Quantum Computers, Factoring, and Decoherence

I. L. Chuang, R. Laflamme, P. W. Shor, W. H. Zurek

It is known that quantum computers can dramatically speed up the task of finding factors of large numbers, a problem of practical significance for cryptographic applications. Factors of an L-digit number can be found in $\sim L^2$ time [compared to $\sim\exp(L^{1/3})$ time] by a quantum computer, which simultaneously follows all paths corresponding to distinct classical inputs, obtaining the solution from the coherent quantum interference of the alternatives. Here it is shown how the decoherence process degrades the interference pattern that emerges from the quantum factoring algorithm. For a quantum computer performing logical operations, an exponential decay of quantum coherence is inevitable. However, even in the presence of exponential decoherence, quantum computation can be useful as long as a sufficiently low decoherence rate can be achieved to allow meaningful results to be extracted from the calculation.

The uniqueness of the prime factorization of a positive integer is the Fundamental Theorem of Arithmetic (*1*). In practice, the determination of the prime factors of a given number can be an exceedingly difficult problem, even though verification is trivial. This asymmetry is the basis for modern cryptography and provides secret codes used not only on your own bank card but also to transfer diplomatic messages between embassies.

Attempts to undermine the security provided by the difficulty of factorization have by and large met with failure, even with the aid of powerful modern computers. In fact, this problem is widely believed to have no polynomial-time solution (*2*), although a proof of this statement has remained elusive. The best known classical computer algorithm (*3*) for factoring a number N of L digits takes a time exponential in $L^{1/3}$. In contrast, Shor (*4*) has shown recently that with the help of a quantum computer, one can factor numbers in a random polynomial amount of time. Therefore, such computers could be a threat to what is presently one of the most common methods of encryption. However, it is still unknown whether such machines are practical, because they depend crucially on quantum-mechanical behavior that is uncommon to our mostly classical world (*5*).

The quantum factoring algorithm uses in an essential way the coherence of a quantum wave function. To factor a number N, one chooses a number x at random and calculates its order, r, modulo N, that is, one finds r such that $x^r \equiv 1 \bmod N$. Once r is known, factors of N may likely be found by computing the greatest common divisor of $x^{r/2} \pm 1$ and N (*1*, *4*). The difficulty is in calculating r, which is solved by the quantum factoring algorithm: First choose a smooth number (one with small prime factors) q such that $N^2 < q < 2N^2$ and build the state

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a,0\rangle \qquad (1)$$

from which can be obtained (with a quantum computer) (*6*)

$$|\psi_2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod N\rangle \qquad (2)$$

We can now Fourier transform this pure state (again, with a quantum computer) to get

$$|\psi_3\rangle = \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \sum_{a=0}^{q-1} e^{i2\pi am/q} |m, x^a \bmod N\rangle \qquad (3)$$

and can measure both arguments of this superposition, obtaining the value c for m in the first argument and some x^k as the answer for the second one (k being any number between 0 and r). Given the pure state $|\psi_3\rangle$, probabilities of different results for this measurement will be given by the probability distribution

$$P(c,x^k) = \left| \frac{1}{q} \sum_{a=0}^{q-1}{}' e^{i2\pi ac/q} \right|^2 \qquad (4)$$

where the prime indicates a restricted sum over values of a that satisfy $x^a \equiv x^k \bmod N$. Independent of k, $P(c, x^k)$ is periodic in c with period q/r, but because we know q, we can determine r with a few trial executions [an example of $P(c, x^k)$ is shown in Fig. 1]. A measurement thus gives with high probability $c = \lambda q/r$, where λ is an integer that corresponds to a particular peak in Fig. 1. With a few runs of the program, we can deduce r and thus the factors of N.

This algorithm assumes that the quantum computer is completely isolated. In practice this will certainly not be the case. It is the effect of imperfect isolation that we study here. An obvious effect is that the quantum computer will lose energy. This happens at the rate τ_{rel}^{-1}, the inverse of the relaxation time scale. It is relatively easy to make systems for which τ_{rel} can be very large and thus allow for a reasonable number of operations. A much more insidious effect of imperfect isolation is decoherence (*7*). Decoherence is caused by continuous interaction between the system (in our case, the quantum computer) and the environment (*7*, *8*). As a result, the state of the environment "monitors," and therefore becomes correlated with, the state of the computer. As a quantum system evolves, information about its states leaks out into the environment, causing the states to loose their purity and, consequently, their ability to interfere.

It is important to realize that the time scale for decoherence τ_{dec} is usually much smaller than the one for relaxation. For example, an oscillator of mass m in a superposition of coherent states (separated by a distance Δx from each other) interacting linearly with a bath at temperature T has the decoherence time (*9*)

$$\tau_{dec} \sim \tau_{rel} \left(\frac{\lambda_{dB}}{\Delta x} \right)^2 \qquad (5)$$

where λ_{dB} is the thermal de Broglie wavelength. This expression is valid for high temperatures only; at low temperatures, τ_{dec} becomes inversely proportional to the cutoff frequency of the bath. No net energy transfer is needed to effect decoherence. This implies a much greater sensitivity of quantum computation to decoherence than to the relaxation process.

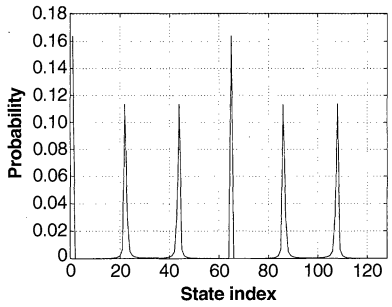

Fig. 1. Probability distribution for the measurement of c in the state given in Eq. 3 with $N = 21$, $q = 128$, $x = 5$, and $k = 3$. The broadening of the peaks is from the use of a discrete Fourier transform with q possible modes; a continuous Fourier transform would have given delta functions.

I. L. Chuang, Edward L. Ginzton Laboratory, Stanford University, Stanford, CA 94305, USA.
R. Laflamme and W. H. Zurek, Theoretical Astrophysics, T-6, MS B288, Los Alamos National Laboratory, Los Alamos, NM 87545, USA.
P. W. Shor, AT&T Bell Labs, 600 Mountain Avenue, Murray Hill, NJ 07974, USA.

The decoherence process has been proposed as a mechanism for enforcing classical behavior in the macroscopic realm. Decoherence results in environment-induced superselection (*7*– *9*), which destroys superpositions between the states of a preferred pointer basis (a set of states selected by the interaction with the environment) (*8*). Classical computers are already decohered: computation takes them through a predictable sequence of such pointer states, which are stable in spite of the environment; thus, classical computers cannot be put in arbitrary superpositions. However, coupling with the environment will be inevitable for any system that implements quantum computation. Here we show the effect of decoherence on the interference pattern produced as a result of executing the quantum factoring algorithm.

Our model involves the introduction of the environment as a system external to the computer; its state is represented by third label. The input state may thus be written as

$$|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle \otimes |\varepsilon \qquad (6)$$

where ε is the initial state of the environment and $\otimes$ is the direct product of vector spaces. The environment is initially uncorrelated with the computer; however, it is likely that the bits necessary for the calculation of x^a mod N will interact with the environment, so that the next state

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod N\rangle \otimes |\varepsilon_a\rangle \qquad (7)$$

leaves the environment partially correlated with the state of the computer. When the physical representation for the computer's quantum bits is diagonal in the pointer basis of the environment, decoherence results in no adverse effects when measuring the second label of $|\tilde{\psi}_2\rangle$. Such a design would be optimal. We thus focus on the effects of decoherence on the first label by suppressing the second label and tracing over the environment to obtain the reduced density matrix

$$\rho_{\text{red}} = \sum_{a=0}^{q-1}{}' \sum_{a'=0}^{q-1}{}' (1 - \beta_{aa'}) |a\rangle \langle a'| \qquad (8)$$

Here $1 - \beta_{aa'} = |\langle \varepsilon_a | \varepsilon_{a'} \rangle|^2$ is a measure of the extent to which the state of the environment has become correlated with the state of the quantum computer. If $|a\rangle$ and $|a'\rangle$ are quantum bit (qubit) register states diagonal in the pointer basis, then we may take

$$1 - \beta_{aa} \approx \exp[-\xi \cdot (a \text{ XOR } a')] \qquad (9)$$

where the exclusive-or (XOR) function gives the Hamming distance (*10*) between a and a'. Decoherence is characterized by a parameter ξ, which depends on the particular realization of the quantum computer. The measurement results in a probability distribution, shown in Fig. 2, which differs from the one in Eq. 4 (see Fig. 1) in that non-zero-probabilities have appeared between the peaks and that these peaks have decreased in amplitude. Note that decoherence does not increase the width of the peaks.

The qualitative effect of decoherence is well approximated by the simpler function $1 - \beta_{aa} \equiv 1 - \beta(1 - \delta_{aa'})$, where β is a constant. For $\beta = 0$ we get the state with complete coherence, and for $\beta = 1$ one with complete decoherence (that is, a matrix diagonal in the pointer states). In the limit of $\beta \sim 0$, we may understand β as the fractional amount of information lost to the environment. For $\beta \approx 0.5$, the probability between the peaks (Fig. 2) is equal to one of the peaks, and thus there is as much chance to get a correct answer as a wrong one. Let $L = \log N$. Once $(1 - \beta)^{-1} \sim O[\exp(L^{1/3})]$, the quantum computer becomes as inefficient as a classical one, requiring a number of trials exponential in $L^{1/3}$ to factor N. Note that β is analogous to the ratio between the amplitude of the destructive and constructive interference in the double-slit experiment, also called the fringe visibility function.

When we assume that the effect of the environment has a Markoffian character, then $\beta \approx 1 - e^{-n_{\text{op}}\alpha M} \approx n_{\text{op}}\alpha M$, where α is the coherence lost per bit in a single logic operation, M is the number of memory qubits involved, and n_{op} is the number of time steps required to complete the computation. To factor a number $N \sim e^L$, the quantum algorithm requires $M \sim L$ and $n_{\text{op}} \sim L^2$. With perfect operation, each execution gives a factor with probability $O(1/L)$, and thus with decoherence, the required number of trials is $O(L/(1 - \beta))$. When this is expressed in terms of α and L, the number of trials required find a factor of N is of order

$$\text{Number of trials} \sim L\exp(L^3\alpha) \qquad (10)$$

To give performance better than the classical algorithm, we must therefore have

$$\alpha < L^{-8/3} \qquad (11)$$

Designs for quantum computers have been suggested (*11*– *14*) and some possible difficulties investigated (*5*, *15*). Common to these designs is the model of a simple two-state system (qubit) interacting with an ensemble of oscillators (the environment), from which we can get an idea of what α is. Such an analysis, with the well-studied spin-boson Hamiltonian (*16*), straightforwardly gives the result that in a typical time step of a quantum computer, the effect of coupling to a zero-temperature environment is to decrease the off-diagonal term of the density matrix by the amount (*17*)

$$\alpha \approx \frac{\varepsilon^2\eta}{2\pi}\left[O(1) - \log\left(\frac{\Delta}{\Lambda}\right)\right] \approx \frac{\gamma}{\Delta} \qquad (12)$$

where ε is the (dimensionless) coupling strength, η is the resulting viscosity on the qubit (which will determine the rate of the loss of energy), Λ is a high-frequency cut-off of the bath, Δ^{-1} defines the time scale of a single operation, and γ is coherence lost per unit time. For example, in the experimental realization of an ion-trap quantum logic gate by Monroe *et al.* (*18*), $\gamma \approx 10^3$ Hz and $\Delta \approx 10^4$ Hz. This gives $\alpha \approx 0.1$, which implies that a quantum computer would outperform a classical one only for a number no more than a few bits in length. On the other hand, the original proposal of Cirac and Zoller (*14*) assumes that the ultimate source of errors will be spontaneous emission and estimates that $\gamma \approx 0.1$ Hz and $\Delta \approx 10^5$ Hz, which naïvely gives $\alpha \approx 10^{-6}$. This value would allow factoring of a number of perhaps a few hundred bits. Although the latter estimate is promising, we stress that it may be overly optimistic, because γ does not reflect all of the decoherence processes that may be taking place.

Unruh has also analyzed the impact of decoherence on quantum computation (*15*). He computed the behavior of a static memory, which exhibited three regimes of the decay of coherence of a qubit [an early one depending on the state of the qubit; a "quantum" regime where $\beta \sim 1/(\lambda t)$; and a "thermal" regime that starts at $\hbar/k_B T$ (k_B, Boltzmann's constant)] in which $\beta \sim \exp(-\varepsilon^2 Tt)$, and concluded that the time taken by the quantum computer to complete the calculation must be smaller than the (thermal) time scale for which the decoherence (β) becomes exponential. We differ with these conclusions on two counts.

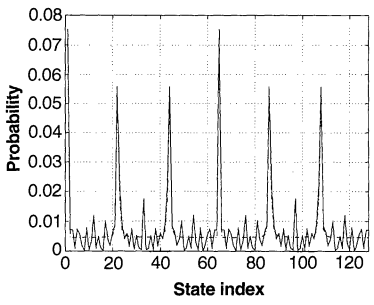

Fig. 2. Effect of decoherence on the probability distribution for the value of c. The state is given by Eq. 8 once a is Fourier transformed. The decoherence parameter (Eq. 9) has been taken to be $\xi = 0.1$. Our constant-beta approximation, with $\beta = 0.58$ (dash-dotted line), shows good agreement.

(i) When the computer is carrying out operations (rather than just trying to remember some state), the decay of quantum coherence is inevitably exponential even in the limit of zero temperature. Nevertheless, (ii) exponential decay is not a reason to give up: It is the rate of that decay that ultimately matters. This rate is given by Eq. 12 in the case studied here, and by $\varepsilon^2 k_B T/\hbar\Delta$ for the temperature-dominated regime. In either case, by increasing isolation (that is, by making ε small) and making the clock rate Δ large, one can take the computation well beyond the time scale (thermal or otherwise) when the loss of coherence becomes exponential with time.

Ultimately, the savior of general-purpose quantum computing lies in the success of quantum error correction. It is generally true that the discrepancy between the correct state of a quantum computer and the actual state will initially increase only quadratically in time (t)

$$|\langle\psi_{\text{actual}}|\psi_{\text{ideal}}\rangle|^2 \simeq 1 - (\delta t)^2 \qquad (13)$$

where δ is the variance of the difference between the ideal and actual energy. Thus, the "watchdog effect" can be used to stabilize the computation (*19*), for when the computer is measured often enough, on a time scale t/ν that is short compared with $1/\delta$, it will stray from the correct evolution only a little, so that the probability of being correct is

$$|\langle\psi_{\text{actual}}|\psi_{\text{ideal}}\rangle|^2 \simeq \left[1 - \left(\frac{\delta t}{\nu}\right)^2\right]^\nu \qquad (14)$$

which can be much closer to unity than Eq. 13. Performing a measurement on a qubit at the instants when it is expected to be in the eigenstate of the measured observable with certainty according to $|\psi_{\text{ideal}}\rangle$ will project the actual state of the computer into a state closer to $|\psi_{\text{ideal}}\rangle$ and may thus offer a way of implementing such a "watchdog stabilization" (*20*). Although this effect is useless once the loss of coherence becomes exponential (as it is for spontaneous emission), such a scheme may be helpful in keeping at bay errors from timing inaccuracies and environmental differences. For example, in the linear ion trap computer (*14*), both the center-of-mass phonon and the auxiliary levels of the ions have predictable occupation numbers at well defined instants during ideal operation. This promise, coupled with the results obtained from our analysis of the impact of decoherence on the quantum factoring algorithm, bring some hope to the eventual reality of quantum computers and motivate further experimental investigations in this field.

REFERENCES AND NOTES

1. R. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics* (Addison-Wesley, Reading, MA, 1994).
2. See A. K. Lenstra and H. W. Lenstra, in *Handbook of Theoretical Computer Science*, J. van Leeuwen, Ed. (MIT Press, Cambridge, MA, 1990), vol. A, pp. 673–715. For an opposing argument, see V. R. Pratt. *SIAM J. Comput.* **4**, 214 (1975).
3. A. K. Lenstra and H. W. Lenstra, Eds., *The Development of the Number Field Sieve*, vol. 1554 of *Lecture Notes in Mathematics* (Springer-Verlag, Berlin, 1993).
4. P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, S. Goldwasser, Ed. (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
5. R. Landauer, in *Proceedings of the Drexel-4 Symposium on Quantum Nonintegrability: Quantum Classical Correspondence*, D. H. Feng and B.-L. Hu, Eds. (International Press, Boston, 1995).
6. D. Deutsch. *Proc. R. Soc. London Ser. A* **400**, 97 (1985).
7. W. H. Zurek. *Phys. Today* **44**, 36 (October 1991).
8. ———, *Phys. Rev. D* **24**, 1516 (1981); *ibid.* **26**, 1862 (1982).
9. W. H. Zurek, in *Frontiers of Nonequilibrium Statistical Physics*, G. T. Moore and M. O. Scully, Eds. (Plenum, New York, 1986), pp. 151–162.
10. E. A. Lee and D. G. Messerschmitt, *Digital Communication* (Kluwer Academic, Dordrecht, Netherlands, 1988).
11. S. Lloyd, *Science* **261**, 1569 (1993).
12. D. P. DiVincenzo, *Phys. Rev. A* **50**, 1015 (1995).
13. I. L. Chuang and Y. Yamamoto, *ibid.* **52**, 3489 (1995).
14. J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **74**, 4091 (1995).
15. W. G. Unruh, *Phys. Rev. A* **51**, 992 (1995).
16. A. J. Leggett *et al.*, *Rev. Mod. Phys.* **59**, 1 (1987).
17. J. P. Paz, unpublished results.
18. C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, D. J. Wineland, "Demonstration of a Universal Quantum Logic Gate," preprint (July 1995).
19. W. H. Zurek, *Phys. Rev. Lett.* **53**, 391 (1984).
20. ———, in preparation.

21. We thank J. Anglin, J. P. Paz, and Y. Yamamoto for useful conversations. I.L.C. acknowledges the support of a fellowship from the Fannie and John Hertz Foundation.

14 February 1995; accepted 10 October 1995

Correlated Variations in the Solar Neutrino Flux and the Solar Wind and the Relation to the Solar Neutrino Problem

R. L. McNutt Jr.

Solar wind parameters from the Massachusetts Institute of Technology (MIT) plasma experiment on the IMP 8 spacecraft overlap ~19 years of published neutrino flux observations from the Homestake experiment. A strong correlation is found between neutrino flux and solar wind properties, in particular, the solar wind mass flux. The correlation is significantly better than any anticorrelation with sunspot number and is comparable to those previously found with photospheric magnetic flux and shifts in *p*-mode frequencies. If current notions of solar structure are correct, these observations require new fundamental physics of neutrinos. For a proper choice of neutrino parameters, the level of variations is consistent with resonant conversion of electron neutrinos to a nondetected flavor eigenstate mediated by the magnetic field in the sun's convective zone. The solar wind mass flux may act as a proxy for this field, producing the solar wind–neutrino flux connection.

The measured average neutrino flux from the sun is low compared with predictions based on solar models. This discrepancy, a factor of more than 3, originally showed up in the data of the ^{37}Cl experiment in the Homestake Gold Mine in South Dakota (*1*) and is known as the solar neutrino problem (*2*). Low neutrino fluxes have been confirmed for neutrino energies other than those measured at Homestake by the Kamiokande-II water Cherenkov experiment (*3*) and the SAGE (*4*) and GALLEX (*5*) gallium experiments.

The Homestake rate appears to exhibit a time-variable component. A possible anticorrelation with solar activity has been studied by a number of investigators. The correlation has remained suspect because of the low counting statistics, questionable correlation, and difficulty of explanation (*6*–*8*). Confirmation from the other solar neutrino experiments now operating is problematic because of the shorter times the experiments have been running and large statistical uncertainties.

Strong (time-dependent) correlations have been reported between shifts in solar *p*-mode frequencies and the Homestake capture rate (*9*, *10*). Recently an anticorrelation of capture rate with photospheric magnetic flux that is stronger than that with sunspot number has been found (*11*); this anticorrelation increases as flux away from the center of the solar disk is excluded. In this report I show that there is a corresponding large correlation between capture rate and the solar wind flux as measured near Earth by the MIT plasma experiment on the IMP 8 satellite.

The solar wind data used here are from the MIT Faraday cup plasma analyzer (*12*). The only significant data gap is from part of 1982 to 1983, resulting from a problem with

The Johns Hopkins University Applied Physics Laboratory, Laurel, MD 20723–6099, USA.