Quantum message compression with application to quantum state redistribution

Anurag Anshu

National University of Singapore

ABSTRACT

We present a new scheme for the compression of one-way quantum messages, in the setting of coherent entanglement assisted quantum communication. For this, we present a new technical tool that we call the convex split lemma, which is inspired by the classical compression schemes that use rejection sampling procedure. As a consequence, we show new bounds on the quantum communication cost of single-shot entanglement-assisted one-way quantum state redistribution task and for the subtasks quantum state splitting and quantum state merging. Our upper and lower bounds are tight up to a constant and hence stronger than previously known best bounds for above tasks. Our protocols use explicit quantum operations on the sides of Alice and Bob, which are different from the decoupling by random unitaries approach used in previous works.

Phi-entropic measures of correlation

Salman Beigi

Sharif University, Iran

ABSTRACT

A measure of correlation is said to have the tensorization property if it is unchanged when computed for i.i.d. copies. Two well-known examples of such measures are the maximal correlation and the hypercontractivity ribbon. We show that the maximal correlation and hypercontractivity ribbons are special cases of Φ ribbon, defined in this paper for any function Φ from a class of convex functions. Φ-ribbon reduces to hypercontractivity ribbon and the maximal correlation for special choices of Φ, and is a measure of correlation with the tensorization property. We show that the Φ-ribbon also characterizes the Φ-strong data processing inequality constant recently introduced by Raginsky. We further study the Φ-ribbon for the choice of $\Phi(t) = t^2$ and introduce an equivalent characterization of this ribbon.

A meta-converse for private communication over quantum channels

Mario Berta

California Institute of Technology, USA

ABSTRACT

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

The meta-converse allows for proving that any quantum channel's relative entropy of entanglement is a strong converse rate for private communication. For covariant channels, the meta-converse also leads to second-order expansions of relative entropy of entanglement bounds for private communication rates. For such channels, the bounds also apply to the private communication setting in which the sender and receiver are assisted by unlimited public classical communication, and as such, they are relevant for establishing various converse bounds for quantum key distribution protocols conducted over these channels. We find precise characterizations for several channels of interest and apply the methods to establish several converse bounds on the private transmission capabilities of all phaseinsensitive bosonic channels.

Secure Network Coding

Ning Cai

ShanghaiTech University, China

ABSTRACT

In this talk we first survey the basic concepts and some important results in secure network coding. Then we turn to results in our recent joint works on secure coding on a relay network with Masahito Hayashi et al in the second part of the talk.

Quantum Sphere-Packing Bounds and Moderate Deviation Analysis for Classical-Quantum Channels

Hao-Chung Cheng

National Taiwan University, Taiwan and University of Technology Sydney, Australia

ABSTRACT

In this talk, we study the tradeoffs between the optimal error probabilities of classical-quantum channels, the blocklength n, and the transmission rate. First, we focus on the lower bounds of the error probability at rates below the capacity, commonly termed quantum sphere-packing bounds. Winter and Dalai have derived such bounds for classical-quantum channels; however, the exponents in their bounds only coincide when the channel is classical. We show that these two exponents admit a variational representation and are related by the Golden-Thompson inequality, reaffirming that Dalai's expression is stronger in general classical-quantum channels. Second, we establish a sphere-packing bound for classical-quantum channels, which significantly improves Dalai's 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. Third, the established sphere-packing bound enables us to estimate the error behaviors when the transmission rates approach the channel capacity at a rate slower than $1/\sqrt{n}$, a research topic known as moderate deviation analysis. We show that the optimal error probability vanishes under this rate convergence. The proof employs a strong large deviation technique, and the asymptotic expansions of the error-exponent functions.

Moderate deviation analysis for classical communication over quantum channels

Christopher Thomas Chubb

University of Sydney, Australia

ABSTRACT

We analyse families of codes for classical data transmission over quantum channels that have both a vanishing probability of error and a code rate approaching capacity as the code length increases. To characterise the fundamental tradeoff between decoding error, code rate and code length for such codes we introduce a quantum generalisation of the moderate deviation analysis proposed by Altŭg and Wagner as well as Polyanskiy and Verdú. We derive such a tradeoff for classical-quantum (as well as image-additive) channels in terms of the channel capacity and the channel dispersion, giving further evidence that the latter quantity characterises the necessary backoff from capacity when transmitting finite blocks of classical data. To derive these results we also study asymmetric binary quantum hypothesis testing in the moderate deviations regime. Due to the central importance of the latter task, we expect that our techniques will find further applications in the analysis of other quantum information processing tasks.

Quantum reading capacity: general definition and bounds

Siddhartha Das

Louisiana State University, USA

ABSTRACT

Quantum reading refers to the task of reading out classical information stored in a classical memory. In any such protocol, the transmitter and receiver are in the same physical location, and the goal of such a protocol is to use these devices, coupled with a quantum strategy, to read out as much information as possible from a classical memory, such as a CD or DVD. In this context, a memory cell is a collection of quantum channels that can be used to encode a classical message in a memory. The maximum rate at which information can be read out from a given memory encoded with a memory cell is called the quantum reading capacity of the memory cell. As a consequence of the physical setup of quantum reading, the most natural and general definition for quantum reading capacity should allow for an adaptive operation after each call to the channel, and this is how we define quantum reading capacity in this paper. In general, an adaptive strategy can give a significant advantage over a non-adaptive strategy in the context of quantum channel discrimination, and this is relevant for quantum reading due to its close connection with channel discrimination. Furthermore, a quantum channel discrimination protocol employing a non-adaptive strategy is clearly a special case of a quantum protocol that uses an adaptive strategy. In this paper, we provide a general definition of quantum reading capacity, and we establish several upper bounds on the quantum reading capacity of a memory cell. We also introduce two classes of memory cells, which we call jointly teleportation-simulable and jointly environment-parametrized memory cells, and we deliver second-order and strong converse characterizations of their quantum reading rates.

Fundamental work cost in implementations of quantum processes

Philippe Faist

California Institute of Technology, USA

ABSTRACT

Recently, the thermodynamic work requirement for erasure and work yield of formation of a quantum state, the conversion rates of one state into another as well as the work cost of logical processes on systems with a trivial Hamiltonian have been successfully characterized. Here, we provide a general and fundamental lower limit, valid for systems with an arbitrary Hamiltonian and in contact with any thermodynamic bath, on the work cost of implementing any logical process. This limit is given by a new information measure—the coherent relative entropy—which measures information relative to the Gibbs state (or more generally, relative to an operator γ which assigns an abstract "weight" to each microstate). The coherent relative entropy is defined as the number of pure qubits which can be distilled (or the negative number of qubits which have to be invested) while performing a fixed effective logical process using Gibbs-preserving operations. It is a natural generalization of both the min- and max-relative entropy, as well as the conditional min- and max-entropy, and obeys a data processing inequality and a chain rule. In the i.i.d. limit, it converges to the difference of the quantum relative entropy of the input and the output state relative to the Gibbs state. Incidentally, our approach provides an alternative proof for the data processing inequality for the quantum relative entropy. Finally, our framework may be applied at any level of knowledge, for instance for microscopic or macroscopic observers, providing an "observer-dependent" approach to thermodynamics where the observers are related by tracing out information inaccessible to the other observer, or by recovering that information with a recovery map.

Recent Results on Input-Constrained Erasure Channels

Guangyue Han

The University of Hong Kong, Hong Kong

ABSTRACT

In this talk, we examine an input-constrained erasure channel and we characterize the asymptotics of its capacity when the erasure rate is low. More specifically, for a general memoryless erasure channel with its input supported on an irreducible finite-type constraint, we derive partial asymptotics of its capacity, using some series expansion type formula of its mutual information rate; and for a binary erasure channel with its first-order Markovian input supported on the so-called golden mean constraint, based on the concavity of its mutual information rate with respect to some parameterization of the input, we numerically evaluate its first-order Markov capacity and further derive its full asymptotics. The asymptotics obtained in this paper, when compared with the recently derived feedback capacity for a binary erasure channel with the same input constraint, enable us to draw the conclusion that feedback may increase the capacity of an input-constrained channel, even if the channel is memoryless.

Pretty good measures in quantum information theory

Raban Iten

ETH Zurich, Switzerland

ABSTRACT

Quantum generalizations of Rényi's entropies are a useful tool to describe a variety of operational tasks in quantum information processing. Two families of such generalizations turn out to be particularly useful: the Petz quantum Rényi divergence and the minimal quantum Rényi divergence. In this talk, we introduce a reverse Araki-Lieb-Thirring inequality that implies a new relation between these two families of divergences. This relation suggests defining a "pretty good fidelity", whose relation to the usual fidelity implies the known relations between the optimal and pretty good measurement as well as the optimal and pretty good singlet fraction. We also find a new necessary and sufficient condition for optimality of the pretty good measurement and singlet fraction.

Finite blocklength bounds for adversarial channels

Oliver Kosut

Arizona State University, USA

ABSTRACT

Two well-known channel models with adversarial state are (i) the compound channel, in which an adversary chooses a fixed state, and (ii) the arbitrarily-varying channel, in which an adversary chooses an arbitrary state sequence. In the finite blocklength or one-shot regime, these channel models are identical, even though they have different asymptotic behavior. We will explore finite blocklength performance bounds that unify these two channel models, as well as the connection between these bounds and second-order (dispersion) results for the two channel models.

Self-guaranteed measurement-based quantum computation

Michal Hajdusek

National University of Singapore

ABSTRACT

In order to guarantee the output of a quantum computation, we usually assume that the component devices are trusted. However, when the total computation process is large, it is not easy to guarantee the whole system when we have scaling effects, unexpected noise, or unaccounted correlations between several subsystems. If we do not trust the measurement basis nor the prepared entangled state, we do need to be worried about such uncertainties. To this end, this paper proposes a "self-guaranteed" protocol for verification of quantum computation under the scheme of measurementbased quantum computation. Since our protocol is self-guaranteed, no prior trusted device (measurement basis nor entangled state) is needed. The approach we present enables the implementation of verifiable quantum computation using the measurement-based model in the context of a particular instance of delegated quantum computation where the server prepares the initial computational resource and sends it to the client who drives the computation by single-qubit measurements. Combining this with self-testing procedures we are able to verify the initial resource prepared as well as the operation of the quantum devices, and hence the computation itself. The overhead of our protocol scales as the size of the initial resource state to the power of 4 times the natural logarithm of the initial state's size.

Bounds on information combining with quantum side information

Christoph Hirche

Universitat Autònoma de Barcelona, Spain

ABSTRACT

Bounds on information combining are entropic inequalities that determine how the information (entropy) of a set of random variables can change when these are combined in certain prescribed ways. Such bounds play an important role in classical information theory, particularly in coding and Shannon theory; entropy power inequalities are special instances of them. The arguably most elementary kind of information combining is the addition of two binary random variables (a CNOT gate), and the resulting quantities play an important role in Belief propagation and Polar coding. We investigate this problem in the setting where quantum side information is available, which has been recognized as a hard setting for entropy power inequalities. Our main technical result is a non-trivial, and close to optimal, lower bound on the combined entropy, which can be seen as an almost optimal quantum Mrs. Gerber's Lemma. Our proof uses three main ingredients: (1) a new bound on the concavity of von Neumann entropy, which is tight in the regime of low pairwise state fidelities; (2) the quantitative improvement of strong subadditivity due to Fawzi-Renner, in which we manage to handle the minimization over recovery maps; (3) recent duality results on classical-quantum-channels due to Renes et al. We furthermore present conjectures on the optimal lower and upper bounds under quantum side information, supported by interesting analytical observations and strong numerical evidence. We finally apply our bounds to Polar coding for binary-input classical-quantum channels, and show the following three results: (A) Even non-stationary channels polarize under the polar transform. (B) The blocklength required to approach the symmetric capacity scales at most sub-exponentially in the gap to capacity. (C) Under the aforementioned lower bound conjecture, a blocklength polynomial in the gap suffices.

Operational measures for squeezing

Martin Idel

TNG Technology Consulting, Germany

ABSTRACT

Squeezed quantum states are continuous variable states with variances smaller than possible for states with symmetric variance. Squeezed states are interesting particularly in quantum optics as they require nonlinear optics for their production. In addition, squeezing is necessary for quantum entanglement in continuous variable systems, which makes it a candidate for an interesting resource theory. In this talk, I will give an overview about our work "An operational measure for squeezing" (https://arxiv.org/abs/1607.00873) starting with the results and their potential use in physics. In the main part, I will focus on the most interesting mathematical concepts used to obtain these results. Particular emphasis shall be on open problems and observations about potential applications.

Optimal performance of generalized heat engines with finite-size baths of arbitrary multiple conserved quantities beyond I.I.D. scaling

Kosuke Ito

Nagoya University, Japan

ABSTRACT

In quantum thermodynamics, effects of finiteness of the baths have been less considered. In particular, there is no general theory to focus on finiteness of the baths of arbitrary multiple conserved quantities. Thus, we focus on how the optimal performance of generalized heat engines with multiple quantities alters in response to the size of the baths. Conventionally, the size of the baths in quantum thermodynamics has been just given in terms of the number of identical copies of a system, which does not cover even such a natural scaling as the 'volume'. In consideration of the asymptotic extensivity, we deal with a generic scaling of the baths to naturally include the 'volume' scaling. Based on it, we derive the bound for the performance of generalized heat engines reflecting finite-size effects of the baths, which we call fine-grained generalized Carnot bound. We also construct a protocol to achieve the optimal performance of the engine given by this bound. Finally, applying the obtained general theory, we deal with simple examples of generalized heat engines. 1D Ising spin chain model and a toy model of two-level particles illustrate strange behaviors of the finite-size effects. The other example is a heat engine with two baths composed of an ideal gas exchanging particles, where the volume scaling is applied. The result implies that the mass of the particle explicitly affects the performance of this engine with finite-size baths.

Fock-majorization relation in passive bosonic channels

Michael G. Jabbour[a] and Nicolas J. Cerf[a]

[a] *Université libre de Bruxelles, Belgium*

ABSTRACT

We introduce a new class of quantum channels, called passive bosonic channels, for which we prove the preservation of a Fock-majorization relation as defined in [New J. Phys. 18, 073047 (2016)]. This means that any two input states that are comparable under Fock-majorization are transformed into equally comparable output states. Passive bosonic channels are interesting from the thermodynamical point of view because they correspond to an energy-preserving coupling of the system with an environment that is passive in the Fock basis (i.e., it is a state from which no work can be extracted using unitary transformations) followed by discarding the environment. The Fock-majorization relation happens to be very well suited in the context of bosonic channels, as, unlike other fundamental relations such as regular majorization, it relates the concepts of energy and disorder of a quantum state. In order to demonstrate our result, we prove the existence of a new majorization-like recurrence relation in a bosonic beam-splitter, which is the realization of the energy-conserving unitary acting on bosonic systems. With this result, which could probably also be generalized to other systems and Hamiltonians, we hope to connect the field of continuous-variable quantum information together with quantum thermodynamics.

Information-theoretic tradeoffs in control

Victoria Kostina

California Institute of Technology, USA

ABSTRACT

Consider a flying drone controlled from the ground by an observer who communicates with it via wireless. We are interested in how well the drone can be controlled via a channel that accepts r bits/sec. Formally, the controller of a linear stochastic system aims to minimize a quadratic cost function in the state variables and control signal, known as the linear quadratic regulator (LQR). We characterize the optimal tradeoff between the communication rate r bits/sec and the limsup of the expected cost b. We consider an information-theoretic rate-cost function, which quantifies the minimum mutual information between the channel input and output, given the past, that is compatible with a target LQR cost. We provide a lower bound to the rate-cost function, which applies as long as the system noise has a probability density function, and which holds for a general class of codes that can take full advantage of the memory of the data observed so far and that are not constrained to have any particular structure. Perhaps surprisingly, the bound can be approached by a simple variable-length lattice quantization scheme, as long as the system noise satisfies a smoothness condition. The quantization scheme only quantizes the innovation, that is, the difference between the controller's belief about the current state and the encoder's state estimate.

This is joint work with B. Hassibi.

Approximate reversal of quantum gaussian dynamics

Ludovico Lami

Universitat Autònoma de Barcelona, Spain

ABSTRACT

Recently, there has been focus on determining the conditions under which the data processing inequality for quantum relative entropy is satisfied with approximate equality. The solution of the exact equality case is due to Petz, who showed that the quantum relative entropy between two quantum states stays the same after the action of a quantum channel if and only if there is a reversal channel that recovers the original states after the channel acts. Furthermore, this reversal channel can be constructed explicitly and is now called the Petz recovery map. Recent developments have shown that a variation of the Petz recovery map works well for recovery in the case of approximate equality of the data processing inequality. Our main contribution here is a proof that bosonic Gaussian states and channels possess a particular closure property, namely, that the Petz recovery map associated to a bosonic Gaussian state σ and a bosonic Gaussian channel $\mathcal{N}$ is itself a bosonic Gaussian channel. We furthermore give an explicit construction of the Petz recovery map in this case, in terms of the mean vector and covariance matrix of the state σ and the Gaussian specification of the channel $\mathcal{N}$.

Upper bounds on the distillable entanglement under one-way and two-way LOCC

Felix Leditzky

University of Colorado, Boulder, USA

ABSTRACT

We derive general upper bounds on the distillable entanglement of a mixed state one-way and two-way LOCC. In both cases, the upper bound is based on a convex d position of the mixed state into 'useful' and 'useless' quantum states. By 'useful', we a state whose distillable entanglement is non-negative and equal to its coherent inforn (and thus given by a single-letter, tractable formula). On the other hand, 'useless' are undistillable, i.e., their distillable entanglement is zero. We prove that in both se the distillable entanglement is convex on such decompositions. Hence, an upper bou the distillable entanglement is obtained from the contributions of the useful states and is equal to a convex combination of the coherent information of the latter. Optin over all such decompositions of the input state yields our upper bound.

In the one-way LOCC setting, the useful and useless states are chosen to be degradab antidegradable states, respectively. Applying our bound to the qubit depolarizing cl yields an upper bound on its quantum capacity that is strictly tighter than prev known bounds for large values of the depolarizing parameter. These results can be in https://arxiv.org/abs/1701.03081. Furthermore, our result can be extended to upper bounds on the quantum capacity of an arbitrary quantum channel, based on a d decomposition of this channel into degradable and antidegradable completely positiv not necessarily trace-preserving) maps. This observation will be included in a future u of arXiv:1701.03081.

In the two-way LOCC setting, the useful and useless states are chosen to be max correlated (MC) states and positive partial transpose (PPT) states, respectively. We that our bound is equal to the PPT-relative entropy of entanglement for Werner sta arbitrary dimension and for isotropic states in prime local dimension. In these cases, w provide new expressions for the PPT-relative entropy of entanglement, which const the best known upper bounds on the distillable entanglement of Werner states (in a c regime of the parameter defining the Werner state) and isotropic states. We also de general method for finding decompositions into MC and PPT states of quantum state are block-diagonal with respect to the generalized Bell basis. These results can be in the attached (unpublished) manuscript titled "Maximally correlated states and tw entanglement distillation".

Covert communication with channel-state information at the transmitter

Si-Hyeon Lee

Pohang University of Science and Technology, Korea

ABSTRACT

We consider the problem of covert communication over a state-dependent channel, where the transmitter has knowledge of the channel states. Here, "covert" means that the probability that a warden on the channel can detect the communication must be small. In contrast with traditional models without channel-state information at the transmitter, we show that covert communication can be possible with positive rate. We derive closed-form formulas for the maximum achievable covert communication rate ("covert capacity") in this setting and derive lower bounds on the rate of the secret key that is needed for the transmitter and the receiver to achieve the covert capacity.

Deconstruction and conditional erasure of quantum correlations

Christian Majenz

University of Copenhagen, Denmark

ABSTRACT

Our work extends the decoupling approach to quantum information theory to the multipartite setting by establishing the quantum conditional mutual information as a measure for the quantum correlations between A and B from the perspective of E. Our results are inspired by thermodynamical considerations and generalize Landauer's erasure principle as well as Groisman et al.'s erasure of correlations to the multipartite setting. This solves a critical problem in understanding multipartite quantum correlations from an operational viewpoint and paves the way to study the variety of applications of decoupling in the multipartite setting.

Two instances where current single-letter expressions are sub-optimal

Chandra Nair

The Chinese University of Hong Kong, Hong Kong

ABSTRACT

I will talk about the sub-optimality of the Han-Kobayashi scheme for interference channel and about the sub-optimality of the superposition scheme for a degraded-message-sets broadcast channel setting. These results resolve open problems 6.4 and 8.2 in the book Network Information Theory. I will briefly mention the ideas that allow us to evaluate the achievable regions usually represented as unions of distributions involving auxiliary variables; ideas that allowed us to show the sub-optimality. For the second setting and for our particular example, we will explicitly deduce parts of the capacity region from limiting multi-letter expressions. This raises the interesting question whether single-letter expressions are really necessary to compute capacity regions.

Finite blocklength and moderate deviation analysis of hypothesis testing of correlated quantum states and application to classical-quantum channels with memory

Cambyse Rouzé

University of Cambridge, UK

ABSTRACT

Martingale concentration inequalities constitute a powerful mathematical tool in the analysis of problems in a wide variety of fields ranging from probability and statistics to information theory and machine learning. Here we apply techniques borrowed from this field to quantum hypothesis testing, which is the problem of discriminating quantum states belonging to two different sequences $\{\rho_n\}_n$ and $\{\sigma_n\}_n$. We obtain upper bounds on the finite blocklength type II Stein- and Hoeffding errors, which, for i.i.d. states, are in general tighter than the corresponding bounds obtained by Audenaert, Mosonyi and Verstraete in [1]. We also derive finite blocklength bounds as well as moderate deviation results for sequences of correlated states satisfying a (non-homogeneous) factorization property. Examples of such sequences include Gibbs states of spin chains with translationinvariant finite range interaction, and finitely correlated quantum states. We apply our results to find bounds on the capacity of a certain class of classical-quantum (c-q) channels with memory which satisfy a so-called channel factorization property, in the finite blocklength as well as moderate deviation regimes. Moderate deviation analysis for quantum hypothesis testing and memoryless c-q channels was recently done in [3, 4]. Our results extend theirs to the case of classes of correlated states and c-q channels with memory.

References

[1] K. M. R. Audenaert, M. Mosonyi, and F. Verstraete. Quantum state discrimination bounds for finite sample size. Journal of Mathematical Physics, 53(12), 2012.

[2] C. Rouze and N. Datta. Analysis of finite sample size quantum hypothesis testing via martingale concentration inequalities. arXiv preprint arXiv:1612.01464, 2016.

[3] C. T. Chubb, V. Y. Tan, and M. Tomamichel. Moderate deviation analysis for classical communication over quantum channels. arXiv preprint arXiv:1701.03114, 2017.

[4] H.-C. Cheng and M.-H. Hsieh. Moderate deviation analysis for classical-quantum channels and quantum hypothesis testing. arXiv preprint arXiv:1701.03195, 2017.

Rényi divergences as weighted non-commutative vector valued L_p-spaces

Mario Berta[a], Volkher Scholz[b], and Marco Tomamichel[c]

[a] *Institute for Quantum Information and Matter, Caltech, USA*
[b] *Ghent University, Belgium*
[c] *The University of Sydney, Australia*

ABSTRACT

Information-theoretic concepts are often developed under the assumption that the underlying physical systems are described by finite-dimensional Hilbert spaces. It is, however, of fundamental interest to understand which finite-dimensional concepts generalize to physical systems modeled by von Neumann algebras, e.g. certain quantum field theories. Moreover, the translation of finite-dimensional arguments to a more abstract theory often requires new proof ideas or at least a streamlining of the original arguments—thereby leading us to a better understanding of the finite-dimensional special case as well. In this work we explore a generalization to the setup of von Neumann algebras of a family of divergences, the sandwiched Rényi divergences [2, 3], which have found operational meaning and applications in quantum information theory. Specifically, we show Araki and Masuda's weighted non-commutative vector valued L_p-spaces [1] correspond to an algebraic generalization of the sandwiched Rényi divergences with parameter $\alpha = \frac{p}{2}$. Using complex interpolation theory, we prove various fundamental properties of these divergences in the setup of von Neumann algebras, including a data processing inequality and monotonicity in α. We thereby also give new proofs for the corresponding finite-dimensional properties. We discuss the limiting cases $\alpha \to \{\frac{1}{2}, 1, \infty\}$ leading to minus the logarithm of Uhlmann's fidelity, Umegaki's relative entropy, and the max-relative entropy, respectively. As a contribution that might be of independent interest, we derive a Riesz-Thorin theorem for Araki-Masuda L_p-spaces and an Araki-Lieb-Thirring inequality for states on von Neumann algebras.

References

[1] H. Araki and T. Masuda. Positive Cones and Lp-Spaces for von Neumann Algebras. *Publications of the Research Institute for Mathematical Sciences, Kyoto University*, 18:339-411, 1982.

[2] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On Quantum Rényi Entropies: A New Generalization and Some Properties. *Journal of Mathematical Physics*, 54(12):122203, 2013. DOI: 10.1063/1.4838856.

[3] M. M. Wilde, A. Winter, and D. Yang. Strong Converse for the Classical Capacity of Entanglement-Breaking and Hadamard Channels via a Sandwiched Rényi Relative Entropy. *Communications in Mathematical Physics*, 331(2):593-622, 2014. DOI: 10.1007/s00220-014-2122-x

Entanglement and coherence in quantum state merging

Alexander Streltsov

Gdańsk University of Technology, Poland

ABSTRACT

Understanding the resource consumption in distributed scenarios is one of the main goals of quantum information theory. A prominent example for such a scenario is the task of quantum state merging where two parties aim to merge their parts of a tripartite quantum state. In standard quantum state merging, entanglement is considered as an expensive resource, while local quantum operations can be performed at no additional cost. However, recent developments show that some local operations could be more expensive than others: it is reasonable to distinguish between local incoherent operations and local operations which can create coherence. This idea leads us to the task of incoherent quantum state merging, where one of the parties has free access to local incoherent operations only. In this case the resources of the process are quantified by pairs of entanglement and coherence. Here, we develop tools for studying this process, and apply them to several relevant scenarios. While quantum state merging can lead to a gain of entanglement, our results imply that no merging procedure can gain entanglement and coherence at the same time. We also provide a general lower bound on the entanglement-coherence sum, and show that the bound is tight for all pure states. Our results also lead to an incoherent version of Schumacher compression: in this case the compression rate is equal to the von Neumann entropy of the diagonal elements of the corresponding quantum state.

Thermodynamics, Statistical Mechanics, and Quantum Mechanics

Hal Tasaki

Gakushuin University, Japan

ABSTRACT

We shall give a brief overview about the basic ways of thinking and mutual relations between thermodynamics, statistical mechanics, and quantum mechanics, placing emphasis on information theoretic point of view. We in particular focus on the second law of thermodynamics, which is among the most fundamental and fascinating laws in nature, and see how it is formulated (and derived) in each framework.

Binary hypothesis testing and sphere-packing bounds

Gonzalo Vazquez Vilar

Universidad Carlos III de Madrid, Spain

ABSTRACT

The error probability of a binary hypothesis test with certain parameters has been shown to yield the exact error probability in the classical-quantum channel coding setting. This expression can be relaxed to obtain several converse bounds in the literature. In the classical setting, these bounds attain the sphere-packing exponent and provide insights on the structure of the optimal coding strategy. In this talk, we study the connections between binary hypothesis testing and sphere-packing bounds. We analyze the decision regions induced by these bounds in the channel coding problem.

Joint work with Albert Guillén i Fàbregas (ICREA, Universitat Pompeu Fabra, University of Cambridge), Sergio Verdú (Princeton University)

Semidefinite programming strong converse bounds for quantum channel capacities

Xin Wang

University of Technology Sydney, Australia

ABSTRACT

We show a meaningful theory of classical communication over quantum channels when assisted by no-signalling and PPT-preserving codes, for which both the optimal success probability of a given rate and one-shot ϵ-error capacity are formalized as semidefinite programs (SDPs). Based on this, we not only obtain improved SDP converse bounds on entanglement-assisted and unassisted codes, but also derive an SDP strong converse bound for the classical capacity. Remarkably, we derive improved upper bounds to the classical capacity of amplitude damping channels and establish the strong converse property for the classical and private capacities of a new class of quantum channels. We also use similar techniques to derive an SDP strong converse bound for the quantum capacity and show that it is always smaller than or equal to the "Partial transposition bound". We further demonstrate that our bound for quantum capacity is better than several previously known bounds for an explicit class of quantum channels.

Neyman-Pearson Test and Hoeffding Test

Shun Watanabe

Tokyo University of Agriculture and Technology, Japan

ABSTRACT

There are two important tests in the hypothesis testing problem: the Neyman-Pearson test and the Hoeffding test. In this talk, we first review asymptotic behaviours and geometric properties of these tests. Then, we move to the multi-terminal hypothesis testing problem in which only partial information of the sufficient statistics is available. We discuss the multi-terminal counterparts of the Neyman-Pearson test and the Hoeffding test. In particular, information geometrical properties of those test are elucidated.The talk is based on arXiv:1611.08175.

One shot entanglement assisted classical and quantum communication over noisy quantum channels: a hypothesis testing and convex split approach

Naqueeb Ahmad Warsi

National University of Singapore

ABSTRACT

In this work we study several communication tasks over noisy quantum channels and provide bounds on the amount of reliable communication between senders and receivers. Our results are in the one-shot setting with the extra resource of quantum entanglement between senders and receivers. We show 1) tight bounds on the amount of reliable communication for the *point-to-point channel*, 2) an achievability bound for point-to-point channel with quantum side information about the channel at the encoder (quantum analogue of the *Gel'fand-Pinsker* channel), 3) an achievability bound for point-to-point channel with limited quantum side information about the channel at the encoder, 4) an achievability bound for the *broadcast-channel*, a quantum analogue of the *Marton inner bound*. We take a unified approach to arrive at all our results, primarily using *hypothesis testing and convex split*. The forms of our results match with that of the corresponding results for similar communication tasks over noisy classical channels. To obtain the quantum analogue of Marton inner bound we prove a (bi-partite) generalization of the convex-split lemma, which may be of independent interest.

Information efficiency of local data hiding in quantum systems

Andreas Winter

Universitat Autònoma de Barcelona, Spain

ABSTRACT

We derive an upper bound on the number of bits that can be encoded into a bipartite system under the constraint of local data hiding, meaning that the information should be extractable by global operations, yet under the restriction of local operations and classical communication (LOCC) the parties cannot learn more than infinitesimally about it. As a corollary, we find that in any tight multipartite local data hiding scheme, the hidden information essentially cannot be larger than the size of the smallest relevant local share, showing that several constructions for bi- and multi-partite data hiding and quantum data hiding are asymptotically optimal regarding their information rate. This echoes a similar well-known statement about (classical) secret sharing: Namely, that the shared secret cannot be larger than the smallest relevant share. The proof relies on one-shot quantum information tools, including min-entropies and state merging.

AIFV codes and their extended codes

Hirosuke Yamamoto

The University of Tokyo, Japan

ABSTRACT

It is well known that the Huffman code is optimal in the class of uniquely decodable FV (fixed-to-variable length) codes if a single fixed code tree is used. However, we showed recently that the AIFV (almost instantaneous FV) code can attain better compression rate than the Huffman code for i.i.d sources. The binary (resp. K-ary) AIFV code uses two (resp. K-1) code trees. Since source symbols are assigned to incomplete internal nodes in addition to leaves, the AIFV codes are not instantaneous codes. But they are devised so that the decoding delay is at most two bits (resp. one code-symbol), and hence they are called "almost instantaneous". The binary AIFV code can be extended to the binary AIFV-m code with m code trees and at most m bit decoding delay. The worst-case redundancy of the binary Huffman code is one while that of the binary AIFV-m code is 1/m for m=2,3,4. We also introduce how to construct the optimal AIFV code for a given source, the total number of possible AIFV code trees, adaptive AIFV coding, and so on.

Compression of identically prepared quantum states

Yuxiang Yang

The University of Hong Kong, Hong Kong

ABSTRACT

We study the compression of arbitrary parametric families of n identically prepared finite- dimensional quantum states. For a family with f free parameters, we propose an asymptotically faithful protocol that requires a memory of overall size $(f/2)\log n$. Our construction uses a quantum version of local asymptotic normality and, as an intermediate step, solves the problem of the optimal compression of n identically prepared displaced thermal states. Our protocol achieves the ultimate bound predicted by quantum Shannon theory. In addition, we showed that the amount of quantum memory used by our protocol can be made arbitrarily small compared to the overall memory cost, while a protocol using only classical memory cannot faithfully encode the input state.

The additive classical capacity of quantum channels assisted by noisy entanglement

Quntao Zhuang

Massachusetts Institute of Technology, USA

ABSTRACT

We give a capacity formula for the classical information transmission over a noisy quantum channel, with separable encoding by the sender and limited resources provided by the receiver's preshared ancilla. Instead of a pure state, we consider the signal-ancilla pair in a mixed state, purified by a "witness". Thus, the signal-witness correlation limits the resource available from the signal-ancilla correlation. Our formula characterizes the utility of different forms of resources, including noisy or limited entanglement assistance, for classical communication. With separable encoding, the sender's signals across multiple channel uses are still allowed to be entangled, yet our capacity formula is additive. In particular, for generalized covariant channels our capacity formula has a simple closedform. Moreover, our additive capacity formula upper bounds the general coherent attack's information gain in various two-way quantum key distribution protocols. For Gaussian protocols, the additivity of the formula indicates that the collective Gaussian attack is the most powerful.