Quantum Information Processing: Compression, Coding, and Related Computations

John H. Reif
Department of Computer Science
Duke University ‡

Abstract

Quantum Computation (QC) is a type of computation where unitary and measurement operations are executed on linear superpositions of basis states. This paper provides a brief introduction to QC, particularly emphasizing methods for quantum data compression and decompression. We also discuss a number of related topics in quantum information theory, including quantum error correction (that is, techniques for decreasing decoherence errors in QC), bounds for quantum communication and I/O complexity. Furthermore, we enumerate a number of methodologies and technologies for doing QC.

1 Introduction

1.1 Reversible Computations

Reversible Computations are computations where each state transformation is a reversible function, so that any computation can be reversed without loss of information. Landauer [Lan61] showed that irreversible computations must generate heat in the computing process, and that reversible computations have the property that if executed slowly enough, they (in the limit) can consume no energy in an adiabatic computation. Bennett [Ben73] (also see Bennett, Landauer [BL85], Landauer [Lan96], Toffoli [T80]) showed that any computing machine (e.g., an abstract machine such as a Turing Machine) can be transformed to do reversible computations. Bennett's reversibility construction required extra space to store information to insure reversibility; Li, Vitanyi [LV96] give trade-offs between time and space in the resulting reversible machine. An innovative technique due to Bennett [B73,B89] can be used to make reversible functions bijective, as required for quantum computations. Given a bijective function f, suppose we can reversibly compute in time $T(x)$ a bijective function f and it's inverse f^{-1} using auxiliary registers for storage of the input. He proves in time $O(T(n))$ we can also reversibly compute the bijective mapping: $(x, 0, 0) \rightarrow (f(x), 0, 0)$ without use of auxiliary registers for storage of the input.

1.2 An Introduction to Quantum Computation

Computations and methods not making use of quantum mechanics will be termed *classical*. In contrast, *Quantum Computation (QC)* applies quantum mechanics to do computation. A single molecule (or collection of particles and/or atoms) may have a number n of degrees of

‡Surface address: Department of Computer Science, Duke University, Durham, NC 27708-0129. E-mail: reif@cs.duke.edu. Supported by Grants NSF/DARPA CCR-9725021, CCR-96-33567, NSF IRI-9619647, and ARO contract DAAH-04-96-1-0448. This paper appeared at an invited paper, Data Compression Conference (DCC'98), Snowbird, UT, March, 1999. A postscript preprint of this paper is available online at http://www.cs.duke.edu/∼ reif/paper/qsurvey.ps.

freedom known as *qubits*. Associated with each fixed setting X of the n qubits to Boolean values is a *basis state* denoted $|a>$.

Quantum mechanics allows for a linear superposition (also termed an *entangled quantum state*) of these basis states to exist simultaneously. Each basis state $|a>$ of the superposition is assigned a given complex amplitude α; this is denoted $\alpha|a>$. *Unitary transformations* are reversible operations on the superpositions which can be represented by unitary matrices A (e.g., permutation matrices, rotation matrices, and the matrices of Fourier transforms) where $AA^T = I$. The sum of the squares of the magnitudes of the amplitudes of all basis states is 1. This sum remains invariant due to the application of a unitary transformations. The Hilbert space H_n is the set of all possible such linear superpositions.

QC is a method of computation where various operations can be executed on these superpositions:

- *unitary operations*, and
- *observation operations*, which allow for the (strong) measurement of each qubit, providing a mapping from the current superposition to a superposition where the measured qubit is assigned a Boolean value with probability given by the square of the amplitude of the qubit in its original superposition.

Elementary unitary operations that suffice for any quantum computation over qubits (see [BBC+95] and [D95]) include a conditional form of the conditional XOR operation $\oplus$, the Boolean operation NOT, and a constant Boolean operation yielding 0. The time bound for a quantum computations is defined to be the number of such elementary unitary operations.

1.3 Surveys of QC

The following are reviews and surveys have been made of QC: Bennett [BD95a, BD95b], Barenco [Bar96], Benio [Ben96], Brassard [Bra96,Bra98], Haroche, Raimond [HR96], Brassard [Bra97], Preskill [Pre97a], Scarani [Sca98], Steane [Ste98], Vedral, Plenio [VP98]. Also, Williams and Clearwater [WC97] is the first text book in QC. (Also, Taubes [Tau96] and Gershenfeld, Chuang [GC98] give popular press descriptions of QC.)

1.4 Initial Work in QC

Benioff [Ben82] and Feynman [Fey86] were the first to suggest the use of quantum mechanical principles for doing computation. Deutsch and Jozsa [DJ92] give the first example of a quantum algorithm that gave a rapid solution of an example problem, where the problem (for a given a black box function) is not quickly solvable by any deterministic conventional computing machine. But their problem could be quickly solved using randomization. Bernstein and Vazirani [BV93] then provided the first example of a fast quantum algorithm for a problem that could not be quickly solved by conventional computing machines even using randomization. (Also see Costantini, Smeraldi [CS97] for a generalization of Deutsch's example and see Collins et al [CKH98] for a simplified Deutsch-Jozsa algorithm, and see Jozsa [Joz96,Joz97,Joz98] for further work in quantum computation and complexity.)

1.5 Quantum Computing Models

• **Quantum TMs and other Automata.** Deutsch [Deu85b] gave the first formal description of a quantum computer, known as a *quantum TM*. The tape contents of the TM are qubits. *Quantum configurations* of the QTM are superpositions of (classical) TM configurations. A transition of the QTM is a unitary mapping on quantum configurations of the QTM. Thus, a computation of the QTM is a unitary mapping from the initial quantum configuration to the final quantum configuration. Various papers generalize machines and automata to the quantum case. Moore, Crutchfield [MC97] propose quantum finite-state and push-down automata, and regular and context-free grammars, and they generalize several formal language and automata theorems, e.g. pumping lemmas, closure properties, rational and algebraic generating functions, and Greibach normal form. Kondacs and Watrous [KW97] partially characterize the power of quantum finite state automata. Dunlavey [Dun98] gives a space-efficient simulation of a deterministic finite state machine (FSM) on a quantum computer (using Grover's search algorithm discussed below). Watrous [Wat95] investigates quantum cellular automata and Dürr et al [DTS96,DS96] give decision procedures for unitary linear (one dimensional) quantum cellular automata.

• **Quantum Gates.** A set of Boolean gates are *universal* if any Boolean operation on arbitrarily many bits can be expressed as compositions of these gates. Toffoli [Tof80] defined an extended XOR 3-bit gate (which is an XOR gate condition on one of the inputs and is known as the *Toffoli gate*) and showed that this gate, in combination with certain 1-bit gates, is universal. A set of quantum qubit gates are *universal* for Boolean computations for QC if any unitary operation on arbitrarily many qubits can be expressed as compositions of these gates. Deutsch defined the extended quantum XOR 3-qubit gate (known as the Deutsch-Toffoli gate) and proved this gate, in combination with certain one qubit gates, is universal. Barenco [Bar95], Sleator et al [DMS+95], Barenco et al [BBC+95], and DiVincenzo [DiV95] proved the 2-qubit XOR gates with certain 1-qubit gates can implement the Deutsch-Toffoli gate, so are universal for QC (also see Smolin and DiVincenzo [SD95], DiVincenzo et al [DiV96, DS98], Poyatos et al [PCZ96], Mozyrsky et al [MPH96a,MPH97, MPH98], Poyatos et al [PCZ96]), Lloyd [Llo97c] then proved that almost any 2-qubit quantum logic gate (with certain 1-qubit gates) is universal for QC. Monroe et al [MMK95], DiVincenz et al [DVL98] gave experimental demonstrations of quantum gates. [Deu89] defined a quantum computing model known as a *quantum gate array* which allows execution of a (possibly cyclic) sequence of quantum gates, where each input is a qubit, and each gate computes a unitary transformation.

• **Quantum Circuits.** Yao [Yao93] restricted the concept to (acyclic) *quantum circuits* which are a generalization of Boolean logic circuits for quantum gates. It suffices that a quantum circuit use only these universal gates. Yao [Yao93] proved that QTM computations are equivalent to uniform quantum circuit families. Aharonov et al [AKN97] discusses a generalization of quantum circuits to allow mixed states, where measurements can be done in the middle of the computation, and showed that such quantum circuits are equivalent in computational power to standard quantum circuits. This generalized an earlier result of Bernstein and Vazirani [BV93,BU97] that showed that all observation operations can be pushed to the end of the computation, by repeated use of a quantum XOR gate construction.

1.6 Organization of this Paper

In this Section 1 we have introduced QC. In Section 2 we discuss methods for quantum errorless compression. In Section 3 we discuss bounds for quantum communication, in Section 4 we discuss methods for quantum error coding, and in Section 5 we describe methods for quantum cryptography. In Section 6 we discuss further algorithmic applications of QC. In Section 7 we discuss quantum complexity classes. In Section 8 we conclude the paper with a review of the resource bounds of quantum computing as compared with the rources required by classical methods for computation. In Appendix Section 9 we enumerate various technologies for doing QC.

2 Quantum Compression

Summary. Holevo [H97] (also see Fuchs and Caves [FC94]) proved that quantum methods can not increase the bandwidth for transmission of classical information. However, entangled states can be compressed even more. Schumacher [Sch95] considered compression and decompression of a noiseless source of n quantum bits (qubits), each sampled independently from a given mixed state quantum ensemble. For such a quantum source, the compression factor obtainable by classical information theory is limited by the Shannon entropy, which in general (except in the case where the quantum ensemble has only orthogonal states) is less than the quantum compression factor given by the von Neumann entropy. In particular, Schumacher [Sch95] proved a *quantum noiseless coding theorem* that states that the source's von Neumann entropy is the number of qubits per source state which is necessary and sufficient to asymptotically (in the limit of large code-block size) encode the output of the source with arbitrarily high fidelity. The quantum noiseless coding of Schumacher has asymptotically optimal fidelity and size; the resulting compressed number of qubits can be far fewer than in the classical case. As an example of a source with low von Neumann entropy, consider N photons polarized randomly, equiprobably at 0 or 1. A quantum encoder can compress these photons into an entangled state just a few photons. Then a quantum decoder can the recover the original N photons (with arbitrarily high fidelity for large N) from the compressed photons. Bennett et al [BBJ+94] gave a quantum algorithm for the extraction of classical information from a quantum noiseless coding. Cleve, DiVincenzo [CD96] then developed the first polynomial time quantum algorithm for doing the Schumacher quantum noiseless coding and decoding, costing $\Omega(n^3)$ elementary quantum operations. Up to then, this was the fastest previous algorithm for the Schumacher encoding and decoding functions. Recently Reif [Rei98b] gave a time efficient algorithm for asymptotically optimal noiseless quantum compression and decompression, costing only $O(n(\log^4 n) \log\log n)$ elementary quantum operations. The coding of [Rei98b] employed a modified coding that was still asymptotically optimal in fidelity and size.

Shannon Entropy and the Limitations of Classical Methods for Noiseless Compression. Suppose n characters from a finite alphabet Σ are each sampled independently over some probability distribution p. In classical information theory, the Shannon entropy of each character is $H_S(p) = -\sum_{a\in\Sigma}^{1} p(a)\log p(a)$. A string of these n bits may be losslessly compressed to a bit string of mean length $H_S(p)n$. Holevo [H97] (also see Fuchs and Caves [FC94]) proved that quantum methods can not increase the bandwidth for transmission of classical information. However, entangled quantum states can be compressed much more.

The von Neumann entropy and Quantum Noiseless Compression. Following Schumacher [Sch95], we assume there is a finite quantum state ensemble (S, p) which is a *mixed state* consisting of a finite number of qubit states $S = \{|a_0>, \ldots, |a_{|S|-1}>\}$, where each $|a_i> \in S$ has probability p_i. The compressor is assumed to act on blocks of n qubits (so is a block compressor), and is assumed to know this underlying ensemble (S, p). The *density matrix* of (S, p) is an $|S| \times |S|$ matrix $\rho = \sum_{i=0}^{|S|-1} p_i |a_i >< a_i|$. The *von Neumann entropy* (see [Neu32,Sch95]) corresponding to (S, p) is $H_{VN}(\rho) = -Tr(\rho log \rho)$. In general, the Shannon entropy $H_S(p)$ is greater than or equal to the von Neumann entropy. These entropies are equal only when the states in S are mutually orthogonal.

An Example: Consider an example of a source consisting of a sequence of n photons polarized randomly, with equal probability of phase 0 or phase angle θ. In this case, the states are $S = \{|a_0>, |a_1>\}$, where the first state $|a_0> = |0>$, corresponds to phase 0, and the other state $|a_1> = \cos\theta|0> + \sin\theta|1>$ corresponds to phase angle θ, and the probabilities are both $p(0) = p(1) = \frac{1}{2}$. The density matrix is $\rho = \frac{1}{2}|a_0 >< a_0| + \frac{1}{2}|a_1 >< a_1| = \frac{1}{2}(|0 >< 0| + (\cos\theta|0>$

$+\sin\theta|1>)(\cos\theta < 0| + \sin\theta < 1|)\ ) = \frac{1}{2}\ ((1+\cos^2\theta)|0><0| + \cos\theta\sin\theta|0><1| + \cos\theta\sin\theta|1><0| + \sin^2\theta|1><1|\ )$ which has 2×2 matrix form $\frac{1}{2}\begin{bmatrix} 1+\cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}$ over the basis vector $\begin{bmatrix} |0> \\ |1> \end{bmatrix}$. Then we can find an appropriate β which gives a change of basis with new basis states $|0'>=|0>$ and $|1'>=\cos\beta|0>+\sin\beta|1>$, providing a diagonal density matrix $\rho' = \frac{1}{2}\begin{bmatrix} (1+\cos^2\theta)+\cos\theta\sin\theta\tan\beta & 0 \\ 0 & \cos\theta\sin\theta+\sin^2\theta\tan\beta \end{bmatrix}$ over the basis vector $\begin{bmatrix} |0'> \\ |1'> \end{bmatrix}$. Although this source has high Shannon entropy $H_S(p)$, it will have low von Neumann entropy $H_{VN}(\rho)$ in the case of a small magnitude phase angle θ. However, note that the entropies are the same in the special case where $\theta = \pi/2$, so the states $|a_0>=|0>$, $|a_1>=|1>$ are orthogonal and the density matrix is simply the diagonal matrix $\rho = \frac{1}{2}(|0><0| + |1><1|)$ which has a diagonal density matrix $\rho = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$ over the basis vector $\begin{bmatrix} |0> \\ |1> \end{bmatrix}$.

For technical reasons, the unitary compression and decompression mappings need to preserve the number of bits (some of which are ignored). An *n-to-n' quantum compressor* is a unitary transformation that maps n-qubit strings to n-qubit strings; the first n' qubits that are output by the compressor are taken as the compressed version of its input, and the remaining $n-n'$ qubits are discarded. An *n'-to-n decompressor* is a unitary transformation that maps n-qubit strings to n-qubit strings; the first n' qubits input to the decompressor are the compressed version of the uncompressed n qubits, and the remaining $n-n'$ qubits are all 0. The *source* to the compression scheme is assumed to be a sequence of n qubits sampled independently from (S,p). The *observed output* is the result of first compressing the input qubits, then decompressing them, and finally measurement of the result (over a basis containing the n inputs) The *compression rate* is n/n' and the *compression factor* is n'/n. The *fidelity* of the compression scheme is the probability the observed output is equal to the original input (that is the probability that the original qubits are correctly recovered, from the compressed qubits). Our goal is a quantum compression with both a high fidelity and a high compression rate.

An Example (Continued): Consider again the example of a source consisting of a sequence of n photons polarized randomly, with equal probability of phase 0 or phase angle θ. If θ has small magnitude, then a quantum encoder can compress these photons into an entangled state using just a few photons. Furthermore, a quantum decoder can the recover n photons with the original distribution (with arbitrarily high fidelity for large n) from these compressed photons.

Schumacher Quantum Noiseless Compression. Schumacher [Sch95] gave a *quantum noiseless coding theorem* which provided asymptotically optimal noiseless compression of a sequence of qubits independently sampled from a finite quantum state ensemble (S,p). The quantum noiseless coding theorem states that for any $\epsilon, \delta > 0$ and sufficiently large n, (i) there is an n-to-n' quantum compression scheme with fidelity at least $1-\epsilon$ and compression to length $n' \le n(H_{VN}(\rho)+\delta)$, and (ii) any n-to-n'' quantum compression scheme which gives compression to length $n'' \le n(H_{VN}(\rho)-\delta)$, has fidelity $< 1-\epsilon$. That is, in the limit of large code-block size, the source's von Neumann entropy $H_{VN}(\rho)$ is asymptotically the number of qubits per source state which is necessary and sufficient to encode the output of the source with arbitrarily high fidelity. Given a known finite quantum state ensemble (S, p), Schumacher's compression scheme assumes a known basis for which the density matrix ρ is diagonal, with non-increasing values along the diagonal.

The proof of the Schumacher quantum noiseless coding theorem and its refinements by Jozsa and Schumacher [JS94], Barnum, et al [BFJ+96], and H.Szeto [S96] make use of the existence of a *typical subspace* Λ (see [JS94]) within a Hilbert space of n qubits over a source of von Neumann entropy $H_{VN}(\rho)$. The typical subspace Λ has dimension $\leq 2^{nH_{VN}(\rho)}$ and with high probability, a sample of n qubits has an almost unit projection onto Λ. The Schumacher compressor simply transposes (via a permutation mapping) the subspace Λ into the Hilbert space of a smaller block of $nH_{VN}(\rho)$ qubits. These proofs are not completely constructive.

Bennett [B97] gave a constructive presentation of the Schumacher compression. He observes that the Schumacher compression can be done by a unitary mapping to a basis for which the density matrix ρ is diagonal (in certain simple cases the density matrix ρ is already diagonal, e.g., when the input is a set of n identical qubits) followed by certain combinatorial computation which we will call the *Schumacher compression function SCHUMACHER*. The Schumacher compression function SCHUMACHER simply orders the basis states first by the number of ones (from smallest to largest) that are in the binary expansion of the bits and then refines this order by a lexical sort of the the binary expansion of the bits. That is, all strings with i ones are mapped before all strings with $i + 1$ ones, and those strings with the same number of ones are lexically ordered. Note that for any given value X of the qubits, this transformation SCHUMACHER(X) is simply a deterministic mapping from an n bit sequence to a n' bit sequence defined by a combinatorial computation. In particular, given an n bit binary string X, the transformation SCHUMACHER(X) is the number of n bit strings so ordered before X. It is easy to show that SCHUMACHER(X) is a permutation. Since it is a permutation, it is a bijective function which is uniquely reversible, and also is a unitary transformation. To insure that the overall transformation (for all the states) is a quantum computation, it is essential that the transformation SCHUMACHER(X) be done using only reversible, quantum-coherent elementary operations. (Bennett et al [BBJ+94] gave a polynomial time quantum algorithm for the related problem of extraction of only classical information from a quantum noiseless coding.) Cleve, DiVincenzo [CD96] then developed the first polynomial time algorithm for Schumacher noiseless compression of n qubits. In particular, they explicitly computed the bijective function SCHUMACHER(X) and it's reverse using $O(n^3)$ reversible, elementary unitary operations. Reif [Rei98b] gives an efficient deterministic algorithm for a modified Schumacher encoding function using $O(n(\log^4 n) \log\log n)$ Boolean operations. This modified Schumacher encoding requires the evaluation of various combinatorial sums, for which Reif provides efficient recursive, reversible quantum algorithms. Due to our use of Schumacher-type encoding, our compression and fidelity bounds are asymptotically optimal.

The Schumacher quantum noiseless coding theorem assumes the compressor knows the source. Jozsa, et al [JHH+98] recently gave a generalization of the Schumacher compression to the case where the compressor does not know the source, thus providing the first asymptotically optimal universal algorithm for quantum compression. Also, Braustein, et al [BFG+95] have recently given a fast algorithm for an quantum analog of Huffman coding, but do not provide a proof that this coding gives asymptotically optimal noiseless quantum compression (that is, reaches the von Neumann entropy), as provided by Schumacher compression. (Reif [Rei98b] assumes the compressor knows the source, but can be (extended to a asymptotically optimal universal algorithm for quantum compression where the compressor does not know the source, using the techniques of Jozsa, et al [JHH+98].)

3 Bounds on Measurement, Sensing, and Communication

3.1 Lower Bounds on Quantum Communication.

Cleve et al [CDN+98] prove linear lower bounds for the quantum communication complexity of the inner product function, and give a reduction from the quantum information theory problem to the problem of quantum computation of the inner product. Knill, Laflamme [KL98] characterize the communication complexity of one qubit.

3.2 Interaction-Free Quantum Measurement

A method for *(nearly) interaction-free measurement (IFM)* specifies the design of a quantum optical sensing system that is able to determine with arbitrarily high likelihood if an obstructing body has been inserted into the system, without moving or modifying its optical components; moreover, In the case that the obstructing body is present, IFM uses at most an arbitrarily small multiplicative factor of the input intensity to do the sensing. Kwiat et al [KWHZK95] (also see [KWZ96]) have given a method for IFM which does repeated rounds of measurement to affect small phase changes that eventually determine (via the quantum Zeno effect) whether an obstructing body has been inserted. The use of their method for IMF however has some limitations, since if the obstructing body has not been inserted, then the amount of sensing can be quite large.

3.3 Interaction-Free Quantum Sensing

Reif [Rei98a] defines *(nearly) interaction-free sensing (IFS)* similarly to IFM, except an upper bound is imposed on both the intensity to do the sensing (which again is an arbitrarily small multiplicative factor of the input intensity) whether or not the obstructing body is present. A quantum optical method for IFS (but not IFM) may be used to do I/O with bandwidth reduced by an arbitrarily small multiplicative factor of the bandwidth required for classical (e.g., conventional optical or electronic) I/O methods Reif [Rei98a] proves there is no method for IFS with unitary transformations, and so concludes I/O bandwidth can not be significantly reduced by such quantum methods for sensing. (Also see Holevo [H97], Fuchs and Caves [FC94] for proof that quantum methods can not increase the bandwidth for transmission of classical information.)

4 Quantum Error Correcting Codes

4.1 Quantum Coding Theory.

The qubit can be defined in quantum information theory as the amount of information that can be carried in a quantum system with two basis states, e.g. the internal degree of freedom of a polarized photon. The qubit is thus fundamental unit of quantum channel capacity. Nielsen [Nie96], (Svozil [Svo95,Svo96], Holevo [Hol97], Knill, Laflamme [KL96a, KL96b], Ohya [Ohy98], develop a theory of quantum error-correcting codes and quantum information theory), e.g., they give the definition of *quantum mutual entropy* for an entangled state. Buhrman et al [BCW98], Adami, Cerf [AC98b] contrast quantum information theory with classical information theory. Quantum channel capacity has been investigated for noisy channels (DiVincenzo, et al [DSS+95], Holevo [Hol96], Barnum et al [BNS+97], Bennett et al [BDS98,BBP+96]), very noisy channels (Shor, Smolin [SS98]), and quantum erasure channels (Bennett et al [BDS97b]). Fuchs [Fuc97] showed that nonorthogonal quantum states maximize classical information capacity. (Also, Helstrom [H97,H98] defines a quantum theory of information detection, and Fuchs [Fuc96] defines a quantum theory of information distinguishability.)

4.2 Decoherence Errors in QC.

Quantum decoherence is the gradual introduction of errors of amplitude in the quantum superposition of basis states. All known experimental implementations of QC suffer from the gradual decoherence of entangled states. The rate of decoherence per step of QC depends on the specific technology implementing QC. A significant property of Shor's algorithm is that the precision of the amplitudes in the superpositions need be only a polynomial number of bits. Although the addition of decoherence errors in the amplitudes may at first not have a major effect on the QC, the affect of the errors may accumulate over time and completely destroy the computation. Researchers have dealt with decoherence errors by extending classical error correction techniques to quantum analogs. Generally, there is assumed a decoherence error model where the errors introduced are assumed to be uniform random with bounded magnitude, independently for each qubit.

4.3 Quantum Codes.

Shor[Sho95] and Steane[Ste96a] gave the first techniques for reducing quantum decoherence, by the addition of extra qubits which are then projected via observation operations to eliminate errors in the superposition. Calderbank, Shor [CS95] and Steane [Ste96b] then proved that QC can be done with bounded decoherence error, assuming the error correction mechanism is without error itself. Bennett et al [BDS+96], Laflamme [LMP+96] gave the first optimal 5-qubit codes, leading to asymptotically optimal (for large code blocks) quantum error correction codes. Shor [Sho96] and Kitaev [KY96,Kit97] extended these techniques to do fault tolerant quantum computation on quantum networks, in the presence of bounded decoherence error, even if the error correction mechanism also suffers from error decoherence errors. A final innovation (Gottesman et al [GEK+96], Aharonov, Ben-O [AB97], Knill et al [KLZ96, KLZ97]) was concatenated versions of the above quantum codes that allow for arbitrarily long QC in the presence of arbitrary (i.e., not necessarily random) decoherence error below a fixed constant threshold. Current bounds on this threshold are very small, and it seems likely (although it is not yet known) they can be increased to above the decoherance error bounds of experimental techniques for QC.

5 Quantum Cryptography

5.1 Quantum Keys

Bennett et al [BBB+82] gave the first methods for quantum cryptography using qubits as keys, which are secure against all possible types of attacks. Surveys of quantum cryptography are given in Bennett, Brassard, Ekert [BBE92], Brassard [Bra93], Bennett, Brassard [BB84b], Brassard [Bra94]. Ozhigov [Ozh97a] gives a protocol for security of information in quantum databases. Hruby [Hru94] discusses further methods for quantum cryptography. Bennett et al [BBB+92], Hughes et al [HLM+96] describes experiments of quantum cryptography, including optical fibers.

Bennett et al [BBC+91] gave a protocol for quantum oblivious transfer. Mayers [May95] gives quantum oblivious transfer and key distribution protocols and Mayers [May96] extends the protocols to noisy channels. Lo, Chau [LC98] give a quantum key distribution protocol which is unconditionally secure over arbitrarily long distance.

Brassard, Crpeau [BC90] gave quantum bit commitment and quantum coin tossing protocols. Brassard et al [BCJ93] gives quantum bit commitment scheme provably unbreakable by both parties. Yao [Yao95] proved quantum protocols secure against coherent measurements. Brassard et al [BCM+98] shows how to defeat classical bit commitments with a quantum computer. Chau, Lo [CL98] gives further methods for qubit commitment. Crpeau et al [CS95] gives protocols for quantum oblivious mutual identification. (Lo, Chau [LC98] have recently argued that quantum bit commitment and ideal quantum coin tossing are impossible in certain cases that may not be covered in the above results.)

5.2 Distributed Quantum Networks

Future hardware will have to be fast, scalable, and highly parallelizable. A *quantum network* is a network of QCs executing over a spatially distributed network, where quantum entanglement is distributed among distant nodes in the quantum network. Thus, using *distributed entanglement*, a quantum network distributes the parts of an entangled state to various processors, which can to act on the parts independently. Pellizzari [Pel97] proposes quantum networks using optical fibers, and Cirac, Zoller et al [CZ97], and Bose, Vedral [BVK97] show state transfer distribution can be done among distant nodes. For example, [CZ97] use a cavity QED device that traps atoms in multiple cavities and exchanges photons between the cavities to establish the distributed entanglement. Various basic difficulties were overcome:
– *How can one do state transfer distribution?* Bennett et al [BBC93, BBP+96], Brassard [Bra96] developed a technique known as *teleportation* to transmit arbitrary input states with perfect fidelity. It does this by separating the input state into classical and quantum components. The input can then be reconstructed from these components with perfect fidelity.
– *How can one cope with communication errors and attenuation in a quantum network?* Wootters, Zurek [WZ82] proved that a single quantum cannot be cloned. (note: Buzek, Hillery [BH98] recently claimed a universal optimal cloning of qubits and quantum registers in a distributed quantum network, but this seem inconsistent with the no-coning theorem). That no-cloning theorem implies that once a signal becomes attenuated in a an optical fiber communication channel, then it cannot in general be amplified. Hence it would at first appear that communication and quantum network links may be limited to distances of the order of the attenuation length in the fiber. However, the range of quantum communication could be extended using *quantum repeaters* that do quantum error correction, restoring the quantum signal without reading the quantum information. Ekert, Huelga et al [CZ97], Knill, Laflamme, Zurek [KLZ96] extend the techniques of distributed quantum computation to noisy channels, and showed that for quantum memories and quantum communication, a state can be transmitted over arbitrary distances with bounded error, provided a minimum gate accuracy can be achieved which is a constant factor of this error.

6 Other Algorithmic Applications of QC

The early literature in QC provided some examples of QC algorithms for problems constructed for the reasonable purpose of showing that QC can solve some problems more efficiently than conventional sequential computing models. Later, quantum algorithms were developed for variety of useful applications.
• **Quantum Fourier Transforms.** Drutsch, Jazsa [DJ92] gave an $O(n)$ time quantum algorithm for creating a uniform superposition of all possible values of n bits, which is a *quantum Fourier transform* over the finite field of size 2. Simon [Sim94] used this quantum Fourier transform to gave an efficient time quantum algorithm for determining whether a function over a finite domain is invariant under some XOR-mask. This provided the one of the first examples of a quantum algorithm that efficiently solves an interesting problem that is costly for classical computation. Brassard, Hoyer [BH97] recently gave improvements to Simon's algorithm. There have been a number of efficient quantum algorithms for extensions of the quantum Fourier transform: to the approximate quantum Fourier transform (Coppersmith [Cop94]), over various domains (Griffiths, Niu [GN96], Hoyer [Hoy97]), over symmetric groups (Beals [Bea98]), over certain non-abelian groups (Pueschel, Roetteler, Bet [PRB98]), Vedral, Barenco, Ekert [VBE96] give efficient quantum networks for elementary arithmetic operations, using the quantum Fourier transform. Grigoriev [Gri97] used the quantum Fourier transform to test shift-equivalence of polynomials.

• **Quantum Factoring.** The most notable algorithmic result in QC to date is the quantum algorithm of Shor [Sho94, Sho97] (also see a review of the algorithm is given by Ekert and Jozsa [EJ96]) for discrete logarithm and integer factorization in polynomial time (with modest amplitude precision). Shor's algorithm uses efficient reduction from integer factoring to the problem of approximately computing the period (length of a orbit) within an integer ring due to Miller [Mil97]. Shor approximates the period by repeated the use of a quantum Fourier transform over an integer ring and greatest common divisor computations. There has been considerable further work on Shor's quantum factoring algorithm: Zalka [Zal98] improved the time complexity, Beckman et al [BCD+96] describe it's execution on quantum networks with small size and depth, Obenland, Despain [OD96a], Plenio, Knight [PK96] consider the feasibility of executing Shor's quantum factoring algorithm on various quantum computer architectures (the latter provide somewhat pessimistic lower bounds for the factorization time of large numbers on a quantum computer in the presence of decoherance errors.) Kitaev [Kit95] gave an independent derivation of Shor's factoring result using a reduction to find an abelian stabilizer.

• **Quantum Search.** Another significant efficient QC algorithmic result is the algorithm of Grover [Gro96], which searches within a data base of size N in time $\sqrt{N}$ (An interesting property of the Grover's algorithm for search is its similarity to the quantum Zeno affect technique for quantum measurement Kwiat et al [KWHZK95,KWZ96]. In particular, the algorithm also uses $O(\sqrt{N})$ stages of unitary operations, each quite similar to a stage of the quantum Zeno sensing method.) Grover refined his result to require only a single query [Gro97], and to use almost any unitary transformation [Gro98], Zalka [Zal97] showed Grover's algorithm can not be further asymptotically sped up and so is optimal for data base search, and Pati [PAT98] gave further improvements to the bounds. Biron et al [BBB+98], extended Grover's algorithm to arbitrary initial amplitude distribution. Cockshott [Coc97] gave fast quantum algorithms for executing more general operations on relational databases, and Benjamin, Johnson [BJ98] discuss the use of Grover's algorithm and related quantum algorithms for other data processing problems. Farhi et al [FGG+98] showed that Grover's algorithm could not be extend to quickly determine parity of N bits; in particular they showed that any quantum algorithm for parity takes at least $N/2$ steps. Brassard et al [BHT96,BHT98] combine the algorithmic techniques of Grover and Shor to give a fast quantum algorithm for approximately counting (i.e., finding the number of matches in a database).

While Grover's algorithm is clearly an improvement over linear sequential search in a data base, it appears less impressive in the case of an explicitly defined data base which needs to be stored in volume N. Parallel computation can do search in a data base of size N in time at most polylogarithmic with N (that is, in time $O(\log^{O(1)} N)$) by relatively straightforward use of parallel search Moreover, Grover's algorithm may not have a clear advantage even in the case of an implicitly defined data base, which does not need to be stored, but instead can be constructed on the fly (e.g., that arising from NP search methods). In this case, Grover's search algorithm can be used to speed up combinatorial search within a domain of size N to a time bound of $O(\sqrt{N})$, (Hogg [Hog96], Hogg, Yanik [HY98] investigate similar quantum search techniques for local and other combinatorial search problems), and in this case Grover's algorithm appears to require only volume logarithmic in the search space size N. In contrast, parallel computation takes volume linear in the combinatorial search space, but takes just time polylogorithmic in the search space.

• **Quantum Simulations in Physics.** The first application proposed for QC (Feynman [Fey82]) was for simulating quantum physics. In principle, quantum computers provide universal quantum simulation of any quantum mechanical physical system (Lloyd [Llo96], Zalka[Zal96a], Boghosian [Bog98])). Proposed QC simulations of quantum mechanical systems include: many-body systems (Wiesner[Wie96]), many-body Fermi systems (Abrams, Lloyd [AL97]), multiparticle (ballistic) evolution (Benioff [Ben96]), quantum lattice-gas models (Boghosian, Taylor [BT96]), Meyer [Mey96a, Mey96b]), Ising spin glasses (Lidar, Biham [LB97]), the thermal rate constant (Lidar, Wang [LW98], quantum chaos (Schack [Sch97]).

• **Quantum Learning.** QC may have some interesting applications the learning theory and related problems. Bshouty, Jackson [BJ95] describe learning Boolean formulas in disjunctive normal form (DNF) over the uniform distribution of inputs, using a quantum example oracle, and Ventura, Martinez [VM98c] describe a QC learning algorithm for learning DNF using a classical example oracle. Also, Yu, Vlasov [YV96] describe image recognition using QC, Tucci [Tuc98] investigates quantum bayesian networks, and Ventura, Martinez [VM98b] describe a quantum associative memory,

• **Quantum Robotics.** Benioff [Ben97] considers a distributed QC system with mobile *quantum robots* that can carry out carrying out measurements and physical experiments on the environment, and as an example gives an algorithm for the problem of measuring the distance between a quantum robot and a particle on a 1D space lattice. Hogg [Hog96] proposes the use of distributed QC to allow small-scale sensors and actuators to be controlled in a distributed manner. Further discussion of the applications of QC are given by Landauer [Lan95,Lan97].

• **Winding Up Quantum Clocks.** The precision of atomic clocks are limited by the spontaneous decay lifetimes of excited atomic states. An interesting application of QC proposed by Huelga [HMP+97]) and Bollinger et al [Bol96] is to extend these lifetimes by using quantum error correcting codes to inhibit the spontaneous decay. A similar idea can be used for improving the precision of frequency standards and interferometers.

7 Complexity Bounds for QC

7.1 Quantum Complexity Classes and Structural Complexity

Berthiaume, Brassard [BB92a] survey open QC structural complexity problems (also see Berthiaume [Ber95]). QC can clearly execute deterministic and randomized computations with no slow down. P (NP, QP, respectively) are the class of problems solved by deterministic (nondeterministic, quantum, respectively) polynomial time computations. Thus QP is the quantum analog of the time efficient class P. It is not known if QP contains NP, that is if QC can solve NP search problems in polynomial time. It is also not known whether QP is a superset of P, nor if there are any problems QC can solve in polynomial time that are not in P (but this is true given quantum oracles; see Berthiaume, Brassard [BB92b, BB94], Machta [MAC98], van Dam [Dam98a, Dam98b] for complexity bounds for computing with quantum oracles).

7.2 Bounded Precision QC

Practical implementations of QC most likely will need to be done within some bounded amplitude precision, and with this motivation Bernstein, Vazirani [BV93,BV97] investigated the power of QTMs that have bounded amplitude precision. Let *BQP* be the class of polynomial time QTM computations that are computed within amplitude precision bounded by an inverse polynomial in the input size. Most of the algorithms we will mention (such as Shor's) are in the class BQP. [BV93, BV97] showed that BQP computations can be done using unitary operations with a fixed irrational rotation. Adleman et al [ADH97] improved this to show that BQP can be computed using only unitary operations with rational rotations, and that BQP is in the class PSPACE of polynomial space computations of (classical) TMs.

7.3 Quantum Parallel Complexity Classes

Let NC (QNC, respectively) be the class of (quantum, respectively) circuits with polynomial size and polylogorithmic depth. Thus QNC is the quantum analog of the processor efficient parallel class NC. Moore, Nilsson [MN98a] define QNC and show various problems are in QNC, for example they show that the quantum Fourier transform can be parallelized to linear depth and polynomial size.

8 Conclusion: Resource Bounds

In this paper, we have discussed many applications of quantum computation which provide advantages over classical methods of computation. Certain of the applications of QC (e.g., quantum cryptography) require only a small or constant number of qubits, where as other applications (e.g., factoring and data base search) require a large number of qubits and moreover require an observation operation at least as the final step of the QC. For these advantages to be practical, we need to determine that there are no unfeasible large resources required by QC. Hence we complete the paper with a review of the resource bounds of quantum computing as compared with the resources required by classical methods for computation. In particular, we will conclude that for the advantages of QC (with a large number of qubits) to be practical for applications requiring a large number of qubits, there needs to be determined (theoretical and practically) bounds on the volume required of observation operations. This seems to us a major missing element in the field of QC.

The energy consumption, processing rate, and volume, are all important resources to consider in computing devices. Conventional (classical) electronic supercomputers of the size of a work station operate in the range of 10^{-9} Joules per operation, at up to about 50 giga-ops per second, with memory of about 10 to 100 giga-bytes, and in a volume of about 10 cm^2. The volume scales as the number of bits of storage.

• **Energy Bounds for QC.** The conventional linear model of QC allows only unitary state transformations and so by definition is reversible (with the possible exception of the observation operation which does quantum state reduction). Benioff [Ben82] noted that as a consequence of the reversibility of the unitary state transformations of QC, these transformations dissipate no energy. The energy bounds for the observation operation are not well understood, and depend on the technology used.

• **Processing Rate of QC.** The rate of execution unitary operations in QC depend largely on the implementation technology (see Appendix Section 9); certain techniques can execute unitary operations in microseconds (e.g., Bulk MNR) and some might execute at microsecond or even picosecond rates (e.g., photonic techniques for MNR) The time duration to do observation can also be very short, but may be highly dependant on the size of the measuring apparatus and on the required precision (see the below discussion on the observation operation and its volume).

• **Volume Bounds for QC.** We now consider (perhaps more closely than usual in the quantum literature) the volume bounds of QC. Potentially, the modest volume bounds of QC may be the one significant advantage over classical methods for computation. Due to the *quantum parallelism* (i.e., the superposition of the basis states allow each basis state to exist in parallel), the volume would at *appear* to be no more that the number of qubits. This may be true, but there are a number of substantial issues that need to be carefully considered. Recall the observation operation both provides a measurement of a qubit with a resulting state reduction. However, the QC literature has not yet carefully considered the volume bounds for the observation operation and as we shall see, it is not yet at all clear what the volume is required. In spite of major works on the mathematical and physical foundations of

quantum observation, the precise nature of quantum state reduction via a strong quantum measurement remains somewhat of a mystery. Two distinct approaches to the mathematical and physical foundations of observation have been developed:
(a) The *Copenhagen Formulation,* where the observation is simply *an assumed basic operation* and is considered to be done by a macroscopic measuring device, and
(b) The *Von Neumann Formulation* [Neu32,Neu96], which views the measuring apparatus as well as the quantum system measured as both part of a quantum system. Hence the evolution of the system (and resulting experimental predictions) can be distinct from that predicted by the Copenhagen formulation of observation (which does not take this into account since the measuring apparatus is assume in their formulation to be very large).

See Cerf and Adami [CA98] for a comparison the Copenhagen and Von Neumann formulations and see Hay and Peres [HP97] for an example of this difference is given in Hay and Peres [HP97]. In summary, the Copenhagen and the von Neumann formulations for observation differ in the assumed context (macroscopic or microscopic measurement apparatus). The Copenhagen formulation for observation is can only be used in the context of quantum physics experiments which use macroscopic measurement apparatus. The von Neumann formulation of observation is not relevant to the vast majority of physics experiments since their experiments generally use large measuring apparatus and small number of degrees of freedom (qubits). But the von Neumann formulation appears very relevant to QC, and it is possible that the volume for quantum observation grows very quickly with the number of qubits in this formulation. In particular, no one has proved a upper bound on the volume for quantum observation (as a function of the number of qubits) assuming the von Neumann formulation. See Reif [Rei98c] for a further discussion of the problem of determining volume bounds for the observation operation in QC.

– **Avoiding Observation Operations.** An alternative approach is to completely avoid observation operations on the basis that the observation operation is not actually essential to many quantum computations. (This seems somewhat surprising, given the extensive use of the observation operation in the QC literature for both algorithms and quantum error correction.) Bernstein and Vazirani [BV93,BU97] (by showing that any given observation operation can be delayed to future steps by use of the using XOR operation) proved that all observation operations can be delayed to the final step of a quantum computation. For a small $\epsilon > 0$, let some particular qubit (of the linear superposition of basis states) be *ϵ-near classic* if had the qubit been observed, the measured value would be a fixed value (either be 0 or 1) with ϵ probability. Suppose the output of a QC consists of the observation of a subset S of the qubits; the resulting reduced superposition will be termed the *output superposition.* Bernstein and Vazirani [BV93,BU97] and Brassard et al [BH97,BHT98] observe that any QC can be repeated to insure the output qubits are ϵ-near classic in the final output superposition after the repetitions. Note that if a QC with bounded amplitude precision is reduced by an observation, the output qubits yield the correct value with high likelihood. Hence we may consider simply not doing the observation reduction to a basis state in the final step; in place of this (reduced) output superposition we simply output the non-reduced quantum state superposition of the QC that exists just prior to the final observation step. This alternative approach can entirely eliminate the observation operation from many quantum computations, and so provides small volume, but has the drawback of providing a non-classic output consisting of a non-reduced quantum state superposition. The potential difficulty with this approach is as follows: if this (non-reduced quantum state superposition) output is then processed by a classical computing machine, it may propagate unwanted quantum effects to the classical computing machine.

9 Appendix: Possible Technologies for Doing QC

As noted previously, any QC can be realized by a *universal* set of gates consisting of the 2-qubit XOR operation along with some 1-qubit operations. There are two basic approaches known to do QC:

(A) Micromolecular QC. Here QC on n qubits is executed using n individual atoms, ions or photons, and each qubit is generally encoded using the quantized states of each individual atom, ion or photon. The readout (observation operation) is by measurement of the (eigen) state of each individual atom, ion or photon. In the following we enumerate a number of proposed micromolecular QC methods:

• **Quantum Dots.** Burkard [BLD98], Loss et al [LD97], Meekhof et al [MMK+96] describe the use of coupled quantum dots to do QC. ([Ave97] proposes quantum computation using Cooper pairs.)

• **Ion Trap QC.** Cirac, Zoller [CZ95], James [Jam97] proposed using a linear array of cold trapped ions (the ions are trapped by electromagnetic fields) whose energy states are used to store the qubits (also, vibrational modes between consecutive ions also can be used to store states of qubits). The coupling of the qubits is by electrostatic repulsion between the ions. Unitary transitions on superpositions can be executed via an associated array of lasers, each of which pulses a distinct ion; these induce electric dipole moments that determine the transitions. A group at the National Institute of Standards at Boulder, CO (Meekhof et al [Mee96], Wineland et al [WMM+96, WMI+98], King et al [KWM98], Turchette et al [TWK+98]) and a group at Los Alamos (Hughes[Hug97], Hughes et al [HJG+98], James [JGH+98]) have experimentally demonstrated trapped ion QC. These and other researchers have addressed various key issues associated with quantum computation with trapped ions:

− Deterministic entanglement of two trapped ions (Myatt et al [MLI98]),

− decoherence bounds (Hughes et al [HJK+96] and Plenio, Knight [PK97]),

− measurement and state preparation, i.e., initialization of the collective motion of the trapped ions (Schneider et al [SWM+98] and King et al [KWM98]),

− coherent quantum-state manipulation of trapped atomic ions (Wineland et al [WMI+98]),

− heating of the quantum ground state of trapped ions (James [Jam98]) and quantum computation with "hot" trapped ions (Schneider et al [SJM98]).

• **Cavity QED.** A group at Cal Tech (Turchette [THL+95]) have experimentally demonstrated the use of trapped photons in a cavity QED system to execute 2-qubit XOR gates and thus in principle can do universal QC. The qubits are encoded by the circular polarization of photons. interacting. The XOR unitary transitions on superpositions can be executed by resonance between interacting photons in the cavity; The coupling of qubits is via resonance between interacting photons using a Cesium atom also in the cavity, and the coupling is tuned by the spacing of mirrors in the cavity.

• **Photonics.** Various groups Chuang et al [CY95, CVZ+98] , Torma, Stenholm [TS96] have experimentally demonstrated QC using optical systems where qubits are encoded by photon phases and universal quantum gates are implemented by optical components consisting of beamsplitters and phase shifters as well as (in the case of [TS96]) nonlinear media (also see the linear optics QC proposed by Adami, Cerf [AC98a]).

• **Heteropolymer.** This is a polymer consisting of a linear array of atoms, each of which can be either in a ground or excited energy state. Teich et al [TOM88] first proposed classical (without quantium superpositions) molecular computations using heteropolymer. Later Lloyd [Llo93] extended the use of heteropolymers to QC, using the energy states to store the state of the qubits. The coupling of qubits may be via electric dipole moments which causes energy shifts on adjacent atoms. Unitary transitions on superpositions can be executed via pulses of a laser at particular frequencies; these induce electric dipole moments that determine the transitions.

• **Nuclear Spin.** DiVincenzo [DiV97b] Wei et al [WXM98a, WXM98b] proposed the use of nuclear spin to do QC; see the remarks following the discussion of Bulk QC.

• **Quantum Propagation Delays.** Castagnoli [Cas97] proposed to do QC using retarded and advanced propagation of particles through various media.

Of these, Ion Trap QC, Cavity QED QC, and Photonics have been experimentally demonstrated up to a very small number of qubits (about 3 bits). The apparent intention of such micromolecular methods for QC is to have an apparatus for storing qubits and executing unitary operations (but not necessarily executing observation operations) which requires only volume linear in the number of qubits. One difficulty (addressed by Kak [Kak98], Murao et al [MPP+97]) is *purification of the initial state*: if the state of a QC is initially in an entangled state, and each of the quantum gate transformations introduces phase uncertainty during the QC, then effect of these perturbations may accumulate to make the output to the QC incorrect. A more basic difficulty for these micromolecular methods is that they all use experimental technology that is not well established as might be; in particular their approaches each involve containment of atomic size objects (such as individual atoms, ions or photons) and manipulations of their states. A further difficulty of the micromolecular methods for QC is that apparatus for the observation operation, for even if observation is approximated, seems to require volume growing exponential with the number of qubits, as described earlier in this paper.

(B) Bulk (or NMR) QC. Nuclear magnetic resonance (NMR) spectroscopy is an imaging technology using the spin of the nuclei of a large collection of atoms. Bulk QC is executed on a macroscopic volume containing, in solution a large number of identical molecules, each of which encodes all the qubits. The molecule can be chosen so that it has n distinct quantized spins modes (e.g., each of the n nuclei may have a distinct quantized spins). Each of the n qubits is encoded by one of these spin modes of the molecule. The coupling of qubits is via spin-spin coupling between pairs of distinct nuclei. Unitary operations such as XOR can be executed by radio frequency (RF) pulses at resonance frequencies determined in part by this spin-spin coupling between pairs of nuclei (and also by the chemical structure of the molecule). Bulk QC was independently proposed by Cory, Fahmy, Havel [CFH96] and Gershenfeld, Chuang [GC97, GC98] Also see Berman et al [BDL+98] and the proposal of Wei et al [WXM98b] for doing MNR QC on doped crystals rather than in solutions, and see Kane [Kan98] for another solid state NMR architecture using silicon.

• **Bulk QC was experimentally tested** for the following: the quantum baker's map on 3 qubits (Brun, Schack [BS98]), quantum search (Jones et al [JMH98] and Jones [Jon98]), approximate quantum counting (Jones, Mosca [JM98a]) Deutsch's problem (Jones, Mosca [JM98b]), Deutsch-Jozsa algorithm on 3 qubits (Linden, Barjat, Freeman[LBR98]).

• **Advantages of Bulk QC:** (i) it can use well established NMR technology and in particular macroscopic devices, The main advantages are (ii) the long time duration until decoherence (due to a low coupling with the environment) and (iii) it currently scales to more qubits than other proposed technologies for QC.

• **Disadvantages of Bulk QC:** A possible disadvantage of Bulk QC is that it appears to allow only a *weak* measurement of the ensemble average which does not provide a quantum state reduction; that is the weak measurement does not alter (at least by much) the superposition of states. Another disadvantage of Bulk QC is that it may require, for a variety of reasons, macroscopic volumes, and in particular volumes which grow exponential with the number of qubits. Macroscopic volumes may be required for measurement via conventional means. Also, Bulk QC requires the initialization to close to a pure state. If Bulk QC is done at room temperature, the initialization methods of Cory, Fahmy, Havel [CFH96] (using logical labeling) and Gershenfeld, Chuang [GC97, GC98] (using spatial averaging) yield a pseudo-pure state, where the number of molecules actually in the pure state drops exponentially as $1/c^n$ with the number n of qubits, for some constant c (as noted by Warren [War95]). If we approximate the resulting measurement error by a normal distribution, the measurement error is (with high likelihood) at least a multiplicative factor of $1 - c'/\sqrt{N}$, for some constant c'. To overcome this measurement error, we need $1/c^n > c'/\sqrt{N}$, and so we require that the volume be at least $N > (c^n/c')^2$. Hence, for the output of the Bulk QC to be (weakly) measured, the volume (the number N molecules) of Bulk QC needs to grow exponentially with the number n of qubits. Recently, there have been various other proposed methods for initialization to a pure state:

- Barnes[Bar98] proposes the use of very low temperatures,
- Gershenfeld, Chuang [GC98] suggest the use of gradient fields.
- Knill et al [KCL97] suggest a randomization technique they call temporal averaging.
- Recent work of Schulman, Vazirani [SV98] provides polynomial volume for initialization, with the assumption of an exponential decrease in spin-spin correlations with the distance between the nuclei located within a molecule (in particular, they assume that the statistical correlation between and two bits on a molecule falls of exponentially with the distance between these bits). Although their methods may provide a solution in practice, known inter-atomic interactions such as the spin-spin correlations are generally considered to be governed by potential force laws which decrease by inverse polynomial powers rather than by an exponential decrease.

It has not yet been experimentally established which of these pure state initialization methods scale to a large number of qubits without large volume.

(Note: Some physicists feel that it has not been clearly established whether: (a) MNR is actually a quantum phenomenon with quantum superposition of basis states, or (b) if MNR just mimics a quantum phenomenon and is actually just classical parallelism, where the quantum superposition of basis states is encoded using multiple molecules where each molecule is in a distinct basis state. If the latter is true with each molecule is in a distinct basis state, then (see Williams and Clearwater [WC96]) the volume may grow grow exponentially with the number n of qubits, since each basis state may need to be stored by at least one molecule, and the number of basis states can be 2^n. Also, even if each molecule is in some partially mixed quantum state (see Zyczkowski et al [ZHS98]), the volume may still need to grow very large.)

Acknowledgements. We would like to thank G. Brassard for his clear explanation of numerous results in the field of QC. Also, I would like to thank P. Shor and U. Vazirani for references and illuminating discussions on quantum computation, and in particular on the issue of volume bounds for quantum observation.

Quantum Computing References

Note: QCQC 98 is an acronym for: Proc. of 1st NASA Workshop on Quantum Computation and Quantum Communication (QCQC 98), Springer-Verlag, (Feb. 1998).

[ADH97] L. M. Adleman and J. Demarrais and M.-D. A. Huang. Quantum computability. SIAM Journal on Computing, 26(5):1524-1540, (October 1997).

[AL97] Abrams, D. S., Lloyd, S. Simulation of many-body fermi systems on a universal quantum computer. (Online preprint quant-ph/9703054.) (1997).

[AB96] D. Aharonov, M. Ben-Or, Polynomial Simulations of Decohered Quantum Computers, (Online preprint quant-ph/9611029), 37th Annual Symposium on Foundations of Computer Science, pages 46-55, Burlington, Vermont, (October 1996). IEEE.

[AB97] D. Aharonov, M. Ben-Or, Fault Tolerant Quantum Computation with Constant Error, (Online preprint quant-ph/9611025), In Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pages 176-188, El Paso, Texas, (May 1997).

[AKN98] D. Aharonov, A. Kitaev, N. Nisan, (Online preprint quantum Circuits with Mixed States, Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computation (STOC), pages 20-30, 1997 (Online preprint quant-ph/9806029), (1998).

[AL97] D. S. Abrams, S. Lloyd, Simulation of Many-Body Fermi Systems on a Universal Quantum Computer, (Online preprint quant-ph/9703054), Phys.Rev.Lett. 79 (1997) 2586-2589.

[AL98] D. S. Abrams, S. Lloyd, Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems, (Online preprint quant-ph/9801041), submitted to Phys. Rev. Lett, (1998).

[Ave97] D.V. Averin, Adiabatic quantum computation with Cooper pairs, (Online preprint quant-ph/9706026), (1997).

[AC98a] C. Adami, N.J. Cerf, Quantum computation with linear optics, (Online preprint quant-ph/9806048), QCQC 98, (Feb. 1998).

[AC98b] C. Adami, N.J. Cerf, What information theory can tell us about quantum reality, (Online preprint quant-ph/9806047), QCQC 98, (Feb. 1998).

[APZ96] J.R. Anglin, J.P. Paz, W.H. Zurek, Deconstructing Decoherence, (Online preprint quant-ph/9611045), (1996).

[Bar95] A. Barenco, A Universal Two–Bit Gate for Quantum Computation, (Online preprint quant-ph/9505016), (1995).

[Bar96] A. Barenco, Quantum Physics and Computers, (Online preprint quant-ph/9612014), Contemp.Phys. 37 (1996) 375.

[BBC+95] Barenco, A., C. H. Bennett, R. Cleve, D. P. D. P. DiVincenzo, Phys. Rev. A 51, 1015 (1995).

[BBC+95] Barenco, A., C. H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. (Online preprint quant-ph/9503016), Phys. Rev. A. 52, 3457 (1995).

[BBD+97] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, Stabilisation of Quantum Computations by Symmetrisation, (Online preprint quant-ph/9604028), SIAM Journal on Computing, 26(5):1541-1557, (October 1997).

[BBS+96] Barenco, A., T. Brun,.A., R. Schack, and T. Spiller, Effects of noise on quantum error correction algorithms. (Online preprint quant-ph/9612047) , (1996).

[BDE95] Barenco, A., D. Deutsch and A. Ekert, Phys. Rev. Lett. 74, 4083 (1995).

[BNS+97] Barnum, H., M. A. Nielsen, and B. Schumacher, Information transmission through a noisy quan tum channel. (Online preprint quant-ph/9702049), (1997).

[Bar98] S. E. Barnes, Efficient quantum computing on low temperature spin ensembles, (Online preprint quant-ph/9804065), (1998).

[Bea98] R. Beals. Quantum computation of Fourier transforms over symmetric groups. In Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pages 48-53, El Paso, Texas, 4-6 May (1997).

[BHG98] H. Bechmann-Pasquinucci, B. Huttner, N. Gisin, Nonlinear quantum state transformation of spin-1/2, (Online preprint quant-ph/9708040), Phys.Lett. A242 (1998) 198-204.

[BCD+96] D. Beckman, A. N. Chari, S. Devabhaktuni, J. Preskill, Efficient Networks for Quantum Factoring, (Online preprint quant-ph/9602016), (1996).

[Ben82] Benioff, P. Quantum mechanical models of Turing machines that dissipate no energy. Phys. Rev. Lett. 48, 1581, (1982).

[Ben96] P. Benioff, Quantum Ballistic Evolution in Quantum Mechanics: Application to Quantum Computers, (Online preprint quant-ph/9605022), to be published in Phys. Rev. A (1996).

[Ben97] P. Benioff, Tight Binding Hamiltonians and Quantum Turing Machines, (Online preprint quant-ph/9610026), Phys.Rev.Lett. 78 (1997) 590-593.

[BJ98] S. C. Benjamin, N. F. Johnson, Structures for Data Processing in the Quantum Regime, University of Oxford, (Online preprint cond-mat/9802127), (1998).

[Ben82] Benio, P. A., Quantum mechanical hamiltonian models of turing machines. Journal of Statistical Physics, 29(3):515-546, (1982).

[Ben96] Benio, P. A., Review of quantum computation. Trends in Statistical Physics by Council of Scientific Information, Trivandrum, India, 1996.

[Ben97] P. Benioff, Quantum Robots and Quantum Computers, (Online preprint quant-ph/9706012), submitted to Phys. Rev. A, (1997).

[B98a] P. Benioff, Quantum Robots and Environments, (Online preprint quant-ph/9802067), accepted for publication, Phys Rev A (1998).

[Ben98b] P. Benioff, (Online preprint quantum Robots Plus Environments, Argonne National Laboratory, (Online preprint quant-ph/9807032), (1998).

[Ben73] Bennett, C. H., Logical reversibility of computations. IBM Journal of Res. Develop., 17:525-532, (1973).

[Ben89] Bennett, C. H., Time/space trade-offs for reversible computation, SIAM J. Comput. 18, 766 (1989).

[B95] C. H. Bennett, *Quantum information and computation*, Physics Today, pp. 24-30, (October 1995).

[BBB+97] Bennett, C. B., E. Bernstein, G. Brassard, and U. Vazirani, Strengths and weaknesses of quantum computing. (Online preprint quant-ph/9701001.), SIAM Journal on Computing, 26(5):1510-1523, (October 1997).

[BDS97b] Bennett, C. H., D. P. DiVincenzo and J. A. Smolin, Capacities of quantum erasure channels. (Online preprint quant-ph/9701015), (1997).

[BDS+96] Bennett, C., D. DiVincenzo, J. Smolin and Wootters, W. Mixed state entanglement and quantum error correction. (Online preprint quant-ph/9604024), Phys. Rev. A 54, 3824, (1996).

[BBP+95] Bennett, C. H., Bernstein, Popescu, and Schumacher, Concentrating Partial Entanglement by Local Operations, Phys. Rev. A., (1995).

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. Journal of Cryptology, 5(1):3-28, 1992.

[BB84a] Bennett, C. H., G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India. New York: IEEE, p. 175. (1984).

[BB84b] C. H. Bennett and G. Brassard. An update on quantum cryptography. In G. R. Blakley and D. Chaum, editors, Advances in Cryptology: Proceedings of CRYPTO 84, volume 196 of Lecture

Notes in Computer Science, pages 475-480, (August 1984). Springer-Verlag, 1995.

[BBB+82] C. H. Bennett, G. Brassard, S. Breidbart, S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In D. Chaum and R. L. Rivest and A. T. Sherman, editors, Advances in Cryptology: Proceedings of Crypto 82, pages 267-275, (August 1982). Plenum Press, New York and London, 1983.

[BBC+91] C. H. Bennett, G. Brassard, C. Crpeau and M.-H. Skubiszewska. Practical quantum oblivious transfer. In J. Feigenbaum, editor, Advances in Cryptology –CRYPTO '91, volume 576 of Lecture Notes in Computer Science, pages 351-366, (August 1991). Springer-Verlag, 1992.

[BBJ+94] Bennett, C. H., G. Brassard, Jozsa, Mayers, Peres, Schumacher, and Wootters, Reduction of Quantum Entropy by Reversible Extraction of Classical Information, in Journal of Modern Optics, (1994).

[BBC93] Bennett, C. H., Brassard, Crepeau, Jozsa, Peres and Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels, PRL 70, 1895 (1993).

[BBE92] Bennett, C. H., G. Brassard, and A Ekert. Quantum cryptography. Scientific American, pages 50-57, (October 1992).

[BBP+96] Bennett, C. H., Brassard, Popescu, Schumacher, Smolin, and Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. 76, 722 (1996).

[BD95a] Bennett, and D. P. DiVincenzo, Progress Towards Quantum Computation, Nature, (October 1995).

[BD95b] Bennett, C.H., D. P. DiVincenzo, Quantum Computing: Towards an Engineering Era?, Nature, Vol. 377, (1995).

[BDS+96] Bennett, C.H., D. P. DiVincenzo, Smolin, and Wootters, Mixed State Entanglement and Quantum Error Correction, submitted to Phys. Rev. A., (1996).

[BL85] Bennett, C.H., R. Landauer, Physical limits of computation, Scientific American, page 48, (July 1985).

[BDL+98] G. P. Berman, G. D. Doolen, G. V. Lopez, V. I. Tsifrinovich, Quantum Entangled States and Quasiclassical Dynamics in Macroscopic Spin Systems, (Online preprint quant-ph/9802015), (1998).

[BV93] Bernstein, E. and U. Vazirani, Quantum complexity theory. In Proceedings of the 25th ACM Symposium on the Theory of Computation. New York: ACM Press, pp. 11-20, (1993).

[BV97] Bernstein, E. and U. Vazirani, Quantum complexity theory. SIAM Journal on Computing, 26(5):1411-1473, (October 1997).

[Ber95] A. Berthiaume. L'ordinateur quantique: complexit'e et stabilisation des calculs. PhD thesis, Dept. d'informatique et de recherche operationelle, Universite de Montreal, (1995).

[BB92a] Berthiaume, A. and G. Brassard, The quantum challenge to structural complexity. In Proceedings of the 7th Annual IEEE Conference on Structure in Complexity, pages 132-137, 1992.

[BB92b] Berthiaume, A. and G. Brassard. Oracle quantum computing, In Proceedings of the Workshop on Physics and Computation - Physcomp '92, pages 195-199. IEEE Press, (October 1992).

[BB94] Berthiaume, A. and G. Brassard. Oracle quantum computing, Journal of Modern Optics, 41(12):2521-2535, (1994).

[BDJ94] A. Berthiaume, D. Deutsch, and R. Jozsa. The stabilisation of quantum computations. In Proceedings of the Workshop on Physics and Computation - Physcomp 94, 60-62, (1994).

[BBB+98] D. Biron, O.Biham, E.Biham, M. Grassl, D.A. Lidar, Generalized Grover Search Algorithm for Arbitrary Initial Amplitude Distribution, (Online preprint quant-ph/9801066), QCQC 98, (Feb. 1998).

[BCK96] M. Biskup, P. Cejnar, R. Kotecky, Decoherence and Efficiency of Quantum Error Correction, (Online preprint quant-ph/9608010), submitted to Phys.Rev.A (1996).

[Bog98] B. M. Boghosian, Simulating quantum mechanics on a quantum computer, (Online preprint quant-ph/9701019), Physica D120 (1998) 30-42.

[BT96] B. M. Boghosian, W. Taylor, Quantum lattice-gas models for the many-body Schrodinger equation, (Online preprint quant-ph/9701016), Sixth International Conference on Discrete Fluid Mechanics, BU, Boston MA, (August 1996).

[BT97]Boghosian, B. M. and Taylor, W. Simulating quantum mechanics on a quantum computer. (Online preprint quant-ph/9701019.), (1997).

[BIW+97] Bollinger, J. J., Itano, W. M., Wineland, D. J. and Heinzen, D. J. Optical frequency measurements with maximally correlated states. Phys. Rev. A 54, R4649, (1997).

[BL95] Dan Boneh and Richard J. Lipton. Quantum cryptanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, Advances in Cryptology – CRYPTO '95, volume 963 of Lecture Notes in Computer Science, pages 424-437, (August 1995). Springer-Verlag.

[BVK97] S.Bose, V.Vedral, P.L.Knight, A Multiparticle Generalization of Entanglement Swapping, (Online preprint quant-ph/9708004), (1997).

[BKS95] Braginsky, V. B., Khalili, F. ya. and Sazhin, M. V., Decoherence in e.m. vacuum. Phys. Lett. A 208, 177, (1995).

[Bra93] Brassard, G., Cryptology column — quantum cryptography: A bibliography. Sigact News, 24(3):16-20, (1993).

[Bra94] Brassard, G., Cryptology Column – Quantum Computing: The End of Classical Cryptography?, SIGACTN: SIGACT News (ACM Special Interest Group on Automata and Computability Theory), Vol. 25, (1994).

[Bra96] Brassard, G., New Trends in Quantum Computing, (Online preprint quant-ph/9602014), 13th Symposium on Theoretical Aspects of Computer Science, Grenoble, Lecture Notes in Computer Science, Springer-Verlag, (Feb. 1996).

[Bra96] G. Brassard, Teleportation as a quantum computation, (Online preprint quant-ph/9605035), Physica D120 (1998) 43-47.

[Bra97] G. Brassard, Quantum information processing: The good, the bad and the ugly. In Burton, S. Kaliski Jr., editor, Advances in Cryptology – CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 337-341, (August 1997).

[Bra98] Brassard, G., New horizons in quantum information processing, Proceedings of the 25th Colloquim on Automata, Languages, and Programming, Aalborg, Denmark, (May 1998). [BC90] G.

Brassard, C. Crpeau. Quantum bit commitment and coin tossing protocols. In A. J. Menezes and S. A. Vanstone, editors, Advances in Cryptology – CRYPTO '90, volume 537 of Lecture Notes in Computer Science, pages 49-61, (August 1990). Springer-Verlag, 1991.

[BCJ93] G. Brassard, C. Crpeau, R. Jozsa,D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In 34th Annual Symposium on Foundations of Computer Science, pages 362-371, Palo Alto, California, (November 1993).

[BCM+98] G. Brassard, C. Crpeau, D. Mayers, L. Salvail, Defeating classical bit commitments with a quantum computer, (Online preprint quant-ph/9806031), (1998).

[BH96] G. Brassard, P. Hoyer, On The Power of Exact Quantum Polynomial Time, (Online preprint quant-ph/9612017), (1996).

[BHT96] Brassard, G., Peter Hoyer, and Alain Tapp, Quantum Counting, (Online preprint quant-ph/9805082), (1996).

[BHT98] Brassard, G., P. Hoyer, and A. Tapp, Quantum Counting, Proceedings of the 25th Colloquim on Automata, Languages, and Programming, Aalborg, Denmark, (May 1998). [BH97] G. Brassard, P.

Hoyer, An Exact Quantum Polynomial-Time Algorithm for Simon's Problem, (Online preprint quant-ph/9704027), Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems (ISTCS'97), (1997).

[BFG+95] S. L. Braustein, C. A. Fuchs, D. Gottesman, H-K. Lo, *A quantum analog of Huffman Coding*, report no. quant-ph/9805080 (May 1998).

[BS96] S. L. Braunstein, J. A. Smolin, Perfect quantum error correction coding in 24 laser pulses, (Online preprint quant-ph/9604036), (1996).

[BDE+97] H.J. Briegel, W. Dr, S. J. van Enk, J. I. Cirac, P. Zoller, Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel, (Online preprint quant-ph/9712027), Royal Society meeting on quantum computation (1997).

[BS98] T. A. Brun, R. Schack, Realizing the quantum baker's map on a 3-qubit NMR quantum computer, (Online preprint quant-ph/9807050), Submitted to Phys. Rev. A, (1998).

[BHD96] Brune, M., Hagley, E., Dreyer, J., Maitre, X., Maali, A., Wunerlich, C., Raimond, J. M. and Haroche, S., Observing the progressive decoherence of the meter in a quantum measurement. Phys. Rev. Lett. 77, 4887, (1996).

[BJ95] N. H. Bshouty and J. C. Jackson. Learning DNF over the uniform distribution using a quantum example oracle. In Proceedings of the Eighth Annual Conference on Computational Learning Theory, pages 118-127, Santa Cruz, California, (July 1995). ACM Press.

[BCW98] Buhrman, H., R. Cleve, and A. Wigderson, Quantum vs. Classical Communication and Computation, (Online preprint quant-ph/9802040), (1998).

[Bur98] W. Burkot, Reversible Mapping for Tree Structured Quantum Computation, (Online preprint quant-ph/9712033), submitted to Phys.Rev.Lett, (1998).

[BH98] V. Buzek, M. Hillery, Universal optimal cloning of qubits and quantum registers, (Online preprint quant-ph/9801009), QCQC 98, (Feb. 1998).

[BLD98] G. Burkard, D. Loss, D. P. DiVincenzo, Coupled quantum dots as quantum gates, (Online preprint cond-mat/9808026), (1998).

[CSS+98a] Calderbank, A. R., E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction and orthogonal geometry, (Online preprint quant-ph/9605005), (1998).

[CRS98b] Calderbank, A. R., E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over GF(4), (Online preprint quant-ph/9608006), IEEE Transactions on Information Theory, Vol. 44, (1998).

[CS95] Calderbank, A. R., and P. W. Shor, Good quantum error-correcting codes exist, (Online preprint quant-ph/9512032), (December 1995), Phys. Rev. A 54, 1098.

[CM97] G. Castagnoli, D. Monti, A diakoptic approach to quantum computation, (Online preprint quant-ph/9712053), (1997).

[Cas97] G. Castagnoli, Quantum Computation Based on Retarded and Advanced Propagation, (Online preprint quant-ph/9706019), (1997).

[CBM98] G. Castagnoli, E. Bailey, D. Monti, (Online preprint quantum computation based on particle statistics, (Online preprint quant-ph/9806010), (1998).

[CK98] N. J. Cerf, S. E. Koonin, Monte Carlo Simulation of Quantum Computation, (Online preprint quant-ph/9703050), Math. and Comp. in Simulation 47 (1998), 143-152.

[CL98] H. F. Chau, H.-K. Lo, An Empty Promise With A Quantum Computer, (Online preprint quant-ph/9709053), Fortsch.Phys. 46 (1998) 507-520.

[CL96] I. L. Chuang, R. Laflamme, Quantum Error Correction by Coding, (Online preprint quant-ph/9511003), (1996).

[CLP96] I. L. Chuang, R. Laflamme, J. Paz, Effects of Loss and Decoherence on a Simple Quantum Computer, (Online preprint quant-ph/9602018), (1996).

[CLS+95] I. L. Chuang, R. Laflamme, P. Shor and W. H. Zurek, Quantum computers, factoring and decoherence, Report LA-UR-95-241 (Online preprint quant-ph/9503007), (1995).

[CVZ+98] I. L. Chuang, L. M.K. Vandersypen, X.Zhou, D. W. Leung, S. Lloyd, Experimental realization of a quantum algorithm, (Online preprint quant-ph/9801037), Nature, 393, 143-146, (1998).

[CY95] I. L. Chuang, Y. Yamamoto, A Simple Quantum Computer, (Online preprint quant-ph/9505011), Submitted to Physical Review A (1995).

[CY96] I. L. Chuang, Y. Yamamoto, Quantum Bit Regeneration, (Online preprint quant-ph/9604031), Phys. Rev. Lett., (May 13, 1996).

[CZ95] Cirac, J. I. and Zoller, P. Quantum computations with cold trapped ions., Phys. Rev. Lett. 74, 4091, (1995).

[CPZ96] Cirac, J. I., Pellizzari and Zoller, P., Enforcing coherent evolution in dissipative quantum dynamics. Science 273, 1207,(1996).

[CZ97] Cirac, J. I., Zoller, P., Kimble, H. J. and Mabuchi, H., Quantum state transfer and entanglement distribution among distant nodes in a quantum network. Phys. Rev. Lett. 78, 3221, (1997).

[CDN+98] R. Cleve, W. van Dam, M. Nielsen, A. Tapp, Quantum Entanglement and the Communication Complexity of the Inner Product Function, (Online preprint quant-ph/970801), QCQC 98, (Feb. 1998).

[CD96] R. Cleve, D. P. DiVincenzo, Schumacher's quantum data compression as a quantum computation, (Online preprint quant-ph/9603009), (1996).

[CEM+98] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, Quantum Algorithms Revisited, (Online preprint quant-ph/9708016), Submitted to Proc. Roy. Soc. Lond. A (1998).

N. J. Cerf, C. Adami, Quantum Information Theory of Entanglement and Measurement, (Online preprint quant-ph/9605039.), Physica D120, 62-81, (1998).

[Cop94] D. Coppersmith. An approximate fourier transform useful in quantum computing. IBM Research Report RC19642, (1994).

[CFH96] Cory, D. G., Fahmy, A. F. and Havel, T. F., Nuclear magnetic resonance spectroscopy: an experimentally accessible paradigm for quantum computing. In Proceedings of the 4th Workshop on Physics and Computation, Boston: New England Complex Systems Institute, (1996).

[CMP+98] D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, S. S. Somaroo, Experimental Quantum Error Correction, (Online preprint quant-ph/9802018), (1998).

[CPH97] D. G. Cory, M. D. Price, T. F. Havel, Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing, (Online preprint quant-ph/9709001), (1997).

[Coc97] P. Cockshott, Quantum Relational Databases, (Online preprint quant-ph/9712025), (1997).

[CKH98] D. Collins, K. W. Kim, W. C. Holton, Deutsch-Jozsa algorithm as a test of quantum computation, (Online preprint quant-ph/9807012), Approved for publication in Phys Rev A, (1998).

[CS97] G. Costantini, F. Smeraldi, A Generalization of Deutsch's Example, (Online preprint quant-ph/9702020), (1997).

[CS95] C. Crpeau, L.Salvail. Quantum oblivious mutual identification. In L. C. Guillou and J.-J. Quisquater, editors, Advances in Cryptology – EUROCRYPT 95, volume 921 of Lecture Notes in Computer Science, pages 133-146. Springer-Verlag, (May 1995).

[Cza98a] M. Czachor, Notes on nonlinear quantum algorithms, (Online preprint quant-ph/9802051), (1998).

[Cza98b] M. Czachor, Local modification of the Abrams-Lloyd nonlinear algorithm, (Online preprint quant-ph/9803019), submitted to PRA (Rapid. Comm.), (1998).

[Dam98a] W. van Dam, Two Classical Queries versus One Quantum Query, (Online preprint quant-ph/9806090), (1998).

[Dam98b] W. van Dam, (Online preprint quantum Oracle Interrogation: Getting all information for almost half the price, U of Oxford, CWI, (Online preprint quant-ph/9805006), (1998).

[Deu85a] D. Deutsch, Three connections between Everetts Interpretation and experiment, Quantum concepts in space and time, (1985).

[Deu85b] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society, London, A400:97-117, (1985).

[Deu89] D. Deutsch. Quantum computational network. Proceedings of the Royal Society, London, A425:73-90, (1989).

[DBE95] D. Deutsch, A. Barenco and A. Ekert, Universality in Quantum Computation, (Online preprint quant-ph/9505018), Proc. Roy. Soc. Lond. A 449, 669 (1995).

[DJ92] D. Deutsch and R. Jozsa. Rapid solutions of problems by quantum computation. In Proceedings of the Royal Society, London, volume A439, pages 553-558, (1992).

[DW73] B. S. DeWitt, In Many-wolds interpretation of Quantum Mechanics, (ed. B. S. DeWitt and N. Graham). Princeton University Press, Princeton, (1973).

[DL94] L. Diosi, B. Lukacs, Eds., Stochastic Evolution of Quantum States in Open Quantum Systems and in the Measurement Process, London: World Scientific, (1994).

[DTS96] C. Dürr and H. L Thanh and M. Santha. A decision procedure for well-formed linear quantum cellular automata. In 13th Annual Symposium on Theoretical Aspects of Computer Science, volume 1046 of Lecture Notes in Computer Science, pages 281-292, Grenoble, France, 22-24 (February 1996). Springer.

[DiV95] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. Physical Review Letters A, 50(1015), (1995).

[DiV96] D. P. DiVincenzo, Quantum Gates and Circuits, (Online preprint quant-ph/9705009), Proceedings of the ITP Conference on Quantum Coherence and Decoherence, (December, 1996), submitted Proc. R. Soc. London A.

[DiV97a] D. P. DiVincenz, Topics in Quantum Computers, (Online preprint), Mesoscopic Electron Transport", edited by L. Kowenhoven, G. Schoen and L. Sohn, NATO ASI Series E, Kluwer Ac. Publ., Dordrecht. (1997).

[DiV97b] D. P. DiVincenzo, Quantum Computation and Spin Physics, (Online preprint cond-mat/9612125), Proceedings of the Annual MMM Meeting, November, 1996, to be published in J. Appl. Phys (1997).

[DFM+98] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. Thapliyal, A. Uhlmann, Entanglement of Assistance, (Online preprint quant-ph/9803033), QCQC 98, (Feb. 1998).

[DVL98] D. P. DiVincenz, D. Loss, Quantum Information is Physical, (Online preprint cond-mat/9710259), to be published in Superlattices and Microstructures, Special Issue on the Occasion of Rolf Landauer's 70th Birthday. (1998).

[DMS+95] D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, Elementary gates for quantum computation, submitted to Phys. Rev. A (1995).

[DS+96] DiVincenzo, D. and Shor, P., Fault-tolerant error correction with efficient quantum codes. Phys. Rev. Lett. 77, 3260, (1996).

[DSS+95] D. P. DiVincenzo, Peter W. Shor, and John A. Smolin, Quantum channel capacity of very noisy channels, (Online preprint quant-ph/9706061), to appear 1998.

[DS98] D. P. DiVincenzo and J. Smolin, Results on Two-bit gate design for quantum computers, (1998).

[DG98] L. Duan, G. Guo, Reducing decoherence in quantum computer memory with all quantum bits coupling to the same environment, (Online preprint quant-ph/9612003), Phys. Rev. A 57 (2), 737 (1998).

[DS96] C. Durr, M. Santha, A decision procedure for unitary linear quantum cellular automata, (Online preprint quant-ph/9604007), In 37th Annual Symposium on Foundations of Computer Science, pages 38-45, Burlington, Vermont, (October 1996). IEEE.

[DG97a] L. Duan, G. Guo, Cooperative loss and decoherence in quantum computation and commuication, (Online preprint quant-ph/9701020), (1997).

[DG97b] L. Duan, G. Guo, Preserving coherence in quantum computation by pairing quantum bits, (Online preprint quant-ph/9703040), Phys. Rev. Lett. 79, 1953, (1997).

[DG98] L. Duan, G. Guo , Pulse controlled noise suppressed quantum computation, University of Science and Technology of China , (Online preprint quant-ph/9807072), (1998).

[Dun98] M. R. Dunlavey, Simulation of finite state machines in a quantum computer, (Online preprint quant-ph/9807026), (1998).

[DMO98] M. Durdevich, H. E. Makaruk, R. Owczarek, Generalized Noiseless Quantum Codes utilizing Quantum Enveloping Algebras, (Online preprint quant-ph/9805084), (1998).

[Eke97] A. Ekert, From quantum-codemaking to quantum code-breaking, (Online preprint quant-ph/9703035), (1997).

[EHM+98] A. Ekert, S.F. Huelga, C. Macchiavello, J.I. Cirac, Distributed Quantum Computation over Noisy Channels, (Online preprint quant-ph/9803017), (1998).

[EJ96] A. Ekert and R. Jozsa. Shor's quantum algorithme for factoring numbers, Review of Modern Physics, (1996).

[EV 93] A. C. Elizur and L. Vaidman, Quantum Mechanical Interaction-free Measurement, Foundations of Physics, 23:7, 987-997, (July, 1993).

[ECZ97] Van Enk, S. J., Cirac, J. I. and Zoller, P., Quantum communication over noisy channels: a quantum optical implementation. (Online preprint quant-ph/9702036.), (1997).

[Eve57] H., Everett, Rev. Modern Physics, 29, pp 454, (1957).

[FGG+98] E. Farhi (MIT), J. Goldstone (MIT), S. Gutmann, M. Sipser, A Limit on the Speed of Quantum Computation in Determining Parity, (Online preprint quant-ph/9802045), (1998).

[FG96] E. Farhi, S. Gutmann, An Analog Analogue of a Digital Quantum Computation, (Online preprint quant-ph/9612026), (1996).

[FG98] E. Farhi, S. Gutmann, Quantum Computation and Decision Trees, (Online preprint quant-ph/9706062), to appear in Phys Rev A (1998).

[Fey82] R. P. Feynman. Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7): pp. 467-488, (1982).

[Fey86] R. P. Feynman. Quantum mechanical computers. Foundation of Physics, 16(6):507-531, (1986).

[FLS64] R. P. Feynman, R. B. Leighton, and M. Sands. The Feynman Lectures on Physics, volume 3. Addison-Wesley, (1964).

[Fuc97] Fuchs, C., Nonorthogonal quantum states maximize classical information capacity. (Online preprint quant-ph/9703043.), (1997).

[Fuc96] C. A. Fuchs, Distinguishability and Accessible Information in Quantum Theory, (Online preprint quant-ph/9601020), (1996).

[FC94] C. Fuchs and C. Caves, Ensemble-dependent bounds for accessible information in quantum mechanics, Physics Rev. Lett. Vol. 73, pp 3047–3050, (1994).

[Gar97] A. Garg, Decoherence in ion-trap quantum computers. Czech. J. Phys. 46, 2375, (1996).

[Gar97] A. Garg, Vibrational Decoherence in Ion Trap Quantum Computers, (Online preprint quant-ph/9710053), (1997).

[Gar98] A. Garg, Vibrational Decoherence in Ion-Trap Quantum Computers, (Online preprint quant-ph/9803071), (1998).

[GH98] R. Garisto, L.Hardy, Entanglement of projection and a new class of quantum erasers, (Online preprint quant-ph/9808007), (1998).

[GC97]Gershenfeld, N. and Chuang, I. Bulk spin resonance quantum computation. Science 275, 350, (1997).

[GC98] N. Gershenfeld and I. L. Chuang Quantum Computing with Molecules, Scientific American, 278(6), pp. 66-71, (June 1998).

[Got97] D. Gottesman, Stabilizer Codes and Quantum Error Correction, (Online preprint quant-ph/9705052), Caltech Ph.D. Thesis (1997).

[Got98a] D. Gottesman, The Heisenberg Representation of Quantum Computers, UC Berkeley, (Online preprint quant-ph/9807006), 1998 International Conference on Group Theoretic Methods in Physic (1998).

[Got98b] D. Gottesman, A Theory of Fault-Tolerant Quantum Computation, (Online preprint quant-ph/9702029), Phys.Rev. A57 (1998) 127.

[Got98c] D. Gottesman, Fault-Tolerant Quantum Computation with Higher-Dimensional Systems, (Online preprint quant-ph/9802007), QCQC 98, (Feb. 1998c).

[Got66] K. Gottfield, Quantum Mechanics. London: Benjamin-Cummings (reprinted by Addison-Wesley, 1989), ch 4, pp. 165-190, (1966).

[GEK+96] Gottesman, D., Evslin, J., Kakade, S. and Preskill, J., (1996).

[GB96] Grassl, M., Beth, Th. and Pellizzari, T., Codes for the quantum erasure channel. (Online preprint quant-ph/9610042.), (1996).

[GN96] R. B. Griffiths, C. Niu, Semiclassical Fourier Transform for Quantum Computation, (Online preprint quant-ph/9511007), Phys.Rev.Lett. 76 (1996) 3228-3231.

[Gri97] D. Grigoriev. Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines. Theoretical Computer Science, 180(1-2):217-228, (June 1997).

[Gro96] L. K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212-219, Philadelphia, PA, (May, 1996).

[Gro97] L. K. Grover, Quantum computers can search arbitrarily large databases by a single query, (Online preprint quant-ph/9706005), (1997).

[Gro98] L. K. Grover, Quantum computers can search rapidly by using almost any transformation, (Online preprint quant-ph/9712011), Phys.Rev.Lett. 80, 4329-4332 (1998).

[Hav98] T. F. Havel Expressing the operations of quantum computing in multiparticle geometric algebra. (Online preprint quant-ph/9801002.), (1998).

[HP97] O. Hay, A. Peres, Quantum and classical descriptions of a measuring apparatus, (Online preprint quant-ph/9712044.), (1997).

[HM97] D'Helon, C. and Milburn, G. J. Quantum measurements with a quantum computer. (Online preprint quant-ph/9705014.), (1997).

[Hir98] M. Hirvensalo, Quantum Error Correction, Technical Report, TUCS - Turku Centre for Computer Science, Number TUCS-TR-178, (May 1998).

[HR96] Haroche, S. and Raimond, J. M. Quantum computing: dream or nightmare? Phys. Today 49 (8), 51, (1996)

[H97] C. W. Helstrom. Detection theory and quantum mechanics. Information and Control, 10(3):254-291, (March 1967).

[H98] C. W. Helstrom. Detection theory and quantum mechanics (II). Information and Control, 13(2):156-171, (August 1968).

[Hog96] T. Hogg, Quantum Computing and Phase Transitions in Combinatorial Search, (Online preprint quant-ph/9508012), J. of Artificial Intelligence Research 4,91-128 (1996).

[HC96] T. Hogg, J. G. Chase, Quantum Smart Matter, (Online preprint uant-ph/9611021), PhysComp96, (1996).

[HY98] T. Hogg, M. Yanik, Local Search Methods for Quantum Computers, (Online preprint quant-ph/9802043), (1998).

[H97] A.S. Holevo, Some estimates of the information transmitted by quantum communication channels, Problemy Peredachi Informatsii, Vol. 9, pp 3–11, (1973). English translation in Problems of Information Transmission, (USSR), 9, pp. 177–183, (1973). [Hol96] Holevo, A. S., The capacity of quantum channel with general signal states. (Online preprint quant-ph/9611023), (1996).

[Hol97] A.S.Holevo, Coding Theorems for Quantum Communication Channels, Steklov Mathematical Institute, (Online preprint quant-ph/9708046), (1997).

[Hoy97] P. Hoyer, Efficient Quantum Transforms, (Online preprint quant-ph/9702028), (1997).

[HMP+97] Huelga, S. F., Macchiavello, C., Pellizzari, T., Ekert, A. K., Plenio, M. B., and Cirac, J. I. 1997 On the improvement of frequency standards with quantum entanglement. (Online preprint quantph/9707014.)

[Hru94] J. Hruby. Q-deformed quantum cryptography. In Alfredo De Santis, editor, Advances in Cryptology – EUROCRYPT 94, volume 950 of Lecture Notes in Computer Science, pages 468-472. Springer-Verlag, 1995, (May 1994).

[Hug97] R. J. Hughes, Cryptography, Quantum Computation and Trapped Ions, (Online preprint quant-ph/9712054), Submitted to "Philosophical Transactions of the Royal Society," proceedings of the Royal Society Discussion Meeting on "Quantum Computation: Theory and Experiment," London, England, (November 1997).

[HJG+98] R. J. Hughes, D. F. V. James, J. J. Gomez, M. S. Gulley, M. H. Holzscheiter, P. G. Kwiat, S. K. Lamoreaux, C. G. Peterson, V. D. Sandberg, M. M. Schauer, C. M. Simmons, C. E. Thorburn, D. Tupa, P. Z., The Los Alamos Trapped Ion Quantum Computer Experiment, (Online preprint quant-ph/9708050), Fortsch.Phys. 46 (1998) 329-362.

[HJK+96] R. J. Hughes, D. F. V. James, E. H. Knill, R. Laflamme, A. G. Petschek, Decoherence Bounds on Quantum Computation with Trapped Ions, (Online preprint quant-ph/9604026), (1996).

[HLM+96] R. J. Hughes and G. G. Luther and G. L. Morgan and C. G. Peterson and C. Simmons. Quantum cryptography over underground optical fibers. In Neal Koblitz, editor, Advances in Cryptology – CRYPTO '96, volume 1109 of Lecture Notes in Computer Science, pages 329-342, (August 1996). Springer-Verlag.

[Jam97] D. F. V. James, Quantum dynamics of cold trapped ions, with application to quantum computation, (Online preprint quant-ph/9702053), (1997).

[Jam98] D. F. V. James, The theory of heating of the quantum ground state of trapped ions, (Online preprint quant-ph/9804048), Phys.Rev.Lett. 81 (1998) 317-320.

[JGH+98] D. F. V. James, M. S. Gulley, M. H. Holzscheiter, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, C. G. Peterson, V. D. Sandberg, M. M. Schauer, C. M. Simmons, D. Tupa, P. Z. Wang, A. G. White, Trapped Ion Quantum Computer Research at Los Alamos, Los Alamos National Laboratory, (Online preprint quant-ph/9807071), QCQC 98, (Feb. 1998).

[Jon98] J. A. Jones, Fast Searches with Nuclear Magnetic Resonance Computers, Science 280, 229, (April 1998).

[JHM98] J. A. Jones, R. H. Hansen, M. Mosca, (Online preprint quantum Logic Gates and Nuclear Magnetic Resonance Pulse Sequences, (Online preprint quant-ph/9805070), Submitted to Journal of Magnetic Resonance, (1998).

[JMH98] J. A. Jones, M. Mosca, R. H. Hansen, Implementation of a Quantum Search Algorithm on a

Nuclear Magnetic Resonance Quantum Computer, (Online preprint quant-ph/9805069), Nature 393 (1998) 344-346.

[JM98a] J. A. Jones, M. Mosca , Approximate quantum counting on an NMR ensemble quantum computer, Submitted to Physical Review Letters, (1998).

[JM98b] J. A. Jones, M. Mosca, Implementation of a Quantum Algorithm to Solve Deutsch's Problem on a Nuclear Magnetic Resonance Quantum Computer, (Online preprint quant-ph/9801027), Journal of Chemical Physics, in press (August 1998).

[Joz96] Jozsa, Proc. R. Soc. Lond. A 435, 563 (1996).

[Joz97] R. Jozsa, Entanglement and Quantum Computation, (Online preprint quant-ph/9707034), Geometric Issues in the Foundations of Science, ed. S. Huggett et. al., (1997).

[Joz98] R. Jozsa, Quantum Effects in Algorithms, (Online preprint quant-ph/9805086), QCQC 98, (Feb. 1998).

[JS94] R. Jozsa and B. Schumacher, *A new proof of the quantum noiseless coding theorem*, J. Mod. Optics 41, 2343-2349 (1994).

[JHH+98] R. Jozsa, M. Horodecki, P. Horodecki, R. Horodecki, *Universal Quantum Data Compression*, preprint quant-ph/9805017 (May 1998).

[Kak98] S. Kak, On Initializing Quantum Registers and Quantum Gates, Louisiana State University, (Online preprint quant-ph/9805002), (1998).

[KWM98] B. E. King, C. S. Wood, C. J. Myatt, Q. A. Turchette, D. Leibfried, W. M. Itano, C. Monroe, D. J. Wineland, Initializing the Collective Motion of Trapped Ions for Quantum Logic, (Online preprint quant-ph/9803023), (1998).

[Kit95] A. Y. Kitaev, Quantum measurements and the Abelian Stabilizer Problem, preprint, (1995).

[KY96] Kitaev, A. Yu., Quantum computing: algorithms and error correction, preprint (in Russian), (1996).

[Kit97] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, (Online preprint quant-ph/9707021), (1997).

[KCL97] E. Knill, Is. Chuang, R. Laflamme, Effective Pure States for Bulk Quantum Computation, (Online preprint quant-ph/9706053), (1997).

[KL96a] E. Knill, R. Laflamme, Concatenated Quantum Codes, (Online preprint quant-ph/9608012), (1996).

[KL96b] E. Knill, R. Laflamme, A Theory of Quantum Error-Correcting Codes, (Online preprint quant-ph/960403), (1996).

[KL98] E. Knill, R. Laflamme, On the Power of One Bit of Quantum Information, (Online preprint quant-ph/9802037), (1998).

[KLZ96] E. Knill, R. Laflamme, W. Zurek, Threshold Accuracy for Quantum Computation, (Online preprint quant-ph/9610011), (1996).

[KLZ97] E. Knill, R. Laflamme, W. H. Zurek, Resilient Quantum Computation: Error Models and Thresholds, (Online preprint quant-ph/9702058), (1997).

[KW97] A. Kondacs and J. Watrous. On the power of quantum finite state automata. In 38th Annual Symposium on Foundations of Computer Science, pages 66-75, Miami Beach, Florida, (October 1997). IEEE.

[Kan98] B.E. Kane, A silicon-based nuclear spin quantum computer, Nature, 393, 133137, (1998).

[KWZ 96] P. G. Kwiat, H. Weinfurter, and A. Zeilinger, Quantum Seeing in the Dark, Scientific American, (November, 1996).

[KWHZK 95] P. G. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, Interaction-free Measurement, Phys. Rev. Lett., 74, pp 4763-4766, (1995).

[LMP+96] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Perfect quantum error correction code, (Online preprint quant-ph/9602019), Phys.Rev. Lett., 77, 198, (1996).

[Lan61] R. Landauer. Irreversability and heat generation in the computing process, IBM Journal of Research Development, 5(183), (1961).

[Lan95] Landauer, R., Is quantum mechanics useful?, Phil. Tran. R. Soc. Lond. 353, 367, (1995).

[Lan97] Landauer, R. 1997 Is quantum mechanically coherent computation useful?, In Proc. Drexel-4 Symposium on Quantum Nonintegrability-Quantum-Classical Correspondence, Philadelphia, PA, 8 September 1994 (ed. D. H. Feng and B.-L. Hu), Boston: International Press, (1997).

[Lan96] Landauer, R., The physical nature of information. Phys. Lett. A 217, 188, (1996).

[LCD+87] Leggett, A. J., Chakravarty, S., Dorsey, A. T., Fisher, M. P. A., Garg, A. and Zwerger, W., Dynamics of the dissipative two-state system. Rev. Mod. Phys. 59, 1, (1987).

[LKZ+97] R. Laflamme, E. Knill, W.H. Zurek, P. Catasti, S.V.S. Mariappan, NMR GHZ, (Online preprint quant-ph/9709025), (1997).

[LV96] M. Li, P. Vitanyi, Reversibility and Adiabatic Computation: Trading Time and Space for Energy, (Online preprint quant-ph/9703022), Proc. Royal Society of London, Series A, 452(1996), 769-789.

[LB97] D. A. Lidar, O. Biham, Simulating Ising Spin Glasses on a Quantum Computer, (Online preprint quant-ph/9611038), Phys. Rev. E vol.56 (1997), p.3661.

[LW98] D. A. Lidar, H. Wang, Calculating the Thermal Rate Constant with Exponential Speed-Up on a Quantum Computer, UC Berkeley, (Online preprint quant-ph/9807009), (1998).

[LCW98] D.A. Lidar, I.L. Chuang, K.B. Whaley, Decoherence Free Subspaces for Quantum Computation, (Online preprint quant-ph/9807004), (1998).
[LBR98] N Linden, H Barjat, R Freeman, An implementation of the Deutsch-Jozsa algorithm on a three-qubit NMR quantum computer, (Online preprint quant-ph/9808039), (1998).

[LP98] N. Linden, S. Popescu, The Halting Problem for Quantum Computers, (Online preprint quant-ph/9806054), (1998).

[LC98] H.-K. Lo, H. F. Chau, Quantum Computers Render Quantum Key Distribution Unconditionally Secure Over Arbitrarily Long Distance, (Online preprint quant-ph/9803006), (1998).
[LC98] H.K. Lo, H. F. Chau, Why Quantum Bit Commitment And Ideal Quantum Coin Tossing Are Impossible, (Online preprint quant-ph/9711065), Accepted for publication in a special issue of Physica D, 177-187, (1998).

[LD97] D. Loss (Basel), D. P. DiVincenzo, Quantum Computation with Quantum Dots, (Online preprint cond-mat/9701055), (1997).

[Llo93] S. Lloyd. A potentially realizable quantum computer. Science, 261, 1569 (1993).

[Llo96] Lloyd, S., Universal quantum simulators. Science 273, 1073, (1996).
[Llo97a] Lloyd, S. The capacity of a noisy quantum channel, Phys. Rev. A 55, 1613, (1997a).

[Llo97b] S. Lloyd, J.-J. E. Slotine, Analog quantum error correction, (Online preprint quant-ph/9711021), (1997b).

[Llo97c] S. Lloyd, Almost any quantum logic gate is universal, Los Alamos National Laboratory preprint (1997c).

[MZ96] Mabuchi, H. and Zoller, P., Inversion of quantum jumps in quantum-optical systems under continuous observation, Phys. Rev. Lett. 76, 3108, (1996).

[GK98] G. Mahler, I. Kim, Correlation between Correlations: Process and Time in Quantum Networks, (Online preprint quant-ph/9803008), QCQC 98, (Feb. 1998).

[MAC98] J. Machta, Phase Information in Quantum Oracle Computing, (Online preprint quant-ph/9805022), (1998).

[Mal94] O. Q. Malhas. Abacus logic: The lattice of quantum propositions as the poset of a theory. The Journal of Symbolic Logic, 59(2):501-515, (June 1994).
[Mal94] J. Malinowski. The deduction theorem for quantum logic – some negative results. The Journal of Symbolic Logic, 55(2):615-625, (June 1990).

[MN96a] N.E. Mavromatos, D.V. Nanopoulos, Microtubules: The neuronic system of the neurons?, (Online preprint quant-ph/9702003), N.E. Mavromatos, D.V. Nanopoulos Workshop on Biophysics of Microtubules, Texas Medical Center, Houston, Texas, (April 1996).

[MN96b] N.E. Mavromatos, D.V. Nanopoulos, A Non-critical String (Liouville) Approach to Brain Microtubules: State Vector reduction, Memory coding and Capacity, (Online preprint quant-ph/9512021), (1996).

[May95] D. Mayers. On the security of the quantum oblivious transfer and key distribution protocols. In Don Coppersmith, editor, Advances in Cryptology – CRYPTO '95, volume 963 of Lecture Notes in Computer Science, pages 124-135, (August 1995). Springer-Verlag.

[May96] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In Neal Koblitz, editor, Advances in Cryptology – CRYPTO '96, volume 1109 of Lecture Notes in Computer Science, pages 343-357, (August 1996). Springer-Verlag.

[May97] P. Maymin, The lambda-q calculus can efficiently simulate quantum computers, (Online preprint quant-ph/9702057), (1997).

[May96] P. Maymin, Programming Complex Systems, (Online preprint quant-ph/9710035), (1996).

[Mee96] Meekhof, D. M., Monroe, C., King, B. E., Itano, W. M. and Wineland, D. J. Generation of nonclassical motional states of a trapped atom. Phys. Rev. Lett. 76, 1796 (1996).

[Mey96a] Meyer, D. A., Quantum mechanics of lattice gas automata I: one particle plane waves and potentials. (Online preprint quant-ph/9611005), (1996)

[Mey96b] D. A. Meyer, From quantum cellular automata to quantum lattice gases, (Online preprint quant-ph/9604003), J. Stat. Phys. 85, (1996) 551-574.

[Mil76] G.L. Miller, Reimann's hypothesis and test for primality, J. Computer Systes Sci., Vol. 12, pp. 300-317, (1976).

[MPP96] C. Miquel, J. P. Paz, R. Perazzo, Factoring in a Dissipative Quantum Computer, (Online preprint quant-ph/9601021), (1996).

[MP97] C. Miquel, J. P. Paz, W. H. Zurek, Quantum computation with phase drift errors, (Online preprint quant-ph/9704003), (1997).

[MMK95] Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. and Wineland, D. J., Demonstration of a fundamental quantum logic gate, Phys. Rev. Lett. 75, 4714, (1995).

[MN98a] C. Moore, M. Nilsson, Parallel Quantum Computation and Quantum Codes, (Online preprint quant-ph/9808027), (1998).

[CN98b] C. Moore, M. Nilsson, Some Notes on Parallel Quantum Computation, (Online preprint quant-ph/9804034), (1998).

[MC97] C. Moore, J. P. Crutchfield, Quantum Automata and Quantum Grammars, (Online preprint quant-ph/9707031), (1997).

[Mor96] T. Mor, Reducing Quantum Errors and Improving Large Scale Quantum, (Online preprint quant-ph/9608025), (1996).

[MPH96a] D. Mozyrsky, V. Privman, S. P. Hotaling, Extended Quantum XOR Gate in Terms of Two-Spin Interactions, (Online preprint quant-ph/9610008), (1996).

[MPH96b] D. Mozyrsky, V. Privman, S. P. Hotaling, Design of gates for quantum computation: the NOT gate, (Online preprint quant-ph/9608029), (1996).

[MPH97] D. Mozyrsky, V. Privman, S. P. Hotaling, International Journal of Modern Physics B 11, 2207-2215 (1997).

[MPH98] D. Mozyrsky, V. Privman, S. P. Hotaling, Design of gates for quantum computation: the three-spin XOR gate in terms of two-spin interactions, (Online preprint uant-ph/9612029), International Journal of Modern Physics B 12 (1998) 591-600.

[MPP+97] M. Murao M.B. Plenio, S. Popescu, V. Vedral, P.L. Knight, Multi-Particle Entanglement Purification Protocols, (Online preprint quant-ph/9712045), (1997).

[Nan96] D. Nanopoulos, Theory of Brain Function, (Online preprint quantum Mechanics and Superstrings, (Online preprint hep-ph/9505374), (1996).

[Neu32] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Chapter 4: Macroscopic Measurement, Springer Verlag, (1932).

[Neu96] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Chapter 4: Macroscopic Measurement, Reprinted in Princeton Landmarks in Mathematics, Princeton University Press, (1996).

[Nie96] M. A. Nielsen, The entanglement fidelity and quantum error correction, (Online preprint quant-ph/9606012), (1996).

[NCS+97] M. A. Nielsen, Caves, C.M., Schumacher, B., and Barnum, H. Information-theoretic approach to quantum error correction and reversible measurement, (Online preprint quant-ph/9706064), (1997).

[Ohy98] M. Ohya, A mathematical foundation of quantum information and quantum computer -on quantum mutual entropy and Entanglement, (Online preprint quant-ph/9808051), (1998).

[OD96a] Obenland, K. and Despain, A. M., Simulation of factoring on a quantum computer architecture. In Proceedings of the 4th Workshop on Physics and Computation, Boston, Nov. (Nov. 1996), Boston: New England Complex Systems Institute.

[OD96b] Obenland, K. and Despain, A. M., Impact of errors on a quantum computer architecture. (Online preprint http://www.isi.eu/acal/quantum/quantum op errors.ps.), (1996)

[OD97] K. M. Obenland, A. M. Despain, Models to Reduce the Complexity of Simulating a Quantum Computer, (Online preprint quant-ph/9712004), (1997).

[OD98a] K. M. Obenland, A. M. Despain, Simulating the Effect of Decoherence and Inaccuracies on a Quantum Computer, (Online preprint quant-ph/9804038), QCQC 98, (Feb. 1998).

[OD98b] K. M. Obenland, A. M. Despain, A Parallel Quantum Computer Simulator, (Online preprint quant-ph/9804039), High Performance Computing, (1998).

[OHT+84] C. K. Ong and G. M. Huang and T. J. Tarn and J. W. Clark. Invertibility of quantum-mechanical control systems. Mathematical Systems Theory, 17(4):335-350, (November 1984).

[Oza98] M. Ozawa, Quantum Nondemolition Monitoring of Universal Quantum Computers, (Online preprint quant-ph/9704028), to appear in Phys.Rev.Lett. 80 (1998) 631.

[Ozh97a] Y. Ozhigov, Protection of information in quantum qatabases, (Online preprint quant-ph/9712016), (1997).

[Ozh97b] Y. Ozhigov, About the quantum mechanical speeding up of classical algorithms, (Online preprint quant-ph/9706003), (1997).

[Ozh97c] Y. Ozhigov, Quantum Computer Can Not Speed Up Iterated Applications of a Black Box, (Online preprint quant-ph/9712051), (1997).

[Ozh98] Y. Ozhigov, Quantum Computers Speed Up Classical with Probability Zero, (Online preprint quant-ph/9803064), (1998).

[PSE96] G. M. Palma, K. Suominen, A. K. Ekert, Quantum Computers and Dissipation, (Online preprint quant-ph/9702001), Proc.Roy.Soc.Lond. A452 (1996) 567-584.

[PSE95] Palma G. M., K.-A. Suominen, and A. Ekert. Decoherence in quantum registers, preprint (1995).

[PAT98] A. K. Pati, Fast quantum search algorithm and Bounds on it, Theory Div. BARC, Mumbai, India, (Online preprint quant-ph/9807067), (1998).

[PGC+95] T. Pellizzari, S. A. Gardiner, J. I. Cirac and P. Zoller, Decoherence, continuous observation and quantum computing: a cavity QED model, preprint, Phys. Rev. Lett. 75, 3788, (1995).

[PGCZ95] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller. Decoherence, continuous observation and quantum computing: A cavity QED model, Submitted to Physical Review Letters, (1995).

[Pel97] T. Pellizzari, Quantum Networking with Optical Fibres, (Online preprint quant-ph/9707001), submitted to PRL (1997).

[Per96] A. Peres, Error symmetrization in quantum computers, (Online preprint quant-ph/9605009), PhysComp96 (1996).

[Per96] A. Peres, Error correction and symmetrization in quantum computers, (Online preprint quant-ph/9611046), Proceedings of PhysComp'96 workshop, Boston 21-24, November 1996, to appear in Physica D (1997).

[Per98] A. Peres, Quantum Disentanglement and Computation, (Online preprint quant-ph/9707047), to appear in special issue of Superlattices and Microstructures, in honor of the 70th birthday of Rolf Landauer (1998).

[Pea84] P. Pearle, State vector reduction as a dynamical process, proceedings of SUNY-Albany conference on Fundamental Questions in Quantum Mechanics (ed. A. Inomata, J. Kimball, and L. Roth), (1984).

[Pea85] P. Pearle, Models for reduction, Quantum concepts in space and time, (1985).

[PK96] M. B. Plenio, P. L. Knight, Realistic lower bounds for the factorization time of large numbers on a quantum computer, (Online preprint quant-ph/9512001), Phys. Rev. A 53, 2986 (1996).

[PK97] M.B. Plenio, P.L. Knight, Decoherence limits to quantum computation using trapped ions, (Online preprint quant-ph/9610015), Proc.Roy.Soc.Lond. A453 (1997) 2017-2041.

[PVK97] M. B. Plenio, V. Vedral, P. L. Knight, Conditional generation of error syndromes in fault-tolerant error correction, (Online preprint quant-ph/9608028), Phys.Rev. A55 (1997) 4593.

[PCZ96] J. F. Poyatos, J. I. Cirac, P. Zoller, Complete Characterization of a Quantum Process: the Two-Bit Quantum Gate, (Online preprint quant-ph/9611013), Physical Review Letters 08, (Nov 1996).

[Pre97] J. Preskill, Fault-tolerant quantum computation, (Online preprint quant-ph/9712048), to appear in "Introduction to Quantum Computation," edited by H.-K. Lo, S. Popescu, and T. P. Spiller (1997).

[Pre97a] J. Preskill, Quantum Computing: Pro and Con, (Online preprint quant-ph/9705032), submitted to Proc. Roy. Soc. Lond. A (1997).

[Pre97b] J. Preskill, Reliable Quantum Computers, (Online preprint quant-ph/9705031), submitted to Proc. Roy. Soc. Lond. A (1997).

[PMH+97] V. Privman, D. Mozyrsky, S. P. Hotaling, Hamiltonians for Quantum Computing, (Online preprint quant-ph/9705026), Proc. Conf. Photonic Quantum Computing. AeroSense 97, SPIE Proc. Vol. 3076, 84-96 (1997).

[PVK98] V. Privman, I. D. Vagner, G. Kventsel, Quantum Computation in Quantum-Hall Systems, (Online preprint quant-ph/9707017), Phys.Lett. A239 (1998) 141-146.

[PRB98] M. Pueschel, M. Roetteler, T. Bet, Fast Quantum Fourier Transforms for a Class of Non-abelian Groups, Universitaet Karlsruhe, (Online preprint quant-ph/9807064), (1998).

[Rei98a] J.H. Reif, On the Impossibility of Interaction-Free Sensing for Small I/O Bandwidth, (Online preprint in postscript http://www.cs.duke.edu/∼reif/paper/quantum.ps), (1998).

[Rei98b] J.H. Reif, Efficient Quantum Compression, submitted for publication, (Online preprint in postscript http://www.cs.duke.edu/∼reif/paper/qcompress.ps), (November. 1998).

[Rei98c] J.H. Reif, Alternative Computational Models: A Comparison of Biomolecular and Quantum Computation, Invited paper, 18th International Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS98), (December, 1998). A postscript preprint of this paper is online at http://www.cs.duke.edu/∼ reif/paper/altcomp.ps.

[Rei99] J.H. Reif, Quantum Information Processing: Compression, Coding, and Related Computations, (Online preprint in postscript http://www.cs.duke.edu/ reif/paper/qsurvey.ps), Jan. 1999.

[Sca98] V. Scarani, Quantum Computing, (Online preprint quant-ph/9804044), Accepted for publ. in American Journal of Physics, (1998).

[Sch97] R. Schack, Using a quantum computer to investigate quantum chaos, (Online preprint quant-ph/9705016), (1997).

[SJM98] S. Schneider, D. F.V. James, G. J. Milburn, Method of quantum computation with "hot" trapped ions, (Online preprint quant-ph/9808012), submitted to PRL, (1998).

[SWM+98] S. Schneider, H.M. Wiseman, W.J. Munro, G.J. Milburn, Measurement and state preparation via ion trap quantum computing, (Online preprint quant-ph/9709042), Fortsch.Phys. 46, 391-400, (1998).

[SV98] L. J. Schulman, U. Vazirani, Scalable NMR Quantum Computation, (Online preprint quant-ph/9804060), (1998).

[Sch95] B. Schumacher, On quantum coding, Physical Review Letters A 51, 2738 (1995).

[SN96] Schumacher, B. and Nielsen, M. A., Quantum data processing and error correction. Phys. Rev. A 54, 2629, (1996).

[Shi98] Y. Shi, Is There a Universal Quantum Computer?, (Online preprint quant-ph/9805083), (1998).

[Sho95] P. Shor, Scheme for reducing decoherence in quantum memory. Phys. Rev. A 52, 2493, (1995).

[Sho94] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, (Nov. 1994).

[Sho96] P. W. Shor, Fault-tolerant quantum computation, (Online preprint quant-ph/9605011), 37th Symposium on Foundations of Computing, Los Alamitos, CA, IEEE Computer Society Press, pp. 56-65 (1996).

[Sho97] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, (Online preprint quant-ph/9508027), SIAM J. Computing 26 (1997) 1484.

[SL98] P. W. Shor and R. Laflamme, Quantum MacWilliams identities, (Online preprint quant-ph/9610040), (1998).

[Sho96] Shor, P. and Smolin, J., Quantum error-correcting codes need not completely reveal the error syndrome. (Online preprint quant-ph/9604006.), submitted to Phys. Rev. Lett. (1996).

[SS98] A.Shnirman, G. Schoen, Quantum Measurements Performed with a Single-Electron Transistor, (Online preprint cond-mat/9801125), submitted to Phys. Rev. B (1998).

[SSH97] A. Shnirman, G. Schoen, Z. Hermon, Quantum Manipulations of Small Josephson Junctions, (Online preprint cond-mat/9706016), submitted to Phys. Rev. Lett., (1997).

[Sid96] J. A. Sidles, The AC Stark, Stern-Gerlach, and Quantum Zeno Effects in Interferometric Qubit Readout, (Online preprint quant-ph/9612001), (1996).
[Sim94] Simon, D. R., On the power of quantum computation. In Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science. IEEE Press, pp. 116-123, (Nov. 1994).

[SW95] T. Sleator and H. Weinfurter, Realizable universal quantum logic gates, Phys. Rev. Lett. 74, 4087 (1995).

[SD95] J. A. Smolin and D. P. DiVincenzo, Five Two-Bit Quantum Gates are Sufficient to Implement the Quantum Fredkin Gate, Phys. Rev. A. 53, 2855 (1995).
[SCH98] S. S. Somaroo, D. G. Cory, T. F. Havel, Expressing the operations of quantum computing in multiparticle geometric algebra, (Online preprint quant-ph/9801002), Phys.Lett. A240 (1998) 1-7, (1998).

[Ste96a] Steane, A. M., Error correcting codes in quantum theory. Phys. Rev. Lett. 77, 793, (1996).

[Ste96b] A. Steane, Multiple particle interference and quantum error correction, (Online preprint quant-ph/9601029, Proceedings of the Royal Society of London Ser. A, 452, 2551, (1996).

[Ste97] A. Steane, Active stabilisation, (Online preprint quantum computation and quantum state synthesis, (Online preprint quant-ph/9611027), Phys.Rev.Lett. 78 (1997) 2252-2255.

[Ste98] A. Steane, Quantum Computing, (Online preprint quant-ph/9708022), Reports on Progress in Physics (1998).

[SZL98] C.P Sun, H.Zhan, X.F, Liu, On decoherence in quantum algorithm via dynamic models for quantum measurement, (Online preprint quant-ph/9802029), (1998).

[Svo94a] K. Svozil, Quantum computation and complexity theory, (Online preprint hep-th/9412047), (1994).

[Svo94b] K. Svozil, Speedup in quantum computation is associated with attenuation of processing probability, (Online preprint hep-th/9412046), (1994).

[Svo95] K. Svozil, Quantum algorithmic information theory, (Online preprint quant-ph/9510005), lectures given at the summer school, Chaitin Complexity and Applications, Mangalia, Mangalia, Romania (June 1995).

[Svo95] K. Svozil. Halting probability amplitude quantum computers. The Journal of Universal Computer Science, 1(3):201-204, (March 1995).

[Svo96] K. Svozil. Quantum information theory. The Journal of Universal Computer Science, 2(5):311-346, (May 1996).

[Tau96] Taubes, All Together for Quantum Computing, Science, Vol. 273, (1996).

[TOM88] W. Teich, K. Obermeyer, G. Mehler, Structural Basis of Multistationary Quantum Systems, II. Effective Few-Particle Dynamics, Physical Review B, Vol. 37, No 14, pp 8111-8120, (1988).
[TM8] W. Teich, G. Mehler, Information Processing at the Molecular Level: Possible Realizations and Physical Constraints. Complexity, Entropy, and the Physics of Information, SFI Studies in the Sciences of Complexity, Vol. VIII, W. Zurek (ed.), Addison Wesley, Reading, MA, pp. 289-300, (1990).

[Tof80] T. Toffoli, in Automata, Languages and Programming, Eds. J. W. de Bakker and J. van Leeuwen (Springer-Verlag, New York, p. 632 (1980).

[Ton98] V. D. Tonchev, Quantum self-dual codes and symmetric matrices, (Online preprint quant-ph/9711047), (1998).

[TS96] P. Torma, S. Stenholm, Polarization in Quantum Computations, (Online preprint quant-ph/9602021), (1996).

[Tuc98] R. R. Tucci, How to Compile A Quantum Bayesian Net, (Online preprint quant-ph/9805016), (1998).

[Tuc 98] R. R. Tucci, A Rudimentary Quantum Compiler, (Online preprint quant-ph/9805015), (1998).

[THL+95] Turchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H. and Kimble, H. J. Measurement of conditional phase shifts for quantum logic. Phys. Rev. Lett. 75, 4710, (1995).

[TWK+98] Q.A. Turchette, C.S. Wood, B.E. King, C.J. Myatt, D. Leibfried, W.M. Itano, C. Monroe, D.J. Wineland, Deterministic entanglement of two trapped ions, Time and Frequency Division, National Institute of Standards and Technology, Boulder, CO, (Online preprint quant-ph/9806012), (1998).

[Ued97] M. Ueda, Logical Reversibility and Physical Reversibility in Quantum Measurement, (Online preprint quant-ph/9709045), Int. Conf. on Frontiers in Quantum Physics, Kuala Lumpur, Malaysia, Springer-Verlag, (July, 1997).

[Unr95] W.G. Unruh. Maintaining coherence in quantum computers, Physical Review Letters A, 51:992-997, 1995.

[VBE96] V. Vedral, A. Barenco, A. Ekert, Quantum Networks for Elementary Arithmetic Operations, (Online preprint quant-ph/9511018), (1996).

[S48] K. Y. Szeto, *Data Compression of Quantum Code*, preprint quant-ph/9607010 (July 1996).

[VP98] V. Vedral, Martin B. Plenio, Basics of Quantum Computation, (Online preprint quant-ph/9802065), invited basic review article for Progress in Quantum Electronics, (1998).

[VM98a] D. Ventura, T. Martinez, Initializing the Amplitude Distribution of a Quantum State, (Online preprint quant-ph/9807054), (1998).

[VM98b] D. Ventura, T. Martinez, Quantum Associative Memory, (Online preprint quant-ph/9807053), (1998).

[VM98c] D. Ventura, T. Martinez, A Quantum Computational Learning Algorithm, (previously entitled "Quantum Harmonic Sieve: Learning DNF Using a Classical Example Oracle"), (Online preprint ph/9807052), (1998).

[VT98] D. Vitali, P. Tombesi, Decoherence Control for Optical Qubits, (Online preprint quant-ph/9802033), QCQC 98, (Feb. 1998).

[Vla98] A. Y. Vlasov, Analogue Quantum Computers for Data Analysis, FCR/IRH, St.-Petersburg, Russia, (Online preprint quant-ph/9802028), (1998).

[YV96] A. Yu. Vlasov, Quantum Computations and Images Recognition, (Online preprint quant-ph/9703010), QCM'96, Japan (September 1996).

[Wat95] J. Watrous. On one-dimensional quantum cellular automata. In 36th Annual Symposium on Foundations of Computer Science, pages 528-537, Milwaukee, Wisconsin, (October 1995). IEEE.

[War95] W.S. Warren. The usefulness if MNR quantum computing. Sience, 277: 1688-1689, (see also response by N. Gerenfeld and I. Chuang, ibid, pp 1689-90), (1997).

[WXM98a] H. Wei, X. Xue, S. D. Morgera, Single Molecule Magnetic Resonance and Quantum Computation, (Online preprint quant-ph/9807057), (1998).

[WXM98b] H. Wei, X. Xue, S. D. Morgera, NMR Quantum Automata in Doped Crystals, (Online preprint quant-ph/9805059), (1998).

[WXM97] H. Wei, X. Xue, S.D. Morgera, Trapping Quantum Coherence in Local Energy Minima, (Online preprint quant-ph/9707020), (1997).

[Wie96] S. Wiesner, Simulations of Many-Body Quantum Systems by a Quantum Computer, (Online preprint quant-ph/9603028), (1996).

[WC97] C.P. Williams and S.H. Clearwater, Explorations in Quantum Computing, Springer-Verlag, Yew York, (1997).

[WMI+98] D.J. Wineland, C. Monroe, W.M. Itano, D. Leibfried, B.E. King, D.M. Meekhof, Experimental issues in coherent quantum-state manipulation of trapped atomic ions, (Online preprint quant-ph/9710025), Journal of Research of the National Institute of Standards and Technology 03, pp 259 (1998).

[WMM+96] D. J. Wineland, C. Monroe, D. M. Meekhof, B. E. King, D. Leibfried, W. M. Itano, J. C. Bergquist, D.Berkeland, J. J. Bollinger, J. Miller, Quantum state manipulation of trapped atomic ions, (Online preprint quant-ph/9705022), Proc. Workshop on Quantum Computing, Santa Barbara, CA, (Dec. 1996), Submitted to Proc. Roy. Soc. A.

[WZ82] Wootters, W. K. and Zurek, W. H., A single quantum cannot be cloned. Nature 299, 802, (1982).

[XW97a] X. Xue, H. Wei, Superconductive Static Quantum Logic, (Online preprint quant-ph/9702041), (1997).

[XW97b] X. Xue, H. Wei, More on Static Quantum Computation, (Online preprint quant-ph/9702056), (1997).

[WX97c] H. Wei, X. Xue, Static Quantum Computation, (Online preprint quant-ph/9702046), (1997).

[Yao93] A. C.-C. Yao. Quantum circuit complexity, In Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, pages 352-361, Palo Alto, California, (Nov. 1993).

[Yao95] A. C.-C. Yao. Q Security of quantum protocols against coherent measurements. In Proceedings of the Twenty-Seventh Annual ACM Symposium on the Theory of Computing, pages 67-75, Las Vegas, Nevada, (May-June 1995).

[Zal96a] C. Zalka, Efficient Simulation of Quantum Systems by Quantum Computers, (Online preprint quant-ph/9603026), (1996).

[Zal96b] C. Zalka, Threshold Estimate for Fault Tolerant Quantum Computation, (Online preprint quant-ph/9612028), (1996).

[Zal97] C. Zalka, Grover's quantum searching algorithm is optimal, (Online preprint quant-ph/9711070), (1997).

[Zal98] C. Zalka, Fast versions of Shor's quantum factoring algorithm, (Online preprint quant-ph/9806084), (1998).

[Zur91] W. H. Zurek. Decoherence and the transition from quantum to classical, Physics Today, vol. 44, pp. 36–44, (1991).

[ZL96] W. H. Zurek, R. Laflamme, Quantum Logical Operations on Encoded Qubits, (Online preprint quant-ph/9605013), submitted to Physical Review Letters, (May 1996).

[ZR97] P. Zanard, M. Rasetti, Preserving Coherence in Quantum Computation by Pairing Quantum Bits, (Online preprint quant-ph/9710002), (1997).

[ZHS98] Zyczkowski, Horodecki, Sanpera, and Lewenstein, On the volume of the set of mixed entangled states, (Online preprint quant-ph/9804024), (1998).