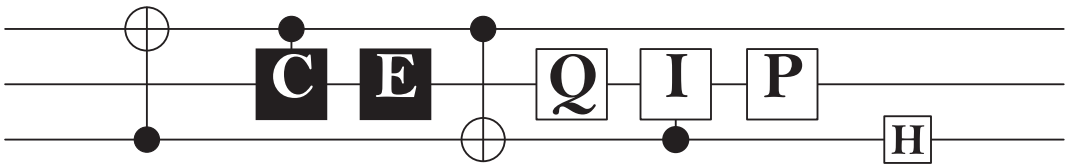

BOOK OF ABSTRACTS

(edited by Daniel Reitzner, Tomáš Rybár, Mário Ziman)

13th Central European Quantum Information Processing Workshop

16th–19th June 2016, Valtice, Czech Republic

http://ceqip.eu

CEQIP 2016

13th Central European Quantum Information Processing workshop — CEQIP'16 — will be traditionally focused on current theoretical challenges and paradigms of quantum information processing from the intersection of physics, computer science and mathematics. It is known to have a unique relaxed atmosphere accompanied with participants-driven non-scientific activities. The program will include traditional wine tasting, entertaining conference trip and mind-teasing cipher game.

Venue

CEQIP 2016 will take place in *Valtice* in Czech republic in the Lednice-Valtice complex. There are not many places in the world which have received such care as the elegant area around the spectacular Lednice and Valtice chateaux. An absolutely unique park has been created here over the centuries, full of rare tree species, romantic little buildings, fishponds and beautiful little corners. The Lednice-Valtice Complex, which has been included in the UNESCO list, is known as the Garden of Europe to this very day.

Invited speakers

- Anne Broadbent (Ottawa, Canada)
- Miguel Navascues (Vienna, Austria)
- Simone Severini (London, United Kingdom)
- Ramon Muñoz Tapia (Barcelona, Spain)
- Mark Wilde (Baton Rouge, USA)
- ~~Michael Wolf (Munchen, Germany)~~

Selection Comittee

- Jan Bouda
- Frédéric Dupuis
- Min-Hsiu Hsieh
- Miguel Navascues
- Marcin Pawlowski
- David Reeb
- Michal Sedlák
- Mário Ziman

Organizing Team

- Jan Bouda
- Šárka Hawerlandová
- Martina Zemanová
- Mário Ziman
- Matej Pivoluska
- Tomáš Rybár
- Daniel Reitzner

The workshop is organized by Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences (Bratislava) and Quantum Laboratory, Faculty of Informatics, Masaryk University (Brno).

Program

Thursday, 16.6.2016

16:00 Arrival and registration (with refreshment)

17:30 Evening session (chaired by *Daniel Reitzner*)
17:30 RAMON MUÑOZ TAPIA (I)
18:10 DANIEL BURGARTH (C)
18:35 DANIEL NAGAJ (C)
19:00 End of session

19:30 Welcome dinner (Valtická Rychta)

Friday, 17.6.2016

08:00 Breakfast

09:00 Morning session (chaired by *Sergey Filippov*)
09:00 MIGUEL NAVASCUES (I)
09:40 JED KANIEWSKI (C)
10:05 MATTHIAS KLEINMANN (C)
10:30 Coffee & Refreshment
11:00 ANNE BROADBENT (I)
11:40 CHRIS PERRY (C)
12:05 THOMAS BROMLEY (C)
12:30 End of session

12:30 Lunch

14:00 Afternoon session (chaired by *Mário Ziman*)
14:00 MARK WILDE (I)
14:40 GIACOMO DE PALMA (C)
15:05 JULIO DE VICENTE (C)
15:30 Coffee & Refreshment
16:00 End of session

16:00 Poster session
18:30 Cipher game registration
19:00 Dinner (conference room)
19:00 Cipher game

Saturday, 18.6.2016

08:00 Breakfast

09:00 Morning session (chaired by *Matej Pivoluska*)
09:00 SIMONE SEVERINI (I)
09:40 ALEXANDER MÜLLER-HERMES (C)
10:05 STEFAN BAEUML (C)
10:30 Coffee & Refreshment
11:00 SERGEY N. FILIPPOV (C)
11:25 FELIX HUBER (C)
11:50 THOMAS BROMLEY (C)
12:15 End of session

12:30 Lunch

13:30 Conference trip
19:00 Conference wine tasting (château cellars)

Sunday, 19.6.2016

08:00 Breakfast

09:00 Morning session (chaired by *Frédéric Dupuis*)
09:00 YASSER OMAR (C)
09:25 NIKOLAJS NAHIMOVS (C)
09:50 MATEUS ARAÚJO (C)
10:15 Coffee & Refreshment
10:45 JUKKA KIUKAS (C)
11:10 MARTIN PLÁVALA (C)
11:35 End of session

12:00 Lunch

(I) Invited talk ($35 + 5$ min.)
(C) Contributed talk ($20 + 5$ min.)

Invited talks

1. **Anne Broadbent:** How to verify a quantum computation

   We give a new interactive protocol for the verification of quantum computations in the regime of high computational complexity. Our results are given in the language of quantum interactive proof systems. Specifically, we show that any language in BQP has a quantum interactive proof system with a polynomial-time classical verifier (who can also prepare random single-qubit pure states), and a quantum polynomial-time prover. Here, soundness is unconditional — i.e. it holds even for computationally unbounded provers. Compared to prior work, our technique does not require the encoding of the input or of the computation; instead, we rely on encryption of the input (together with a method to perform computations on encrypted inputs), and show that the random choice between three types of input (defining a computational run, versus two types of test runs) suffice. We also present a new soundness analysis, based on a reduction to an entanglement-based protocol

2. **Miguel Navascues:** The structure of Matrix Product States

   For the past twenty years, Tensor Network States (TNS) have been widely used to model the low energy sector of local Hamiltonians. Their success in doing so has led to the wide-held mantra that TNS of low bond dimension are the 'only physical states' of natural condensed matter systems. However, given our experimental limitations to interact with such systems, it is not clear how this conjecture translates into any observable effect. In this talk I will identify particular operational features pertaining to all Matrix Product States (MPS), the class of TNS used to model non-critical one-dimensional spin chains. By exploiting two surprising structural constraints of MPS, we see how to systematically derive 'bond dimension witnesses', or k-local operators whose expectation value allows us to lower bound the bond dimension of the underlying quantum state. We extend some of these results to the ansatz of Projected Entangled Pairs States (PEPS). As a bonus, we use our insight on the structure of MPS to: a) derive some limitations on the use of MPS and PEPS for ground state energy computations; b) show how to decrease the complexity and boost the speed of convergence of the semidefinite programming hierarchies described in [1] for the characterization of finite-dimensional quantum correlations.

   [1] M. Navascués, T. Vértesi, *Bounding the Set of Finite Dimensional Quantum Correlations,* Phys. Rev. Lett. **115,** 020501 (2015).

3. **Simone Severini:** Combinatorial Entanglement

   We present new combinatorial objects, which we call grid-labelled graphs, and show how these can be used to represent the quantum states arising in a scenario which we refer to as the faulty emitter scenario: we have a machine designed to emit a particular quantum state on demand, but which can make an error and emit a different one. The device is able to produce a list of candidate states which can be used as a kind of debugging information for testing entanglement. By reformulating the Peres-Horodecki and matrix realignment criteria we are able to capture some characteristic features of entanglement: we construct new bound entangled states, and demonstrate the limitations of matrix realignment. We show how the notion of LOCC is related to a generalisation of the graph isomorphism problem. We give a simple proof that asymptotically almost surely, grid-labelled graphs associated to very sparse density matrices are entangled. We develop tools for enumerating grid-labelled graphs that satisfy the Peres-Horodecki criterion up to a fixed number of vertices, and propose various computational problems for these objects, whose complexity remains an open problem. The proposed mathematical framework also suggests new combinatorial and algebraic ways for describing the structure of graphs. The talk is practically [1].

   [1] J. Lockhart, S. Severini, *Combinatorial Entanglement*, preprint `arXiv:1605.03564 [quant-ph]`.

4. **Ramon Muñoz Tapia:** The quantum change point

   Sudden changes are ubiquitous in nature. The exact time when they happen is usually not known and identifying it is often of crucial importance. We propose a primitive quantum task that encapsulates this situation in its bare-bones. A source assumed to prepare a sequence of identical states starts to prepare a different state after some point. The length of the string of states where the change has occurred is given and the alteration is assumed to happen with equal probability at any point. We find the analytical expression of the optimal success probability of correct identification of the change point for large string lengths, which requires collective measurements on the whole string of states. We also analyse protocols that measure systems individually and provide an online answer at any stage of the measurement process and hence that do no require the use of a quantum memory. We show that these underperform quite substantially the optimal collective procedure.

5. **Mark Wilde:** Trading communication resources in quantum Shannon theory

   What are the net rates at which a sender and receiver can generate classical communication, quantum communication, and entanglement by using a quantum channel many times? A priori, this question might seem challenging, but there is a surprisingly simple answer for several channels of interest: Just combine a single protocol with teleportation, super-dense coding, and entanglement distribution. In this talk, I will discuss this theorem in some detail and show how the "triple trade-off" capacity region simplifies for a number of quantum channels of interest. If a particular minimum output entropy conjecture holds, then we have a full characterization of this triple trade-off capacity region for degradable quantum-limited attenuator channels and all quantum-limited amplifier channels. Based on [1–7].

[1] Haoyu Qi, Mark M. Wilde, *Capacities of Quantum Amplifier Channels,* preprint `arXiv:1605.04922` [quant-ph].

[2] Mark M. Wilde, Patrick Hayden, Saikat Guha, *Information trade-offs for optical quantum communication,* Phys. Rev. Lett. **108,** 140501 (2012).

[3] Mark M. Wilde, Patrick Hayden, Saikat Guha, *Quantum trade-off coding for bosonic communication,* Phys. Rev. A **86,** 062306 (2012).

[4] Mark M. Wilde, Min-Hsiu Hsieh, *The quantum dynamic capacity formula of a quantum channel,* Quantum Information Processing **11,** 1431 (2012).

[5] Kamil Bradler, Patrick Hayden, Dave Touchette, Mark M. Wilde, *Trade-off capacities of the quantum Hadamard channels,* Phys. Rev. A **81,** 062312 (2010).

[6] Min-Hsiu Hsieh, Mark M. Wilde, *Trading classical communication, quantum communication, and entanglement in quantum Shannon theory,* IEEE Transactions on Information Theory **56,** 4705 (2010).

[7] Min-Hsiu Hsieh, Mark M. Wilde, *Entanglement-assisted communication of classical and quantum information,* IEEE Transactions on Information Theory **56,** 4682 (2010).

Contributed talks

1. **Mateus Araújo:** A PURIFICATION POSTULATE FOR QUANTUM MECHANICS WITH NO CAUSAL ORDER

   Our common understanding of the physical world deeply relies on the notion that events are ordered with respect to some time parameter, with past events serving as causes for future ones. Nonetheless, it was recently found that it is possible to formulate quantum mechanics without any reference to a global time or causal structure. The resulting framework includes new kinds of quantum resources — called processes — that allow performing tasks which are impossible for events ordered according to a global causal order. It is not known, however, which of these processes are physical and which are just mathematical artefacts of the formalism. Here we make the first step in this direction, by proposing a purification postulate: processes are physical only if they can be expressed as a part of a pure process in a larger space, i.e., if they are purifiable. We show then that several known processes are not purifiable, and are therefore physically suspect.

2. **Stefan Baeuml:** BOUNDING MULTIPARTITE KEY RATE IN QUANTUM BROADCAST NETWORKS

   The ability to distribute entanglement to be used as cryptographic key over complex quantum networks is an important step towards a quantum version of the Internet. Most attention so far has been given to the distribution of bipartite entanglement. In this work we derive upper bounds on the rate at which GHZ states and multipartite private states can be distributed using a given network architecture consisting of broadcast channels. This is of particular interest for possible applications of multi-receiver cryptography or quantum secret sharing. Our bounds apply to general network architectures consisting of quantum broadcast channels and general adaptive LOCC protocols.

3. **Thomas Bromley:** ACCESSIBLE QUANTIFICATION OF MULTIPARTICLE ENTANGLEMENT

   Entanglement is a key ingredient for quantum technologies and a fundamental signature of quantumness in a broad range of phenomena encompassing many-body physics, thermodynamics, cosmology, and life sciences. For arbitrary multiparticle systems, entanglement quantification typically involves nontrivial optimisation problems, and may require demanding tomographical techniques. Here we develop an experimentally feasible approach to the evaluation of geometric measures of multiparticle entanglement. Our approach provides analytical results for particular classes of mixed states of N qubits, and computable lower bounds to global, partial, or genuine multiparticle entanglement of any general state. For global and partial entanglement, useful bounds are obtained with minimum effort, requiring local measurements in just three settings for any N. For genuine entanglement, a number of measurements scaling linearly with N is required. We demonstrate the power of our approach to estimate and quantify different types of multiparticle entanglement in a variety of N-qubit states useful for quantum information processing and recently engineered in laboratories with quantum optics and trapped ion setups.

4. **Thomas Bromley aka Marco Piani:** ROBUSTNESS OF ASYMMETRY AND COHERENCE OF QUANTUM STATES

   We introduce and study the robustness of asymmetry, a quantifier of asymmetry of states that we prove to have many attractive properties, including efficient numerical computability via semidefinite programming, and an operational interpretation in a metrology context. We also introduce the notion of asymmetry witnesses, whose measurement detects the presence of asymmetry. We prove that properly constrained asymmetry witnesses provide lower bounds to the robustness of asymmetry, which is shown to be a directly measurable quantity itself. We then focus our attention on coherence witnesses and the robustness of coherence, for which we prove a number of additional results.

5. **Daniel Burgarth:** DYNAMICAL DECOUPLING IN INFINITE DIMENSIONS

   We consider dynamical decoupling - a flexible and promising control technique to average out unwanted interactions - in infinite dimensions. Firstly, we look at finite dimensional systems coupled to infinite baths. Then we look at infinite systems described by Gaussian interactions. Finally we consider more general systems. We describe some interesting connections with non-Markovian dynamics and collapse models.

6. **Giacomo de Palma:** GAUSSIAN OPTIMIZERS IN QUANTUM INFORMATION

   Most communication schemes encode the information into pulses of electromagnetic radiation, that travels through metal wires, optical fibers or free space and is unavoidably affected by attenuation and noise. Quantum Gaussian channels provide a faithful model for these effects, and a fundamental issue is determining the maximum rate at which information can

be transmitted along such channels. The determination of the classical capacity region of the degraded quantum Gaussian broadcast channel, where the sender wants to communicate with two parties, relies on a still unproven constrained minimum output entropy conjecture, stating that Gaussian thermal input states minimize the output von Neumann entropy of a Gaussian quantum-limited attenuator among all the states with a given entropy. With the proof of the so-called quantum Entropy Power Inequality we have put nearly optimal bounds to the minimum output entropy of any quantum Gaussian channel in terms of the input entropy, and hence a nearly optimal bound to the classical capacity region of the Gaussian broadcast channel. Moreover, we have proved that for any one-mode quantum Gaussian channel the input state with a given entropy that minimizes the output entropy is always diagonal in the energy eigenbasis with eigenvalues decreasing as the energy increases, thus reducing the proof of the constrained minimum output entropy conjecture to a problem on discrete classical probability distributions.

7. **Julio de Vicente:** SIMPLE CONDITIONS CONSTRAINING THE SET OF QUANTUM CORRELATIONS

   The characterization of the set of quantum correlations in Bell scenarios is a problem of paramount importance for both the foundations of quantum mechanics and quantum information processing in the device-independent scenario. However, a clear-cut (physical or mathematical) characterization of this set remains elusive and many of its properties are still unknown. We provide here simple and general analytical conditions that are necessary for an arbitrary bipartite behaviour to be quantum. Although the conditions are not sufficient, they are shown to be strong and non-trivial. Moreover, we provide several applications of this result: we prove a quantitative separation of the quantum set from extremal nonlocal no-signaling behaviours in several general scenarios, we provide a relation to obtain Tsirelson bounds for arbitrary Bell inequalities and a construction of Bell expressions whose maximal quantum value is attained by a maximally entangled state of any given dimension.

8. **Sergey N. Filippov:** POSITIVE TENSOR PRODUCTS OF QUBIT MAPS AND 2-TENSOR-STABLE POSITIVE QUBIT MAPS

   We analyze positivity of a tensor product of two linear qubit maps, $\Phi_1 \otimes \Phi_2$. Positivity of maps Φ_1 and Φ_2 is a necessary but not a sufficient condition for positivity of $\Phi_1 \otimes \Phi_2$. We find a non-trivial sufficient condition for positivity of the tensor product map beyond the cases when both Φ_1 and Φ_2 are completely positive or completely co-positive. We fully characterize 2-tensor-stable positive qubit maps, i.e. qubit maps Φ such that $\Phi \otimes \Phi$ is positive. The case of non-unital maps is reduced to the case of appropriate unital maps. Decomposability of 2-tensor-stable positive qubit maps is discussed. Finally, 3-tensor-stable positive qubit maps Φ (such that $\Phi \otimes \Phi \otimes \Phi$ is positive) are characterized via semianalytical methods. We believe that the developed explicit procedure of reducing non-unitary qubit maps to the unitary ones may find applications in many quantum information problems.

   [1] Sergey N. Filippov, Kamil Yu. Magadov, *Positive tensor products of qubit maps and 2-tensor-stable positive qubit maps*, preprint `arXiv:1604.01716 [quant-ph]`.

9. **Felix Huber:** CHARACTERIZING GROUND AND THERMAL STATES OF FEW-BODY HAMILTONIANS

   We provide methods to characterize the states generated by two- and, more generally, k-body Hamiltonians as well as the convex hull of these sets. This leads to new insights into the question which states are uniquely determined by their marginals and to a generalization of the concept of entanglement. Finally, certification methods for quantum simulation can be derived.

10. **Jed Kaniewski:** SELF-TESTING OF THE SINGLET: ANALYTIC BOUNDS FROM OPERATOR INEQUALITIES

    We present a new method for deriving analytic bounds for self-testing of quantum states. Our method can turn any Werner-Wolf-Zukowski-Brukner scenario (a two-input, two-outcome correlation Bell inequality with an arbitrary number of parties) into an operator and placing a lower bound on the spectrum of that operator immediately yields a self-testing statement. For the case of self-testing the singlet using the CHSH inequality we obtain an explicit analytic bound which improves on all previously existing results.

11. **Jukka Kiukas:** TWO EXAMPLES OF QUANTUM RESOURCE CONTROL WITH SINGLE QUBIT PROBES

    Understanding and controlling quantum resources is crucial for practical applications of quantum technologies. We consider two examples where numerical quantum optimal control can be used to enhance a quantum protocol between two local parties, Alice and Bob, embedded in a common dynamical system. By resource control we mean that the figures of merit used in the optimisation directly quantify the relevant quantum resource; this is in contrast to the typical optimal control based on distance from a specific target state or process. The first example focuses on the optimisation of Bob's quantum Fisher information on an unknown local parameter in Alice's system, at a given evolution time. This demonstrates how information propagates from Alice to Bob across the large system. We assume that Bob's probe system consists of a single qubit, so that the Fisher information has an explicit formula which we use in the optimisation. Our second example is the optimal control of Einstein-Podolski-Rosen steering from Alice to Bob, which is known to be characterised by the incompatibility of certain effective measurements on Bob's system. Again assuming that Bob is restricted to a single qubit, we look mainly at the case where Alice steers with a pair of two-outcome measurements; then an easily computable quantification exists. The results demonstrate how quantum correlations propagate or decay in time, in the presence of overall dynamics.

12. **Matthias Kleinmann:** DEVICE-INDEPENDENT DEMONSTRATION THAT A QUBIT IS MORE THAN A QUANTUM COIN

    Qubits are the simplest quantum systems and as such they have a pronounced binary structure. Therefore, the qubit is sometimes compared to a "quantum coin" having infinitely many sets of two sides which can only be tossed when specifying the desired set. However, this picture fails to capture the richness of the quantum world and we here present an experiment on pairs of polarization-entangled photonic qubits which cannot be explained by two-outcome measurements. We combine this with device-independent evidence that the system is best described by two qubits thus showing that quantum measurements on a qubit are fundamentally non-binary and that the binary picture of the qubit thus cannot be uphold. Since such measurements cannot be sharp, in addition this constitutes the first device-independent certification of a genuine generalized quantum measurement.

13. **Alexander Müller-Hermes:** RELATIVE ENTROPY BOUNDS ON QUANTUM, PRIVATE AND REPEATER CAPACITIES

    We find a strong-converse bound on the private capacity of a quantum channel assisted by unlimited two-way classical communication. The bound is based on the max-relative entropy of entanglement and its proof uses a new inequality for the sandwiched Renyi divergences based on complex interpolation techniques. We provide explicit examples of quantum channels where our bound improves both the transposition bound (on the quantum capacity assisted by classical communication) and the bound based on the squashed entanglement introduced by Takeoka et al. As an application we study a repeater version of the private capacity assisted by classical communication and provide an example of a quantum channel with negligible private repeater capacity.

14. **Daniel Nagaj:** QUANTUM PROOFS CAN BE VERIFIED USING ONLY SINGLE QUBIT MEASUREMENTS

    Quantum Merlin Arthur is the class of problems which, potentially hard to solve, have a quantum solution which can be verified efficiently using a quantum computer. In this paper, we study what happens when we restrict the quantum resources of the verifier to a minimum: individual measurements on single qubits received as they come, one-by-one. We find that despite not having quantum memory or multiqubit operations, it is still possible to soundly verify any problem in QMA. We provide two independent proofs, based on measurement based quantum computation and the local Hamiltonian problem, respectively. The former also applies to QMA_1.

15. **Nikolajs Nahimovs:** EXCEPTIONAL CONFIGURATIONS OF QUANTUM WALKS WITH GROVER'S COIN

    We study search by quantum walks on general graphs with multiple marked locations. We prove what the most natural choice of coin transformation — Grover's diffusion transformation — has a wide class of exceptional configurations of marked locations, for which the probability of finding any of the marked locations does not grow over time. We analyze configurations of two and three near-by marked locations and show the necessary and sufficient conditions for the configuration to be exceptional. Next, we formulate general conditions for the configuration of multiple marked locations to be exceptional and show how one can extend our analysis to configurations consisting of more than three marked locations. Our result greatly extends the class of known exceptional configurations; until now the only known such configuration was the "diagonal construction" by [1].

    [1] A. Ambainis, A. Rivosh, *Quantum walks with multiple or moving marked locations*, Proceedings of SOFSEM'08, 485 (2008).

16. **Yasser Omar:** SPATIAL SEARCH BY QUANTUM WALK IS OPTIMAL FOR ALMOST ALL GRAPHS

    The problem of finding a marked node in a graph can be solved by the spatial search algorithm based on continuous-time quantum walks (CTQW). However, this algorithm is known to run in optimal time only for a handful of graphs. In this work, we prove that for Erdös-Renyi random graphs, i.e., graphs of n vertices where each edge exists with probability p, search by CTQW is almost surely optimal as long as $p \geq \log^{3/2}(n)/n$. Consequently, we show that quantum spatial search is in fact optimal for almost all graphs, meaning that the fraction of graphs of n vertices for which this optimality holds tends to one in the asymptotic limit. We obtain this result by proving that search is optimal on graphs where the ratio between the second largest and the largest eigenvalue is bounded by a constant smaller than 1. Finally, we show that we can extend our results on search to establish high fidelity quantum communication between two arbitrary nodes of a random network of interacting qubits, namely, to perform quantum state transfer, as well as entanglement generation. Our work shows that quantum information tasks typically designed for structured systems retain performance in very disordered structures.

17. **Chris Perry:** DOUBLY INFINITE SEPARATION OF QUANTUM INFORMATION AND COMMUNICATION

    How big a separation can there be between the amount of information that must be exchanged to compute a function and the amount of actual communication required? Here we exhibit an enormous gap between the quantum information complexity and quantum communication complexity of a communication task — vanishing versus diverging, which we call "doubly infinite." Such a separation is qualitatively different to those that have been discovered between their classical counterparts. We do so by studying a one-way communication task called the exclusion game. For this game we show that as the size of the task, n, increases, the quantum communication complexity scales at least logarithmically in n, while the information cost of a winning quantum strategy tends to zero. The logarithmic lower bound on the quantum communication complexity and the doubly infinite gap is further shown to hold even if we allow a small probability of error. In this regime however, a strategy requiring a sub-linear, polynomial, amount of communication exists.

18. **Martin Plávala:** CONDITIONS FOR OPTIMAL INPUT STATES FOR DISCRIMINATION OF QUANTUM CHANNELS

    We find optimality conditions for testers in discrimination of quantum channels. These conditions are obtained using semidefinite programming and are similar to optimality conditions for POVMs obtained by Holevo for ensembles of quantum states. We get a simple condition for existence of an optimal tester with any given input state with maximal Schmidt rank, in particular with a maximally entangled input state and we show the pitfalls of using input states with not maximal Schmidt rank. In case when maximally entangled state is not the optimal input state an error estimate is obtained. The results for maximally entangled input state are applied to covariant channels, qubit channels, unitary channels and simple projective measurements.

Posters

1. **Libor Caha:** VERY ENTANGLED SPIN CHAINS

   How much entanglement can the ground state of a qudit spin chain with a reasonable spectral gap and low qudit dimension ($d = 3, 4, 5$) possess? It turns out that a power law scaling of the entanglement entropy with the inverse of the gap is possible, even for frustration-free systems. We investigate how far this trade-off can go, and present a family of translationally invariant *pair-creation* models, with $d \geq 4$, $1/\mathrm{poly}(N)$ gap, $\sqrt{N}$ entanglement entropy, and power-law trade-off $S \propto \Delta^{-1/4}$ (numerical), surpassing the colored bracket model of Movassagh & Shor [1], with $d \geq 5$ and $S \propto \Delta^{-1/6}$.

   [1] Ramis Movassagh, Peter W. Shor, *Power law violation of the area law in quantum spin chains*, preprint `arXiv:1408.1657 [quant-ph]`.

2. **Krzysztof Domino:** TENSOR NETWORKS OF THE CUMULANT TENSORS

   The cumulant tensors and their application in the multivariate random variable statistics is discussed. Cumulant tensors are used to analyse non-Gaussian distributed data, such as hyper-spectral data (small target detection), financial data, weather data, auto-correlated time series. The method of calculation and update of cumulant tensors is presented. The method is based on tensor networks, which are inspired by the quantum mechanics.

3. **Máté Farkas and Péter Vrana:** HOMOLOGICAL CODES AND ABELIAN ANYONS

   We study a generalization of Kitaev's abelian toric code model defined on CW complexes. In this model qudits are attached to n dimensional cells and the interaction is given by generalized star and plaquette operators. These are defined in terms of coboundary and boundary maps in the locally finite cellular cochain complex and the cellular chain complex. We find that the set of energy-minimizing ground states and the types of charges carried by certain localized excitations depend only on the proper homotopy type of the CW complex. As an application we show that the homological product of a CSS code with the infinite toric code has excitations with abelian anyonic statistics.

4. **Aurél Gábris:** MEASURING TOPOLOGICALLY PROTECTED EDGE STATES IN DISORDERED DISCRETE TIME QUANTUM WALKS

   Discrete time quantum walks have been shown to exhibit features similar to topological insulators. A characteristic feature of the latter are robust edge states which appear on the boundary of systems in different topological phases. We have provided the yet strongest experimental evidence of topologically protected edge states in quantum walks. Observation of localization over time is complemented by the direct measurement of the topological phase of the associated bulk systems.

5. **Piotr Gawron:** NUMERICAL RANGE FOR RANDOM MATRICES

   We analyze the numerical range of high-dimensional random matrices, obtaining limit results and corresponding quantitative estimates in the non-limit case. For a large class of random matrices their numerical range is shown to converge to a disc. In particular, numerical range of complex Ginibre matrix almost surely converges to the disk of radius $\sqrt{2}$. Since the spectrum of non-hermitian random matrices from the Ginibre ensemble lives asymptotically in a neighborhood of the unit disk, it follows that the outer belt of width $\sqrt{2} - 1$ containing no eigenvalues can be seen as a quantification the non-normality of the complex Ginibre random matrix. We also show that the numerical range of upper triangular Gaussian matrices converges to the same disk of radius $\sqrt{2}$, while all eigenvalues are equal to zero and we prove that the operator norm of such matrices converges to $\sqrt{2e}$.

6. **Iulia Ghiu:** DESCRIBING POLARIZATION OF NON-GAUSSIAN STATES

   In classical optics, the degree of polarization is defined in terms of the Stokes parameters. Quantum analogues were then written in terms of expectation values of the Stokes operators. More recently, taking inspiration from quantum information tool-box, the degree of polarization was quantified by means of a distance between the given field state and the set of all unpolarized states.

   We here review the traditional Stokes definitions based on the first- and second-order moments, as well as the recently modified second-order degree that is obtained by minimizing over all the directions of the Poincare sphere. We further consider two distance-type measures based on the Hilbert-Schmidt and Bures metrics.

The above-mentioned quantum degrees of polarization are considered for a tensor product of Fock-diagonal states. We get analytic and numerical results for an important class of non-Gaussian states, namely, the two-mode photon-added thermal states. The obtained degrees of polarization are finally compared and their consistency is discussed.

7. **Adam Glos:** CONSTRUCTIVE QUANTUM SCALING OF UNITARY MATRICES

   In this work we present a method of decomposition of arbitrary multiqubit unitary matrix into a product of single-qubit negator and controlled square root of NOT. Since the product results in a negator matrix, which can be treated as complex analogue if bistochastic matrix, our method can be seen as complex analogue of Sinkhorn-Knopp algorithm, where diagonal matrices are replaced by adding and removing an one-qubit ancilla. The decomposition can be found constructively and resulting circuit consists of $O(4^k)$ entangling gates, which is proved to be optimal. An example of such transformation is presented.

8. **Craig Hamilton:** GAUSSIAN BOSON SAMPLING

   Boson sampling involves launching single photon Fock states into an interferometer, where the probability of any output distribution of photons is related to the permanent of a matrix. This makes the output distribution of events difficult to sample from unless certain complexity classes are equivalent. The use of input states different from Fock states, namely Gaussian states, is interesting both theoretically and experimentally. In this work we show that the output distribution of photon numbers from a Gaussian state is given by a matrix function which can be conjectured to be as difficult as the permanent.

9. **Christoph Hirche:** ASYMPTOTICALLY OPTIMAL RATES FOR MINIMUM ERROR DISCRIMINATION WITH FIXED MEASUREMENTS

   In this work we investigate the asymptotic error rate of fixed POVM's when optimizing over possible input states. This can be seen as dual problem to asymptotically optimal state discrimination, leading to the well known quantum Chernoff bound. As such we are interested in finding the optimal error exponents. Here we investigate the general problem, provide insights concerning the optimal signaling states and solve special cases by stating an optimal error exponent in the form of a relative entropy expression.

10. **Felix Huber:** CHARACTERIZING GROUND AND THERMAL STATES OF FEW-BODY HAMILTONIANS

    We provide methods to characterize the states generated by two- and, more generally, k-body Hamiltonians as well as the convex hull of these sets. This leads to new insights into the question which states are uniquely determined by their marginals and to a generalization of the concept of entanglement. Finally, certification methods for quantum simulation can be derived.

11. **Waldemar Klobus:** ON NONLOCALITY AND CONTEXTUALITY AS RESOURCE THEORIES

    We present a unified axiomatic approach to contextuality and non-locality based on the fact that both are resource theories. In those theories the main objects are consistent boxes, which can be transformed by certain operations to achieve certain tasks. The amount of resource is quantified by appropriate measures of the resource. Following recent paper [1], and recent development of abstract approach to resource theories, such as entanglement theory, we propose axioms and welcome properties for operations and measures of resources. As one of the axioms of the measure we propose the asymptotic continuity, which we prove for relative entropy of contextuality. Considering another concept from entanglement theory — the convex roof of a measure — we prove that for some non-local and contextual polytopes, the relative entropy of a resource is upper bounded up to a constant factor by the cost of the resource. Finally, we prove that providing a measure X of resource does not increase under allowed class of operations, such as e.g. wirings, the maximal distillable resource which can be obtained by these operations is bounded from above by the value of X up to a constant factor. We also make use of the known distillation protocol of bipartite nonlocality to show how contextual resources can be distilled.

    [1] J.I. de Vicente, J. Phys. A: Math. Theor. 47, 424017 (2014).

12. **Dariusz Kurzyk:** QUANTUM MARKOV FIELDS IN IMAGE PROCESSING

    Graphical models of probability distributions are powerful known methods for deriving probabilistic inferences amongst many numbers of random variables. Discrete probability distribution can be seen as a diagonal density matrix, therefore quantum information theory can be considered as a generalization of probability theory. In the field of image processing, the models are widely used for segmentation, denoising, inpainting, feature extraction and feature matching. In this paper we proposed the usage of a quantum formalism based on quantum Markov field, H2SI color space and simulated annealing for image processing.

13. **Ludovico Lami:** BIPARTITE DEPOLARIZING CHANNELS

    We introduce a 3-parameter class of maps acting on a bipartite system that are a natural generalisation of the depolarizing channel (and include it as a special case). Then, we find the exact regions of the parameter space that alternatively determine a positive, completely positive, entanglement-breaking or entanglement-annihilating map. This model displays a much richer behaviour than the one shown by a simple depolarizing channel, yet it stays exactly solvable. As an example of this

richness, PPT but not entanglement-breaking maps are found. Dually, a simple example of a positive yet indecomposable map is provided. Then, the study of the entanglement-annihilating property is fully addressed. Finally, we apply our results to solve the problem of the entanglement annihilation caused in a bipartite system by a tensor product of local depolarizing channels. In this context, some conjectures recently proposed in the literature are solved, leading to a complete characterization of the behavior of entanglement under the action of local white noises. To arrive at these results we employ some techniques that to the extent of our knowledge have not been used before. For instance, we show that the Hadamard (i.e. entrywise) product between density matrices is well-behaved with respect to many crucial properties in entanglement theory.

14. **Lvzhou Li:** LOWER BOUNDS ON THE SIZE OF SEMI-QUANTUM FINITE AUTOMATA

In the literature, there exist several interesting hybrid models of finite automata which have both quantum and classical states. We call them semi-quantum finite automata. In this paper, we compare the descriptional power of these models and DFA. Specifically, we present a uniform method that gives a lower bound on the size of the three existing main models of semi-quantum finite automata, and this bound shows that semi-quantum finite automata can be at most exponentially more concise than DFA. Compared with a recent work [1], our method has the following two advantages: (i) it is much more concise; and (ii) it is universal, since it is applicable to the three existing main models of semi-quantum finite automata, instead of only one specific model.

[1] M.P. Bianchi, C. Mereghetti, B. Palano, Theoret. Comput. Sci. **551** 102 (2014).

15. **Justyna Łodyga:** THE UNCERTAINTY PRINCIPLE BEYOND QUANTUM MECHANICS

Heisenberg uncertainty principle is a trademark of quantum mechanics. In its original form it states that one cannot gain information about a system without disturbing it, which is a core of novel cryptographic techniques based on quantum effects. The principle can be derived from mathematical formalism of quantum theory. However the formalism itself is very abstract - unlike in classical mechanics, it does not directly refer to what we perceive. The question arises: can we derive the principle from more comprehensible assumptions? Here we derive Heisenberg trade-off from two assumptions: impossibility of instantaneous messaging at a distance (no-signaling), and violation of Bell inequalities (non-locality). The former is a natural and simple assumption, while the latter is an observable phenomenon implied by quantum mechanics. That the trade-off is a consequence of the above two assumptions is indirectly implied by existing schemes of secure cryptography based on the above two assumptions. Surprisingly, despite of vast literature on such crypto-systems, no direct connection between no-signaling, non-locality and Heisenberg principle was ever proposed. We also analyze a Bayesian trade-off, and note that there exists a range of parameters, where assumptions of no-signaling precisely reconstruct quantum predictions.

16. **Ilia Luchnikov:** NON-LINEAR DYNAMICS INDUCED BY SUCCESSIVE RANK-r SELECTIVE MEASURMENTS

Selective measurements are known to lead to nonlinear transformations of quantum states. We consider measurements which are performed not on the system itself but on the probe (coupled to the system), which is in contrast to Zeno and anti-Zeno effects. The total "system + probe" density operator ρ is transformed as follows:

$$\rho \to \frac{E_i \rho E_i}{\mathrm{tr}[E_i \rho E_i]},$$

where E_i is a projector, which acts as an identity transformation in the system Hilbert space $\mathcal{H}_1$ and as a rank-r projector in the probe Hilbert space $\mathcal{H}_2$. Stroboscopic measurements of the probe with a time interval τ between successive shots result in a new interesting type of quantum dynamics, which explains the emergence of effective Hamiltonians in some physical problems. For instance, let $\sum_i \gamma A_i \otimes B_i$ be the "system + probe" Hamiltonian, where $A_i \in \mathcal{H}_1$ and $B_i \in \mathcal{H}_2$. If rank $r = 1$ and $\tau \to 0$, $\gamma \to \infty$, with $\gamma^2 \tau = \Omega$, then the system evolution is described by the effective Hamiltonian $H_{eff} = \sum_i \gamma A_i \langle B_i \rangle - \sum_{i,j} \frac{i}{2} \Omega A_i A_j (\langle B_i B_j \rangle - \langle B_i \rangle \langle B_j \rangle) + O(\sqrt{\tau})$, where $\langle \cdot \rangle$ denotes averaging over the state, which is supported by the probe measurements. We also generalize this approach to higher ranks r. In the limit above, analytical solutions are shown to converge to the exact dynamics. Possible applications of the developed theory include measurements of weak populations via amplification induced by such a non-linear dynamics.

17. **Christian Majenz:** CATALYTIC DECOUPLING

We introduce the notion of catalytic decoupling. Traditional decoupling is about finding a large subsystem of a quantum system that is independent of a reference. The novel paradigm appears nat- urally when focusing on the size of remainder system, and relaxes the requirement of a randomized decoupled state. We show that this notion unifies two previous techniques that have been applied to one shot quan- tum source coding. We characterize it tighly, allowing finding the second order i.i.d. asymptotics, and discuss applications. We also correct an error in the decoupling converse of [1].

[1] F. Dupuis, M. Berta, J. Wullschleger, R. Renner, *One-Shot Decoupling*, Communications in Mathematical Physics **328** 251 (2014).

18. **Marcin Markiewicz:** THREE-DIMENSIONAL VISUALISATION OF A QUTRIT

We present a surprisingly simple three-dimensional Bloch sphere representation of a qutrit, i.e., a single three-level quantum system. We start with a symmetric state of a two-qubit system and relate it to the spin-1 representation. Using this representation we associate each qutrit state with a three-dimensional vector $\mathbf{a}$ and a metric tensor $\hat{\mathbf{\Gamma}}$ which satisfy $\mathbf{a} \cdot \hat{\mathbf{\Gamma}} \cdot \mathbf{a} \leq 1$.

This resembles the well known condition for qubit Bloch vectors in which case $\hat{\mathbf{\Gamma}} = \mathbb{1}$. In our case the vector **a** corresponds to spin-1 polarization, whereas the tensor $\hat{\mathbf{\Gamma}}$ is a function of polarization uncertainties. Alternatively, **a** is a local Bloch vector of a symmetric two-qubit state and $\hat{\mathbf{\Gamma}}$ is a function of the corresponding correlation tensor.

19. **Ugo Marzolino:** ENTANGLEMENT AND TELEPORTATION WITH IDENTICAL PARTICLES

We report on teleportation with identical massive particles. Indistinguishability imposes that the relevant degrees of freedom to be teleported are not particles, but rather addressable orthogonal modes. We show that teleportation performances are inevitably decreased under the constraint of conservation of the total number of particles. Perfect teleportation is only achievable with some special resource entangled states and when the number of particles goes to infinity. Interestingly, some of such states are the many-particle atomic coherent states and the ground state of cold atoms loaded into a double well potential, which are routinely prepared in experiments.

20. **Darren Moore:** QUANTUM COMPUTATION WITH OPTOMECHANICAL CLUSTER STATES

Given a procedure for building a resource for Measurement Based Quantum Computation, a cluster state, two further steps towards Universal Computation are the verification of the cluster and the implementation of measurements on local nodes of the cluster. Here we provide a full scheme for state reconstruction of an array of mechanical oscillators in an optomechanical setting and detail how a method for continuous measurement of the mechanical quadratures is sufficient to provide the single-mode Gaussian transformations needed to drive parts of a computation forward. These will supplement recent research detailing a method for generating mechanical cluster states in the optomechanical setting.

21. **Mateusz Ostaszewski:** LIVELY QUANTUM WALKS ON CYCLES

We introduce a family of quantum walks on cycles parametrized by their liveliness, defined by the ability to execute a long-range move. We investigate the behavior of the probability distribution and time-averaged probability distribution. We show that the liveliness parameter, controlling the magnitude of the additional long-range move, has a direct impact on the periodicity of the limiting distribution. We also show that the introduced model provides a simple recipe for improving the efficiency of the network exploration.

22. **Łukasz Pawela:** DISTINGUISHABILITY OF RANDOM QUANTUM CHANNELS

Properties of random mixed states of dimension N distributed uniformly with respect to the Hilbert-Schmidt measure are investigated. We show that for large N, due to the concentration of measure, the trace distance between two random states tends to a fixed number $\tilde{D} = 1/4 + 1/\pi$, which yields the Helstrom bound on their distinguishability. To arrive at this result we apply free random calculus and derive the symmetrized Marchenko–Pastur distribution, which is shown to describe numerical data for the model of coupled quantum kicked tops. Asymptotic value for the root fidelity between two random states, $\sqrt{F} = 3/4$, can serve as a universal reference value for further theoretical and experimental studies. Analogous results for quantum relative entropy and Chernoff quantity provide other bounds on the distinguishablity of both states in a multiple measurement setup due to the quantum Sanov theorem. We study also mean entropy of coherence of random pure and mixed states and entanglement of a generic mixed state of a bi–partite system. For quantum channels, we show that their level density is also described by the Marchenko-Pastur distribution. This allows us to deduce some properties of the diamond norm of large dimensional quantum channels and provide a new upper bound on tthe diamond norm.

23. **Matej Pivoluska:** EXPERIMENTALLY SECURE RELATIVISTIC BIT COMMITMENT

Bit commitment is a well known cryptographic primitive used as a subroutine for different protocols. Unfortunately it is known to be impossible to perform without further limitations, such as limiting the computation power of an adversary. Relativistic bit commitment relays on a more general feature, namely the impossibility of instantaneous communication between distant parties. In this paper we first derive a tight classical upper bound for the winning probability for a specific family of non-local games, known as $\mathsf{CHSH}_q(p)$ and introduced recently in [1]. Using our bound, we show that the security of relativistic bit commitment of [2] against classical adversaries can be extended to any commitment time and distance of the parties that can be expected to be experimentally needed now and in the future — hence the notion of experimentally secure. For full version of the paper see [3].

[1] K. Chakraborty, A. Chailloux, A. Leverrier, *Arbitrarily Long Relativistic Bit Commitment*, Phys. Rev. Lett. **115,** 250501 (2015).

[2] Lunghi et. al., *Experimental Bit Commitment Based on Quantum Communication and Special Relativity*, Phys. Rev. Lett. **111,** 180504 (2013).

[3] M. Pivoluska, M. Pawlowski, M. Plesch, *Experimentally Secure Relativistic Bit Commitment*, preprint `arXiv:1601.08095 [quant-ph]`.

24. **Martin Plesch:** AN EXPLICIT CLASSICAL STRATEGY FOR WINNING A CHSHQ GAME

A CHSHq game is a generalization of the standard two player CHSH game, having q different input and output options. In contrast to the binary game, the best classical and quantum winning strategies are not known exactly. In our work [1] we provide a constructive classical strategy for winning a CHSHq game, with q being a prime. Our construction achieves a winning probability better than $1/22q^{-2/3}$, which is in contrast with the previously known constructive strategies achieving only the winning probability of $O(q^{-1})$.

[1] M. Pivoluska, M. Plesch, An explicit classical strategy for winning a CHSHq game, New J. Phys **18,** 025013 (2016).

25. **Zbigniew Puchała:** ASYMPTOTIC ENTROPIC UNCERTAINTY RELATIONS

We analyze entropic uncertainty relations for two orthogonal measurements on a N-dimensional Hilbert space, performed in two generic bases. It is assumed that the unitary matrix U relating both bases is distributed according to the Haar measure on the unitary group. We provide lower bounds on the average Shannon entropy of probability distributions related to both measurements. The bounds are stronger than those obtained with use of the entropic uncertainty relation by Maassen and Uffink, and they are optimal up to additive constants. We also analyze the case of a large number of measurements and obtain strong entropic uncertainty relations, which hold with high probability with respect to the random choice of bases.

26. **Daowen Qiu and Shenggen Zheng:** TIME-SPACE TRADEOFFS FOR TWO-WAY FINITE AUTOMATA

We explore bounds of *time-space tradeoffs* in language recognition on *two-way finite automata* for some special languages. We prove: (1) a time-space tradeoff upper bound for recognition of the languages $L_{EQ}(n)$ on *two-way probabilistic finite automata* (2PFA): $TS = \mathbf{O}(n \log n)$, whereas a time-space tradeoff lower bound on *two-way deterministic finite automata* is $\mathbf{\Omega}(n^2)$; (2) a time-space tradeoff upper bound for recognition of the languages $L_{INT}(n)$ on *two-way finite automata with quantum and classical states* (2QCFA): $TS = \mathbf{O}(n^{3/2} \log n)$, whereas a lower bound on 2PFA is $TS = \mathbf{\Omega}(n^2)$; (3) a time-space tradeoff upper bound for recognition of the languages $L_{NE}(n)$ on exact 2QCFA: $TS = \mathbf{O}(n^{1.87} \log n)$, whereas a lower bound on 2PFA is $TS = \mathbf{\Omega}(n^2)$.

It has been proved (Klauck, STOC'00) that the exact one-way quantum finite automata have no advantage comparing to classical finite automata in recognizing languages. However, the result (3) shows that the exact 2QCFA do have an advantage in comparison with their classical counterparts, which has been the first example showing that the exact quantum computing have advantage in time-space tradeoff comparing to classical computing.

Usually, two communicating parties, Alice and Bob, are supposed to have an access to arbitrary computational power in *communication complexity* model that is used. Instead of that we will consider communication complexity in such a setting that two parties are using only finite automata and we prove in this setting that quantum automata are better than classical automata and also probabilistic automata are better than deterministic automata for some well known tasks.

27. **Daniel Reitzner:** INCOMPATIBLE MEASUREMENTS ON QUANTUM CAUSAL NETWORKS

The existence of incompatible measurements, epitomized by Heisenberg's uncertainty principle, is one of the distinctive features of quantum theory. So far, quantum incompatibility has been studied for measurements that test the preparation of physical systems. Here we extend the notion to measurements that test dynamical processes, possibly consisting of multiple time steps. Such measurements are known as testers and are implemented by interacting with the tested process through a sequence of state preparations, interactions, and measurements. Our first result is a characterization of the incompatibility of quantum testers, for which we provide necessary and sufficient conditions. Then, we propose a quantitative measure of incompatibility. We call this measure the robustness of incompatibility and define it as the minimum amount of noise that has to be added to a set of testers in order to make them compatible. We show that (i) the robustness is lower bounded by the distinguishability of the sequence of interactions used by the tester and (ii) maximum robustness is attained when the interactions are perfectly distinguishable. The general results are illustrated in the concrete example of binary testers probing the time-evolution of a single-photon polarization.

28. **Przemysław Sadowski:** FIXED POINT QUANTUM SPATIAL SEARCH FOR MULTIPLE MARKED LOCATIONS

In this work we propose a quantum walk algorithm for spatial search in the case of multiple marked locations on two-dimensional grid.

29. **Gniewomir Sarbicki:** GENERALISING WIGNER'S THEOREM

[missing]

30. **Martin Schwarz:** APPROXIMATING LOCAL OBSERVABLES ON PROJECTED ENTANGLED-PAIR STATES

In condensed matter physics, the PEPS approximation conjecture states that ground states of gapped, local Hamiltonians can be efficiently approximated by a class of tensor networks known as projected entangled-pair states, or PEPS.

We show that this commonly believed conjecture implies that expectation values of local observables on such ground states can be efficiently approximated assuming the PEPS is also injective, which is generically the case.

To arrive at our result, we combine the specific structure of injective PEPS with the known exponential decay of correlations in ground states of gapped Hamiltonians. This result is in stark contrast with the known $P^{\#P}$-hardness of contracting more general PEPS, which — by this result — cannot represent ground states of a gapped local lattice Hamiltonian, unless the PEPS approximation conjecture is false.

31. **Kaushik P. Seshadreesan:** UNCONSTRAINED DISTILLATION CAPACITIES OF A PURE-LOSS BOSONIC BROADCAST CHANNEL

Bosonic channels are important in practice as they form a simple model for free-space or fiber-optic communication. We consider a single-sender two-receiver pure-loss bosonic broadcast channel and determine the unconstrained capacity region for the distillation of bipartite entanglement and secret key between the sender and each receiver, where they are allowed

arbitrary public classical communication. We show how the state merging protocol leads to achievable rates in this setting, giving an inner bound on the capacity region. We also evaluate an outer bound on the region and find that the outer bound matches the inner bound in the infinite-energy limit, thereby establishing the unconstrained capacity region for such channels.

32. **Kaushik P. Seshdareesan:** OPERATIONAL MEANING OF QUANTUM MEASURES OF RECOVERY

    Several information measures have recently been defined which capture the notion of recoverability of a tripartite quantum state. In particular, the fidelity of recovery quantifies how well one can recover a system A of a tripartite state, defined on systems ABC, by acting on system C alone. The relative entropy of recovery is an associated measure in which the fidelity is replaced by relative entropy. In this paper, we provide concrete operational interpretations of these measures in the contexts of computational complexity and asymmetric hypothesis testing. Additionally, we find that the fidelity of recovery computational problem is contained in QIP(2) and is hard for QSZK.

33. **Anna Szczepanek:** QUANTUM DYNAMICAL ENTROPY AND HADAMARD MATRICES

    We consider successive measurements performed on a d-dimensional quantum system, whose evolution between two subsequent measurements is described by a given unitary operator, and study the dynamics of the thus generated Markov chain of the measurement outcomes by means of a unitary invariant called quantum dynamical entropy. We single out a special class of entropy-maximising unitaries and point out their straightforward connection with complex Hadamard matrices. Moreover, although the volume of the set of entropy-maximising operators appears to be shrinking to zero as the dimension of the system grows, we show that the entropy of a generic unitary map is in fact nearly maximal i.e. close to $ln(d)$. Furthermore, the role played in this problem by POVMs is analysed. We show that at least in dim 2 POVMs cannot provide any extra information about the quantum dynamical entropy (independent of measurement) of a given unitary dynamics. However, we provide examples showing that quantum dynamical entropy of a given unitary dynamics with respect to a suitably chosen POVM can take on negative values. This effect is due to the complicated interplay between the two sources of randomness considered in this model, i.e. the underlying unitary dynamics and the process of measurement.

34. **Mikko Tukiainen:** APPROXIMATE QUANTUM PROGRAMMING

    We present an analysis on the approximate programming of quantum observables and channels via quantum multimeters. For this purpose, we introduce upper bounds to the fidelity of programming states in terms of the programmed quantum devices. Our observations clarify the programmability of quantum circuits, e.g. quantum computer, and allows us in particular to negatively answer an open question "whether a post-processing assisted universal programmable quantum multimeter exists or not?". We also suggest some possible applications in open quantum scenarios, such as a novel quantum thermometer not requiring any a priori knowledge of the system-environment interaction.

35. **Péter Vrana:** See 3.

36. **Zizhu Wang:** NONLOCALITY AND ENTANGLEMENT OF SPIN SQUEEZED STATES

    Spin squeezed states are known to have good bipartite entanglement properties and have been proven useful in quantum metrology. Here we show that they are also good candidates to violate a recently proposed multiparty Bell's inequality with bipartite correlators. We also show that spin squeezed states have interesting multiparty entanglement properties by using the Majorana representation and exploiting the connection between entanglement classification and the Möbius transformation.

37. **Hania Wojewódka:** TOWARDS REALISTIC RANDOMNESS AMPLIFICATION

    Randomness is a potentially important resource with applications in numerical simulations, cryptography or gambling, just to name a few. The aim of randomness amplification is to use partially random (so not deterministic, but biased or correlated with other variables) bits in order to obtain almost random and secure bits. Although unattainable through any deterministic method, it becomes possible if the no-signaling principle is assumed and quantum-mechanical correlations (revealed operationally through the violation of Bell inequalities) are used. The first device-independent protocol for free randomness amplification (together with its security proof) was provided by [1]. Their result has certainly contributed to the rapid development of the research on randomness amplification. The problem has been considered from many different points of view. Soon, a wide range of protocols has been proposed. All of them, however, seem to be impossible to implement in reality. Indeed, they are trapped between two restrictive alternatives: need for many devices and fragility to noise.

    Here we present protocols which use a finite number of devices, work even with correlations attainable by noisy quantum-mechanical resources and are composably secure against general no-signalling adversaries. The only assumptions are the following. Firstly, devices are shielded one from another and, secondly, they are fixed independently of the values of bits from a source. In our scenario just one weak source of randomness (an SV source) is provided at the beginning. We, however, we manage to prove (in a device-independent way) that output bits from devices constitute a second min-entropy source, which is independent from the given SV source. This in turn allows to apply a classical source-independent extractor, which finally generates almost perfect randomness.

Moving one step further, we want to relax one of the assumptions mentioned above. To be more precise, our intention is to ask whether randomness amplification is still possible when source and devices are not independent. We first give an example, which clearly illustrates that perfect correlations between SV-bits, used as inputs, and devices exclude any possibility of obtaining secure random bits (when only weakly random bits are provided at the beginning). Further, we formulate the so called SV condition for boxes, which is the weakest (thus far) condition allowing for randomness amplification.

The poster is based on the results [2,3].

[1] R. Colbeck, R. Renner, *Free randomness can be amplified*, Nat. Phys. **8,** 450453 (2012).

[2] F.G.S.L. Brandao, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Ramanathan, T. Szarek, H. Wojewódka, *Realistic noise-tolerant randomness amplification using finite number of devices*, Nat. Commun. **7,** 11345 (2016).

[3] H. Wojewódka, F.G.S.L. Brandao, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, R. Ramanathan, *Amplifying the randomness of weak sources correlated with devices*, preprint `arXiv:1601.06455 [quant-ph]` (2016).

38. **Shenggen Zheng:** See 26.

Cipher Game

The annual cipher game will now have its fifth anniversary. Join the game on Friday evening and enjoy it with your friends. The aim of the game is not only to solve the ciphers but to bring you all together. In fact, the puzzles are much easier to solve when you exchange ideas. Unlike in real life the smart collective ideas pop out of the "stupid" individual ones. You are strongly encouraged (not forced) to join this game. Without any consequences you can stop playing whenever you want. Experiencing the game is the main reward, however, there is some prize for the first team (or five?).

OK, I'm in. What should I do to play? Get together a team of 3–5 players, make up your team name and register before dinner (roughly from 18:30 at the location of dinner) either with Daniel Reitzner or Tomáš Rybár (a.k.a. the organizers). But never mind if you do not have time to create the team before the game registration. Just come to registration and find the team members directly there.

Then what? You will get starting envelope which you are allowed to open only after the organizers will tell you so (will be no sooner than 19:00).

How do I play? Your aim is to follow the route from cipher to cipher. In the envelope you will find the first cipher. Solution to each of the cipher will tell you the position of the next cipher. The last cipher will tell you the passphrase you should tell to the organizers. The ciphers are not really hidden (digging is not forbidden, but it is not needed) in their locations. Hiding is not the primary goal of this game. They are only not easily visible for random people wandering around. We know it is a moment full of emotions, however, try to avoid attracting all the people around to location of the ciphers.

Do I need to bring something with me? Yes, you will need the contents of the starting envelope and your brains to solve the ciphers. You will also need your legs to run for the ciphers and you might find useful some ciphering tools, scissors or flashlights that we will provide on start. Also, one might need a swimming suit or swimming trunks.

Will I miss the dinner then? No, the game is not meant to distract you from enjoying the food and drinks. The ciphers are situated in the walking distance (<15 minutes) from the dinner place and it should be a nice relaxing walk to find them and still let you enjoy the dinner buffet. It is possible to make the team base camp in the dinner place and always return with the found cipher there and take some refreshment while solving it.

What if we cannot solve a cipher? Do not worry, the organizers will be providing hints. First hints will be available when the organizers are fed, i.e. around 19:30 (you really do not want to talk to hungry organizers). Otherwise, please find one of the organizers and ask for hints only if you have spent more than 20 minutes on the cipher and you are out of any ideas. There is no guarantee the hints will help, but you can ask for new hint every 10 minutes until the organizers give up and provide you with an absolute hint. Typically all teams finish the game. There is no hint for last cipher, but never say never.

How do we finnish the game? Deliver the final phrase written on the piece of paper to the organizers. When incorrect, you can try again in 10 minutes. Yes, you are allowed to guess the phrase without solving ciphers, but you know what your chances are.

Are there some rules? Of course there are. Basically you should enjoy the game, solving the ciphers and you should avoid unfair behavior. The rules are presented here as 10 commandments.

The Book of Abstracts 14:1

THE TEN COMMANDMENTS

I. Honor thy Organizers.

II. Thou shall not solve random ciphers without a proper logo.

III. Thou shall not share ideas with other teams.

IV. Thou shall not follow other teams.

V. Thou shall not curse in vain, even if it is cold and rainy.

VI. Thou shall not read italics as part of a cipher.

VII. Thou shall not fill the crosswords without thinking.

VIII. Thou shall not beg the organizers for a solution or help before the allotted time limit.

IX. Thou shall not take more than two copies of a cipher or misplace the rest.

X. Thou shall not shout out the solutions.

Map of Valtice