Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 1634–1639, March 1997
Computer Sciences

Ensemble quantum computing by NMR spectroscopy

(NMR/quantum computing/DNA computing/nondeterministic polynomial-time complete)

DAVID G. CORY[‡], AMR F. FAHMY[§], AND TIMOTHY F. HAVEL[§¶]

[‡]Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139; and [§]Biological Chemistry and Molecular Pharmacology, Harvard Medical School, Boston, MA 02115

Communicated by Richard Karp, University of Washington, Seattle, WA, December 23, 1996 (received for review October 15, 1996)

ABSTRACT A quantum computer (QC) can operate in parallel on all its possible inputs at once, but the amount of information that can be extracted from the result is limited by the phenomenon of wave function collapse. We present a new computational model, which differs from a QC only in that the result of a measurement is the expectation value of the observable, rather than a random eigenvalue thereof. Such an expectation value QC can solve nondeterministic polynomial-time complete problems in polynomial time. This observation is significant precisely because the computational model can be realized, to a certain extent, by NMR spectroscopy on macroscopic ensembles of quantum spins, namely molecules in a test tube. This is made possible by identifying a manifold of statistical spin states, called pseudo-pure states, the mathematical description of which is isomorphic to that of an isolated spin system. The result is a novel NMR computer that can be programmed much like a QC, but in other respects more closely resembles a DNA computer. Most notably, when applied to intractable combinatorial problems, an NMR computer can use an amount of sample, rather than time, which grows exponentially with the size of the problem. Although NMR computers will be limited by current technology to exhaustive searches over only 15 to 20 bits, searches over as much as 50 bits are in principle possible, and more advanced algorithms could greatly extend the range of applicability of such machines.

Several physical implementations of computational models other than the standard von Neumann model have recently been proposed, which in principle scale better on certain types of computational problems. Most notably, Adleman (1) has solved a traveling salesman problem by DNA computing, and Shor (2) has shown theoretically that a quantum computer (QC) should be able to factorize integers in polynomial time. Nondeterministic polynomial-time complete (NP-complete) problems are a class of computationally intractable problems of particular interest, both because they are "polynomially equivalent" to one another and because they are encountered in many important applications (3–5). The traveling salesman problem includes a set of NP-complete instances, which indicates that DNA computing may someday be useful in solving NP-complete problems. In contrast, it is widely believed that a QC cannot solve NP-complete problems in polynomial time (6). Until now, however, only very small problems have been solved by DNA computing (7), and no one has yet succeeded in building a QC able to handle more than two bits of information (8–10).

In this paper, we consider another physical mechanism that is capable of computation, namely NMR spectroscopy. This approach is based on the fact that the spins in each molecule of a liquid sample are largely isolated from the spins in all other molecules. As a result, each molecule is effectively an independent QC. Via radio-frequency electromagnetic pulses, it is straightforward to manipulate each of the spins in every molecule identically across the sample, as in a synchronous, single-instruction parallel machine. Similarly, what one observes in an NMR spectrum is the sum of certain observables over all the molecules in the sample, which is proportional to the ensemble average expectation value of the observable. Thus, such a machine performs a calculation using quantum parallelism at the molecular level and then amplifies its results to the macroscopic level via a form of classical parallelism. We call a computer based on this principle an ensemble QC (EQC).

Other researchers have proposed implementing an atomic-scale QC by NMR and analogous physical mechanisms (e.g., refs. 8–11). The reason a macroscopic version has not previously been pursued lies in the fact that the magnetic moments of the individual spins are very small, so that even with superconducting magnets, it is not possible to perfectly align the spins at temperatures above ≈1 mK. This in turn makes it impossible to prepare a liquid sample in a pure state, in which the spin states of all the molecules are identical. We have solved this problem by introducing a new concept into NMR spectroscopy, called pseudo-pure states, the behavior of which is similar in many respects to a pure state. In particular, they can be described by a type of spinor, which evolves via unitary transformations under the Hamiltonians of NMR and whose expectation values are easily obtained from the corresponding ensemble-average expectation values. We call these spinors pseudo-spinors, to emphasize the fact that their physical interpretation differs from that of the spinors that describe isolated spin systems.

Such an NMR computer can be programmed electronically much like a QC, but it can be implemented using macroscopic liquid samples at room temperature and pressure like a DNA computer. In principle, it can also trade an exponential increase in the amount of time required to solve intractable combinatorial problems, including NP-complete problems, for an exponential increase in the size (physical dimensions) of the sample on which it operates. Preliminary experiments that validate this novel approach to computing have already been performed (12). Although scaling it to problems beyond the reach of conventional computers promises to be very difficult, the theoretical implications of such a machine are intriguing, and its general principles may prove more broadly applicable. Because these principles are derived from several very different fields, an elementary exposition is needed to provide a common knowledge base for future interdisciplinary research. That is the purpose of the present paper.

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "*advertisement*" in accordance with 18 U.S.C. §1734 solely to indicate this fact.

Abbreviations: QC, quantum computer; EQC, ensemble QC; EVQC, expectation value QC; SAT, satisfiability; NP-complete, nondeterministic polynomial-time complete.

[¶]To whom reprint requests should be addressed.

Quantum Computing and Exponential State Spaces

Because of its importance in what follows, we begin with a brief account of how a QC works; more detailed accounts may be found in refs. 10, 11, 13, and 14. A distinctive property of multiparticle quantum systems is that the dimensionality of their state space grows exponentially with the number of particles (15). This is because the Hilbert space for a system of distinguishable particles must be taken as the tensor product of the Hilbert spaces of the individual particles, to model the correlations among them. In particular, if one considers the spin dynamics of a system of n spin 1/2 particles, the Hilbert spaces of which are all of dimension two, the dimension of the Hilbert space of the combined system is 2^n. It is for this reason that many researchers have proposed constructing a QC from a system of spin particles, for example, in an ion trap (16).

The vectors (or "wave functions") in the Hilbert space of a system of spins are called spinors. The standard basis consists of the joint eigenvectors of the total and z-component of the spin angular momentum. The encoding used in quantum computing maps each integer k in the range $[0, 2^n - 1]$ to the kth basis element versus a particular ordering of the basis. For a single spin 1/2 particle, the basis consists of the spin "down" (antiparallel to the z-axis) state, which is represented by the vector $[1, 0]$ and is denoted by the "bra" $\langle 0|$, together with the spin "up" state, which is represented by the vector $[0, 1]$ and is denoted as $\langle 1|$; the corresponding column vectors are denoted by the "kets" $|0\rangle$ and $|1\rangle$, respectively. The basis vectors of an n-spin system are formed by taking the tensor or Kronecker products of the basis vectors of its constituent spins in some arbitrary but fixed order. The general definition of the Kronecker product $\otimes$ of an $M \times N$ matrix $\mathbf{A}$ with an $M' \times N'$ matrix $\mathbf{B}$ is the matrix $MM' \times NN'$ given by:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1N}\mathbf{B} \\ \cdots & \cdots & \cdots \\ a_{M1}\mathbf{B} & \cdots & a_{MN}\mathbf{B} \end{bmatrix},$$

$$\text{where} \quad \mathbf{A} = \begin{bmatrix} a_{11} & \cdots & a_{1N} \\ \cdots & \cdots & \cdots \\ a_{M1} & \cdots & a_{MN} \end{bmatrix}. \qquad \textbf{[1]}$$

Thus the basis vectors of a two-spin system are given by:

$$|00\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \equiv \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \quad |01\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \equiv \begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$

$$|10\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \equiv \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \quad |11\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \equiv \begin{bmatrix}0\\0\\0\\1\end{bmatrix}. \qquad \textbf{[2]}$$

In a QC, any logical operation on a register in the basis state $|k\rangle$ must transform it to another basis state $|l\rangle$. Because energy dissipation rapidly destroys microscopic order and hence the ability to store information, a QC must be essentially completely isolated from its surroundings. Isolated quantum systems naturally evolve by unitary transformations, which are necessarily reversible. This prevents one from implementing conventional logic gates, such as the AND gate. Fortunately, any gate can be made reversible by copying some of the input bits to the output bits. For example, the quantum XOR gate, which copies the first input bit and overwrites the second bit with its output, has the truth table shown on the left in Eq. **3.**

$$\begin{matrix} [1\ 0\ 0\ 0] \equiv \langle 00| & \to \langle 00| \equiv [1\ 0\ 0\ 0] \\ [0\ 1\ 0\ 0] \equiv \langle 01| & \to \langle 01| \equiv [0\ 1\ 0\ 0] \\ [0\ 0\ 1\ 0] \equiv \langle 10| & \to \langle 11| \equiv [0\ 0\ 0\ 1] \\ [0\ 0\ 0\ 1] \equiv \langle 11| & \to \langle 10| \equiv [0\ 0\ 1\ 0] \end{matrix} \Leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad \textbf{[3]}$$

The unitary matrix for the quantum XOR gate is shown on the right.

A nontrivial complex linear combination of the basis vectors is called a coherent superposition. Because unitary transformations are linear, the result of operating on a superposition is the same superposition of the results of the transformation applied to the individual basis states. In this sense, a QC can operate in parallel on exponentially many basis states at once. There are, however, serious problems with this approach. The first is that it promises to be very difficult to build a QC of any significant size, because it requires the precise assembly, isolation, control, and measurement of atomic-scale systems. A more fundamental problem lies in the fact that the amount of information that can be extracted from even perfectly precise measurements on quantum systems is extremely limited, because the act of observation irreversibly alters the system.

For example, if one places a two-spin system in the superposition

$$c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle = [c_0{}^* \ c_1{}^* \ c_2{}^* \ c_3{}^*]^\dagger, \qquad \textbf{[4]}$$

where * denotes the complex conjugate and † denotes the Hermitian transpose, and measures the z-component of the spins, one will observe one of the four basis states $k = 0, \ldots, 3$, each with probability $|c_k|^2 = c_k c_k{}^*$. The system is forced into the observed state by the act of observation, and all subsequent measurements of the same observable will therefore yield the same result. This phenomenon is sometimes called wave function collapse. Thus, it is not possible to completely determine the state of the system (i.e., the coefficients c_k) from a finite number of measurements on identically prepared copies of a given quantum system.

The Expectation Value QC (EVQC)

Let us imagine an abstract computer that functions like a quantum computer in every respect but one: instead of a random eigenvalue, the result of a measurement of an observable on the system is the expectation value of that observable. This computational model further assumes that the expectation value can be measured to arbitrarily high precision, and in an amount of time proportional to the number of digits in the result. We shall call our abstract computer an EVQC.

The following result serves as the motivation for much of the rest of this paper: an EVQC is capable of solving NP-complete problems in polynomial time.

We shall prove this by showing that an EVQC can solve a well known NP-complete problem, namely the satisfiability (SAT) problem (5), in linear time. In this problem, one is given a Boolean function f: $\{0, 1\}^n \to \{0, 1\}$ in conjunctive normal form. This is a logical conjunction of clauses, where each clause is a disjunction of Boolean variables or their negations. The variables are assigned values from the set $\{0, 1\}$, and such an assignment is said to satisfy f if the value of f on the assignment is 1. The SAT problem is then to determine if there exists a satisfying assignment for the function f.

If the state w of the system is given by the ket $|w\rangle$ versus a fixed basis, and $\mathbf{K}$ is the Hermitian matrix that represents some observable K versus the same basis, elementary quantum mechanics tells us that the expectation value of K is the value of the quadratic form $\langle w|\mathbf{K}|w\rangle$. Given a system of $n + 1$ spin 1/2 particles, we may represent each assignment $x \in \{0, 1\}^n$, together with the state of the $(n + 1)$th output bit $y \in \{0, 1\}$, by an elementary basis vector $|x, y\rangle$ in a Hilbert space of dimension 2^{n+1}. Using results from quantum computing (13), it is possible to convert the Boolean operations in f into a sequence of unitary transformations, the product of which, $\mathbf{U}_f$, applied to any single basis state $|x, 0\rangle$, yields $\mathbf{U}_f|x, 0\rangle = |x, f(x)\rangle$. If we now prepare the input in the superposition of all its possible states given by $\Sigma_{x\in\{0,1\}^n} c_{(x,0)}|x, 0\rangle$, where $c_{(x,0)} = 2^{-n/2}$ and $c_{(x,1)} = 0$ for all x, then the result of performing the computation on this superposition is

$$\mathbf{U}_f \sum\nolimits_{x\in\{0,1\}^n} c_{(x,0)}|x, 0\rangle = \sum\nolimits_{x\in\{0,1\}^n} c_{(x,0)}|x, f(x)\rangle$$
$$\equiv \sum\nolimits_{x\in\{0,1\}^n} d_{(x,f(x))}|x, f(x)\rangle \equiv z_f. \qquad [5]$$

There exists an observable S, with Hermitian matrix $\mathbf{S}$, such that the expectation value of S is $\langle z_f|\mathbf{S}|z_f\rangle = 2^{-n}|\{\mathrm{x} \in \{0, 1\}^{\mathrm{n}}|\mathrm{f(x)} = 1\}|$—i.e., 2^{-n} times the number of satisfying assignments. If the basis states $|x, y\rangle$ inherit the order of the integer for which each bit string (x,y) is the binary representation, then $\mathbf{S}$ is the diagonal matrix

$$\mathbf{S} = \mathbf{1} \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1} \otimes |1\rangle\langle 1|$$
$$= \mathbf{Diag}(0, 1, 0, 1, \cdots, 0, 1), \qquad [6]$$

where $\mathbf{1}$ is the 2 × 2 identity matrix and **Diag** is the diagonal matrix of its arguments. Since $\langle z_f|\mathbf{S}|z_f\rangle = \Sigma_{x\in\{0,1\}^n}|d_{(x,1)}|^2$ where each nonzero output coefficient $d_{(x,1)} = c_{(x,0)} = 2^{-n/2}$, the expectation value of S is the fraction of all assignments that satisfy the given function f, as claimed.

The time required to program $\mathbf{U}_f$, to prepare the superposition, and (in our computational model) to measure the expectation value of S to the requisite precision of 2^{-n}, are all $O(n)$, thus showing that an EVQC can solve SAT in linear time. Because all NP-complete problems are polynomially reducible to SAT by Cook's theorem (3), this proves that an EVQC can solve NP-complete problems in polynomial time. Since our EVQC essentially counts the number of satisfying assignments, we have further shown that it is capable of solving #P-complete problems in polynomial time (5).

It should be noted that the operator $S \equiv S_{n+1}$, the expectation value of which tells us the fraction of states in which the $(n + 1)$th spin is 1, can easily be altered to an operator S_k, the expectation value of which provides the same information about the kth spin. Thus given any computable function g: $\{0, 1\}^m \rightarrow \{0, 1\}^n$ and a unitary transformation $\mathbf{U}_g$ such that $\mathbf{U}_g|x, 0\rangle = |x, g(x)\rangle$, we can find the value of $g(x)$ on any single input state $x \in \{0, 1\}^m$ by simply measuring the expectation values of the n operators S_{m+1} through S_{m+n}. The implication is that any Turing computable function can be computed by an EVQC, and hence we can use implicit parallelism in any such computation by operating on a superposition.

Ensemble Quantum Computing and NMR Spectroscopy

An EVQC cannot be precisely realized by any finite physical system, but it can be approximated by an ensemble (large collection) of independent and identical QCs, over which one can measure the sum of the observable evaluated on each QC in the ensemble. Such an EQC performs a calculation using quantum parallelism and then uses a form of classical parallelism to estimate an expectation value. Although an EQC differs from a single QC in significant respects, it also depends on quantum parallelism in an essential way and cannot be equated with an ensemble of conventional computers. In particular, each QC in the ensemble operates on a superposition over all possible inputs, rather than different (or random) single inputs as in an ordinary massively parallel computer. Even more importantly, whereas conventional computers do not appear to occur naturally on the molecular scale, QCs do! In this section, we describe how this fact makes it possible to construct an EQC with ≈10^{23} QCs in it, using NMR spectroscopy. In the next section, we shall consider the physical limits on what such an NMR computer can do.

All atomic nuclei with intrinsic spin behave like tiny magnets (17). Therefore, when they are placed in a magnetic field, their magnetic dipoles tend to align themselves parallel to the field. The Hamiltonian that gives the energy difference between the parallel and antiparallel states is called the Zeeman Hamiltonian. Even with superconducting magnets, this energy difference is very small compared with the thermal energy $k_{\mathrm{B}}T$. Hence when a macroscopic ensemble of identical spins is placed in a magnetic field, the net alignment of their magnetic moments with the field is likewise very small at room temperature. If one could reduce the temperature sufficiently close to absolute zero, however, near perfect alignments would be obtained. Under these conditions, all the spins are in the same quantum state, which is described by saying that the ensemble as a whole is in a pure state.

In such a system, the magnetization of the sample is the sum of the magnetizations due to the individual spins. Each of the microscopic observations is a random variable, but when one takes the sum over a macroscopic number of observations, the result is a deterministic quantity equal to the expectation value of the observable times the number of spins. If all the spins in the ensemble were identical, we would only have a one-bit EQC. If all the spins were distinguishable, on the other hand, the result would be a massive QC, but without the ability to measure well defined expectation values. What is needed is a partition of the spins into distinguishable equivalence classes of indistinguishable spins. Fortunately, such a partitioning occurs very naturally in chemistry, where the spin-active nuclei in a molecule are distinguished by their electronic environments, but in a macroscopic sample of identical molecules, each type of spin is indistinguishable between molecules.

A standard technique in NMR spectroscopy is to use pulses of radio-frequency radiation to transform the state of the spins by unitary transformations. Since the inequivalent spins in a molecule generally have distinct resonance frequencies, the frequency range of these pulses can be made selective for single spins. For example, a selective pulse that imparts sufficient energy to rotate the net magnetization of the kth spin by $\pi/2$ and is in-phase with the imaginary component of the carrier corresponds to the unitary matrix

$$\mathbf{1} \otimes \cdots \otimes \mathbf{1} \otimes \mathbf{U}_{\pi/2} \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1}$$
$$\left(\mathbf{U}_{\pi/2} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\right), \qquad [7]$$

where the matrix $\mathbf{U}_{\pi/2}$ occurs as the kth factor of the Kronecker product.

For a two-spin system, we have the energy level diagram shown in Fig. 1. The four dashed double-headed arrows are the

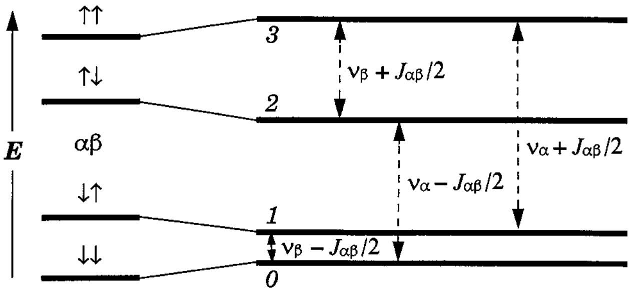
↑↑
↑↓
αβ
↓↑
↓↓
E
3
2
1
0
$\nu_\beta + J_{\alpha\beta}/2$
$\nu_\alpha - J_{\alpha\beta}/2$
$\nu_\alpha + J_{\alpha\beta}/2$
$\nu_\beta - J_{\alpha\beta}/2$

FIG. 1. The four energy levels associated with two spins α and β, whose resonance frequencies are ν_α and ν_β (in Hz). The energy levels when there is no coupling between the spins are shown on the left, and those with a coupling of $J_{\alpha\beta}$ (in Hz) on the right. The allowed transitions between the energy levels are indicated with dashed double-headed arrows.

transitions allowed by the selection rules for angular momenta, and they connect pairs of states that differ by only single spin flips (i.e., pairs with a Hamming distance of 1). The spins are generally also coupled to one another, either by through-space dipole–dipole interactions or by a through-bond effect called scalar coupling. This coupling causes the energy differences associated with the various transitions to be generically distinct. Tipping both spins into the *xy*-plane with a nonselective $\pi/2$ pulse $\mathbf{U}_{\pi/2} \otimes \mathbf{U}_{\pi/2}$ causes them to precess in phase, generating a detectable (macroscopic) rotating magnetic moment. The real part of the Fourier transform of the resulting signal gives an NMR spectrum with two pairs of peaks, as shown in Fig. 2. The intensity of each pair is proportional to the total population difference between states in which the corresponding spin is up and those in which it is down.

The quantum XOR gate introduced above flips one of these spins, given that the other spin is up, which in turn corresponds to the transitions 1–3 and 2–3, for an output on the first and second spins, respectively. Thus, one can implement the quantum XOR gate by a single radio-frequency pulse, the frequency range of which spans only the peak of one of these transitions, and which imparts sufficient energy to invert the populations of the corresponding pair of states. This is an example of a Pound–Overhauser double resonance experiment (17). More generally, we have shown that one can implement the universal Toffoli gate via NMR pulse sequences and hence compute any desired Boolean function by these means (12). In particular, the unitary transformation $\mathbf{U}_f$ needed to compute the Boolean function f in SAT can be performed by an appropriate pulse sequence.

The expectation value of the operator S in the SAT algorithm above corresponds to the sum of the intensities of the 2^n peaks that are obtained by flipping the $(n + 1)$th spin. For a two-spin system, the matrix $\mathbf{S} = \mathbf{S}_2$ can be written in terms of the operators $\mathbf{P}_{01} = \mathbf{Diag}(1,-1,0,0)$ and $\mathbf{P}_{23} = \mathbf{Diag}(0,0,1,-1)$, the expectation values of which give the population differences between the subscript states (and hence the intensities of the corresponding peaks), as

$$\mathbf{S}_2 = (\mathbf{1} \otimes \mathbf{1} - \mathbf{P}_{01} - \mathbf{P}_{23})/2 = (\mathbf{1} \otimes \mathbf{1} - \mathbf{1} \otimes \mathbf{I}_z)/2, \quad \mathbf{[8]}$$

where $\mathbf{I}_z = \mathbf{Diag}(1,-1)$ is the matrix of the operator for the *z*-component of the spin. Finally, a superposition in which all the basis states are equiprobable is easily obtained by applying a $\pi/2$ pulse with a frequency range that spans all the peaks, due to flips of the input spins, but which misses those peaks due to the output spin. Thus the SAT problem is easily and naturally solved by NMR spectroscopy, at least in small instances.

The Physical Limitations of NMR Computing

Although straightforward in principle, there are several theoretical and practical considerations that limit how large of a problem can be solved by an NMR implementation of an EQC. In this section we shall consider the most important such obstacles and, where possible, establish bounds on the corresponding limits. In the following, we denote the number of spins in a molecule by n, the number of molecules present in the sample by M, and the total number of spins by $N = nM$.

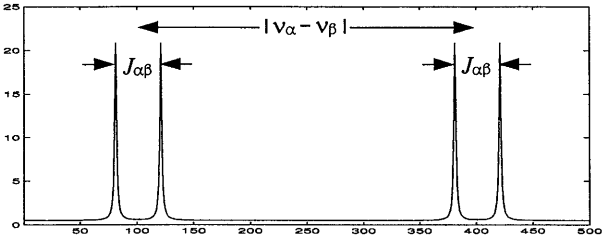

FIG. 2. The simulated NMR spectrum of a two-spin system, with $\nu_\alpha = 100$ Hz, $\nu_\beta = 400$ Hz, and $J_{\alpha\beta} = 40$ Hz. From left to right, the four peaks in this spectrum correspond to the transitions 0 ↔ 1, 2 ↔ 3, 0 ↔ 2, and 1 ↔ 3 indicated in Fig. 1 (be forewarned, however, that NMR spectroscopists traditionally plot their spectra with frequency increasing from right to left). In practice, this spectrum would be obtained by applying a nonselective $\pi/2$ pulse to the equilibrium state and Fourier transforming the resulting signal.

The mean-square error in an estimated expectation value is σ^2/M, where the variance σ^2 depends on the problem instance. To reliably solve, for example, a SAT problem on n variables, this error must be less than 2^{-2n}, but the resulting bound on n depends on σ^2. To avoid this, we instead require only that at least one molecule samples at least one solution with at least some fixed probability $p_{\min}$. This probability is given by $p = 1 - e^{-r}$, where $r = M/2^n$ is the average number of molecules per state. The result turns out to depend on $p_{\min}$ only through the term $\log(\log((1 - p_{\min})^{-1}))$, and hence we shall simply set $p_{\min} = 1 - e^{-1}$—i.e., $r > 1$. We typically have $N \approx 10^{23} \approx 2^{76}$ in an NMR sample, so if we wish to solve a problem of size n, we would have $M \approx 2^{76}/n$, or $r \approx 2^{76}/(n2^n)$. This leads to the approximate bound

$$(n2^n < 2^{76}) \Rightarrow (\log_2(n) + n < 76) \Rightarrow (n < 70). \quad \mathbf{[9]}$$

This bound on the number of bits over which we can perform a reliable search for a single desired state can be increased by 7 or 8 by time-averaging the signals, and perhaps as much as 10 by using very large samples. Because the number of bits that can be handled depends logarithmically on the number of repetitions and/or size, the absolute limit on what any practical NMR computer can handle remains well below 100 bits. In practice, the finite signal-to-noise ratio of the receiver will reduce these estimates substantially. These estimates, however, apply only to solving combinatorial problems by exhaustive search. With the use of more sophisticated search procedures, it may be possible to reduce the rate of growth in the sample size required and so go considerably larger. It is also conceivable that algorithms for some problems exist that can be implemented more efficiently (in terms of time) on an NMR computer than they can be on conventional or QCs, using only a fixed sample size.

Several other obstacles to scaling an NMR computer to large problems also exist, but it is more difficult to establish hard bounds on the size of the problem that these obstacles permit us to solve. For example, it is difficult to find molecules with more than ≈10 spins in them and with a large coupling constant between every pair of spins (particularly if one is relying upon only scalar coupling). In addition, the number of peaks that can be independently resolved in the NMR spectrum of a molecule is limited by both the separation as well as the width of the peaks. Nevertheless, we need only find one suitable molecule (out of the myriads available in chemistry) to obtain a general EQC on that number of spins. As a result, we do not expect this obstacle to be the ultimate bottleneck.

The width of the peaks is also important because it is equal to the inverse spin–spin relaxation time T_2, otherwise known as the decoherence time in quantum computing. Since decoherence introduces errors into the intermediate results, it limits the time available for computation. The difficulty of isolating microscopic systems from their environment well enough to attain long decoherence times has proven to be one of the chief obstacles to implementing a true QC. In contrast, the nuclear spins in a molecule are generally quite well isolated from its motional and electronic degrees of freedom.

In solids, the dominant mechanism of spin–spin relaxation is the dipole–dipole interaction, which typically results in decoherence times of a small fraction of a millisecond. In liquids, on the other hand, the dipole–dipole interaction is averaged to zero by the rapid rotational diffusion of nearby molecules, leading to decoherence times that can be on the order of many seconds. The intramolecular scalar couplings between spins, however, are not averaged to zero, and can exceed 100 Hz. The number of selective pulses that can be used in one experiment, which is of order the ratio of the coupling constants to the decoherence rate, can therefore be over a thousand. It is possible that error correcting schemes like those proposed to control decoherence and other errors in quantum computation (21) can be developed for NMR computing, further increasing the time available for computation.

More importantly, this dipolar averaging effect largely isolates the spins in different molecules from one another, thus making each molecule into an independent QC. It follows that liquid NMR samples are an extremely suitable means of implementing an EQC. Unfortunately, the small energies associated with the Zeeman Hamiltonian make it impossible to prepare a pure state at temperatures above about 10^{-3} K, but molecules do not remain in the liquid state as one approaches the absolute zero of temperature. For this reason we have developed a novel means of simulating pure states at room temperature.

Pseudo-Pure States

A mixed state is a statistical mixture of independent quantum systems that are not all in the same quantum state. The mixed states of spin systems are described by a generalization of spinors, known as the density matrix, that enables us to compute their statistical properties (18). The density matrix Ψ of a pure state is obtained from the corresponding spinor ψ simply by taking a dyadic product—i.e., $\Psi = |\psi\rangle\langle\psi|$. Such a density matrix is necessarily an idempotent projection operator that has only one nonzero eigenvalue with the value 1. In the case of a two-spin system in the state $|00\rangle$, for example, we have $\Psi = |00\rangle\langle 00| = \mathbf{Diag}(1,0,0,0)$. The density matrix of a mixed state is obtained by taking the average of the density matrix over a representative ensemble of pure states—i.e.,

$$\Psi = \int_{\{\psi\}} p(\psi)\, |\psi\rangle\langle\psi|\, d\psi, \qquad \textbf{[10]}$$

where $p(\psi)$ is the probability density of the pure state described by the spinor ψ and $\{\psi\}$ denotes the set of all unit norm spinors. Thus a density matrix can be an arbitrary positive semi-definite Hermitian matrix normalized to unit trace. In a basis of eigenstates of the Hamiltonian, the diagonal elements are the relative populations of the various energy levels, while the off-diagonal elements represent coherences—i.e., correlations in the phases of precessing spins in pairs of energy levels across the sample.

Eq. **10** is usually regarded as a Gibbs ensemble average, which is a purely thought construction used to compute time averages. As described above, however, the spins in the different molecules of a liquid are essentially independent of one another. As a consequence, a large number of copies of a single type of molecule in a liquid sample constitutes an excellent physical approximation to a Gibbs ensemble, at least for the spin degrees of freedom. The result is that we can work with a reduced density matrix Ψ of size 2^n, where n is the number of spins in a single molecule, rather than a density matrix of size 2^N, where $N = nM$ is the total number of spins in the sample.

The (reduced) density matrix evolves in time according to the Liouville–von Neumann equation

$$d\Psi/dt = i[\Psi, \mathbf{H}] = i(\Psi\mathbf{H} - \mathbf{H}\Psi), \qquad \textbf{[11]}$$

where $\mathbf{H}$ is a matrix representation of the spin Hamiltonian of the molecule, and $[\Psi,\mathbf{H}]$ denotes the matrix commutator. This has the general solution

$$\Psi(t) = \mathbf{U}(t)\Psi(0)\mathbf{U}^{\dagger}(t), \qquad \textbf{[12]}$$

where $\mathbf{U}(t)$ is a time-dependent unitary matrix. For a time-independent Hamiltonian, this matrix has the form $\mathbf{U}(t) = \mathbf{Exp}(-it\mathbf{H})$. Finally, the ensemble average of the expectation value of any observable K is obtained as the trace product $\mathrm{tr}(\mathbf{K}\Psi)$ of the corresponding matrix $\mathbf{K}$ with the density matrix.

We define a pseudo-pure state to be one that has a density matrix that can be shifted by adding a multiple of the unit matrix to it so as to obtain a scalar multiple of the density matrix of a pure state. Such a density matrix can be written as

$$\Psi = \frac{(1-\alpha)\mathbf{1} + 2\alpha|\psi\rangle\langle\psi|}{(1-\alpha)2^n + 2\alpha} \quad (-1 \leq \alpha \leq 1), \qquad \textbf{[13]}$$

where $|\psi\rangle$ is a unit spinor. In other words, it is a unit trace Hermitian matrix of size $2^n \times 2^n$, with eigenvalues that lie in the interval [0,1], and with $2^n - 1$ of them degenerate. The spinor $|\psi\rangle$ in Eq. **13** will be called a pseudo-spinor, to emphasize the fact that its physical interpretation differs from that of the spinor for an isolated spin system.

Pseudo-pure states promise to be of great utility in implementing an EQC for the following reasons. (*i*) Each pseudo-spinor determines a unique pseudo-pure density matrix via Eq. **13** above, and each pseudo-pure density matrix determines a pseudo-spinor that is unique up to an overall phase factor (assuming that the polarization α is known). (*ii*) When the density matrix of a pseudo-pure state (as in Eq. **13**) is transformed by a given unitary transformation (as in Eq. **12**), the corresponding pseudo-spinor is transformed by the same unitary matrix, since $\mathbf{U}\Psi\mathbf{U}^{\dagger} \propto (1-\alpha)\mathbf{1} + 2\alpha(\mathbf{U}|\psi\rangle)(\mathbf{U}|\psi\rangle)^{\dagger}$. (*iii*) The ensemble average expectation value of an observable versus a pseudo-pure density matrix as in Eq. **13** yields the ordinary expectation value of the observable versus the corresponding pseudo-spinor, since $\mathrm{tr}(\mathbf{K}\Psi) \propto (1-\alpha)\mathrm{tr}(\mathbf{K}) + 2\alpha\langle\psi|\mathbf{K}|\psi\rangle$, where $\mathrm{tr}(\mathbf{K})$ is a known constant.

The molecules of a sample in a pseudo-pure state are in a statistical mixture of quantum states. Nevertheless, there is a preponderance of one particular state present, which manifests itself when we add up the magnetizations of all the molecules, in effect making each molecule cast its "vote" for the final spectrum. The net result is that we can "emulate" a QC by NMR spectroscopy on macroscopic liquid samples in open test tubes at room temperature and pressure. Moreover, the number of operations required to do this is identical to the number of operations executed by the QC! The only real difference is that one can determine the state of the system in terms of its expectation values without wave function collapse, which shows that the requirement for an exponential state space is logically and physically distinct from the probabilistic aspects of quantum computing. For an experimental demonstration of the fact that one can apply quantum logic gates to coherent superpositions of pseudo-spinors, please see ref. 12.

The price one pays for using pseudo-pure states in NMR samples at room temperature is the loss of a factor of about one million in the effective number of molecules per state, because even with superconducting magnets, the net polarization of the spins is only about one part in a million. Since this factor figures only logarithmically in the physical limits (Eq. **9**), we can in principle still perform exhaustive searches over as many as 50 bits using an NMR computer with ordinary liquid samples. Of course, a number of practical considerations will limit us to substantially smaller problems, at least using the presently available materials and technologies. Prominent among these is the signal-to-noise ratio that can be attained with conventional electronics at room temperatures, which will probably make exhaustive searches over all inputs on more than ≈15–20 bits impractical in the foreseeable future. This should nevertheless be sufficient to motivate considerable research into alternative materials, technologies, and perhaps algorithms that enable us to push these limits back yet further.

Conclusions

Researchers today are divided concerning whether or not it will ever be possible to build a QC of any significant size. We have described a macroscopic analogue of a QC that can be implemented today, using commercially available NMR spectrometers and ordinary liquid samples. Such an NMR computer differs from a QC in that it uses the parallelism inherent in macroscopic ensembles to estimate expectation values, instead of the filtering and amplification concomitant upon wave function collapse. This enables it to efficiently solve a wider variety of problems, including NP-complete problems, although it may need an exponentially increasing sample size to do so.

A classical parallel computer can also use an exponentially increasing number of processors to achieve exponential speedups, but the only other type of machine that has been implemented with anything approaching 10^{23} "processors" in it is a DNA computer. Unlike a DNA computer, however, an NMR computer can be fully programmed by purely electronic means, much like a QC in principle could be. The fact that one can combine quantum parallelism with thermodynamic averaging to actually implement a machine with many of the advantages of both DNA and quantum computing is decidedly nontrivial.

The experimental issues involved in NMR computing, and in particular general methods for the preparation of pseudopure states, are being investigated (unpublished work; see also ref. 12). Despite its acknowledged limitations, it is possible that an NMR computer (or possibly some other type of EQC) will someday be built that can (with suitable algorithms) solve problems beyond the reach of conventional computers. Besides NP-complete problems, an NMR computer should be able to factorize integers by either a direct search procedure, or possibly by procedures based on Miller's approach which scale better (2, 11). Another likely application would be to simulate the statistical behavior of open quantum systems, as originally proposed for closed quantum systems using QCs by R. P. Feynman (see ref. 19). These theoretical questions are likewise under study (unpublished work).

Note. Gershenfeld and Chuang also presented many of the same ideas described in this paper at the workshop cited in ref. 12 and have recently published a paper on the subject (20).

We thank G. Wagner (Harvard Medical School) and R. Griffin (Massachusetts Institute of Technology) for their support and encouragement. This work was funded by National Science Foundation Grants MCB 9527181 and BIR 9511892 (T.F.H.) and DMR 9357603 (D.G.C.).

1. Adleman, L. (1994) *Science* **266,** 1021–1024.
2. Shor, P. W. (1994) *Proceedings of the 35th Symposium on Foundations of Computer Science.* (IEEE Press, Los Alamitos, CA), 124–134.
3. Cook, S. A. (1971) *Proceedings of the Third Annual ACM Symposium on Theory of Computing* (Assoc. for Comput. Machinery, New York), pp. 151–158.
4. Karp, R. M. (1972) in *Complexity of Computer Computations*, eds. Miller, R. E. & Thatcher, J. W. (Plenum, New York), 85–103.
5. Garey, M. R. & Johnson, D. S. (1979) *Computers and Intractability* (Freeman, San Francisco).
6. Bennett, C. H., Bernstein, E., Brassard, G. & Vazirani, U. (1997) *SIAM J. Comput.*, in press.
7. Lipton, R. J. (1995) *Science* **268,** 542–545.
8. Lloyd, S. (1993) *Science* **261,** 1569–1571.
9. Lloyd, S. (1994) *Science* **263,** 695.
10. DiVincenzo, D. P. (1995) *Science* **270,** 255–261.
11. Ekert, A. and Jozsa, R. (1996) *Rev. Mod. Phys.* **68,** 733–753.
12. Cory, D. G., Fahmy, A. F. & Havel, T. F. (1996) Proceedings of the Fourth Workshop on Physics and Computation, Nov. 22–24, 1996 (N. Engl. Complex Syst. Inst., Cambridge, MA), pp. 87–91 (abstr.).
13. Deutsch, D. (1989) *Proc. R. Soc. London A* **425,** 73–90.
14. Brassard, G. (1995) in *Computer Science Today*, Lecture Notes in Computer Science No. 1000, ed. van Leeuwen, J. (Springer, Berlin), 1–14.
15. Cohen-Tannoudji, C., Diu, B. & Laloë, F. (1977) *Quantum Mechanics* (Wiley, New York), Vols. 1 and 2.
16. Cirac, J. I. & Zoller, P. (1995) *Phys. Rev. Lett.* **74,** 4091–4094.
17. Slichter, C. P. (1990) *Principles of Magnetic Resonance* (Springer, Berlin), 3rd Ed.
18. Blum, K. (1981) *Density Matrix Theory and Applications* (Plenum, New York).
19. Lloyd, S. (1996) *Science* **273,** 1073–1078.
20. Gershenfeld, N. A. & Chuang, I. L. (1996) *Science* **275,** 350–356.
21. Shor, P. W. (1996) *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Press, Los Alamitos, CA), pp. 56–65.