CEQIP 2014

11th CENTRAL EUROPEAN QUANTUM INFORMATION PROCESSING WORKSHOP

BOOK OF ABSTRACTS

http://ceqip.eu/2014

Invited speakers:
Fernando Brandao, Daniel Burgarth, Frédéric Dupuis, Ciara Morgan, Valerio Scarani, Giannicola Scarpa, Andreas Winter

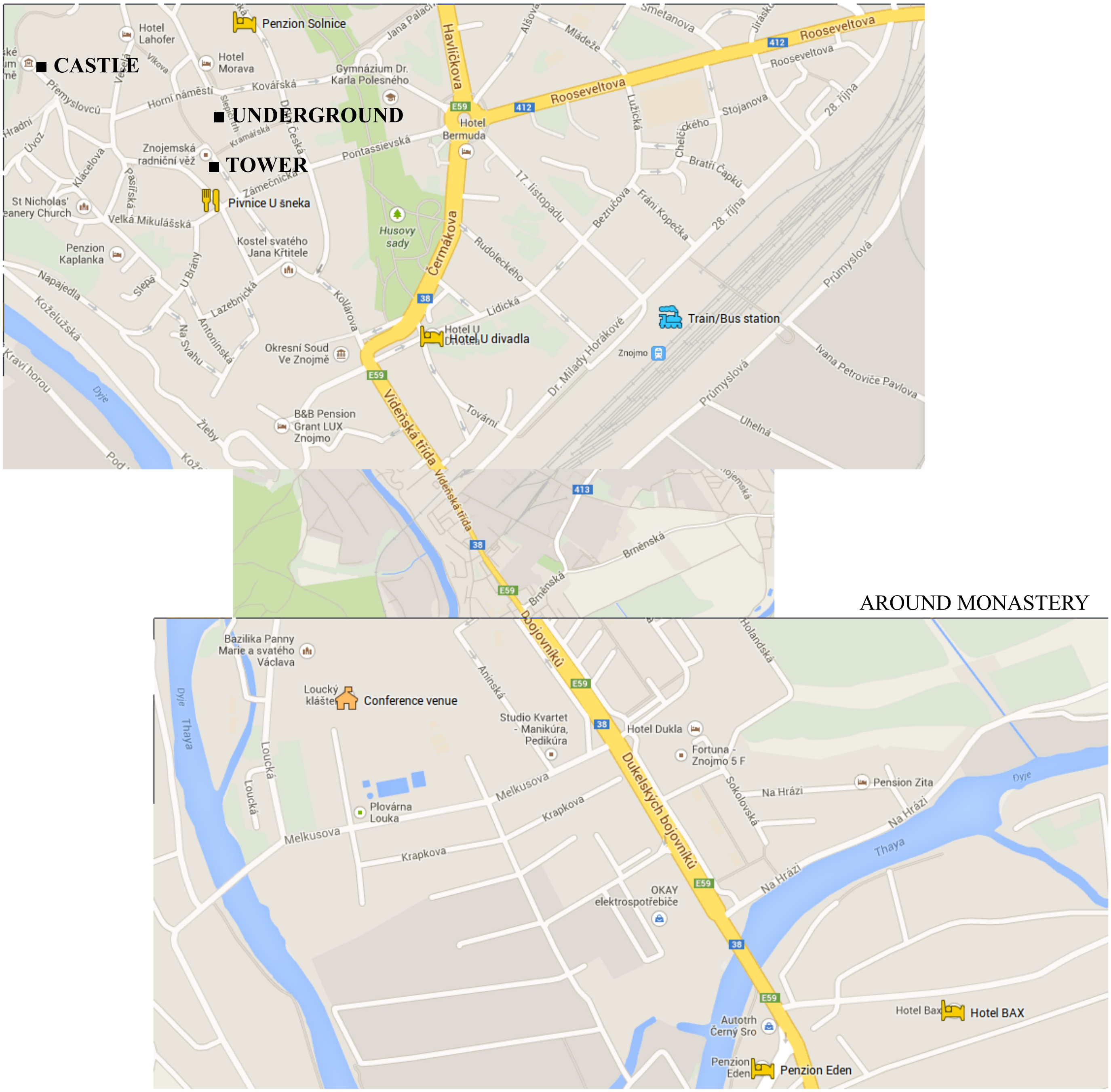
Program committee:
Andris Ambainis, Jan Bouda, Fernando Brandao, Frédéric Dupuis, Matyas Koniorczyk, Milan Mosonyi, David Reeb, Simone Severini, Ramon Munoz-Tapia, Mário Ziman

Orgs: Jan Bouda, Zuzana Komárková, Mário Ziman, Martina Zemanová

05-08 June 2014 **Znojmo, Czech Republic**

CONFERENCE MAP OF ZNOJMO

CITY CENTER



AROUND MONASTERY

WELCOME

Dear CEQIP participants,
welcome at CEQIP in Znojmo. If you encounter any problem do not hesitate to contact the organizers. In general, we are happy to help. Especially, if we can help.
Orgs.

CONFERENCE PROGRAM
Program is available at the end of this booklet. Everything should be written there.

CONFERENCE ADVENTURE
Saturday afternoon is reserved for get-together activities. As for the main attraction we plan to visit **Znojmo underground** (find street called *Slepičí trh*, the courtyard of house number 2 is the entrance). We have planned three tours. The first one is special (so-called adrenaline) and starts at 14:00 (be there 20 minutes before, because there is a small test of your physical conditions before). For this tour the number is limited to ten. Selection will be made according to currently unspecified criteria (being local is disadvantage, having good poster is an advantage). We are sorry, but due to local rules, we could not organize it for more people within one afternoon. The second and the third tours (each of them is for 40 people) are the typical ones and will start at 14:30 and 15:00. Please be there 10 minutes in advance. Otherwise you will miss your chance. The tour lasts one hour. The second place we plan to visit is the **town tower** (you should be able to find it). It will be open for us between 15:30-16:30 (have your badge with you). The visit takes at most 20 minutes and it is a nice exercise before the conference dinner. Last (optional) activity is the exhibition inside **Znojmo castle** (also this one is easy to notice). It is planned for at most 30 participants and please be there at 16:10 at latest. So if you wish to visit the castle please sign in for the underground tour starting at 14:30, or the adrenaline one.

During Thursday and Friday (somewhere at the conference room) you will find papers to sign in for all the activities (especially for the adrenaline underground tour and the castle). Do not hesitate too much with signing in. The selection of 10 lucky ones will be announced during Saturday's morning session. There will not be any selection for the castle tour unless too many of you apply, or too many of you come on time. Please keep in mind that it is approximatively 40 minutes walk from the monastery to underground entrance, or city center in general.

CIPHER GAME INVITATION
The goal is to find a phrase being the so-called CEQIP password. You can either guess it, or join the game itself. All players will be rewarded by unforgettable experience and the winners will receive nice prizes. It is a game for teams of 3-5 people. One of the first tasks (once the team is formed) is to name your team.

Cipher game will have two phases. Finding the start of the first phase (in city centre) is part of the game. Keep your eyes open during the activities and look for some CEQIP signs. There is no formal registration for the game at this stage. You can form teams either before, or even during this first phase. Whether you inform other players about the position of the starting cipher is up to you. Altogether there are three ciphers in this phase. The first one will point you to second, second to third, etc. Participating in the first phase give you an advantage for the second phase, however, it is not necessary to join the first phase. Please do not lose your advantage by explaining other teams how and what you found during the first phase.

The second phase starts at 20:00 during the conference dinner (registration at 19:45). At this phase you should register your team and you will receive some basic equipment (map, light and ciphering toolkit). The starting point will not be hidden (search for Mario Ziman). This phase consists of 4 ciphers located somewhere around the monastery and solution of cipher 7 reveals the magic phrase. Do not worry, playing does not mean to leave food and drinks for non-players. Your team can find a corner for its basecamp that is arbitrarily close to resources of all types. The game (this phase) is expected to take 1-3 hours. When you spent 30 minutes on the cipher you can ask for basic hints (not before 20:30 for cipher 3, 21:00 for cipher 4, 21:15 for cipher 5, 21:30 for cipher 6). More hints can be negotiated, but orgs will try to resist. Once you find the principle of the cipher it should not take you more than 10 minutes to solve it. No computers, or calculators are needed. Ciphers are in English of course. May fun be with you. Puzzles are everywhere.

INVITED SPEAKERS

Fernando Brandao

Limitations for quantum PCPS

An interesting current open problem in quantum complexity theory is the quantum PCP conjecture. In analogy with the PCP theorem, the conjecture states that it is QMA-hard to tell whether a quantum constraint satisfaction problem (aka a local quantum Hamiltonian) is satisfiable or far from satisfiable, with a constant fraction of the constraints being violated in any assignment. In this talk I will discuss limitations for quantum PCPs due to one of the most distinguishing features of quantum entanglement: its monogamous character. The monogamy of entanglement is the principle that the more entangled a system is with another one, the less entangled it can be with anything else. I will show how a quantitative understanding of entanglement monogamy leads both to limitations on the parameters that a potential quantum analogue of the PCP theorem might have, and to potential approaches to proving such an analogue (for instance by attempting to quantize the main steps of Dinur's proof of the PCP theorem). The talk will be mostly based on joint work with Aram Harrow (arXiv:1310.0017).

Andreas Winter

Weak locking capacity of quantum channels can be much larger than private capacity

We show that it is possible for the so-called weak locking capacity of a quantum channel [Guha et al., PRX 4:011016, 2014] to be much larger than its private capacity. Both reflect different ways of capturing the notion of reliable communication via a quantum system while leaking almost no information to an eavesdropper; the difference is that the latter imposes an intrinsically quantum security criterion whereas the former requires only a weaker, classical condition. The channels for which this separation is most straightforward to establish are the complementary channels of classical-quantum (cq-)channels, and hence a subclass of Hadamard channels. We also prove that certain symmetric channels (related to photon number splitting) have positive weak locking capacity in the presence of a vanishingly small pre-shared secret, whereas their private capacity is zero. These findings are powerful illustrations of the difference between two apparently natural notions of privacy in quantum systems, relevant also to quantum key distribution (QKD): the older, naive one based on accessible information, contrasting with the new, composable one embracing the quantum nature of the eavesdropper's information. Assuming an additivity conjecture for constrained minimum output Renyi entropies, the techniques of the first part demonstrate a single-letter formula for the weak locking capacity of complements to cq-channels, coinciding with a general upper bound of Guha et al. for these channels. Furthermore, still assuming this additivity conjecture, this upper bound is given an operational interpretation for general channels as the maximum weak locking capacity of the channel activated by a suitable noiseless channel. [arXiv:1403.6361]

Valerio Scarani

Randomness from quantum systems: a guided tour

What are randomness generation, expansion, and amplification? Under which assumptions does quantum physics provide "better" randomness than classical? Do Bell inequalities really allow us to buy our cryptographic apparatus from the enemy? Are all "experimental demonstrations" of randomness meaningful? This talk will review these questions. References: arXiv:1303.3081 (lecture notes on device-independence), arXiv:1401.4243v2

Frédéric Dupuis

Bounding the uncertainty of constrained adversaries

In many cryptographic protocols, the main ingredient of the security proof involves showing that a dishonest party has a limited amount of information about a particular string or quantum system of interest. This bound on the adversary's information often comes from a physical constraint, such as a limited or noisy quantum memory, which must then be harnessed by the security proof. In this talk, I will present a general technique for making use of this type of constraint in security proofs, and will give concrete applications to cryptography in the bounded storage model and to bounds on random-access codes. For more information, see arXiv:1305.1316. (Joint work with Omar Fawzi and Stephanie Wehner)

Daniel Burgarth

Quantum Computing in Plato's Cave

We show that mere observation of a quantum system can turn its dynamics from a very simple one into a universal quantum computation. This effect, which occurs if the system is regularly observed at short time intervals, can be rephrased as a modern version of Plato's Cave allegory. More precisely, while in the original version of the myth, the reality perceived within the Cave is described by the projected shadows of some more fundamental dynamics which is intrinsically more complex, we found that in the quantum world the situation changes drastically as the "projected" reality perceived through sequences of measurements can be more complex than the one that originated it. After discussing examples we go on to show that this effect is generally to be expected: almost any quantum dynamics will become universal once "observed" as outlined above. Conversely, we show that any complex quantum dynamics can be "purified" into a simpler one in larger dimensions.

Giannicola Scarpa
Graphs, classical channels and nonlocality: the interplay
Certain graph parameters, like the independence number and the chromatic number, can be redefined as nonlocal games. When the players of the game are allowed to share entanglement, we obtain the notion of quantum graph parameters. There are graphs for which such quantities exhibit a different behaviour. Interestingly, this property is reflected in zero-error information theory, where noisy classical channels are studied through their confusability graphs. We will see an application of this idea, but there is more: quantum graph parameters also help us in the study of nonlocality in general. We will see how every nonlocal game has a characteristic "game graph" and how different parameters provide information about the winning probability of quantum and classical strategies.

Ciara Morgan
Additivity and quantum channel capacity: an old problem revisited
One of the fundamental tasks in quantum information theory is to establish the capacity of noisy quantum channels, that is, the maximum rate at which information can be transmitted from one party to another over the channel with vanishing error. In this talk we focus on the task of classical information transmission and revisit the additivity problem, providing an overview of the current state and presenting new results involving the amplitude damping channel. Based on joint work with Tony Dorlas.

CONTRIBUTED TALKS

Juan Bermejo-Vega, Cedric Yen-Yu Lin and Maarten Van den Nest
The computational power of normalizer circuits over ∞ Abelian groups
Normalizer circuits are a family of quantum circuits that generalize Clifford circuits to Hilbert spaces associated with finite Abelian groups. They can be efficiently simulated classically although they may involve quantum Fourier transforms, logic gates that are essential in Shor's factoring algorithm. In this work, we consider extended classes of normalizer circuits over infinite groups and black-box groups. We characterize the computational power of these black-box normalizer circuits, showing that they can achieve exponential quantum speed-ups and implement several celebrated quantum algorithms, including Shor's. This yields a precise formal connection between Clifford/normalizer circuits and the latter famous quantum algorithms.

Rafael Chaves, Lukas Luft, Thiago O. Maciel, David Gross, Dominik Janzing and Bernhard Schölkopf
An Entropic Approach to Causal Inference and Applications to Nonlocality and Machine Learning
Bell's theorem in physics, as well as causal discovery in machine learning, both face the problem of deciding whether observed data is compatible with presumed causal relationships. The main problem to be circumvented comes from the fact that, in terms of probabilities, causal relations introduce non-linear constraints. Those lead to non-convex compatibility regions that are very difficult to be characterized. Here, we advocate analyzing the joint entropies of observed variables for the purpose of causal inference. The entropy region associated with any given causal constraints is a convex polyhedron - a relatively simple geometric object, described completely by finitely many linear inequalities. Entropic relations naturally describe causal relationships while still retaining quantitative and useful information about causation. In this work we provide a general algorithm and discuss its application in machine learning and quantum nonlocality problems.

Julio De Vicente, Cornelia Spee and Barbara Kraus
The maximally entangled set of multipartite quantum states
Entanglement is a resource in quantum information theory when state manipulation is restricted to Local Operations assisted by Classical Communication (LOCC). It is therefore of paramount importance to decide which LOCC transformations are possible and, particularly, which states are maximally useful under this restriction. While the bipartite maximally entangled state is well known, no such state exists in the multipartite case. In order to cope with this fact, we introduce here the notion of the Maximally Entangled Set (MES) of n-partite states. This is the set of states which are maximally useful under LOCC manipulation. We study LOCC transformations in the multipartite realm, determine the MES for states of three and four qubits and provide a simple characterization for them.

Sergey Filippov and Mário Ziman

Dissociation and annihilation of multi-partite entanglement structures

We study the entanglement structure dynamics of multipartite system experiencing a dissipative evolution. We characterize processes leading to a particular form of output system entanglement and provide a recipe for their identification via concatenations of peculiar linear maps with entanglement-breaking operations. We illustrate the applicability of our approach by considering local and global depolarizing noises for multi-qubit systems and local Gaussian noisy channels for infinite quantum systems. The difference in typical entanglement behavior of systems subjected to these noises is observed: the originally genuine entanglement dissociates by splitting particles one by one in case of local noise, whereas the intermediate stages of entanglement clustering are present in case of global noise. We also analyze the definitive phase of evolution when the annihilation of entanglement compound finally takes place. Further, the characterization of local Gaussian channels from entanglement-annihilation perspective is given. In particular, it is shown that when restricted to Gaussian input states, the local entanglement-annihilation channels is asymptotically (in the limit of infinite number of modes) different from local entanglement-breaking property. This work is mainly based on Ref. [PRA 88, 062328 (2013), arXiv:1310.4790].

Daniela Frauchiger, Renato Renner and Matthias Troyer

True Randomness from Realistic Quantum Devices

Even if the output of a Random Number Generator (RNG) is perfectly uniformly distributed, it may be correlated to pre-existing information and therefore be predictable. Statistical tests are thus not sufficient to guarantee that an RNG is usable for applications, e.g., in cryptography or gambling, where unpredictability is important. To enable such applications a stronger notion of randomness, termed "true randomness", is required, which includes independence from prior information. Quantum systems are particularly suitable for true randomness generation, as their unpredictability can be proved based on physical principles. Practical implementations of Quantum RNGs (QRNGs) are however always subject to noise, i.e., influences which are not fully controlled. This reduces the quality of the raw randomness generated by the device, making it necessary to post-process it. Here we provide a framework to analyse realistic QRNGs and to determine the post-processing that is necessary to turn their raw output into true randomness.

Erkka Haapasalo, Michal Sedlák and Mário Ziman

Boundariness and minimum-error discrimination

We introduce the concept of boundariness capturing the most efficient way of expressing a given element of a convex set as a probability mixture of its boundary elements. In other words, this number measures (without the need of any explicit topology) how far the given element is from the boundary. It is shown that one of the elements from the boundary can be always chosen to be an extremal element. We focus on evaluation of this quantity for quantum sets of states, channels and observables. We show that boundariness is intimately related to (semi)norms that provide an operational interpretation of this quantity. In particular, the minimum error probability for discrimination of a pair of quantum devices is lower bounded by the boundariness of each of them. We prove that for states and observables this bound is saturated and conjectured this feature for channels. The boundariness is zero for infinite-dimensional quantum objects as in this case all the elements are boundary elements. The complete paper linked to this submission is arXiv:1401.7460 [quant-ph].

Josh Cadney, Marcus Huber, Noah Linden and Andreas Winter

Inequalities for the Ranks of Quantum States

We investigate relations between the ranks of marginals of multipartite quantum states. These are the Schmidt ranks across all possible bipartitions and constitute a natural quantification of multipartite entanglement dimensionality. We show that there exist inequalities constraining the possible distribution of ranks. This is analogous to the case of von Neumann entropy (α-Renyi entropy for $\alpha=1$), where nontrivial inequalities constraining the distribution of entropies (such as e.g. strong subadditivity) are known. It was also recently discovered that all other \alpha-Renyi entropies for all $\alpha\neq1$ satisfy only one trivial linear inequality (non-negativity) and the distribution of entropies for $0<\alpha<1$ is completely unconstrained beyond non-negativity. Our result resolves an important open question by showing that also the case of $\alpha=0$ (logarithm of the rank) is restricted by nontrivial linear relations and thus the cases of von Neumann entropy (i.e., $\alpha=1$) and 0-Renyi entropy are exceptionally interesting measures of entanglement in the multipartite setting.

Mária Kieferová and Nathan Wiebe

On The Power Of Coherently Controlled Quantum Adiabatic Evolutions

A major challenge facing adiabatic quantum computing is that algorithm design and error correction can be difficult for adiabatic quantum computing. Recent work has considered addressing this challenge by using coherently controlled adiabatic evolutions in the place of classically controlled evolution. An important question remains: what is the relative power of controlled adiabatic evolution to traditional adiabatic evolutions? We address this by showing that coherent control and measurement provides a way to average different adiabatic evolutions in ways that cause their diabatic errors to cancel, allowing for adiabatic evolutions to combine the best characteristics of existing adiabatic optimizations strategies that are mutually exclusive in conventional adiabatic QIP. This result shows that coherent control and measurement can provide advantages for adiabatic state preparation. We also provide upper bounds on the complexity of simulating such evolutions on a circuit based quantum computer and provide sufficiency conditions for the equivalence of controlled adiabatic evolutions to adiabatic quantum computing. http://arxiv.org/abs/1403.6545

Richard Kueng and David Gross

Stabilizer states are complex projective 3-designs

A complex projectivel t-design is a configuration of vectors which is "evenly distributed" on a sphere in the sense that it reproduces Haar measure up to t-th moments. Here, we show that the set of all n-qubit stabilizer states forms a complex spherical 3-design in dimension 2n. In addition to this we prove that this statement is wrong for quidits. Stabilizer states had previously only been known to constitute 2-designs. The problem is reduced to the task of counting the number of stabilizer states with pre-described overlap with respect to a reference state. This, in turn, reduces to a counting problem in discrete symplectic vector spaces for which we find a simple formula.

John Lapeyre

The role of local and global geometry in quantum entanglement percolation

We prove that enhanced entanglement percolation via lattice transformation is possible even if the new lattice is more poorly connected in that: i) the coordination number (a local property) decreases, or ii) the classical percolation threshold (a global property) increases. In searching for protocols to transport entanglement across a network, it seems reasonable to try transformations that increase connectivity. In fact, all examples that we are aware of violate both conditions i and ii. One might therefore conjecture that all good transformations must violate them. Here we provide a counter-example that satisfies both conditions by introducing a new method, partial entanglement swapping. This result shows that a transformation may not be rejected on the basis of satisfying conditions i or ii. Both the result and the new method constitute steps toward answering basic questions, such as whether there is a minimum amount of local entanglement required to achieve long-range entanglement.

Alexander Müller-Hermes, David Reeb and Michael Wolf

Quantum Subdivision Capacities and Continuous Quantum Coding

Quantum memories can be regarded as quantum channels that transmit information through time without moving it through space. Aiming at a reliable storage of information we may thus not only encode at the beginning and decode at the end, but also intervene during the transmission -- a possibility not captured by the ordinary capacities in Quantum Shannon Theory. In this work we introduce capacities that take this possibility into account and study them in particular for the transmission of quantum information via dynamical semigroups of Lindblad form. When the evolution is subdivided and supplemented by additional continuous semigroups acting on arbitrary block sizes, we show that the capacity of the ideal channel can be obtained in all cases. If the supplementary evolution is reversible, however, this is no longer the case. Upper and lower bounds for this scenario are proven. Finally, we provide a continuous coding scheme and simple examples showing that adding a purely dissipative term to a Liouvillian can sometimes increase the quantum capacity.

Marcin Pawlowski, Nicolas Brunner and Joseph Bowles

Dimension Witness Networks

The problem of estimating the dimension of an unknown physical system has attracted attention recently. In particular, a framework was presented for the simplest case of a prepare-and-measure scenario. Such a setup features two devices. First a preparation device, which allows the observers to prepare a physical system in various (but uncharacterized) ways. Second, a measurement device, which allows the observer to perform an (uncharacterized) measurement on the prepared physical system. It is then possible to find the minimal dimension, for describing the physical system, that is compatible with the data, i.e. the frequencies of obtaining a certain measurement outcome for a given choice of preparation and measurement. Techniques tailored for classical, and quantum systems were reported, as well as for the case in which the devices are assumed to be independent. An interesting features of these techniques is that they can certify the use of quantum systems under the assumption that the system's dimension is upper bounded. These ideas were also shown to be relevant in practice, as well as for quantum information processing. More generally, it is desirable to consider a scenario featuring several preparation and/or measurement devices. Moreover, one may also consider another type of device, namely a transformation device. Such a device allows the observer to perform one out several possible uncharacterized transformations on a physical system. Here we present a framework for testing dimensionality and quantumness in networks consisting of preparation, transformation, and measurement devices. For the simplest case, i.e. a network featuring 2 devices, there is only one relevant configuration, namely the previously studied prepare-and-measure scenario. For a network featuring N>2 devices, many different configurations are possible, hence leading to a rich structure. Here we discuss in detail the case of networks consisting of 3 devices, and show a series of interesting new phenomenon. In this case of 3 devices, there are 3 relevant configurations : (i) one preparation device, two measurement devices, (ii) one preparation device, two measurement devices, and (iii) one preparation device, one transformation device, and one measurement device. Configuration (i) is basically a Bell test scenario, which have been well studied. Configuration (ii) can be viewed as a dual (or time-reversed Bell test), and has been discussed in the context of testing entangled measurements, as well as the context of the PBR theorem. Configuration (iii) has not been investigated in the present context, to the best of our knowledge. We will discuss examples of each of these configurations where the advantage offered by quantum systems over classical ones (of the same dimension) is enhanced compared to the simple prepare-and-measure scenario. This suggests that the problem of simulating the statistics of quantum networks with classical systems, will require classical systems of extremely high dimension.

Jan Bouda, Marcin Pawlovski, Matej Pivoluska and Martin Plesch

Device-independent randomness extraction for arbitrarily weak min-entropy source

Expansion and amplification of weak randomness plays a crucial role in many security protocols. Using quantum devices, such procedure is possible even without trusting the devices used, by utilizing correlations between outcomes of parts of the devices. We show here how to extract random bits with an arbitrarily low bias from a single arbitrarily weak min-entropy source in such a device independent setting. To do this we use Mermin devices that exhibit super-classical correlations. Number of devices used scales polynomially in the length of the random sequence n, containing entropy of at least two bits. Our protocol is robust, it can tolerate devices that malfunction with a probability dropping polynomially in n at the cost of constant increase of the number of devices used. Full paper can be found on [arXiv 1402.0974].

David Reeb and Peter Vrana

Trace-norm contraction under tensor product channels

We examine upper bounds on the information storage time in a quantum memory under independent noise in the case where active error correction is allowed. For this, we provide an upper bound on the trace-norm contraction coefficient of a tensor product of quantum channels. Our method yields nontrivial bounds in cases where others fail. We also investigate the behaviour of all bounds under taking tensor products. Specializing to qubit channels, this solves a conjecture by Ben-Or/Gottesmann/Hassidim (arXiv:1301.1995).

Tomáš Rybár and Mário Ziman.

Estimation in presence of memory effects

When memory effects are present the estimation cannot be based on repetitions of statistically independent experimental runs, hence new methods of data analysis must be developed. Under the assumption of ergodicity of the evolution of the memory system we design an estimation algorithm to estimate the parameters of the interaction between the memory and the input systems. No control over the memory is assumed and the experimenter has no access to it. We also prove that for control unitary interactions (in that case the evolution of memory is not ergodic) the experimenter can only learn at most one of the local unitaries and cannot spot any memory effects. Note that the considered estimation problem is different from estimation of matrix product states (which can be used to describe the action of memory channels), because in our consideration we do not have access to copies of the matrix product state, hence, memory process estimation does reduce to single-copy MPS estimation.

Martin Schwarz and Maarten Van Den Nest

Simulating Quantum Circuits with Sparse Output Distributions

We show that several quantum circuit families can be simulated efficiently classically if it is promised that their output distribution is approximately sparse i.e. the distribution is close to one where only a polynomially small, a priori unknown subset of the measurement probabilities are nonzero. Classical simulations are thereby obtained for quantum circuits which—without the additional sparsity promise—are considered hard to simulate. Our results apply in particular to a family of Fourier sampling circuits (which have structural similarities to Shor's factoring algorithm) but also to several other circuit families, such as IQP circuits. Our results provide examples of quantum circuits that cannot achieve exponential speed-ups due to the presence of too much destructive interference i.e. too many cancelations of amplitudes. The crux of our classical simulation is an efficient algorithm for approximating the significant Fourier coefficients of a class of states called computationally tractable states. The latter result may have applications beyond the scope of this work. In the proof we employ and extend sparse approximation techniques, in particular the Kushilevitz-Mansour algorithm, in combination with probabilistic simulation methods for quantum circuits.

Alessandro Tosini, Giacomo D'Ariano, Paolo Perinotti and Franco Manessi.

The Feynman problem and Fermionic entanglement: Fermionic theory versus qubit theory

We consider the relations between Fermionic theories and qubits theories, both regarded in the novel framework of operational probabilistic theories. On the computational side the two theories are equivalent, as shown by Bravyi and Kitaev in Annals of Physics 298, 210 (2002). On the operational side the quantum theory of qubits and the quantum theory of Fermions are different, mostly in the notion of locality, with relevant consequences on the informational features of the Fermionic systems. We show that the computational model based on local Fermionic modes in place of qubits does not satisfy local tomography and monogamy of entanglement allowing for mixed states with maximal entanglement of formation.

LIST OF POSTERS

Miroslav Gavenda, Lucie Celechovská, Miloslav Dušek and Radim Filip

Quantum noise eater for a single photonic qubit

We propose quantum noise eater for a single photonic qubit and experimentally verify its performance for recovery of a superposition carried by a dual-rail photonic qubit. A coherent but randomly arriving photon penetrating into single rail of this system causes a change of its state, which results in an error in subsequent quantum information processing. We theoretically prove and experimentally demonstrate a conditional full recovery of the superposition by the quantum noise eater.

Gábor Balló and Katalin Hangos

Experiment design for d-level Pauli channel estimation

The optimal experiment design problem for the quantum process tomography of Pauli channels is studied here for d-level channels, where d can be any prime number. The problem is formulated as an optimization problem, where the objective is the Fisher information of the channel parameters, and the decision variable is an experiment configuration consisting of an input quantum state and a POVM used for measurements. It is shown that the optimal experiment configurations are pure state--extremal POVM pairs which are elements of the complementary subalgebras used to define the channel.

Dariusz Kurzyk and Piotr Gawron

Quantum queuing networks

We study models for quantum queues based on discrete time quantum random walks. Our considerations refer to multi-servers queueing models. Input and output of jobs in the queue are realized by systems consisting of coins and walkers. We presents numerical methods for optimization of transitions of jobs in the queues. We assume maximization of flow of jobs into the queue and minimization number of lost jobs in the same time. Next, we show that presented models behaves differently from the classical one.

Przemysław Sadowski

Grover's search on Apollonian networks

In this work we provide a quantum search algorithm on Apollonian network. We show that such networks are sufficient for search tasks due to the small-world and scale-free properties.In particular we present a strategy that allows to design measurement rules that remains effective regardless of the marked node.We derive the optimal measurement step for the repeatable search approachand we estimate the complexity of the introduced algorithm.

Bálint Kollár and Mátyás Koniorczyk

Entropy rate of discrete time quantum walks

The amount of information generated in a single step of a discrete time stochastic process can be quantified by the so-called entropy rate. We study a quantum process, bearing a well defined classical correspondence: the periodically measured quantum walk. The limit of measuring the discrete time quantum walk in every steps results the complete loss of quantum interference, i. e. a classical walk. We investigate the differences between such quantum and classical walks in the terms of the entropy rate. We develop general analytical methods for the approximation and exact calculation of the entropy rate. We aim to take a step toward investigating the information production of simple physical systems, at the boundaries of the classical and quantum world.

Łukasz Pawela and Przemysław Sadowski

Different methods of optimizing control pulses for quantum systems with decoherence

We study three methods of obtaining an approximation of unitary evolution of a quantum system under decoherence. We use three methods of obtaining the piecewise constant control pulses: genetic optimization, approximate evolution method and approximate gradient method. To incorporate noise in our model we use the Lindblad equaiton for he time evolution of our system. We obtain results showing that genetic optimization may give a better approximation of a unitary evolution in the case of high noise.

Shenggen Zheng

Revisit superiority of exact quantum automata for promise problems

In this paper, we generalize the promise problem studied by Ambainis and Yakaryilmaz [Information Processing Letters 112 (2012) 289--291]. Let $A_{yes}^{N,\,l}=\{a^{iN}\,|\,\ i\geq 0\}$ and $A_{no}^{N,\,l}=\{a^{iN+l}\,|\,\ i\geq 0\}$, where N and l are fixed positive integers such that $0< l< N$. If we choose $N= 2^{k+1}$ and $l=N/2$, then $A^{N,\,l}$ is exactly the promise problem studied by Ambainis and Yakaryilmaz. We prove that the promise problem $A^{N,\,l}=(A_{yes}^{N,\,l},A_{no}^{N,\,l})$ can be solved exactly by a measure-once one-way quantum finite automaton (MO-1QFA) with three basis states. If N is a prime, then the minimal DFA solving promise problem $A^{N,\,l}$ has N states. Furthermore, we prove that for any positive integer N, the minimal DFA solving the promise problem $A^{N,\,l}$ has d states, where d is the smallest integer such that $d\mid N$ and $d\nmid l$.

Martin Plesch and Matej Pivoluska

Device Independent Amplification of a Single Min--Entropy Random Source

Expansion and amplification of weak randomness with the help of untrusted quantum devices has recently become a very fruitful topic of current research. Here we contribute with a procedure for amplifying a single weak random source with the help of tri-partite GHZ-type entangled states. If the quality of the source measured in min--entropy rate reaches a fixed threshold 1/4 log$_2$10, perfect random bits can be produced. Unlike recent papers dealing with the problem of min-entropy amplification, our protocol works as few as three non-communicating devices [arXiv:1305.0990].

Cosmo Lupo, Mark Wilde and Seth Lloyd

From quantum data locking to the quantum enigma machine

Quantum data locking is a unique quantum phenomenon that allows a relatively short key to (un)lock an arbitrarily long message encoded in a quantum state, in such a way that an eavesdropper who measures the state but does not know the key has essentially no information about the encrypted message. The application of quantum data locking in cryptography would allow one to overcome the limitations of the one-time pad encryption, which requires the key to have the same length as the message. However, one may notice that the strength of quantum data locking is also its Achilles heel, as the leakage of a few qubits of the key or the message may in principle allow the eavesdropper to unlock a disproportionate amount of information. In this paper we show that quantum data locking can be made resilient against information leakage simply by increasing the length of the shared key by a proportionate amount. This implies that a constant size key can still encrypt an arbitrary long message as long as a fraction of it remains secret to the eavesdropper. Moreover, we greatly simplify the structure of the protocol by proving that phase modulation suffices to generate strong locking schemes, paving the way to optical experimental realizations. Also, we show that successful data locking protocols can be constructed using random codewords, which very well could be helpful in discovering random codes for data locking of noisy quantum channels.

Mikko Tukiainen and Teiko Heinosaari.

Quantum programming and compression

Our work is on the effectiveness of quantum measurements. We tackle this problem from two different angles: how much can be measured with a single measurement device and how large it should be to be able to perform given tasks? These two topics are captured in the theory of the programmable quantum multimeters and the minimal measurement dilation respectively -- our results clarify these two points of view. Furthermore we unify these aspects to give limits to efficient quantum programming.

Karen V. Hovhannisyan, Marti Perarnau-Llobet, Marcus Huber and Antonio Acin

The role of entanglement in work extraction

We consider reversible work extraction from identical quantum systems. From an ensemble of individually passive states, work can be produced only via global unitary (and thus entangling) operations. However, we show here that there always exists a method to extract all possible work without creating any entanglement, at the price of generically requiring more operations (i.e., additional time). We then study faster methods to extract work and provide a quantitative relation between the amount of generated multipartite entanglement and extractable work. Our results suggest a general relation between entanglement generation and the power of work extraction.

Sergey Filippov and Mário Ziman
To fight fire with fire: a tale of how local noise prolongs entanglement lifetime
Quantum technologies are based on coherent dynamics of quantum systems. The inevitable interaction with environment is a challenge toward the future development. As concerns individual quantum systems, the techniques of dynamic decoupling are often used to prevent them from decoherence. However, as far as entangled composite systems are concerned, one resorts to a global control of the system. In this case, not only unitary manipulations can be used, for instance, common baths that drive the system in a non-unitary way to some entangled state are widely known. The question of interest is the following: can one locally intervene in the decoherence process to save global entanglement? In our report, we show that the answer is positive. The local actions should not be unitary in general, which means that additional noise can diminish the effect of entanglement degradation.

Ryszard Weinar, Marcin Pawlowski
Security of SDI protocol
Random access codes allow to build communication protocols in which we do not trust devices and only the probability of success is a safety parameter. When the detectors are perfect and the probability of correct decoding is greater than 75% the communication is safe. Not perfect detectors provide excellent opportunities for Eve to attack by deliberate blanking detectors in a way they are expected to work and, at the same time, allowing to read the maximum amount of transmitted key by Eve. In this work we present security conditions for SDI protocols based on RAC with two parameters – probability of success and efficiency of the detectors. Protocols based on RAC 2to1 and RAC 3to1 are considered.

Nikolajs Nahimovs, Andris Ambainis and Renato Portugal
Spatial Search on Grids with Minimum Memory
We study quantum algorithms for spatial search on finite dimensional grids. Patel et al. and Falk have proposed algorithms based on a quantum walk without a coin, with different operators applied at even and odd steps. Until now, such algorithms have been studied only using numerical simulations. We present the first rigorous analysis for an algorithm of this type, showing that the optimal number of steps is O(\sqrt{N logN}) and the success probability is O(1/logN), where N is the number of vertices. This matches the performance achieved by algorithms that use other forms of quantum walks.

Stefan Schauer and Martin Suda
On the Optimality of Basis Transformations to Secure Entanglement Swapping Based QKD Protocols
In this contribution, we discuss the optimality of basis transformations as a security measure for quantum key distribution protocols based on entanglement swapping. To estimate the security, we focus on the information an adversary obtains on the raw key bits from a generic version of a collective attack strategy. In this context, we show that the angles, which describe the basis transformations, can be optimized compared to the application of a Hadamard operation, which is the standard basis transformation recurrently found in literature. As a main result, we show that the adversary's information can be reduced to an amount of $I_{AE} \simeq 0.20752$ when using one single and to an amount of $I_{AE} \simeq 0.0548$ when combining two different basis transformations.

Piotr Gawron, Łukasz Pawela and Zbigniew Puchała
Restricted numerical ranges and numerical shadows - numerical methods
The poster presents recent developments in the numerical methods useful for approximation of restricted numerical ranges and restricted numerical shadows. Restricted numerical range of a given matrix is a generalization of the concept of numerical range. It can be defined as the set of all complex numbers that are obtained from the overlap of a given matrix with unit product vectors. Given a measure on the set of those vectors one can extend this notion to restricted numerical shadow. For more information please refer to www.numericalshadow.org.

Sandra Rankovic, Yeong-Cherng Liang and Renato Renner
The alternate ticks time game
Time, considered as a classical parameter, has always played a special role both in classical and in non-relativistic quantum mechanical descriptions of physical systems. But is this parametric view of time unavoidable? By constructing a suitable quantum game, we outline an attempt to introduce a new, more general, operational notion of time, and investigate limitations of its measurement in quantum theory.

László Ruppert, Vladyslav Usenko and Radim Filip

Long-distance continuous-variable quantum key distribution with efficient channel estimation

We investigate the main limitations which prevent the continuous-variable quantum key distribution protocols from achieving long distances in the finite-size setting. We propose a new double modulation protocol, which allows using each state for both channel estimation and key distribution. As opposed to the standard method, we optimize the parameters of the protocol and consider squeezed as well as coherent states as a signal. By optimally combining the resources the key rate can approach the theoretical limit for long distances and one can obtain about 10 times higher key rate using 10 times shorter block-size than the current state of the art method.

Subhadipa Das, Manik Banik, Md. Rajjak Gazi, Ashutosh Rai and Samir Kunkri

Local Orthogonality provides better upper bound for Hardy's nonlocality

The amount of nonlocality in quantum theory is limited compared to that allowed in generalized no-signaling theory [Found. Phys. 24, 379 (1994)]. This feature, for example, gets manifested in the amount of Bell inequality violation as well as in the degree of success probability of Hardy's (Cabello's) nonlocality argument. Physical principles like information causality and macroscopic locality have been proposed for analyzing restricted nonlocality in quantum mechanics---viz. explaining the Cirel'son bound. However, these principles are not that much successful in explaining the maximum success probability of Hardy's as well as Cabello's argument in quantum theory. Here we show that, a newly proposed physical principle namely Local Orthogonality does better by providing a tighter upper bound on the success probability for Hardy's nonlocality. This bound is relatively closer to the corresponding quantum value compared to the bounds achieved from other principles.

Felipe G. Lacerda, Joseph M. Renes and Renato Renner

Classical leakage resilience from fault-tolerant quantum computation

Physical implementations of cryptographic algorithms leak information, which makes them vulnerable to so-called side-channel attacks. The problem of secure computation in the presence of leakage is generally known as leakage resilience. In this work, we establish a connection between leakage resilience and fault-tolerant quantum computation. We first show that for a general leakage model, there exists a corresponding noise model in which fault tolerance implies leakage resilience. Then we show how to utilize specific constructions for fault tolerant quantum computation to construct classical circuits which are secure in the independent leakage model.

Nicolai Friis, Vedran Dunjko, Wolfgang Dür and Hans J. Briegel

Implementing quantum control for unknown subroutines

We present setups for the practical realization of adding control to unknown subroutines, supplementing the existing quantum optical scheme for black-box control with a counterpart for the quantum control of the ordering of sequences of operations. We also provide schemes to realize either task using trapped ions. These practical circumventions of recent no-go theorems are based on existing technologies. We argue that the possibility to add control to unknown operations in practice is a common feature of many physical systems. Based on the proposed implementations we discuss the apparent contradictions between theory and practice.

Michal Mičuda, Michal Sedlák, Ivo Straka, Martina Miková, Miloslav Dušek, Miroslav Ježek and Jaromír Fiurášek

Efficient estimation of fidelity of N-qubit controlled-Z gates

We propose an efficiently measurable lower bound on quantum process fidelity of N-qubit controlled-Z gates. This bound is determined by average output state fidelities for N partially conjugate product bases. A distinct advantage of our approach is that only fidelities with product states need to be measured while keeping the total number of measurements much smaller than what is necessary for full quantum process tomography. As an application, we use this method to experimentally estimate quantum process fidelity F of a three-qubit linear optical quantum Toffoli gate and we find that $F > 0.83$.

Tom Bullock and Paul Busch

Joint position-momentum measurements with entangled probes

In this talk we discuss how using entangled probes in an Arthurs-Kelly measurement model can allow for sequential measurements that are more precise than those performed in the case of individual measurements. Further to this, it is shown that for any preparation of the state of the probes, the observable derived from an Arthurs-Kelly model is covariant under phase space translations, and as such any approximate position and momentum observables derived from an Arthurs-Kelly measurement model must satisfy Heisenberg's error-disturbance relation.

Denis Vasilyev, Sebastian Hofer and Klemens Hammerer

Time-Continuous Bell Measurements

We combine the concept of Bell measurements, in which two systems are projected into a maximally entangled state, with the concept of continuous measurements, which concerns the evolution of a continuously monitored quantum system. For such time-continuous Bell measurements we derive the corresponding stochastic Schrödinger equations, as well as the unconditional feedback master equations [PRL 111, 170404 (2013)]. Our results apply to a wide range of physical systems, and are easily adapted to describe an arbitrary number of systems and measurements. Time-continuous Bell measurements therefore provide a versatile tool for the control of complex quantum systems and networks. As examples we show that (i) two two-level systems can be deterministically entangled via homodyne detection, tolerating photon loss up to 50%, and (ii) a quantum state of light can be continuously teleported to a mechanical oscillator, which works under the same conditions as are required for optomechanical ground-state cooling.

Waldemar Klobus, Andrzej Grudka, Karol Horedecki, Michal Horodecki and Marcin Pawłowski

Relation between random access codes and (non-)signaling boxes

We study a problem of interconvertibility of two supra-quantum resources: one is so called PRbox,which violates CHSH inequality up to maximal algebraic bound, and second is so called random access code (RAC) - a functionality that enables Bob (receiver) to choose one of two bits of Alice. To this end we introduce racbox: a box such that supplemented with one bit of communication oers RAC. It has been known, that PR-box supplemented with one bit of communication can be used to simulate RAC. The question we raise is the converse: can any racbox can simulate PR-box? We show that a non-signaling racbox indeed can simulate PR-box, hence the two resources are equivalent. We also provide an example of signalling racbox which cannot simulate PR-box, and also present a resource inequality between racboxes and PR-boxes.

Martina Miková, Michal Sedlák, Ivo Straka, Michal Mičuda, Mário Ziman, Miroslav Ježek, Miloslav Dušek and Jaromír Fiurášek

Optimal entanglement-assisted discrimination of quantum measurements

We investigate optimal discrimination between two projective single-qubit measurements in a scenario where the measurement can be performed only once. We consider general setting involving a tunable fraction of inconclusive outcomes and we prove that the optimal discrimination strategy requires an entangled probe state for any nonzero rate of inconclusive outcomes. We experimentally implement this optimal discrimination strategy for projective measurements on polarization states of single photons. Our setup involves a real-time electrooptical feed-forward loop which allows us to fully harness the benefits of entanglement in discrimination of quantum measurements. The experimental data clearly demonstrate the advantage of entanglement-based discrimination strategy as compared to unentangled single-qubit probes.

Lukasz Czekaj, Anna Przysiezna, Michal Horodecki and Pawel Horodecki

Quantum metrology: Heisenberg limit with bound entanglement

Quantum metrology allows for a huge boost in the precision of parameters estimation. However, it seems to be extremely sensitive to noise. Bound entangled states are states with large amount of noise what makes them unusable for almost all quantum informational tasks. Here we provide a counterintuitive example of a family of bound entangled states which can be used in quantum enhanced metrology. We show that these states give advantage as big as maximally entangled states and asymptotically reach the Heisenberg limit. Moreover, entanglement of the applied states is very weak which is reflected by its so called unlockability poperty.

Junghee Ryu, James Lim, Sunghyuk Hong and Jinhyoung Lee.

Nonclassicality for discrete system by using quasiprobability function

We propose an operational quasiprobability function for qudits, enabling a comparison between quantum and hidden variable theories. We show that the quasiprobability function becomes a legitimate probability function if sequential measurements are described by a hidden variable with noninvasive measurability. Otherwise, it is negative valued. Based on the result, we classify classical and nonclassical states of a qubit. Also, we discuss a sufficient condition for the entanglement of two qudits using our approach.

Ondrej Černotík and Jaromír Fiurášek

Transformations of continuous-variable entangled states of light

Gaussian states and Gaussian transformations represent an interesting counterpart to two-level systems in quantum optics, on the one hand easily described using first and second moments of quadrature operators and on the other hand simple to implement experimentally using linear optics and optical parametric amplifiers. Here, we propose and analyse protocols for manipulation of entangled Gaussian states of light using local operations and classical communication. Firstly, we study entanglement concentration based on photon subtraction enhanced by local coherent displacements for states in the form of a single-mode squeezed vacuum state split on a beam splitter. We show that coherent displacements can enhance entanglement concentration based on photon subtraction. Secondly, we study transformations of multipartite permutation invariant Gaussian states. We investigate how entanglement classification is changed by these transformations. In addition, as a figure of merit characterising the quality of the entanglement, we use fidelity of assisted quantum teleportation. We study two different strategies to achieve this objective. The first one is based on adding correlated noise to each mode while the other employs partial non-demolition measurements.

Sergey Bravyi, Libor Caha, Ramis Movassagh, Daniel Nagaj and Peter W. Shor

Criticality without frustration for quantum spin-1 chains

Frustration-free (FF) spin chains have a property that their ground state minimizes all individual terms in the chain Hamiltonian. We ask how entangled the ground state of a FF quantum spin-s chain with nearest-neighbor interactions can be for small values of s. While FF spin-1/2 chains are known to have unentangled ground states, the case s = 1 remains less explored. We propose the first example of a FF translation-invariant spin-1 chain that has a unique highly entangled ground state and exhibits some signatures of a critical behavior. The ground state can be viewed as the uniform superposition of balanced strings of left and right parentheses separated by empty spaces. Entanglement entropy of one half of the chain scales as 1 log n + O(1), where n is the number of 2 spins. We prove that the energy gap above the ground state is polynomial in 1/n. The proof relies on a new result concerning statistics of Dyck paths which might be of independent interest. Based on Phys. Rev. Lett. 109, 207202 (2012).

Christoph Hirche and Ciara Morgan

Efficient achievability for quantum protocols using decoupling theorems

Proving achievability of protocols in quantum Shannon theory usually does not consider the efficiency at which the goal of the protocol can be achieved. Nevertheless it is known that protocols such as coherent state merging are efficiently achievable at optimal rate. We aim to investigate this fact further in a general one-shot setting, by considering certain classes of decoupling theorems and give exact rates for these classes. Moreover we compare results of general decoupling theorems using Haar distributed unitaries with those using smaller sets of operators, epsilon-approximate 2-designs. We also observe the behavior of our rates in special cases such as epsilon approaching zero and the asymptotic limit.

András Gilyén, Tamás Kiss, Igor Jex and Gernot Alber

Complex chaos with positive Lyapunov exponents emerging from selective qubit protocols

Measurement and selection in quantum protocols can lead to non-linear behaviour which, in turn, may result in truly chatic dynamics [Phys. Rev. A 74, 040301(R) (2006)]. Chaotic evolution of the entanglement between qubits is also possible in this type of systems [Phys. Rev. Lett. 107, 100501 (2011)]. We explore the properties of the chaos emerging from these protocols. More concretely, we analyse the dynamics of the one-qubit protocol of [Phys. Rev. A 74, 040301(R) (2006)] using mathematical tools and theory of Complex Dynamical Systems. We show that the dynamics features positive Lyapunov exponent for a rather large set of parameters and initial conditions. In fact, we could prove that for certain parameters all possible initial states lead to chaotic behaviour.

Zbigniew Puchała, Łukasz Rudnicki, Karol Życzkowski

Strong Majorization Entropic Uncertainty Relations

We analyze entropic uncertainty relations in a finite dimensional Hilbert space and derive several strong bounds for the sum of two entropies obtained in projective measurements with respect to any two orthogonal bases. We improve the recent bounds by Coles and Piani, which are known to be stronger than the well known result of Maassen and Uffink. Furthermore, we find a novel bound based on majorization techniques, which also happens to be stronger than the recent results involving largest singular values of submatrices of the unitary matrix connecting both bases. The first set of new bounds give better results for unitary matrices close to the Fourier matrix, while the second one provides a significant improvement in the opposite sectors. Some results derived admit generalization to arbitrary mixed states, so that corresponding bounds are increased by the von Neumann entropy of the measured state. The majorization approach is finally extended to the case of several measurements.

Wojciech Slomczynski and Anna Szczepanek

Maximum dynamical entropy and Hadamard matrices

We consider successive measurements performed on a d–dimensional quantum system, whose evolution between two subsequent measurements is given by a unitary operator. As a result, we obtain a random sequence of the measurement outcomes. We quantify the randomness arising from the unitary evolution by means of dynamical entropy (with respect to a measurement) and investigate unitary operators for which some PVM measurement leads to the maximum possible value of dynamical entropy, i.e. ln(d). We indicate a straightforward connection between these operators and complex Hadamard matrices of size d. For d = 2 we give a complete characterization of the set of operators for which PVMs give the maximum possible dynamical entropy and compute the volume of this set in the ensemble U(2). For an arbitrary unitary operator we calculate the maximum possible entropy attainable for PVMs and the mean value of this quantity over U(2).

Erkka Haapasalo, Juha-Pekka Pellonpää and Roope Uola

Compatibility properties of extreme quantum observables

Problem of simultaneous measurability of observables lies in the heart of quantum mechanics. Two basic notions of simultaneuos measurability are coexistence and joint measurability. I will give an introduction to these concepts and discuss briefly a more general notion of simultaneous measurement. I will also clarify the physical motivation behind these formulations and present a connection between them using extreme quantum observables. Possible applications to non-contextuality and non-locality schemes are also discussed. The content is based on an upcoming paper.

Stefan Baeuml, Matthias Christandl, Karol Horodecki and Andreas Winter

Limitations on Quantum Key Repeaters

A major application of quantum communication is the distribution of entangled particles for use in quantum key distribution (QKD). Due to unavoidable noise in the communication line, QKD is in practice limited to a distance of a few hundred kilometers, and can only be extended to longer distances by use of a so-called quantum repeater, a device which performs iterated entanglement distillation and quantum teleportation. The existence of entangled particles that are undistillable but nevertheless useful for QKD raises the question of the feasibility of a quantum key repeater, which would work beyond the limits of entanglement distillation, hence possibly tolerating much higher noise than existing protocols. Here, we show that any such apparatus is severely limited in its performance; in particular, we exhibit entanglement suitable for QKD but unsuitable for the most general conceivable quantum key repeater protocol. Our results are in the form of general bounds on the rate at which secure key can be obtained by such protocols. The mathematical techniques we develop may be seen as a step towards opening the theory of entanglement measures to networks of communicating parties.

Viktor Eisler and Zoltán Zimborás

Area law violation for the mutual information in a nonequilibrium steady state

We study the nonequilibrium steady state of an infinite chain of free fermions, resulting from an initial state where the two sides of the system are prepared at different temperatures. The mutual information is calculated between two adjacent segments of the chain and is found to scale logarithmically in the subsystem size. This provides the first example of the violation of the area law in a quantum many-body system outside a zero temperature regime. The prefactor of the logarithm is obtained analytically and, furthermore, the same prefactor is shown to govern the logarithmic increase of mutual information in time, before the system relaxes locally to the steady state. [Published as Phys. Rev. A 89, 032321 (2014)]

CEQIP 2014

THURSDAY, 05/06/2014

16:00-17:30 Registration and refreshment

Afternoon session (chaired by Jan Bouda)

17:30-18:15 I **Fernando Brandao:** Limitations for quantum PCPS

18:15-18:40 C **Martin Schwarz:** Simulating Quantum Circuits with Sparse Output Distributions

18:40-19:05 C **Alexander Müller-Hermes:** Quantum Subdivision Capacities and Continuous Quantum Coding

19:30 TAKE-ME-OUT-FOR-DINNER TRAIN, in front of the Loucky monastery (conference venue)

20:00 WELCOME DINNER, Pivnice u Šneka, Zelenářská 1 (GPS 48°51'17.205"N, 16°2'55.892"E)

FRIDAY, 06/06/2014

08:00 Breakfast (in your hotel)

Morning session (chaired by Fernando Brandao)

09:00-09:45 I **Andreas Winter:** Weak locking capacity of quantum channels can be much larger than private capacity

09:45-10:10 C **Juan Bermejo-Vega:** The computational power of normalizer circuits over ∞ Abelian groups

10:10 Break and refreshment

10:40-11:25 I **Valerio Scarani:** Randomness from quantum systems: a guided tour

11:25-11:50 C **David Reeb:** Trace-norm contraction under tensor product channels

11:50-12:15 C **Marcus Huber:** Inequalities for the Ranks of Quantum States

12:15 Lunch

Afternoon Session (chaired by Valerio Scarani)

13:45-14:30 I **Frédéric Dupuis:** Bounding the uncertainty of constrained adversaries

14:30-14:55 C **Julio De Vicente:** The maximally entangled set of multipartite quantum states

14:55-15:20 C **Sergey N. Filippov:** Dissociation and annihilation of multi-partite entanglement structures

15:20 Break and refreshment

15:50-16:15 C **Daniela Frauchiger:** True Randomness from Realistic Quantum Devices

16:15-16:40 C **Matej Pivoluska:** Device-independent randomness extraction for arbitrarily weak min-entropy source

16:40-17:05 C **Marcin Pawlowski:** Dimension Witness Networks

17:05-19:00 Poster session

19:30 BARBEQUE IN WINE CELLARS, Loucký monastery

SATURDAY, 07/06/2014

08:00 Breakfast (in your hotel)

Morning session (chaired by David Reeb)

09:00-09:45 I **Daniel Burgarth:** Quantum Computing in Plato's Cave

09:45-10:10 C **Mária Kieferová:** On The Power Of Coherently Controlled Quantum Adiabatic Evolutions

10:10 Break and refreshment

10:40-11:25 I **Giannicola Scarpa:** Graphs, classical channels and nonlocality: the interplay

11:25-11:50 C **Rafael Chaves:** Entropic Approach to Causal Inference - Applications to Nonlocality and Machine Learning

11:50-12:15 C **Erkka Haapasalo:** Boundariness and minimum-error discrimination

12:20 Group photo

12:30 Lunch

14:00 CONFERENCE ADVENTURE (City center)

15:00 CIPHER GAME (downtown part)

19:30 CONFERENCE DINNER, Loucký monastery

20:00 CIPHER GAME (monastery part)

SUNDAY, 08/06/2014

08:00 Breakfast (in your hotel)

Morning session (chaired by Mário Ziman)

09:00-09:45 I **Ciara Morgan:** Additivity and quantum channel capacity: an old problem revisited

09:45-10:10 C **Tomáš Rybár:** Estimation in presence of memory effects

10:10 Break and refreshment

10:40-11:05 C **Alessandro Tosini:** The Feynman problem and Fermionic entanglement: Fermions versus qubits

11:05-11:30 C **Richard Kueng:** Stabilizer states are complex projective 3-designs

11:30-11:55 C **John Lapeyre:** The role of local and global geometry in quantum entanglement percolation

12:00 Lunch