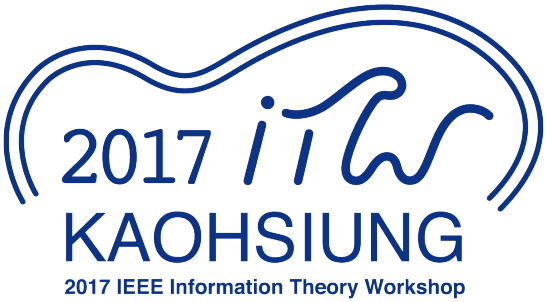
Book of Abstracts

2017 IEEE Information Theory Workshop



Kaohsiung, Taiwan
November 6–10, 2017


IEEE INFORMATION THEORY SOCIETY

A Word from the General Co-Chairs

Welcome to the 2017 IEEE Information Theory Workshop (ITW) at Kaohsiung Exhibition Center, Kaohsiung. It is our great pleasure to host the ITW in Taiwan's second largest city.

In order to increase student attendance from the local and international academic communities, this ITW experiments with a 3-day Information Theory Society Student Special registration rate. We hope that the idea will attract more students to the topics of coding and information theory. A recent results poster session will be held on Tuesday morning, in addition to the traditional 20 minute talk sessions. Key local industries on coding for memories are invited to present their newest developments at a specially arranged Wednesday invited session. We hope that this event will establish a dialog between principle and practice.

We very much appreciate the great efforts of our Technical Program Chairs Hsiao-feng Francis Lu (NCTU, Taiwan), Stefan M. Moser (ETHZ, Switzerland) and Chih-Chun Wang (Purdue Univ., USA). They invited the keynote speakers and reviewed many poster submissions, all the while handling 146 regular submissions from 24 countries with the assistance of an outstanding technical program committee.

We wish to especially thank the five invited session organizers: Lara Dolecek (UCLA, USA) organized the session on IT and Coding for Memories; Andrew Eckford (York Univ., Canada) organized the session on IT and Biology; Min-Hsiu Hsieh (UTS, Australia) organized the sesion on IT and Quantum Communications; Mohammad Ali Maddah-Ali (Bell Labs, USA) organized the session on IT for Content Distribution; and Yeong-Luh Ueng (NTHU, Taiwan) organized the session on IT and Coding for Memories which has speakers from local industries.

Finally, we would like to express our deep gratitude to our dedicated Organizing Committee, in particular Stefano Rini (NCTU, Taiwan) for initiating the idea of bringing ITW to Taiwan, Yao-Win Peter Hong (NTHU, Taiwan) for his great web maintenance, and the three local arrangements committee members, Celeste Lee (NSYSU, Taiwan), Fan-Shuo Tseng (NSYSU, Taiwan), and Chao-Kai Wen (NSYSU, Taiwan), for taking care of the local organization in an impeccable manner. Without their enthusiasm and hard work, this workshop would not have been possible.

We hope that you will have an unforgettable experience visiting and enjoying the many attractions in Kaohsiung. Please do let us know if there is anything we can do to make your stay a memorable one.

General co-Chairs

Po-Ning Chen
National Chiao Tung University (NCTU), Taiwan

Gerhard Kramer
Technische Universität Müchen (TUM), Germany

Chih-Peng Li
National Sun Yat-Sen University (NSYSU), Taiwan

Welcome from the Technical Program Committee Chairs

On behalf of the Technical Program Committee (TPC), it is our greatest pleasure to welcome all of you to the *2017 IEEE Information Theory Workshop (ITW)* at the Kaohsiung Exhibition Center, Kaohsiung, Taiwan.

This year we have put up four main themes for the ITW: *IT for Content Distribution*, *IT and Coding for Memories*, *IT and Biology*, and *IT and Quantum Communications*. We believe these are topics of growing significance and strong impact for the future of information and coding theory. We are particularly in debt to the plenary speakers, Professor Michael C. Gastpar, Professor Shu Lin, Professor Ilya Shmulevich, and Professor Mark Wilde, for giving plenary talks on these main themes.

In addition, this year's ITW has five invited paper sessions and a recent-result poster session that aim to further support and complement these four overarching themes. The invited paper sessions, comprising 22 papers in total, have been organized by the invited session organizers, Professor Lara Dolecek, Professor Andrew Eckford, Dr. Mohammad Ali Maddah-Ali, Professor Min-Hsiu Hsieh, and Professor Yeong-Luh Ueng. We are extremely thankful to them for their help.

For the regular oral papers, this year we received a total of 146 submissions from 24 countries, covering a broad range of important and timely topics related to information and coding theory. Due to the time and space constraints of our conference, we had to make a selection and, after extensive and careful paper-reviewing, 103 papers were selected and grouped into 21 regular sessions for presentation, distributed over five days. We could not be more grateful to all 46 TPC members during the review process, who dedicated their precious time and efforts to evaluate all the submissions in a professional and constructive way.

We would also like to express our gratitude to all the paper authors for submitting their excellent works to the ITW and for sharing their ideas and contributions with our society. Finally, we thank all Organizing Committee Members of the 2017 ITW for their tremendous support.

Technical Program co-Chairs

Hsiao-feng Francis Lu
National Chiao Tung University (NCTU), Taiwan

Stefan M. Moser
Eidgenössische Technische Hochschule Zürich (ETHZ), Switzerland

Chih-Chun Wang
Purdue University, USA

Monday, November 6 10:30–17:30

MA1: **Content Distribution (Invited)**

Mohammad Ali Maddah-Ali Room 304A

10:30

Novel Decentralized Coded Caching through Coded Prefetching

Yi-Peng Wei and Sennur Ulukus (University of Maryland, USA)

We propose a new decentralized coded caching scheme for a two-phase caching network. This is a coded prefetching scheme for decentralized caching networks. The new scheme is based on maximal distance separable (MDS) codes. By utilizing the reconstruction property of MDS codes, the proposed scheme reduces the transmission of the messages beneficial only to very few users resulting in a better rate memory trade-off. Unlike previous coded prefetching schemes for centralized setting, the proposed scheme does not require the constraint of more users than files. The proposed scheme can be viewed as a generalization of the original uncoded prefetching decentralized coded caching scheme, and therefore can also be applied to different network topologies.

10:50

Communication-Optimal Coding Designs for Caching Networks

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

In this servery paper, we review three recent main results on cache networks, which not only considerably sharpen the approximate characterization of the rate-memory trade off, but also extend those results to more general networks. In these systems, a server with a database of some files (e.g. movies) is connected to multiple users via a communication network. Each user has an isolated memory of limited size that can be used for caching. The system operates in two phases: a *placement phase* where users each store a portion of the files in their local cache, and a *delivery phase*, where the users each request a file and the server delivers coded messages to the users, fulfilling their file requests. We start by considering the shared bottleneck network in two flavors of the system, with uncoded prefetching and with coded prefetching. First, for uncoded prefetching, an optimal design is proposed, under both centralized and decentralized settings, for both peak rate and average rate. The exact optimality is proven through a matching converse. Second, for caching with coded prefetching, we present a design that is optimal within a factor of approximately 2, which strictly improves the state of the art. Lastly, we move the focus to more general network topologies, and present an order-wise optimal scheme that is independent of the underlying communication network between the server and the users. This scheme is shown to achieve the minimum delivery delay with a constant factor for all memoryless networks.

11:10

Coded Caching for Wiretap Broadcast Channels

Sarah Kamel and Michele A Wigger (Telecom ParisTech, France); Mireille Sarkiss (CEA LIST, France)

The paper studies the wiretap erasure broadcast channel (BC) with an external eavesdropper when the legitimate receivers have cache memories. Various secure coding schemes are proposed for a scenario where K_w weak receivers have same erasure probabilities and K_s strong receivers have same erasure probabilities. The coding schemes achieve the cache-aided secrecy capacity when only weak receivers have cache memories and this cache memory is either small or large. Furthermore, the schemes allow to conclude that under a total cache budget it is often beneficial to assign the cache memories unequally across the strong and the weak receivers; that joint cache-channel coding is necessary; and that generally the secrecy capacity is positive even when the eavesdropper is stronger than the legitimate receivers.

11:30

Fundamental Limits of Latency in a Cache-Aided 4x4 Interference Channel

Joan Pujol Roig (Imperial College of London, United Kingdom (Great Britain)); Abolfazl Motahari (Sharif University of Technology, Iran); Filippo Tosato (Toshiba Research Europe, United Kingdom (Great Britain)); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain))

Fundamental limits of communication is studied in a 4×4 interference network, in which the transmitters are equipped with cache memories. Each of the receivers requests one file from a library of N equal-size files. The caches at the transmitters are filled without the knowledge of the user demands, such that all possible demand combinations can be satisfied reliably over the interference channel. The achievable *normalized delivery time* (NDT) is studied under *centralized* cache placement. By combining the interference alignment (IA) and zero-forcing (ZF) techniques, a novel caching and transmission scheme is presented, and is shown to be optimal for all possible cache sizes; fully characterizing the NDT for the 4×4 interference network with caches at the transmitter side.

11:50

On the Min-Max-Delay Problem: NP-completeness, Algorithm, and Integrality Gap

Qingyu Liu (Virginia Tech, USA); Lei Deng (The Chinese University of Hong Kong, Hong Kong); Haibo Zeng (Virginia Tech, USA); Minghua Chen (The Chinese University of Hong Kong, P.R. China)

We study a delay-sensitive information flow problem where a source streams information to a sink over a directed graph $G = (V, E)$ at a fixed rate R possibly using multiple paths to minimize the maximum end-to-end delay, denoted as the Min-Max-Delay problem. Transmission over an edge incurs a constant delay within the capacity. We prove that Min-Max-Delay is weakly NP-complete, and demonstrate that it becomes strongly NP-complete if we require integer flow solution. We propose an optimal pseudo-polynomial time algorithm for Min-Max-Delay, with time complexity $O(\log(Nd_{\max})(N^5 d_{\max}^{2.5})(\log R + N^2 d_{\max} \log(N^2 d_{\max})))$, where $N = \max\{|V|, |E|\}$ and $d_{\max}$ is the maximum edge delay. Besides, we show that the integrality gap, which is defined as the ratio of the maximum delay of an optimal integer flow to the maximum delay of an optimal fractional flow, could be arbitrarily large.

MB1: Codes for Distributed Storage

Pascal Vontobel — Room 304B

10:30

On One Generalization of LRC Codes with Availability

Stanislav Kruglik (Moscow Institute of Physics and Technology & Skolkovo Institute of Science and Technology, Russia); Marina Dudina (Skolkovo Institute of Science and Technology, Russia); Valeriya Potapova and Alexey A. Frolov (Skolkovo Institute of Science and Technology & IITP RAS, Russia)

We investigate one possible generalization of locally recoverable codes (LRC) with all-symbol locality and availability when recovering sets can intersect in a small number of coordinates. This feature allows us to increase the achievable code rate and still meet load balancing requirements. In this paper we derive an upper bound for the rate of such codes and give explicit constructions of codes with such property. These constructions utilize LRC codes developed by Wang et al.

10:50

On the Weight Hierarchy of Locally Repairable Codes

Jie Hao, Shutao Xia and Bin Chen (Tsinghua University, P.R. China); Fang-Wei Fu (Nankai University, P.R. China)

An (n, k, r) *locally repairable code* (LRC) is an $[n, k, d]$ linear code where every code symbol can be repaired from at most r other code symbols. An LRC is said to be optimal if the minimum distance attains the Singleton-like bound $d \leq n - k - \lceil k/r \rceil + 2$. The *generalized Hamming weights* (GHWs) of linear codes are fundamental parameters which have many useful applications. Generally it is difficult to determine the GHWs of linear codes. In this paper, we study the GHWs of LRCs. Firstly, we obtain a generalized Singleton-like bound on the i-th $(1 \leq i \leq k)$ GHWs of general (n, k, r) LRCs. Then, it is shown that for an optimal (n, k, r) LRC with $r \mid k$, its weight hierarchy can be completely determined, and the i-th GHW of an optimal (n, k, r) LRC with $r \mid k$ attains the proposed generalized Singleton-like bound for all $1 \leq i \leq k$. For an optimal (n, k, r) LRC with $r \nmid k$, we give lower bounds on the GHWs of the LRC and its dual code. Finally, two general bounds on linear codes in terms of the GHWs are presented.

11:10

Maximally Recoverable Codes: Connections to Generic Network Coding and Maximal Matching

Chi Wan Sung (City University of Hong Kong, Hong Kong); Kenneth W. Shum (Institute of Network Coding, Hong Kong); Quan Yu (Wuhan University of Technology); Guangping Xu (Tianjin University of Technology, P.R. China)

The instantiation of a maximally recoverable (MR) code is shown to be a special case of generic network coding. The defining condition of MR codes, called potential independence, is shown to be equivalent to maximal matching in bipartite graphs. Algorithms for MR instantiation are proposed and upper bounds of the required field size are derived.

11:30

Product Matrix Minimum Storage Regenerating Codes with Flexible Number of Helpers

Kaveh Mahdaviani (University of Toronto, Canada); Soheil Mohajer (University of Minnesota, USA); Ashish Khisti (University of Toronto, Canada)

In coding for distributed storage systems, efficient data reconstruction and repair through accessing a predefined number of arbitrarily chosen storage nodes is guaranteed by regenerating codes. Traditionally, code parameters, specially the number of helper nodes participating in a repair process, are predetermined. However, depending on the state of the system and network traffic, it is desirable to adapt such parameters accordingly in order to minimize the cost of repair. In this work a class of regenerating codes with minimum storage is introduced that can simultaneously operate at the optimal repair bandwidth, for a wide range of exact repair mechanisms, based on different number of helper nodes.

11:50

The Storage vs Repair Bandwidth Trade-off for Multiple Failures in Clustered Storage Networks

Vitaly Abdrashitov (Massachusetts Institute of Technology, USA); N. Prakash and Muriel Médard (MIT, USA)

We study the trade-off between storage overhead and inter-cluster repair bandwidth in clustered storage systems, while recovering from multiple node failures within a cluster. A cluster is a collection of m nodes, and there are n clusters. For data collection, we download the entire content from any k clusters. For repair of $t \geq 2$ nodes within a cluster, we take help from ℓ local nodes, as well as d helper clusters. We characterize the optimal trade-off under functional repair, and also under exact repair for the minimum storage and minimum inter-cluster bandwidth (MBR) operating points. Our bounds show the following interesting facts: $1)$ When $t|(m-\ell)$ the trade-off is the same as that under $t = 1$, and thus there is no advantage in jointly repairing multiple nodes, $2)$ When $t \nmid (m - \ell)$, the optimal file-size at the MBR point under exact re-

pair can be strictly less than that under functional repair. 3) Unlike the case of $t = 1$, increasing the number of local helper nodes does not necessarily increase the system capacity under functional repair.

MA2: **Content Distribution**

Chi Wan Sung Room 304A

13:40

Fractional Repetition Codes Based on Partially Ordered Sets

Harout Aydinyan and Holger Boche (Technical University Munich, Germany)

Fractional repetition (FR) codes is a class of codes which were recently introduced for distributed storage systems. These codes are intended for exact uncoded repair of node failures, by downloading symbols from a suitable subset of surviving nodes. The repair procedure in FR codes is table based, unlike the regenerating codes, where the repair of a failed node is possible using arbitrary subset of a given size from surviving nodes. The advantage of this relaxation is that it allows to achieve low complexity in repair process, while these codes have minimum repair bandwidth like minimum bandwidth regenerating (MBR) codes. In this paper we give new and simple constructions for universally good FR codes based on partially ordered sets. These codes allow for efficient uncoded repair and the resulting designs are scalable and easy to implement. In particular, they allow to store larger files as compared to MBR codes. Furthermore, the constructions can be extended to FR codes for heterogeneous storage systems.

14:00

On the Duality of Fractional Repetition Codes

Bing Zhu (Peking University, P.R. China); Kenneth W. Shum (Institute of Network Coding, Hong Kong); Hui Li (Peking University, P.R. China)

Erasure codes have emerged as an efficient technology for providing data redundancy in distributed storage systems. However, it is a challenging task to repair the failed storage nodes in erasure-coded storage systems, which requires large quantities of network resources. In this paper, we study fractional repetition (FR) codes, which enable the minimal repair complexity and also minimum repair bandwidth during node repair. We focus on the duality of FR codes, and investigate the relationship between the supported file size of an FR code and its dual code. Furthermore, we present a dual bound on the supported file size of FR codes.

14:20

Caching with Partial Matching under Zipf Demands

Jad Hachem (University of California, Los Angeles, USA); Nikhil Karamchandani and Sharayu Moharir (Indian Institute of Technology Bombay, India); Suhas Diggavi (University of California Los Angeles, USA)

We study the caching problem when we are allowed to match each user to one of a subset of caches after its request is revealed. We focus on non-uniformly popular content, specifically when the file popularities obey a Zipf distribution. We study two extremal schemes, one focusing on coded server transmissions while ignoring matching capabilities, and the other focusing on adaptive matching while ignoring potential coding opportunities. We derive the rates achieved by these schemes and characterize the regimes in which one outperforms the other. We also compare them to information-theoretic outer bounds, and finally propose a hybrid scheme that generalizes ideas from the two schemes and performs at least as well as either of them in most regimes.

14:40

An Improved Secretive Coded Caching Scheme exploiting Common Demands

Hari Hara Suthan Chittoor; Ishani Chugh and Prasad Krishnan (International Institute of Information Technology Hyderabad, India)

Coded caching schemes on broadcast networks with user caches help to offload traffic from peak times to off-peak times by prefetching information from the server to the users during off-peak times and thus serving the users more efficiently dur-

ing peak times using coded transmissions. We consider the problem of secretive coded caching which was proposed recently, in which a user should not be able to decode any information about any file that the user has not demanded. We propose a new secretive coded caching scheme which has a lower average rate compared to the existing state-of-the-art scheme, for the same memory available at the users. The proposed scheme is based on exploiting the presence of common demands between multiple users.

15:00

Linear Symmetric Private Information Retrieval for MDS Coded Distributed Storage with Colluding Servers

Qiwen Wang and Mikael Skoglund (KTH Royal Institute of Technology, Sweden)

The problem of *symmetric private information retrieval (SPIR)* from a coded database which is distributively stored among colluding servers is studied. Specifically, the database comprises K files, which are stored among N servers using an (N, M)-MDS storage code. A user wants to retrieve one file from the database by communicating with the N servers, without revealing the identity of the desired file to any server. Furthermore, the user shall learn nothing about the other $K-1$ files in the database. In the T-colluding SPIR problem (hence called TSPIR), any T out of N servers may collude, that is, they may communicate their interactions with the user to guess the identity of the requested file. We show that for linear schemes, the information-theoretic capacity of the MDS-TSPIR problem, defined as the maximum number of information bits of the desired file retrieved per downloaded bit, equals $1-\frac{M+T-1}{N}$, if the servers share common randomness (unavailable at the user) with amount at least $\frac{M+T-1}{N-M-T+1}$ times the file size. Otherwise, the capacity equals zero.

MB2: **Shannon Theory**

Abdellatif Zaidi Room 304B

13:40

A Tight Upper Bound on the Second-Order Coding Rate of Parallel Gaussian Channels with Feedback

Silas L. Fong and Vincent Y. F. Tan (National University of Singapore, Singapore)

This paper investigates the asymptotic expansion of the maximum coding rate of a parallel Gaussian channel with feedback under the following setting: A peak power constraint is imposed on every transmitted codeword, and the average error probabilities of decoding the transmitted message are non-vanishing as the blocklength increases. The main contribution of this paper is proving an upper bound on the first- and second-order asymptotics. Combined with existing achievability results, our result implies that the presence of feedback does not improve the first- and second-order asymptotics.

14:00

A Converse Bound on Wyner-Ahlswede-Körner Network via Gray-Wyner Network

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

We show a reduction method to construct a code for the Gray-Wyner (GW) network from a given code for the Wyner-Ahlswede-Korner (WAK) network. By combining this reduction with a converse bound on the GW network, we derive a converse bound on the WAK network. The derived bound gives an alternative proof of the strong converse theorem for the WAK network.

14:20

Asymptotic High-SNR Capacity of MISO Optical Intensity Channels

Stefan M. Moser (ETH Zurich, Switzerland & National Chiao Tung University (NCTU), Taiwan); Ligong Wang (ETIS & CNRS, France); Michele A Wigger (Telecom ParisTech, France)

This paper derives the asymptotic capacity for the multiple-input single-output free-space optical intensity channel in the regime of high signal-to-noise ratio (SNR). The asymptotic result is proven via upper and lower bounds on capacity at finite SNR.

14:40

On the Capacity of the Slotted Strongly Asynchronous Channel with a Bursty User

Sara Shahi, Daniela Tuninetti and Natasha Devroye (University of Illinois at Chicago, USA)

The slotted strongly asynchronous channel with a bursty user consists of a window of $A_n = e^{n\alpha}$ blocks of length n channel uses. A user transmits a randomly selected message among $M_n = e^{nR}$ different ones in exactly $K_n = e^{n\nu}$ randomly selected but distinct blocks in the window. The receiver must locate and decode, with vanishing error probability in n, each one of the transmitted messages. Capacity region (R, α, ν) is derived.

15:00

Two-letter Capacity Formula for Channels with Memory and Feedback

Christos K Kourtellaris, Charalambos D Charalambous and Ioannis Tzortzis (University of Cyprus, Cyprus)

For a class of channels with unit memory on previous channels outputs, we identify necessary and sufficient conditions, to test whether the capacity achieving channel input distributions with feedback are time-invariant, and whether feedback capacity is characterized by a two-letter expression, similar to that of memoryless channels. The method is based on showing that a certain dynamic programming equation, which in general, is a nested optimization problem over the sequence of channel input distributions, reduces to a non-nested optimization problem. We then apply these conditions to derive a two-letter expression for the feedback capacity of the Binary State Symmetric Channel and to evaluate explicitly the capacity and the capacity achieving input distribution. Further we derive computationally efficient upper bounds on the probability of error and evaluate the performance in the finite-blocklength regime.

MA3: Coding Theory & Practice I

Kenneth W. Shum — Room 304B

15:50

Multi-Kernel Polar Codes: Proof of Polarization and Error Exponents

Meryem Benammar (ISAE-Supaero, France); Valerio Bioglio (France Research Center, Huawei Technologies Co. Ltd., Italy); Frederic Gabry (Huawei Technologies, France Research Center, France); Ingmar Land (Huawei Technologies, French Research Centre, France)

In this paper, we investigate a novel family of polar codes based on multi-kernel constructions, proving that this construction actually polarizes. To this end, we derive a new and more general proof of polarization, which gives sufficient conditions for kernels to polarize. Finally, we derive the convergence rate of the multi-kernel construction and relate it to the convergence rate of each of the constituent kernels.

16:10

Robust Decoding Schemes for Polar Coding over Compound Channels

Mine Alsan and Vincent Y. F. Tan (National University of Singapore, Singapore)

We consider the problem of designing robust and low complexity decoding schemes for polar coding over a given finite class of channels. We propose two schemes based on multiple runs of the polar successive cancellation decoder, where at each run a different metric adapted to a channel

in the class is used in the decoder's decision procedure. The first scheme is a modified polar coding scheme which accommodates Cyclic Redundancy Check bits to help the decoder eliminate the estimates that do not pass the test. We show that this scheme achieves the symmetric capacity of the transmission channel with a vanishing rate loss of $O(1/\sqrt{N})$, where N is the length of the code. The second scheme introduces a polar decoding algorithm which implements a generalized likelihood ratio test. We show that over classes of channels which satisfy certain mild channel conditions, this scheme achieves the symmetric capacity of the transmission channel. The analysis also reveals that, in terms of error exponents, both schemes perform asymptotically in the blocklength as well as the polar successive cancellation decoder operating with the law of the true channel. Finally, we compare the schemes in terms of their performances and complexity, and discuss the extension to infinite class of channels.

16:30

Low-Rate Regular Concatenated Zigzag Codes are Capacity-Approaching over the BEC

Liu Hai Yang (Chinese academy of Science, P.R. China); Li Ping (City University of Hong Kong, Hong Kong)

Concatenated zigzag (CZ) codes have been widely studied for practical applications due to their low encoding complexity and excellent performance. However, there still lacks rigorous analysis and optimization techniques for CZ codes. This paper presents an analysis technique for CZ codes under belief propagation (BP) decoding over the binary erasure channel (BEC). We derive a pair of closed-form density evolution (DE) equations to characterize the asymptotic behavior of a CZ code under BP decoding. We show that capacity-approaching CZ codes can be designed by matching the curves corresponding to the DE equations. We also prove that the gap between the BP threshold of a regular CZ code and the corresponding Shannon threshold diminishes when the rate approaches zero. This suggests that regular CZ codes are good candidates for low-rate communication systems, where good low-density parity-check codes are difficult to construct.

16:50

Codes for Erasures over Directed Graphs

Lev Yohananov and Eitan Yaakobi (Technion, Israel)

In this work we continue the study of a new class of codes, called codes over graphs. Here we consider storage systems where the information is stored on the edges of a complete directed graph with n nodes. The failure model we consider is of node failures which are erasures of all edges, both incoming and outgoing, connected to the failed node. It is said that a code over graphs is a ρ-node-erasure-correcting code if it can correct the failure of any ρ nodes in the graphs of the code. While the construction of such optimal codes is an easy task if the field size is $O(n^2)$, our main goal in the paper is the construction of codes over smaller fields. In particular, our main result is the construction of optimal binary codes over graphs which correct two node failures with a prime number of nodes.

17:10

A User-Independent Serial Interference Cancellation Based Coding Scheme for the Unsourced Random Access Gaussian Channel

Avinash Vem, Krishna Narayanan and Jean-Francois Chamberland (Texas A&M University, USA); Jun Cheng (Doshisha University, Japan)

We propose a novel coding scheme for the unsourced multiple access channel model introduced by Polyanskiy. This new paradigm is composed of four main ingredients: (i) the transmission period is partitioned into sub-blocks, thereby instituting a slotted framework; (ii) The message (data) is split into two parts and one part chooses an interleaver for a low density parity check (LDPC) type code. This part of the message is encoded using spreading sequences or codewords that are designed to be decoded by a compressed sensing type decoder; (iii) The other part of the message is encoded using a low density parity check (LDPC) type code and decoded using a joint message passing decoding algorithm designed for the T-user binary input real adder channel; (iv) users repeat their codeword in multiple sub-blocks, with the

transmission pattern being a deterministic function of message content and independent of the identity of the user. When this coding scheme is combined with successive interference cancellation, the ensuing communication infrastructure can offer significant performance improvements compared to the coding scheme recently proposed by Ordentlich and Polyanskiy and results in the best performing coding scheme to date.

MB3: Graph-based Codes & Iterative Decoding

Eirik Rosnes Room 304B

15:50

Improved Sliding Window Decoding of Spatially Coupled Low-Density Parity-Check Codes

Shiyuan Mo and Li Chen (Sun Yat-sen University, P.R. China)

Spatially coupled low-density parity-check (SC-LDPC) codes can achieve capacity approaching performance with a small message recovery latency due to the sliding window decoding (SWD). Using a partial Tanner graph, the SWD performs iterative message passing until the average error probability $\overline{\mathcal{P}}_e$ of the target symbols falls below a threshold or the maximum iteration number is reached. However, $\overline{\mathcal{P}}_e$ does not decrease monotonically as iteration progresses. This implies the symbol likelihoods that were yielded when the decoding terminates may not be optimal for making decisions. Therefore, this paper proposes an improved SWD (ISWD) for SC-LDPC codes. The proposal monitors the achievable minimum of $\overline{\mathcal{P}}_e$ and stores its associated likelihoods, so that when the decoding terminates the target symbols will be estimated based on the stored likelihoods. Our research shows the ISWD is able to enhance the decoding performance, especially in the waterfall region. It exhibits an asymptotic convergence to the SWD performance. A complexity reducing variant of the ISWD is also proposed to facilitate the decoding but at the cost of error-correction performance.

16:10

Spatially-Coupled LDPC Codes for Two Dimensional Erasure Channel

Gou Hosoya and Hiroyuki Yashima (Tokyo University of Science, Japan)

In this study, we developed spatially coupled LDPC codes on the two-dimensional array erasure (2DAE) channel. We propose a method of generating new codes with the restriction on the check node constraint. We evaluate by density evolution analysis that the improvement of the threshold for the proposed two-dimensional SC-LDPC codes over the one-dimensional SC-LDPC codes. Moreover we verify that the BP threshold of the proposed codes can approach the corresponding MAP threshold of the original residual graph on the 2DAE channel.

16:30

Double-Edge Factor Graphs: Definition, Properties, and Examples

Michael Cao and Pascal Vontobel (The Chinese University of Hong Kong, Hong Kong)

Some of the most interesting quantities associated with a factor graph are its marginals and its partition sum. For factor graphs without cycles and moderate message-update complexities, the sum-product algorithm (SPA) can be used to efficiently compute these quantities exactly. Moreover, for various classes of factor graphs with cycles, the SPA has been successfully applied to efficiently compute good approximations to these quantities. Note that in the case of factor graphs with cycles, the local functions are usually non-negative real-valued functions.

In this paper we introduce a class of factor graphs, called double-edge factor graphs (DE-FGs), which allow local functions to be complex-valued and only require them, in some suitable sense, to be positive semi-definite kernel functions. We discuss various properties of the SPA when running it on DE-FGs and we show promising numerical results for various example DE-FGs, some of which have connections to quantum information processing.

16:50

Analysis of Practical LDPC Decoders in Tanner Graphs with Absorbing Sets

Marco Ferrari (CNR-IEIIT, Italy); Alessandro Tomasoni (CNR, Italy); Sandro Bellini (Politecnico di Milano, Italy)

Absorbing sets (ASs) cause the error floor phenomenon in many Low-Density Parity-Check (LDPC) codes. A recent, simplified system model for Min-Sum (MS) LDPC decoding [1] predicts that ASs exhibit a threshold behavior: if all variable nodes in an AS have channel messages above the threshold, the AS cannot trap the decoder. The threshold is a real-valued parameter that depends on the topology of the AS, and can be evaluated by a nonlinear optimization. In this paper we describe a simple, fast algorithm for evaluating the AS threshold. Additionally, we show that the algorithm is valid also for scaled-MS decoding. We show with an example that the threshold values under scaled-MS decoding are smaller than under MS decoding. Accordingly, scaling decreases the error floor.

17:10

Lowering the Error Floors of Low-Density Parity-Check Codes with Additional Check Nodes

Dongming Yuan; Lu Li and Yuanan Liu (Beijing University of Posts and Telecommunications, P.R. China)

This paper proposes a novel scheme for lowering the error floors of Low-Density Parity-Check (LDPC) Codes. Firstly, the most erroneous and the most reliable bits are located by searching the codeword bits. Subsequently, new check nodes are added to connect them, thus the negative effects of the most erroneous bits along with the corresponding trapping sets are avoided. Eventually, the BER performance is dramatically improved in the error-floor region according to the simulated results. This idea could be a more concise and simple alternative to weaken the effects of trapping sets in LDPC applications.

Tuesday, November 7
10:30–12:10.

URR: **Recent Results Poster Session**

Room 304A

10:30

Improvement of UEP Generalized LT Codes with Error-floor Reduction

Li-Jen Chang and Chung-Hsuan Wang (National Chiao-Tung University, Taiwan)

10:30

Prioritized Resource Reservation for Reducing Random Access Delay in 5G URLLC

Yu-Jia Chen, Li-Yu Cheng and Li-Chun Wang (National Chiao-Tung University, Taiwan)

10:30

Unitary Matrices Constructed from QAM Golay Complementary Pairs

Yu-Chun Chen and Ying Li (Yuan-Ze University, Taiwan)

10:30

A (21150, 19050) Two-Phase GC-LDPC Decoder Design for NAND Flash Applications

Chien Lin, Kin-Chu Ho and Hsie-Chia Chang (National Chiao-Tung University, Taiwan)

10:30

Polar Decoding of BCH Codes

Chien-Ying Lin, Yu-Chih Huang, Shin-Lin Shieh and Po-Ning Chen (National Chiao-Tung University, Taiwan)

10:30

On the Minimum Distance Criterion for Optimal Inter-constellation Rotation in URLLC Uplink NOMA Scenario

Chia-Hung Lin, Shin-Lin Shieh, Tzung-Cheng Chi and Po-Ning Chen (National Chiao-Tung University, Taiwan)

10:30

Dispersion of Dirty Paper Coding vs. Superposition Coding for Gaussian BC

Ayşe Ünsal and Jean-Marie Gorce (INSA Lyon, France)

10:30

Soft-Decision List Decoding of Reed-Solomon Codes using Modules

Jiongyue Xing, Li Chen and Martin Bossert (Sun Yat-sen Univ., China)

10:30

Refined Asymptotics for A Rate-Distortion Saddle-point Problem

Lin Zhou, Vincent Y. F. Tan and Mehul Motani (National Univ. of Singapore, Singapore)

Wednesday, November 8 09:00–17:30

WA1: **Codes for Memories (Invited)**

Yao-Win Peter Hong Room 304A

09:00

Weakly Constrained Codes via Row-by-Row Coding

Paul H. Siegel (University of California, San Diego, USA); Sarit Buzaglo (UCSD, USA)

A constrained code is a set of finite-length codewords that entirely avoid the occurrences of certain patterns. In some applications, it may be preferable to merely limit the number of occurrences of certain patterns in codewords rather than to completely forbid them. Constrained codes that involve such weaker constraints are called weakly constrained codes.
In this paper we construct capacity-achieving weakly constrained codes. The construction is based on a row-by-row coding scheme in which messages are encoded into the rows of a 2-dimensional array in which the frequency of occurrence of patterns along columns is controlled.

09:20

Optimal Compression of Element Pairs in Fixed-Width Memories

Ori Rottenstreich (Princeton University, USA); Yuval Cassuto (Technion, Israel)

Data compression is a well-studied (and well-solved) problem in the setup of long coding blocks. But important emerging applications need to compress data to memory words of small fixed widths. This new setup is the subject of this paper. In the problem we consider we have a source with a known discrete distribution, and we wish to find a code that maximizes the success probability that two source instances can be represented together in L bits or less. A good practical use for this problem is a table with two-element entries that is stored in a memory of a fixed width L. Such tables of very large sizes are used in data-intensive computing applications. We solve the problem by efficiently finding an optimal code that uses a dictionary of linear size in the number of source elements.

09:40

Codes Correcting Position Errors in Racetrack Memories

Yeow Meng Chee and 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 is structured like a tape 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 continue our recent study and 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 overshifted 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. We will show how to take advantage of this special feature of racetrack memories in order to construct codes correcting deletions and sticky insertions.

10:00

Context-Aware Resiliency: Unequal Message Protection for Random-Access Memories

Clayton Schoeny and Frederic Sala; Mark Gottscho, Irina Alam, Puneet Gupta and Lara Dolecek (University of California, Los Angeles, USA)

A common way to protect data stored in DRAM and related memory systems is through the use of a single-error-correcting/ double-error-detecting (SECDED) code. Traditionally, these error-correcting codes provide equal protection guarantees to all messages. In a recent work, we demonstrated enhanced error correction capabilities for SECDED codes by taking into account contextual side-information about the data. This paper is concerned with a closely related scenario: unequal message protection (UMP), where a subset of special messages is afforded additional error-correction ability. UMP is relevant to computing systems where certain messages are critical and failures cannot be tolerated. We study practical UMP constructions where messages are guaranteed either one or two bit-error-correction. We provide upper and lower bounds on the number of special messages. We introduce an explicit and practical code construction based on BCH subcodes and demonstrate the efficacy of our technique on data from the AxBench and SPEC CPU2006 benchmark suites.

WB1: **Communication Theory I**

Yanling Chen — Room 304B

09:00

Uplink Sum-Rate Analysis of C-RAN With Interconnected Radio Units

Seok-Hwan Park (Chonbuk National University, Korea); Osvaldo Simeone (King's College London, United Kingdom (Great Britain)); Shlomo (Shitz) Shamai (The Technion, Israel)

This study addresses the achievable sum-rate for the uplink of a cloud radio access network (C-RAN) operating in a linearWyner-type topology, i.e., with partial channel connectivity. In the system, the radio units (RUs) communicate with a central, or cloud, unit (CU) by means of digital finite-capacity fronthaul links. The messages sent by the user equipments (UEs) are jointly decoded by the CU based on the compressed baseband signals received on the fronthaul links. Unlike prior works, each RU is assumed to be also connected to its neighboring RUs via finitecapacity fronthaul links. Under the standard assumption that the RUs do not perform channel decoding (i.e., oblivious RUs), each RU performs in-network processing of the uplink received signal and of the compressed baseband signal received from the adjacent RU, with the CU carrying out channel decoding. A closedform expression of the achievable sum-rate is derived assuming point-to-point compression, and then analytical expressions are provided for more advanced fronthaul compression schemes that leverage side information. Numerical examples provide insights into the advantages of inter-RU communications and into the performance gap to existing sum-rate upper bounds.

09:20

Delay-aware Massive Random Access: Adaptive Framing and Successive Decoding

Qizhong Yao (Zhejiang University, P.R. China); Zhengchuan Chen (Chongqing University, P.R. China); Howard Yang and Tony Q. S. Quek (Singapore University of Technology and Design, Singapore)

In Internet of Things, wireless access networks need to support a large number of user equipments (UEs) in real time, where UEs frequently arrive and leave and plenty of packet collisions occur. In this paper, we propose a protocol termed adaptive framing with successive decoding (AFSD), that not only supports vast connectivity but also involves little signalling overhead. By using AFSD, the frame length can be adaptively adjusted based on the present UE number to deal with the fluidity of UEs, and successive decoding is adopted to recover the signal from the mixed received signal to alleviate the packet collision. We explicitly analyze the average delay of our protocol. Numerical results verify the accuracy of our analysis, as well as the effectiveness of the proposed protocol on handling massive access.

09:40

Wireless Information and Power Transfer over an AWGN channel: Nonlinearity and Asymmetric Gaussian Signaling

Morteza Varasteh; Borzoo Rassouli and Bruno Clerckx (Imperial College London, United Kingdom (Great Britain))

Simultaneous transmission of information and power over a point-to-point complex Additive White Gaussian Noise (AWGN) channel is studied. In contrast with the literature that relies on an inaccurate linear model of the energy harvester, an experimentally-validated nonlinear model is considered. A general form of the delivered Direct Current (DC) power in terms of system baseband parameters is derived, which demonstrates the dependency of the delivered DC power on higher order statistics of the channel input distribution. The optimization problem of maximizing Rate-Power (R-P) region is studied. Assuming that the Channel gain is known at both the receiver and the transmitter, and constraining to independent and identically distributed (i.i.d.) channel inputs determined only by their first and second moment statistics, an inner bound for the general problem is obtained. Notably, as a consequence of the harvester nonlinearity, the studied inner bound exhibits a tradeoff between the delivered power and the rate of received information. It is shown that the tradeoff-characterizing input distribution is with mean zero and with asymmetric power allocations to the real and imaginary dimensions.

10:00

Channel Capacity and Simple Correlators for Nonlinear Communication Channel at Large SNR and Small Dispersion

Aleksey Reznichenko and Ivan Terekhov (Budker Institute of Nuclear Physics & Novosibirsk State University, Russia)

We consider the optical fiber channel modelled by the nonlinear Schrodinger equation with additive white Gaussian noise. Using Feynman path-integral approach for the model with small dispersion we find the estimations for the first nonzero corrections to the conditional probability density function, to the optimal input signal distribution, and to the channel capacity at large signal-to-noise ratio. On the base of the factorization assumption of the conditional probability density function we demonstrate that the correction to the channel capacity in small dimensionless dispersion parameter is quadratic and positive therefore increasing the earlier calculated capacity for a nondispersive nonlinear optical fiber channel in the intermediate power regime. To illustrate our approach we also find the analytical expressions for simple correlators of the output signal in our noisy channel with small dispersion.

WA2: Codes for Memories (Industry, Invited)

Yeong-Luh Ueng — Room 304B

10:30

On Practical LDPC Code Construction for NAND Flash Applications

Shiuan-Hao Kuo, Zhen-U Liu and Jeff Yang (Silicon Motion, Inc., Taiwan)

As increasing storage density accompanies increasing adoption of 3D NAND flash, the data integrity turns to more important. The error floor problem is known to have critical impact on the correction capability of LDPC code in NAND flash storage. Herein we propose an analytical method based on a simplified NAND flash error model to relate harmful trapping sets to small cycles, by which we can avoid certain cycle combination during code construction for NAND flash memory applications.

10:50

Polar Codes for NAND-based SSD Systems: A Joint Source Channel Coding Perspective

Tingjun Xie; Ying Y. Tai and Jiangli Zhu (VIA Technologies, Inc., USA)

Polar codes [1] are a class of provably capacity achieving error correcting codes (ECC) for memory-less symmetric channels with low-complexity code structures; they have been shown to enjoy better decoding performance over low-density parity-check (LDPC) and Turbo codes under certain scenarios. In this work, we study

the application of polar codes for NAND based solid state drives (SSDs), and mainly focus on the joint source channel coding (JSCC) aspect of polar codes for flash data protection. In a practical SSD system, in addition to the host data, both flash translation layer (FTL) and host side will write on NAND a small amount of non-host data (a.k.a. metadata) for system managing purposes. We demonstrate that the metadata information can be readily and efficiently utilized by polar codes, whereas such property is lacking in LDPC-based systems. With the help of the side information provided by metadata, the decoding capability of polar codes can be further enhanced with little or no modifications on the decoder side. Simulation results verify the performance improvement of metadata-based JSCC scheme, and indicate that polar codes have competitive advantages over LDPC codes on flash memories.

11:10

3X Endurance Enhancement by Advanced Signal Processor for 3D NAND Flash Memory

Wei Lin; Yu-Cheng Hsu, Tsai-Hao Kuo, Yu-Siang Yang, Szu-Wei Chen, Chun-Wei Tsao, An-Chang Liu, Lih-Yuarn Ou, Tien-Ching Wang, Shao-Wei Yen, Yu-Hsiang Lin, Kuo-Hsin Lai, Chi-Heng Yang, Li-Chun Liang and Pei-Jung Hsu (Phison Electronics Corp., Taiwan)

In order to keep reducing the bit cost, NAND Flash memory vendors have changed the NAND Flash technology from 2D to 3D since 2014. Moreover, 3D NAND Flash is becoming the mainstream of the NAND Flash based storage system from 2017. Owing to the storage material of NAND Flash changing from heavy doped poly-silicon to silicon-nitride, the inter-cell interference is ignored during programming operation to increase the write performance on 3D NAND Flash memory. However, in order to reduce the aspect ratio of the memory hole, the thickness of the inter word-line dielectric is reduced with the increasing of the stacking number. Accordingly, the Vth distribution is widened by the interference between the electrons in the silicon-nitride and the conductive channel between memory cells. This paper provides the measurement results of the cell-to-cell interference with the mass-produced 3D NAND Flash memory and proposes a method to reduce the cell-to-cell interference on 3D NAND Flash. Furthermore, the error bit of the 3D NAND Flash memory is 15% reduced and the endurance is 3X increased by the proposed method.

11:30

LDPC Coded Modulation for TLC Flash Memory

Huang Chang Lee (Chang Gung University, Taiwan); Jieng-Heng Shy (National Tsing Hua University, Taiwan); Yen-Ming Chen (National Sun Yat-sen University); Yeong-Luh Ueng (National Tsing Hua University, Taiwan)

In this paper, a coded modulation scheme using extremely sparse low-density parity-check (LDPC) codes is proposed for the stored signal of triple-level-cell (TLC) NAND flash, where both the encoding and the decoding complexity can be significantly reduced with the advantage of the extremely sparse code graph. In order to enhance the performance of decoder, iterative detection decoding (IDD) is introduced to extract the extrinsic information from the symbol detector, and the cooperative non-Gray mapping is also designed. In addition, for error floor lowering, an interleaver is inserted to ensure the cascaded degree-2 variable nodes are separated to individual symbols. The simulation results show that the proposed coded modulation scheme can provide a practical error floor performance with a low decoding complexity.

WB2: **Quantum Information Theory & Communication**

Masahito Hayashi — Room 304B

10:30

Applications of Position-Based Coding to Classical Communication over Quantum Channels

Haoyu Qi and Qingle Wang (Louisiana State University, P.R. China); Mark M Wilde (Louisiana State University, USA)

We exploit a coding technique called position-based coding in the entanglement-assisted setting to establish lower bounds for one-shot capac-

ity, lower bounds on error exponents, and lower bounds on the second-order coding rate, and we also demonstrate that position-based coding can be a powerful tool for analyzing other communication settings. In particular, we reduce the quantum simultaneous decoding conjecture for entanglement assisted or unassisted communication over a quantum multiple access channel to open questions in multiple quantum hypothesis testing. We then determine an achievable rate region for entanglement-assisted or unassisted classical communication over a quantum multiple-access channel, when using a particular quantum simultaneous decoder. The achievable rate regions given in this latter case are generally suboptimal, involving differences of Renyi-2 entropies and conditional quantum entropies.

10:50

An Upper Bound on Quantum Capacity of Unital Quantum Channels

Anurag Anshu (National University of Singapore, Singapore)

We analyze the quantum capacity of a unital quantum channel, using ideas from the proof of near-optimality of Petz recovery map [Barnum and Knill 2000] and give an upper bound on the quantum capacity in terms of regularized output 2-norm of the channel. We also show that any code attempting to exceed this upper bound must incur large error in decoding, which can be viewed as a weaker version of the strong converse results for quantum capacity. As an application, we find nearly matching upper and lower bounds (up to an additive constant) on the quantum capacity of quantum expander channels. Using these techniques, we further conclude that the 'mixture of random unitaries' channels arising in the construction of quantum expanders in [Hastings 2007] show a trend in multiplicativity of output 2-norm similar to that exhibited in [Montanaro 2013] for output ∞-norm of random quantum channels.

11:10

Entanglement Assisted Binary Quantum Tensor Product Codes

Priya Nadkarni and Shayan Garani (Indian Institute of Science, Bangalore, India)

We propose the construction and error correction procedures of an entanglement assisted binary quantum tensor product code. We devise an efficient procedure to construct the code with complexity $\mathcal{O}(\max\{\rho_1^2, \rho_2^2\})$ compared to $\mathcal{O}(\rho_1^2\rho_2^2)$ using symplectic Gram-Schmidt orthogonalization, where ρ_1 and ρ_2 are the number of parity bits of the component codes. Our error correction procedures can correct quantum burst errors without destroying the quantum state.

WA3: Coding for Memories

Chung-Hsuan Wang — Room 304B

13:40

Union Bound Analysis of Multilevel Flash Memory Channels

Guanghui Song (Doshisha University, Japan); Kui Cai (Singapore University of Technology and Design, Singapore); Jun Cheng (Doshisha University, Japan)

A union bound and its asymptotic analysis are presented for the multilevel flash memory channels. The bound reveals an asymptotic decoding error behaviour under the maximum-likelihood decoding, based on which code design criteria are proposed for the multilevel flash memories.

14:00

High Performance Non-Binary Spatially-Coupled Codes for Flash Memories

Ahmed Hareedy, Homa Esfahanizadeh and Lara Dolecek (University of California, Los Angeles (UCLA)

Modern dense Flash memory devices operate at very low error rates, which require powerful error correcting coding (ECC) techniques. An emerging class of graph-based ECC techniques that has broad applications is the class of spatially-coupled (SC) codes, where a block code is partitioned into components that are then rewired multiple times to construct an SC code. Here, our focus is on SC codes with the underlying circulant-based structure. In this paper, we present a three-stage approach for the design of high performance non-binary SC (NB-SC) codes optimized for practical

Flash channels; we aim at minimizing the number of detrimental general absorbing sets of type two (GASTs) in the graph of the designed NB-SC code. In the first stage, we deploy a novel partitioning mechanism, called the optimal overlap partitioning, which acts on the protograph of the SC code to produce optimal partitioning corresponding to the smallest number of detrimental objects. In the second stage, we apply a new circulant power optimizer to further reduce the number of detrimental GASTs. In the third stage, we use the weight consistency matrix framework to manipulate edge weights to eliminate as many as possible of the GASTs that remain in the NB-SC code after the first two stages (that operate on the unlabeled graph of the code). Simulation results reveal that NB-SC codes designed using our approach outperform state-of-the-art NB-SC codes when used over Flash channels.

14:20

Order-Optimal Permutation Codes in the Generalized Cayley Metric

Siyi Yang and Clayton Schoeny and Lara Dolecek (University of California, Los Angeles, USA)

Permutation codes have recently garnered substantial research interest. In this paper, we study the permutation codes in the generalized Cayley metric. The generalized Cayley metric captures the number of generalized transposition errors in a permutation, and subsumes existing error types including transpositions and translocations without imposing restrictions on the lengths and positions of the translocated segments. Relying on the breakpoint analysis proposed by Chee and Vu, we construct a new class of permutation codes without interleaving. Our coding scheme, although it is non-constructive, has an order-optimal rate, and in certain circumstances, the rate is higher than that of existing codes based on interleaving.

14:40

Construction of Parallel RIO Codes using Coset Coding with Hamming Codes

Akira Yamawaki, Hiroshi Kamabe and Shan Lu (Gifu University, Japan)

Random input/output (RIO) code is a coding scheme that enables reading of one logical page using a single read threshold in multilevel flash memory. The construction of RIO codes is equivalent to the construction of WOM codes. Parallel RIO (P-RIO) code is a RIO code that encodes all pages in parallel. In this paper, we utilize coset coding with Hamming codes to construct P-RIO codes. Coset coding is a technique that constructs WOM codes using linear binary codes. We leverage the information on the data of all pages to encode each page. Our constructed codes store more pages than RIO codes constructed via coset coding.

15:00

LDPC Turbo Decoder using Generalized Belief Propagation over Two-Dimensional Inter-Symbol Interference Channel

Akiyoshi Hashimoto and Kenta Kasai (Tokyo Institute of Technology, Japan)

Error correction using LDPC codes over two-dimensional inter-symbol interference channel has been considered to be difficult because belief propagation(BP) does not work well. Hence a method that uses generalized belief propagation(GBP) for detection is proposed because GBP's approximation precision is better than BP's in general. However, the method's decoding algorithm is BP and the detector and the decoder are separated. Therefore, we tried to unify a detector and a decoder. And we discovered a problem of GBP detector for unification. Moreover, we found out a resolution of the problem. And we constructed unified GBP decoder and evaluated its error performance.

WB3: **Cryptography & Data Security**

Matthieu Bloch Room 304B

13:40

A Construction of the Progressive (3,n)-Threshold Visual Cryptography Using a BIBD and Analysis of its Optimality

Koutaro Okada and Hiroki Koga (University of Tsukuba, Japan)

We consider a certain class of (t,n)-threshold visual cryptography scheme called (t,n)-PVCS in which quality of the reproduced image that appears in the superimposition of more than t shares improves as the number of the superimposed shares increases. We first formulate a linear programming problem followed by an integer programming problem in order to maximize the relative difference of the n superimposed shares. Next, we propose a construction of a (3,n)-PVCS using the incident matrix of a BIBD and discuss conditions under which the obtained pair of basis matrices becomes optimal.

14:00

On the Minimum Worst-Case Cost and the Minimum Average Cost to Erase Information

Tetsunao Matsuta and Tomohiko Uyematsu (Tokyo Institute of Technology, Japan)

We normally hold a lot of confidential information in hard disk drives and solid-state drives. When we want to erase such information to prevent the leakage, we have to overwrite the sequence of information with a sequence of symbols that is independent of the information. The overwriting is needed only at places where overwritten symbols are different from original symbols. Then, the cost of overwrites such as the number of overwritten symbols to erase information is important. In this paper, we deal with the worst-case cost which is the cost to erase the most laborious sequence and the average cost which is the expectation of the cost with respect to sequences. We clarify the minimum worst-case cost such that the mutual information between the original sequence and the overwritten sequence normalized by the blocklength of the sequences goes to zero as the blocklength tends to infinity. We also clarify the minimum average cost for stationary memoryless sources in the finite blocklength regime.

14:20

Tighter Bounds on Entropy of Secret Keys in Authentication Codes

Junji Shikata (Yokohama National University, Japan)

The traditional theory of information-theoretically secure authentication codes (A-codes) developed by Simmons and others usually assumes that a uniformly random source for truly random keys is available. However, if we consider the scenario without the assumption, previously known bounds on key-entropy are not tight. In this paper, tighter lower bounds of A-codes with non-uniformly random secret keys are investigated and derived in terms of the Renyi entropy.

14:40

Secure Computation of Randomized Functions: Further Results

Deepesh Data and Vinod M Prabhakaran (Tata Institute of Fundamental Research, India)

We consider secure computation of randomized functions by two users, where both the users (Alice and Bob) have inputs, Alice sends a message to Bob over a rate-limited, noise-free link, and then Bob produces the output. We study this problem when privacy is required only against Bob, i.e., from the message, Bob must not learn any information about Alice's input other than what can be inferred by his own input and output. We give a single-letter expression for the optimal rate. We also explicitly characterize securely computable randomized functions when input has full support, which leads to a much simpler expression for the optimal rate. Recently, Data (ISIT 2016) studied the other two cases (first, when privacy is required against both the users; and second, when privacy is required only against Alice) and obtained single-letter expressions for optimal rates in both the scenarios. Yassaee, Gohari, and Aref (IEEE Transactions on Information Theory 2015) studied the case when there is no privacy requirement and

obtained a single-letter expression for the optimal rate, when Alice and Bob interact for arbitrary but finite number of rounds, and both of them may produce potentially different outputs.

15:00

On the Geometric Ergodicity of Gibbs Algorithm for Lattice Gaussian Sampling

Zheng Wang and Cong Ling (Imperial College London, United Kingdom (Great Britain))

Sampling from the lattice Gaussian distribution is emerging as an important problem in coding and cryptography. In this paper, the conventional Gibbs sampling algorithm is demonstrated to be geometrically ergodic in tackling with lattice Gaussian sampling, which means its induced Markov chain converges exponentially fast to the stationary distribution. Moreover, as the exponential convergence rate is dominated by the spectral radius of the forward operator of the Markov chain, a comprehensive analysis is given and we show that the convergence performance can be further enhanced by the usages of blocked sampling strategy and reasonable choice of selection probabilities.

WA4: Index Coding & Function Computation

Emanuele Viterbo — Room 304B

15:50

Real-Time Status Updates for Correlated Source

Sudheer Poojary and Sanidhay Bhambay and Parimal Parag (Indian Institute of Science, India)

For timely sensor update, the traditional approach is to send new information at every available opportunity. Recent research has shown that with limited receiver feedback, sensors can improve the update timeliness by transmitting differential information for slowly varying correlated sources. In general, correlated sources can elect to transmit actual or differential state information depending on the current state. This encoding scheme generalizes the actual and differential updates schemes. Using this generalized scheme, we quantify the timeliness gains for some example sources. Further, we show a stochastic ordering among the actual update, the differential update, and the generalized update schemes.

16:10

Communication vs Distributed Computation: an Alternative Trade-off Curve

Yahya H. Ezzeldin; Mohammed Karmoose and Christina Fragouli (University of California, Los Angeles, USA)

In this paper, we revisit the communication vs. distributed computing trade-off, studied within the framework of MapReduce in [1]. An implicit assumption in the aforementioned work is that each server performs all possible computations on all the files stored in its memory. Our starting observation is that, if servers can compute only the intermediate values they need, then storage constraints do not directly imply computation constraints. We examine how this affects the communication-computation trade-off and suggest that the trade-off be studied with a predetermined storage constraint. We then proceed to examine the case where servers need to perform computationally intensive tasks, and may not have sufficient time to perform all computations required by the scheme in [1]. Given a threshold that limits the computational load, we derive a lower bound on the associated communication load, and propose a heuristic scheme that achieves in some cases the lower bound.

16:30

Information Theoretic Converse Proofs for some PICOD Problems

Tang Liu and Daniela Tuninetti (University of Illinois at Chicago, USA)

This paper provides information theoretic converse proofs for some classes of Pliable Index CODing (PICOD) problems. PICOD is a variant of the index coding problem in which a user is satisfied whenever it can successfully decode any one message that is not in its side information set. Past work on PICOD provided a number of achievable schemes based on linear codes, some of which are known

to be optimal when the server is restricted to use linear codes only. This paper proves that for some of those cases linear codes are indeed optimal in an information theoretic sense, i.e., they cannot be beaten by non-linear codes. It also shows the information theoretic optimality for other classes of PICOD problems that were open.

16:50

The Benefit of Being Flexible in Distributed Computation

Linqi Song (University of California, Los Angeles, USA); Sundara Rajan Srinivasavaradhan (University of California at Los Angeles, USA); Christina Fragouli (UCLA, USA)

In wireless distributed computing, networked nodes perform intermediate computations over data placed in their memory and exchange these intermediate values to calculate function values. In this paper we consider an asymmetric setting where each node has access to a random subset of the data, i.e., we cannot control the data placement. The paper makes a simple point: we can realize significant benefits if we are allowed to be "flexible", and decide which of the nodes in our system computes which function. We make this argument in the case where each function depends on only two of the data messages, as is the case in similarity searches. We establish a percolation in the behavior of the system, where, depending on the amount of observed data, by being flexible, we may need no communication at all.

17:10

On the Capacity of Index Coding Problems with Symmetric Neighboring Interference

Mahesh Babu Vaddi and B. Sundar Rajan (Indian Institute of Science, India)

A single unicast index coding problem (SUICP) with symmetric neighboring interference (SNI) has equal number of K messages and K receivers, the kth receiver R_k wanting the kth message x_k and having the side-information $\mathcal{K}_k = (\mathcal{I}_k \cup x_k)^c$, where $I_k = \{x_{k-U}, \ldots, x_{k-2}, x_{k-1}\} \cup \{x_{k+1}, x_{k+2}, \ldots, x_{k+D}\}$ is the interference with D messages after and U messages before its desired message. Maleki, Cadambe and Jafar obtained the capacity of this symmetric neighboring interference single unicast index coding problem (SNI-SUICP) with (K) tending to infinity and Blasiak, Kleinberg and Lubetzky for the special case of $(D = U = 1)$ with K being finite. In this work, for any finite K and arbitrary D we obtain the capacity for the case $U = \text{gcd}(K, D + 1) - 1$. Our proof is constructive, i.e., we give an explicit construction of a linear index code achieving the capacity.

WB4: Physical Layer Security

Selma Belhadj Amor — Room 304B

15:50

Covert Communication over Broadcast Channels

Keerthi Suria Kumar Arumugam and Matthieu Bloch (Georgia Institute of Technology, USA)

We analyze a two-receiver binary-input discrete memoryless degraded channel, in which the transmitter communicates a common message simultaneously to both users and a covert message to only one of them while treating the other as an adversary. This model captures the problem of embedding covert messages in an innocuous transmission and generalizes previous models in which the innocent behavior corresponds to the absence of communication between legitimate users. We identify the exact asymptotic behavior of the number of covert bits that can be transmitted when the rate of the innocuous transmission is close to the capacity of the channel to the adversary. Our results also reveal the dependance of the number of covert bits on the channel parameters and the characteristics of the innocent codebook.

16:10

Error Exponent for Covert Communications over Discrete Memoryless Channels

Mehrdad Tahmasbi and Matthieu Bloch (Georgia Institute of Technology, USA); Vincent Y. F. Tan (National University of Singapore, Singapore)

We define and study the error exponent of covert communications over binary-input DMC. Our main result consists of upper and lower bounds for the exponent, which match in a regime that we explicitly characterize. While our proofs follow standard techniques, the vanishing rate regime inherent to covert communications and the low-weight of codewords introduces specific technical challenge. In particular, the lower bound of the error exponent follows from a non-standard constant-composition ensemble instead of an iid ensemble, and the upper bound requires a careful treatment of higher order terms that does not appear in the traditional treatment of error exponent.

16:30

Alphabet Size Reduction for Secure Network Coding

Xuan Guang and Raymond W. Yeung (The Chinese University of Hong Kong, Hong Kong)

We consider a communication network where there exist wiretappers who can access a subset of channels, called a *wiretap set*, which is chosen from a given collection of wiretap sets. The collection of wiretap sets can be arbitrary. Secure network coding is applied to prevent the source information from being leaked to the wiretappers. In secure network coding, the minimum required alphabet size is an open problem not only of theoretical interest but also of practical importance, because it is closely related to the implementation of such coding schemes in terms of computational complexity and storage requirement. In this paper, we develop a systematic graph-theoretic approach for improving Cai and Yeung's lower bound on the required alphabet size for the existence of secure network codes. The new lower bound thus obtained, which depends only on the network topology and the collection of wiretap sets, can be significantly smaller than Cai and Yeung's lower bound. A polynomial-time algorithm is devised for efficient computation of the new lower bound.

16:50

Privacy Through Familiarity

Wasim Huleihel and Muriel Médard (MIT, USA)

This paper considers the problem of transmitting digital data from a source reliably to a legitimate user, subjected to a wiretap at a receiver that employs a fixed decoding strategy. Specifically, we assume that the wiretapper views the same channel output as the legitimate user, but decodes the message using some fixed decoding strategy which might be mismatched with respect to the channel. This model aims to capture the natural situation in privacy where knowledge of the privacy mapping at the source can me modeled as channel statistics. In that case, all observers receive the same data, but have different levels of knowledge, or familiarity, regarding the observed user who uses a privacy mapping. We analyze two different security metrics; probability of error at the eavesdropper and semantic-security, and provide achievable rates under both criteria.

17:10

Revealing One Thing Without Revealing Another

Matthew P Johnson and Liang Zhao (City University of New York, USA); Supriyo Chakraborty (IBM T. J. Watson Research Lab, USA)

We study a lossy coding scenario, posed as an algorithmic optimization problem, where we trade off between the conflicting goals of accuracy and privacy, motivated by scenarios such as the public release of *estimates* of data that accurately reflect *some* aspects of the raw data without revealing other sensitive confidential aspects of it, or permitting it to be inferred. More precisely, given a discrete probability distribution $p(D, X, Y)$, where X represents the *whitelisted* inferences from D and Y represents the *blacklisted* inferences, we seek to construct a conditional distribution $p(M|D)$ with the dual goals of making $I(M;X)$ large and $I(M;Y)$ small. Chakraborty et al. 2013 [1]. provided optimal solutions within this model to the two extreme points on the two objectives' Pareto frontier: maximizing $I(M;X)$ subject to the constraint that $I(M;Y)$ be as small as possible ("perfect privacy", using linear programming (LP)) and vice versa ("perfect utility", which is trivial). In this paper we provide a faster *combinatorial* optimal algorithm for the perfect privacy problem, which does not require the use of an LP solver. Moreover, this algorithm any be used to compute Pareto-optimal solutions at *any* point on

the Pareto frontier. (En route to this algorithm, we also provide a mathematical programming-based solution.) This solves the primary open problem posed by [1].

Thursday, November 9 10:30–17:30

TA1: **Information Theory & Biology (Invited & Regular)**

Andrew Eckford Room 304A

10:30

Spatial Coding Techniques for Molecular MIMO

Martin Damrath (University of Kiel, Germany); H. Birkan Yilmaz (Yonsei University, Yonsei Institute of Convergence Technology, Korea); Chan-Byoung Chae (Yonsei University, Korea); Peter A. Hoeher (University of Kiel, Germany)

This paper presents spatial diversity techniques applied to multiple-input multiple-output (MIMO) diffusion-based molecular communications (DBMC). Two types of spatial coding techniques, namely Alamouti-type coding and repetition MIMO coding are suggested and analyzed. In addition, we consider receiver-side equal-gain combining, which is equivalent to maximum-ratio combining in symmetrical scenarios. For numerical analysis, the channel impulse responses of a symmetrical 2x2 MIMO-DBMC system are acquired by a trained artificial neural network. It is demonstrated that spatial diversity has the potential to improve the system performance and that repetition MIMO coding outperforms Alamouti-type coding.

10:50

Simplified Cooperative Detection for Multi-Receiver Molecular Communication

Yuting Fang (Australian National University, Australia); Adam Noel (University of Ottawa, Canada); Yiran Wang (The Australian National University, Australia); Nan Yang (Australian National University, Australia)

Diffusion-based molecular communication (MC) systems experience significant reliability losses. To boost the reliability, a MC scheme where multiple receivers (RXs) work collaboratively to de-

cide the signal of a transmitter (TX) by sending the same type of molecules to a fusion center (FC) is proposed in this paper. The FC observes the total number of molecules received and compares this number with a threshold to determine the TX's signal. The proposed scheme is more bio-realistic and requires relatively low computational complexity compared to existing cooperative schemes where the RXs send and the FC recognizes different types of molecules. Asymmetric and symmetric topologies are considered, and closed-form expressions are derived for the global error probability for both topologies. Results show that the tradeoff for simplified computations leads to a slight reduction in error performance, compared to the existing cooperative schemes.

11:10

Decoding Dynamic Signals in Molecular Communication

Tadashi Nakano (Osaka University, Japan)

Information may be embedded in a dynamic signal, a temporal pattern in concentration of information molecule, for molecular communication. This paper proposes a design of decoders that can respond to the period in periodic pulses, and shows that the proposed design allows decoders to exhibit period- dependent responses. This paper also examines how a designed decoder responds to complex temporal patterns found in calcium oscillations in biological cells and demonstrates the ability of the designed decoder to respond to the periodicity in in calcium oscillations.

11:30

Effect of Local Population Uncertainty on Cooperation in Bacteria

Adam Noel (University of Ottawa, Canada); Yuting Fang and Nan Yang (Australian National University, Australia); Dimitrios Makrakis (University of Ottawa, Canada); Andrew Eckford (York University, Canada)

Bacteria populations rely on mechanisms such as quorum sensing to coordinate complex tasks that cannot be achieved by a single bacterium. Quorum sensing is used to measure the local bacteria population density, and it controls cooperation by ensuring that a bacterium only commits the resources for cooperation when it expects its neighbors to reciprocate. This paper proposes a simple model for sharing a resource in a bacterial environment, where knowledge of the population influences each bacterium's behavior. Game theory is used to model the behavioral dynamics, where the net payoff (i.e., utility) for each bacterium is a function of its current behavior and that of the other bacteria. The game is first evaluated with perfect knowledge of the population. Then, the unreliability of diffusion introduces uncertainty in the local population estimate and changes the perceived payoffs. The results demonstrate the sensitivity to the system parameters and how population uncertainty can overcome a lack of explicit coordination.

11:50

Computing Framework in Biological Cells via Stochastic Methods

Afshin Abdi, Arash Einolghozati and Faramarz Fekri (Georgia Institute of Technology, USA)

In this paper, we propose using stochastic framework for computations by biological cells. The key observation is that the input molecules activate receptors of a biological cell independently with probability p that is dependent on the molecule's concentration. Hence, the (active/inactive) states of the receptors can be viewed as a stochastic number representing the input concentration or probability p. We construct the addition operation via a cell having two different types of receptors. We also develop the multiplication by using a receptor that is active (with some probability) when both types of input molecules present. We analyze the computing accuracy of a cell w.r.t. parameters such as number of receptors and the input sensitivity of the cell.

TB1: **Multiple Terminal Information Theory I**

Daniela Tuninetti Room 304B

10:30

Role of Feedback in Modulo-Sum Computation over K-User Erasure Multiple-Access Channels

I-Hsiang Wang (National Taiwan University, Taiwan); Yu-Chih Huang (National Taipei University, Taiwan); Shih-Chun Lin (National Taiwan University of Science and Technology, Taiwan)

The modulo-sum computation of messages over a K-user finite-field erasure multiple access channel (MAC) is studied, with emphasis on the role of feedback in the large system regime. For the non-feedback case, we propose a grouping scheme which has higher computation rate than that of the conventional "compute-and-forward" (CF) scheme where each transmitter uses the same linear code and the receiver leverages the additive structure of the multiple access channel to compute the modulo sum. Furthermore, with a growing number of users, the proposed grouping scheme strictly outperforms the conventional "decode-and-forward (DF)" scheme when the erasure probability is smaller than $1 - e^{\frac{1}{e}} \approx 0.3078$, where the receiver first decodes messages of all users and then computes the modulo sum. This is in contrast to the two-user case where the currently best known achievability reported in [1] coincides with the better one between DA and CF. For the case with delayed state feedback, a new hybrid-ARQ-type scheme is proposed, and in the large system regime, it achieves a computation rate scaling like $\Omega(\frac{1}{\log(K)})$, much higher than the scaling $\Theta(\frac{1}{K})$ achieved by the grouping scheme without feedback. Our result hints significant gain in function computation due to feedback in the large system regime when the transmitters are connected intermittently to the receiver, in sharp contrast to the static case where feedback provides no gain at all.

10:50

A Generalization of Blahut-Arimoto Algorithm to Compute Rate-Distortion Regions of Multiterminal Source Coding Under Logarithmic Loss

Yigit Ugur (Université Paris-Est Marne la Vallée & Huawei Technologies, France Research Center, Mathematical and Algorithmic Sciences Lab, France); Inaki Estella (Huawei Technologies Co., Ltd., France); Abdellatif Zaidi (Université Paris-Est, France)

In this paper, we present iterative algorithms that numerically compute the rate-distortion regions of two problems: the two-encoder multiterminal source coding problem and the Chief Executive Officer (CEO) problem, both under logarithmic loss distortion measure. With the clear connection of these models with the distributed information bottleneck method, the proposed algorithms may find usefulness in a variety of applications, such as clustering, pattern recognition and learning. We illustrate the efficiency of our algorithms through some numerical examples.

11:10

Lossy Transmission of Correlated Sources over Two-Way Channels

Jian-Jia Weng, Fady Alajaji and Tamas Linder (Queen's University, Canada)

Achievability and converse results for the lossy transmission of correlated sources over Shannon's two-way channels (TWCs) are presented. A joint source-channel coding theorem for independent sources and TWCs for which adaptation cannot enlarge the capacity region is also established. We further investigate the optimality of scalar coding for TWCs with discrete modulo additive noise as well as additive white Gaussian noise. Comparing the distortion of scalar coding with the derived bounds, we observe that scalar coding achieves the minimum distortion over both families of TWCs for independent and uniformly distributed sources and independent Gaussian sources.

11:30

Codes for T-user Asymmetric Multiple-Access Channel with Independent Sources

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

An asymmetric multiple access channel (AMAC) is a multiple-access channel where a portion of the users can observe the messages of other users. We propose a T-user coding scheme for a noisy AMAC. Given the T_a-user δ_a-decodable k-ary code $\mathcal{A}$ and T_d-subset δ_d-decodable difference set $\mathcal{D}$, with its two component sets $\mathcal{D}^+$ and $\mathcal{D}^-$ *a priori*, a larger error-correcting multi-user code $\mathcal{C}$ is obtained. The codewords of each constituent code in $\mathcal{C}$ are obtained by replacing each element of a row in a Hadamard matrix with vectors from $\mathcal{A}$, $\mathcal{D}^+$, or $\mathcal{D}^-$, depending on the values of the elements and their locations in the Hadamard matrix. Introducing the difference set $\mathcal{D}$ makes the total rate of generated code $\mathcal{C}$ higher than that of the conventional code.

11:50

The Approximate Capacity for the Three-Receiver Writing on Random Dirty Paper Channel

Stefano Rini (National Chiao Tung University, Taiwan); Shlomo (Shitz) Shamai (The Technion, Israel)

The capacity of the three-receiver "writing on random dirty paper" channel is investigated. In this model, the channel output is obtained as the sum of the channel input, white Gaussian noise and a state sequence randomly selected among three possible independent Gaussian realizations. The transmitter has non-causal knowledge of the set of possible state sequences, but does not know which one is selected to produce the channel output. This model is equivalent to a threereceiver compound channel with Gaussian independent states known at the transmitter. For this model, upper and lower bounds to capacity are derived which are to within a distance of at most 3 bits-per-channel-use for all channel parameters. In the achievability proof, the receiver opportunistically decodes a different set of transmitted codewords, depending on the variance of the state realization appearing in the channel output. Time-sharing among multiple transmission phases is employed to guarantee that the transmitted message can be decoded regardless of the state realization. In the converse proof, a novel outer bounding technique is used to match the time-sharing prelog which arises in the achievability proof.

TA2: Detection, Estimation & Compressed Sensing

Wasim Huleihel — Room 304B

13:40

Hypothesis Testing over Cascade Channels

Sadaf Salehkalaibar (University of Tehran, Iran); Michele A Wigger (Telecom ParisTech, France); Ligong Wang (ETIS & CNRS, France)

Binary hypothesis testing over single and parallel cascade channels is considered where sensors communicate with dedicated relays, and these relays with a single final receiver. All relays as well as the final receiver decide on the binary hypothesis governing the joint probability distribution of the observations at the sensors, relays, and final receiver. The quantity of interest is the set of feasible type-II error exponents that allow for the type-I error probabilities to vanish asymptotically as the observation length increases. A coding scheme is proposed and the corresponding set of feasible type-II error exponents is analyzed by means of a modified Han-type analysis that can account for distributed decisions based on different codebooks and for nodes forwarding their decisions to other nodes. The obtained exponent region is optimal in some special cases.

14:00

Learning via Active Hypothesis Testing over Networks

Anusha Lalitha and Tara Javidi (University of California San Diego, USA)

This paper considers a problem of distributed active hypothesis testing. At every time instant, individual nodes in the network adaptively choose a sensing action and receive noisy local (private)

observations as sensing outcomes. The distribution of observations is parameterized by a discrete parameter (hypotheses). The marginals of the joint observation distribution conditioned on each hypothesis and the action are known locally at the nodes, but the true parameter/hypothesis is not known. An update rule is analyzed in which nodes first choose a possibly randomized action as a function of their past observations and actions. Nodes then perform a Bayesian update of their belief (distribution estimate) on each hypothesis based on their current local observations. Each node communicates these updates to its neighbors, and then performs a "non-Bayesian" linear consensus using the log-beliefs of its neighbors. Under mild assumptions and for a general class of action selection strategies, we show that the belief of any node on a wrong hypothesis converges to zero exponentially fast, and the exponential rate of learning is characterized by the nodes' influence of the network and average distinguishability between the observations' distributions for the (randomized) action under the true hypothesis.

14:20

Recovery of Sign Vectors in Quadratic Compressed Sensing

Hang Zhang, Afshin Abdi and Faramarz Fekri (Georgia Institute of Technology, USA)

In certain applications, recovering the signs of values may be more critical than the values themselves. Inspired by advances of sparse recovery of signals with fewer measurements, we would like to study the sign recovery problem and generalize it from a linear case to a non-linear setup. We focus on the sign values in quadratic measurement systems and provide theorems for the consistency condition, which ensures the signs are recovered correctly with probability close to 1. In deriving the consistency condition, we adopt a new penalty term using the trace operation and transform the optimization problem to the widely known Lasso problem. We also present simulation results to verify the correctness of our theorems.

14:40

Stability Threshold and Phase Transition of Generalized Censored Block Models

Chun Lam Chan (Ecole Polytechnique Fédérale de Lausanne, Switzerland); Nicolas Macris (EPFL, Switzerland)

The generalized censored block model considers the problem of inferring hidden binary variables from observations that are outputs of pairwise measurements from a symmetric channel. We give an exact formula for the stability threshold of density evolution by using an analysis of the potential functional of the model. In this model the phase transition is continuous so that this threshold is also the one for partial recovery of hidden variables. The formula is valid for all symmetric channels and generalizes the one already known for binary symmetric channels. We also give a bound on the finite slope of the Bhattacharyya parameter at the stability threshold. Finally, we briefly discuss implications for a heuristic derivation of the replica formula for the conditional entropy of the model.

15:00

Compressive Sensing with Energy Constraint

Hang Zhang, Afshin Abdi and Faramarz Fekri (Georgia Institute of Technology, USA)

In many sparse sensing applications, it is desirable to limit not only the number of non-zero variables but also the amplitude or energy of the signal, i.e., the non-zero variables are expected to be in a certain range. One approach to incorporate the energy constraint is using objective functions such as $||x||_2 + \lambda||x||_0$. In this paper, we consider minimizing this objective function, given the linear sensing system y = Ax. As this optimization problem is not convex, we first find the convex envelope of the objective function and then analyze the relation between the uniqueness of the solution and the required number of sensors. Further, we show as to how the sparsity of the measurement matrix A has negative effects on the required number of sensors.

TB2: **Quantum Information Theory & Communication**

Masahito Hayashi Room 304B

13:40

Joint Secrecy over the K-Transmitter Multiple Access Channel

Yanling Chen (University of Duisburg-Essen, Germany); O. Ozan Koyluoglu (University of California, Berkeley, USA); Han Vinck (University of Duisburg-Essen & University of Johannesburg, Germany)

This paper studies the problem of secure communication over a K-transmitter multiple access channel in the presence of an external eavesdropper, subject to a joint secrecy constraint (i.e., information leakage rate from the collection of K messages to an eavesdropper is made vanishing). As a result, we establish the joint secrecy achievable rate region. To this end, our results build upon two techniques in addition to the standard information-theoretic methods. The first is a generalization of Chia-El Gamal's lemma on entropy bound for a set of codewords given partial information. The second is to utilize a compact representation of a list of sets that, together with properties of mutual information, leads to an efficient Fourier-Motzkin elimination. These two approaches could also be of independent interests in other contexts.

14:00

On the Gaussian MAC with Degraded Message Sets and Long-Term Power Constraints

Selma Belhadj Amor and Vincent Y. F. Tan (National University of Singapore, Singapore)

In this paper, asymptotic expansions for the two-user Gaussian multiple access channel with degraded message sets under long-term power constraints and non-vanishing error probabilities $\epsilon \in [0, 1)$ are studied. The ϵ-capacity region is established and bounds on the second-order terms are derived.

14:20

The Multi-Layer Information Bottleneck Problem

Qianqian Yang (Imperial College London, United Kingdom (Great Britain)); Pablo Piantanida (CentraleSupélec-CNRS-Université Paris-Sud, France); Deniz Gündüz (Imperial College London, United Kingdom (Great Britain))

The muti-layer Information Bottleneck problem, where information is propagated from layer to layer, is considered. Based on information forwarded by the preceding layer, each layer is required to preserve a certain level of relevance with regards to a specific hidden variable, quantified by the mutual information. The relevant variables can be arbitrarily related. The optimal trade-off between relevance and complexity is obtained through a single-letter characterization, referred to as rate-relevance region. Conditions of successive refinabilty are given and investigated for binary sources with BSC relevant variables and BSC/BEC relevant variables, respectively. A counterexample of successive refinability is also included. We further extend the result to Guassian sources.

14:40

Delay Scaling Laws of Random Wireless Networks: Impact of Blocklength

Cheng-Hsiung Liu (National Taiwan University, Taiwan); Vincent Y. F. Tan (National University of Singapore, Singapore); I-Hsiang Wang (National Taiwan University, Taiwan)

We investigate the end-to-end delay of multiple-unicast wireless networks. In contrast to previous works where the end-to-end delay is measured by the queuing delay, in this work we measure the delay by the total blocklength of the communication scheme. As the capacity characterization of multiple-unicast networks is open, we consider random wireless networks (the Gupta-Kumar model) and investigate the end-to-end delay scaling law with respect to the number of nodes. The end-to-end delay of delivering a file depends on the file size as well as the throughput. Our main contribution is the characterization of the end-to-end delay scaling law of the multihopping scheme,

which depends on the file size. Our main finding is that if the file size is sufficiently large, the end-to-end delay scaling law is proportional to it. While this is expected, if the file size is not large enough, the end-to-end delay scaling law becomes independent of it. In particular, in a network with $2k$ randomly one-to-one paired users and area k and a source with $F(k)$ bits to send, we show that the delay is $\omega(\sqrt{k}F(k))$ if $F(k) = \Omega(\sqrt{k}\log k)$, while it is $\omega(k \log k)$ if $F(k) = o(\sqrt{k}\log k)$. Our result is derived by studying the multihopping scheme for large random wireless networks. Using ideas from moderate deviations theory and finite length bounds in the literature, we derive a lower bound on the required blocklength for the network.

15:00

The Dispersion of Superposition Coding for Gaussian Broadcast Channels

Ayşe Ünsal (EURECOM, France); Jean-Marie Gorce (INSA-Lyon & CITI, Inria, France)

In this paper, we analyze the performance of superposition coding for Gaussian broadcast channels with finite blocklength. To this end, we adapt two different achievability bounds, the dependence testing and the KB bounds introduced by Polyanskiy et al. in 2010 to the broadcast setting. The distinction between these bounds lies in fixing either the input or the output distributions of the channel. For the first case of the dependence testing bound, an upper bound on the average error probability of the system is derived whereas for the latter, lower bounds on the maximal code sizes of each user are presented.

TA3: **Information Theory & Statistics**

Carol Wang — Room 304B

15:50

Distance Spectrum Formula for the Largest Minimum Hamming Distance of Finite-Length Binary Block Codes

Ling-Hua Chang (National Chiao Tung University, Taiwan); Carol Wang (National University of Singapore, Singapore); Po-Ning Chen (National Chiao Tung University, Taiwan); Yunghsiang Sam Han (Dongguan University of Technology, P.R. China); Vincent Y. F. Tan (National University of Singapore, Singapore)

In this paper, an exact distance spectrum formula for the largest minimum Hamming distance of finite-length binary block codes is presented. The exact formula indicates that the largest minimum distance of finite-length block codes can be fully characterized by the information spectrum of the Hamming distance between two independent and identically distributed (i.i.d.) random codewords. The distance property of finite-length block codes is then connected to the distance spectrum. A side result of this work is a new lower bound to the largest minimum distance of finite-length block codes. Numerical examinations show that the new lower bound improves the finite-length Gilbert-Varshamov lower bound and can reach the minimum distance of existing finite-length block codes.

16:10

Explicit Symmetric Pseudo-Random Matrices

Ilya Soloveychik, Yu Xiang and Vahid Tarokh (Harvard University, USA)

We consider the problem of generating symmetric pseudo-random sign $(+/-1)$ matrices based on the similarity of their spectra to Wigner's semicircular law. Using binary m-sequences (Golomb sequences) of lengths $n = 2^m - 1$, we give a simple explicit construction of circulant n by n sign matrices and show that their spectra converge to the semicircular law when n grows. The Kolmogorov complexity of the proposed matrices equals to that of Golomb sequences and is at most 2log(n) bits.

16:30

Information Geometry of The Family of Markov Kernels Defined by A Context Tree

Junichi Takeuchi (Kyushu University, Japan); Hiroshi Nagaoka (University of Electro-Communications, Japan)

We prove that a tree model is an exponential family (e-family) of Markov kernels, if and only if it is an

FSMX model. The notion of e-family of Markov kernels was first introduced by Nakagawa and Kanaya ('93) in the one-dimensional case. Then, Nagaoka ('05) gave its established form, and Hayashi & Watanabe ('16) discussed it. A tree model is the Markov model defined by a context tree. It is noted by Weinberger et al., ('95) that tree models are classified into two classes; FSMX models and non-FSMX models, depending on the shape of their context trees. The FSMX model is a tree model and a finite state machine. We further show that, for Markov models, the e-family of Markov kernels is equivalent to the asymptotic e-family, which was introduced by Takeuchi & Barron ('98). Note that Takeuchi & Kawabata ('07) proved that non-FSMX tree models are not asymptotic e-families for the binary alphabet case. This paper enhances their result and reveals the information geometrical properties of tree models.

16:50

An Information-theoretic Approach to Unsupervised Feature Selection for High-Dimensional Data

Shao-Lun Huang and Lin Zhang (Tsinghua-Berkeley Shenzhen Institute, P.R. China); Lizhong Zheng (Massachusetts Institute of Technology, USA)

In this paper, we model the unsupervised learning of a sequence of observed data vector as a problem of extracting joint patterns among random variables. In particular, we formulate an information-theoretic problem to extract common features of random variables by measuring the loss of total correlation given the feature. This problem can be solved by a local geometric approach, where the solutions can be represented as singular vectors of some matrices related to the pairwise distributions of the data. In addition, we illustrate how these solutions can be transferred to feature functions in machine learning, which can be computed by efficient algorithms from data vectors. Moreover, we present a generalization of the HGR maximal correlation based on these feature functions, which can be viewed as a nonlinear generalization to linear PCA. Finally, the simulation result shows that our extracted feature functions have great performance in real-world problems.

17:10

Rumor Source Detection in Unicyclic Graphs

Pei Duo Yu and Chee Wei Tan (City University of Hong Kong, Hong Kong); Hung Lin Fu (National Chiao Tung University, Taiwan)

Detecting information source in viral spreading has important applications such as to root out the culprit of a rumor spreading in online social networks. In particular, given a snapshot observation of the network topology of nodes having the rumor, how to accurately identify the initial source of the spreading? In the seminal work by Shah and Zaman in 2011, this problem was formulated as a maximum likelihood estimation problem and solved using a rumor centrality approach for graphs that are cycle-free. This however is optimal only for degree-regular trees, and even the special case of a single cycle is an open problem. In this paper, we address the maximum likelihood estimation problem by a generalized rumor centrality for spreading in graphs with cycles. In particular, we derive analytical characterization of the optimal solution and a polynomial-time algorithm to solve the special case of unicyclic graphs.

TB3: **Coding Theory & Practice II**

Li Chen — Room 304B

15:50

Novel Outer Bounds for Combination Networks with End-User-Caches

Kai Wan (L2S - CNRS - Supelec - Univ Paris-Sud, France); Mingyue Ji (University of Utah, USA); Pablo Piantanida (CentraleSupélec-CNRS-Université Paris-Sud, France); Daniela Tuninetti (University of Illinois at Chicago, USA)

This paper studies the tradeoff between the memory size M and the download time / rate R for networks where a server with N files is connected to H relays (without caches), which in turns are connected to K users equipped with caches of size M files. When each user is connected to a different subset of r relays, the system is referred to as a *combination network with end-user-caches*. In

this work, outer bounds are derived for the practically motivated case of *uncoded* cache contents, that is, bits of the various files are directly copied in the user caches without any coding. In this case, once the cache contents and the user demands are known, the problem reduces to a general index coding problem. This paper shows that relying on a well known "acyclic index coding outer bound" results in bounds that are not tight for combination networks with end-user-caches (as opposed to the case without relays) and provides two novel ways to derive the tightest known outer bounds to date. As a result of independent interest, an inequality that generalizes the well-known sub-modularity of entropy is derived.

16:10

Multilayer Codes for Synchronization from Deletions

Mahed Abroshan and Ramji Venkataramanan (University of Cambridge, United Kingdom (Great Britain)); Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra & University of Cambridge, Spain)

A coding scheme is proposed for synchronization from a small number of deletions via a one-way error-free link. The scheme is based on multiple layers of Varshamov-Tenengolts codes combined with off-the-shelf linear error-correcting codes.

16:30

Syndrome-Coupled Rate-Compatible Error-Correcting Codes

Pengfei Huang and Yi Liu (University of California, San Diego, USA); Xiaojie Zhang (CNEX Labs Inc., USA); Paul H. Siegel (University of California, San Diego, USA); Erich Haratsch (Seagate Technology, USA)

Rate-compatible error-correcting codes (ECCs), which consist of a set of extended codes, are of practical interest in both wireless communications and data storage. In this work, we first study the lower bounds for rate-compatible ECCs, thus proving the existence of good rate-compatible codes. Then, we propose a general framework for constructing rate-compatible ECCs based on cosets and syndromes of a set of nested linear codes. We evaluate our construction from two points of view. From a combinatorial perspective, we show that we can construct rate-compatible codes with increasing minimum distances. From a probabilistic point of view, we prove that we are able to construct capacity-achieving rate-compatible codes.

16:50

Locality-Aware Hybrid Coded MapReduce for Server-Rack Architecture

Sneh Gupta and V. Lalitha (International Institute of Information Technology, India)

MapReduce is a widely used framework for distributed computing. Data shuffling between the Map phase and Reduce phase of a job involves a large amount of data transfer across servers, which in turn accounts for increase in job completion time. Recently, Coded MapReduce has been proposed to offer savings with respect to the communication cost incurred in data shuffling. This is achieved by creating coded multicast opportunities for shuffling through repeating Map tasks at multiple servers. We consider a server-rack architecture for MapReduce and in this architecture, propose to divide the total communication cost into two: intra-rack communication cost and cross-rack communication cost. Having noted that cross-rack data transfer operates at lower speed as compared to intra-rack data transfer, we present a scheme termed as Hybrid Coded MapReduce which results in lower cross-rack communication than Coded MapReduce at the cost of increase in intra-rack communication. In addition, we pose the problem of assigning Map tasks to servers to maximize data locality in the framework of Hybrid Coded MapReduce as a constrained integer optimization problem. We show through simulations that data locality can be improved considerably by using the solution of optimization to assign Map tasks to servers.

17:10

Block-Diagonal Coding for Distributed Computing With Straggling Servers

Albin Severinson and Alexandre Graell i Amat (Chalmers University of Technology, Sweden); Eirik Rosnes (University of Bergen, Norway)

We consider the distributed computing problem of multiplying a set of vectors with a matrix. For this scenario, Li et al. recently presented a unified coding framework and showed a fundamental tradeoff between computational delay and communication load. This coding framework is based on maximum distance separable (MDS) codes of code length proportional to the number of rows of the matrix, which can be very large. We propose a block-diagonal coding scheme consisting of partitioning the matrix into submatrices and encoding each submatrix using a shorter MDS code. We show that the assignment of coded matrix rows to servers to minimize the communication load can be formulated as an integer program with a nonlinear cost function, and propose an algorithm to solve it. We further prove that, up to a level of partitioning, the proposed scheme does not incur any loss in terms of computational delay (as defined by Li et al.) and communication load compared to the scheme by Li et al.. We also show numerically that, when the decoding time is also taken into account, the proposed scheme significantly lowers the overall computational delay with respect to the scheme by Li et al.. For heavy partitioning, this is achieved at the expense of a slight increase in communication load.

Friday, November 10 10:30–17:30

FA1: **Quantum Communication (Invited)**

Min-Hsiu Hsieh Room 304A

10:30

Asymptotic Analysis for Hidden Markovian Process with Quantum Hidden System

Masahito Hayashi (Nagoya University, Japan)

We focus on a hidden Markovian process whose internal hidden system is given as a quantum system, and we address a sequence of data obtained from this process. Using a quantum version of Perron-Frobenius theorem, we derive novel upper and lower bounds for the cumulant generating function of the sample mean of the data. Using these bound, we derive the central limit theorem and large and moderate deviation for the tail probability. Further, our results can be extended to general probabilistic system.

10:50

Achievability Bounds on Quantum State Redistribution Using Convex Split and Position Based Decoding

Anurag Anshu, Rahul Jain and Naqueeb Warsi (National University of Singapore, Singapore)

Quantum state redistribution is a fundamental quantum information theoretic primitive that captures a generic quantum communication scenario. In this work, we study the problem of entanglement assisted quantum state redistribution in one-shot setting and provide a new achievability result on the quantum communication required. Our bounds are in terms of max relative entropy and Rényi relative entropy of order $\frac{1}{2}$. We show that our result is upper bounded by the result obtained in Berta, Christandl, Touchette (2016) (which is in terms of smooth conditional max and min entropies). We use the techniques of convex split and position based decoding (through pretty good

measurement) to arrive at our result. Furthermore, in order to clarify the connection between our result and other recent results that use convex split and position based decoding, we prove a new relation between the hypothesis testing relative entropy and Rényi relative entropy of order $\frac{1}{2}$.

11:10

Sphere-Packing Bound for Classical-Quantum Channels

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

We study lower bounds on the optimal error probability in channel coding at rates below capacity, commonly termed sphere-packing bounds. In this work, we establish a sphere-packing bound for classical-quantum channels, which significantly improves previous prefactor from the order of subexponential to polynomial. Furthermore, the gap between the obtained error exponent for constant composition codes and the best known classical random coding exponent vanishes in the order of $o(\log n/n)$, indicating our sphere-packing bound is almost exact in the high rate regime. The main technical contributions are two converse Hoeffding bounds for quantum hypothesis testing and the saddle-point properties of error exponent functions.

11:30

Quantum and Private Capacities of Low-noise Channels

Felix Leditzky (University of Colorado Boulder, USA); Debbie Leung (University of Waterloo, Canada); Graeme Smith (IBM T. J. Watson Research Centre, USA)

We determine both the quantum and the private capacities of low-noise quantum channels to leading orders in the channel's distance to the perfect channel. It has been an open problem for more than 20 years to determine the capacities of some of these low-noise channels such as the depolarizing channel. We also show that both capacities are equal to the single-letter coherent information of the channel, again to leading orders. We thus find that, in the low noise regime, super-additivity and degenerate codes have negligible benefit for the quantum capacity, and shielding does not improve the private capacity beyond the quantum capacity, in stark contrast to the situation when noisier channels are considered.

11:50

Comparison of Noisy Channels and Reverse Data-Processing Theorems

Francesco Buscemi (Nagoya University, Japan)

This paper considers the comparison of noisy channels from the viewpoint of statistical decision theory. Various orderings are discussed, all formalizing the idea that one channel is "better" than another for information transmission. The main result is an equivalence relation that is proved for classical channels, quantum channels with classical encoding, and quantum channels with quantum encoding.

FB1: Network Communication Theory

Stefano Rini — Room 304B

10:30

On the Two-User Erasure Broadcast Channel with One-Sided Feedback

Chao He (SUPELEC, France); Sheng Yang (CentraleSupélec, France)

In this paper, we investigate the two-user erasure broadcast channel in which only one of the receivers feeds the output back to the transmitter. We propose a transmission scheme based on joint source-channel coding and show that the achievable rate region can be strictly larger than the ones previously known for this channel. In particular, the proposed scheme is partially optimal in the sense that the boundary of the achievable region overlaps in part with the boundary of the capacity region of the same channel with two-sided feedback. Thus, we identify a condition under which one-sided feedback is as good as two-sided feedback. Our result also demonstrates the limitation of bit-wise linear transmission schemes previously used for such channels.

10:50

On the Capacity of the Two-User Erasure Broadcast Channel with Mixed CSIT

Zheng Li (CentraleSupelec, France); Chao He (SUPELEC, France); Sheng Yang (CentraleSupelec, France)

This paper investigates the two-user Erasure Broadcast Channel (EBC), where the channel state information (CSI) is fully known at the destination, while the transmitter is only aware of the strictly causal CSI by state feedback and an estimate of the instantaneous CSI. We propose a novel transmission scheme that exploits both the delayed and the instantaneous CSI. Our scheme includes both the case with full CSI and the case with delayed CSI as special cases. We also derive a new outer bound region for this channel. For the symmetric EBC, we show that our scheme is capacity achieving in some nontrivial cases. Since both the inner and outer bound regions are characterized with linear constraints, numerical evaluation can be done easily.

11:10

Optimal Transmission Strategy in Full-duplex Relay Networks

Alessandro Nordio (IEIIT-CNR, Italy); Carla-Fabiana Chiasserini (Politecnico di Torino, Italy); Emanuele Viterbo (Monash University, Australia)

In this work, we consider a dual-hop, decode-and-forward network where the relay can operate in FD mode. We model the residual self interference as an additive Gaussian noise with variance proportional to the relay transmit power, and we assume a Gaussian input distribution at the source. Unlike previous work, however, we assume that the source is only aware of the transmit power distribution adopted by the relay over a given time horizon, not of the symbols that the relay is currently transmitting. This scenario better reflects practical situations in which the relay node may also have to forward signaling traffic, or data originated by other sources. Under these conditions, we show that the optimal communication strategy that source and relay can adopt is a time-division scheme, and, for each slot, we determine the optimal transmit power level that source and relay should adopt depending on the channel gains. Interestingly, the distribution of the optimal transmit power turns out to be discrete with two probability masses.

11:30

The Necessity of Scheduling in Compute-and-Forward

Ori Shmuel (Ben Gurion University, Israel); Asaf Cohen (Ben-Gurion University of the Negev, Israel); Omer Gurewitz (Ben-Gurion University Of The Negev, Israel)

Compute and Forward (CF) is a promising relaying scheme which, instead of decoding single messages or forwarding/amplifying information at the relay, decodes linear combinations of the simultaneously transmitted messages. The current literature includes several coding schemes and results on the degrees of freedom in CF, yet for systems with a fixed number of transmitters and receivers. It is unclear, however, how CF behaves at the limit of a large number of transmitters.

In this paper, we investigate the performance of CF in that regime. Specifically, we show that as the number of transmitters grows, CF becomes degenerated, in the sense that a relay prefers to decode only one (strongest) user instead of any other linear combination of the transmitted codewords, treating the other users as noise. Moreover, the sum-rate tends to zero as well. This makes scheduling necessary in order to maintain the superior abilities CF provides. Indeed, under scheduling, we show that non-trivial linear combinations are chosen, and the sum-rate does not decay, even without state information at the transmitters and without interference alignment.

11:50

Preserving Privacy while Broadcasting: k-Limited-Access Schemes

Mohammed Karmoose; Linqi Song; Martina Cardon and Christina Fragouli (University of California, Los Angeles, USA)

Index coding employs coding across clients within the same broadcast domain. This typically assumes that all clients learn the coding matrix so that they can decode and retrieve their requested data. However, learning the coding matrix can

pose privacy concerns: it may enable clients to infer information about the requests and side information of other clients [1]. In this paper, we formalize the intuition that the achieved privacy can increase by decreasing the number of rows of the coding matrix that a client learns. Based on this, we propose the use of k-limited-access schemes: given an index coding scheme that employs T transmissions, we create a k-limited-access scheme with $T_k \geq T$ transmissions, and with the property that each client learns at most k rows of the coding matrix to decode its message. We derive upper and lower bounds on T_k for all values of k, and develop deterministic designs for these schemes for which T_k has an order-optimal exponent for some regimes.

FA2: **Source Coding**

Ying Li Room 304B

13:40

An Iterative Algorithm to Construct Optimal Binary AIFV-m Codes

Ken-ichi Iwata (University of Fukui, Japan); Hirosuke Yamamoto (The University of Tokyo, Japan)

We propose an algorithm to construct an optimal code that achieves the minimum average codeword length in the class of binary AIFV-m codes with m code trees T_0, T_1, $\cdots$, T_{m-1} for a given stationary memoryless source. The algorithm is an iterative algorithm such that the optimal T_k for a given set of costs is derived by dynamic programming (DP) and the costs are updated from the set of code trees (T_0, T_1, $\cdots$, T_{m-1}), iteratively. The proposed DP works with polynomial time and space for source alphabet size. We prove the AIFV-m code obtained by the proposed algorithm is optimal for $m = 2, 3, 4, 5$ although the algorithm works for any m and we conjecture the optimality also holds for $m \geq 6$. Furthermore, we verify by some examples of sources that the average codeword length of the optimal binary AIFV-m codes can be decreased as m becomes large.

14:00

Design of Optimal Entropy-constrained Scalar Quantizer for Sequential Coding of Correlated Sources

Huihui Wu and Sorina Dumitrescu (McMaster University, Canada)

This work addresses the design of a sequential code for correlated sources using entropy-constrained scalar quantization at each encoder. We consider discrete sources and propose a globally optimal algorithm to minimize a weighted sum of distortions and rates. Our algorithm is based on solving the minimum weight path problem in a series of appropriately constructed weighted directed acyclic graphs. Its asymptotical time complexity is $O(N_1^2 N_2^2)$, where N_1 and N_2 denote the alphabet sizes of the two sources, respectively.

14:20

Sequential Coding of Gauss-Markov Sources With Packet Erasures and Feedback

Anatoly Khina and Victoria Kostina (California Institute of Technology, USA); Ashish Khisti (University of Toronto, Canada); Babak Hassibi (California Institute of Technology, USA)

We consider the problem of sequential transmission of Gauss-Markov sources. We show that in the limit of large spatial block lengths, greedy compression with respect to the squared error distortion is optimal; that is, there is no tension between optimizing the distortion of the source in the current time instant and that of future times. We then extend this result to the case where at time t a random compression rate r_t is allocated independently of the rate at other time instants. This, in turn, allows us to derive the optimal performance of sequential coding over packet-erasure channels with instantaneous feedback. For the case of packet erasures with delayed feedback, we connect the problem to that of compression with side information that is known at the encoder and may be known at the decoder - where the most recent packets serve as side information that may have been erased, and demonstrate that the loss due to a delay by one time unit is rather small.

14:40

An Upper Bound to Zero-delay Rate Distortion via Kalman Filtering for Vector Gaussian Sources

Photios A. Stavrou and Jan Østergaard (Aalborg University, Denmark); Charalambos D. Charalambous (University of Cyprus, Cyprus); Milan S. Derpich (Universidad Tecnica Federico Santa Maria, Chile)

In this work, we deal with zero-delay source coding of a vector Gaussian autoregressive (AR) source in state space form under average mean square error (MSE) fidelity criterion. We use the time-domain realization scheme with feedback, which was recently proposed in [1] that is known to give a lower bound to the zero-delay rate distortion function (RDF) via information nonanticipative rate distortion function (INRDF). In this scheme, the feedback path comprises a Kalman filter, which produces an estimate of the source (innovations' encoder). Our idea is to encode the vector innovations due to Kalman filtering via lattice quantization with subtractive dither and memoryless entropy coding which is a standard approach when quantizing innovations. We give conditions on the source so that the resulting system is stable (bounded performance) and furthermore, we provide generalizations and explicit expressions of existing bounds to the zero-delay RDF. We also extend our results to vector Gaussian AR sources of any finite order. With this, we are able to establish a time-domain approach with feedback, which with the use of a single filter (Kalman filter) gets very close to the zero-delay RDF. Compellingly, for infinite dimensional vector sources, the INRDF coincides with the zero-delay RDF. We demonstrate our theoretical results with a simulation example.

15:00

Compress-and-Estimate Source Coding for a Vector Gaussian Source

Ruiyang Song (Stanford University, USA); Stefano Rini (National Chiao Tung University, Taiwan); Alon Kipnis and Andrea Goldsmith (Stanford University, USA)

We consider the remote vector source coding problem in which a vector Gaussian source is estimated from noisy linear measurements. For this problem, we derive the performance of the compress-and-estimate (CE) coding scheme and compare it to the optimal performance. In the CE coding scheme, the remote encoder compresses the noisy source observations so as to minimize a local distortion measure, independent from the joint distribution between the source and the observations. In reconstruction, the decoder, having full knowledge of the joint distribution of the source and observations, estimates the original source realization from the lossy-compressed noisy observations. For the CE scheme in the vector Gaussian case, we show that, if the code rate is less than a specific threshold, then the CE coding scheme attains the same performance as the optimal coding scheme. For code rates above this threshold, we introduce lower and upper bounds on the performance gap between the CE and the optimal scheme. The case of a two-dimensional Gaussian source observed through two noisy measurements is studied to illustrate the behavior of the performance gap.

FB2: Network & Coding

Yunghsiang Sam Han — Room 304B

13:40

Linear Programming based Finite Blocklength Converses for Some Network-like Problems

Sharu Jose and Ankur A. Kulkarni (Indian Institute of Technology Bombay, India)

The linear programming (LP) based approach we introduced in [1] for finding finite blocklength converses for joint source-channel coding is extended to some network-like settings. Finite blocklength channel coding of compound and averaged channels under the maximum probability error criterion is considered. Through the LP approach new converses are obtained which imply a weak converse for both channels and a strong converse for the compound channel. The LP approach is also extended to the networked setting and a new finite blocklength converse for Slepian-Wolf coding which improves on the converse in Han [8, Lemma 7.2.2] is derived.

14:00

The Stability of Exponential Backoff Protocols for Slotted-Aloha with Saturated Queues

Luca Barletta and Flaminio Borgonovo (Politecnico di Milano, Italy)

The Slotted-Aloha protocol has been widely studied in the past forty-five years. Nonetheless, when the Exponential Backoff (EB) is used to stabilize its behavior, the characterization of stability conditions have eluded all efforts. Here we prove that the EB with geometric law $i \mapsto b^{-i-i_0}$, with queues in saturation, is ergodic if and only if $b > 1$ and the initial offset is $i_0 > 1$, for any number of users. If $i_0 = 0$ the system is transient, and null recurrent for $0 < i_0 \leq 1$, where some intermediate behavior is possible, since not all backoff indexes are unstable.

14:20

Coding for the Binary Energy Harvesting Channel with Finite Battery

Carol Wang and Mehul Motani (National University of Singapore, Singapore)

In this paper, we give a framework for constructing codes over the binary energy harvesting channel when the energy arrivals are random and the battery has large but finite size. We study both noiseless and noisy binary channels (i.e., bit flips). In the noiseless case, we present an encoding strategy (called exponential backoff encoding) which uses a decreasing amount of energy in consecutive transmissions between energy arrivals. We analyze the achievable rate of backoff encoding and show that it can outperform a uniform energy usage policy. We then extend the encoding strategy to a noisy binary channel, suggest a corresponding decoder, and analyze its performance. We believe our constructive approach complements existing approaches which focus on the information capacity of energy harvesting channels.

14:40

Physical-layer Network Coding: A Random Coding Error Exponent Perspective

Shakeel Salamat Ullah (The Chinese University of Hong Kong, Hong Kong); Gianluigi Liva (DLR - German Aerospace Center, Germany); Soung Chang Liew (The Chinese University of Hong Kong, Hong Kong)

In this work, we derive the random coding error exponent for the uplink phase of a two-way relay system where physical layer network coding (PNC) is employed. The error exponent is derived for the practical (yet sub-optimum) XOR channel decoding setting. We show that the random coding error exponent under optimum (i.e., maximum likelihood) PNC channel decoding can be achieved even under the sub-optimal XOR channel decoding. The derived achievability bounds provide us with valuable insight and can be used as a benchmark for the performance of practical channel-coded PNC systems employing low complexity decoders when finite-length codewords are used.

15:00

A Simpler Proof for the Existence of Capacity-Achieving Nested Lattice Codes

Renming Qi (UBC, Canada); Chen Feng (University of British Columbia, Canada); Yu-Chih Huang (National Taipei University, Taiwan)

Nested lattice codes have played an important role in network information theory. However, their achievability proofs are often involved, even for the case of the additive white Gaussian noise (AWGN) channel. In sharp contrast, their finite- field counterparts, nested linear codes, enjoy much simpler achievability proofs. In this paper, we present a simple and direct proof that nested lattice codes achieve the AWGN channel capacity. In particular, we make use of an intriguing connection between nested lattice codes and nested linear codes, which allows us to keep the proof as simple as that for nested linear codes.

FA3: **Source & Channel Coding**

Ayşe Ünsal Room 304B

15:50

Explicit Lower Bounds on the Outage Probability of Integer Forcing over $N_r \times 2$ Channels

Elad Domanovitz and Uri Erez (Tel Aviv University, Israel)

The performance of integer-forcing equalization for communication over the compound multiple-input multipleoutput channel is investigated. An upper bound on the resulting outage probability as a function of the gap to capacity has been derived previously, assuming a random precoding matrix drawn from the circular unitary ensemble is applied prior to transmission. In the present work a simple and explicit lower bound on this outage probability is derived for the case of a system with two transmit antennas, leveraging the properties of the Jacobi ensemble. The derived lower bound is also extended to random space-time precoding, and may serve as a useful benchmark for assessing the relative merits of various algebraic space-time precoding schemes.

16:10

Outage Probability Bounds for Integer-Forcing Source Coding

Elad Domanovitz and Uri Erez (Tel Aviv University, Israel)

Integer-forcing source coding has been proposed as a low complexity method for compression of distributed correlated Gaussian sources. In this scheme, each encoder quantizes its observation using the same fine lattice and reduces the result modulo the coarse lattice. Rather than directly recovering the individual quantized signals, the decoder first recovers a full rank set of judiciously chosen integer linear combinations of the quantized signals, and then inverts it. It has been observed that the method works very well for "most" but not all source covariance matrices. The present work quantifies the measure of bad covariance matrices by studying the probability that integer forcing source coding fails as a function rate allocated in excess to the Berger-Tung benchmark, where the probability is with respect to a random unitary transformation that is applied to the sources prior to quantization. For the important case where the signals to be compressed correspond to the antenna inputs of relays in an i.i.d. Rayleigh fading environment, this unitary transformation can be viewed as if it is performed by nature. Hence, the results provide guarantees for distributed source coding via integer forcing in this scenario.

16:30

On Independent Distributed Source Coding Problems with Exact Repair

Congduan Li (City University of Hong Kong, Hong Kong); Fangwei Ye (The Chinese University of Hong Kong, Hong Kong); Xuan Guang (The Chinese University of Hong Kong, P.R. China); Zhiheng Zhou (University of Electronic Science and Tech of China, P.R. China); Chee Wei Tan and Raymond W. Yeung (The Chinese University of Hong Kong, Hong Kong)

In conventional distributed storage exact repair problems, all sources are reconstructed when the decoder has access to a certain number of encoders (disks). So, the underlying reconstruction network is equivalent to a single-source problem. This paper considers a variant of the exact repair problem, where the underlying reconstruction network is the independent distributed source coding problem, a type of multi-source problem. As the first non-trivial case with two sources and three encoders, the storage-repair tradeoff regions are proved for all the 33 instances, and it is shown that binary codes are optimal.

16:50

Random-Coding Error Exponent of Variable-Length Codes with a Single-Bit Noiseless Feedback

Shai Ginzach (Rafael Ltd., Israel); Neri Merhav and Igal Sason (Technion - Israel Institute of Technology, Israel)

We study the random-coding error exponent function of variable-length codes in the presence of a noiseless feedback channel, which is allowed

to be used merely for a single bit feedback per each transmitted message. In this study, we harness results and analysis techniques from the theory of sequential hypothesis testing, and combine them with modern distance enumeration methods which are used in the literature on error exponents. For this setup, sometimes referred to as stop-feedback, we derive an exact single-letter expression for the random-coding error exponent over the binary symmetric channel. For symmetric discrete memoryless channels, the exact error exponent at zero rate is obtained, and a lower bound is provided for any other positive rate below capacity.

17:10

Overflow Probability of Variable-Length Codes Allowing Non-Vanishing Error Probability

Ryo Nomura (Senshu University, Japan); Hideki Yagi (University of Electro-Communications, Japan)

The variable-length coding problem allowing the error probability up to some constant is considered for general sources. In this problem, we focus on the overflow (or excess codeword length) probability, instead of the mean codeword length and derive a general formula of the infimum of thresholds under the constraint that both of the error probability and the overflow probability are smaller than or equal to some constant. We also consider another expression of our general formula so as to reveal the relationship with the optimum coding rate in the fixed-length source coding problem.

FB3: Communication Theory II

Asaf Cohen — Room 304B

15:50

XY Precoder for MIMO Systems

Shuiyin Liu, Yi Hong and Emanuele Viterbo (Monash University, Australia)

In multiple-input multiple-output (MIMO) channels with discrete input alphabets, at high signal-to-noise ratio (SNR), maximizing the minimum Euclidean distance ($d_{\min}$) between all possible received constellation points is known to be the optimal precoding strategy. However, finding the optimal precoder has been proved to be NP-hard. For large MIMO, a promising practical approach is to transform the channel into parallel 2×2 MIMO subchannels and then precode each of them separately. However, existing methods are mostly based on heuristic subchannel pairing schemes and require numerical search/optimization in the design phase. In this work, we propose a novel real-valued precoder, named as *XY-precoder*, which enjoys an explicit construction, a provable $d_{\min}$, a provably optimal subchannel pairing scheme, and low ML-decoding complexity. We prove that the XY-precoder achieves the same diversity order as the best known precoder, but with a much lower decoding complexity. Simulation results confirm that the error performance of XY-precoder is almost the same as that of the best known precoders.

16:10

A General Framework for MIMO Receivers with Low-Resolution Quantization

Stefano Rini (National Chiao Tung University, Taiwan); Luca Barletta (Politecnico di Milano, Italy); Yonina C. Eldar (Technion-Israel Institute of Technology, Israel); Elza Erkip (New York University, USA)

The capacity of a discrete-time multi-input multioutput (MIMO) Gaussian channel with output quantization is investigated for different receiver architectures. A general formulation of this problem is proposed in which the antenna outputs are processed by analog combiners while sign quantizers are used for analog-to-digital conversion. To exemplify this approach, four analog receiver architectures of varying generality and complexity are considered: (a) multiple antenna selection and sign quantization of the antenna outputs, (b) single antenna selection and multilevel quantization, (c) multiple antenna selection and multilevel quantization, and (d) linear combining of the antenna outputs and multilevel quantization. Achievable rates are studied as a function of the number of available sign quantizers and compared among different architectures. In particular, it is shown that architecture (a) is sufficient to attain the optimal high signalto- noise ratio performance for a MIMO receiver in which the number of antennas is larger than the number of sign quantizers. Numerical

evaluations of the average performance are presented for the case in which the channel gains are i.i.d. Gaussian.

16:30

An Achievable DoF Region for the Two-User Non-Coherent MIMO Broadcast Channel with Statistical CSI

Khac-Hoang Ngo (CentraleSupélec & Mathematical and Algorithmic Sciences Lab, France Research Center, Huawei Technologies, France); Sheng Yang (CentraleSupélec, France); Maxime Guillaud (Huawei Technologies, Mathematical and Algorithmic Sciences Lab, France)

In this paper, we study the two-user non-coherent multiple-input multiple-output broadcast channel with spatially correlated Rayleigh block fading. We propose a scheme to exploit the statistical channel state information, namely, the knowledge of the covariance matrix, and derive the corresponding achievable degrees of freedom region. The main idea of the proposed scheme is based on rate-splitting, additive superposition coding, and channel training. Our result shows that statistical CSI can play an important role in enhancing the degrees of freedom of a non-coherent broadcast channel.

16:50

On the Benefit of Delayed CSIT in Fading MIMO Broadcast Channel with CSIR Locality

Yao-Shan Hsiao and I-Hsiang Wang (National Taiwan University, Taiwan)

The benefit of delayed channel state information (CSI) at the transmitter is investigated in fast-fading MIMO broadcast channels (BC) with local CSI at receivers (CSIR). The seminal work by Maddah-Ali and Tse shows that delayed CSI at the transmitter (DCSIT) can increase the degrees of freedom (DoF) in fast-fading MIMO BC. A caveat, however, is that each receiver is assumed to know the channel coefficients of other receivers, and the cost of disseminating such global CSIR was not considered. In this paper, we propose a model to capture the cost of achieving global CSIR. In this model, each receiver only knows its own channel (local CSIR) while rate-limited capacitated links among the receivers are available. These rate-limited links can be used for exchanging CSIR or other purposes such as facilitating cooperative MIMO. Our main contribution is the evaluation of achievable DoF of two classes of schemes in two-user MISO BC. One class leverages delayed CSIT following the Maddah-Ali-and-Tse (MAT) scheme together with the rate-limited links for exchanging CSIR. The other uses cooperative MIMO and does not leverage delayed CSIT at all. We first show that when the transmitter has delayed CSI of both receivers, leveraging delayed CSIT with MAT scheme cannot outperform cooperative MIMO in terms of DoF. Next, we turn our attention to the hybrid CSIT scenario where the CSI of on receiver is instantaneously known at the transmitter and the other receiver. Delayed CSIT can strictly improve DoF in this case.

17:10

Capacity Outer Bound and Degrees of Freedom of Wiener Phase Noise Channels with Oversampling

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

The discrete-time Wiener phase noise channel with an integrate-and-dump multi-sample receiver is studied.
A novel outer bound on the capacity with an average input power constraint is derived as a function of the oversampling factor.
This outer bound yields the degrees of freedom for the scenario in which the oversampling factor grows with the transmit power P as P^{α}.
The result shows, perhaps surprisingly, that the largest pre-log that can be attained with phase modulation at high signal-to-noise ratio is at most $1/4$.

Author Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z