authors establish a matrix ∞-EPI analogous to the generalization of the classical EPI established by Zamir and Feder. The result is achieved by demonstrating uniform distributions as extremizers of a certain class of ∞-Rényi entropy inequalities, and then putting forth a new rearrangement inequality for the ∞-Rényi entropy. Quantitative results are then derived as consequences of a new geometric inequality for uniform distributions on Euclidean balls

Fr3-5: Machine Learning 2

Friday, June 30, 14:40-16:20
Room: K4
Chair: Parimal Parag (Indian Institute of Science, India)

Noisy Inductive Matrix Completion Under Sparse Factor Models (14:40)

Akshay Soni (Yahoo Research, USA); Troy Chevalier (Yahoo, USA); Swayambhoo Jain (University of Minnesota, USA)

Inductive Matrix Completion (IMC) is an important class of matrix completion problems that allows direct inclusion of available features to enhance estimation capabilities. These models have found applications in personalized recommendation systems, multilabel learning, dictionary learning, etc. This paper examines a general class of noisy matrix completion tasks where the underlying matrix is following an IMC model, i.e., it is formed by a mixing matrix (a priori unknown) sandwiched between two known feature matrices. The mixing matrix here is assumed to be well approximated by the product of two sparse matrices – referred here to as "sparse factor models". We extend an existing result to provide theoretical error bounds for the sparsity-regularized maximum likelihood estimators for the class of problems discussed in this paper. The main result is general in the sense that it can be used to derive error bounds for various noise models. In this paper, we instantiate our main result for the case of Gaussian noise and provide corresponding error bounds in terms of squared loss.

On the Problem of On-line Learning with Log-Loss (15:00)

Yaniv Fogel (Tel-Aviv University, Israel); Meir Feder (Tel-Aviv University, Israel)

In this paper we consider the problem of on-line learning with respect to the logarithmic loss, where the learner provides a probability assignment for the next label given the past and current data samples and the past labels. We consider the problem in the individual and the stochastic settings. Our first result is a class of new universal on-line probability assignment schemes based on the mixture approach. Now, in classical learning, it is well known that there are model classes that can be learned in batch, but cannot be learned sequentially for all data samples sequences. We show that for these model classes the proposed mixture schemes lead to a vanishing regret in the individual setting when the adversary is somewhat constrained. In the stochastic setting we show that any on-line solution for the log-loss may be used to obtain a solution for a wide variety of loss functions.

Multiclass MinMax Rank Aggregation (15:20)

Pan Li (University of Illinois Urbana-Champaign, USA); Olgica Milenkovic (UIUC, USA)

We introduce a new family of minmax rank aggregation problems under two distance measures, the Kendall τ and the Spearman footrule. As the problems are NP-hard, we proceed to describe a number of constant-approximation algorithms for solving them. We conclude with illustrative applications of the aggregation methods on the Mallows model and genomic data.

Adiabatic Persistent Contrastive Divergence Learning (15:40)

Hyeryung Jang (KAIST, Korea); Hyungwon Choi (KAIST, Korea); Yung Yi (KAIST, Korea); Jinwoo Shin (KAIST, Korea)

This paper studies the problem of parameter learning in graphical models having latent variables, where the standard approach is the expectation maximization algorithm alternating expectation (E) and maximization (M) steps. However, both E and M steps are computationally intractable for high dimensional data, while the substitution of one step to a faster surrogate for combating against intractability can often cause failure in convergence. To tackle the issue, the Contrastive Divergence (CD) learning scheme has been popularly used in the deep learning community, where it runs the mean-field approximation in E step and a few cycles of Markov Chains (MC) in M step. In this paper, we analyze a variant of CD, called Adiabatic Persistent Contrastive Divergence (APCD), which runs a few cycles of MCs in both E and M steps. Using multi-time-scale stochastic approximation theory, we prove that APCD converges to a correct optimum, where the standard CD is impossible to have such a guarantee due to the mean-field approximation gap in E step. Despite of such stronger theoretical guarantee of APCD, its possible drawback is on slow mixing on E step for practical purposes. To address the issue, we also design a hybrid approach applying both mean-field and MC approximations in E step, where it outperforms the standard mean-field-based CD in our experiments on real-world datasets.

Online Nonparametric Anomaly Detection based on Geometric Entropy Minimization (16:00)

***Yasin Yilmaz** (University of South Florida, USA)*

We consider the online and nonparametric detection of abrupt and persistent anomalies, such as a change in the regular system dynamics at a time instance due to an anomalous event (e.g., a failure, a malicious activity). Combining the simplicity of the nonparametric Geometric Entropy Minimization (GEM) method with the timely detection capability of the Cumulative Sum (CUSUM) algorithm we propose a computationally efficient online anomaly detection method that is applicable to high-dimensional datasets, and at the same time achieve a near-optimum average detection delay performance for a given false alarm constraint. We provide new insights to both GEM and CUSUM, including new asymptotic analysis for GEM, which enables soft decisions for outlier detection, and a novel interpretation of CUSUM in terms of the discrepancy theory, which helps us generalize it to the nonparametric GEM statistic. We numerically show, using both simulated and real datasets, that the proposed nonparametric algorithm attains a close performance to the clairvoyant parametric CUSUM test.

Fr3-6: Estimation 2

Friday, June 30, 14:40-16:20
Room: K5
Chair: Laura Cottatellucci (EURECOM, France)

Spectral Initialization for Nonconvex Estimation: High-Dimensional Limit and Phase Transitions (14:40)

***Yue Lu** (Harvard University, USA); Gen Li (Tsinghua University, P.R. China)*

We study a simple spectral method that serves as a key ingredient in a growing line of work using efficient iterative algorithms for estimating signals in nonconvex settings. Unlike previous work, which focuses on the phase retrieval setting and provides only bounds on the performance, we consider arbitrary generalized linear sensing models and provide an exact characterization of the performance of the spectral method in the high-dimensional regime. Our analysis reveals a phase transition phenomenon that depends on the sampling ratio. When the ratio is below a critical threshold, the estimates given by the spectral method are no better than random guesses drawn uniformly from the hypersphere; above the threshold, however, the estimates become increasingly aligned with the underlying signal. Worked examples and numerical simulations are provided to illustrate and verify the analytical predictions.

Jackknife estimation for Markov processes with no mixing constraints (15:00)

Kevin Oshiro (University of Hawaii at Manoa, USA); Changlong Wu (University of Hawaii at Manoa, USA); Narayana Prasad Santhanam (University of Hawaii at Manoa, USA)

The jackknife resampling procedure is widely used to reduce the bias of a statistic. As with other resampling techniques,the jackknife procedure is motivated by and is well understood in the i.i.d. regime. However, its analysis when samples have memory is limited, and predominantly restricted to cases with strong mixing or memory constraints. In this paper, we analyze a natural jackknife resampling procedure for Markov sources with no mixing assumptions. For the problem to be well posed, we instead adopt a physically motivated continuity condition that ensures that the information a bit in the past provides about the current bit, conditioned on all bits in between, diminishes with the amount of history we have. We compute the jackknife procedure for variance of transition probability estimates given arbitrary contexts. We show that the bias of this jackknife procedure can be bounded close to the true variance.

Minimax Risk for Missing Mass Estimation (15:20)

Nikhilesh Rajaraman (IIT Madras, India); Andrew Thangaraj (IIT Madras, India); Ananda Suresh (University of California, San Diego, USA)

The problem of estimating the missing mass or total probability of unseen elements in a sequence of n random samples is considered under the squared error loss function. The worst-case risk of the popular Good-Turing estimator is shown to be between $0.6080/n$ and $0.6179/n$. The minimax risk is shown to be lower bounded by $0.25/n$. This appears to be the first such published result on minimax risk for estimation of missing mass, which has several practical and theoretical applications.

Fr3-7: Information Theory and Statistics 2

Friday, June 30, 14:40-16:20
Room: K6
Chair: Himanshu Tyagi (Indian Institute of Science, India)

Ensemble Estimation of Mutual Information (14:40)

*Kevin Moon (Yale University, USA); Kumar Sricharan (Xerox PARC, USA); **Alfred Hero III** (University of Michigan, USA)*

We derive the mean squared error convergence rates of kernel density-based plug-in estimators of mutual information measures between two multidimensional random variables $\mathbf{X}$ and $\mathbf{Y}$ for two cases: 1) $\mathbf{X}$ and $\mathbf{Y}$ are both continuous; 2) $\mathbf{X}$ is continuous and $\mathbf{Y}$ is discrete. Using the derived rates, we propose an ensemble estimator of these information measures for the second case by taking a weighted sum of the plug-in estimators with varied bandwidths. The resulting ensemble estimator achieves the $1/N$ parametric convergence rate when the conditional densities of the continuous variables are sufficiently smooth. To the best of our knowledge, this is the first nonparametric mutual information estimator known to achieve the parametric convergence rate for this case, which frequently arises in applications (e.g. variable selection in classification). The estimator is simple to implement as it uses the solution to an offline convex optimization problem and simple plug-in estimators. Ensemble estimators that achieve the parametric rate are also derived for the first case ($\mathbf{X}$ and $\mathbf{Y}$ are both continuous) and another case: 3) $\mathbf{X}$ and $\mathbf{Y}$ may have any mixture of discrete and continuous components.

Minimum Rates of Approximate Sufficient Statistics (15:00)

*Masahito Hayashi (Nagoya University, Japan); **Vincent Tan** (National University of Singapore, Singapore)*

Given a sufficient statistic for a parametric family of distributions, one can estimate the parameter without access to the data itself. However, the memory or code size for storing the sufficient statistic may nonetheless still be prohibitive. Indeed, for n independent data samples drawn from a k-nomial distribution with $d = k - 1$ degrees of freedom, the length of the code scales as $d \log n + O(1)$. In many applications though, we may not have a useful notion of sufficient statistics and also may not need to reconstruct the generating distribution exactly. By adopting a Shannon-theoretic approach in which we consider allow a small error in estimating the generating distribution, we construct various notions of approximate sufficient statistics and show that the code length can be reduced to $\frac{d}{2} \log n + O(1)$. We consider errors measured according to the relative entropy and variational distance criteria. For the code construction parts, we leverage Rissanen's minimum description length (MDL) principle, which yields a non-vanishing error measured using the relative entropy. For the converse parts, we use Clarke and Barron's asymptotic expansion for the relative entropy of a parametrized distribution and the corresponding mixture distribution. The limitation of this method is that only a weak converse for the variational distance can be shown. We develop new techniques to achieve vanishing errors and we also prove strong converses for all our statements. The latter means that even if the code is allowed to have a non-vanishing error, its length must still be at least $\frac{d}{2} \log n$.

Information-theoretic characterizations of Markov random fields and subfields (15:20)

Raymond W. Yeung (The Chinese University of Hong Kong, Hong Kong); Ali Al-Bashabsheh (Beijing Advanced Innovation Center for Big Data and Brain Computing (BDBC), Beihang University, P.R. China); Chao Chen (Xi'dian, P.R. China); Qi Chen (The Chinese University of Hong Kong, Hong Kong); Pierre Moulin (University of Illinois at Urbana-Champaign, USA)

Let $X_i, i \in V$ form a Markov random field (MRF) represented by an undirected graph $G = (V, E)$, and V' be a subset of V. We determine the smallest graph that can always represent the subfield $X_i, i \in V'$ as an MRF. Based on this result, we obtain a necessary and sufficient condition for a subfield of a Markov tree to be also a Markov tree. When G is a path so that $X_i, i \in V$ form a Markov chain, it is known that the I-Measure is always nonnegative [2]. We prove that Markov chain is essentially the only MRF that possesses this property. Our work is built on the set-theoretic characterization of an MRF in [4]. Unlike most works in the literature, we

do not make the standard assumption that the underlying probability distribution is factorizable with respect to the graph representing the MRF.

Conditional Central Limit Theorems for Gaussian Projections (15:40)

Galen Reeves (Duke University, USA)

This paper addresses the question of when projections of a high-dimensional random vector are approximately Gaussian. This problem has been studied previously in the context of high-dimensional data analysis, where the focus is on low-dimensional projections of high-dimensional point clouds. The focus of this paper is on the typical behavior when the projections are generated by an i.i.d. Gaussian projection matrix. The main results are bounds on the deviation between the conditional distribution of the projections and a Gaussian approximation, where the conditioning is on the projection matrix. The bounds are given in terms of the quadratic Wasserstein distance and relative entropy and are stated explicitly as a function of the number of projections and certain key properties of the random vector. The proof uses Talagrand's transportation inequality and a general integral-moment inequality for mutual information. Applications to random linear estimation and compressed sensing are discussed.

An Information Theoretic Analysis of Sequential Decision-Making (16:00)

Meik Dörpinghaus (TU Dresden, Germany); Édgar Roldán (Max-Planck-Institute for the Physics of Complex Systems, Germany); Izaak Neri (Max-Planck-Institute for the Physics of Complex Systems, Germany); Heinrich Meyr (RWTH Aachen University, Germany); Frank Jülicher (Max Planck Institute for the Physics of Complex Systems, Germany)

We provide a novel analysis of Wald's sequential probability ratio test based on information theoretic measures for symmetric thresholds, symmetric noise, and equally likely hypotheses. This test is optimal in the sense that it yields the minimum mean decision time. To analyze the decision-making process we consider information densities, which represent the stochastic information content of the observations yielding a stochastic termination time of the test. Based on this, we show that the conditional probability to decide for hypothesis H_1 (or the counter-hypothesis H_0) given that the test terminates at time instant k is independent of time k. An analogous property has been found for a continuous-time first passage problem with two absorbing boundaries in the contexts of non-equilibrium statistical physics and communication theory. Moreover, we study the evolution of the mutual information between the binary variable to be tested and the output of the Wald test. Notably, we show that the decision time of the Wald test contains no information on which hypothesis is true beyond the decision outcome.

Fr3-8: Index Coding 2

Friday, June 30, 14:40-16:00
Room: K7+8
Chair: Guido Montorsi (Politecnico di Torino, Italy)

On the Capacity for Distributed Index Coding (14:40)

Yucheng Liu (Australian National University, Australia); Parastoo Sadeghi (The Australian National University, Australia); Fatemeh Arbabjolfaei (University of California, San Diego, USA); Young-Han Kim (UCSD, USA)

The distributed index coding problem is studied, whereby multiple messages are stored at different servers to be broadcast to receivers with side information. First, the existing composite coding scheme is enhanced for the centralized (single-server) index coding problem, which is then merged with fractional partitioning of servers to yield a new coding scheme for distributed index coding. New outer bounds on the capacity region are also established. For 213 out of 218 non-isomorphic distributed index coding problems with four messages the achievable sum-rate of the proposed distributed composite coding scheme matches the outer bound, thus establishing the sum-capacity for these problems.

Improved Bounds for Multi-Sender Index Coding (15:00)

Min Li (The University of Newcastle, Australia); Lawrence Ong (The University of Newcastle, Australia); Sarah Johnson (University of Newcastle, Australia)

We establish new capacity bounds for the multi-sender unicast index-coding problem. We first revisit existing bounds proposed by Sadeghi et al. and identify the suboptimality of their inner bounds in general. We then present a simplified version of the existing multi-sender maximal-acyclic-induced-subgraph outer bound. For the inner bound, we propose joint link-and-sender partitioning to replace sender partitioning in partitioned Distributed Composite Coding (DCC). This leads to a modified DCC (mDCC) that outperforms partitioned DCC and suffices to achieve optimality for some index-coding instances. We also propose cooperative compression of composite messages in composite coding to exploit messages common to different senders to support larger composite rates than those by point-to-point compression in the existing schemes. We then develop a new multi-sender Cooperative Composite Coding (CCC) scheme. CCC further improves upon mDCC in general, and is instrumental to achieve optimality for a number of index-coding instances.

Uniprior Index Coding (15:20)

Vijaya Kumar Mareedu *(International Institute of Information Technology, Hyderabad (IIIT H), India); Prasad Krishnan (IIIT Hyderabad, India)*

The index coding problem is a problem of efficient broadcasting with side-information. We look at the uniprior index coding problem, in which the receivers have disjoint side-information symbols and arbitrary demand sets. Previous work has addressed single uniprior index coding, in which each receiver has a single unique side-information symbol. Modeling the uniprior index coding problem as a *supergraph*, we focus on a class of uniprior problems defined on *generalized cycle* supergraphs. For such problems, we prove upper and lower bounds on the optimal broadcast rate. Using a connection with Eulerian directed graphs, we also show that the upper and lower bounds are equal for a subclass of uniprior problems. We show the NP-hardness of finding the lower bound for uniprior problems on generalized cycles. Finally, we look at a simple extension of the generalized cycle uniprior class for which we give bounds on the optimal rate and show an explicit scheme which achieves the upper bound.

Rate $\frac{1}{3}$ Index Coding: Forbidden and Feasible Configurations (15:40)

Lalitha Vadlamani (International Institute of Information Technology, India); Prasad Krishnan (IIIT Hyderabad, India)

Linear index coding can be formulated as an interference alignment problem, in which precoding vectors of the minimum possible length are to be assigned to the messages in such a way that the precoding vector of a demand (at some receiver) is independent of the space of the interference (non side-information) precoding vectors. An index code has rate $\frac{1}{l}$ if the assigned vectors are of length l. In this paper, we introduce the notion of strictly rate $\frac{1}{L}$ message subsets which must necessarily be allocated precoding vectors from a strictly L-dimensional space ($L = 1, 2, 3$) in any rate $\frac{1}{3}$ code. We develop a general necessary condition for rate $\frac{1}{3}$ feasibility using intersections of strictly rate $\frac{1}{L}$ message subsets. We apply the necessary condition to show that the presence of certain interference configurations makes the index coding problem rate $\frac{1}{3}$ infeasible. We also obtain a class of index coding problems, containing certain interference configurations, which are rate $\frac{1}{3}$ feasible based on the idea of *contractions* of an index coding problem. Our necessary conditions for rate $\frac{1}{3}$ feasibility and the class of rate $\frac{1}{3}$ feasible problems obtained subsume all such known results for rate $\frac{1}{3}$ index coding.

Fr3-9: Statistics 2

Friday, June 30, 14:40-16:20
Room: K9
Chair: Raymond W. Yeung (The Chinese University of Hong Kong, Hong Kong)

Divergence Scaling of Fixed-Length, Binary-Output, One-to-one Distribution Matching (14:40)

Patrick Schulte (Technische Universität München, Germany); Bernhard Geiger (Technical University of Munich, Germany)

Distribution matching is the process of invertibly mapping a uniformly distributed input sequence onto sequences that approximate the output of a desired discrete memoryless source. The special case of a binary output alphabet and one-to-one mapping is studied. A fixed-length distribution matcher is proposed that is optimal in the sense of minimizing the unnormalized informational divergence between its output distribution and a binary memoryless target distribution. Upper and lower bounds on the unnormalized divergence are computed that increase logarithmically in the output block length n. It follows that a recently proposed constant composition distribution matcher performs within a constant gap of the minimal achievable informational divergence.

Lower Bounds on the Minimax Risk for the Source Localization Problem (15:00)

Praveen Venkatesh (Carnegie Mellon University, USA); Pulkit Grover (Carnegie Mellon University, USA)

The “source localization” problem is one in which we estimate the location of a point source observed through a diffusive medium using an array of sensors. We give lower bounds on the minimax risk (mean squared-error in location) in estimating the location of the source, which apply to all estimators, for certain classes of diffusive media, when using a uniformly distributed sensor array. We show that for sensors of a fixed size, the lower bound decays with increasing numbers of sensors. We also analyze a more physical sensor model to understand the effect of shrinking the size of sensors as their number increases to infinity, wherein the bound saturates for large sensor numbers. In this scenario, it is seen that there is greater benefit to increasing the number of sensors as the signal-to-noise ratio increases. Our bounds are the first to give a scaling for the minimax risk in terms of the number of sensors used.

On the Optimality of Some Group Testing Algorithms (15:20)

Matthew Aldridge (University of Bath & Heilbronn Institute for Mathematical Research, United Kingdom (Great Britain))

We consider Bernoulli nonadaptive group testing with $k = n^\theta$ defectives, for $\theta \in (0, 1)$. The practical definite defectives (DD) detection algorithm is known to be optimal for $\theta > 1/2$. We give a new upper bound on the rate of DD, showing that DD is strictly suboptimal for $\theta < 0.41$. We also show that the SCOMP algorithm and algorithms based on linear programming achieve a rate at least as high as DD, so in particular are also optimal for $\theta > 1/2$.

Measurement Dependent Noisy Search: The Gaussian Case (15:40)

***Anusha Lalitha** (University of California San Diego, USA); Nancy Ronquillo (UCSD, USA); Tara Javidi (UCSD, USA)*

This paper considers the problem of searching for the unknown location of a target among a finite number of possible locations by probing multiple locations simultaneously. Outcome of each search measurement is corrupted by Gaussian noise whose intensity is proportional to the number of locations probed. We characterize a non-asymptotic lower bound on adaptivity gain; i.e. reduction in the expected number of measurements under an adaptive search strategies over the non-adaptive search strategies. Then we investigate the adaptivity gain in two complementary asymptotic regimes: one where the total search area is kept fixed but the location width is shrinking or the search resolution is increasing, and the other where each location width is fixed but the total search area is growing. Interestingly, adaptivity gain grows in distinctly different manner in these two regimes. In particular, adaptivity gains are significant in the later regime when the total search space grows; implying adaptivity is far more critical when either total search area or the noise intensity is large.

Scalable Multichannel Joint Sequential Change Detection and Isolation (16:00)

***Sourabh Banerjee** (University of Illinois at Urbana-Champaign, USA); Georgios Fellouris (University of Illinois at Urbana-Champaign, USA)*

The problem of joint sequential change detection and isolation in a multichannel system is considered. It is assumed that a disruption occurs at some unknown time, and changes the distributions of the observations in an unknown subset of channels. The problem is to quickly detect the change, and at the same time to reliably isolate the affected channels. A novel scheme is proposed for this task, which admits a recursive structure, is scalable with respect to the number of channels, and does not require any prior information about the change-point. Its performance is analyzed in the special case that the number of affected channels is known. Specifically, explicit critical values are obtained for the control of the false alarm rate and the conditional probability of wrong isolation below arbitrary levels to be prescribed by the practitioner. Finally, the asymptotic optimality of the average detection delay of the proposed scheme is established as the error probabilities go to 0 and the effect of the prior distribution for the change point vanishes in the limit.

Fr4-1: Coding Theory 4

Friday, June 30, 16:40-18:00
Room: Europa
Chair: Hans-Andrea Loeliger (ETH Zurich, Switzerland)

A New Approach for Constructing and Decoding Maximum Rank Distance Codes (16:40)

Hessam Mahdavifar (University of Michigan, USA)

A rank-metric code is a subset of $\mathbb{F}_q^{n\times m}$, where $\mathbb{F}_q$ is a finite field. Gabidulin codes are a well-known class of algebraic rank-metric codes that meet the Singleton bound on the minimum rank distance of a code. The construction, encoding, and decoding of Gabidulin codes use the extension field $\mathbb{F}_{q^m}$, where the code is regarded as a linear block code of length n over $\mathbb{F}_{q^m}$. However, the parameter m can be large in certain applications and therefore, performing field operations over $\mathbb{F}_{q^m}$ can become very complex. In this paper, we investigate methods for constructing and decoding rank-metric codes by looking into linear codes of length nm over the base field $\mathbb{F}_q$. Random coding bounds are derived on the minimum distance of such codes and an explicit structure is demonstrated to construct maximum rank distance codes. It is shown how to construct sparse parity-check matrices for these structures which enables low complexity parallelized decoders with complexity that scales linearly with m.

Individually-Secure Multi-Source Multicast (17:00)

***Alejandro Cohen** (Ben-Gurion University, Israel); Asaf Cohen (Ben-Gurion University of the Negev, Israel); Omer Gurewitz (Ben-Gurion University Of The Negev, Israel); Muriel Médard (MIT, USA)*

The principal mission of Multi-Source Multicast (MSM) is to disseminate all messages from all sources in a network to all destinations. MSM is utilized in numerous applications. In many of them, securing the messages disseminated is critical. A common secure model is to consider a network where there is an eavesdropper which is able to observe a subset of the network links, and seek a code which keeps the eavesdropper igno-

rant regarding all the messages. While this is solved when all messages are located at a single source, Secure MSM (SMSM) is an open problem, and the rates required are hard to characterize in general. In this paper, we consider Individual Security, which promises that the eavesdropper has zero mutual information with each message individually. We completely characterize the rate region for SMSM under individual security, and show that such a security level is achievable at the full capacity of the network, that is, the cut-set bound is the matching converse, similar to non-secure MSM. Moreover, we show that the field size is similar to non-secure MSM and does not have to be larger due to the security constraint.

Lattice coding for Rician fading channels from Hadamard rotations (17:20)

Alex Karrila (Aalto University, Finland); Niko Väisänen (Aalto University, Finland); David Karpuk (Aalto University, Finland); ***Camilla Hollanti*** *(Aalto University, Finland)*

In this paper, we study lattice coding for Rician fading wireless channels. This is motivated in particular by preliminary studies suggesting the Rician fading model for millimeter-wavelength wireless communications. We restrict to lattice codes arising from rotations of $\mathbb{Z}^n$, and to a single-input single-output (SISO) channel. We observe that several lattice design criteria suggest the optimality of Hadamard rotations. For instance, we prove that Hadamard rotations maximize the diamond-packing density among all rotated $\mathbb{Z}^n$ lattices. Finally, we provide simulations to show that Hadamard rotations outperform optimal algebraic rotations and cross-packing lattices in the Rician channel.

Fr4-2: DNA and Coding

Friday, June 30, 16:40-18:00
Room: Brussels
Chair: Olgica Milenkovic (UIUC, USA)

Mutually Uncorrelated Codes for DNA Storage (16:40)

Maya Levy (Technion - Israel Institute of Technology, Israel); Eitan Yaakobi (Technion, Israel)

Mutually Uncorrelated (MU) codes is a class of codes in which no proper prefix of one codeword is a suffix of another codeword. These codes were originally studied for synchronization purposes and recently, Yazdi et al. showed their applicability to enable random access in DNA storage. In this work we follow the research of Yazdi et al. and study MU codes along with their extensions to correct errors and balanced codes. We first study a well known construction of MU codes and show that its existing lower bound on the cardinality is tight. We also present efficient algorithm for MU codes with linear encoding and decoding. We then extend these results for (d_h, d_m)-MU codes that impose a minimum Hamming distance of d_e between different codewords and d_m between prefixes and suffixes. Particularly we show an efficient construction of these codes with nearly optimal redundancy. We provide similar results for the edit distance and balanced MU codes.

Noise and Uncertainty in String-Duplication Systems (17:00)

Siddharth Jain (California Institute of Technology, USA); Farzad Farnoud (Hassanzadeh) (California Institute of Technology, USA); Moshe Schwartz (Ben-Gurion University of the Negev, Israel); Jehoshua Bruck (California Institute of Technology, USA)

Duplication mutations play a critical role in the generation of biological sequences. Simultaneously, they have a deleterious effect on data stored using in-vivo DNA data storage. While duplications have been studied both as a sequence-generation mechanism and in the context of error correction, for simplicity these studies have not taken into account the presence of other types of mutations. In this work, we consider the capacity of duplication mutations in the presence of point-mutation noise, and so quantify the generation power of these mutations. We show that if the number of point mutations is vanishingly small compared to the number of duplication mutations of a constant length, the generation capacity of these mutations is zero. However, if the number of point mutations increases to a constant fraction of the number of duplications, then the capacity is nonzero. Lower and upper bounds for this capacity are also presented. Another problem that we study is concerned with the mismatch between code design and channel in data storage in the DNA of living organisms with respect to duplication mutations. In this context, we consider the uncertainty of such a mismatched coding scheme measured as the maximum number of input codewords that can lead to the same output.

Rank Modulation Codes for DNA Storage (17:20)

Netanel Raviv (Technion & Tel-Aviv University, Israel); Moshe Schwartz (Ben-Gurion University of the Negev, Israel); Eitan Yaakobi (Technion, Israel)

Synthesis of DNA molecules offers unprecedented advances in storage technology. Yet, the microscopic world in which these molecules reside induces error patterns that are fundamentally different from their digital counterparts. Hence, to maintain reliability in reading and writing, new coding schemes must be developed. In a reading technique called shotgun sequencing, a long DNA string is read in a sliding window fashion, and a profile vector is produced. It was recently suggested by Kiah et al. that such a vector can represent the permutation which is induced by its entries, and hence a rank modulation scheme arises.

Although this interpretation suggests high error tolerance, it is unclear which permutations are feasible, and how to produce a DNA string whose profile vector induces a given permutation. In this paper, by observing some necessary conditions, an upper bound for the number of feasible permutations is given. Further, a technique for deciding the feasibility of a permutation is devised. By using this technique, an algorithm for producing a considerable number of feasible permutations is given, which applies to any alphabet size and any window length.

Fundamental Limits of DNA Storage Systems (17:40)

Reinhard Heckel (University of California, Berkeley, USA); Ilan Shomorony (UC Berkeley, USA); Kannan Ramchandran (University of California at Berkeley, USA); David Tse (Stanford University, USA)

Due to its longevity and enormous information density, DNA is an attractive medium for archival storage. In this work, we study the fundamental limits and tradeoffs of DNA-based storage systems under a simple model, motivated by current technological constraints on DNA synthesis and sequencing. Our model captures two key distinctive aspects of DNA storage systems: (1) the data is written onto many short DNA molecules that are stored in an unordered way and (2) the data is read by randomly sampling from this DNA pool. Under this model, we characterize the storage capacity, and show that a simple index-based coding scheme is optimal.

Fr4-3: Error Exponents

Friday, June 30, 16:40-18:00
Room: K2
Chair: Meir Feder (Tel-Aviv University, Israel)

Distributed Identity Testing with Zero-Rate Compression (16:40)

Wenwen Zhao (University of California, Davis, USA); Lifeng Lai (University of California, Davis, USA)

In this paper, we consider the identity testing problems in the distributed setting, in which each terminal has data only relates to one random variable. Each terminal sends zero-rate message to the decision maker, and the decision maker decides the distribution of $(X^n; Y^n)$, which is indirectly revealed from the encoded messages, is the same as or λ-far from a given distribution. Interpreting this as a distributed composite hypothesis testing problem, we characterize the best error exponent of the type 2 error probability using a universal coding scheme under the exponential-type constraint on the type 1 error probability.

Exponential source/channel duality (17:00)

Sergey Tridenski (Tel Aviv University, Israel); Ram Zamir (Tel Aviv University, Israel)

We propose a source/channel duality in the exponential regime, where success/failure in source coding parallels error/correctness in channel coding, and a distortion constraint becomes a log-likelihood ratio (LLR) threshold. We establish this duality by first deriving exact exponents for lossy coding of a memoryless source P, at distortion D, for a general i.i.d. codebook distribution Q, for both encoding success (R<R(P,Q,D)) and failure (R>R(P,Q,D)). We then turn to maximum likelihood (ML) decoding over a memoryless channel P with an i.i.d. input Q, and show that if we substitute P=QP, Q=Q, and D=0 under the LLR distortion measure, then the exact exponents for decoding-error (R < I(Q, P)) and strict correct-decoding (R > I(Q, P)) follow as special cases of the exponents for source encoding success/failure, respectively. Moreover, by letting the threshold D take general values, the exact random-coding exponents for erasure (D>0) and list decoding (D<0) under the simplified Forney decoder are obtained. Finally, we derive the exact random-coding exponent for Forney's optimum tradeoff erasure/list decoder, and show that at the erasure regime it coincides with Forney's lower bound and with the simplified decoder exponent, settling a long standing conjecture.

Error Exponents for Sparse Communication (17:20)

Lóránt Farkas (Budapest University of Technology and Economics, Hungary); Tamás Kói (Budapest University of Technology and Economics, Hungary); Imre Csiszár (Renyi Institute, Hungarian Academy of Science, Hungary)

Communication over a discrete memoryless channel is addressed when codewords are transmitted in certain time intervals of arbitrary locations, at other times the channel outputs pure noise. The receiver has to locate and decode the codewords. Exponential error bounds are derived, jointly achievable via a semi-universal or universal decoder. Implications are discussed for the familiar model of communication under strong asynchronism when in exponentially long time only one codeword is transmitted.

Universal Random Access Error Exponents for Codebooks with Different Word-Lengths (17:40)

Lóránt Farkas (Budapest University of Technology and Economics, Hungary); Tamás Kói (Budapest University of Technology and Economics, Hungary)

Csiszár's channel coding theorem for multiple codebooks is generalized allowing the codeword lengths differ across codebooks. Also in this case, for each codebook an error exponent can be achieved that equals the random coding exponent for this codebook

alone, in addition, the overload detection failure probability tends to 0. This is proved even for sender and receiver not knowing the channel. As a corollary, a substantial improvement is obtained when the sender knows the channel.

Fr4-4: Bounds 4

Friday, June 30, 16:40-18:00
Room: K3
Chair: Itzhak Tamo (Tel Aviv University, Israel)

Bounds on the Rate and Minimum Distance of Codes with Availability (16:40)

***Balaji Srinivasan Babu** (IISc, India); P Vijay Kumar (Indian Institute of Science & University of Southern California, India)*

In this paper we investigate bounds on rate and minimum distance of codes with t availability. We present bounds on minimum distance of a code with t availability that are tighter than existing bounds. For bounds on rate of a code with t availability, we restrict ourselves to a sub-class of codes with t availability called codes with strict t availability and derive a tighter rate bound. Codes with strict t availability can be defined as the null space of an $(m \times n)$ parity-check matrix H, where each row has weight $(r+1)$ and each column has weight t, with intersection between support of any two rows at most one. We also present two general constructions for codes with t availability.

Improved existence bounds on IPP codes using the Clique Lovász Local Lemma (17:00)

Cástor Aranda (Technical University of Catalonia, Spain); Marcel Fernández (Technical University of Catalonia, Spain)

Codes with the Identifying Parent Property constitute a powerful type of codes with many uses in fingerprinting. Thus, it is of great interest to find sharp existence bounds for that class of codes. By applying a specific variation of the Lovász Local Lemma, we get existence bounds on q-ary IPP codes that improve previously stated ones.

Explicit bounds on the length of optimal X-codes (17:20)

***Yu Tsunoda** (Chiba University, Japan); Yuichiro Fujiwara (Chiba University, Japan)*

X-codes are linear maps with a special combinatorial property that generalizes superimposed codes, disjunct matrices, and cover-free families. In the context of circuit testing, a (t, n, d, x) X-code compresses n-bit output from the circuit under test into t bits while allowing for detecting the existence of up to d erroneous output bits even if up to x bits of the correct behavior are unknowable. A simple counting argument shows that a (t, n, d, x) X-code with $t = O(\log n)$ exists, where the coefficient of the logarithmic term when the base is 2 is at most $2^{x+1}(d+x)\ln 2$ with $\ln$ being the natural logarithm to base e. While there are also known constructions that provide X-codes with smaller t for given n and some specific d and x, no stronger general upper bounds on the smallest possible t that work for any d and x are available in the literature. Here, we derive general upper bounds in closed form that reduce the coefficient of the basic general bound to $(x+1)(d+x-1)e\ln 2$. In terms of the highest achievable rate, our results exponentially improve the known asymptotic lower bound $1/(2^{x+1}(d+x)\ln 2)$ to $1/((x+1)(d+x-1)e\ln 2)$.

A convolution inequality for entropy over Z2 (17:40)

Varun Jog (University of Wisconsin - Madison, USA)

We prove an inequality for the entropy of a sum of two independent random variables taking values in the group $\mathbb{Z}_2$. Our inequality is very simply stated, and may be interpreted as a lower bound on the capacity of a cascade of two BSC channels in terms of the capacities of the component BSC channels. The inequality provides an upper bound on the entropy of a sum of two $\mathbb{Z}_2$-valued random variables, and thus it may also be thought of as a reverse entropy power inequality. One of the intriguing features of this inequality is that it only holds if entropy is measured in bits; i.e., the base with respect to which logarithms are taken matters crucially.

Fr4-5: Shannon Theory and Applications

Friday, June 30, 16:40-18:00
Room: K4
Chair: Sergio Verdú (Princeton University, USA)

Topological Structures on DMC spaces (16:40)

Rajai Nasser (École Polytechnique Fédérale de Lausanne, Switzerland)

Two channels are said to be equivalent if they are degraded from each other. The space of equivalent channels with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$ can be naturally endowed with the quotient of the Euclidean topology by the equivalence relation. We show that this topology is compact, path-connected and metrizable. A topology on the space of equivalent channels with fixed input alphabet $\mathcal{X}$ and arbitrary but finite output alphabet is said to be natural if and only if it induces the quotient topology on the subspaces of equivalent channels sharing the same output alphabet.

We show that every natural topology is σ-compact, separable and path-connected. On the other hand, if $|\mathcal{X}| \geq 2$, a Hausdorff natural topology is not Baire and it is not locally compact anywhere. This implies that no natural topology can be completely metrized if $|\mathcal{X}| \geq 2$. The finest natural topology, which we call the strong topology, is shown to be compactly generated, sequential and T_4. On the other hand, the strong topology is not first-countable anywhere, hence it is not metrizable. We show that in the strong topology, a subspace is compact if and only if it is rank-bounded and strongly-closed. We provide a necessary and sufficient condition for a sequence of channels to converge in the strong topology. We introduce a metric distance on the space of equivalent channels which compares the noise levels between channels. The induced metric topology, which we call the noisiness topology, is shown to be natural. We also study topologies that are inherited from the space of meta-probability measures by identifying channels with their Blackwell measures. We show that the weak-$*$ topology is exactly the same as the noisiness topology and hence it is natural. We prove that if $|\mathcal{X}| \geq 2$, the total variation topology is not natural nor Baire, hence it is not completely metrizable. Moreover, it is not locally compact anywhere. Finally, we show that the Borel σ-algebra is the same for all Hausdorff natural topologies.

A Strong Data Processing Inequality for Thinning Poisson Processes and Some Applications (17:00)

Ligong Wang (ETIS & CNRS, France)

This paper derives a simple strong data processing inequality (DPI) for Poisson processes: after a Poisson process is passed through p-thinning—in which every arrival remains in the process with probability p and is erased otherwise, independently of the other points—the mutual information between the Poisson process and any other random variable is reduced to no more than p times its original value. This strong DPI is applied to prove tight converse bounds in several problems: hypothesis testing with communication constraints, a mutual information game, and a CEO problem.

Continuity of Channel Parameters and Operations under Various DMC Topologies (17:20)

Rajai Nasser (École Polytechnique Fédérale de Lausanne, Switzerland)

We study the continuity of several channel parameters and operations under various topologies on the space of equivalent discrete memoryless channels (DMC). We show that mutual information, channel capacity, Bhattacharyya parameter, probability of error of a fixed code, and optimal probability of error for a given code rate and blocklength, are continuous under various DMC topologies. We also show that channel operations such as sums, products, interpolations, and Arıkan-style transformations are continuous.

SCW Codes for Optimal CSI-Free Detection in Diffusive Molecular Communications (17:40)

Vahid Jamali *(Friedrich-Alexander-University Erlangen-N¨urnberg, Germany); Arman Ahmadzadeh (University of Erlangen-Nuremberg, Germany); Nariman Farsad (Stanford University, USA); Robert Schober (University of British Columbia, Canada)*

Instantaneous or statistical channel state information (CSI) is needed for most detection schemes developed in the molecular communication (MC) literature. Since the MC channel changes, e.g., due to variations in the velocity of flow, the temperature, or the distance between transmitter and receiver, CSI acquisition has to be conducted repeatedly to keep track of CSI variations. Frequent CSI acquisition may entail a large overhead whereas infrequent CSI acquisition may result in a low CSI estimation quality. To cope with these issues, we design codes which facilitate maximum likelihood sequence detection at the receiver without instantaneous or statistical CSI. In particular, assuming concentration shift keying modulation, we show that a class of codes, referred to as strongly constant-weight (SCW) codes, enables optimal CSI-free sequence detection at the cost of decreasing the data rate. For the proposed SCW codes, we analyze the code rate and the error rate. Simulation results verify our analytical derivations and reveal that the proposed CSI-free detector for SCW codes outperforms the baseline coherent and non-coherent detectors for uncoded transmission.

Fr4-6: Quantum IT 5

Friday, June 30, 16:40-18:00
Room: K5
Chair: Masahito Hayashi (Nagoya University, Japan)

Pretty good measures in quantum information theory (16:40)

Raban Iten *(ETH Zurich, Switzerland); Joseph Renes (ETH Zurich, Switzerland); David Sutter (ETH Zurich, Switzerland)*

Quantum generalizations of Rényi's entropies are a useful tool to describe a variety of operational tasks in quantum information processing. Two families of such generalizations turn out to be particularly useful: the Petz quantum Rényi divergence $\bar{D}_\alpha(\rho||\sigma)$ and the minimal quantum Rényi divergence $\tilde{D}_\alpha(\rho||\sigma)$. In this paper, we prove a reverse Araki-Lieb-Thirring inequality that implies a new relation between these two families of divergences, namely that $\alpha\bar{D}_\alpha(\rho||\sigma) \leq \tilde{D}_\alpha(\rho||\sigma)$ for $\alpha \in [0,1]$ and where ρ and σ are density operators. This bound suggests defining a "pretty good fidelity", whose relation to the usual fidelity implies the known

relations between the optimal and pretty good measurement as well as the optimal and pretty good singlet fraction.

Linear Programming Bounds for Entanglement-Assisted Quantum Codes (17:00)

Ching-Yi Lai *(Academia Sinica, Taiwan); Alexei Ashikhmin (Nokia Bell Labs, USA)*

In this paper, we define two split weight enumerators for general quantum codes with entanglement assistance, including nonadditive codes. We show that they obey a MacWilliams identity, which allows us to prove algebraic linear programming bounds, such as the Singleton bound, the Hamming bound, and the first linear programming bound. On the other hand, we derive additional constraints on the size of Pauli subgroups for quantum codes, which helps to improve the linear programming bounds on the minimum distance of quantum codes of small length.

Estimating the Information Rate of a Channel with Classical Input and Output and a Quantum State (17:20)

Michael Cao *(The Chinese University of Hong Kong, Hong Kong); Pascal Vontobel (The Chinese University of Hong Kong, Hong Kong)*

We consider the problem of transmitting classical information over a time-invariant channel with memory. A popular class of time-invariant channels with memory are finite-state-machine channels, where a classical state evolves over time and governs the relationship between the classical input and the classical output of the channel. For such channels, various techniques have been developed for estimating and bounding the information rate. In this paper we consider a class of time-invariant channels where a quantum state evolves over time and governs the relationship between the classical input and the classical output of the channel. We propose algorithms for estimating and bounding the information rate of such channels. In particular, we discuss suitable graphical models for doing the relevant computations.

Fundamental limits of quantum-secure covert optical sensing (17:40)

Boulat Bash (Raytheon BBN Technologies, USA); Christos Gagatsos (University of Warwick, United Kingdom (Great Britain)); Animesh Datta (University of Warwick, United Kingdom (Great Britain)); Saikat Guha (Raytheon BBN Technologies, USA)

We present a square root law for active sensing of phase θ of a single pixel using optical probes that pass through a single-mode lossy thermal-noise bosonic channel. Specifically, we show that, when the sensor uses an n-mode covert optical probe, the mean squared error (MSE) of the resulting estimator $\hat{\theta}_n$ scales as $\langle(\theta-\hat{\theta}_n)^2\rangle = \mathcal{O}(1/\sqrt{n})$; improving the scaling necessarily leads to detection by the adversary with high probability. We fully characterize this limit and show that it is achievable using laser light illumination and a heterodyne receiver, even when the adversary captures every photon that does not return to the sensor and performs arbitrarily complex measurement as permitted by the laws of quantum mechanics.

Fr4-7: Source Coding 5

Friday, June 30, 16:40-18:00
Room: K6
Chair: Galen Reeves (Duke University, USA)

Source Coding with Distortion Profile Constraints (16:40)

Pierre Moulin (University of Illinois at Urbana-Champaign, USA)

In rate-distortion theory, three main types of distortion constraints have been popular: average, pointwise, and excess probability (*aka* ϵ-fidelity). A new setup is proposed here, which is suitable for fixed-length codes and constrains the distribution (profile) of distortions. This is accomplished by imposing multiple constraints on excess-distortion probabilities as well as an optional constraint on average distortion. We show that coding redundancy for compressing discrete memoryless sources is upper-bounded by $R_2/\sqrt{n} + \frac{\log n}{2n} + O(\frac{\log\log n}{n}) + \overline{R}_4 + o(1)$ where n is the block length, R_2 the second-order coding rate, and $\overline{R}_4$ a constant. For the special case of coding with a single ϵ-fidelity constraint, $R_2 = \sqrt{V}\,\mathcal{Q}^{-1}(\epsilon)$ where V is the source rate-dispersion function, and $\mathcal{Q}$ is the tail probability of a normal random variable. The upper bound is proved using a random coding scheme and deriving exact asymptotics for the probability of distortion balls with input type dependent radius.

Lower Bounds on Rate of Fixed-Length Source Codes under Average- and ϵ-Fidelity Constraints (17:00)

Pierre Moulin (University of Illinois at Urbana-Champaign, USA)

This paper studies lossy coding of discrete memoryless sources and derives new asymptotic lower bounds on the rate of optimal fixed-length codes. Both average and excess-probability distortion constraints are studied. We show that in each case the rate of optimal codes is lower bounded by $R(D) + R_2/\sqrt{n} + (\log n)/(2n) + \underline{R}_4/n + o(1)$ where n is the block length, $R(D)$ is Shannon's rate-distortion function, R_2 is the second-order coding rate, and $\underline{R}_4$ a constant that is explicitly identified.

Enhanced MDL with Application to Atypicality (17:20)

Elyas Sabeti (University of Hawaii, USA); Anders Høst-Madsen (University of Hawaii, USA)

With the enormous amount of data generated through the internet and sensors, Internet of Things, it becomes too overwhelming for humans to examine it all. One solution is to reduce the data to a set of statistics. The perspective in this paper is the opposite, namely that most of this data is just background noise, and the interesting parts are those that deviate from background noise, the parts that are atypical. In order to find such ”interesting” parts of data, universal approaches are required, since it is not known in advance what we are looking for. Our approach is to use Rissanen’s minimum description length (MDL) as a tool for that. We would like to be able to find both short and long atypical sequences of data, and we therefore need accurate expressions of MDL, without prior assumptions. In this paper we develop a modified predictive MDL method that works better for short sequences.

Distributed Coding of Multispectral Images (17:40)

Maxim Goukhshtein (University of Toronto, Canada); Petros Boufounos (Mitsubishi Electric Research Laboratories & Rice University, USA); Toshiaki Koike-Akino (Mitsubishi Electric Research Laboratories (MERL), USA); Stark Draper (University of Toronto, Canada)

The acquisition and compression of multispectal images is often performed in an environment where resources such as computational power and memory are scarce. To that end, we propose a new extremely low-complexity encoding approach for compression of multispectral images, that shifts the complexity to the decoding. Our method combines principles from compressed sensing and distributed source coding. Specifically, the encoder compressively measures blocks of the band of interest and uses syndrome coding to encode the bitplanes of the measurements. The decoder has access to side information, which is used to predict the bitplanes and to decode them. The side information is also used to guide the reconstruction of the image from the decoded measurements. Our experimental results demonstrate significant improvement in the rate-distortion trade-off when compared to similar low-complexity coding schemes.

List of Authors

A

B

C

D

E

F

G

H

I

L

M

P

Q

R

S

U

V

W

Z