Alternative Computational Models: A Comparison of Biomolecular and Quantum Computation

John H. Reif
Department of Computer Science
Duke University *

Abstract

Molecular Computation (MC) is massively parallel computation where data is stored and processed within objects of molecular size. *Biomolecular Computation (BMC)* is MC using biotechnology techniques, e.g. recombinant DNA operations. In contrast, *Quantum Computation (QC)* is a type of computation where unitary and measurement operations are executed on linear superpositions of basis states. Both BMC and QC may be executed at the micromolecular scale by a variety of methodologies and technologies. This paper surveys various methods for doing BMC and QC and discusses the considerable theoretical and practical advances in BMC and QC made in the last few years. We compare bounds on key resource such as time, volume (number of molecules times molecular density), energy and error rates achievable, taking particular note of the scalability of these methods with the size of the problem solved. In addition to NP search problems and database search problems, we enumerate a wide variety of further potential practical applications of BMC and QC.

We observe that certain problems (e.g., NP search problems), if solved with polynomial time bounds, requires exponentially large volume for BMC, so BMC does not scale well to solve very large NP search problems. However, we describe a number of applications (e.g., search within large data bases and simulation of parallel machines) where the volume grows polynomial.

Also, we note that the observation operation of QC, which is a fundamental operation of QC used for obtaining classical output, may potentially suffer from exponentially large volume requirements. Observation operations in quantum physics are generally done by a macroscopic measurement apparatus, and the original formulations of QC implicity assumed that macroscopic measurement apparatus would be used for QC. However, if the measurement apparatus is very small, it will be subject to quantum effects. At this time, no one has demonstrated or proved that the observation operation (for a quantum system with n entangled qubits) can even be approximated within a larger unitary quantum system in volume growing less than exponentially with n. Hence it is unknown whether QC (with the observation operation) scales to even moderate numbers of qubits within small volume. We pose a major open problem in QC: to determine (i.e., provide a formal proof) whether or not observation, in a closed quantum system, can be approximated in small volume: say, growing as a polynomial in the number of qubits.

We also discuss techniques for decreasing errors in BMC (e.g., annealing errors) and QC (e.g., decoherence errors), and volume where possible, to insure the scalability of BMC and QC to problems of large input size. In addition, we consider how BMC might be used to assist QC (e.g., to do observation operations for Bulk QC) and also how quantum techniques might be used to assist BMC (e.g., to do exquisite detection of very small quantities of a molecule in solution within a large volume).

*Surface address: Department of Computer Science, Duke University, Durham, NC 27708-0129. E-mail: reif@cs.duke.edu.
An extended abstract of this paper appeared in the 18th International Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS98), 102–121, (December, 1998). A postscript preprint of this paper is online at http://www.cs.duke.edu/∼ reif/paper/altcomp.ps . This work was supported in part by Grants NSF/DARPA CCR-9725021, CCR-96-33567, NSF IRI-9619647, ARO contract DAAH-04-96-1-0448, and ONR contract N00014-99-1-0406. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied of the Advanced Research Projects Agency, NSF, ONR or the U.S. government.

1 Introduction

Conventional silicon based methods for computation have made great strides in the later 20th century, both in miniaturization as well as the use of innovative architectures, e.g., parallel architectures. However, there may well be limitations to the size of components using silicon technology, due to manufacturing limitations (e.g., the wavelength used in lithography) or device limitations in the function of very small components.

1.0 Molecular Computation (MC). A molecule will be (somewhat arbitrarily) termed a *micromolecule* if it has at most 10^4 atoms, and otherwise a macromolecule. We may envision in the perhaps near future doing computation at an *ultra-scale*: that is submicroscopic and even micromolecular scale. In particular, we will define *MC* to be parallel computation, where data is stored and processed within micromolecule size objects. Some key resource bounds for MC are:

- *time* of computation (which if the computation is synchronous, this is the time duration of each operations times the number of steps of the computation),
- *volume* (which if the computing media is homogeneous, this is the the number of molecules (size) times molecular density), and
- *energy*.

Furthermore, we need to bound the errors of MC, to insure the computations are correct. A key issue is the *scalability* of MC methods: that is by how much do these resource metrics increase with the size of the problem solved? There is not just one way to do MC, and in fact there are a number of quite distinct alternative technologies which will be discussed in this paper.

1.1 Biomolecular Computation (BMC). A large number of biotechnology laboratory techniques, known collectively as *recombinant DNA operations*, have been developed for manipulating DNA and related techniques have been developed to manipulate RNA and certain other bio-molecules in sophisticated ways. One basic approach to MC, which will be termed *Biomolecular Computation (BMC)* is to apply such biotechnology operations to do computation. In this approach, data may be encoded within individual molecules, for example via DNA or RNA base coding. This data may be stored as vast numbers of DNA or RNA molecules in solution in a test tube or in solid support on a surface.

• **Distributed Molecular Parallelism.** In the *distributed molecular parallelism (DP-BMC)* paradigm for BMC, the operations of a computation are executed in parallel on a large number of distinct molecules in a distributed manner, using the massive parallelism inherent in BMC. Feynman [F 61] first proposed doing computation via distributed molecular parallelism, but his idea was not tested for a number of decades.

• **Initial Work in BMC.** Adleman was the first to actually do an experiment demonstrating BMC, solving a small NP search problem. NP search problems are considered intractable via conventional methods for macroscopic sequential and parallel computation. The *Hamiltonian path* problem is to find a path in a graph that visits each node exactly once. Adleman [A94] employed molecular parallelism in the solution of the Hamiltonian path problem, by forming a set of DNA strings encoding sequences of nodes of the graph and restricting the set of sequences to only Hamiltonian paths. The number of recombinant DNA operations grew linearly with the size of the input graph. In a lab experiment, he tested his techniques on DNA for a 7 node Hamiltonian path problem. As previously stated, This was the first major experimental milestone achieved in the field of BMC.

1.2 Quantum Computation (QC). Another basic approach to MC is to apply quantum mechanics to do computation. (In contrast, computations and methods not making use of quantum mechanics will be termed *classical*.) A single molecule (or collection of particles and/or atoms) may have a number n of degrees of freedom known as *qubits*. A *basis state* is associated with each fixed setting (to Boolean values) of the qubits. 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 $\alpha|a>$. A *unitary operation* is a reversible operation on the superpositions which can be represented by a unitary matrix 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 transformation. 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.

• **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.)
• **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.)
1.3 Organization of this Paper. In this Section 1 we have introduced BMC and QC. In Section 3 we discuss resource bounds for BMC and QC, including time, volume, and energy. In Section 2 we describe mathematical models and complexity bounds for BMC and QC. In Section 4 we discuss enabling technologies and experimental paradigms for doing BMC and QC. In Section 5 we discuss the type of errors encountered in BMC and QCC, and methods for decreasing errors. In Section 6 we discuss applications of BMC and QC. In Section 7 we discuss hybrids of BMC and QC, including as an example of an applications of QC to BMC as well as an example of an application of BMC to QC. In Section 8 we give a conclusion and acknowledgements for the paper.

2 Models and Complexity Bounds for BMC.

2.1 Models for BMC.
• **Splicing Models.** *Splicing* is a paradigm for BMC which provides a theoretical model of enzymatic systems operating on DNA. Splicing models a solution with enzymatic actions (restrictions and the ligations) operating on DNA in parallel in a common test tube. The DNA strands are modeled as strings over a finite alphabet. Splicing allows for the generation of new strings from an initially chosen set of strings, using a specified set of splicing operations. The splicing operations on the DNA are string editing operations such as cutting, appending, etc. These operations can be applied in any order, and thus the splicing system can be considered to be autonomously controlled. Also, the operations may be nondeterministic: a large number of possible results may be obtained from a small number of operations. Splicing predates all other BMC paradigms and it has its roots in formal language theory [H87] and Lindenmayer systems [H92]. Pioneering work on splicing was done by Head [H92]. There is now a rather extensive literature (including thirty or so papers) in splicing and related string rewrite systems, written by a dozen researchers, including Paun [P96a, P96b, P97] and Paun et al [CFKP96, HPP96, PRS96], Culik and Harju [CH89] Pixton[Pi95, Pi96, Pi97], [StM97], Yokomori and Kobayashi [YK97a, YK97b], Kim and Kyungpook [KK97]. All of these investigations were theoretical in nature, and established the computational power of splicing systems of various sorts. For example, [HPP96] provided solution of the characterization problem for splicing system H(Fin,Fin). A number of researchers, including Csuhaj-Varju, Freund, Kari, and Paun [CFKP96, Kar97A, FKP98], Rothemund [Ro95], and Smith and Schweitzer [SS95] independently proved that a universal Turing Machine can be simulated by recombinant DNA operations in splicing models. Also, Kari, Paun, Rozenberg, Salomaa, Yu proved that DNA sticker systems are universal [KPRS98]. Garzon and Jonoska, [GJ98] (also see Fu, Beigel [FB98]) characterize the complexity of splicing with strands of bounded length, to be PSPACE. Manca et al [ADL+98] give some further splicing models and Conrad [Con98] considers context free and context sensitive splicing methods. Margenstern and Rogozhin [MR98] consider time-varying splicing systems. Li [Li98]gives an algebraic characterization of certain splicing languages. Landweber and Kari [LK98] present a splicing model for the natural DNA editing and compression that occurs in certain protozoa. Surveys of DNA computing in the context of the splicing model are given by Kari [Kar98, Kar97B, Kar96] and Kari, Sakakibara [KarS97].

In summary, splicing provided the first theoretical studies of BMC and and has contributed to our understanding of the potential power of BMC. It has evolved to be a very active subfield of formal language theory. At this time, splicing is primarily a theoretical rather than an experimental area of BMC.

- **Models for Distributed Molecular Parallelism.**

– **Test Tube and Memory Models.** Lipton [L94] defined the first abstract model of BMC that takes into account distributed molecular parallelism. The elements of his *test tubes* are strings as in the case of DNA. His model allowed a number of operations on test tubes to be executed in one lab step. The subsequent *Memory* model of Adleman [A95] refined the model of Lipton by restricting the set of operations to the following:

Merge: Given tubes T_1, T_2, produce the union $T_1 \cup T_2$.

Copy: Given a tube T_1, produce a tube T_2 with the same contents.

Detect: Given a tube T, say 'yes' if T contains at least one element and say 'no' if it contains none.

Separation: Given a tube T_1 and a word w, produce a tube T_2 with all elements of T_1 that contain w.

– **A Surface-Based Model for BMC.** An abstract model of surface-based BMC computation has been developed by [LGCCL+96] (comparable with Lipton and Adelman's models), and it is shown that the surface-based model is also capable of general circuit simulation.

– **A Parallel Associative Memory Model for BMC.** This is a very high level model proposed by Reif [R95] which (i) allows any of the operations for the Memory model of Adleman to be executed in one step, and also (ii) has a Parallel Associative Matching (PA-Match) operation, which provides for the combination of all pairs of DNA strings with subsequences that have a complementary match at a specified location. This PA-Match operation is very similar to the data base join operation.

– **A Recombinant DNA Model for BMC.** Is a low level model for BMC proposed by Reif [R95] which allows operations that are abstractions of very well understood recombinant DNA operations and provides a graph representation, known as a *complex*, for the relevant structural properties of DNA. To insure realism, the RDNA model allows complementary pairing of only very short sequences of DNA in constant time. Reif [R95] showed that the PA-Match operation of the PAM model can be simulated in the RDNA model with a slow down which is linear in the pattern match length.

– **Other Models of BMC.** Yokomori and Kobayashi [YK97b] developed a model of BMC based on equality checking, which may be related to the PAM model. Kurtz, Mahaney, Royer, and Simon [KMRS96] formulated a model of BMC which takes into account solution concentrations.

– **Speed-Ups using Molecular Parallelism.** Beaver [BeA95] and Reif [R95] (also Papadimitriou [P95]) independently proved that any linear space bounded sequential computation can be exponentially speeded up by PMC; in particular, they showed that sequential Turing Machine computations with space s and time $2^{O(s)}$ can be simulated by BMC in polynomial time. All their proofs made use of a pointer jumping technique (this pointer jumping technique dates to the 1978 work of Fortune and Wyllie [FW 78], who gave a parallel simulation of a space bounded TM by a PRAM) which required a large volume to implement in BMC. The paper of [R95] proved this speed-up result for the (very high level) PAM model, and then [R95] described in detail its implementation by recombinant DNA operations in the RDNA model. The proof of [B95] used a DNA string-editing operation known as site-directed local mutagenesis (see [WGWZ92], page 192-193, [OP94], page 191-206, and Chapter 5 of [SFM89]) to implement pointer jumping. Khodor and Gifford [KG98] have recently implementated BMC methods using programmed mutagenesis.

– **Molecular PRAMs.** A Parallel Random Access Machine (PRAM) is a parallel machine with a large shared memory. It is CREW if its memory allows concurrent reads and exclusive writes. This same technique of pointer jumping is essential also for Reif's [R95] molecular simulation of a CREW PRAM. Given a CREW PRAM with time bound D, with M memory cells, and processor bound P, [R95] showed that the PRAM can be simulated in the PAM model using t PA-Match operations as well as $O(s \log s)$ PAM operations where $s = O(\log(PM))$ and $t = O(D + s)$. This result immediately implied that in $t = O(D + s)$ PAM steps, one can evaluate and find the satisfying inputs to a Boolean circuit constructable in s space with n inputs, unbounded fan-out, and depth D. Subsequently, Ogihara and Ray [OR97b] obtained a similar result as [R95] for parallel circuit evaluation, implicitly assuming a model similar to the PAM model. (Also see [HA97] for BMC methods for parallel evaluation of a Boolean μ-formulas.) To allow the PRAM to use shared global memory, we need to do massively parallel message (DNA strand) routing. As a consequence, the volume bounds for this simulation of a PRAM required volume growing at least quadratically with size of the storage of the PRAM. Gehani and Reif [GR98a] propose a MEMS micro-flow device technology that requires a substantial decreased volume to do the massively parallel message routing required for the shared memory operations of the PRAM.

2.2 Models and Complexity Bounds for QC.

• **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 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).

• **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.

• **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.

• **Quantum Parallel Complexity Classes.** Let NC (QNC, respectively) be the class of (quantum, respectively) circuits with polynomial size and polylogorithmic depth (that is, with depth $O(\log^{O(1)} n)$). 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.

• **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.

• **Quantum Logics and Algebraic Semantics.** Various logics have been developed for reasoning about quantum computations, Including logics using lattices Malhas [Mal94], and modal logics. Malinowski [Mal94] has considered a quantum logic and shown that it has no decision procedure. Havel [Hav98] gives a geometric algebra (with multiple particles) for expressing the operations of a Bulk QC.

• **Quantum Programming Languages and Their Compilers.** Malhas [May96] defines a quantum version of the lambda calculus (the lambda calculus is a formal programming system similar to lisp) and Malhas [May97] shows that it can efficiently simulate quantum computations. Tucci [Tuc 98] describes a procedure for compiling unitary quantum transformations into elementary 2-qubit gates.

3 Resource Bounds

In this paper, we discuss many applications of BMC and QC which provide advantages over classical methods of computation.

For these advantages to be practical, we need to determine that there are no unfeasible large resources required by BMC and QC. Here we review of the resource bounds of quantum computing as compared with the resources required by classical methods for computation.

The energy consumption, processing rate, and volume, are all important resources to consider in miniaturized and mobile computing devices, and in particular molecular scale computations. Conventional 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.

3.1 Resource Bounds for BMC

• **Energy Bounds for BMC.**

– **Energy Consumption and Reversible Computation.** *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]) 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.

Many recombinant DNA operations such as denaturing and annealing, are reversible, so they require arbitrarily small energy (they require heating or cooling, but this can be done using heat baths). Other recombinant DNA operations such as separation, do not seem to be reversible, and use approximately 10^{-19} Joules per operation.

• **Volume Bounds for BMC.** A small amount of water can contain a vast number of DNA molecules. A reasonable solution concentration to do recombinant DNA operations is 5 grams of DNA per one liter of water. Then a liter of water contains in solution about 10^{21} DNA bases. For an associative memory (see Baum [B95]) of this scale, we can provide a few bytes of memory per DNA strand, by use of at most 100 base pairs per DNA strand. Thus a liter of solution provides an associative memory with 10^{19} to 10^{20} bytes, which is 10^7 to 10^8 tera-bytes. It is important to note that the scale of the BMC approach is limited by the volume. Known BMC techniques can solve any NP search problem in time polynomial in the input size, but require volume which grows linearly with the combinatorial search space, and thus exponentially with the input size (However, some recent approaches (Hagiya and Arita [HA97] and Cukras et al [CFL+98]) to solving NP search problems via BMC have decreased the volume by iterative refinement of the search space).

• **Processing Rate Bounds for BMC.** The time duration of the recombinant DNA operations such as annealing, which depends on hybridization, is strongly dependent on the length of sequences to be matched and may also depend on temperature, pH, solution concentration, and possibly other parameters. These recombinant DNA and other biotechnology operations can take from a few seconds up to 100 minutes. A DNA strand may need $1,000$ base pairs to encode a processor state and so a liter of solution encodes the state of approximately 10^{18} distinct processors. Since a liter of water contains in solution about 10^{21} DNA bases, the overall potential for BMC using DNA is 10^{15} to 10^{16} operations per second in the liter of solution, which is $1,000$ tera-ops. While this number is very large, it is finite, so there is a finite constant upper limit to the enhanced power of MC using BMC within moderate volume. Nevertheless, the size of this constant is so large that it way well be advantageous in certain key applications, as compared to conventional (macroscopic) computation methods.

3.2 Resource Bounds for QC

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. 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.

• **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; techniques can execute unitary operations in microseconds (e.g., Bulk NMR) and some might execute at microsecond or even picosecond rates (e.g., photonic techniques for NMR) 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.** In this paper we consider (perhaps more closely than usual in the quantum literature due to our interest in MC) the volume bounds of QC. Potentially, the modest volume bounds of QC may be the one significant advantage over other methods for MC. (In contrast, BMC methods for solving an NP search problem requires volume growing linearly with the combinatorial search space, and thus exponentially with the input size.) 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.

– **QC Observation.** 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 (see below) 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. Some aspects of this issue might be purely philosophical and not affect experimental predictions; for example Everett's [Eve57] many-wolds interpretation of quantum mechanics (see a discussion of quantum state reduction by DeWitt [DW73] and Deutsch [Deu85] in connection to a many-wolds interpretation of quantum mechanics). In contrast, the aspects of quantum observation we discuss below will be concerned with its experimental predictions in the case of large scale QC.

– **Formulations.** Two distinct approaches to the mathematical and physical foundations of observation have been developed:

(a) The Copenhagen Formulation. In this formulation, the observation is simply *an assumed basic operation*. The observation is considered to be done by a macroscopic measuring device. The precise size or molecular volume of such a macroscopic measuring apparatus (say as a function of the number of qubits) is unclear. The assumptions of the Copenhagen formulation imply that you can make the measurements required for quantum computing on a set of n qubits by measuring each one individually, and that this can be done with n one-qubit measurement operations. However, this is only valid in the context of a macroscopic measuring device. The case of a macroscopic measuring device is reasonable in the context of most physics experiments that involve a large measurement device and which involve a very few number of degrees of freedom (qubits). However, this is not the case for a number of molecular scale

QC applications (e.g., factoring very large numbers) where the quantum computer (including its measuring device) is to be in a very small volume and the number of qubits might be in the hundreds or larger. Hence, in the molecular scale QC context, the Copenhagen formulation's assumption, that observation is simply a basic operation (and not related to a quantum unitary evolution), does not seem appropriate.

(b) The Von Neumann Formulation. The mathematical foundations of quantum mechanics as developed by von Neumann [Neu32] differ fundamentally from the Copenhagen formulation in the case of measurement. His formulation remains very well considered (for example note the recent reprint [Neu96]); see Cerf and Adami [CA98] for a comparison the Copenhagen and Von Neumann formulations. Von Neumann 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). An example of this difference is given in Hay and Peres [HP97]. The von Neumann formulation of observation is not relevant to the vast majority of physics experiments since (as pointed out above), their experiments generally use large measuring apparatus and small number of degrees of freedom (qubits). But it appears very relevant to molecular scale QC.

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. Since the vast majority of quantum physics experiments only use macroscopic measurement apparatus, it is not surprising that the Copenhagen formulation is the most generally used formulation. The original formulations of QC implicity assumed that macroscopic measurement apparatus would be used for QC; the Copenhagen formulation was certainly applicable to QC that employs macroscopic measurement apparatus. However, the Copenhagen formulation does to seem to be applicable in the context of a microscopic measurement apparatus, which is so small that it is subject to quantum effects (and thus is within a unitary quantum system); in that context the von Neumann formulation for observation seems to be required. Thus the Copenhagen formulation for observation is not appropriate for molecular size QC, whereas the von Neumann formulation for observation may be appropriate for molecular size QC. (Attempts to rectify the difference between the Copenhagen and the von Neumann formulation for observation are given in Hay and Peres [HP97] and in Zurek [Zur91], but it appears not yet resolved.)

– **Proposed Constructions Need Proofs:** Note that one might be tempted to give a constructive proof, that observation can be done on n qubits in small volume, along the following lines:

(i) *Basis Step.* We begin with a simple, well established experimental method for observation of a single qubit in small quantum system with say n_0 qubits, for a constant n_0. There are many other examples of experimentally verified methods for observation, using macroscopic measurement apparatus. (For example, a number of proposed QC architectures (e.g., the Cirac and Zoller [CZ95] proposed ion trap QC and Kane's [Kan98] silicon-based NMR QC) give specific descriptions of measuring apparatus that have been experimentally verified for observation of a single qubit within a quantum computing systems with a constant number of qubits. While their measuring apparatus is macroscopic, it still must have just some finite volume. However,

(ii) *Inductive Step.* Then we just scale up by using the same experimental apparatus to do observation on each of n qubits (that is, repeating the observation for each of the other qubits). This seems to result in a small volume (perhaps even liner size) apparatus for observation.

The potential fallacy of this line of argument is that:

(a) In the basis step, the experiments of [CZ95,Kan98] did not provide bounds on the errors (or fidelity) of the measurement as a function of the volume of the measuring apparatus.

(b) the inductive step fails to take into account quantum effects involving both the measuring apparatus and the n qubits, as might be predicted by the von Neumann formulation of quantum measurement in the case where the measuring apparatus is so small that it is subject to quantum effects.

That is, there needs to be given, in addition to the experimental description (which is only established for n_0 qubits):

(iii) *A mathematical analysis of the quantum effects (in the context of a closed unitary system) involving the measuring apparatus as the number n of qubits grows large.* In particular, there need to be determined bounds on the errors (or fidelity) of the measurement as a function of the size of the measuring apparatus.

Without this crucial final element, the proof is certainly not complete. Since the observation operation is not reversible, such a proof (in the context of a closed unitary system) seem unlikely to be obtainable.

– **Possible Experimental Demonstrations of Measurement:** Another approach would be to experimentally test a proposed small volume apparatus for observation on n qubits for moderate size n (say, in the rang of a few hundred, which is required for a nontrivial factoring computation). But the experimental evidence of the volume bounds for observation is unclear, since the QC experiments have not yet been scaled to large or even moderate numbers (say dozens) of qubits, and there are few if any physics experiments for this case. (Shnirman, Schoen [SS98] describe the use of a single-electron transistor to perform quantum measurements, D'Helon, Milburn [HM97] describe quantum measurements with quantum computers, and Ozawa [Oza98] describes methods for nondestructive quantum measurements of certain quantum computations.)

Hence, at this time that there appears to be *neither a mathematical proof nor an experimental demonstration* (for even a moderately large number of qubits n) *that observation can be done in small volume* (in a closed quantum system). Thus at this time, there is no evidence (either mathematical or experimental) that QC using measurement scales to large numbers of qubits with small volume.

We next consider (but do not fully determine): *Is it reasonable to expect that such a mathematical proof (or such experimental demonstrations) of small volume quantum observation will ever be done ?* We first consider a number of related questions concerning measurement and quantum state reduction:

– **Is a Quantum Observation Instantaneous?** It appears not. Brune et al [BHD96] describe the progressive decoherence of the meter in a quantum measurement.

– **Is an Observation Always Reversible?** It appears the answer be both no (in a narrow mathematical sense of a state reduction), yes (for small closed state spaces), and no (in a practical sense for entanglements in a large state space):

- By the strict mathematical definition of the state reduction due to observation, in general an observation is not reversible. Under what conditions is a measurement reversible in the strict mathematical sense? That is, when can we measure classical information from a quantum source (yielding a set of pure states with their probabilities with a reduction of quantum entropy), but later be able to reverse this process to regenerate the entangled source state ? Bennett et al [BBJ+94] show that this is possible in the very special case where the source states can be partitioned into two or more mutually orthogonal subsets. (Other necessary and sufficient conditions for measurements to be reversible have been proved in Bennett, et al [BBJ+94] and Chuang, Yamamoto [CY96] describe how to regenerate a qubit if it has observable error.)
- There is experimental evidence that the physical execution of some reductions via measurement are in fact reversible (at least in very small closed systems). Mabuchi, Zoller [MZ96] have observed inversions of quantum jumps in very small quantum-optical systems under continuous observation, and Ueda [Ued97] compares the notions of mathematical and physical reversibility.
- On the other hand, in the case of entanglements in a large state space, even if a measurement is in principle reversible in a closed system due the reversible nature of the diffusion process, the likelihood of such a reverse to the original state, within a moderate (say polynomial in n) time duration, appears to drop exponentially with the number of qubits n. Gottfield [Got66] Diosi, Lukacs [DL94] (also see Pearle [Pea84,Pea85]) explain quantum state vector reduction via strong measurement as a physical process, e.g, state diffusion into the atoms of the measurement apparatus. This diffusion due to reduction may be modeled by a system similar to a rapidly mixing markov system in probability theory, which seems to provide a very low (dropping exponentially with n) likelihood for reversibility within a polynomial time duration. (Others have modeled measurement by a nonlinear interactions with the environment, which are irreversible.)

– **Approximate Observation Operations.** An approach to this difficulty is to only do the observation operation approximately within accuracy ϵ; this may suffice for many QC applications. However, even if the observation operation is done ϵ-approximately by unitary operations, it appears to require a number of additional qubits n' growing exponentially with the n, the original number of qubits of the QC. In fact, we know of no upper bound on n' better than $2^n \log(1/\epsilon)$.

– **Why Volume Bounds May Not Be Small.** We now give an informal argument (it should be emphasized that the following is not a formal proof in any sense) that even an ϵ-approximate observation can not be done in polynomial time using small volume, where ϵ is the inverse of a polynomial. Since for n qubits, the size of the basis state space grows as 2^n in the general case, it seems reasonable to assume (e.g., where the physics of the strong measurement is modeled by a diffusion process [Got66,DL94] that is rapidly mixing) that the likelihood of reversibility within polynomial time bounds drops exponentially with the number n of qubits. Thus, in the context of polynomial time computations, the ϵ-approximate observation is assumed irreversible with high likelihood. Let us also assume that n is small (at most a few hundreds). For sake of contradiction, let us for the moment suppose that (i) quantum computing scales to at least moderate size (say a few tens of thousands of qubits), and (ii) an ϵ-approximate observation operation can be done on one of n qubits by a microscopic measuring device of size $n' = n^c$, for a constant c, and operating within time polynomial in n. Since n is small, the measuring device is surely of sufficiently small size so that it's physics is consistent with established quantum physics (for observe that if quantum computing is to scale to at least moderate size n', then surely quantum effects need to hold for molecules of size n'). Hence we need to view the apparatus for the observation as executing polynomial time unitary quantum computation, which is reversible, so the reverse of the observation also executes in quantum polynomial time. Hence we have an apparent contradiction, since we have assumed the ϵ-approximate observation is not reversible in polynomial time. (Note. This argument does not require that the world shift at some definite size from a quantum-mechanical paradigm to a classical paradigm; instead the argument requires that if the quantum-mechanical paradigm is valid at size n then it also is valid at some what larger size $n' = n^c$.)

Due to informal nature of this argument, it only provides partial evidence that (with the above assumption), QC with the observation operation does not scale to a large number of qubits within small volumes, and in particular that a polynomial time ϵ-approximate observation operation requires very large volume and can not be done at the micromolecular scale for moderate large n. It remains a major open problem in QC to *provide a formal proof that either there is large volume required for observation or there is not.*

– **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.

4 Technologies and Paradigms

4.1 Enabling Technologies and Experimental Paradigms for BMC. An *enabling technology* is a technology that allows a task to be done. Here we discuss various alternative enabling technologies for BMC and QC, and discuss their experiment in BMC and QC using these technologies.

• **Recombinant DNA Technology.** In the last two decades, there have been revolutionary advances in the field of biotechnology. Biotechnology has developed a large set of procedures for modifying DNA, known collectively known as *recombinant DNA*. DNA is a molecule consisting of a linear sequence of nucleotides. There are 4 types of nucleotides, which are complementary in pairs. A key property of DNA is *Watson-Crick complementation*, which allows the binding of complementary nucleotides. DNA may be single stranded (ssDNA) or double stranded. An ssDNA has an orientation $3' - 8'$ or $5' - 3'$. If two ssDNA are Watson-Crick complementary and $3' - 8'$ and $5' - 3'$ oriented in opposite directions, they are said to be *sticky.* At the appropriate conditions (determined by temperature and salinity, etc.), they may hybridize into double-stranded DNA. This resulting double-stranded DNA has complementary strands in opposite orientation. This allows the *annealing* of large strands of single DNA into double DNA, and the formation of complex 3D structures (this is known as *secondary structure*). The reverse process (usually induced by heating) is the *denature* of complex structures into single stranded linear structures. See [MH87, PP97, W97, RDGS97, HG97] for mathematical models of DNA hybridization and their simulation via thermodynamics. Short strands of ssDNA of length n are sometimes called *n-mers*. Many recombinant DNA operations use hybridization and are specific to a DNA segment with a prescribed n-mer subsequence. Such recombinant DNA operations include *cleavage* of DNA strands, *separation* of DNA strands, *detection* of DNA strands, and *fluorescent tagging* of specific DNA words. In addition, there are operations that are not specific, including *ligation* of DNA segments to form covalent bonds that join the DNA strands together, *merging* of test tube contents, the denature operation discussed above, and separation by molecular weight. Basic principles of recombinant DNA technology are described in [WGWZ92] [WHR87, OP94]. Detailed theoretical discussions of dynamics, thermodynamics, and structure of DNA, RNA and certain proteins are given by [BKP90, S94, EC]. Also see [ER82, MH87] for the dynamics and chemistry of nucleic acids and enzymes.

Due to the industrialization of the biotechnology field, laboratory techniques for recombinant DNA and RNA manipulation are becoming highly standardized, with well written lab manuals (e.g. [SFM89]) detailing the elementary lab steps required for recombinant DNA operations. Many of those recombinant DNA operations which where once considered highly sophisticated are now routine, and many have been automated by robotic systems. As a further byproduct of the industrialization of the biotechnology field, many of the constraints (such as timing, pH, and solution concentration, contamination etc.) critical to the successful execution of recombinant DNA techniques for conventional biological and medical applications (but not necessarily for all BMC applications), are now quite well understood, both theoretically and in practice.

• **Alternative Recombinant DNA Methodologies.** The most pervasive enabling biotechnology for BMC is solution-based recombinant DNA, that is the recombinant DNA operations are done on test tubes with DNA in solution. However, there are a number of alternative enabling biotechnologies, that allow similar and sometimes enhanced capabilities.

– **Solid Support BMC.** An example of an alternative recombinant DNA methodology is the *solid support* of individual DNA, for example by *surface attachments*. In solid support, the DNA strands are affixed to supports of some sort. In surface-based chemistry, surface attachments are used to affix DNA strands to organic compounds on the surface of a container. This can allow for more control of recombinant DNA operations, since this insures (i) that distinct DNA strands so immobilized can not interact, and also (ii) allows reagents and complementary DNA to have easy access to the DNA, and (iii) allows for easy removal of reagents and secondary by-products. Also, handling of samples is simpler and more readily automated. Surface-based chemistry has been used in protein sequencing, DNA synthesis, and peptide synthesis [S88]. Surface attachment methods can also be used for optical read-out (e.g., via fluorescent tagging of specific DNA words) on 2D arrays. A possible drawback of surface attachment technology, in comparison to solution-based recombinant DNA techniques, is a reduction on the total number of DNA strands that can be used.

– **Automation and Miniaturization of BMC.** MEMS is the technology of miniature actuators, valves, pumps, sensors and other such mechanisms, and when controlling fluids it is known as *MEMS micro-flow device technology*. [EE92, VSJMWR92, MEBH92]. Some of the current limits of BMC stem from the labor intensive nature of the laboratory work, the error rates, and the large volumes needed for certain bio-molecular reactions to occur (e.g., for searching and associative matching in wet data bases). [GR98a] (also see Ikuta [Iku96], Suyama [Suy98] for use of micro-flow devices for various biological applications) propose the use of MEMS micro-flow device technology for BMC which may provide several advantages: it would allow automation of the laboratory work, parallel execution of the steps of a BMC algorithm (for improved speed and reliability), and for transport of fluids and DNA among multiple micro-test tubes. [GR98a] provide a model for micro-flow based bio-molecular computation (MF-BMC) which uses abstractions of both the recombinant DNA (RDNA) technology as well as of the micro-flow technology, and takes into account both of their limitations (e.g., concentration limitations for reactants in RDNA, and the geometric limitations of the MEMS device fabrication technology). [GR98a] also give a time and volume efficient MF-BMC architecture for routing DNA strands among multiple micro-test tubes (this gives a substantial decrease in the volume required for the PRAM simulation of [R95]).

• **Experimental Paradigms for BMC.** Even within BMC, there are a number of distinct methods to do computation:
(A) Splicing, which provides a (theoretical) model of enzymatic systems operating on DNA,
(B) Distributed Molecular Parallelism, where a operations are done on a large number of molecules in parallel, and the operations execute within a molecule in a sequential fashion (either synchronously or asynchronous with other

molecules),
(C) Local Molecular Parallelism, where operations are done within each molecule in a parallel fashion, and does computation by assembly of DNA tiles, and
(D) Cellular Processing, where BMC is done using a microorganism such as bacteria to do computation, by re-engineering the regulatory feedback systems used in cellular metabolism.

We now consider the experimental demonstration of each of these paradigms for BMC.

(A) Splicing. At this time, splicing is primarily a theoretical rather than an experimental area of BMC. There are a number of practical issues (e.g., the number of distinct enzymes with distinct recognition sequences for DNA splicing operations are limited to at most a few hundred) that may limit the scale of experimental implementations of splicing, but it is quite possible that evolutionary techniques (using RNA enzymes) may be used to solve such difficulties. Recently an experimental test of splicing was done by Laun and Reddy [LR97], which provided a laboratory demonstration of splicing, testing a system with enzymatic actions (restrictions and the ligations) operating on DNA in parallel in a test tube.

(B) The Distributed Molecular Parallelism Paradigm. In this paradigm for BMC, the operations are executed in parallel on a large number of distinct molecules in a distributed manner, using the massive parallelism inherent in BMC.

• **NP Search using DP-BMC.** As mentioned in the introduction, Adleman [A94] did the first experiment demonstrating BMC, solving the Hamiltonian path problem on 7 nodes. This and many other BMC experiments have used distributed molecular parallelism to solve small NP search problems (see a discussion of NP search experiments in Section 6).

• **General-purpose Molecular Computers using DP-BMC.** BMC machines using molecular parallelism and providing large memories, are being constructed at Wisconsin [LGCCL+96], [CCCFF+97, LTCSC97] and USC [A95, RWBCG+96, ARRW96]. In both projects, a large number of DNA strands are used, where each DNA strand stores multiple memory words. Both these machines will be capable of performing, in parallel, certain classes of simple operations on words within the DNA molecules used as memory. Both projects developed error-resistant word designs. Successful prototyping at moderate scale of either of these machines will be a major experimental milestone in BMC.

The Wisconsin project is employing a surface to immobilize the DNA strands which correspond to the solution space of a NP search problem. Since they are all on the same surface, all DNA strands are operated in a Single Instruction Multiple Data (SIMD) fashion. Their operations on words are restricted to mark, unmark, and destroy operations, which suffice for certain NP search problems. A key challenge in their approach is to provide scaling to a sufficiently large number of DNA strands within the constraints of surface attachment technology.

In contrast, the USC project uses a combination of solution-based and solid support methods, which are used to improve the efficiency of the separation operations. In this method, the computation is done without formation and breaking of covalent bonds. Their operations on words include the Boolean logic operations. All DNA strands within a given test tube are operated on in a SIMD fashion. However, their approach allows splitting of the solution space into separate test tubes, and thus potentially allows for DNA strands to be operated on in a very limited Multiple Instruction Multiple Data (MIMD) fashion, where the number of distinct instructions executed at the same time is limited to the number of test tubes used in parallel. A key challenge in their approach, and the major focus of their effort, is to provide for efficient error-resistant separations.

• **Parallel Arithmetic.** To compete with silicon, it is important to develop the capability of BMC to quickly execute basic operations, such as arithmetic and Boolean operations, that are executed in single steps by conventional machines. Furthermore, these basic operations should be executable in massively parallel fashion (that is, executed on multiple inputs in parallel).

Guarnieri and Bancroft [GB96] developed a DNA-based addition algorithm employing successive primer extension reactions to implement the carries and the Boolean logic required in binary addition (similar methods can be used for subtraction). Guarnieri, Fliss, and Bancroft prototyped [GFB96] the first BMC addition operations (on single bits) in recombinant DNA. This experimental work was very significant. However, it suffered from some limitations: (i) only two numbers where added, so it did not take advantage of the massive parallel processing capabilities of BMC and (ii) the outputs were encoded distinctly from the inputs, so it did not allow for repeated operations. Subsequent proposed methods [OGB97, LKSR97, GPZ97, RKL98] for basic operations such as arithmetic (addition and subtraction) permit chaining of the output of these operations into the inputs to further operations, and to allow operations to be executed in massive parallel fashion. Rubin el al [RKL98] gave an experimental demonstration of a BMC method for chained integer arithmetic. This work also gave one of the first demonstrations in BMC of logically reversible computation. An experimental demonstration of such a method for parallel arithmetic, at large scale, will be a major experimental milestone in BMC. (See also the last subsection of Section 4 for fast local assembly methods for parallel addition and subtraction.)

(C) The Local Assembly Paradigm. The *local parallelism (LP-BMC)* paradigm for BMC allows operations to be executed in parallel on a given molecule (in contrast to the parallelism where operations are executed in parallel on a large number of distinct molecules but execute sequentially within any given molecule). Before we describe these local assembly techniques, we first discuss DNA nano-assembly techniques, and some previously known tiling results, which provided the intellectual foundations for local assembly.

• **DNA Nano-Fabrication Techniques.** Feynman [F 61] proposed nano-fabrication of structures of molecular size. Nanotechnology, without use of DNA, is discussed in the texts [CL92, M93]. Nano-fabrication of structures in DNA was pioneered by Seeman (e.g., see [SZC94]) in the 1990s. His work may well be of central importance to the progress of the emerging field of BMC. Seeman and his students such as Chen and Wang nano-fabricated in DNA (see [ZS92, ZS94, SWLQ+96, SQLYL+96, SZDC95] and [SZC94, SC91, SZDWM+94, SQLYL+96]): $2D$ *polygons,* including interlinked squares, and $3D$ *polyhedra,* including a cube and a truncated octahedron. Seeman's ingenious constructions used for basic constructive components:

– *DNA junctions:* i.e., immobile and partially mobile DNA n-armed branched junctions [SCK89],
– *DNA knots:* i.e., ssDNA knots [MDS91, DS92] and Borromean rings[MS97],
– *DNA crossover molecules:* i.e., DX molecules of Fu and Seeman[FS93].

Many of Seeman's constructions used DX molecules for rigidity or dsDNA for partial rigidity. Most of the constructions utilized hybridization in solution, usually followed by ligation. The octahedron used solid-support [S88], to avoid interaction between constructed molecules [ZS92]. See [CRFCC+96, MLMS96] for other work in DNA nano-structures. Recently, Seeman, Liu et al [SMY+98] constructed from DNA a nanomechanical device capable of controlled movement.

• **Known Tiling Results.** A class of *(domino) tiling problems* were defined by Wang [W61] as follows: we are given a finite set of tiles of unit size square tiles each with top and bottom sides labeled with symbols over a finite alphabet. These labels will be called *pads*. We also specify the initial placement of a specified subset of these tiles, and the borders of the region where tiles must be placed defining the *extent of tiling*. The problem is to place the tiles, chosen with replacement, in all these square regions within the specified borders, so that each pair of vertical abutting tiles have identical symbols on their contacting sides. Let the *size* of the tiling assembly be the number of tiles placed. Berger [B66] (also see Buchi [B62]) proved that given a finite set of tile types, the tiling problem is undecidable if the extent of tiling is infinite. Direct simulations of a single tape deterministic Turing Machines are given in [R71] and [LP81], (pages 296–300). Also, [GJP77] (see [GJ79], page 257) and [LP81](pages 345–348) proved that the domino tiling problem is NP-complete if the extent of tiling is a rectangle of polynomial size. Grunbaum, Branko, and Shepard [GBS87] surveyed these and related results on the complexity of tiling.

• **Computation via Local Assembly.** Winfree [W96] proposed a very intriguing idea: to do these tiling constructions by application of the DNA nano-fabrication techniques of Seeman et al [SZC94], which may be used for the construction of small DNA molecules that can function as square tiles with pads on the sides. The pads are ssDNA. Recall that if two ssDNA are sticky (i.e., Watson-Crick complementary and $3' - 8'$ and $5' - 3'$ oriented in opposite directions), they may hybridize together at the appropriate conditions into doubly stranded DNA. The assembly of the tiles is due to this hybridization of pairs of matching sticky pads on the sides of the tiles. We will call this innovative paradigm for BMC *unmediated self-assembly* since the computations advance with no intervention by any controllers. The advantages of the unmediated DNA assembly idea of Winfree is potentially very significant for BMC since the computations advance with no intervention by any controllers, and require no thermal cycling. It is a considerable paradigm shift from distributed molecular parallelism, which requires the recombinant DNA steps (which implement the molecular parallelism) to be done in sequence. To simulate a $1D$ parallel automata or a one tape Turing Machine, Winfree et al [W96, WYS96] proposed self-assembly of $2D$ arrays of DNA molecules, applying the recombinant DNA nano-fabrication techniques of Seeman et al [SZC94] in combination with the tiling techniques of Berger [B66]. Winfree et al [WYS96] then provided further elaboration of this idea to solve a variety of computational problems using unmediated DNA self-assembly. For example, they propose the use of these unmediated DNA assembly techniques to directly solve the NP-complete directed Hamiltonian path problem, using a construction similar to the NP-completeness proof of [GJP77] (see also [GJ79], page 257) for tiling of polynomial size extent. Winfree et al [WYS96] also provided a valuable experimental test validating the preferential pairing of matching DNA tiles over partially non-matching DNA tiles. Winfree [Win98a] made computer simulations of computing by self-assembly of DNA tiles, with a detailed simulation model of the kenetics of annealing during the self assembly of DNA tiles.

Erik Winfree, et al [WLW+98] recently experimentally constructed the first large (involving thousands of individual times) two dimensional arrays of DNA crystals by self-assembly of nearly identical DNA tiles. The tiles consisted of two double-crossovers (DX) which self-assemble into a periodic 2D lattice. They produced spectacular atomic force microscope(AFM) images of these tilings (by insertion of a hairpin sequence into one of the tiles they created 25 nm stripes in the lattice). They also verified the assembly by the use of "reporter" ssDNA sequences. This experiment provided strong evidence of the feasibility of large scaling self-assembly, but it was not in itself computational. LaBean, et al [LYR+98] recently designed and experimentally tested in the lab a new DNA tile (TAO35) which is a rectangular shaped triple crossover molecule with sticky ends on each side that can match with other such tiles and with a "reporter" ssDNA sequence that runs through the tile from lower left to upper right, facilitating output of the tiling computation.

Future major milestones will be to experimentally demonstrate: (i) DNA self-assembly for a (non-trivial) computation, and (ii) DNA self-assembly of a (possibly non-computational) 3D tiling.

• **Assemblies of Small Size and Depth.** To increase the likelihood of success of assembly, Reif [R97] proposed a *step-wise assembly* which provides control of the assembly in distinct steps. The total number of steps is bound by the depth of the assembly. Also, [R97] proposed the use of *frames*, which are rigid DNA nano-structures used to constrain the geometry of the assembly and to allow for the placement of input DNA strands on the boundaries of the tiling assembly. Using these assembly techniques, [R97] proposed LP-BMC methods to solve a number of fundamental problems that form the basis for the design of many parallel algorithms, for these decreased the size of the assembly to linear in the input size and and significantly decreased the number of time steps. For example, the *prefix computation problem* is the problem of applying an associative operation to all prefixes of a sequence of n inputs, and can be used to solve arithmetic problems such as integer addition, subtraction, multiplication by a constant number, finite state automata simulation, and to fingerprint (hash) a string. [R97] gave step-wise assembly algorithms, with linear assembly size and logarithmic time, for the prefix computation problem. As another example, *normal parallel algorithms* [S71, U84, L92] are a large class of parallel algorithms that can be executed in logarithmic time on shuffle-exchange networks (for example DFT, bitonic merge, and an arbitrary fixed permutation of n data elements in logarithmic time). [R97] gave LP-BMC methods for perfect shuffle and pair-wise exchange using a linear size assembly and constant assembly depth, and thus constant time. This allows one to execute normal parallel algorithms using LP-BMC in logarithmic time. Also, this implies a method for parallel evaluation of a bounded degree Boolean circuit in time bounded by the circuit depth times a logarithmic factor. Previously, such operations had been implemented using DP-BMC techniques [R95] in similar time bounds but required a large amount of volume; in contrast the LP-BMC methods of [R97] require very modest volume. All of these LP-BMC algorithms of [R97] can also use DP-BMC to simultaneously solve multiple problems with distinct inputs (e.g. do parallel arithmetic on multiple inputs, or determine satisfying inputs of a circuit), so they are an enhancement of the power of DP-BMC. Jonoska et al [JKS98] describes techniques for solving the Hamiltonian path problem by self assembly of single strand DNA into three dimensional DNA structures representing a Hamiltonian path.

(D) The Cellular Processor Paradigm. BMC may make use of microorganisms such as bacteria to do computation. A *cellular processor* is a microorganism such as a bacteria, which does computation via a re-engineered regulatory feedback system for cellular metabolism. The re-engineering involves the insertion of modified regulatory genes. whose DNA has been modified and engineered so that the cell can compute using regulatory feedback systems used in cellular metabolism. This paradigm for BMC was first discussed in a science fiction article of Bear [Bea83]. The recent papers Ji [Ji98] and Kazic [Kaz98] discuss models for doing BMC using cellular processors. Knight and Sussman [KS97] gave a design for logic gates using cellular processing and are planning an experimental demonstration of a cellular processor.

Alternative Paradigms for BMC. There may well be further alternative paradigms for BMC. For example, Landweber [La96] proposes the use of RNA rather than DNA as the basis of the biotechnology.

4.2 Enabling Technologies and Experimental Paradigms for QC. As noted above, 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 NMR 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: 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 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. (Later we suggest an interesting BMC technique for doing observations (with quantum state reduction) for Bulk QC.) However, known quantum algorithms can still be executed even in this case (e.g., see Gershenfeld, Chuang [GC97, GC98]). So the lack of strong measurement is not a major disadvantage.

Another disadvantage of Bulk QC is that it appears to require, for a variety of reasons, macroscopic volumes, and in particular volumes which grow exponential with the number of qubits. Macroscopic volumes appear to 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) NMR is actually a quantum phenomenon with quantum superposition of basis states, or (b) if NMR 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.)

In summary, some possible disadvantages of Bulk QC that may make it difficulty to scale are (i) the inability to do observation (strong measurement with quantum state reduction), (ii) the difficulty to do even a weak measurement without the use of exponential volume, (iii) difficulty (possibly now resolved) to obtain pure initial states without the use of exponential volume, (iv) the possibility that Bulk QC is not a quantum phenomena at all (an unresolved controversy within physics), and so may require use of exponential volume.

It is interesting to consider whether NNR can be scaled down from the macroscopic to molecular level. DiVincenzo [DiV97b] Wei et al [WXM98a, WXM98b] propose doing QC using the nuclear spins of atoms or electrons in a single trapped molecule. The main advantages are (i) small volume and (ii) the long time duration until decoherence (an advantage shared with NMR). The key difficulty of this approach is the measurement of the state of each spin, which does not appear to be feasible by the mechanical techniques for detection of magnetic resonance usual used in NMR, which can only do detection of the spin for large ensembles of atoms.

5 Correcting Errors

5.1 Correcting Errors in BMC. BMC has certain requirements not met by conventional recombinant DNA technology. Various methods have been developed which improve conventional recombinant DNA to obtain high yields and to allow for repeatability of operations. Also, analytic and simulation models of key recombinant DNA operations are being developed.

• **Efficient Error-resistant Separations.** Separation operations involve the isolation of all DNA with particular n-mer subsequences. Certain BMC methods require separation operations with high efficiency and high specificity. Approaches to solve this problem include the use of solid support, and most importantly the careful design of the n-mers used in separations. See Chen and Wood [CW97] and Deputat, Hajduczok, and Schmitt [KG97] for DNA separation techniques which may provide low error rates. Also see Boneh and Lipton [BL95a], Amos, Gibbons, and Hodgson [AGH96] and Deputat, Hajduczok, and Schmitt [DHS97] for methods that make BMC error resistant.

• **Ligation Errors.** Yoshinobu et al [YAT+98] describe models for ligation errors and propose methods for compensating for them in BMC.

• **Word Design for BMC** is the problem of designing of a library of short n-mer sequences (DNA words) for information storage. Word design is crucial to error control in BMC. Ideally, a good word design will minimize unwanted secondary structure, and minimize mismatching, by maximizing binding specificity. Note that there are conflicting requirements on word design for BMC: as strand length decreases (which is desirable), the Hamming distance between distinct words of information decreases (which is not desirable). Adleman [A94] and Lipton [L94] first suggested the use of random strings for word design, noting that DNA strings are non-degenerate with high likelihood. Evolutionary search methods for word designs are described in [DMRGF+97]. Other word designs for BMC are described in [B96, DMGFS96, M96, GDNMF97]. Laboratory experiments of word designs are described in Libchaber [KCL96] and ligation experiments are described by Jonoska and Karl [JK97a]. Related issues in DNA computer system design have been addressed in [A96] by Amenyo. Word designs for surface-based chemistry is considered in [GFBCL+96] and in [FTCSC97], which provides a four-base mismatch word design. [CRFCC+96] shows that surface morphology may be an important factor for discrimination of mismatched DNA sequences. Wood [Woo98] considers the use of error correcting codes for word design and to decrease errors in BMC. Hartemink et al [HGL98] describes an automated constraint-based procedure for nucleotide sequence selection for BMC.

5.2 Correcting Errors in QC.

• **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.

• **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.

• **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.)

5.3 Quantum Compression 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 [Rei98a] 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 [Rei98a] employed a modified coding that was still asymptotically optimal in fidelity and size.

6 Applications

6.1 Applications of BMC.

There are a wide variety of problems (up to moderate sizes) that may benefit from the massive parallelism and nano-scale miniaturization available to BMC.

• **NP search problems.** These are a class of computational problems apparently requiring a large combinatorial search for their solution, but requiring modest work to verify a correct solution. NP search problems may be solved by BMC by (i) assembling a large number of potential solutions to the search problem, where each potential solution is

encoded on a distinct strand of DNA, and (ii) then performing recombinant DNA operations which separate out the correct solutions of the problem. DP-BMC has been proposed for the following NP search problems:
(*i*) **Hamiltonian path.** In additon to Adleman [A94], see [G94, KTL97] and Fu et al [FBZ98] for improvements to Adleman's [A94] Hamiltonian path BMC experiment, and see [MoS97] for related methods.
(*ii*) **SAT** is the problem of finding variable assignments that satisfy a Boolean formula. Lipton [L94] proposed use of DP-BMC for finding satisfying inputs to a Boolean expression, and this approach was generalized in [BDLS95] to solve the SAT problem. Also Eng [Eng98] proposed in vivo BMC methods for SAT.
(*iii*) **Graph coloring** (Jonoska and Karl [JK96]).
(*iv*) **Shortest common superstring problem** (Gloor et al [GKG+98]).
(*v*) **Integer factorization** (Beaver [Be94]).
(*vi*) **Breaking the DES cryptosystem** ([BDL95] and [ARRW96]).
(*vii*) **Protein conformation** (Conrad and Zauner [CZ97]).
– **Surface-Based NP search.** Eng, and Serridge [ES97] give a surface-based DP-BMC algorithm for minimal set cover. Wang [WQF+98] describe the experimental execution, within surface based BMC, of the operations: DESTROY and READOUT DNA computing operations: DESTROY and READOUT using a one word approach to solve a satisfiability problem. Liu et al [LFW+98] give an experimental demonstration of surface based BMC using a one word approach to solve a SAT problem.

Eng [Eng98] proposes in vivo BMC methods for the NP complete problem of satisfiability of Boolean formula in 3CNF form.
– **NP search using RNA.** Recently Cukras, Faulhammer, Lipton, and Landweber [CFL+98] gave an impressive experimental demonstration of a BMC method for the solution of a class of SAT problems (derived from the knights problem in Chess), that appears likely to scale to at least moderate number of Boolean variables (say 18 to 24). Their method was also significant due to their use of RNA rather than DNA and their development of a powerful evolutionary method for doing the combinatorial search to optimize their DNA word codes.
– **Whiplash PCR** (Hagiya and Arita [HA97]) Is a DP-BMC method that uses the end segments of DNA strands to do editing and processing within the interior of the strand. Hagiya and Arita [HA97] showed that Whiplash PCR can be used for SAT problems for a class of Boolean formulas known as μ-formulas, and Winfree [Win98b] extended these techniques to solve general SAT problems. Sakamoto et al [SKK+98] describe how to do finite state transitions using Whiplash PCR, using a graduated scale of melting temperatures to reduce the number of laboratory steps, and also describes implementations of these methods.
– **Decreasing the Volume Used in NP search.** In all these methods, the number of steps grows as a polynomial function of the size of the input, but the volume grows exponentially with the input. For exact solutions of NP complete problems, we may benefit from a more general type of computation than simply brute force search. The molecular computation needs to be general enough to implement sophisticated heuristics, which may result in a smaller search space and volume. For example, Ogihara and Ray [OR97a] proposed a DP-BMC method for decreasing the volume (providing a smaller constant base of the exponential growth rate) required to solve the SAT problem. The difficulty with many of these approaches for NP search is that they initially generate a very large volume containing all possible solutions. An alternative heuristic approach of iteratively refining the solution space. to solve NP search problems has been suggested by Hagiya and Arita [HA97] and Cukras et al [CFL+98], and may in practice give a significant decrease in the volume.
• **Combinatorial Chemistry as NP Searches.** *Combinatorial chemistry* techniques (also known as *diversity* techniques) have been used by biochemists to do combinatorial searches for biological objects with special properties. These techniques were very similar to the use of massive parallelism in BMC to solve NP search problems. Generally, they use recombinant DNA techniques to first construct a large pool of random sequences and then choose elements with specific properties from within the pool. For example, in a widely cited paper, Alper [Al94] discusses the use of diversity techniques for drug discovery. Also, Bartel and Szostak [BS91] constructed a large pool of random sequences and then isolated new ribozymes. Also, Eigen and Rigler [ER94] developed techniques for sorting molecules by closeness metrics. The disciplines of combinatorial chemistry and BMC may benefit by combining some of their techniques. For example, the search space of combinatorial chemistry might be decreased by sophisticated heuristics used in NP search methods.
• **Huge Associative Memories.** BMC has the potential to provide huge memories. Each individual strand of DNA can encode binary information. A small volume can contain a vast number of molecules. As we have discussed in

Section 3, DNA in weak solution in one liter of water can encode 10^7 to 10^8 tera-bytes, and we can perform massively parallel associative searches on these memories. Baum [B95] (also see Lipton [L96]) proposed a parallel memory where DNA strands are used to store memory words, and provided a method for doing associative memory searches using complementary matching. Lipton [Lip98] describes the use of web data bases and associative search within them to do cryptoanalysis.

This idea for associative memory can be extended to allow us to execute operations in parallel, that is to do concurrent word searches. From this follows the concept of a data base molecular computer using DP-BMC. The time and volume efficiency of associative memory searches can be improved by the use of MEMS micro-flow device technology (Gehani and Reif [GR98a]) to segragate pools (micro-Test Tubes) of DNA strands to be searched, and to apply the searches in parallel for each pool.

• **Massively Parallel Machines.** BMC also has the potential to supply massive computational power. BMC can be used as a parallel machine where each processor's state is encoded by a DNA strand. BMC can perform massively parallel computations by executing recombinant DNA operations that act on all the DNA molecules at the same time. These recombinant DNA operations may be performed to execute massively parallel local memory read/write, logical operations and also further basic operations on words such as parallel arithmetic. As we have discussed in Section 3, DNA in weak solution in one liter of water can encode the state of about 10^{18} processors, and since certain recombinant DNA operations can take many minutes, the overall potential for a massively parallel BMC machines is about $1,000$ tera-ops. (This assumes the parallel machine uses local rather than global shared memory. To allow such a parallel machine to use global shared memory, we need to do massively parallel message (DNA strand) routing. As observed in Section 2, Reif's [R95] BMC simulation of a PRAM with shared memory required volume growing at least quadratically with size of the storage of the PRAM, but Gehani and Reif [GR98a] describe a MEMS micro-flow device technology that can do the massively parallel message routing with a substantial decrease in the volume.)

• **Other Algorithmic Applications of DP-BMC.** DP-BMC may also be used to speed up computations that would require polynomial time on conventional machines: Beigel and Fu [BF97] discuss approximation algorithm for NP search problems, Baum and Boneh discuss DP-BMC methods for executing dynamic programming algorithms, and Oliver [O96] discusses DP-BMC methods for matrix multiplication.

• **Neural Network Learning and Image Recognition.** Mills, Yurke, and Platzman [MYP98] propose a rather innovative BMC system for error-tolerant learning in a neural network, which is intended to be used for associative matching of images. They use a DP-BMC method for matrix multiplication (Oliver [O96]) to implement the inner products required for neural network training and evaluation, and their proposed BMC system also makes innovative use of DNA chips for I/O.

• **DNA Nano-fabrication and Self-assembly.** BMC techniques combined with Seeman's DNA nano-fabrication techniques may allow for the self-assembly of DNA tiles into lattices in 2 and 3 dimensions and the construction of complex nano-structures that encode computations.

• **Biological Applications: Processing of Natural DNA.** The field of BMC has restricted its attention mostly to applications which are computational problems, e.g., NP search problems. In this respect, it is still in search of a *killer application* [R96]. BMC techniques may also be used in problems that are not implicitly digital in nature, for example the processing of natural (biologically derived) DNA. These techniques may be used to provide improved methods for the sequencing and fingerprinting of natural DNA, and the solution of other biomedical problems. The results of processing natural DNA can be used to form *wet data bases* with re-coded DNA in solution, and BMC can be used to do fast searches and data base operations on these wet databases. However, BMC techniques might be ideally suited to solve problems in molecular biology which inherently involve *natural DNA*, that is DNA that is biologically derived (as opposed to artificially synthesized DNA which is coded over a given word alphabet). Lipton, Boneh, and Landweber [LBL 96] considered such a class of problems, including sequencing, fingerprinting and mutation detection. These may well be the *killer applications* of BMC. An experimental demonstration, at moderate scale, of a BMC method for solving a significant problem in molecular biology with natural DNA inputs, will be a major milestone in BMC.

– **Re-coding DNA.** One interesting approach to use BMC to solve problems concerning natural DNA is to allow natural DNA to be *re-coded.* The natural DNA is re-coded as sequences of encoded n-mers. This re-coding allows the DNA to be then operated in a purely digital manner. The processing of re-coded DNA can then be done by the usual BMC techniques. This is the DNA^{2}DNA paradigm of Landweber and Lipton [LL97].

– **DNA Sequencing.** One possible application considered by [LL97] is DNA sequencing by hybridization [DDSPL+ 93], which is quite different to the enzymatic sequencing techniques commonly used [S88]. Redundant re-coding of n-mers

may be used to reduce errors due to incomplete hybridize. These redundant encodings would be constructed and attached to the n-mers using known BMC methods, yielding an encoded array of n-mers providing the DNA sequence information (also see Boneh and Lipton [BL95b] for a quite distinct divide and conquer approach to DNA sequencing).
–**Further Processing of Re-coded DNA.** Once natural DNA is re-coded, general BMC methods may be used to speed up many other key applications in biology and medicine [SM97], such as fingerprinting and mutation detection. Re-coded natural DNA derived from many sources can be used to assemble large *wet data bases* containing DNA that encodes data of biological interest, without the problem inherent in I/O to an electronic medium. BMC, with its huge memory capacity, has a considerable advantage over conventional technologies for storing such biological data bases. Once the wet data bases are assembled then we can do further processing using BMC techniques, for example we can do fast associative searches (Baum [B96]) in these wet data bases.
• **Approximate Counting of DNA.** Faulhammer, Lipton, and Landweber [FLL98] give a BMC method for estimating the number of DNA strands within a test tube.
6. 2 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, Jozsa [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. Methods for BMC (and also a number of methods for massively parallel computation) can do search in a data base of size N in time at most polylogarithmic with 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, BMC 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 Cryptography.** 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.)

• **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.

• **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 Hybrids of BMC and QC

7.1 Applications of QC to BMC. It is interesting to envision a BMC that uses quantum affects to aid in its I/O. 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. 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.) We can apply the quantum Zeno affect (using techniques similar to those used for IMF) to do exquisite detection (of say, of a single molecule) within a large container of fluid, by taking quantum samples of the volume, and doing repeated rounds of sensing. If the molecule to be detected is in fact in the fluid, then the amount of sensing is very small quantity quickly decreasing with the number of rounds. However, if a molecule is not in the fluid, then the amount of sensing by this method can be quite large. (The result of Reif [Rei98a] implies that quantum techniques can not reduce the amount of sensing for both cases.)

7.2 Applications of BMC to QC. One interesting application of BMC is to do the observation operation for Bulk QC. Here we assume that the Bulk QC is being executed on a macroscopic volume of solution, containing a large number of micromolecules which are the quantum components for the Bulk QC unitary operations. Recall that Bulk QC can only do a weak measurement of the state of the spins; the weak measurement does not much affect the state superposition. We would like instead to do an observation operation which reduces the current state superposition. A possible technique is to place each of these micromolecule onto or within a host (e.g., a natural or artificial cell, or a macromolecule such as a protein, DNA, or RNA). The host should be much larger than the micromolecule, but still microscopic. There are a number of techniques where by the host might be used to a do an observation of the state of the qubit spins of the micromolecule (perhaps via a nearly irreversible chemical reaction), which results in a reduction of the micromolecule's state superposition. (This idea has two precedents: (i) it is mentioned in a novel of Bear [Bea83] (which incidentally was the first science fiction novel involving BMC), and (ii) Mavromatos [Nan96]and

Mavromatos et al [MN96a,MN96b] conjectured (but there is little or no concrete experimental evidence to this) a quantum mechanism in microtubules of neurons.) A key reservation to this technique the apparent large growth of the size of the measurement apparatus with the number of qubits.

8 Conclusion and Acknowledgements

Comparison of Current BMC and QC with early VLSI. BMC and QC are new fields, with largely unexplored methodologies. We find it interesting to compare BMC in the later 1990's with the state of VLSI in 1970s, which had (i) multiple enabling technologies which were quickly advancing, (ii) evolving algorithmic paradigms, (iii) lack of simulation models and software for design and simulation of chip designs, and thus (iv) (at the time) high risk. In particular, in the 1970's, the design and fabrication of a VLSI chip was perhaps less an engineering discipline than an art prone to failures, due in part to the lack of developement of (a) exact models for the device physics, (b) software tools for software for design and simulation, and (c) parallel algorithmic design principles.

Through the late 1980's and 1990's, these problems were alleviated for VLSI by the stabilization of the major enabling technology (CMOS), and by major investment by the US government and industry in process modeling and software tools for simulation, allowing for much higher yields in fabrication, and thus considerably lower risk. Also, by this time, there is a mature understanding of parallel algorithmic design principles and high performance architectures (e.g., systolic) for VLSI, thanks to major federal funding programs in these areas. A high pace of improvement in VLSI performance has been sustained for many years, but may slow in the future due to ultimate physical limitations.

Both BMC and QC suffer from difficulties similar to those suffered by VLSI in the 1970's. Currently, the design and execution of a BMC or QC experiment in the laboratory is supported with only a few software tools for design and simulation prior to doing the experiment:

- **Computer Simulations of BMC.** A preliminary version of a Java software tool for simulating BMC has been developed by Gehani, Reif [GR98b].
- **Computer Simulations of QC.** Obenland, Despain [OD97, D98a, D98b] have given efficient computer simulations of QC, including errors and decoherence, and Cerf, S. E. Koonin [CK98] have given Monte Carlo simulations of QC.

In spite of advanced technologies for Recombinant DNA and for quantum apparatus, experiments in BMC and QC are highly prone to errors. We have discussed techniques that alleviate some of these errors, but this clearly motivates the need to further develope software tools for design and simulation of BMC and QC experiments.

Also, there is at this time no consensus on which methods for doing BMC and QC are the best; as we have seen there are multiple approaches that may have success. While some of the current experiments in BMC are using conventional solution-based recombinant DNA technology, others are employing alternative biotechnology (such as surface attachments). It is also not yet clear which of the paradigms for BMC will be preeminent. There is a similar lack of consensus within QC of the best and most scalable technologies. To a degree, this diversity of approaches may in itself be an advantage, since it will increase the likelihood of prototyping and establishing successful methodologies.

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.

Note: This paper has approximately 646 references, including 270 references to BMC and 385 references to QC. Due to page length constraints, the references are partitioned into a list of references for BMC followed by and a separate reference list of references for QC.

Biomolecular Computing References

[ALL95] R. A. Adey and A. Lahrmann and C. LeBmollmann, *Simulation and Design of Micro-systems and Micro-structures*, Computational Mechanics Publication, (1995).

[A94] Adleman, L., *Molecular Computation of Solution to Combinatorial Problems*, Science, **266**, 1021–7pt24, (1994).

[A95] Adleman, L., *On Constructing a Molecular Computer*, Dept of CS, U.S.C., Available via anonymous ftp from ftp.usc.edu /pub/csinfo/papers/adleman/molecular_computer·ps, (1995).

[ARRW96] Adleman, L.M., P.W.K. Rothemund, S. Roweis, E. Winfree, *On Applying Molecular Computation To The Data Encryption Standard*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton, June, 1996.

[AJPWL+96] Alivisatos, A.P., K.P. Johnsson, X. Peng, T.E. Wilson, C.J. Loweth, M. P. Bruchez Jr., P. G. Schultz, *Organization of 'nanocrystal molecules' using DNA*, Nature, bf 382, 609–611, August 1996.

[Al94] Alper, *Drug discovery on the assembly line*, Science, **264**, 1399–1401, (1994).

[A96] Amenyo, J.-T., *Mesoscopic computer engineering: Automating DNA-based molecular computing via traditional practices of parallel computer architecture design*, Proceedings of the 2nd Annual DIMACS Meeting on DNA Based Computers, June 1996.

[AGH96] Amos, M., A. Gibbons, D. Hodgson, *Error-resistant Implementation of DNA Computations*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton University, June 1996.

[AH97] Arita , M. and M. Hagiya, *Joining and Rotating Data with Molecules*, ICEC'97 Special Session on DNA Based Computation, Indiana, April 1997.

[BCGT96] Bach, E., A. Condon, E. Glaser, and C. Tanguay, *Improved Models and Algorithms for DNA Computation*, Proc. 11th Annual IEEE Conference on Computational Complexity, Submitted (by invitation) to: J. Computer and System Sciences, May 1996.

[BS91] Bartel, D. and J. Szostak, *Isolation of new ribozymes from a large pool of random sequences*, Science, **261**, 1411–1418, (1991).

[B68] Batcher,K. *Sorting Networks and their applications*, Spring Joint Computer Conference, **32**, 307–314, AFIPS Press, Montvale, N. J., (1968).

[B95] Baum, E. B. *How to build an associative memory vastly larger than the brain*, Science, April 28, 1995.

[B96] Baum, E. B. *DNA Sequences Useful for Computation*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton University, June 1996.

[BB96] Baum, E. B. and D. Boneh, *Running dynamic programming algorithms on a DNA computer*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton, June, 1996.

[Bea83] G. Bear, *Blood Music*, Analog, (June, 1983). Also, appearing in Nanodreams, (Ed. by E Elliott), Baen Pub., (1995). Also, appearing as a full novel as *Blood Music*, Ace Pub., (1985). *Blood Music*, Analog, (june, 1983).

[Be94] Beaver, D. *Factoring: The DNA Solution*, Advances in Cryptology, Asia Crypt94 Proceedings, Lecure Notes in Computer Science, (1994), Springer Verlag, (http:// www.cse.psu.edu/ beaver/ publications/ pubindex.html),

[BeB95] Beaver, D. *Computing with DNA*, J. Comp. Biol., **2**, 1–7, (1995).

[BeA95] Beaver, D. *A Universal Molecular Computer*, revised as *Molecular Computing*, Penn State University Technical Memo CSE-95-001, Pond Lab, http:// www.cse.psu.edu/ beaver/ publications/ pubindex.html, (1995).

[BF97] Beigel, R. and Bin Fu, *Molecular Approximation Algorithm for NP Optimization Problems*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[B65] Beneš, V. *Mathematical Theory of Connecting Networks and Telephone Traffic*, Academic Press, New York, NY (1965).

[B66] Berger, R. *The Undecidability of the Domino Problem*, Memoirs of the American Mathematical Society, **66**, (1966).

[B97] Blumberg, A.J. *Parallel Computation on a DNA Substrate*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[BDL95] Boneh, D., C. Dunworth, R. Lipton, *Breaking DES Using a Molecular Computer*, Princeton CS Tech-Report number CS-TR-489-95 (1995).

[BDLS95] Boneh, D., C. Dunworth, R. Lipton, J. Sgall, *On the Computational Power of DNA*, Princeton CS Tech-Report number CS-TR-499-95 (1995). Also published in Discrete Applied Math, (Dec 96)

[BL95a] Boneh, D., and R. Lipton, *Making DNA Computers Error Resistant*, Princeton CS Tech-Report CS-TR-491-95 Also in 2nd Annual DIMACS Meeting on DNA Based Computers,, Princeton University, June 1996.

[BL95b] Boneh, D., and R. Lipton, *A Divide and conquer approach to DNA sequencing*, Princeton University, 1996.

[BKP90] Brooks, C., M. Karplus, M. Pettitt, *Proteins, A Theoretical Perspective of Dynamics, Structure & Thermodynamics*, John Wiley & Sons,

[B62] Buchi, J.R *Turing Machines and the Entscheidungsproblem*, Mathematiche Annalen, **148**, 201–213, (1962).

[CCCFF+97] Cai, W., A. Condon, R.M. Corn, Z. Fei, T. Frutos, E. Glaser, Z. Guo, M.G. Lagally, Q. Liu, L.M. Smith, and A. Thiel, *The Power of Surface-Based Computation*, Proc. First International Conference on Computational Molecular Biology (RECOMB97), January, 1997.

[CRFCC+96] Cai, W., E. Rudkevich, Z. Fei, A. Condon, R. Corn, L.M. Smith, M.G. Lagally, *Influence of Surface Morphology in Surface-Based DNA Computing*, Submitted to the 43rd AVS National Symposium, Abstract No. BI+MM-MoM10, (1996).

[CCTKS88] J.-H. Chen, M.E.A. Churchill, T.D. Tullius, N.R. Kallenbach, N.C. Seeman, *Construction and Analysis of Monomobile DNA Junctions*, Biochemistry, **27**, (1988).

[CRWEC95] Chen, J. , C.A. Rauch, J.H. White, P.T. Englund, N.R. Cozzarelli, em The Topology of the Kinetoplast DNA Network, rm Cell, **80**, 61–69, January 1995.

[CW97] Chen, J., and D. Wood, *A New DNA Separation Technique with Low Error Rate*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[Con98] Conrad, M., *Molecular and evolutionary computation: The tug of war between context freedom and context sensitivity*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[CZ97] Conrad, M. and K.-P. Zauner, *Design for a DNA Conformational Processor*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[CL92] Crandall, B. and J. Lewis (eds.), *Nanotechnology*, MIT Press, (1992).

[CFKP96] E. Csuhaj-Varju, R. Freund, L. Kari, and G. Paun, *DNA Computing Based on Splicing: Universality Results*, Proceedings of 1st Annual Pacific Symposium on Biocomputing, Hawaii, (L.Hunter, T.Klein, eds.), World Scientific Publ., Singapore, 179–190. (1996).

[CFL+98] Cukras, A., D. Faulhammer, R. Lipton, L. Landweber, *Chess games: A model for RNA-based computation*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[CH89] K. Culik II and T. Harju, *The regularity of splicing systems and DNA*, Proc. ICALP'89, Lec. Notes. in C.S., **372**, 222–233, (1989).

[DMGFS96] Deaton, R., R.C. Murphy, M. Garzon, D.R. Franceschetti, and S.E. Stevens, Jr., *Good encodings for DNA-based solutions to combinatorial problems*, Proceedings of the 2nd Annual DIMACS Meeting on DNA Based Computers, June 1996.

[DMRGF+97] Deaton, R., R.C. Murphy, J.A. Rose, M. Garzon, D.R. Franceschetti, and S.E. Stevens, Jr., *A DNA Based Implementation of an Evolutionary Search for Good Encodings for DNA Computation*, ICEC'97 Special Session on DNA Based Computation, Indiana, April 1997.

[DHK96] Delcher, A. L., L. Hood, R.M. Karp, *Report on the DNA/Biomolecular Computing Workshop*, June 1996.

[DHS97] Deputat, M., G. Hajduczok, E. Schmitt, *On Error-Correcting Structures Derived from DNA*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[DDSPL+ 93] Drmanac, R, S. Drmanac, Z. Strezoska, T. Paunesku, I. Labat, M. Zeremski, J. Snoddy, W. K. Funkhouser, B. Koop, L. Hood, and R. Crkenjakov *DNA Sequence Determination by Hybridize: A Strategy for Efficient Large-Scale Sequencing*, Science, **260**, 1649–1652, (1993).

[DS92] Du, S.M., and N.C. Seeman, *The Synthesis of a DNA Knot Containing both Positive and Negative Nodes*, J. Am. Chem. Soc., **114**, 9652–9655, (1992).

[DZS92] Du, S.M., S. Zhang and N.C. Seeman, *DNA Junctions, Antijunctions and Mesojunctions*, Biochem., **31**, 10955–7pt963, (1992).

[ER94] Eigen, M., and R. Rigler, *Sorting Single Molecules - applications to diagnostic and evolutionary biotechnology*, Proc. of the National Academy of Science, **91**, 5740–8747, (1994).

[EC] Eisenberg and Crothers, *Physical Chemistry with applications to the life sciences.*

[E97] Eng, T. *Linear DNA Self-Assembly with Hairpins Generates the Equivalent of Linear Context-Free Grammars*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[Eng98] Eng, T., *On solving a 3CNF-Satisfiability with an in vivo algorithm*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[ES97] Eng, T., and B.M. Serridge, *A Surface-Based DNA Algorithm for Minimal Set Cover*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[ER82] Engler, M., and C. Richardson, *The Enzyme*, (P. Boyer, ed.) Academic Press, 3–29, (1982).

[FF97] Faulhammer, D. and Michael Famulok, *In Vitro Selection and Characterization of DNA Enzymes*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[FLL98] Faulhammer, D., R. Lipton, L. Landweber, *Counting DNA: Estimating the complexity of a test tube of DNA*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[F 61] Feynman, R. There's Plenty of Room at the Bottom, Miniaturization (D. Gilbert, ed.), Reinhold, 282–296, (1961). Reprinted in B.C. Crandall and J. LKewis, eds., Nanotechnology: Research and Perspectives, Cambridge: The MIT Press, p. 360, (1992).

[FW 78] Fortune, S. and J. Wyllie, *Parallelism in random access machines*, Proc. 10th Annual ACM S.T.O.C., San Diego, CA, 114–118, (1978).

[F97] Freund, R. *Test Tube Systems with Controlled Applications of Rules*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[FKP98] R.Freund, L.Kari, G.Paun, *DNA computing: the existence of universal computers*, to appear in Theory of Computer Science, (1998).

[FPRS97] Freund, R., G. Paun, G. Rozenberg, A. Salomaa *Watson-Crick Finite Automata*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[FTCSC97] Frutos, A.G., A.J. Thiel, A.E. Condon, L.M. Smith, R.M. Corn, *DNA Computing at Surfaces: 4 Base Mismatch Word Design*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[FB98] Fu, B., R. Beigel, *Length bounded molecular computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[FBZ98] Fu, B., R. Beigel, F. Zhou, *An $O(2^n)$ volume molecular algorithm for Hamiltonian Path*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[FS93] Fu, T.-J., and N.C. Seeman, *DNA Double Crossover Structures*, Biochemistry, **32**, 3211–3220, (1993).

[GGM97] Gao, Y. M. Garzon, R.C. Murphy, J.A. Rose, R. Deaton, D.R. Franceschetti, S.E. Stevens Jr., *DNA Implementation of Nondeterminism*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[GJ79] Garey, M. R., and D. S. Johnson *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H Freeman and Company, page 257, (1979).

[GJP77] Garey, M.R., D. S. Johnson, and C. H. Papadimitriou, unpublished manuscript, (1977).

[GDNMF97] Garzon, M., R. Deaton, P. Neathery, R.C. Murphy, D.R. Franceschetti, S.E. Stevens Jr., *On the Encoding Problem for DNA Computing*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[GJ98] Garzon, M., N. Jonoska, *The bounded complexity of DNA computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[GLR99] A. Gehani, T. H. LaBean, and J.H. Reif, DNA-based Cryptography, 5th DIMACS Workshop on DNA Based Computers, MIT, June, 1999. To appear in DNA Based Computers, V, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, (ed. E. Winfree), American Mathematical Society, 2000. http://www.cs.duke.edu/∼reif/paper/DNAcypt/crypt.ps

[GR98a] Gehani, A., J. Reif, *Micro flow bio-molecular computation*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998). http://www.cs.duke.edu/∼ reif/paper/geha/microflow.ps or http://www.cs.duke.edu/∼ geha/public_html/misc/biosystems.ps

[GR98b] Gehani, A., J. Reif, *A Simulation System for Bio-molecular Computation*, to appear, (Oct., 1998).

[G94] Gifford, D. *On the Path to Computing with DNA*, Science, **266**, 993–994, November, 1994.

[GKG+98] Gloor, G., L. Kari, M. Gaasenbeek, S. Yu, *Towards a DNA solution to the shortest common superstring problem*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998). Also, Proceedings of IEEE'98 International Joint Symposia on Intelligence and Systems, Rockville, MD, 140–145, (May 1998).

[GFBCL+96] Gray, J. M. , T. G. Frutos, A.M. Berman, A.E. Condon, M.G. Lagally, L.M. Smith, R.M. Corn, *Reducing Errors in DNA Computing by Appropriate Word Design*, University of Wisconsin, Department of Chemistry, October 9, 1996.

[GBS87] Grunbaum, S., Branko, and G.C. Shepard *Tilings and Patterns*, H Freeman and Company, **Chapter 11**, (1987).

[GB96] Guarnieri, F., and C. Bancroft, *Use of a Horizontal Chain Reaction for DNA-Based Addition*, Proceedings of the 2nd Annual DIMACS Meeting on DNA Based Computers., June 10-12, 1996, American Mathematical Society, Providence, RI (in press), (1996).

[GFB96] Guarnieri, F., Fliss, M., and C. Bancroft, *Making DNA add*, Add. Science, **273**, 220–223, (1996).

[GPZ97] Gupta, V., S. Parthasarathy, M.J. Zaki, *Arithmetic and Logic Operations with DNA*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[HA97] Hagiya, M., and M. Arita, *Towards Parallel Evaluation and Learning of Boolean μ-Formulas with Molecules*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[HG97] Hartemink, A.J., D.K. Gifford *Thermodynamic Simulation of Deoxyoligonucleotide Hybridize for DNA Computation*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[HGL98] Hartemink, A., David Gifford, J. Khodor, *Automated constraint-based nucleotide sequence selection for DNA computation*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[H87] Head, T., *Formal language theory and DNA: an analysis of the generative capacity of specific recombinant behaviors*, Bull. Math. Biology, **49**, 737–759, (1987).

[H92] Head, T., *Splicing schemes and DNA*, In: *Lindenmayer Systems: Impacts on Theoretical Computer Science, Computer Graphics, and Developmental Biology*, Ed. by G.Rozenberg and A.Salomaa, Springer-Verlag, 371-383, (1992). Also appears in: *Nanobiology*, **1**, 335–342, (1992).

[H97] Head, T., *Splicing System and Molecular Processes*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[HPP96] Head, T., G. Paun, and D. Pixton, *Language Theory and Molecular Genetics-generative mechanisms suggested by DNA recombination*, A chapter in: *Handbook of Formal Language Theory*, Springer-Verlag, (1996 or to appear).

[Iku96] K. Ikuta *3D Micro Integrated Fluid System Toward Living LSI*, International Workshop on Artificial Life (1996).

[J92] JáJá, J. *An Introduction to Parallel Algorithms*, Addison Wesley, (1992).

[JKS98] Jonoska, N, S. Karl, M. Saito, *Three dimensional DNA structures in computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[Ji98] Ji, S., *The cell as a DNA-based molecular computer*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[JK96] Jonoska, N., and S.A. Karl, *A Molecular Computation of the Road Coloring Problem*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton University, June 1996.

[JK97a] Jonoska, N., and S.A. Karl, *Ligation Experiments in Computing with DNA*, ICEC'97 Special Session on DNA Based Computation, Indiana, April 1997.

[JK97b] Jonoska, N., and S.A. Karl, *Creating 3-Dimensional Graph Structures with DNA*, 3nd Annual DIMACS Meeting on DNA Based Computers, University of Pens., (June 1997).

[KCL96] Kaplan, P., G. Cecchi, and A. Libchaber, *DNA based molecular computation: Template-template interactions in PCR*, The 2nd Annual Workshop on DNA Based Computers, American Mathematical Society, To appear, (1996).

[KTL97] Kaplan, P., D. Thaler, A. Libchaber, *Parallel Overlap Assembly of Paths Through a Directed Graph*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[Kar96] L.Kari, *DNA computers: tomorrow's reality* , Tutorial in the Bulletin of EATCS, no.59, pp.256-266, (1996).

[Kar97A] L.Kari, *DNA computing based on insertions and deletions*, Proceedings of the conference Conceptual tools for understanding dynamics in biological systems, London, 1996. In COENOSES, C.E.T.A. Gorizia, Italy, N. Kenkel, ed., Vol. 12, pp. 2–3, 89-95, (1997).

[Kar97B] L.Kari, *DNA computing - the arrival of biological mathematics*, The Mathematical Intelligencer, vol.19, **2:** 9–22, (1997).

[Kar98] L.Kari, *Computing with DNA*, In Computer Methods in Molecular Biology, (S.Misener, S.Krawetz, Eds.), in Methods in Molecular Biology series, Humana Press. To appear, (1998).

[KPRS98] L.Kari, G.Paun, G.Rozenberg, A.Salomaa, S.Yu, *DNA computing, sticker systems, and universality*, Acta Informatica, **35:** 401-420, (1998).

[KPTY97] Kari, L., G. Paun, G. Thierrin, Sheng Yu, *At the Crossroads of DNA Computing and Formal Languages: Characterizing Recursively Enumerable Languages Using Insertion-Deletion Systems*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[KarS97] L.Kari, Y.Sakakibara., *DNA Computers* Journal of the Institute of Electronics, Information and Communication Engineers, vol.80, no.9, 1997, pp. 935-939 (in Japanese), (1997)

[Kaz98] Kazic, T., *After the Turing machine: A metamodel for molecular computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[KG97] Khodor, J., and David K. Gifford, *The Efficiency of Sequence-Specific Separation of DNA Mixtures for Biological Computing*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[KG98] Khodor, J., D. Gifford, *Design and implementation of computational systems based on programmed mutagenesis*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[KK97] Kim, S.M., and Kyungpook, *Identifying Genetically Spliced Languages*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[KS97] Knight,T. F., G.J. Sussman, *Cellular Gate Technology*, MIT Artificial Intelligence Labratory, July 1997.

[KMRS96] Kurtz, S.A., S.R. Mahaney, J.S. Royer, J. Simon, *Active Transport in Biological Computing*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton University, June 1996.

[LYR+98] Thomas H. LaBean, Hao Yan, John H. Reif and Nadrian Seeman, *Construction and Analysis of a DNA Triple Crossover Molecule*, (November. 1998).

[LF80] Ladner, R.E., and M.J. Fischer, *Parallel Prefix Computation*, JACM, **27(4)**:831–838, (1980).

[La96] Landweber, L.F., *RNA Based Computing*, American Mathematical Society, R. J. Lipton and E. B. Baum, eds., 2nd Annual DIMACS Meeting on DNA Based Computers, DIMACS Workshop, Princeton, June, 1996

[L97] Landweber, L., *In vitro evolution of a novel RNA ligase ribozyme from a large pool of random sequences*, to appear, (1997).

[LG 93] Landweber, L.F. and W. Gilbert, *RNA editing as a source of genetic variation*, Nature, **363**, 179–182, (1993).

[LK98] Landweber, L., L. Kari, *The evolution of cellular computing: Nature's solution to a computational Problem*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998). Also, Proceedings of the 3rd Annual Genetic Programming Conference, Morgan Kaufmann Publishers, San Francisco, pp.700-708, (July 22-25, 1998).

[LG 94] Landweber, L.F. and W. Gilbert, *Phylogenetic analysis of RNA editing: A primitive genetic phenomenon*, Proc. Natl. Acad. Sci., **91**, 918–921, (1994).

[LL97] Landweber, L.F. and R. Lipton, *DNA 2 DNA Computations: A Potential 'Killer App'?*, 3nd Annual DIMACS Meeting on DNA Based Computers, University of Pens., (June 1997).

[LR97] Laun, E., and K.J. Reddy, *Wet Splicing Systems*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[LKSR97] Leete, T.H., J. Klein, J.S. Salem, and H. Rubin, *Bit Operations Using a DNA Template*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[LS+96] Leete, T.H., M.D. Schwartz, R.M. Williams, D.H. Wood, J.S. Salem, and H. Rubin, *Massively Parallel DNA Computation: Expansion of Symbolic Determinants*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton, June, 1996, Also, **American Mathematical Society**, To appear, (1997). (Also U.S. Patent Application, 1996).

[L92] Leighton, F.T. *Introduction to Parallel Algorithms and Architectures*, Morgan Kaufmann Press, San Mateo, CA, Chapter 3, (1992).

[LP81] Lewis, H.R., and C.H. Papadimitriou *Elements of the Theory of Computation*, Prentice-Hall, pages 296–300 and 345–348 (1981).

[Li98] Z. Li, Z., *Algebraic properties of DNA operations*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[LYQS96] Li, X.J., X.P. Yang, J. Qi, and N.C. Seeman, *Antiparallel DNA Double Crossover Molecules as Components for Nanoconstruction*, J. Am. Chem. Soc., **118**, 6131–6140, (1996).

[L94] Lipton, R. *Speeding Up Computations via Molecular Biology*, Princeton University Draft, (1994).

[L95] Lipton, R.J. *DNA Solution of Hard Computational Problems*, Science, **268**, 542–845, (1995).

[L96] Lipton, R.J. *DNA Computations Can Have Global Memory*, unpublished manuscript, April 1996.

[Lip98] Lipton, R., *A memory based attack on cryptosystems with application to DNA computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[LBL 96] Lipton, R.J., D. Boneh, and L. Landweber, *Analog DNA Based Computation*, in preparation. (1996).

[LFW+98] Liu, Q., A. Frutos, L. Wang, A. Thiel, S. Gillmor, T. Strother, A. Condon, R. Corn, M. Lagally, L. Smith, *Progress towards demonstration of a surface based DNA computation: A one word approach to solve a model satisfiability problem*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[LGCCL+96] Liu, Q., Z. Guo, A.E. Condon, R.M. Corn, M.G. Lagally, and L.M. Smith, *A Surface-Based Approach to DNA Computation,*, Proc. 2nd Annual Princeton Meeting on DNA-Based Computing, June 1996.

[LTCSC97] Liu, Q., A.J. Thiel, A.G. Frutos, R.M. Corn, L.M. Smith, *Surface-Based DNA Computation: Hybridize and Destruction*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[ADL+98] Manca, V., C. Martin-Vide, G. Paun, *New computing paradigms suggested by DNA computing by carving*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[MR98] Margenstern, M., Y. Rogozhin, *A universal time-varying distributed H system of degree 2*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[MEBH92] A. Manz, C. S. Effenhauser, N. Burggraf, D. J. Harrison, K. Seiler, and K. Fluri, *Electro-osmotic Pumping and Electro-osmotic Pumping and Electro-phoretic Separations for Miniaturized Chemical Analysis Systems*, Journal of Micro-mechanics and Micro-engineering, (1992).

[MH87] McCammon, J., and S. Harvey, *Dynamics of Proteins and Nucleic Acids*, Cambridge University Press, (1987).

[M93] Merkle, R. Nanotechnology, **4** 21, (1993).

[M97] Mihalache, V. *Prolog Approach to DNA Computing*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[MYP98] Mills, A., B. Yurke, P. Platzman, *Error-tolerant massive DNA neural-network computation*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[M96] Mir, K.U. *A Restricted Genetic Alphabet for DNA Computing*, 2nd Annual DIMACS Meeting on DNA Based Computers,, Princeton University, June 1996.

[MLMS96] Mirkin, C.A., R.L. Letsinger, R.C. Mucic, J.J. Storhoff, *A DNA-based Method for Rationally Assembling Nanoparticles Into Macroscopic Materials*, Nature, **382**, 607–611, August 1996.

[MS97] Mao, C., and N.C. Seeman, *Construction of Borromean Rings from DNA*, Nature, **386**(6621), 137–138, (March,1997).

[MoS97] Morimoto, N., M.A.A. Suyama, *Solid Phase DNA Solution to the Hamiltonian Path Problem*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[MDS91] Mueller, J.E., S.M. Du, and N.C. Seeman, *The Design and Synthesis of a Knot from Single-Stranded DNA*, J. Am. Chem. Soc., **113**, 6306–6308, (1991).

[MDFS97] Murphy, R.C., R. Deaton, D.R. Franceschetti, S.E. Stevens, *A New Algorithm for DNA Based Computation*, ICEC'97 Special Session on DNA Based Computation, Indiana, April 1997.

[OR97a] Ogihara, M., and A. Ray, *Breadth first search 3SAT algorithms for DNA computer*, Technical Report TR-629, Department of Computer Science, University of Rochester, (July 1996).

[OR97b] Ogihara, M., and A. Ray, *Simulating Boolean circuits on a DNA computer*, 1st Annual International Conference On Computational Molecular Biology (RECOMB97), Santa Fe, New Mexico, January 1997.

[OR97c] Ogihara, M., and A. Ray, *DNA-Based Parallel Computation by 'Counting'*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[OP94] Old, R., and S. Primrose, *Principles of Gene Manipulation, An Introduction to Genetic Engineering*, Blackwell Scientific Publications, Fifth Edition, (1994).

[O96] Oliver, J.S. *Computation With DNA-Matrix Multiplication*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton, June, 1996.

[OGB97] Orlian, M., F. Guarnieri, C. Bancroft, *Parallel Primer Extension Horizontal Chain Reactions as a Paradigm of Parallel DNA-Based Computation*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[P95] Papadimitriou, C. personal communication, (1995).

[P96a] Paun, G., *On the splicing operation*, Discrete Applied Math., **70**, 57–79, (1996).

[P96b] Paun, G., *Five Universal DNA Computing Models Based on the Splicing Operation*, to appear, (1996).

[P97] Paun, G., *Computing by Splicing: Programmed and Evolving Splicing Systems*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[PRS96] Paun, G., Rozenberg, and A. Salomaa, *Computing by splicing,*, Theor. Computer Sci., **168**, 321–336, (1996).

[Pi95] Pixton, D., *Linear and circular splicing systems*, Proc. 1st Intn. Symp. on Intelligence in Neural and Biological Systems, IEEE Press, 181-188, (1995).

[Pi96] Pixton, D., *Regularity of splicing languages*, Discrete Applied Math., **69**, 101–124, (1996).

[Pi97] Pixton, D., *Splicing systems and AFL theory*, (to be submitted shortly).

[PP97] Plum, G.E., and D. S. Pilch, *Nucleic Acid Hybridize: Triplex Stability and Energetics.*, Annu. Rev. Biophys. Biomol. Struct. , **24:**, 319–350, (February 1997).

[Po97] Pool, R. *Dr. Tinkertoy*, Discover, **18:2**, 50–87, (February 1997).

[QYS96] Qi, J., X.J. Li, X.P. Yang, and N.C. Seeman, *Ligation of triangles built from bulged 3-arm DNA branched junctions*, J. Am. Chem. Soc., **v118:26**, 6121–6130, (July, 1996).

[R93] Reif, J. (ed.), *Synthesis of Parallel Algorithms*, Morgan Kaufmann, (1993).

[R95] Reif, J., *Parallel Molecular Computation: Models and Simulations*, Seventh Annual ACM Symposium on Parallel Algorithms and Architectures (SPAA95), ACM, Santa Barbara, 213–223, June 1995. Also accepted and to appear in Algorithmica, special issue on Computational Biology, 1998. This paper in postscript, can be found at *http : //www.cs.duke.edu/r̃eif/paper/Molecular.ps* and figures can be found at *http : //www.cs.duke.edu/r̃eif/paper/mole.fig.ps* .

[R97] Reif, J.H., *Local Parallel Biomolecular Computation*, (A postscript preprint of this paper and its figures are at http://www.cs.duke.edu/∼reif/paper/Assembly.ps and http://www.cs.duke.edu/∼reif/paper/Assembly.fig.ps), 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[R98] Reif, J.H., *Alternative Computational Models: A Comparison of Biomolecular and Quantum Computation*, (A postscript preprint of the full paper can be found at http://www.cs.duke.edu/∼ reif/paper/paper.html/altcomp.ps.), invited paper,18th International Conference on Foundations of Software Technology and Theoretical Computer Sceince (FST&TCS98), (December, 1998).

[RE97] Robertson, M.P., and Andrew D. Ellington, *New Directions in Nucleic Acid Computing: Selected Ribozymes that Can Implement Re-Write Rules*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[R71] Robinson, R.M. *Undecidablility and Nonperiodicity for Tilings of the Plane*, Inventiones Mathematicae, **12**, 177–209, (1971).

[RDGS97] Rose, J.A., R. Deaton, M. Garzon, and S.E. Stevens Jr., *The Effect of Uniform Melting Temperatures on the Efficiency of DNA Computing*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[Ro95] Rothemund, P.W.K. *A DNA and restriction enzyme implementation of Turing Machines*, manuscript available at http://www.ugcs.caltech.edu/ pwkr/oett.html, (1995).

[RW95] Rooβ, D., and K.W. Wagner, *On the power of Bio-Computers*, unpublished manuscript.

[RWBCG+96] Roweis, S., E. Winfree, R. Burgoyne, N.V. Chelyapov, M.F. Goodman, P.W.K. Rothemund, L. M. Adleman, *A Sticker Based Architecture for DNA Computation*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton University, June1996, Also as Laboratory for Molecular Science, USC technical report *A Sticker Based Model for DNA Computation*, May 1996.

[RS97] Rozenberg, G., and A. Salomaa, ICEC'97 Special Session on DNA Based Computation, Indiana, April 1997.

[R96] Rubin, H. *Looking for the DNA killer app.*, Nature, **3**, 656–658, (1996).

[RKL98] Rubin, H., J. Klein, T. Leete, *A biomolecular implementation of logically reversible computation with minimal energy dissipation*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[SF97] Sakakibara, Y., and C. Ferretti, *Splicing on Tree-like Structures*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[SKK+98] Sakamoto, K., D. Kiga, K. Komiya, H. Gouzu, S. Yokoyama, S. Ikeda, H. Sugiyama, M. Hagiya, *State transitions by molecules*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[SFM89] Sambrook, J., E. Fritsch, and T. Maniatis, *Molecular Cloning*, Cold Spring Harbor Lab, NY, (1989).

[S82] Seeman, N.C. *Nucleic Acid Junctions and Lattices*, J. Theor. Biol., **99**, 237-247, (1982).

[S85] Seeman, N.C. *Macromolecular Design, Nucleic Acid Junctions and Crystal Formation*, Journal of Biomolecular Structure and Dynamics, **3**, 1-34, (1985).

[SC91] Seeman, N. C., and J. Chen, *Synthesis from DNA of a molecule with the connectivity of a cube*, Nature, **350**, 631–633, (1991).

[SCDMZ+93] Seeman, N. C., J. Chen, S.M. Du, John E. Mueller, Yuwen Zhang, Tsu-Ju Fu, Yinli Wang, Hui Wang, Siwei Zhang, *Synthetic DNA knots and catenanes*, New Jour. of Chemistry, **17**, 739–755, (1993).

[SCK89] Seeman, N. C., J.-H. Chen, N.R. Kallenbach, *Gel electrophoretic analysis of DNA branched junctions*, Electrophoresis, **10**, 345–354, (1989).

[SMY+98] Seeman, N., F. Liu, C. Mao, X. Yang, L. Wenzler, E. Winfree, *DNA nanotechnology: Control of 1-D and 2-D arrays and the construction of a nanomechanical device*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[SQLYL+96] Seeman, N. C., J. Qi, X. Li, X. Yang, N.B. Leontis, B. Liu, Y. Zhang, S.M. Du, and J. Chen, *The control of DNA structure: From topological modules to geometrical modules*, Modular Chemistry, J. Michl, ed., Kluwer, To appear, (1996).

[SWLQ+96] Seeman, N. C., H. Wang, B. Liu, J. Qi, X. Li, X. Yang, F. Liu, W. Sun, Z. Shen, R. Sha, C. Mao, Y. Wang, S. Zhang, T.-J. Fu, S. Du, J. E. Mueller, Y. Zhang, and J. Chen, *The Perils of Polynucleotides: The Experimental Gap Between the Design and Assembly of Unusual DNA Structures*, The 2nd Annual Workshop on DNA Based Computers, American Mathematical Society, June 1996.

[SZC94] Seeman, N. C., Y. Zhang, and J. Chen, *DNA nanoconstructions*, J. Vac. Sci. Technol., **12:4**, 1895–1905, (1994).

[SZDC95] Seeman, N. C., Y. Zhang, S.M. Du, and J. Chen, *Construction of DNA polyhedra and knots through symmetry minimization*, Supramolecular Stereochemistry, J. S. Siegel, ed., 27–32, (1995).

[SZDWM+94] Seeman, N. C., Y. Zhang, S. Du, H. Wang, J.E. Mueller, and J. Chen, *The control of DNA structure and topology: An overview*, Mat. Res. Soc. Symp. Proc., **356**, 57–66, (1994). DNA, Molecular Biology

[SM97] Setubal, J., and J. Meidanis *Introduction to Computational Molecular Biology*, PWS Pub. Co., Chapt 9, (1997).

[EE92] S. Shoji and M. Esashi., *Micro-flow Devices and Systems*, Journal of Micro-mechanics and Micro-engineering (1992).

[S94] Sinden, R. *DNA Structure and Function*, Academic Press, (1994).

[S88] Smith, L.M. *Automated Synthesis and Sequence Analysis of Biological Macromolecules*, Anal. Chem., **60**, 381A–390A, (1988).

[SS95] Smith, W., and A. Schweitzer, *DNA Computers in Vitro and Vivo*, NEC Research Inst. Tech Report 95-057-3-0058-3. (1995).

[StM97] Stefan, G., and M. Malita, *The Splicing Mechanism and the Connex Memory*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[S71] H.S. Stone *Parallel Processing with the perfect shuffle*, IEEE Trans. on Computers, **C-20**:2, 153-161 (1971).

[Suy98] A. Suyama, *DNA chips - Integrated Chemical Circuits for DNA Diagnosis and DNA computers*, to appear, (1998).

[U84] J. Ullman, *Computational Aspects of VLSI*, Computer Science Press, (1984), Chapter 6.

[VSJMWR92] E. M. J. Verpoorte, van der Schoot, B. H., S. Jeanneret , A. Manz, H. M. Widmer, and de Rooij, N. F., *Three-Dimensional Micro-flow Manifolds for Miniaturized Chemical Analysis Systems*, Journal of Micro-mechanics and Micro-engineering, (1992).

[W61] H. Wang, *Proving Theorems by Pattern Recognition*, Bell System Technical Journal, **40**, 1–141, (1961).

[WQF+98] Wang, L., Q. Liu, A. Frutos, S. Gillmor, A. Thiel, T. Strother, A. Condon, R. Corn, M. Lagally, L. Smith, *Surface-based DNA computing operations: DESTROY and READOUT"*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[WGWZ92] Watson, J., M. Gilman, J. Witkowski, M. Zoller, *Recombinant DNA (2nd ed.)*, Scientific American Books, W.H. Freeman and Co., (1992).

[WHR87] Watson, J., N. Hoplins, J. Roberts, et. al., *Molecular Biology of the Gene*, Benjamin/Cummings, Menlo Park, CA, (1987).

[W97] Wetmur, J. G. *Physical Chemistry of Nucleic Acid Hybridize*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[WW95] Williams, R.M., and David H. Wood, *Computational algebras for RNA processes*, Gene-Finding and Gene Structure Prediction Workshop, Unrefereed poster presentation, (1995).

[WW96] Williams, R.M., and David H. Wood, *Exascale Computer Algebra Problems Interconnect with Molecular Reactions and Complexity Theory*, The 2nd Annual Workshop on DNA Based Computers, American Mathematical Society, June, 1996.

[W95] Winfree, E. *Complexity of Restricted and Unrestricted Models of Molecular Computation*, California Institute of Technology technical report May, 1995. Also Princeton DIMACS Technical Report workshop on DNA-based computers, April 4, 1995.

[W96] Winfree, E. *On the computational power of DNA annealing and ligation*, DNA based computers, Lipton, R.J. and Baum, E.B. eds., Am. Math. Soc., Providence, RI, (1996).

[Win98a] Winfree, E., *Simulations of computing by self-assembly*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[Win98b] Winfree, E., *Whiplash PCR for O(1) computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[WLW+98] Erik Winfree, Furong Liu, Lisa A. Wenzler, Nadrian C. Seeman, *Design and Self-Assembly of Two Dimensional DNA Crystals*, Nature 394: 539–544, 1998. (1998).

[WYS96] Winfree, E., X. Yang, N.C. Seeman, *Universal Computation via Self-assembly of DNA: Some Theory and Experiments*, 2nd Annual DIMACS Meeting on DNA Based Computers, Princeton, June, 1996.

[YK97a] Yokomori, T., and S. Kobayashi, *On the Power of Circular Splicing Systems and DNA Computability*, ICEC'97 Special Session on DNA Based Computation, Indiana, April, 1997.

[YK97b] Yokomori, T., and S. Kobayashi, *DNA-EC: A Model of DNA-Computing Based on Equality Checking*, 3rd DIMACS Meeting on DNA Based Computers, Univ. of Penns., (June, 1997).

[Woo98] Wood, D. H., *Applying error correcting codes to DNA computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[YAT+98] Yoshinobu, T., Y. Aoi, K. Tanizawa, Hiroshi Iwasaki, *Ligation errors in DNA computing*, 4th Int. Meeting on DNA-Based Computing, Baltimore, Penns., (June, 1998).

[ZS92] Zhang, Y., and N.C. Seeman, *A Solid-Support Methodology for the Construction of Geometrical Objects from DNA*, J. Am. Chem. Soc., **114**, 2656–2663, (1992).

[ZS94] Zhang, Y., and N.C. Seeman, *The Construction of a DNA Truncated Octahedron*, J. Am. Chem. Soc., **116**, 1661–1669, (1994).

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/qsense/qsense.ps), Accepted and to appear in Information and Computation, (1999).

[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).

[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 NMR 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).