LA-UR-95-241

Quantum Computers, Factoring and Decoherence

I. L. Chuang[1], R. Laflamme[2], P. W. Shor[3] *and* W. H. Zurek[2]

[1] Edward L. Ginzton Laboratory, Stanford University, Stanford, CA, 94305, USA

[2]Theoretical Astrophysics, T-6, MS B288
Los Alamos National Laboratory, Los Alamos, NM87545, USA

[3]AT& T Bell Labs, 600 Mountain Ave., Murray Hill, NJ 07974, USA

October 12, 1995

Abstract

It has been demonstrated recently that quantum computers can dramatically speed up the task of finding factors of large numbers – a problem of great practical significance because of its 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 utilizing the ability of a quantum computer to simultaneously follow all of the paths corresponding to distinct classical inputs, and to obtain the solution as a result of coherent quantum interference between the alternatives. Here it is shown how the decoherence process degrades the interference pattern which emerges from the quantum factoring algorithm. Furthermore it is argued that for a quantum computer which is actually performing logical operations an exponential decay of quantum coherence is inevitable. However, even in presence of exponential decoherence quantum computation can be useful, so that for example, the thermal timescale $\hbar/k_BT$ does not impose a fundamental cutoff on the duration of a computation, as has been speculated previously.

The uniqueness of the prime factorization of a positive integer is the Fundamental Theorem of Arithmetic (*1*). However, in practice, the determination of the prime factors of a given number can be an exceedingly difficult problem, although 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 met with failure by and large, even with the aid of powerful modern computers. In fact, this problem is widely believed to have no polynomial-time algorithm (*2*), although a proof of this statement has remained elusive. The best known classical computer algorithm (*3*) to factor a number N of L digits takes a time exponential in $L^{1/3}$.

In contrast, one of us (*4*) has shown recently that with the help of a quantum computer one can factor numbers in a random *polynomial* amount of time. Therefore these new computers could be a threat to what is presently the most common method of encrypted message transfer. However, it is still unknown whether such machines are *practical*, because they depend crucially on quantum-mechanical behavior which is uncommon to our mostly classical world (*5*). This issue includes the problem of decoherence (*6*), the subject of our study.

The quantum factoring algorithm uses in an essential way the coherence of a quantum wavefunction. In a nutshell, 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 (*4,1*). The difficulty is to calculate r, and this task is solved by the quantum factoring algorithm as follows. First choose a smooth number (one with small prime factors) q such that $N^2 < q < 2N^2$ and build the state:

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

from which can be obtained (using a quantum computer) (*8*)

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

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

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

and measure both arguments of this superposition, obtaining $c = m$ for the first one 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;

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

where the prime indicates a restricted sum over values of a which satisfy $x^a \equiv x^k \bmod N$. Independent of k, $P(c, x^k)$ is periodic in c with period q/r, but as 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 which 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.

The algorithm discussed above assumes that the quantum computer was completely isolated. In practice this will certainly not be the case. It is the effect of imperfect isolation which we study here. A first 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* (*6*). Decoherence is caused by the continuous interaction between the system (in our case the quantum computer) and the environment (*6,7*). 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 them 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*)

$$\tau_{dec} \sim \tau_{rel} \left[\frac{\lambda_{dB}}{\Delta x}\right]^2 , \tag{5}$$

where λ_{dB} is the thermal de Broglie wavelength. This expression is valid for high temperatures only; at low temperatures, the τ_{dec} becomes inversely proportional to the cut-off frequency of the bath. It is crucial to realize that 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.

The decoherence process has been proposed as a mechanism for enforcing classical behavior in the macroscopic realm. Decoherence results in environment-induced superselection (*6,7,9*) which destroys superpositions between the states of preferred pointer basis (a set of states selected by the interaction with the environment) (*7*). 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. But coupling with the environment will also be inevitable for any system employed to implement quantum computation. Here, we show the effect of decoherence on the interference pattern which is produced as a result of the execution of 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

$$|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle \otimes |\epsilon\rangle , \tag{6}$$

where ϵ is the initial state of the environment. 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,

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \text{mod } N\rangle \otimes |\epsilon_a\rangle , \tag{7}$$

leaves the environment partially correlated with the state of the computer. Now, 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;

$$\rho_{red} = \frac{1}{q} \sum_{a=0}^{q-1}{}' \sum_{a'=0}^{q-1}{}' \left[1 - \beta_{aa'}\right] |a\rangle\langle a'| \,. \tag{8}$$

Here $1 - \beta_{aa'} = |\langle\epsilon_a|\epsilon_{a'}\rangle|^2$ 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;

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

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 $\beta = 1$ 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 (see Fig. 2) is equal to the one of the peaks, and thus there is as much chance to get a correct answer than a wrong one. Let $L = \log N$. Once $(1 - \beta)^{-1} \sim \mathcal{O}(\exp[L^{1/3}])$, the quantum computer becomes as inefficient as a classical one, requiring a number of trials exponential in $L^{1/3}$ in order to factor the number 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 $\beta \approx 1 - \exp(-n_{op}\alpha M) \approx n_{op}\alpha M$, 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 $N \sim \exp(L)$ the quantum algorithm requires $M \sim L$ and $n_{op} \sim L^2$. With perfect operation, each execution gives a factor with probability $\mathcal{O}(1/L)$, and thus with decoherence, the required number of trials is $\mathcal{O}(L/(1 - \beta))$. When this is expressed in terms of α and L, the number of trials required find a factor of N is of order

$$\text{Number of trials} \sim L \exp\left[L^3\alpha\right] . \tag{10}$$

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

$$\alpha < L^{-8/3} . \tag{11}$$

Designs for quantum computers have been suggested (*11,12,13,14*) and some possible difficulties investigated (*5,16*). 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 for what α is. Such an analysis, using the well-studied spin-boson Hamiltonian (*17*), straightforwardly gives the result that in a typical timestep 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 (*18*)

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

where ϵ is the (dimensionless) coupling strength and the resulting viscosity on the qubit (which will determine the rate of the loss of energy) is denoted by the coefficient η. Moreover, Λ is a high-frequency cutoff 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. (*15*), it is found that $\gamma \approx 10^3$ 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 the ultimate source of errors will be due to spontaneous emission and estimates that $\gamma \approx 0.1$ Hz, and $\Delta \approx 10^5$ Hz, which naively gives $\alpha \approx 10^{-6}$. This 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, since γ does *not* reflect all of the decoherence processes which may be taking place.

Unruh has also analysed the impact of decoherence on quantum computation (*16*). He computed behavior of a static memory, exhibited three regimes of the decay of coherence of a qubit (early one where $\beta \sim \exp(-\epsilon^2\Lambda^2t^2/4\pi)$; "quantum" regime where $\beta \sim 1/(\Lambda t)$; and "thermal" regime which starts at $\hbar/k_BT$) and concluded that the time taken by the quantum computer to complete the calculation must be smaller than the (thermal) timescale for which the decoherence process becomes exponential. We differ with these conclusions on two counts: (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 zero temperature limit. Nevertheless, (ii) exponential decay is not a reason to give up: it is the rate of that decay which ultimately matters! This rate is given by Eq. (12) in the case studied here, and by $\epsilon^2 k_B T/\hbar\Delta$ for the temperature dominated regime. In either case, by increasing isolation (i. e., by making ϵ small) and making the clock rate Δ large, one will be able to take the computation well beyond the timescale (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:

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

where δ is the variance of the difference between the ideal and actual energy. Thus, as it was suggested by one of us some time ago, 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 short compared with $1/\delta$ – it will stray from the correct evolution only a little, so that the probability of being correct is

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

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 $|\psi_{\rm ideal}\rangle$ will project the actual state of the computer into a state closer to $|\psi_{\rm ideal}\rangle$ 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 does for spontaneous emission), such a scheme may be helpful in keeping at bay errors due to timing inaccuracies as well as 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 new and exciting field.

References

[1] R. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison Wesley, 1994.

[2] See A. K. Lenstra and H. W. Lenstra in Handbook of Theoretical Computer Science Vol. A, ed. J. van Leeuwen, (MIT Press/Elsevier, 1990), pp. 673–715. For an opposing argument, see: V. R. Pratt. *SIAM J. Comput.*, 4(1):214, 1975.

[3] A. K. Lenstra and H. W. Lenstra, editors. *The Development of the Number Field Sieve.*, Lecture Notes in Mathematics volume 1554. Springer-Verlag, 1993.

[4] P. W. Shor. In *Proc. 35th Annual Symposium on Foundations of Computer Science*, ed. S. Goldwasser. (IEEE Computer Society Press, Nov. 1994) pp. 124–134.

[5] R. Landauer. Is Quantum Mechanically Coherent Computation Useful? In D.H.Feng and B-L. Hu, editors, *Proc. of the Drexel-4 Symposium on quantum Nonintegrability – Quantum Classical Correspondence*, 1995.

[6] W. H. Zurek. *Physics Today*, 44:36, 1991.

[7] W. H. Zurek. *Phys. Rev. D*, 24:1516, 1981, W. H. Zurek. *Phys. Rev. D*, 26:1862, 1982.

[8] D. Deutsch. *Proc. R. Soc. Lond. A*, **400**, 97-117 (1985).

[9] W. H. Zurek. In G.T. Moore and M.O.Scully, editors, *Frontiers of Nonequilibrium Statistical Physics*, New York, 1986. Plenum.

[10] E. A. Lee and D. G. Messerschmitt. *Digital Communication.* Kluwer Academic Publishers, 1988.

[11] S. Lloyd. *Science*, 261:1569, 1993.

[12] David P. DiVincenzo. *Phys. Rev. A*, 50:1015, 1995.

[13] I. L. Chuang and Y. Yamamoto. A Simple Quantum Computer. *Submitted to Phys. Rev. A*, 1994.

[14] J. I. Cirac and P. Zoller. *Phys. Rev. Lett.*, 74:4091, 1995.

[15] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Preprint, July, 1995.

[16] W. G. Unruh. *Phys.Rev. A*51:992, 1995.

[17] A. J. Leggett, S. Chakravarty, A. T. Dorsey, M. P. A. Fisher, A. Garg and W. Zwerger. *Rev.Mod.Phys.*, 59:1, 1987.

[18] J. P. Paz. *unpublished*, 1994.

[19] W. H. Zurek. *Phys. Rev. Lett.*, 53:391, 1984.

[20] W. H. Zurek. In preparation.

[21] We would like to thank J. Anglin, J.P. Paz, and Y. Yamamoto for useful conversations. ILC gratefully acknowledges the support of a fellowship from the John and Fannie Hertz Foundation.

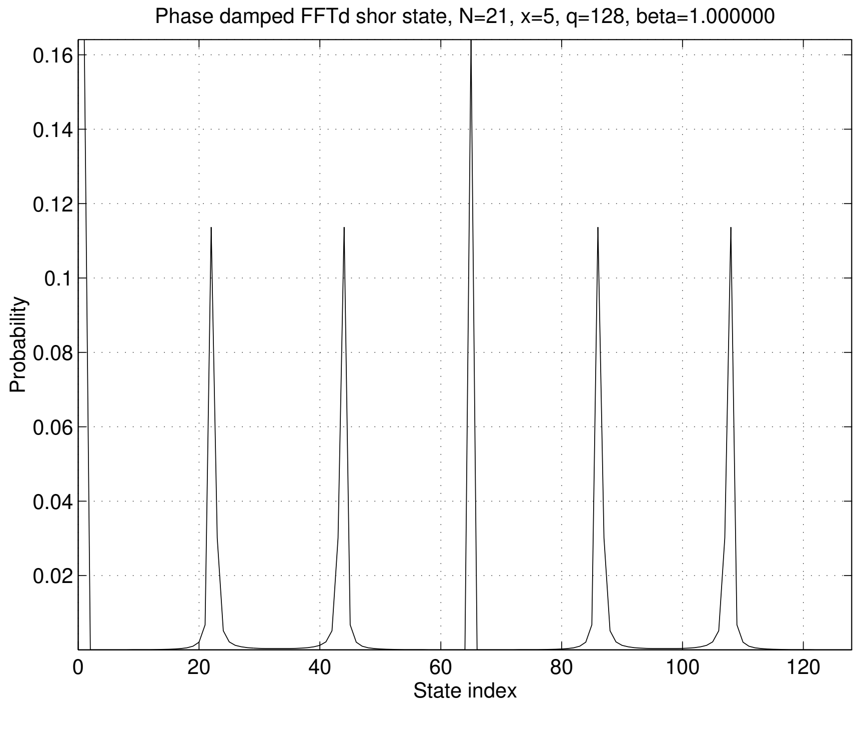

FIG. 1: Probability distribution for the measurement of c in the state given in Eq.(3) with $N = 21$, $q = 128$, $x = 5$, $k = 3$. The broadening of the peaks is a result of using discrete Fourier transform with q possible modes; a continuous Fourier transform would have given delta functions.

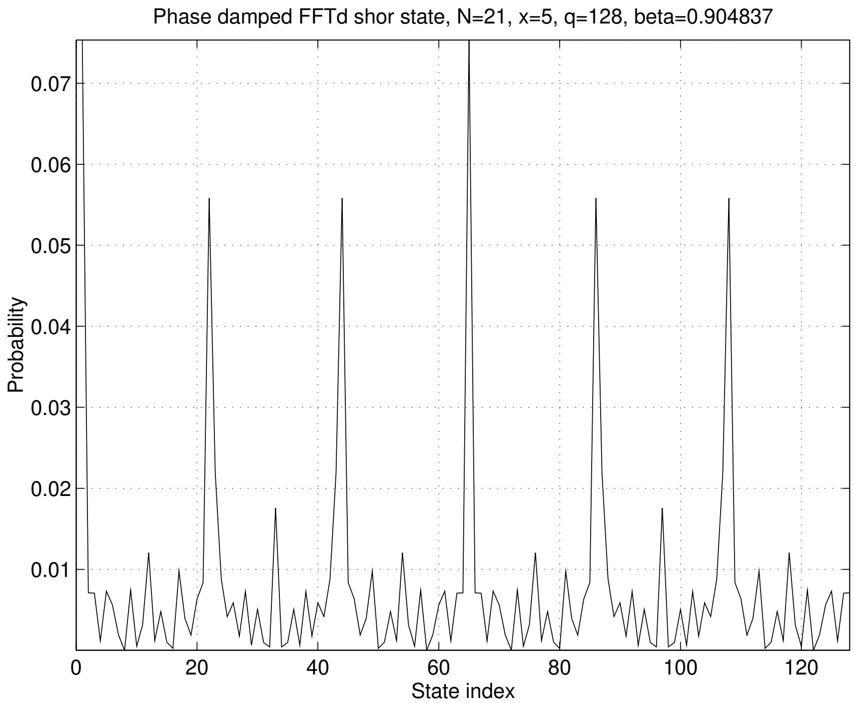

FIG. 2: Effect of decoherence on the probability distribution for the value of c. The state given by Eq.(8) once a is Fourier transformed. The decoherence parameter Eq.(9) has been taken to be $\xi = 0.1$. The dotted line shows the good agreement of our constant-beta approximation, taking $\beta = 0.58$.