Quantum Algorithms

11.05 - 15.05.1998

organized by

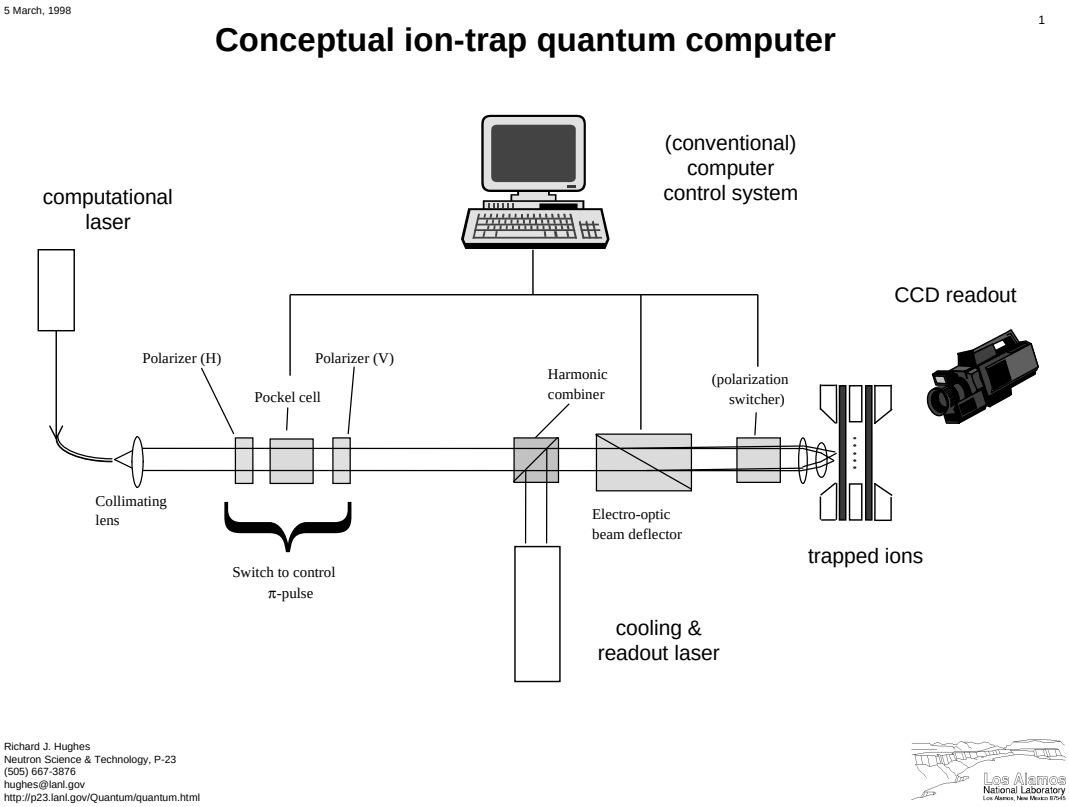
Thomas Beth and Gilles Brassard

Quantum algorithms — a new topic in both informatics and physics has become a central theme of one of the most challenging areas of interdisciplinary research of modern science. This seemingly esoteric area of research which has been stimulated by Feynman in 1980 and Benioff, who was the first to suggest quantum-mechanical evolution for computation in 1982, has become a serious challenge after Shor's publication of the "Algorithms for quantum computation: Discrete logarithms and factoring" in 1994. This breakthrough in theoretical computer science has stimulated a new field of physics, especially on the experimental side, namely the investigation of controlled quantum systems which is motivated by the promise that algorithmic processing of quantum information may provide an exponential gain in speed and space over classical computers. As a consequence of this joint research there has been a surprising progress during the last years towards new algorithms and especially complexity bounds for certain problems. However, up to today there are no exact theorems available on the relation between quantum complexity classes and classical complexity classes.
Quantum algorithms rely on three effects:

- superposition,
- entanglement,
- interference.

If several qubits are combined in a quantum register by the laws of quantum mechanics, the state space of such a processor allows the handling of exponentially many data by superposition of entangled states. Owing to the linearity of quantum mechanics each operation of so-called quantum gates will act on all states simultaneously which have non-zero population in the superposition. This phenomenon is the basis for quantum parallelism which leads to a completely new model of computation: While a classical probabilistic algorithm can be well described through the tree of all possible computations weighed with the respective probabilities, the sum of probabilities of all positive results are added to give the total probability of a successful computation, the use of quantum states based on complex amplitudes instead of probabilistic weights will allow the enhancement

or deletion of amplitudes. This, in a nutshell, is the essential advantage of quantum algorithms. Each desirable computational path can be designed to "absorbe" the probability amplitude on the account of the amplitudes of other paths. This principle is known from physics as constructive and destructive interference.
Physical realizations of quantum computers are envisaged as hybrid systems consisting of a classical computer and a quantum register controlled by classical electromagnetic fields, see e. g. the figure. The control of this system at runtime especially and the design of program loops are performed by classical computers on the basis of measurements carried out on the quantum register. For obvious physical reasons such programming languages are rather restricted even though it has been proved by Deutsch in 1985 that the class of quantum Turing machines encompasses the class of classical Turing machines, following a proposal by Benioff who was the first to think that computation can be done entirely in a quantum mechanical unitary manner.



The Dagstuhl seminar 98191 has brought together scientists from computer science, mathematics, theoretical physics, and experimental physics to discuss the most recent developments of this very new and possibly revolutionizing concept of modern computing.
As opposed to most "classical" computer science conferences, the unusual concept of this conference can be described by the fact that the theoretical aspects

of algorithm design are, at least at the present state of the field, not to be seen device-independent: In other words, in contrast to classical computer science approaches to algorithms and their application, where the actual physical realization on the bit level is not taken into account, it is the feature of this field that in quantum algorithms the physical realization is intrinsically connected with the design of algorithms: Thus, everyone working in the area has to be relatively well acquainted with both, the computer science sides and the physics sides where the modeling of both physics and computer science on the basis of quantum theory and their applications relies on rather strong mathematical foundations such as Hilbert space theory, group theory, combinatorics, information theory, coding theory, and signal processing.

The organizers have judiciously combined the topics to be addressed at this conference to bring together those experts in the fields which can contribute to each of the questions from the mentioned side, ranging from pure theory to actual experiment. Owing to the relative youth of the field and the demanding requirements for a successful work in this area, this Dagstuhl seminar did not only bring together a considerable set of the world experts in the area but also a relatively dominating majority of young scientists which have been attracted by this area. The success of this workshop was not only noted by the computer scientists who have been able to learn from fundamental physical developments of the last years, but also especially physicists have been attracted by the methods of algorithm design and theoretical computer science to be applied to design new physical processes.

So, all in all, we had a successful workshop of mostly three sessions a day lasting late into the night. The interruption of the intensive discussions were only due to the fine food during the day and the expectancy of good spirits at night. This was made possible by the wonderful surroundings of Schloß Dagstuhl accompanied by an exceptionally good weather and the hospitality of the Dagstuhl staff.

Contents

1 The Quantum Communication Complexity of Sampling

U. Vazirani

Sampling is an important primitive in quantum algorithms. We consider the following sampling problem in a communication complexity setting: Alice has a subset $A \subseteq \{1, 2, \ldots, n\}$ of cardinality $\sqrt{n}$ and Bob must pick a uniformly random subset of cardinality $\sqrt{n}$ and disjoint from A. We shall allow Bob a probability ε of error, by requiring that the distribution of the subset he chooses is $1-\varepsilon$ close to the uniform distribution. We show that there is a constant ε such that the minimum number of bits that Alice and Bob must exchange to carry out this task in a classical setting is $\Omega(\sqrt{n})$. By contrast the number of qubits exchanged by our quantum protocol to solve this problem is $O(\log n)$. Therefore this provides the first example of an exponential separation between classical and quantum communication complexity in the bounded urd model.

2 Simulating Quantum Operations with Mixed Environments

B. Terhal

One of the possible applications of a future quantum computer is the study of the behavior of open quantum systems and the nature of decoherence. For these tasks the quantum computer must be prepared to perform quantum operations that in general will involve an "environment", i. e., a quantum system is discarded at some point in the calculation. We study the space-efficiency of the implementation of such quantum operations in terms of the dimension of the environment. In particular, we study a class of quantum operations on a qubit input, the generalized depolarizing channel, for which we show that qutrit environment is sufficient to implement any channel in this class, whereas not all of these channels can be implemented using a qubit environment. The "2 Pauli" channel is one such channel that cannot be implemented with a qubit-environment and an explicit proof using the Gröbner-basis technique is given for this case.

3 Quantum Lower Bounds by Polynomials

R. de Wolf

In the black-box model of computation, we want to compute a Boolean function f of a vector X of N Boolean variables. We can only access the variables in X by making queries to a black-box or oracle. Many significant quantum algorithms, like Deutsch-Jozsa's, Simon's, and Grover's work in this model. We examine the number of black-box queries required by a quantum algorithm to compute f in exact, zero-error and bounded-error model. We show that the acceptance probability of a quantum gate network that contains T black-box queries can be written as a polynomial of X of degree at most $2T$. Using this fact, we derive lower bounds on the number of queries in terms of the degree of polynomials that represent or approximate f and in terms of the block sensitivity of f. In particular we tightly characterize the query complexity of all symmetric f in the three error models. Furthermore we show that computing `PARITY` takes $N/2$ queries in each model, and that `OR` and `AND` take N queries in the exact and zero-error model and $\Theta(\sqrt{N})$ for bounded-error. The latter result is an easy way to the well known $\sqrt{N}$ lower bound on database search.

4 $D \breve{} Q^6$

H. Buhrman

We study the speedup that a quantum bounded error algorithm can have with respect to a deterministic classical one in the black-box model. We show that for arbitrary total functions f, the gain cannot be more than a polynomial. In particular we show that if a quantum algorithm queries T queries, there is a deterministic strategy that makes at most T^6 queries and computes the same function.

5 What is Needed to Build a Quantum Computer?

D. DiVincenzo

The criteria which a physics experiment must satisfy for the construction of a quantum computer are summarized in five points: 1) control over the Hilbert space; 2) initialization (cooling) of the quantum state; 3) minimal decoherence;

4) ability to perform quantum states; 5) ability to perform strong quantum measurements. Experiments in nuclear magnetic resonance cavity quantum electrodynamic, and superconducting circuits are contemplated. Details were presented of my proposal for quantum-dot quantum computer, and of a brand-new proposal for a nuclear-spin silicon quantum computer.

6 Enlargement of CSS Codes and Requirements for Reliable Quantum Computing

A. Steane

First a new class of error correcting codes is obtained, drawing on the stabilizer group formalism which greatly simplifies the task of finding codes. The new codes take a classical code $C = [n, k, d]$, $C^{\perp} \subseteq C$, which can be enlarged to $C' = [n, k' > k + 1, d']$, and by combining produce a quantum code of parameters $[[n, k + k' - n, \min(d, \lceil 3d'/s \rceil)]]$. Next, requirements on space, time, parallelism, and noise are discussed with the aim of realizing large-scale quantum computing in a fault-tolerant manner. The scale-up in computer size must be considered in conjunction with other parameters such as gate noise and memory noise in order to say anything meaningful. The most successful fault-tolerant recovery method is based on prepared ancillary blocks of qubits. An estimate of the noise requirements to permit reliable computing is made by counting error opportunities and paths. It is then found that $[[n, 1, d]]$ block codes permit reliable computing with fewer resources and less stringent noise requirements than 7^L-bit concatenated codes, even for large computations such as factorization of thousand-digit (3000 bits) numbers.

7 Quantum Repeaters for Communication

H. Briegel, W. Dür, I. Cirac, P. Zoller

In quantum communication via noisy channels, the error probability scales exponentially with the length of the channel. We present a scheme of a quantum repeater that overcomes this limitation. The central idea is to connect a string of (imperfect) entangled pairs of particles by using a novel nested purification pro-

tocol, thereby creating a single distant pair of high fidelity. The scheme operates with imperfect means (i. e. gates and measurements) and tolerates general errors on the percent level.

8 Security of Quantum Key Distribution

H.-K. Lo, H. F. Chau

We construct a new quantum key distribution scheme and prove its security against the most general type of attacks and the most type of noises allowed by quantum physics. The novel technique we use is reduction from a quantum scheme to a classical scheme. We first show that, rather surprisingly, the proof of security of our quantum key distribution in the error-free case can be reduced to that of a classical verification scheme. In other words, the quantum verification procedure employed by us has a classical interpretation by proving the security of the classical scheme, the security of our quantum key distribution scheme in the error-free case follows immediately. The security against the most general types of noises (channel noises, storage errors, and computational errors) is then proven by using fault-tolerant quantum computation.Our result implies that, given quantum computers, quantum key distribution over an arbitrarily long distance of a realistic noisy channel can be made unconditionally secure.

9 Pauli Cloning Machines and N-dimensional Extensions

N. J. Cerf

A family of asymmetric cloning machines for quantum bits and N-dimensional quantum states is introduced. These machines produce two approximate copies of a single quantum state that emerge from two distinct channels. In particular, an asymmetric Pauli cloning machine is defined that makes two imperfect copies of a quantum bit, while the overall input-to-output operation for each copy is a Pauli channel. A no-cloning inequality is derived, characterizing the impossibility of copying imposed by quantum mechanics. If p and p' are the probabilities of the depolarizing channels associated with the two outputs, the domain in $(\sqrt{p}, \sqrt{p'})$-

space located inside a particular ellipse representing close-to-perfect cloning is forbidden. This ellipse tends to a circle when copying an N-dimensional state with $N \to \infty$, which has a simple semi-classical interpretation. The symmetric Pauli cloning machines are then used to provide an upper bound on the quantum capacity of the Pauli channel of probabilities p_x, p_y, and p_z. The capacity is proven to be vanishing if $(\sqrt{p_x}, \sqrt{p_y}, \sqrt{p_z})$ lies outside an ellipsoid whose pole coincides with the depolarizing channel that underlies the universal cloning machine. Finally, the tradeoff between the quality of the two copies is shown to result in general from a complementarity akin to Heisenberg uncertainty principle.

10 Quantum Error Correction: Stabilizer/GF(4) Codes

D. Gottesman

Quantum error correction solves the problem of the corruption of quantum data by encoding qubits as part of a quantum error-correcting code. For many codes, it is very helpful to look at the stabilizer, a group of operators which leave all codewords invariant. Stabilizer codes are equivalent to additive codes over GF(4) which are weakly self-dual under a symplectic inner product.

11 Scalable NMR Quantum Computation

U. Vazirani, L. J. Schulman

Nuclear magnetic resonance offers an appealing prospect for implementation of quantum computers, because of the long coherence times associated with nuclear spins, and extensive laboratory experience in manipulating the spins with radio frequency pulses. Existing proposals, however, suffer from a signal-to-noise ratio that decays exponentially in the number of qubits in the quantum computer. This places a severe limit on the size of the computations that can be performed by such a computer; estimates of that limit are well within the range in which a conventional computer taking exponentially more steps would still be practical. We give an NMR implementation in which the signal-to-noise ratio depends only on features of NMR technology, not the size of the computer. This provides a

means for NMR computation techniques to scale to sizes at which the exponential speedup enables quantum computation to solve problems beyond the capabilities of classical computers.

12 Testing Quantum Networks: Pattern Formation and Invariants

G. Mahler

It is now widely accepted that the implementation of large-scale quantum networks will pose a "physically hard" problem as a result of the isolation-, wiring-, and measurement-bottlenecks. One special variant of the measurement problem is testing: Rather than measuring a state or state features, testing aims at verifying the intended dynamical structure of the whole network without being forced to check the complete network state from time step to time step. For this purpose we propose to run the given network as a periodic quantum Turing machine and analyze the motion of the reduced density matrix (Bloch vector) of the Turing head over an extended period of time (a Hilbert-space version of the classical Poincare cut). The resulting pattern depend sensitively on the control parameters and the type and size of the Turing machine. We restrict ourselves to small networks of up to $N = 5$ pseudo spins. Even then a remarkable variety of pattern results, which can be understood to result from a superposition of certain "primitive" Turing machines associated with Floquet-states. In particular, higher order invariants show up with an intuitive geometric meaning. This should pave the way to a better understanding of quantum parallelism, which is believed to underly the non-classical efficiency of quantum computation.

13 Josephson Junction Qubits

G. Schön, A. Shnirman

Low-capacitance Josephson junction arrays in the parameter range where single charges can be controlled are suggested as possible physical realizations of qubits [1]. The coherent tunneling of Cooper pairs mixes different charge states. By controlling the gate voltages we can control the strength of the mixing and perform

the manipulation of the quantum states required for 1-bit and 2-bit operations. We estimate that the phase coherence time of the super conducting junction system, which is limited by the fluctuations of the electrodynamic environment, is sufficiently long for the experimental demonstration of the principles of quantum computation.
In addition, the quantum mechanical state of the system has to be read out. We suggest to measure it by coupling a single-electron transistor to the qubit [2]. As long as no transport voltage is applied, the transistor influences the quantum dynamics of the qubit only weakly. We have analyzed the time evolution of the density matrix of the transistor and qubit when a voltage is turned on. We show that the process is characterized by three different time scales: (i) the dephasing time, which is short when the SET transistor carries a dissipative current; (ii) the measurement time, after which the measured current allows the distinction between the different quantum states; (iii) the mixing time, after which all the information about the initial quantum state is lost due to the transitions induced by the measurement.
We estimate the values of the capacitances and temperatures required to perform a good quantum measurement and conclude that they can be realized by modern nano-techniques.

14 Ion Strings for Quantum Gates

F. Schmidt-Kahler, H. C. Nägerl, D. Leibfried, W. Bechter,
G. Thalhammer, H. Rohde, J. Eschner, R. Blatt

Ion traps have been shown to provide an ideal environment for isolated quantum systems such as a single, trapped and laser cooled atom. Ion storage has long been applied to ultra-high precision spectroscopy and the development of frequency standards. More recently, single trapped ions have been used to demonstrate and test some of the intriguing internal electronic state and the motional state of a trapped ion can be modified using laser light. Decoherence of internal superposition states is nearly negligible even for very long interaction times. A very exciting proposal is the application of linear ion traps and the collective quantum motion of a trapped string of ions for the realization of a quantum gate. Crystal structures of Calcium ions have been prepared in a linear Paul trap and their collective motion excited with resonant RF-fields. The trapped ions are laser-cooled and images of the fluorescing ions are obtained with a CCD camera and show high spatial resolution. Crystals with up to 15 ions arrange

in a linear string and their eigenmodes can subsequently be selectively excited. The collective motion of the string can then be observed via the CCD images. In experiments with the Be and Ca ions it is found that the excitation of the modes of relative ion motion is substantially suppressed relative to that of the center-of-mass modes, suggesting the use of these modes for future experiments towards quantum computation.

15 Optimal Eavesdropping in Quantum Cryptography with Six States

D. Bruß

A generalization of the quantum cryptographic protocol by Bennett and Brassard is discussed, using three conjugate bases, i. e., six states. By calculating the optimal mutual information between sender and eavesdropper it is shown that this scheme is safer against eavesdropping on single qubits than the one based on two conjugate bases. We also address the question for a connection between the maximal classical correlation in a generalized Bell inequality and the intersection of mutual informations between sender/receiver and sender/eavesdropper.

16 Implementing the Quantum Baker's Map on a Quantum Computer

R. Schack, T. Brun, M. Mosca

The quantum Baker's map, a prototypical map invented for theoretical studies of quantum chaos, is defined in terms of discrete Fourier transforms and therefor has an efficient realization in terms of quantum gates. We show that, in a qubit representation, the quantum Baker's map is equivalent to a shift map, which leads to a much simplified approach to the chaotic properties of the map. The quantum Baker's map can be implemented with present-day technology on a 3-qubit NMR quantum computer. In order to investigate the feasibility of quantum chaos experiments using this system, we have solved numerically the master equation for a specific NMR machine, including the Hamiltonian time evolution, the RF pulses, and phase noise due to the environment. We find that the quantum Baker's map displays interesting behaviour even for the small Hilbert space of three qubits.

17 Threshold for Fault-Tolerant Quantum Computation

D. Gottesman

To perform long quantum computations in the presence of noise, both during storage of qubits and during quantum gates, it is necessary to encode the quantum data using a quantum error-correcting code. Computational protocols must also restrict error propagation so that errors do not overwhelm the code's abilities to correct them. Using concatenated codes, one can show that there exists an error threshold below which arbitrarily long fault-tolerant computations are possible. A calculation including only lowest order effects shows this threshold is at least 5×10^{-4}, although higher-order effects may reduce this by approximately an order of magnitude.

18 Quantum Information Primitives and Nonlocality without Entanglement

C. H. Bennett, D. P. DiVincenzo

Quantum information theory has provided a variety of primitive acts and consumable resources, such as the sending of a classical bit or qubit, the sharing of an EPR pair (or ebit), and the performance of an elementary gate operation such as XOR (controlled-NOT). Another resource, of a negative sort, is waste entropy that must be disposed of, for example the two unwanted bits left over at the end of teleportation. The remote-XOR (RXOR) is a positive resource consisting of the ability to perform a single XOR between a qubit of Alice's and a qubit of Bob's. (Imagine Bob and Alice are in love, but married to two other people. Then the ability to have an elementary private interaction would be valuable to them). Some circuits recently discovered by D. Gottesman relate the RXOR to other resources, for example a RXOR can be synthesized from an ebit plus a classical bit transmission in each direction. Generalizing the parardigm of communication complexity we ask "what combinations of resources suffice to perform a specified initial-state to final-state transformation of a multipartite quantum system?" In particular with Fuchs, Mor, Rains, Shor, Smolin, and Wootters (quant-ph/9804053), we have found a set of nine orthogonal product states of two 3-state particles that cannot be reliably distinguished by any sequence of local operations and classical communication. The states can, of course, be prepared locally from classical

directions, but this preparation is necessarily irreversible, generating waste entropy. The proof of immeasurability of the nine states involves first showing that any bilocal processing can be made to occur continuously, i. e., as a sequence of arbitrarily small steps, and then showing that when, during such processing, one of the nine states' posterior probabilities rises significantly above 1/9 but still far from 1, then the nine residual states must be significantly non-orthogonal.

19 Nested Quantum Search

N. J. Cerf

A quantum algorithm is known that solves an unstructured search problem in a number of iterations of order $\sqrt{d}$, where d is the dimension of the search space, whereas any classical algorithm necessarily scales as $O(d)$. It is shown here that an improved quantum search algorithm can be devised that exploits the structure of a search problem by *nesting* this standard search algorithm. The number of iterations required to find the solution of an average instance of a tree search problem scales as $\sqrt{d^x}$, with a constant $x < 1$ depending on the problem considered. For a problem with constraints of size 2 such as the graph coloring problem, this constant x is estimated to be around 0.6 for average instances of maximum difficulty. This corresponds to a square-root speedup over a classical nested search algorithm, of which our presented algorithm is the quantum counterpart.

20 On the Power of One Bit of Quantum Information

E. Knill, R. Laflamme

In standard quantum computation, the initial state is pure and the answer is determined by making a measurement of some of the bits in the computational basis. What can be accomplished if the initial state is a highly mixed state and the answer is determined by measuring the expectation of σ_z on the first bit with bounded sensitivity? This is the situation in high temperature ensemble quantum computation. We explore the above question by introducing the model of quantum computing with one bit (DQC1). An arbitrary number of additional

bits in a completely mixed state are available. DQC1 computations are easily implemented using nuclear magnetic resonance, at least for small numbers of qubits. In DQC1 it is possible to perform interesting physics simulations which have no known efficient classical algorithms. However the model is less powerful then standard quantum computing (DQCp) in the presence of oracles, and is not robust against noise. We define two different types of problems for which the power of solving them is polynomially equivalent to the ability of predicting DQC1 and DQCp outputs. The first type involves estimating the coefficients of operator expansions of unitary operators in a given basis. The second is a class of sums over binary linear codes closely related to weight enumerators.

21 Ensemble Quantum Computing by NMR Spectroscopy: Product Operators, Pseudo-Pure States, and an Implementation of Quantum Error Correction

T. F. Havel, S. S. Somaroo, D. G. Cory

Quantum computers are able to operate on coherent superpositions of states, and to isolate a single gobal property of the set of computed quantities via interference. In principle, this permits them to solve certain problems exponentially faster than a classical computer, but no one has yet succeeded in implementing a true quantum computer on more than two quantum bits. Recently, however, it has been found that an ensemble of independent and identical quantum computers can perform most of the same feats that a single quantum computer could, while at the same time bringing massive classical parallelism to bear on its computations. Such an ensemble quantum computer can be realized, to a limit extend, by nuclear magnetic resonance (NMR) spectroscopy on ordinary liquids at room temperature and pressure. This simple implementation depends on special kinds of mixed states, called pseudo-pure states, whose preparation entails a loss of signal that is exponential in the number of spins. While this would appear to limit such an implementation to ca. 8-10 spins in the foreseeable future, NMR spectroscopy has now permitted the first experimental demonstration of all the basic features of quantum computing. We claim, moreover, that the product operator formalism, on which the theory of NMR spectroscopy is based, provides an efficient framework within which to analyze algorithms and decoherence effects in quantum computing more generally. This is illustrated by presenting our recent experimental implementation of a quantum error correcting code.

22 Algorithms for Encoding and Decoding Quantum Error-Correcting Codes

M. Grassl

Systems using quantum error-correcting codes can be divided into three subsystems:

- The encoder to map K qubit states to N qubit states ($N > K$).
- The decoder, consisting of
  - syndrome calculation
  - mapping syndromes to errors (the very hard part!)
  - error correction
- The inverse encoder.

Methods to construct quantum circuits for encoding and syndrome computation are presented. The networks can be derived in a canonical way from the generating matrix of the special case of cyclic codes, it is shown how to reduce the complexity of the circuit correcting the error given the syndrome.

23 Quantum Counting

A. Tapp, G. Brassard, P. Hoyer

Shor's algorithm for factorization and Grover's algorithm for table lookup are no doubt among the most important results in quantum algorithms. In this presentation, we will show how to use ideas coming from these two algorithms to perform a completely novel task. Suppose a function F is given as a black-box, one can find an x for which $F(x) = 1$ much more efficiently with Grover's algorithm than with any classical technique. Now suppose one wants to evaluate the size of $\{x|F(x) = 1\}$, that is, to count the number of solutions to F. We will present an algorithm that can approximate this size with a selected accuracy. Let P be the number of calls to the function F, N the size of the domain of F, t the size of $\{x|F(x) = 1\}$ and $\tilde{t}$ our estimate of t. For selected values of P, which is a good indicator of the time available for computation, we have the following results.

- If we take $P = c\sqrt{N}$ then $|\tilde{t} - t| < (2\pi/c)\sqrt{t} + \pi^2/c^2$.
- For $P = c\sqrt{N/t}$ we have $(1 + \pi/c)^2 < \tilde{t}/t < 1/(1 + \pi/c)^2$.
- Finally with $P = c\sqrt{\tilde{t}N}$ we have $\tilde{t} = t$ with bounded probability.

Of course, the algorithm does not need any prior information about t. The number of evaluations of F needed to obtain the selected precision is quite lower than the best possible sampling algorithm. This technique is also more efficient than naive classical uses of Grover's algorithm.

24 Polynomial Invariants of Quantum Systems

M. Rötteler

Given a group G (which should be thought of as a finite resp. compact group) consisting of $n \times n$-matrices, a basic object of study is the ring $C[x_1, \ldots, x_n]^G$ of polynomial invariants under this group. An important property of this ring is that it separates the orbits in most cases of interest. We present the concept of generating functions to tackle the hard problem of finding a finite set of generators for this invariant ring. In case of the group of local transforms on one wire, a closed form of the Molien series is given. Also a correspondence between binary trees and fundamental invariants is given. Finally the case of $U(2) \times U(2)$ operating on density matrices is addressed. Again (using a result of R. Brauer, 1937) a correspondence between invariants and binary trees could be established.

25 Generalized Bell Basis

A. Otte

A generalization of the Bell basis for a system consisting of an arbitrary number of particles and each particle having an arbitrary number of levels is discussed. These generalized cat states have some nice properties like evenly spread out entanglement, taken the von Neumann entropy as a measure of entanglement. The introduced unitary operator formalism allows one to gain insight into any quantum network by separating its local, bilocal and characteristic higher order using a cluster expansion of the density operator in unitary operators.

26 Some Problems in Quantum Channel Capacity for Shannon Information

M. Ban, C. A. Fuchs, O. Hirota, M. Osaki, M. Sasaki

Recently, Hausladen et. al, and Holevo proved quantum version of Shannon's second theorem by introducing a typical sub-space in addition to random coding scheme and square root measurement as a quantum decoding. As a result, it was shown that the zero error channel capacity is von Neumann entropy for an ensemble of signal states. So it is important to formulate the maximization problem of the von Neumann entropy with respect to a priori probability of signals. We show in the case of discrete pure states that the eigenvalue of density operator is given by eigenvalue of the Gram matrix involving a priori probability. As a result, one can solve the maximization and minimization problems of the von Neumann entropy. However, still to give analytical solution for this problem is difficult. As examples, the binary pure state case is solved, and numerical analysis for several pure state problems are shown. As the second topics, the importance of channel capacity without coding is introduced. It is shown that only binary pure state can be solved analytically. Based on this capacity, we show that the code words selected by scheme of BCH error correcting code gives super additiveness.

27 On Quantum Algorithms: Theory and Practice

M. Mosca

Most quantum algorithms known to date have networks of the following form:

- There a two registers: a "control" register and a "target" register.
- A Fourier (or similar) transform is performed on the control register to prepare a superposition of computational paths.
- An operation U, controlled by the state of the first register is applied to the second register; when the second register is in an eigenstate of U, this operation effects a phase factor corresponding to the eigenvalue.
- An inverse Fourier transform is performed on the control register to recombine the computational paths and permit them to interfere.

- The control register is observed (the interference pattern usually corresponds to an estimate of a phase).

The hidden subgroup problem (e. g. Deutsch's problem, factoring via order finding, discrete logarithms, Abelian stabilizers etc.) and quantum counting (i. e. amplitude estimation) can be viewed as such. I will describe these algorithms and our (i. e. Jones and M.M.) implementations of an algorithm for Deutsch's problem and quantum counting. I will briefly describe how quantum searching is the interference of the two eigenvectors used in quantum counting, and present our (i. e. Jones, Hansen, M.M.) NMR implementation. Lastly I will describe how many instances (e. g. factoring, discrete logarithms) of quantum algorithms can be implemented with one re-usable control bit instead of an entire register of control bits, which might render the algorithm easier to implement.

28 Non-Distillable Entanglement of Mixed States

M. Horodecki, P. Horodecki, R. Horodecki

A mixed state of a two-component quantum system is called inseparable (entangled), if it is not a mixture of product states. It is called distillable, if it can be brought to the singlet form by means of local quantum operations and classical communication. We provide examples of states which are entangled, but cannot be distilled. We also provide a characterization of distillable states which indicates that distillable entanglement is in fact two-bit entanglement. The results are discussed by use of analogy with thermodynamics.

29 Quantum vs Classical Communication and Computation

R. Cleve, H. Buhrman, A. Wigderson

We present a simple general simulation technique that transforms any black-box quantum algorithm (*a la* Grover's database search algorithm) to a quantum communication protocol for a related problem, in a way that fully exploits the

quantum parallelism. This allows us to obtain new positive and negative results. The positive results are novel quantum communication protocols that are built from nontrivial quantum algorithms via this simulation. These protocols, combined with (old and new) classical lower bounds, are shown to provide the first asymptotic separation results between the quantum and classical (probabilistic) two-party communication complexity models. In particular, we obtain a quadratic separation for the bounded-error model, and an exponential separation for the zero-error model. The negative results transform known quantum communication lower bounds to computational lower bounds in the black-box model. In particular, we show that the quadratic speed-up achieved by Grover for the `OR` function is impossible for the `PARITY` function or the `MAJORITY` function in the bounded-error model, nor is it possible for the `OR` function in the exact case. This dichotomy naturally suggests a study of bounded-depth predicates (i. e. those in the polynomial hierarchy) between `OR` and `MAJORITY`. We present black-box algorithms that achieve near quadratic speed-up for all such predicates.

30 An Ideal Approach to the Invariant Ring of the Tensor Product

J. Müller-Quade

The problem of deciding if two quantum states $|\psi\rangle$ and $|\phi\rangle$ have the same entanglement motivates the study of the group $SU_2 \otimes \ldots \otimes SU_2$. One is interested in classifying the orbits of $SU_2 \otimes \ldots \otimes SU_2$ which resemble the equivalence classes of states with identical entanglement. To classify the orbits of a group G one can use the generators of the ring $C[X]^G$ of invariants of G. This relates to the old question: "Is there a correspondence between $C[X]^G$ and $C[X]^{G \otimes G}$?" We answer (avoid) this question by looking at what we call the orbit relation of G: $\{(x, gx) | x \in$ Vector space $, g \in G\}$. The defining equations of the orbit relation of G can be computed from the defining equations of G. Furthermore the invariant ring can be computed from the defining equations of the orbit relation (Derksen's Algorithm). The orbit relation reflects the (direct) product of groups by the relation product and additionally allows to compute the orbit relation of $G \otimes 1$ from the orbit relation of G. As the tensor product can be written as a product of direct sums: $G_1 \otimes G_2 = (G_1 \otimes 1)(1 \otimes G_2)$ we can conclude that the orbit relation of $G_1 \otimes G_2$ can be computed from the orbit relations of G_1 and G_2.