7th Central European Quantum Information Processing Workshop

3–6 June 2010, Valtice, Czech Republic

http://www.quniverse.org/ceqip

CEQIP 2010

CEQIP'10 (Central European Quantum Information Procesing workshop) is focused on current challenges and paradigms of quantum information processing. The selected topics for this year are: quantum protocols, quantum dynamics, quantum algorithms and computation, quantum tomography.

Venue

Valtice is a small charming town near Austrian border and it has the official title "The capital of wine". Indeed, it lies in heart of the best Moravian wine regions famous mainly due to white aromatic wines. It is surrounded by beautiful system of lakes and historical buildings, romantic ruins and unique parks, which is a part of the UNESCO world heritage. Its written records date back to the late 12th century. The conference itself takes place in *chateaux Valtice.*

Social program

Guided tour in the chateaux Valtice followed by a social dinner at the courtyard of the chateau with free access for degustation to the National salon of the wine exposition (top 100 Czech wines), which is housed in the cellars under the chateau.

Invited speakers

- ⋆ Časlav Brukner (Wien, Austria)
- ⋆ Beatrix Hiesmayr (Wien, Austria)
- ⋆ Richard Jozsa (Cambridge, United Kingdom)
- ⋆ Simon Perdrix (Grenoble, France)
- ⋆ Renato Renner (Zurich, Switzerland)
- ⋆ Andreas Winter (Bristol, United Kingdom & Singapore)

Focused tutorials

- ⋆ Jan Bouda (Brno, Czech Republic)
- ⋆ Daniel Nagaj (Bratislava, Slovak Republic)

Steering Comittee

- ⋆ Vladimír Bužek (RCQI, Bratislava & FI MU, Brno)
- ⋆ Jozef Gruska (FI MU, Brno)

Organizing Comittee

- ⋆ Jan Bouda (FI MU, Brno)
- ⋆ Libor Caha (FI MU, Brno)
- ⋆ Matej Pivoluska (FI MU, Brno)
- ⋆ Martina Zemanová (RCQI, Bratislava)
- ⋆ Daniel Reitzner (RCQI, Bratislava)
- ⋆ Mário Ziman (RCQI, Bratislava & FI MU, Brno)

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

List of participants

- ⋆ Theodor Adaktylos (University of Vienna, Austria)
- ⋆ Emilio Bagan (Universitat Autonoma de Barcelona, Spain)
- ⋆ Alessandro Bisio (Università di Pavia, Italy)
- ⋆ Jan Bouda (Masaryk University, Czech Republic)
- ⋆ Libor Caha (Masaryk University, Czech Republic)
- ⋆ Časlav Brukner (University of Vienna, Austria)
- ⋆ Miloslav Dušek (Palacký University, Czech Republic)
- ⋆ Paul Erker (University of Vienna, Austria)
- ⋆ Jozef Gruska (Masaryk University, Czech Republic)
- ⋆ Beatrix Hiesmayr (University of Vienna, Austria; University of Sofia, Bulgaria)
- ⋆ Marcus Huber (University of Vienna, Austria)
- ⋆ Fabrizio Illuminati (Università di Salerno, Italy)
- ⋆ Ivan Fialík (Masaryk University, Czech Republic)
- ⋆ Florian Hipp (University of Vienna, Austria)
- ⋆ Richard Jozsa (University of Cambridge, U.K.)
- ⋆ Janek Kolodynski (University of Warsaw, Poland)
- ⋆ Mátyás Koniorczyk (University of Pécs, Hungary)
- ⋆ Dmitry Kravchenko (University of Latvia)
- ⋆ Ramon Muñoz Tapia (Universitat Autonoma de Barcelona, Spain)
- ⋆ Daniel Nagaj (Slovak Academy of Sciences)
- ⋆ Nikolajs Nahimovs (University of Latvia)
- ⋆ Zeynep Nilhan Gurkan (Izmir Institute of Technology, Turkey)
- ⋆ Michael Noelle (Austrian Institute of Technology)
- ⋆ Marcin Pawłowski (University of Gdansk, Poland)
- ⋆ Simon Perdrix (Grenoble, France)
- ⋆ Matej Pivoluska (Masaryk University, Czech Republic)
- ⋆ Martin Plesch (University of Vienna, Austria; Slovak Academy of Sciences)
- ⋆ Sasa Radic (University of Vienna, Austria)
- ⋆ Peter Rapčan (Slovak Academy of Sciences)
- ⋆ Daniel Reitzner (Slovak Academy of Sciences)
- ⋆ Renato Renner (ETH Zürich, Switzerland)
- ⋆ Alexander Rivosh (University of Latvia)
- ⋆ Tomáš Rybár (Slovak Academy of Sciences)
- ⋆ Stefan Schauer (Austrian Institute of Technology)
- ⋆ Hans Schimpf (University of Vienna, Austria)
- ⋆ Michal Sedlák (Università di Pavia, Italy)
- ⋆ Christoph Spengler (University of Vienna, Austria)
- ⋆ Martin Suda (Austrian Institute of Technology)
- ⋆ Levente Szabó (University of Pécs, Hungary)
- ⋆ Josef Šprojcar (ERATO-SORST, Japan)
- ⋆ Jan Vlach (Masaryk University, Czech Republic)
- ⋆ Heidi Maria Waldner (University of Vienna, Austria)
- ⋆ Andreas Winter (University of Bristol, U.K.; National University of Singapore)
- ⋆ Mário Ziman (Masaryk University, Czech Republic)

Program

Thursday, 3.6.2010

12:00	Accommodation
14:00	Registration (Lecture hall)
15:30	Afternoon session
	(chaired by *Jozef Gruska*)
15:30	Andreas Winter, part I (I)
16:15	Emili Bagan (C)
16:35	Coffee Break
17:00	Richard Jozsa (I)
17:45	Fabrizio Illuminatti (C)
18:05	Miloslav Dušek (C)
18:25	Daniel Reitzner (C)
18:45	End of session
19:00	Dinner

Friday, 4.6.2010

08:00	Breakfast
09:00	Morning session
	(chaired by *Miloslav Dušek*)
09:00	Daniel Nagaj (T)
10:00	Coffee break
10:20	Časlav Brukner (I)
11:05	Jan Bouda (T)
12:05	End of session
12:15	Lunch
15:00	Afternoon session
	(chaired by *Jan Bouda*)
15:00	Andreas Winter, part II (I)
16:00	Coffee break
16:30	Renato Renner (I)
17:15	Alessandro Bisio (C)
17:35	Marcus Huber (C)
17:55	End of session
18:00	Poster session
19:00	Social dinner

Saturday, 5.6.2010

08:00	Breakfast
09:00	Morning session
	(chaired by *Časlav Brukner*)
09:00	Simon Perdrix (I)
09:45	Coffee break
10:10	Beatrix Hiesmayr (I)
10:55	Ramon Muñoz-Tapia (C)
11:15	Michal Sedlák (C)
11:35	Josef Šprojcar (C)
11:50	End of session
12:00	Lunch
14:30	Conference trip
19:00	Conference dinner

Sunday, 6.6.2010

08:30	Breakfast
09:30	Morning session
	(chaired by *Mário Ziman*)
09:30	Marcin Pawłowski (C)
09:50	Martin Plesch (C)
10:05	Tomáš Rybár (C)
10:20	Coffee break
10:45	Peter Rapčan (C)
11:00	Janek Kolodynski (C)
11:15	Levente Szabó (C)
11:30	Ivan Fialík (C)
11:45	End of session
12:00	Lunch

(I) Invited talk
(T) Focused tutorial
(C) Contributed talk

Invited talks

1. **Časlav Brukner:** Probabilistic theories and quantum mechanics: Is entanglement special?

   Quantum theory makes the most accurate empirical predictions and yet it lacks simple, comprehensible physical principles from which the theory can be uniquely derived. A broad class of probabilistic theories exist which all share some features with quantum theory, such as probabilistic predictions for individual outcomes (indeterminism), the impossibility of information transfer faster than speed of light (no-signaling) or the impossibility of copying of unknown states (no-cloning). A vast majority of attempts to find physical principles behind quantum theory either fall short of deriving the theory uniquely from the principles or are based on abstract mathematical assumptions that require themselves a more conclusive physical motivation. It will be shown that classical probability theory and quantum theory can be reconstructed from three reasonable axioms:

   (a) (Information capacity) All systems with information carrying capacity of one bit are equivalent.

   (b) (Locality) The state of a composite system is completely determined by measurements on its subsystems.

   (c) (Reversibility) Between any two pure states there exists a reversible transformation.

   If one requires the transformation from the last axiom to be continuous, one separates quantum theory from the classical probabilistic one. A remarkable result following from our reconstruction is that no probability theory other than quantum theory can exhibit entanglement without contradicting one or more axioms.

2. **Beatrix Hiesmayr:** Testing entanglement and its manifestations at different energy scales

   Entanglement is at the heart of the quantum theory. Though intensive investigations simple questions as e.g. whether a given state is entangled or not, have no simple answer. To that question and related ones concerning the type of entanglement we present different sets of entanglement measures [1,2] and inequalities [3,4] which detect and distinguish different types of entanglement in systems of arbitrary dimension and arbitrary number of particles. To demonstrate the tightness and usefulness we introduce a certain state space, also known as the *magic simplex* [5–8], where e.g. bound entanglement [7,9], unlockable entanglement [8] and the geometry of Bell inequalities [10] can be investigated. However, also if one considers different physical systems a variety of additional interesting phenomena due to entanglement occur. We focus on the change of entanglement of massive entangled spin $\frac{1}{2}$ particles observed by different reference frames [11] and we will discuss entanglement and its manifestation of systems in high energy physics, e.g. the entanglement in flavor [12,13].

[1] B.C. Hiesmayr and M. Huber: *Multipartite entanglement measure for all discrete systems,* Phys. Rev. A **78,** 012342; preprint `arXiv:0712.0346 [quant-ph]` (2008).

[2] B.C. Hiesmayr, M. Huber and Ph. Krammer: *Two computable sets of multipartite entanglement measures,* Phys. Rev. A **79,** 062308; preprint `arXiv:0903.5092 [quant-ph]` (2009).

[3] M. Huber, F. Mintert, A. Gabriel and B.C. Hiesmayr: *Detection of high-dimensional qenuine multipartite entanglement of mixed state,* Accepted by Phys. Rev. Lett.;
preprint `arXiv:0912.1870 [quant-ph]` (2009).

[4] A. Gabriel, B.C. Hiesmayr, and M. Huber: *Criterion for k-separability in mixed multipartite system,* preprint arXiv:1002.2953 [quant-ph] (2010).

[5] B. Baumgartner, B.C. Hiesmayr and H. Narnhofer: *The state space for two qutrits has a phase space structure in its core,* Phys. Rev. A **74,** 032327; preprint arXiv:quant-ph/0606083 (2006).

[6] B. Baumgartner, B.C. Hiesmayr and H. Narnhofer: *A special simplex in the state space for entangled qudits,* J. Phys. A: Math. Theor. **40** 7919–7938; preprint arXiv:quant-ph/0610100 (2007).

[7] B. Baumgartner, B.C. Hiesmayr and H. Narnhofer: *The geometry of bipartite qutrits including bound entanglement,* Physics Letters A **372,** 2190; preprint arXiv:quant-ph/0705.1403 (2008).

[8] B.C. Hiesmayr, F. Hipp, M. Huber, Ph. Krammer and Ch. Spengler; *A simplex of bound entangled multipartite qubit states,* Phys. Rev. A **78,** 042327; preprint arXiv:0807.4842 [quant-ph] (2008).

[9] J. Bae, M. Tiersch, S. Sauer, F. de Melo, F. Mintert, B.C. Hiesmayr, and A. Buchleitner: *Detection and typicallity of bound entangled states,* Phys. Rev. A **80,** 022317; preprint arXiv:0902.4372 [quant-ph] (2009).

[10] Ch. Spengler, M. Huber and B.C. Hiesmayr: *On the state space geometry of the CGLMP-Bell inequality,* preprint arXiv:0907.0998 [quant-ph] (2009).

[11] N. Friis, R.A. Bertlmann, M. Huber and B.C. Hiesmayr: *Relativistic entanglement of two massive particles,* Accepted by Phys. Rev. A; preprint arXiv:0912.4863 [quant-ph] (2009).

[12] B.C. Hiesmayr: *Nonlocality and entanglement in a strange system,* European Physical Journal C, Vol. **50,** 73–79; preprint arXiv:quant-ph/0607210 (2007).

[13] R.A. Bertlmann, W. Grimus and B.C. Hiesmayr: *Open-quantum-system formulation of particle decay,* Phys. Rev. A **73,** 054101; arXiv:quant-ph/0602116 (2006).

3. **Richard Jozsa:** CLASSICAL SIMULATIONS AND COMMUTING QUANTUM COMPUTATIONS

4. **Simon Perdrix:** COMPUTATIONAL DEPTH COMPLEXITY OF MEASUREMENT-BASED QUANTUM COMPUTATION

We mainly show that the "depth of computations" — i.e. parallel time — in the one-way model is equivalent, up to a classical side-processing of logarithmic depth, to the quantum circuit model augmented with unbounded fan-out gates. It demonstrates that the one-way model is not only one of the most promising models of physical realisation, but also a very powerful model of quantum computation. It confirms and completes previous results which have pointed out, for some specific problems, a depth separation between the one-way model and the quantum circuit model. Since one-way model has the same parallel power as unbounded quantum fan-out circuits, the quantum Fourier transform can be approximated in constant depth in the one-way model, and thus the factorisation can be done by a polytime probabilistic classical algorithm which has access to a constant-depth one-way quantum computer. The extra power of the one-way model, comparing with the quantum circuit model, comes from its classical-quantum hybrid nature. We show that this extra power is reduced to the capability to perform unbounded classical parity gates in constant depth.

5. **Renato Renner:** RANDOMNESS EXTRACTION RELATIVE TO QUANTUM INFORMATION

Randomness extraction is the art of turning weak randomness, about which only a bound on the entropy is known, into almost perfectly uniform randomness. The talk starts with the observation that, even if we are only interested in "classical" randomness, quantum information-theoretic considerations are unavoidable. The reason for this is that knowledge *about* the random values, i.e. "side information", may be quantum-mechanical in nature. In fact, one can show that an extractor that works well in a purely classical world may be insecure in the presence of quantum side information. In this talk, I will show that randomness extraction is nevertheless possible in the real (quantum!) world.

6. **Andreas Winter:** Zero-error communication via quantum channels

   Quantum channels have all sorts of capacities: classical, quantum, private, etc. In addition, the capacity typically changes in the presence of additional resources, such as feedback, shared entanglement, etc. Very recently, quite a lot of progress was made regarding the limit of perfect communication in the above settings, at finite block length. I will review some of the most exciting results found, among them the superactivation of zero-error capacities; the fact that entanglement can increase the (0-error) communication capability even of a classical channel; an extension of Lovasz' theta upper bound to entanglement-assisted quantum channels; and a complete characterisation of zero-error channel coding, including a reverse zero-error Shannon theorem, when assisted by general non-signalling correlations.

   Based on joint work with T.S. Cubitt, D. Leung, W. Matthews, S. Severini and R. Duan [arXiv:0911.5300, arXiv:1002.2514 and arXiv:1003.3195]

Focused tutorials

1. **Jan Bouda:** Randomness extractors

   The main problem of many practical random number generators is that they produce non-uniform, i.e. biased, output. Moreover, the actual probability distribution may be not fixed and can be (in a limited way) controlled by an adversary. The main goal of randomness extractors is to postprocess the output of an extractor in such a way that the extractor output is (almost) uniformly distributed. Extractors are, however, also tightly related e.g. to the problem of privacy amplification.

2. **Daniel Nagaj:** Local Hamiltonians and quantum complexity

   How hard is it to find ground states of quantum systems? Sometimes the answer is: too hard. In this talk, we will introduce a few concepts from computer science and add quantum mechanics to the mix. We will see how to classify the complexity of tough questions, and show that finding the ground state properties (e.g. the energy) of quantum systems will likely be tough even for quantum computers (i.e. QMA-complete).

Contributed talks

1. **Emilio Bagan:** Discrimination of mixed states with local measurements

   The error probability of discriminating between states when N copies of them are provided is a fundamental quantity in quantum statistical inference with important consequences in quantum computation and communication applications. There are known asymptotic expressions and efficient numerical methods to compute this quantity when collective measurements on the N copies are allowed. There is still, however, an important void in the literature regarding the minimum error probability that can be attained by discrimination protocols that use only local operations assisted with classical communication (LOCC). In this talk, I will show how to exploit the symmetries of the problem to provide a rigorous (and tight) lower-bound on this error probability using semidefinite programming (SDP)techniques. This bound can, furthermore, be computed efficiently for large number of qubits.

   We find that, in contrast to the pure-state case, LOCC, experimentally feasible, protocols cannot attain the collective bound. Our numerical results for moderately large number of copies ($N \sim 40$) indicate that the gap between the error probability for collective and LOCC protocols persists even in the asymptotic limit ($N \to \infty$).

   The proposed techniques can be used to bound the power of LOCC strategies in other similar settings, which is still one of the most elusive questions in quantum communication.

2. **Alessandro Bisio:** Optimization of quantum circuits

   The recently proposed quantum comb formalism [1,2] is a useful tool when dealing with quantum circuits optimization problems. Many results have been achieved in this direction, for example the optimal cloning of a unitary transformation [3], channel discrimination [4], optimal tomography [5], and optimal learning of a unitary [6].

   In this talk I will present the basic features of this formalism emphasizing a new result [7] about the realization of a quantum network. Solving an optimization problem provides the expression of the optimal network in terms of its Choi-Jamiołkowski operator. This representation, even if extremely concise and efficient, is lacking physical intuition, and some features of the network can remain quite obscure. Moreover, a description of the network in terms of its inner components is essential for the purpose of experimentally achieving of the network. In a recent work we exhibit a procedure that, given the Choi-Jamiołkowski operator of a quantum network, provides its minimal representation as a concatenation of isometries.

   After this introductory section I will expose the most recent applications of the quantum comb framework to the optimization of quantum circuits:

   - ⋆ Information-disturbance trade-off in estimating a unitary transformation [8]. We are provided with a single use of an unknown unitary channel $\mathcal{U}$ and we want both to extract some information about it and to use it on some input state. This task can be achieved by the following scenario. Consider a quantum circuit board with an empty slot that is filled with the single use of $\mathcal{U}$; we want that this circuit board gives us some information about $\mathcal{U}$ but without affecting the performance $\mathcal{U}(\rho)$ of the uknown unitary channel itself on the input state ρ of the circuit.
   - ⋆ Optimal cloning and learning of an observable [9]. We consider a quantum circuit that works as a POVM after we insert a measurement into its open slots. We analyse the situation

in which the inserted measurement is unknown and the aim of the circuit is to create two replicas of the original measurement.

[1] G. Chiribella, G.M. D'Ariano, and P. Perinotti: *Quantum circuits architecture,* Phys. Rev. Lett. **101,** 060401 (2008).

[2] G. Chiribella, G.M. D'Ariano, and P. Perinotti: *A theoretical framework for quantum networks,* Phys. Rev. A **80,** 022339 (2009).

[3] G. Chiribella, G.M. D'Ariano, and P. Perinotti: *Optimal cloning of unitary transformations,* Phys. Rev. Lett. **101,** 180504 (2008).

[4] G. Chiribella, G.M. D'Ariano, and P. Perinotti, *Memory effects in quantum channel discrimination,* Phys. Rev. Lett. **101,** 180501 (2008).

[5] A. Bisio, G. Chiribella, G.M. D'Ariano, S. Facchini and P. Perinotti: *Optimal quantum tomography for states, measurements, and transformations,* Phys. Rev. Lett. **102,** 010404 (2009).

[6] A. Bisio, G. Chiribella, G.M. D'Ariano, S. Facchini and P. Perinotti: *Optimal quantum learning of a unitary transformation,* Phys. Rev. A **81,** 032324 (2010).

[7] A. Bisio, G. Chiribella, G.M. D'Ariano and P. Perinotti: *Realization algorithm for quantum networks,* in preparation.

[8] A. Bisio, G. Chiribella, G.M. D'Ariano and P. Perinotti, *Information-disturbance tradeoff in estimating a unitary transformation,* in preparation.

[9] A. Bisio, G.M. D'Ariano, P. Perinotti and M. Sedlák: *Optimal cloning vs optimal learning of a von Neumann observable,* in preparation.

3. **Miloslav Dušek:** Experimental implementation of the optimal linear-optical controlled phase gate

We report on the experimental realization of the optimal linear-optical controlled phase gate. The gate is implemented using bulk optical elements and polarization encoding of qubit states. Changing parameters of the setup one can tune the phase shift introduced by the gate to an arbitrary value. All such controlled phase gates are optimal with respect to their success probabilities which are maximal within the framework of linear-optical implementations. This implementation of the gate was proposed last year at CEQIP by Jens Eisert. This year we will present its realization in the lab.

4. **Ivan Fialík:** Unitary Noise and the Mermin-GHZ Game

Alice, Bob and Charles have each one bit as an input with the promise that the parity of the input bits is 0 [1]. We denote the input bits x_1, x_2 and x_3. The task for each player is to produce one bit so that the parity of the output bits is equal to the disjunction of the input bits. Thus, if a_1, a_2 and a_3 are the outputs, then the equation $a_1 \oplus a_2 \oplus a_3 = x_1 \vee x_2 \vee x_3$ must hold.

In a quantum winning strategy for the Mermin-GHZ game Alice, Bob and Charles share the entangled state $|\varphi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. After the players have received their inputs x_1, x_2, x_3, respectively, each of them does the following:

(a) Applies to his or her register the unitary transformation U which is defined as

$$U(|0\rangle) = |0\rangle,$$

$$U(|1\rangle) = e^{\frac{\pi \imath x_i}{2}}|1\rangle.$$

(b) Applies to his or her register the Hadamard transformation H.

(c) Performs a measurement in the computational basis on his or her register. Outputs the bit a_i which he or she has measured.

The best possible classical strategy for the Mermin-GHZ game enables the players to win with probability $\frac{3}{4}$.

The players are supposed not to be able to perform the required unitary transformations exactly. More precisely, we will focus on what happens if one of them, say Alice, performs the required rotation in the Bloch sphere around the right axis, but with an incorrect rotation angle. Thus, her erroneous unitary transformation is specified by a rotation angle $\alpha_x^\epsilon = \alpha_x + \epsilon$ where α_x is Alice's correct rotation angle. The rotation angle ϵ is called an *error*. In the following we will focus on two basic types of errors, systematic errors and random errors. An error is said to be *systematic* if it is constant. An error is said to be *random* with bound δ if it is chosen uniformly and randomly from an interval $[-\delta, \delta]$.

Results. If Alice performs the transformation U imperfectly with systematic error ϵ, then

$$p_\epsilon(x_1, x_2, x_3) = \begin{cases} 1 & \text{if } x_1 = 0 \\ \frac{1+\cos\epsilon}{2} & \text{otherwise.} \end{cases}$$

If the players are given a question chosen uniformly and randomly from P, they win with probability $p_\epsilon = \frac{1}{2} + \frac{1+\cos\epsilon}{4}$. Quantum players are better than classical ones in the presence of a systematic error in the first unitary transformation if $\epsilon \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.

If Alice performs the unitary transformation U imperfectly with random error with bound δ, then the quantum winning strategy for the Mermin-GHZ game gives a correct answer with probability

$$P_\delta(x_1, x_2, x_3) = \begin{cases} 1 & \text{if } x_1 = 0 \\ \frac{\delta+\sin\delta}{2\delta} & \text{otherwise} \end{cases}$$

for any inputs x_1, x_2 and x_3 satisfying the promise. It gives a correct answer with probability $P_\delta = \frac{1}{2} + \frac{\delta+\sin\delta}{4\delta}$ for a question chosen uniformly and randomly from P. Quantum players are better than classical ones in the presence of a random error in the first unitary transformation if $\delta \in (-\pi, \pi)$.

If Alice performs the Hadamard transformation H imperfectly with systematic error ϵ, then the quantum winning strategy for the Mermin-GHZ game gives a correct answer with probability

$$P_\epsilon(x_1, x_2, x_3) = \frac{1}{2} + \sin\left(\frac{\pi}{4} + \frac{\epsilon}{2}\right)\cos\left(\frac{\pi}{4} + \frac{\epsilon}{2}\right)$$

for any inputs x_1, x_2 and x_3 satisfying the promise. It gives a correct answer with probability $P_\epsilon = \frac{1}{2} + \sin(\frac{\pi}{4} + \frac{\epsilon}{2})\cos(\frac{\pi}{4} + \frac{\epsilon}{2})$ for a question chosen uniformly and randomly from P. Quantum players are better than classical ones in the presence of a systematic error in the Hadamard transformation if $\epsilon \in \left(-\frac{\pi}{3}, \frac{\pi}{3}\right)$.

If Alice performs the Hadamard transformation H imperfectly with random error with bound δ, then the quantum winning strategy for the Mermin-GHZ game gives a correct answer with probability

$$P_\delta(x_1, x_2, x_3) = \frac{1}{2\delta}\left[\delta + \sin^2\left(\frac{\pi}{4} + \frac{\delta}{2}\right) - \sin^2\left(\frac{\pi}{4} - \frac{\delta}{2}\right)\right]$$

for any inputs x_1, x_2 and x_3 satisfying the promise. It gives a correct answer with probability $P_\delta = \frac{1}{2\delta}\left[\delta + \sin^2\left(\frac{\pi}{4}+\frac{\delta}{2}\right) - \sin^2\left(\frac{\pi}{4}-\frac{\delta}{2}\right)\right]$ for a question chosen uniformly and randomly from P. Quantum players are better than classical ones in the presence of a random error in the Hadamard transformation if $\delta \in (-1.896, 1.896)$. This is only an approximate result since it has been computed using numerical methods.

If Alice performs both transformations U, H imperfectly with systematic errors ϵ_1, ϵ_2, respectively, then the quantum winning strategy for the Mermin-GHZ game gives a correct answer with probability

$$P_\epsilon(x_1,x_2,x_3) = \begin{cases} \frac{1}{2} + \sin(\frac{\pi}{4}+\frac{\epsilon_2}{2})\cos(\frac{\pi}{4}+\frac{\epsilon_2}{2}) & \text{if } x_1 = 0 \\ \frac{1}{2} + \sin(\frac{\pi}{4}+\frac{\epsilon_2}{2})\cos(\frac{\pi}{4}+\frac{\epsilon_2}{2})\cos\epsilon_1 & \text{otherwise.} \end{cases}$$

for any inputs x_1, x_2 and x_3 satisfying the promise.

If Alice performs both transformations U, H imperfectly with random errors with bounds δ_1, δ_2, respectively, then the quantum winning strategy for the Mermin-GHZ game gives a correct answer with probability

$$P_\delta(x_1,x_2,x_3) = \begin{cases} \frac{1}{2} + \frac{1}{2\delta_2}\left[\sin^2\left(\frac{\pi}{4}+\frac{\delta_2}{2}\right) - \sin^2\left(\frac{\pi}{4}-\frac{\delta_2}{2}\right)\right] & \text{if } x_1 = 0 \\ \frac{1}{2\delta_1\delta_2}\left(\sin\delta_1\left[\sin^2\left(\frac{\pi}{4}+\frac{\delta_2}{2}\right) - \sin^2\left(\frac{\pi}{4}-\frac{\delta_2}{2}\right)\right] + \delta_1\delta_2\right) & \text{otherwise} \end{cases}$$

for any inputs x_1, x_2 and x_3 satisfying the promise.

[1] D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger: *Bell's theorem without inequalities,* American Journal of Physics **58** (12), pp. 1131–1143 (1990).

[2] G. Brassard, A. Broadbent, A. Tapp: *Quantum pseudo-telepathy,* preprint `arXiv:quant-ph/0407221`.

5. **Marcus Huber:** DETECTION AND CLASSIFICATION OF MULTIPARTITE ENTANGLEMENT

We present a general framework to identify genuinely multipartite entangled mixed quantum states in arbitrary-dimensional systems and show on exemplary cases that the constructed criteria are stronger than previously known ones. Our criteria are simple inequalities involving matrix elements of the given quantum state and detect genuine multi-partite entanglement that had not been identified so far. They are experimentally accessible without quantum state tomography and are easily computable as no optimization or eigenvalue evaluation is needed. We also provide an optimal way for constructing the observables needed to identify the separability. Also we show that with such inequalities it is possible to distinguish certain classes of genuinely multipartite entangled states, e.g. the GHZ and W class. Furthermore these criteria prove to be versatile tools for detecting separability with respect to different partitions of multipartite states and provide novel ways of deriving lower bounds on concurrence based entanglement measures. In the end we show how with the help of such a framework, one can go further and not only identify genuine multipartite entanglement, which is constituted by non-2-separability, but generalize it to achieve criteria for non-k-separability in arbitrary dimensional multipartite states.

[1] M. Huber, F. Mintert, A. Gabriel and B. Hiesmayr: *Detection of high-dimensional genuine multi-partite entanglement of mixed states,* preprint `arXiv:0912.1870 [quant-ph]`.

[2] A. Gabriel, B.C. Hiesmayr and M. Huber: *Criterion for k-separability in mixed multipartite systems,* preprint `arXiv:1002.2953 [quant-ph]`.

6. **Fabrizio Illuminati:** QUANTUM INFORMATION AND COLLECTIVE SYSTEMS: FACTORIZATION VS. FRUSTRATION, LONG-DISTANCE ENTANGLEMENT, AND BELL INVERSION LAWS

   I will present some recent work on quantum many-body systems from the viewpoint of quantum information theory. I will discuss ground state factorization and its use as a diagnostic tool to probe quantum frustrated systems. I will then review the phenomenon of long-distance entanglement in quantum spin models, the generalization to modular entanglement, and schemes of implementation in coupled cavity arrays and optical lattices. Finally, I will introduce the use of a geometric measure of block bipartite entanglement that allows to identify a hierarchy of *inversion points* in the ordering of the reduced k-body states in the ground state of quantum spin systems.

7. **Janek Kolodynski:** LOSSY PHASE ESTIMATION

   The problem of *"lossy" phase estimation* has recently been analysed using *local* approaches [1]. Those implied finding the quantum states, which are most sensitive to the phase variations around a given value and maximise the *quantum Fisher information.* Some experimental realisations of local quantum enhancement have already been realised [2]. Here, we extend the analysis to the *global* cases, when *no "a priori" knowledge* is present and all phase values are equiprobable.

   We use the *covariant positive operator valued measurement scheme* [3], in order to find the optimal states that yield the highest estimation fidelities. We investigate the effect of losses in the system via the fictitious beamsplitters' models. By discretising the optimal covariant POVMs, we also propose the *measurement schemes* that can be used to reach the maximal fidelities of estimation.

   We analytically prove that, in the case of any losses present, the variance of the estimated phase asymptotically tends to the Standard Quantum Limit (SQL) scaling $\propto \frac{1}{N}$, with the state's mean number of photons. This further confirms the previous *local* results, [4], that *only the lossless estimation,* e.g of [5] type, can asymptotically reach the *Heisenberg Limit scaling* $\propto \frac{1}{N^2}$.

   We also derive the *optimal usage of coherent states* of light for in the lossy phase estimation. We compute analytically the maximal fidelities reached in this case and prove the SQL scaling bound.

   Finally, we compare fully our results with the Fisher information based schemes.

[1] U. Dorner, R. Demkowicz-Dobrzanski, B.J. Smith, J.S. Lundeen, W. Wasilewski, K. Banaszek and I.A. Walmsley, Phys. Rev. Lett. **102,** 040403 (2009); S.D. Huver, C.F. Wildfeuer and J.P. Dowling, Phys. Rev. A **78,** 063828 (2008).

[2] B.L. Higgins, D.W. Berry, S.D. Bartlett, M.W. Mitchell, H.M. Wiseman, and G.J. Pryde, New Journal of Physics **11,** 073023 (2009); M. Kacprowicz, R. Demkowicz-Dobrzanski, W. Wasilewski, K. Banaszek and I.A. Walmsley, Nature Photonics `doi:10.1038/nphoton.2010.39` (2010).

[3] A.S. Holevo: *Probabilistic and Statistical Aspects of Quantum Theory,* North Holland, Amsterdam (1982).

[4] R. Demkowicz-Dobrzanski, U. Dorner, B.J. Smith, J.S. Lundeen, W. Wasilewski, K. Banaszek, and I.A. Walmsley, Phys. Rev. A **80,** 013825 (2009).

[5] B.C. Sanders and G.J. Milburn, Phys. Rev. Lett. **75,** 2944 (1995); D.W. Berry and H.M. Wiseman, Phys. Rev. Lett. **85,** 5098 (2000).

8. **Marcin Pawłowski:** Information Causality

   Information Causality [M. Pawłowski et al. Nature **461,** 1101 (2009)] is a recently discovered physical principle, which can be considered a generalized version of no-signalling. It is satisfied by quantum mechanics and violated by most of the theories that allow for probability distributions not possible to be obtained by the measurements of quantum systems. This fact allows to derive from Information Causality tight bounds on some properties of quantum mechanics (e.g. Tsirelson bound) or the efficiency of quantum information protocols (e.g. random access codes).

   We start by deriving the Information Causality form information-theoretic principles and give their justification. Then we use it to derive the Tsirelson bound. Finally, we show how it can be used to find the bounds on random access codes. We also present the family of the codes form [M. Pawłowski and M. Żukowski, accepted in PRA] that saturates these bounds.

9. **Martin Plesch:** Efficient preparation of quantum states

   We have suggested an efficient way for preparation of arbitrary states of qubits using a gate library consisting of a single two-qubit gate (C-NOT) and one-qubit rotations. For even number of qubits we have reduced the previously known upper bound on the number of C-NOT gates needed by more than 50%, for odd number of qubits by more than 40%. For the special case of four qubits, we have reduced the number of C-NOT gates from 22 to 9, which shall be an experimentally accessible number already in near future.

   Using the suggested procedure, we can also efficiently prepare apply operations that transform any given state $|\psi\rangle$ of n qubits to any other given state $|\phi\rangle$. In the first part we run the preparation procedure for $|\psi\rangle$ in reversed order, which shall bring us to the state $|0\rangle^{\otimes n}$. In the second part we just prepare the wished state $|\phi\rangle$. The number of C-NOT gates needed to perform such a transformation is just double the amount needed to prepare an arbitrary state $|0\rangle^{\otimes n}$.

   Moreover, many of the C-NOT operations can be executed in parallel. In fact, during the first step no action is performed on the second half of the qubits. The whole second step ($\frac{N}{2}$ C-NOT gates) can be performed in one shot, as none of them act on the same qubit. Also steps three and four can be performed in parallel. For instance for four qubits we can divide our procedure into five parts, where in the first part we only perform action on the first two qubits and in the remaining four parts we always perform two parallel C-NOT gates on all four qubits, followed up with single qubit rotations, for every part. This opens further optimization possibilities for experimental implementation of the state preparation.

10. **Peter Rapčan:** Unambiguous comparison of squeezed vacua

    We propose a scheme for the unambiguous state comparison (USC) of two unknown squeezed vacuum states. We show that our setup, based on linear optical elements and photon-number resolving detectors, thus feasible with the current technology, achieves the optimal USC in the ideal case (unit quantum efficiency). The realistic scenario of non-ideal detection (non-unit quantum efficiency) is analyzed in some detail and the corresponding probability of getting an ambiguous result as well as the reliability of the setup are given. Possible extensions of the scheme are finally considered.

11. **Daniel Reitzner:** Scattering quantum walks in searches for graph anomalies

It was shown in [1] that Grover search is implementable also as a quantum-walk search under special conditions. It is, however, a different story to show, that the quantum-walk searches comprise much larger area of possible searches. Not only are they described by an evolution that sits in higher dimensional space [2] than the Grover search, but, naturally, they can provide us with searches that are not based just on a simple rotation composed of two phase-flips. We show an example of such quantum-walk search where the phase-flip is not present and is replaced by a combination of other factors. In a special case, this example is reducible also to the Grover search under special conditions.

[1] A. Ambainis, J. Kempe, and A. Rivosh, in Proceedings of the 16th Annual ACM-SIAM SODA (SIAM, Philadelphia, 2005).

[2] D. Reitzner, M. Hillery, E. Feldman, V. Bužek, Phys. Rev. A **79,** 012323 (2009).

12. **Tomáš Rybár:** Quantum Finite-Depth Memory Channels: Case Study

We analyze the depth of the memory of quantum memory channels generated by a fixed unitary transformation describing the interaction between the principal system and internal degrees of freedom of the process device. We investigate the simplest case of a qubit memory channel with a two-level memory system. In particular, we explicitly characterize all interactions for which the memory depth is finite. We show that the memory effects are either infinite, or they disappear after at most two uses of the channel. Memory channels of finite depth can be to some extent controlled and manipulated by so-called reset sequences. We show that actions separated by the sequences of inputs of the length of the memory depth are independent and constitute memoryless channels.

13. **Michal Sedlák:** Unambiguous comparison of quantum measurements

The goal of comparison is to reveal the difference of compared objects as fast and reliably as possible. In this paper we formulate and investigate the unambiguous comparison of unknown quantum measurements represented by non-degenerate sharp POVMs. We distinguish between measurement devices with apriori labeled and unlabeled outcomes. In both cases we can unambiguously conclude only that the measurements are different. For the labeled case it is sufficient to use each unknown measurement only once and the average conditional success probability decreases with the Hilbert space dimension as $1/d$. If the outcomes of the apparatuses are not labeled, then the problem is more complicated. We analyze the case of two-dimensional Hilbert space. In this case single shot comparison is impossible and each measurement device must be used (at least) twice. The optimal test state in the two-shots scenario gives the average conditional success probability 3/4. Interestingly, the optimal experiment detects unambiguously the difference with nonvanishing probability for any pair of observables.

14. **Josef Šprojcar:** Are there any untraceable quantum ballots?

We formulate and prove theorem that gives a negative answer to the following question. Is it possible to create secure voting protocols based on quantum ballots which allow, thanks to the no cloning theorem, protection against ballot counterfeiting. We provided an explicit attack that the adversary can execute to break anonymity of all voters simultaneously and the results of the elections can still be computed.

15. **Levente Szabó:** OPTIMAL UNIVERSAL ASYMMETRIC COVARIANT QUANTUM CLONING CIRCUITS FOR QUBIT ENTANGLEMENT MANIPULATION

    In my talk I will present our recent results regarding entanglement manipulation capabilitiesof the universal covariant quantum cloner [UCQC, c.f. Braunstein, Bužek and Hillery, Phys. Rev. A **63,** 052313 (2001)] or quantum processor circuit for quantum bits. I shall investigate its use for cloning a member of a bipartite or a genuine tripartite entangled state of quantum bits. In the case of bipartite entangled state applying an optimal universal quantum cloning operation to clone one of the members of a maximally entangled pair the resulting state is a Werner state. It is likely, however, that a cloning transformation is realized by some quantum circuit, which uses ancillae for carrying out the operation. It is obviously interesting how the entanglement between the different quantum bits of such a scenario (including also ancillae) behaves.

    I will consider the UCQC as a circuit, not only the cloning operation itself. As it will be shown in detail the ancillae play a very specific role and the behavior of bipartite entanglement as measured by concurrence, shows a rather interesting pattern. The main feature is that behavior of the entanglement between the not cloned part of the pair and the cloned one is repeated in the entanglement of certain ancillae, and so is that of the not cloned qubit and the clone, provided that the original qubit pair was maximally entangled initially. The recent optical realization of certain programmable quantum gate arrays also contributes to the relevance of this question.

    Another similar question might be the partial extraction of bipartite entanglement from a GHZ-type threepartite resource. It is known that if three qubits are in a GHZ state, then a measurement on either of the three qubits in the $|\pm\rangle$ basis (eigenbasis of the σ_x Pauli-operator) projects the state of the remaining two qubits into a maximally entangled state. I will demonstrate that if the given particle is cloned in advance, it is possible to create bipartite entanglement by measuring the clone, while there still remains some purely threepartite entangled resource in the state of the three parties. This is indicated by the possibility of entangling a different pair of qubits by a next measurement. It follows that the universal quantum cloning circuit facilitates the partial extraction of bipartite entangled resources from a genuine tripartite entangled resource. The nature of the entanglement in the multipartite system can be also analyzed with the aid of the Coffman-Kundu-Wootters inequalities, which quantify the monogamy of entanglement. I shall present such an analysis, too.

    In conclusion, I shall show that the universal quantum cloning circuit (or quantum processor) for qubits is found to be useful as an entanglement manipulator as well. It can perform entanglement manipulations which are potentially applicable in quantum information processing. More details can be found in our recent paper: Szabó et al., Phys. Rev. A **81,** 032323 (2010).

16. **Ramon Muñoz-Tapia:** UNIVERSAL PROGRAMMABLE DISCRIMINATION OF GENERAL QUBIT STATES

    Discrimination between quantum states is perhaps the most basic task in quantum information, and yet one of the most non-trivial and theoretically-rich ones. In this talk we consider this task from the perspective of programmable discriminators: devices able to discriminate between any two unknown states. The device has three inputs, two of them are loaded with copies of each state (input registers), and the third is loaded copies of the state one wishes to identify (input data). The device is able to assign the correct nature of the input data with some error probability which depends on the number of copies used. We compute the unambiguous and minimum error probability for any number of pure qubit states in the input ports.

We extend the applicability of the device when the ports are fed with mixed states. In this case no unambiguous answers can be given, but the minimum error probability can be readily computed. The performance of the device for a given purity of the input states allows to quantify the how the discrimination power is degraded in the presence of noise. We also analyse the case of completely unknown input states, i.e. when their purity is randomly distributed according to some reasonable priors. We consider hard-sphere, Bures and Chernoff priors. Such a device can be regarded as the universal programmable device.

When the input ports are fed with n copies of pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ and the data port with m copies, it is possible to give closed expressions for both unambiguous and minimum error probabilities. In the limit of $n \to \infty$ they coincide with the results of the discrimination of *known* states when m copies are available for measurement. When instead $m \to \infty$ keeping a the number of copies at register ports finite, the results coincide with state comparison.

The expressions for mixed states are much more involved. However one can still exploit the permutation symmetry of the input states to write the problem in a block-diagonal form. We then obtain a closed expression for the probability of error that can be computed analytically for small number of copies and numerically evaluated for a fairly large number of copies.

[1] J.A. Bergou and M. Hillery, Phys. Rev. Lett. **94,** 160501 (2005).

[2] A. Hayashi, M. Horibe, and T. Hashimoto, Phys. Rev. A **73,** 012328 (2006).

[3] M. Sedlák, et al., Phys. Rev. A **76,** 022326 (2007).

[4] G. Sentas, E. Bagan, J. Calsamiglia and R. Muñoz-Tapia, work in progress.

Posters

1. **Dmitry Kravchenko:** CHSH GAME WITH ARBITRARY INPUT DISTRIBUTION

CHSH game is a popular illustration of difference between classical and quantum world. Namely, it shows violation of the original Bell's inequality. In terms of the CHSH game, the biggest such violation can be achieved by choosing uniformly distributed players' input. It could be interesting however to study more general case, i.e. CHSH games with different input distributions.

This work is dedicated to those CHSH games, where probabilities of different inputs are restricted only by the requirement of the symmetry with respect to the players. In other words, we describe optimal strategies and outcomes for arbitrary probabilities of input $Pr(0,0)$, $Pr(1,1)$, and $Pr(0,1) = Pr(1,0) = \frac{1-Pr(0,0)-Pr(1,1)}{2}$. Optimal results are given for both quantum and classical versions of such CHSH games.

It turns out that almost all such games demonstrate positive quantum-over-classical advantage. Although formula of this advantage is quite complicated, it can still be computed in $O(1)$.

In order to find optimal strategy for players, we can make some useful restrictions:

(a) Strategies for both players should be equal to each other.

(b) Given x as input, a player should apply operation $\begin{pmatrix} \exp(\phi_x) & 1 \\ -1 & \exp(-\phi_x) \end{pmatrix}$ to a qubit and then make a measurement.

(c) Players always answer with the result of the measurement applied to their qubits.

In fact, there always exists optimal strategy of the form as described above. Winning probability for such strategy is as follows:

$$(1 - Pr(0,0) - Pr(1,1)) \cos(\phi_0 + \phi_1) + Pr(0,0) \cos 2\phi_0 - Pr(1,1) \cos 2\phi_1.$$

In order to find optimal angles ϕ_0 and ϕ_1, it is sufficient to check only limited count of values. These are:

(a) $\phi_0 = \phi_1 = 0$.

(b) $\phi_0 = 0$, $\phi_1 = \frac{\pi}{2}$.

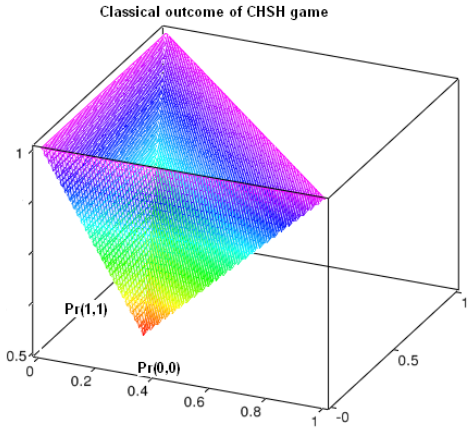
(c) $\phi_0 = -\frac{\pi}{2}$, $\phi_1 = \frac{\pi}{2}$.

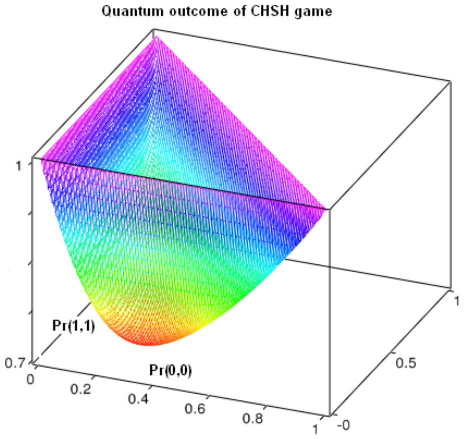
(d) ϕ_0, ϕ_1 such that

$$(1 - Pr(0,0) - Pr(1,1)) \sin(\phi_0 + \phi_1) = -2Pr(0,0) \sin 2\phi_0 = 2Pr(1,1) \sin 2\phi_1.$$

The last case needs some computation, which hardly can be described shortly.

Pictures show that classical outcome depends linearly on input distribution. On the other hand, quantum outcome is of more complicated nature, but is representable by smooth function of input distribution.





2. **Nikolajs Nahimovs:** On fault-tolerance of Grover's algorithm

Grover's algorithm is a quantum search algorithm solving the unstructured search problem in about $\frac{\pi}{4}\sqrt{\frac{N}{M}}$ queries, where M is a number of solutions [1]. It has been analyzed in great detail. The analysis has been mainly focused on the optimality and generalization of the algorithm [2–4], as well as on fault-tolerance of the algorithm to a certain kind of "low-level" (i.e. physical) errors, such as unitary noise and decoherence [5,6].

We study a fault-tolerance of the Grover's algorithm to a "high-level" errors, in our case a failure of a single or multiple queries (omissions of a query transformation). It can be shown that this model is equivalent to other, seemingly more realistic, model [7] in which the oracle's operation is subject to small random phase fluctuations.

We show, that even a single omitted query transformation will on average decrease a number of successful algorithm steps twice (or will twice increase the average runing time of the algorithm). However if a query transformation is omitted right in the middle of the transformation sequence of the algorithm, the transformation sequence changes to an identity transformation. Thus the algorithm will leave the initial state unchanged. The interesting fact is that this property does not depend on a number of solutions. This makes the quantum case completely different from the classical case.

In the general case, we show that $k-1$ omitted query transformations change the length of the resulting transformation sequence of the algorithm from l to a random variable with a mean 0 (even k) or $\frac{l}{k}$ (odd k) and variance $O\left(\frac{l^2}{k}\right)$. Thus k failed queries with a very high probability decrese the length of the resulting transformation sequence of the algorithm $O(\sqrt{k})$ times.

We also show that a similar argument can be applied to a wide range of other quantum query algorithms, such as amplitude amplification, some variants of quantum walks and NAND formula evaluation, etc. That is to any quantum query algorithm for which a transformation X applied between queries has the property $X^2 = I$.

[1] L.K. Grover: *A fast quantum mechanical algorithm for database search,* in proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), pp. 212-219, preprint `arXiv:quant-ph/9605043` (1996).

[2] C. Zalka: *Grovers quantum searching algorithm is optimal,* preprint `arXiv:quant-ph/9711070`.

[3] G. Brassard et al.: *Quantum Amplitude Amplification and Estimation,* preprint arXiv:quant-ph/0005055.

[4] C. Bennett et al.: *Strengths and Weaknesses of Quantum Computing,* SIAM Journal on Computing (special issue on quantum computing) **26,** pp. 1510-1523, preprint arXiv:quant-ph/9701001.

[5] D. Shapira et al.: *Effect of unitary noise on Grover's quantum search algorithm,* Phys. Rev. A **67,** 042301 (2003).

[6] P.H. Song, I. Kim: *Computational leakage: Grover's algorithm with imperfections,* The European Physical Journal D **23,** 299 (2003), preprint arXiv:quant-ph/0010075.

[7] N. Shenvi et al.: *Effects of Random Noisy Oracle on Search Algorithm Complexity,* preprint arXiv:quant-ph/0304138.

3. **Zeynep Nilhan Gurkan:** Entanglement Dependence on Distance Between Interacting Qubits

One of the most important manifestation of nonlocality in quantum mechnanics is entanglement for composite quantum systems [1]. Intriguing nonclassical property of entangled states where illustrated by Einstein, Podolsky and Rosen (EPR) in 1935 [2]. In EPR paradox entangled states maybe located arbitrarily far from each other, then measurement on one of the system allows to determine the state of the second system independent of the distance between the subsystems. In the present paper we study entangled two qubit states and distance dependence of entanglement between the states. We consider the Heisenberg magnetic model which appears not only in spin interactions but also in different realization of qubit interactions as quantum dots, nuclear spins and H_2 molecule. For two qubit interaction in Heisenberg model we calculated entanglement as a function of parameters of the system like the exchange integrals, magnetic fields and DM anisotropic exchange interactions [3].

Recently a relation between entanglement and the electron correlation energy in H_2 molecule has been analyzed in [4] and it was shown that the entanglement can be used as an alternative measure of the electron correlation in quantum chemistry calculations. Despite of the standard definition of electron correlation as the difference between the Hartree-Fock energy and the exact solution of the nonrelativistic Schrödinger equation, it is found that entanglement can be used as an alternative measure of electron correlations. Calculations of the von Neumann entropy and its dependence on distance for various values of magnetic field B has been considered. In these calculations following Herring-Flicker, the exchange coupling constant J for H_2 molecule has been approximated as a function of the interatomic distance $R : J(R) = -0.821R^{5/2}e^{-2R}+O(R^2e^{-2R})$. From another side in condensed matter physics several generalizations of the Heisenberg model by the distance dependent exchange interaction has been studied. In the present work we study two qubit entanglement in XX model versus distance between two qubits for the distance dependent exchange interactions in the form of the Van der Waals type forces, $J(R) \sim e^{-R}$ and for exactly solvable spin models like the Calogero-Sutherland model: $J(R) = 1/R^2$. Firstly we calculate Von Neumann entropy and Wooters concurrence for the ground state of two qubits and compare the results. Then the concurrence for the thermal entanglement and its dependence on the distance at different temperatures are studied.

[1] E. Schrödinger, Proc. Camb. Phil. Soc. **31,** 555 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47,** 777 (1935).

[3] Z.N. Gurkan, O.K. Pashaev, Int. J. Mod. Phys. B **24,** 943.

[4] Z. Huang, S. Kais, Chem. Phys. Lett. **413,** 1 (2005).

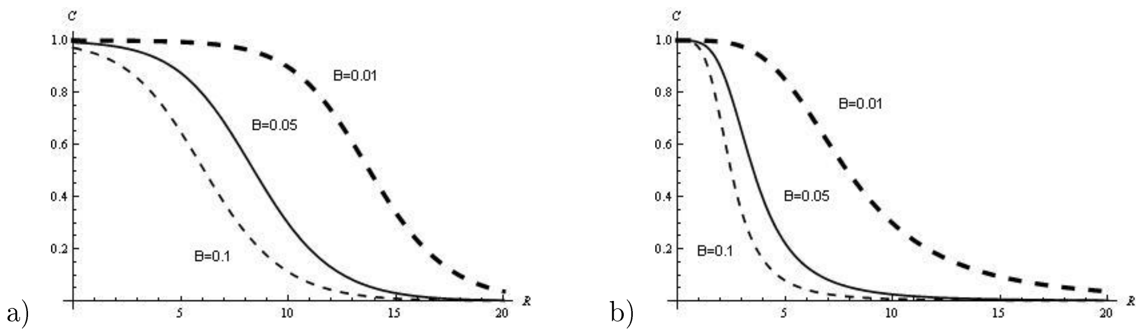


Figure 1: a) Van der Waal. Entropy-Distance, $B = 0.1$, $B = 0.05$, $B = 0.01$, b) Calogero Sutherland. Entropy-Distance, $B = 0.1$, $B = 0.05$, $B = 0.01$.

[5] C. Herring, M. Flicker, Phys. Rev. **134,** A362 (1964).

[6] W.K. Wooters, Phys. Rev. Lett. **80,** 2245 (1998).

[7] W.K. Wooters, Phys. Rev. Lett. **78,** 5022 (1997).

4. **Alexander Rivosh:** A QUANTUM ALGORITHM FOR FUNCTION RECONSTRUCTION

We present an improved algorithm for reading the entire contents of the black box, i.e. all values of oracle function for selected range of arguments. Our approach employs sliding window technique; this reduces necessary quantum or classical memory. Our algorithm can use Grover's algorithm, quantum algorithm for NAND-formula evaluation or quantum random walks as a subroutine. It works best with oracle functions that returns long sequence of 0's followed by a large number of 1's (or vice versa). The algorithm has the same complexity for functions with small number of solutions compared to entire search space. Similar approach can be used to find all local minima/maxima in case of non-binary output of oracle function. That make possible to reconstruct the original oracle function approximately.

[1] L.K. Grover: *A fast quantum mechanical algorithm for database search,* in proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), pp. 212–219 (1996), preprint `arXiv:quant-ph/9605043`.

[2] C. Zalka: *Grovers quantum searching algorithm is optimal,* Phys. Rev. A **60,** 2746 (1999), preprint `arXiv:quant-ph/9711070`.

[3] C. Zalka: *A Grover-based quantum search of optimal order for an unknown number of marked elements,* preprint `arXiv:quant-ph/9902049`.

[4] G.L. Long: *Grover Algorithm with zero theoretical failure rate,* Phys. Rev. A **64,** 022307 (2001), preprint `arXiv:quant-ph/0106071`

[5] A. Ambainis: *Quantum search algorithms (survey),* SIGACT News **35,** 22 (2004), preprint `arXiv:quant-ph/0504012`.

[6] A. Ambainis, A. Childs, B. Reichardt, R. Spalek, S. Zhang: *Any AND-OR Formula of Size N can be Evaluated in time $N^{1/2+o(1)}$ on a Quantum Computer,* in proceedings of FOCS'2007, pp. 363–372, preprint `arXiv:quant-ph/0703015` and `arXiv:quant-ph/0704.3628`.

[7] A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R. Putra, S. Yamashita: *Quantum identification of Boolean oracles,* in proceedings of STACS'04, pp. 105–116, preprint `arXiv:quant-ph/0403056`.

5. **Christoph Spengler:** The state space geometry of the CGLMP-Bell inequality

   We compare entanglement with the violation of a Bell inequalitiy using a geometric structure in the state space of bipartite qudits. Determining whether a given quantum state obeys or violates a Bell inequality is a high-dimensional nonlinear constrained optimization problem for which in most cases there is no analytic solution available. Based on an advantageous parameterization we are able to study numerically a special set of states of bipartite qudit systems, namely convex combinations of generalized Bell states defining a simplex. This simplex is ideal for studying properties of density matrices due to the fact that any element can be descriptively represented by a real vector. We find that the shape of the boundaries of separability and states violating the CGLMP-Bell inequality are significantly different. Moreover, we confront the strength of violation with a recently proposed entanglement measure. We show that the implied orders for these density matrices are different, i.e. in general there exists no monotonous relation between a Bell inequality violation and the amount of entanglement.

6. **Martin Suda:** Quantum interference between a single-photon Fock state and a coherent state

   Optical quantum computing became feasible using linear optical elements, single-photon sources, and detectors. It requires an integrated optics architecture for improved performance, miniaturization, and scalability. We present a simple analytical expression for the single mode quantum field state at the individual output ports of a beam splitter when a coherent state and a single-photon Fock state are incident on the input ports. This output state turns out to be a statistical mixture between a coherent state and a displaced Fock state. Consequently we are able to find an analytical expression for the corresponding Wigner function. We further extend our calculations to the case of a Mach-Zehnder interferometer with the same input fields, obtaining analytical results formally analogous to those of the beam splitter output ports. We also make some remarks about the general case for which the single-photon Fock state is replaced with an arbitrary input state.

7. **Jan Vlach:** Gaussian quantum marginal problem

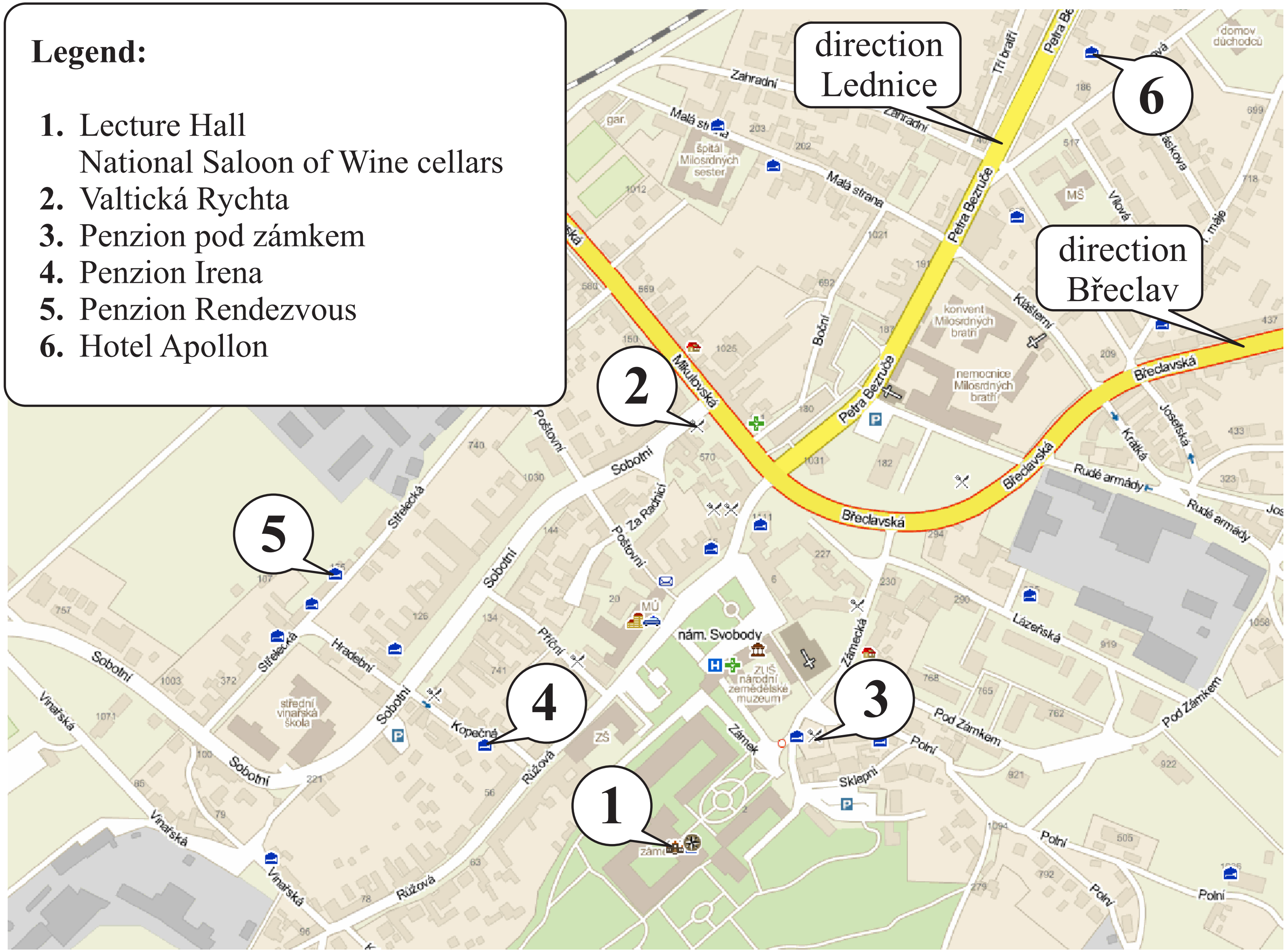
   Marginal problem deals with the existence of the probability distribution on the n-dimensional space V when we have given marginal probability distributions on subspaces of V. In quantum physics it can be thought of as the problem of compatibility between quantum states of some physical system and quantum states of its subsystems. The restrictions can be given in terms of inequalities between eigenvalues of involved systems. Many forms of the quantum marginal problem have been solved. The simplest cases include pure state of 2 qubits, pure state of 3 qutrits, etc. Their solution is given by system of a few inequalities. Quantum marginal problem was solved in full generality for finite-dimensional systems [1].

   Solution of the general quantum marginal problem for infinite-dimensional systems is not known. However we can consider only Gaussian states which are most important in contemporary quantum-optical experiments. Their advantage is that they can be fully described only by their first and second moments. Moreover the first moments do not affect entanglement properties and can always be made zero by local displacement in phase space. Therefore Gaussian states can be represented only by covariance matrix γ. Gaussian quantum marginal problem is concerned with the relation between symplectic eigenvalues of the composite system and its subsystems.

The most general Gaussian quantum marginal problem deals with composite systems with n modes and reduced systems which have m, $m < n$. There is a known solution for the case where all reduced systems consist of exactly one mode [2]. My talk will be focused on generalizations of this result.

[1] A. Klyachko: *Quantum marginal problem and representations of the symmetric group,* preprint `arXiv:quant-ph/0409113` (2004).

[2] J. Eisert, T. Tyc, T. Rudolph, and B.C. Sanders: *Gaussian Quantum Marginal Problem,* Commun. Math. Phys. **280,** 263 (2008).



Legend:

1. Lecture Hall
   National Saloon of Wine cellars
2. Valtická Rychta
3. Penzion pod zámkem
4. Penzion Irena
5. Penzion Rendezvous
6. Hotel Apollon