QIP 2001 Program

January 29, 2001

1 Schedule

Overview

	Tuesday	Wednesday	Thursday	Friday	
9:00	coffee & registration				9:00
9:30		coffee	coffee	coffee	9:30
9:50	welcome				9:50
10:00	Jozsa	Tapp	Nielsen	't Hooft	10:00
10:45	Plenio	Ambainis	Brassard	coffee	10:45
11:15				Cleve	11:15
11:30	coffee	coffee	coffee		11:30
12:00	Vedral	Terhal	de Wolf	van Dam	12:00
12:45	lunch break	lunch break	lunch break	lunch break	12:45
14:30	Høyer	Aharonov	DiVincenzo	open session	14:30
15:15	Farhi	Vazirani	Gács		15:15
16:00	coffee	poster session	coffee		16:00
16:15	Watrous	& reception	Bennett	QAIP meeting	16:15
18:00	mayor's reception				18:00
19:00			banquet		19:00

Sessions

Information Theory I

Tuesday, January 9, Morning — Session Chair: Harry Buhrman
9:50 *Gerard van Oortmerssen*: **Welcome by the Director of CWI**
10:00 *Richard Jozsa*: **On the Reversible Extraction of Classical Information from a Quantum Source**
10:45 *Martin Plenio*: **A New Inequality for the Quantum Relative Entropy and some Applications**
12:00 *Vlatko Vedral*: **Classical and Quantum Correlations in Quantum Computation**

Algorithms and Complexity I

Tuesday, January 9, Afternoon — Session Chair: Umesh Vazirani
14:30 *Peter Høyer*: **Quantum Ordered Searching**
15:15 *Edward Farhi*: **Quantum Computation by Adiabatic Evolution**
16:15 *John Watrous*: **Quantum Algorithms for Solvable Groups**

Cryptography

Wednesday, January 10, Morning — Session Chair: Gilles Brassard
10:00 *Alain Tapp*: **Private Quantum Channels and Quantum Authentication**
10:45 *Andris Ambainis*: **A New Protocol and Lower Bounds for Quantum Coin Flipping**
12:00 *Barbara Terhal*: **Data Hiding with Mixtures of Bell States**

Algorithms and Complexity II

Wednesday, January 10, Afternoon — Session Chair: Charles Bennett
14:30 *Dorit Aharonov*: **Do Quantum Drunks Walk Faster?**
15:15 *Umesh Vazirani*: **The Non-Abelian Hidden Subgroup Problem**

Communication and Complexity

Thursday, January 11, Morning — Session Chair: Richard Cleve
10:00 *Michael Nielsen*: **Entanglement and Distributed Quantum Computation**
10:45 *Gilles Brassard*: **Trading Entanglement for Communication**
12:00 *Ronald de Wolf*: **Quantum Fingerprinting, Simultaneous Message Passing, and Data Structures**

Information Theory II

Thursday, January 11, Afternoon — Session Chair: Richard Jozsa
14:30 *David DiVincenzo*: **Remote State Preparation**
15:15 *Peter Gács*: **Quantum Algorithmic Entropy**
16:15 *Charles Bennett*: **Degrees of Knowledge of Quantum States and Operations**

Closing Session

Friday, January 12, Morning — Session Chair: Harry Buhrman
10:00 *Gerard 't Hooft*: **Quantum Mechanics and Determinism at the Planck Scale**
11:15 *Richard Cleve*: **Fast Parallel Algorithms for the Quantum Fourier Transform**
12:00 *Wim van Dam*: **Efficient Quantum Algorithms for Shifted Quadratic Character Problems**

Open Session

Friday, January 12, Afternoon — Session Chair: Ronald de Wolf

14:30 *Howard Barnum*, Bristol:
Quantum Data Authentication

14:40 *Guifré Vidal*, Innsbruck:
Probabilistic programmable quantum gates

14:50 *Julia Kempe*, Berkeley:
A New Separability Criterion

15:00 *Robert Raussendorf*, Munich:
A One-Way Quantum Computer

15:10 *Erich Novak*, Jena:
Quantum Complexity of Integration

15:20 *Frank Verstraete*, Leuven:
Mixing Versus Entanglement in Two Qubits

15:30 *Hartmut Klauck*, CWI:
Rounds in Quantum Communication

15:40 *Ernesto Galvão*, Oxford:
Experimental Requirements for Quantum Communication Complexity

Events

Mayor's Reception

January 9, 6pm–7pm at the "Koffiekamer Raad," City Hall, Amstel 1. Requires the invitation included in the conference portfolio.

Poster Session and Reception

January 10, 4pm–6pm. Abstracts of the posters will be published during the conference on a billboard.

Koenraad Audenaert, KU Leuven:
Negativity and Concurrence of mixed 2×2 states

Howard N. Barnum, University of Bristol:
Multipartite Entanglement Monotones

Jan Bouda, Masaryk University, Brno:
Entanglement Swapping between Qudit Systems

Paul Cain/Dimitris Dovinos, Cambridge University:
Coupled Quantum Dots by Trench Isolation in SiGe

Keath Chen, Rochester Institute of Technology:
On the Reconciliation Procedure for Quantum Key Distribution

Dong Pyo Chi, Seoul National University:
Initialization-free Function-dependent Phase Transform

Andrew Childs, MIT:
Finding Cliques by Quantum Adiabatic Evolution

Igor Devetak, Cornell University:
Quantum Rate-Distortion Theory

Gerald Gilbert, MITRE, USA:
High-Speed Quantum Cryptography SATCOM

Gil Harel, Free University Amsterdam:
Non-holonomic Quantum Devices

Sofyan Iblisdir, Université Libre de Bruxelles:
Optimal N-to-M Cloning and Phase-conjugation Transformations for Continuous-variable Quantum Systems

Sinisa Karnas, University of Hannover:
Separability in $C^2 \times C^2 \times C^N$ Composite Quantum States

Viv Kendon, Imperial College, London:
Entanglement in Arrays of Qubits

Hirotada Kobayashi, ERATO, Japan:
Two-way Quantum One-counter Automata

Debby Leung, IBM, USA:
Quantum Vernam Cipher

Keiji Matsumoto, JST, Japan:
Asymptotic Theory of Statistical Estimation of the Positive Full Model

Fumiaki Morikoshi, NTT Basic Research Laboratories:
Deterministic Entanglement Concentration

Mio Murao, Semiconductor Labs, RIKEN:
Remote Information Concentration Using a Bound Entangled State

Arkadiusz Orlowski, Institute of Physics PAS, Poland:

Teleportation of Entanglement

Massimo Pica Ciamarra, Università di Napoli:
Quantum Automata and the Link between Reversibility and Space Complexity

Robert Raussendorf, LMU Munich:
Quantum Computing with Cluster States

Yu Shi, Cavendish Laboratory, Cambridge:
Extracting Computational Power From Macroscopic Quantum Coherence

Robert Spreeuw, University of Amsterdam:
Classical Analogy of Quantum Information Processing

Gilles Van Assche, Université Libre de Bruxelles:
Quantum Distribution of Gaussian Keys with Squeezed States

Paolo Zanardi, ISI, Torino:
Entanglement and Entangling power of Quantum Evolutions

Conference Banquet

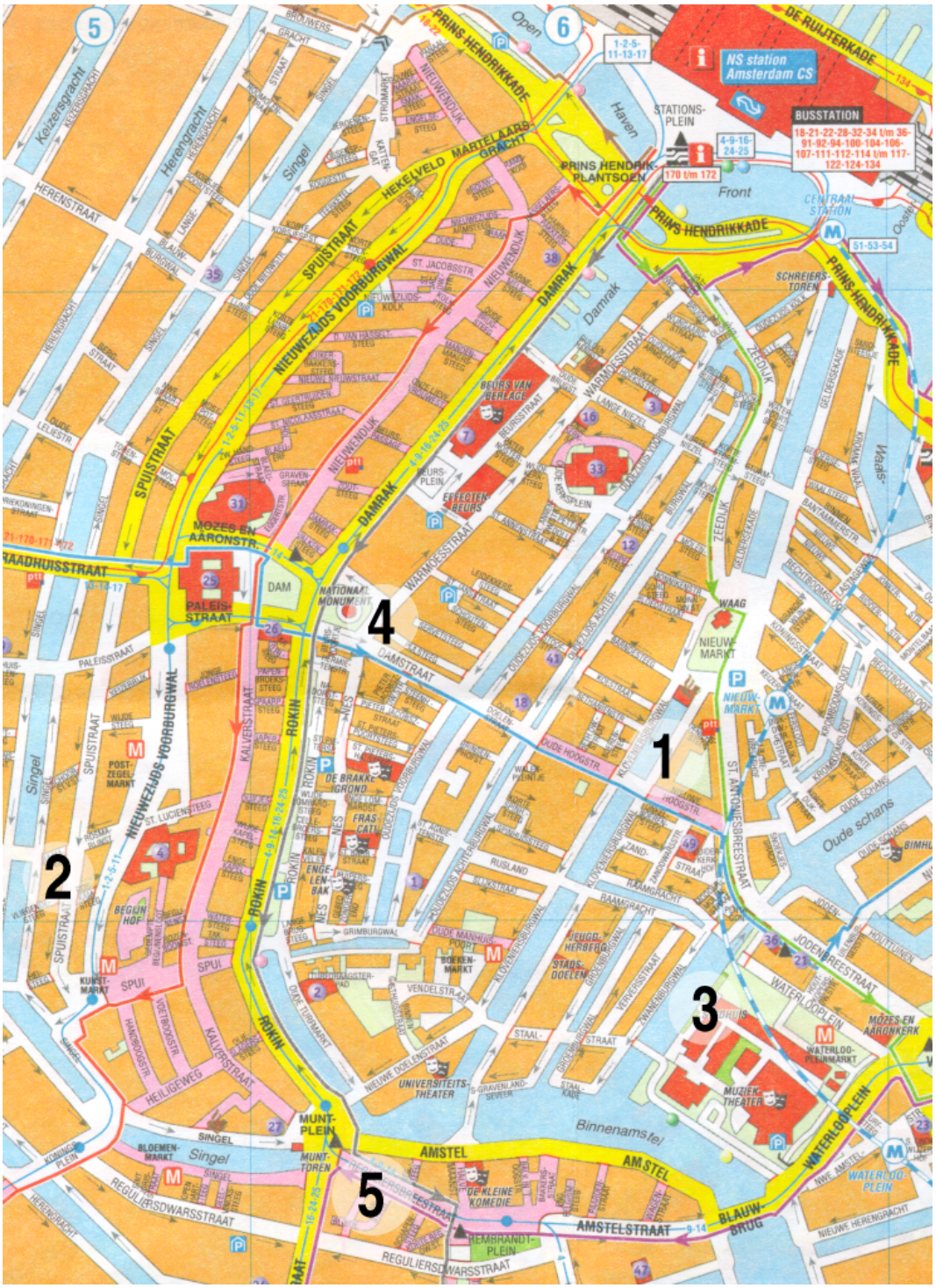
January 11, 7pm–11pm at the Hotel Krasnapolsky on Dam Square 9. Banquet ticket required.

QAIP Meeting

For separately invited members of the EU QAIP project.

2 Directions

Map



1. Conference venue: Het Trippenhuis, Kloveniersburgwal 29
2. Conference hotel: Tulip Inn, Spuistraat 288-292
3. Mayor's reception: "Koffiekamer Raad" of City Hall, Amstel 1
4. Conference banquet: "Wintertuin" of Hotel Krasnapolsky, Dam Square 9
5. Internet Café easyEverything: Regulierstraat 22 (open 24 hours, ticket included in portfolio)

Lunch Restaurants

Amsterdam is full of restaurants. Most areas offer expensive as well as inexpensive restaurants, of many ethnic varieties, and the Nieuwmarkt-area is one of the better areas. Below we list some suggestions for places to have lunch in the vicinity of the conference venue. Additional information can be found in the Internet Guide to Amsterdam, which is included in the conference portfolio.

Kloveniersburgwal

- 6–8: Amsterdam Brouwhuis Maximiliaan
- 14: Song Kwae (Thai)
- 18: Raan Phad Thai
- 34: Avi's Roti Shop (Surinam)

Nieuwmarkt

- In the middle of the square: De Waag
- 10: Chao Praya (Thai)
- 15: Café Fonteyn
- 18: Albert Heijn (a supermarket, also selling sandwiches etc.)
- 24: Poco Loco (Mexican)
- 26: Plein 26 (snack bar, French fries)
- 34: Lokaal 't Loosje (sandwiches)
- 38: Toho Joyce (Indonesian)

Geldersekade

- 109: 't Tuinfeest
- 129: Eetcafé Stevens

Zeedijk

- Many small and inexpensive restaurants, particularly Chinese ones

Sint Antoniebreestraat

- 1: Dutch Bakery
- 25: Bonjour Madame (bakery)
- 142: Tisfris

Jodenbreestraat

- 3: Katz
- 94: Soup en zo (soup and sandwiches)

Nieuwe Doelenstraat

- 20: De Jaren

3 Abstracts of Invited Talks

Do Quantum Drunks Walk Faster?

Dorit Aharonov, Hebrew University

Finite Markov Chains have algorithmic applications in many areas, where the efficiency of the algorithm depends crucially on the mixing time. Can Quantum walks mix faster than Random walks?

We define quantum walks on finite graphs. An interesting question is how to capture the notion of mixing time in such processes; Quantum walks are unitary, and therefore we cannot expect convergence to a stationary distribution. Nevertheless, the notion of *quantum mixing time* can be defined, which captures the speed at which the process evolves.

We show that for the quantum walk on a circle of length n, the quantum mixing time is almost quadratically faster than its classical analogue. On the other hand, we prove a lower bound, showing that for any graph, a quantum walk can mix at most polynomially faster than its classical analogue.

Joint work with Andris Ambainis, Julia Kempe, and Umesh Vazirani.

http://arxiv.org/abs/quant-ph/0012090

A New Protocol and Lower Bounds for Quantum Coin Flipping

Andris Ambainis, UC Berkeley

Alice and Bob want to flip a coin but they do not trust one another. They want to have a protocol that

- would produce each of two results (0 and 1) with probability 1/2 each if both Alice and Bob follow the protocol
- if one of them follows the protocol but the other does not, the person who follows the protocol is guaranteed that each outcome has probability at most $1/2 + \epsilon$.

Mayers, Salvail and Chiba-Kohno showed that there is no quantum protocol that achieves $\epsilon = 0$. However, arbitrarily small $\epsilon > 0$ might be achievable. In this talk, I will present two new results about quantum coin flipping.

First, I will show a simple quantum protocol for coin flipping in which no cheating party can achieve one outcome (0 or 1) with probability more than 0.75. This is the best provable result known and it improves the previous 0.91... of Aharonov, Ta-Shma, Vazirani and Yao (STOC'00.) I will also show that the new protocol is optimal for a restricted class of protocols.

Second, I will show a general lower bound on how good can be protocols that are restricted to k messages between Alice and Bob. This bound implies that, to decrease the bias ϵ, one needs to increase the number of messages (rounds), not just exchange a lot of qubits in few rounds.

http://www.cs.berkeley.edu/~ambainis/papers.html#qc

Degrees of Knowledge of Quantum States and Operations

Charles Bennett, IBM T.J. Watson Research Center

It is possible to "know" or "possess" a quantum state in infinitely many physically inequivalent ways, ranging from complete classical knowledge, through possession of a single specimen of the state, to weaker and less compactly embodiable forms such as the ability to simulate the outcome of a single POVM measurement on the state. A less well understood hierarchy of degrees of knowledge or possession holds for unitary operations and completely positive maps.

http://www.research.ibm.com/people/b/bennetc/home.html

Trading Entanglement for Communication

Gilles Brassard, Université de Montréal

Can entanglement be used to save on classical communication? It is well-known that entanglement on its own is useless for the transmission of information. Yet, there are distributed tasks that cannot be accomplished at all in a classical world when communication is not allowed, but that become possible if the non-communicating parties share prior entanglement. This leads to wondering how expensive it is, in terms of classical communication, to provide an exact simulation of the spooky power of entanglement.

We show that a small constant number of bits of communication is sufficient to simulate the effect of a single bit of entanglement, but exponentially many bits of communication are required to simulate the effect of several bits of entanglement. Therefore, quantum entanglement can always be traded for classical communication, but the cost may be prohibitive.

This is joint work with Richard Cleve and Alain Tapp.

http://arxiv.org/abs/quant-ph/9901035

Fast Parallel Algorithms for the Quantum Fourier Transform

Richard Cleve, University of Calgary

We give new bounds on the circuit complexity of the quantum Fourier transform (QFT). We give an upper bound of $O(\log n + \log\log(1/\epsilon))$ on the circuit depth for computing an approximation of the QFT with respect to the modulus 2^n with error bounded by epsilon. Thus, even for exponentially small error, our circuits have depth $O(\log n)$. The best previous depth bound was $O(n)$, even for approximations with constant error. Moreover, our circuits have size $O(n \log(n/\epsilon))$.

As an application of the above depth bound, we show that Shor's factoring algorithm may be based on quantum circuits with depth only $O(\log n)$ and polynomial size, in combination with classical polynomial-time pre- and post-processing.

Next, we prove an $\Omega(\log n)$ lower bound on the depth complexity of approximations of the QFT with constant error. This implies that the above upper bound is asymptotically tight (for a reasonable range of values of ϵ).

We also give an upper bound of $O(n(\log n)^2 \log\log n)$ on the circuit size of the exact QFT modulo 2^n, for which the best previous bound was $O(n^2)$.

Finally, based on our circuits for the QFT with power-of-2 moduli, we show that the QFT with respect to an arbitrary modulus m can be approximated with accuracy ϵ with circuits of depth $O((\log\log m)(\log\log(1/\epsilon)))$ and size polynomial in $\log m + \log(1/\epsilon)$.

This is joint work with John Watrous.

http://arxiv.org/abs/quant-ph/0006004

Efficient Quantum Algorithms for Shifted Quadratic Character Problems

Wim van Dam, UC Berkeley and CWI

We introduce the Shifted Legendre Symbol Problem and some variants along with efficient quantum algorithms to solve them. The problems and their algorithms are different from previous work on quantum computation in that they do not appear to fit into the framework of the Hidden Subgroup Problem. The classical complexity of the problem is unknown despite the various results on the irregularity of Legendre Sequences.

This is joint work with Sean Hallgren.

http://arxiv.org/abs/quant-ph/0011067

Remote State Preparation

David DiVincenzo, IBM T.J. Watson Research Center

Both remote state preparation (RSP) and quantum teleportation have the same goal, to transmit a quantum state using prior entanglement and classical communication. But in RSP, the sender has full classical knowledge of the state to be transmitted. This knowledge permits RSP to use less resources than teleportation, in which both one ebit and two classical bits are necessary to send a qubit. RSP exhibits a non-trivial tradeoff between the use of entanglement and classical bit resources. On one end of this tradeoff, we show that the asymptotic classical communication cost of RSP can be reduced to one bit per qubit, half of that of teleportation, if about 4 ebits can be consumed. At the other end, if a large number of bits n can be used, the ebit cost goes like $n2^{-n}$. We will also introduce a new capacity, an RSP capacity, for a general quantum channel, and consider RSP for parts of entangled states.

Joint work with C. H. Bennett, J. A. Smolin, B. M. Terhal, and W. K. Wootters.

http://arxiv.org/abs/quant-ph/0006044

Quantum Computation by Adiabatic Evolution

Edward Farhi, MIT

Quantum adiabatic evolution is the basis of a new class of quantum algorithms for combinatorial search problems. This method is guaranteed to work if the running time of the algorithm is long enough. In general it is difficult to determine the required running time. In certain special cases of classically easy problems it can be shown that the required running time grows only polynomially in the number of bits. I will present encouraging numerical results on randomly generated instances of the NP-complete problem Exact Cover. I will also present similarly encouraging results for the time required to find the largest clique in a random graph.

http://arxiv.org/abs/quant-ph/0001106

Quantum Algorithmic Entropy

Peter Gács, Boston University

We extend algorithmic information theory to quantum mechanics, with a universal semicomputable density matrix ("apriori probability") as a starting point, and define complexity (an operator) 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.

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 $2n - 2\log n$) and the qubit complexity defined by Berthiaume, van Dam, and Laplante. With respect to cloning, our complexity behaves similarly to the latter one.

http://arxiv.org/abs/quant-ph/0011046

Quantum Mechanics and Determinism at the Planck Scale

Gerard 't Hooft, University of Utrecht

http://arxiv.org/abs/quant-ph/9612018

Quantum Ordered Searching

Peter Høyer, BRICS, Århus

Any comparison-based classical algorithm for searching an ordered set of N items requires at least $\log_2(N)$ comparisons. The celebrated binary search algorithm meets this bound, and its behavior can be illustrated by a binary tree. Each node of the tree is labelled by a comparison, and each leaf by one of the N items. Initially, the state of the algorithm is represented by the root of the tree, and at each step of the algorithm, a comparison determines whether we go to the left or right child. Eventually, the walk ends at a leaf, which represents the result of the algorithm.

We give a quantum version of this classical binary search algorithm. The algorithm initiates several independent walks at the root, each walk advancing down the tree at its own speed. Then, instead of having each walk advancing only (at most) 1 node at each step, we give a routine that allows them to cooperate. Two walks that are at neighboring nodes (which must be in a parent-child relation) can, by cooperating, jump simultaneously to the same child, hereby advancing 1 and 2 nodes, respectively. Having a routine that allows 1 walk to advance 1 node, while another walk advances 2 nodes, yields, after taking care of details, a $\log_3(N)$ exact quantum algorithm for ordered searching.

Our quantum algorithm can be implemented in parts by the quantum version of the Haar transform, which is the most basic wavelet transform. We find this to be an interesting aspect since most existing quantum algorithms are based primarily on quantum Fourier transforms and amplitude amplification. Little in our algorithm seems to render impossible similar enhanced quantum versions of other classical algorithms based on graphs.

The currently best known upper bound for exact ordered searching is roughly $0.526 \log_2(N)$, due to Farhi, Goldstone, Gutmann, and Sipser. We also give a lower bound of $\frac{1}{\pi}(\ln(N) - 1)$ for any exact quantum algorithm, improving upon Ambainis' bound of $\frac{1}{12}\log_2(N) - \mathrm{O}(1)$. Our lower bound is based on a weighted all-pairs inner product argument.

This talk is based on joint work with Jan Neerbek.

http://arxiv.org/abs/quant-ph/0009032

On the Reversible Extraction of Classical Information from a Quantum Source

Richard Jozsa, University of Bristol

Consider a source E of pure quantum signal states $|a_i\rangle$ having prior probabilities p_i. By analogy with classical information theory we may think of the "quantum information content" of the source operationally as the least number of qubits/signal needed to faithfully encode long sequences of signals emitted by the source. According to Schumacher's quantum source coding theorem this is S qubits/signal where S is the von Neumann entropy of E.

Now we may think of classical information as a separate kind of resource and ask a more probing question: to what extent can the quantum information of E be faithfully encoded into A qubits/signal and B classical bits/signal in such a way that A is minimised while B may be as large as desired? Our main result is that the minimal A in this scenario is still S (assuming that the signal states do not fall into two or more orthogonal subspaces). Thus in this sense, quantum information is fully robust against classicization.

In this talk we will discuss various aspects of this result including some interesting information-disturbance relations that are needed in the proof and some remaining open questions.

Joint work with Howard Barnum, Patrick Hayden, and Andreas Winter.

http://arxiv.org/abs/quant-ph/0011072

Entanglement and Distributed Quantum Computation

Michael Nielsen, University of Queensland

Protocols for performing distributed quantum computation can be modified into protocols for creating entanglement between the parties performing the computation. I explain how the amount of entanglement created by the modified protocol can be used to obtain non-trivial lower bounds on the quantum communication complexity of classical functions, and of quantum operations such as the quantum Fourier transform.

http://www.physics.uq.edu.au/people/nielsen/

A New Inequality for the Quantum Relative Entropy and some Applications

Martin Plenio, Imperial College, London

I derive a non-trivial lower bound for the decrease of the relative entropy under partial trace given that one of the density operators is non-distillable. After proving this inequality using operator monotonicity of the logarithm and the reduction criterion I move on to some interpretations of the inequality and finally I present a number of its applications. These applications include lower bounds on entanglement measures, bounds on the capacity of superdense coding and bounds of multi-partite entanglement measures in terms of bipartite entanglement measures .

http://www.lsr.ph.ic.ac.uk/TQO/People/Plenio/plenio.html

Private Quantum Channels and Quantum Authentication

Alain Tapp, University of Waterloo

In 1949 Claude Shannon published one of the most important papers in cryptography, "Communication theory of secrecy systems." In this paper he shows that in order to achieve perfect secrecy in a private key cryptosystem the entropy of the private key must be as large as the length of the message to be transmitted secretly. Combined with the one-time pad (Vernam cipher) we obtain that in order to encrypt an n-bit message, a private key of n random bits is necessary and sufficient.

What about the transmission of quantum messages ? Is it possible in this case to perform encryption using a finite secret key ? The answer to this question is trivially yes. It requires actually a key of $2n$ secret bits to encrypt n qubits. In this talk, I will discuss this issue and also show that $2n$ bits of key are necessary.

Another important question in quantum cryptography is the authentication of quantum messages. I will sketch some very recent result on this topic. I will present a protocol to code a quantum message using a finite private key in such a way that it is possible for the receiver (possibly the sender in the future) to perform a test such that if it succeeds then the fidelity of the transmitted state is exponentially close to the original state except with exponentially small probability. That is, if a malicious player tries to forge a message or even only to modify the content of a message, he will be caught with probability exponentially close to 1.

Joint work with Andris Ambainis, Claude Crepeau, Daniel Gottesman, Michele Mosca and Ronald de Wolf.

http://arxiv.org/abs/quant-ph/0003101

Data Hiding with Mixtures of Bell States

Barbara Terhal, IBM T.J. Watson Research Center

One of two orthogonal, bipartite quantum states are distributed to Alice and Bob. Can they distinguish which of the two they have received by doing local quantum operations along with classical communications? It has recently been shown that if the quantum states are pure, such states can

be perfectly distinguished. But we now show mixed states about which Alice and Bob can obtain no information by LOCC operations. These states have two descriptions, either as mixtures of collections of Bell states with a definite singlet parity, or as particular examples of Werner states. The proof of this result will be outlined. Possible applications to bit commitment will be explored.

Joint work with David DiVincenzo and Debbie Leung.

http://arxiv.org/abs/quant-ph/0011042

The Non-Abelian Hidden Subgroup Problem

Umesh Vazirani, UC Berkeley

http://www.cs.berkeley.edu/~vazirani/

Classical and Quantum Correlations in Quantum Computation

Vlatko Vedral, Imperial College, London

In my talk I will review the notion of classical and quantum correlations and show how these concepts can be applied to analysing quantum algorithms. In particular, I will discuss Grover's search algorithm from this perspective. I show that, surprisingly, classical correlations play a more prominent role in determining the speed-up in this algorithm than does entanglement. I then analyse Shor's algorithm and the presence (or absence) of classical and quantum correlation between and inside the registers during the entire computation. This approach will provide a basis for analysing the efficiency of quantum computation with mixed states.

http://arxiv.org/abs/quant-ph/0003072

Quantum Algorithms for Solvable Groups

John Watrous, University of Calgary

In this talk I will present polynomial-time quantum algorithms for various problems regarding finite solvable groups, including the problems of computing the order of solvable groups, testing membership in solvable groups, and testing isomorphism of two solvable groups. The algorithms work in the setting of black-box groups, wherein it has been proved that none of the above problems can be solved classically in polynomial time. While the algorithms rely heavily on Shor's algorithm, these problems do not appear to reduce to problems that can be solved in the context of the Abelian Hidden Subgroup problem.

http://arxiv.org/abs/quant-ph/0011023

Quantum Fingerprinting, Simultaneous Message Passing, and Data Structures

Ronald de Wolf, CWI and University of Amsterdam

Classical hashing associates with a string x a shorter string h_x (x's *fingerprint*), such that with high probability, x and y are equal if and only if their fingerprints h_x and h_y are equal. The fingerprints can be exponentially smaller than the original strings if the party making h_x and the party making h_y share randomness, but not if they are uncorrelated. If we allow the fingerprints to consist of qubits, then such fingerprints *can* be made to work even without any correlations between the parties. We give a scheme where the quantum fingerprint $|h_x\rangle$ is easy to construct and exponentially shorter than the original string x, and we give a test which distinguishes any two such (unknown) quantum fingerprints from each other with high probability. We also derive nearly tight bounds on the optimal achievable success probability when k copies of both fingerprints are given.

We give two applications of this quantum fingerprinting scheme. Firstly, in the variant of communication complexity known as "simultaneous message passing", we give an exponential quantum-classical gap for the equality function. Secondly, we show that quantum data structures for representing very sparse sets can be made exponentially smaller than classical data structures representing those sets.

This is joint work with Harry Buhrman, Richard Cleve, and John Watrous

http://www.cwi.nl/~rdewolf