2nd Bielefeld Workshop on Quantum Information and Complexity

AG Information und Komplexität,
Fakultät für Mathematik, Universität Bielefeld

October 12–14, 2000

Editors:
R. Ahlswede and A. Winter

Collected abstracts

Quantum Distribution of Gaussian Keys with Squeezed States

Gilles van Assche
Ecole Polytechnique, CP 165/56, Université Libre de Bruxelles,
50 avenue F. D. Roosevelt, B–1050 Bruxelles, Belgium.
`gvanassc@ulb.ac.be`

A continuous key distribution scheme is proposed that relies on a pair of canonically conjugate quantum variables. A Gaussian secret key can be shared between two parties by encoding it into one of the two quadrature components of a single-mode electromagnetic field. In the case of an individual attack based on the optimal continuous cloning machine, it is shown that the information gained by the eavesdropper simply equals the information lost by the receiver.

Quantum message authentication codes

Howard Barnum
Department of Computer Science, University of Bristol,
Merchant Venturers' Building, Bristol BS8 1UB, UK.
`hbarnum@cs.bris.ac.uk`

I describe protocols intended to enable the recipient of a quantum state to assure himself that the state has come from a sender with whom he has previously shared secret key. As with the classical protocols of Simmons, of Gilbert, MacWilliams, and Sloane, and of Wegman and Carter, security is information-theoretic rather than based on computational assumptions. The protocol is conjectured to be efficient in that the probability of undetected tampering drops exponentially with key size with only weak, perhaps logarithmic dependence on message size. For various classes of attacks, this conjecture is verified.

Measure of Quantum Entanglements and Invariants

Shao-Ming Fei
Institute of Applied Mathematics, University of Bonn,
D–53115 Bonn, Germany.
`fei@wiener.iam.uni-bonn.de`

We study the measure of quantum entanglements according to the invariance under local unitary transformations. A generalized explicit formula of concurrence for M N-dimensional quantum systems is presented.

Quantum Finite Automata

Rūsiņš Freivalds
University of Latvia, Raia bulvris 29, LV–1459, Riga, Latvia.
`rusins@paul.cclu.lv`

It was shown in [KW97] that the class of languages recognized by 1–way QFAs is a proper subset of regular languages.

If we wish to find out whether a QFA recognizes the given language, the answer depends on the accepting probability of the QFA. It was proved in [AF98] that if the QFA is to give the correct answer with a large probability (greater than $\frac{7}{9}$), then the same language can be recognized with probability 1. However, some of such languages can be recognized by QFA with a probability 0.68... However, $\frac{7}{9}$ is greater than 0.68 ... Now we have found the precise value of the crucial threshold. It is $\frac{52+4\sqrt{7}}{81}$.

In [AF98] a property of deterministic finite automata was found such that if the minimal automaton for a regular language has this property, then the language cannot be recognized with a probability higher than the crucial probability above. [BP99] generalized this property to show that if for various input words this property can happen unlimited number of times, then the regular language cannot be recognized by a QFA with any probability exceeding $\frac{1}{2}$.

Māris Valdats proved that the construction in [BP99] is not the only obstacle for a language to be recognized by a QFA. This way he proved that there are regular languages L_1 and L_2 such that they are recognizable by QFA with a probability exceeding $\frac{1}{2}$ but their intersection is not recognizable by a QFA with any probability exceeding $\frac{1}{2}$.

References

[AF98] Andris Ambainis and Rūsiņš Freivalds, "1–way quantum finite automata: their strengths, weaknesses and generalizations", in: Proc. 39th FOCS, 1998, pp. 332–341. Also e–print quant-ph/9904066.

[BP99] Alex Brodsky, Nicholas Pippenger, " Characterizations of 1–Way Quantum Finite Automata", e–print `quant-ph/9903014`.

[KW97] Attila Kondacs and John Watrous, "On the power of quantum finite state automata", in: Proc. 38th FOCS, 1997, pp. 66–75.

Quantum algorithmic entropy

Peter Gács
Computer Science Department, Boston University,
Boston, MA 02215, USA.
`gacs@bu.edu`
Presently at CWI, Kruislaan 413, P.O. Box 94079,
1090 GB Amsterdam, The Netherlands.
`Peter.Gacs@cwi.nl`

We extend algorithmic information theory to quantum mechanics. Due to difficulties and ambiguities in finding an appropriate notion of description complexity for quantum states, we take the construction of a universal semicomputable density matrix ("apriori probability") as a starting point, and define complexity as its negative logarithm.

A number of properties of Kolmogorov complexity extend naturally to the new domain. Approximately, a quantum state is simple if it is within a small distance from a low-dimensional subspace of low Kolmogorov complexity. The von Neumann entropy of a computable density matrix is within an additive constant from the average complexity. Some of the theory of randomness translates to the new domain, but new questions arise due to non-commutativity.

We explore the relations of the new quantity to the quantum Kolmogorov complexity defined by Vitányi (we show that the latter is sometimes as large as $n - 2\log n$) and the qubit complexity defined by Berthiaume, van Dam and Laplante.

On the Uniqueness of Chentsov Metric in Quantum Information Geometry

Matheus Grasselli
Department of Mathematics, King's College, Strand,
London WC2R 2LS, UK.
`matheus@math.kcl.ac.uk`

We study the metrics on a finite quantum information manifold for which the exponential and mixture connections are dual (in the sense of Amari). Combining this result with the characterization of monotone metrics given by Petz, we reduce the set of possible such metrics to multiples of the BKM (Bogoliubov-Kubo-Mori) inner product.

This is joint work with R. F. Streater, e-print `math-ph/0006030`.

Kuhn-Tucker Conditions for Quantum Capacity

Peter Harremoës
Roenne Alle 1 st., DK–Soeberg, Denmark.
`moes@post7.tele.dk`

When sending classical information through a quantum channel we search for the optimal output state. In the talk the necessity and sufficiency of Kuhn-Tucker conditions for optimality will be demonstrated. Some related inequalities will be discussed.

Large deviation type bounds in quantum estimation

Masahito Hayashi
Laboratory for Mathematical Neuroscience, Brain Science Institute,
RIKEN, Tokyo, Japan.
`masahito@brain.riken.go.jp`

We discuss that two kinds of Bahadur type bounds (large deviation bounds) appear in the quantum parameter estimation for a one-dimensional parameter. In the classical case, we can derive Bahadur type bound from Stein's lemma of the hypothesis testing. It was proved that the bound can be attained by the maximum likelihood estimator under a regularity condition on the probability family.

Recently, the quantum version of Stein's lemma has been proved from the combination of Hiai–Petz's results and Ogawa–Nagaoka's. As in the classical case, this seems to imply that the quantum version of Bahadur type bound is given by the half of Bogoljubov inner product which is the limit of quantum relatve entoropy. We should note, however, that in the one–parameter case the bound of mean square error (MSE) under the unbiasedness condition is given by SLD-inner prodect, which is introduced by Helstrom. In general, these two inner products don't coincide. In the quantum case, Bahadur type bound under the weak consistency is different from Bahadur type bound under the uniformal convergence of the exponential rate. The former is given by Bogoljubov inner product, and the latter is by SLD inner product. These two bounds can be attained in the respective senses.

Error Exponents for Quantum Gaussian Channels

Alexander S. Holevo
Steklov Mathematical Institute, Russian Academy of Sciences,
Moscow, Russia.
`holevo@mi.ras.ru`

Basing on the general expressions for the random coding and expurgation bounds for the reliability function of classical-quantum channel with continuous alphabet and constrained inputs, we compute several important information quantities for a general quantum Gaussian channel, such as: the Gallager functions, the cutoff rate and margins for the reliability function at zero rate. This reqires some new formulas for quantum Gaussian states, namely the quantum Fourier transform of arbitrary positive degree of a Gaussian density operator and the fidelity between two Gaussian states.

Tools for quantifying entanglement and evaluating quantum capacities

Michal Horodecki
Institute of Theoretical Physics and Astrophysics, University of Gdansk,
ul. Wita Stwosza 57, 80–952 Gdansk, Poland.
`michalh@iftia.uni.gda.pl`

Teleportation and quasidistillation fidelity thresholds

Pawel Horodecki
Faculty of Applied Physics and Mathematics,
Technical University of Gdansk, 80–952 Gdansk, Poland.
`pawel@mif.pg.gda.pl`

Comparing the power of classical and quantum computation

Richard Jozsa
Department of Computer Science, University of Bristol,
Merchant Venturers' Building, Bristol BS8 1UB, UK.
`R.Jozsa@bristol.ac.uk`

It is well known that for some computational tasks (such as integer factorisation) quantum processes can offer an exponential speedup in time over any known classical computational method. We will consider the question: what is the physical origin of the extra power of quantum computation? We show that for quantum computations on pure states an exponential benefit can be obtained only if there is increasing multi-partite entanglement with increasing input size. Computations with mixed states are more complicated and it seems possible that exponential benefits might be exhibited by processes operating with only separable mixed states. However recent work of Popescu, Linden and Braunstein has shown that the special case – of implementing the known quantum algorithms with so-called pseudo-pure states (eg as in liquid state NMR quantum computing) – cannot exhibit an exponential benefit in physical resources over classical computation, if the states remain separable throughout the computation. Finally we will make some remarks on the comparison of quantum computation with classical analogue computation.

Generalized Shannon's Information Between Quantum Systems

Lev B. Levitin
Boston University, College of Engineering, Department of Electrical and
Computer Engineering, 8 St. Mary's Street, Boston, MA 02215, USA.
`levitin@bu.edu`

The concepts of conditional entropy of a physical system given the state of another system and of information in a physical system about another one are generalized for quantum systems. The fundamental difference between the classical case and the quantum one is that those quantities in quantum systems depend on the choice of measurements performed over the systems. It is shown that some equalities of the classical information theory turn into inequalities for the generalized quantities. Examples such as EPR pairs and "superdense coding" are described and explained in terms of the generalized conditional entropy and information.

Noncommutative tomography of analytical signal and entanglement in the probability representation of quantum mechanics

Margarita M. Man'ko
P. N. Lebedev Physical Institute, Leninskii Prospect 53,
Moscow 117924, Russia.
`mmanko@sci.lebedev.ru`

Review of tomographic representation of quantum states [1], in which the standard probability is used instead of wave function, is presented. The corresponding procedure of noncommutative tomography of analytic signal introduced in [2] is used for the description of an analytic signal depending both on time and spatial variables [3]. Quantumlike information coded by states of charged-particle beam is considered within the framework of tomographic probability [4]. Entropy and entanglement theory of the analytic signal in the noncommutative-tomography scheme is discussed in connection with information processing.

[1] S. Mancini, V.I. Man'ko, and P. Tombesi, Phys. Lett. A, Vol. 213, p. 1 (1996); Found. Phys., Vol. 27, p. 801 (1997).

[2] V.I. Man'ko and R.V. Mendes, Phys. Lett. A, Vol. 263, p. 53 (1999).

[3] M.A. Man'ko, J. Russ. Laser Res. (Kluwer/Plenum), Vol. 20, p. 225 (1999); Vol. 21, p. 411 (2000).

[4] R. Fedele, M.A. Man'ko, and V.I. Man'ko, J. Russ. Laser Res. (Kluwer/Plenum), Vol. 21, p. 1 (2000); J. Opt. Soc. Am. (2000, in press).

The asymptotic quantum Cramér–Rao type bound of the positive full model

Keiji Matsumoto
Quantum Computation and Information Project, JST,
5–28–3, Hongo, Bunkyo–ku, Tokyo 113–0033, Japan.
`keiji@expm.t.u-tokyo.ac.jp`

Calculation of the asymptotic lower bound of error of the estimate is made, when

1. the quantum correlation between samples are used,
2. the Hilbert space is finite dimensional,
3. the model is the positive full model,

which is the set of all the strictly positive density matrices.

The conjecture about the theory in the general case is presented with naive proof.

Protocols for Quantum Steganography

David J. Santos
Departamento de Tecnologías de las Comunicaciones, Universidad de Vigo,
Campus Universitario s/n. E–36200 Vigo, Spain.
`dsantos@tsc.uvigo.es`

We investigate the concept of quantum steganography. Fundamental concepts from quantum information processing such as quantum superposition, particle entanglement and dense-coding are used to show the feasibility of subliminal quantum communication channels. Like in quantum cryptography, the use of these quantum-mechanical techniques leads to more robust hidden communication strategies.

A new construction of quantum error correcting codes

Dirk Schlingemann
Institut für Mathematische Physik, TU Braunschweig,
Mendelssohnstraße 3, D–38106 Braunschweig, Germany.
`d.schlingemann@tu-bs.de`

Ground state cooling, quantum state engineering, and study of decoherence of ions in Paul traps

Ferdinand Schmidt–Kaler
Institut für Experimentalphysik, Universität Innsbruck,
Technikerstraße 25, A–6020 Innsbruck, Austria.
`ferdinand.schmidt-kaler@uibk.ac.at`

Single ions in Paul traps are investigated for quantum information processing. Single $^{40}\mathrm{Ca}^{+}$ ions are either held in a spherical Paul trap or alternatively, in a linear Paul trap.

We report on the following steps towards a ion–quantum processor:

1. addressing individual ions the trap [1].
2. cooling of single ions and of ion–crystals into the vibrational ground state [2,3].
3. coherent manipulation of the ion's qubit state [2].
4. theoretical and experimental investigations of the speed limits of gate operations [4].
5. measurements of the vibrational and the internal decoherence of the qubit states [2,3].
6. a novel method for simultaneously cooling all vibrational modes of an ion–crystal.

As a conclusion, we will give the perspective of small–scale ion–trap quantum–processors.

[1] H. C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt–Kaler, and R. Blatt, Phys. Rev. A 60, 145 (1999).

[2] Ch. Roos, Th. Zeiger, H. Rohde, H. C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt–Kaler, and R. Blatt, Phys. Rev. Lett., 83, 4713 (1999).

[3] F. Schmidt–Kaler, Ch. Roos, H. C. Nägerl, H. Rohde, S. Gulde, A. Mundt, M. Lederbauer, G. Thalhammer, Th. Zeiger, P. Barton, L. Hornekaer, G. Reymond, D.Leibfried, J. Eschner, and R. Blatt, e-print `quant-ph/0003096`.

[4] A. Steane, C. F. Roos, D. Stevens, A. Mundt, D. Leibfried, F. Schmidt–Kaler, and R. Blatt, e–print `quant-ph/0003087`, Phys. Rev. A. 62, 0423XX.

The definition of a random sequence of qubits: from noncommutative algorithmic probability to quantum algorithmic information theory and back

Gavriel Segre
Dipertimento di Fisica Nucleare e Teorica and I.N.F.N.,
Universitá di Pavia, Via Bassi 6, 27100 Pavia, Italy.
`Gavriel.Segre@pf.infn.it`

The issue of defining a random sequence of qubits is studied in the framework of Algorithmic Free Probability Theory. Its connection with Quantum Algorithmic Information Theory is shown.

The SU(2) Quantum Phase of Photons and Polarization Entanglement

Alexander S. Shumovsky
Physics Department, Bilkent University, Bilkent, 06533 Ankara, Turkey.
`shumo@fen.bilkent.edu.tr`

In recent years, the entanglement has been recognized as one of the most fundamental features of quantum systems as well as an important tool for quantum communications and quantum information processing. One of the most important ways of practical realization of entangled states is related to the so-called two-photon polarization entanglement, when the measurement of polarization of one photon gives information about the polarization of the second photon (e.g., see Section 12.14 in [1]). We now note that the quantum electrodynamics interprets the polarization as a given spin state of photons [2]. Since, the photon spin is 1, the polarization can be described by the Stokes operators, forming a representation of the SU(3) sub-algebra in the Weyl-Heisenberg algebra of photon operators [3]. The multipole photons emitted by the atomic transitions correspond to the states with given angular momentum, consisting of the spin and orbital parts, and therefore have no well-defined polarization.

It is shown that the quantum noise of polarization measurements with multipole photons strongly exceeds that of the plane waves of photons [4]. This result is important for estimation of precision of measurements in the two-photon polarization entanglement as well as in the engineered atomic entanglement due to the photon exchange between the trapped atoms [5].

It is also shown that an adequate picture of the interaction between the atomic transitions and multipole photons is provided by a new dual representation of the Weyl-Heisenberg algebra of the photon operators, taking into account the SU(2) symmetry of the multipole photon states [6]. In particular, this representation permits us to define the intrinsic quantum phase of photons referred to the SU(2) phase of the angular momentum. The sine and cosine of the phase operators coincide with the Cartan algebra of the SU(3) algebra of Stokes operators. The representations of quantum phase are constructed in the case of multipole radiation in empty space as well as in the spherical and one-dimensional (Fabry-Pérot) resonant cavities. The SU(2) quantum phase of photons has discrete spectrum in the interval $(0,2\pi)$. In the classical limit of infinitely many photons in coherent state, the eigenstates of phase cover this interval uniformly. The problem of phase-intensity entanglement is discussed.

[1] L. Mandel, E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, New York, 1995).

[2] V. B. Berestetskii, E. M. Lifshitz, and L. P. Pitaevskii, *Quantum Electrodynamics* (Pergamon Press, Oxford, 1982).

[3] A. S. Shumovsky and Ö. E. Müstecaplioğlu, Phys. Rev. Lett. 80, 1202 (1998); Optics Commun. 146, 124 (1998).

[4] A. S. Shumovsky, e-print `quant-ph/0007109` (2000).

[5] S. Haroche, "Cavity Quantum Electrodynamics: a Review of Rydberg Atom-microwave Experiments", AIP Conf. Proc., vol. 464, issue 1, p. 45 (1999).

[6] A. S. Shumovsky, J. Phys. A 32, 6589 (1999)

Fidelity, concurrence, and the geometry of state space

Armin Uhlmann
Institut für Theoretische Physik, Universität Leipzig,
Augustusplatz 10, D–04109 Leipzig, Germany.
`armin.uhlmann@itp.uni-leipzig.de`

Entanglement measures under symmetry

Karl Gerd Vollbrecht
Institut für Mathematische Physik, TU Braunschweig,
Mendelssohnstraße 3, D–38106 Braunschweig, Germany.
`k.vollbrecht@tu-bs.de`

One of the reasons the general theory of entanglement has proved to be so difficult is the rapid growth of dimension of the state spaces. By restricting to symmetric states, the state space can be reduced and entanglement measurements can be calculated more easily. These examples of state spaces may be helpful to gain intuition for the entanglement measurements and for testing hypotheses. One result is a counterexample for the additivity of the relative entropy of entanglement.

Some remarks on quantum tomography

Andreas Winter
SFB 343, Fakultät für Mathematik, Universität Bielefeld,
Postfach 100131, D–33501 Bielefeld, Germany.
`winter@mathematik.uni-bielefeld.de`

Bound entangled Gaussians

Michael Wolf
Institut für Mathematische Physik, TU Braunschweig,
Mendelssohnstraße 3, D–38106 Braunschweig, Germany.
`mm.wolf@tu-bs.de`

States relevant in quantum optics are often of a special kind, having Gaussian Wigner distributions. For this class of "continuous variable systems" typical questions of quantum information theory are luckily of the same complexity as for the usual finite dimensional systems since basic entanglement properties of a Gaussian state can easily be translated into properties of its covariance matrix. Investigating the relationship between separability and positive partial transpose it turns out that for systems of $1 \times N$ oscillators these two properties are indeed equivalent. However this equivalence fails for all higher dimensions, i.e. there exist bound entangled Gaussian states for 2×2 oscillators.