Maintaining coherence in quantum computers

W. G. Unruh*
Canadian Institute for Advanced Research, Cosmology Program, Department of Physics, University of British Columbia, Vancouver, Canada V6T 1Z1
(Received 10 June 1994)

The effects of the inevitable coupling to external degrees of freedom of a quantum computer are examined. It is found that for quantum calculations (in which the maintenance of coherence over a large number of states is important), not only must the coupling be small, but the time taken in the quantum calculation must be less than the thermal time scale $\hbar/k_BT$. For longer times the condition on the strength of the coupling to the external world becomes much more stringent.

PACS number(s): 03.65.−w

I. INTRODUCTION

Quantum computers have recently raised a lot of interest. A number of papers [1] have argued that quantum computers can solve certain problems much more efficiently than can classical computers. Shor [2] has shown that a quantum computer could solve the problem of finding discrete logarithms (mod$N$) and of finding the factors of a large number N in a time which is a polynomial function of the length L (number of bits) of the number. For factoring the best-known algorithm, the number field sieve [3] takes a time of order $\exp(c(L)[\ln(2)L]^{1/3}\{\ln[\ln(2)L]\}^{2/3})$, where $c(L)$ is roughly constant and believed to be approximately equal to 1.9 for large L. Although this is subexponential, it is worse than any polynomial for large N. A crucial feature of the ability of quantum computers to be more efficient in certain problems involves having the computer placed in the coherent superposition of a very large number (exponential in L) of "classical states" and having the outputs interfere in such a way that there is a very high probability that on the appropriate reading of the output, one would obtain the required answer. One is replacing the exponential in time with the exponential in quantum coherence. This requires that the computer be able to maintain the coherence during the course of the calculation. This paper examines this requirement and the constraints placed on the ability to maintain this coherence in the face of coupling to external heat baths. Landauer [4] has long emphasized the necessity of examining the effect of both imperfections and the coupling to the external world of any realistic device on the ability of quantum computers to realize their promise. This paper is thus a first step in that direction.

II. DECOHERING NOISE

I will look at only the simplest model, in which I ask about the maintenance of coherence in a memory of length L. This does not take into account the effect that the course of the computation itself would have on the rate of loss of coherence, but I would expect that only to increase the problem. Thus let us assume that that the number is represented in the computer as a string of binary digits of length $L = \log_2(N)$. The memory cells will each be taken to be two-level systems, with each of the two levels having the same energy. The two states will be taken to be the eigenstates of a "spin" operator σ_z.

In a conventional computer, the way in which the calculation is "kept on track" is by including dissipation in order to damp out any attempt by the system to make a transition (except of course those driven by the computation) [5]. In a quantum computer, dissipation cannot be used and the accuracy of the computation must be built in. However, some interaction with the dissipative environment will always be present. As a first look at the effect that this coupling to the environment has on the course of the quantum computation, I will assume that the interaction with the environment has the two desired eigenstates of the memory; the eigenstates of the interaction represent the bit values of a number. This means that the environment will not cause bit flips to occur. Such bit flips would be sources of error even for the classical calculation. Later I will argue that even bit flipping interactions with the environment will behave in the same way as the bit conserving interactions I am looking at here.

Obviously, the effect that the environment has on the system will depend on the details of the environment and on the details of the interaction between the computer and its environment. In any engineering of a quantum computer, one would have to take into account all of the details of that interaction. As a first examination of the problem, in this paper I will choose a specific model for the environment and for the interaction with the environment. I thus choose the environment to be modeled by a massless scalar field [7] derivatively coupled to the memory cell, so that the full Hamiltonian is

$$H = \frac{1}{2}\{[\pi(x) + \epsilon h(x)\sigma_z]^2 + [\partial_x\phi(x)]^2\}dx \ . \qquad (1)$$

The associated Lagrangian has the simple derivative cou-

*Electronic address: unruh@physics.ubc.ca

pling form

$$L = \frac{1}{2}\int[(\partial_t\phi)^2 - (\partial_x\phi)^2 - 2\epsilon h(x)\partial_t\phi(x)\sigma_z]dx \ . \quad (2)$$

Here $h(x)$ is some interaction range function and π is the momentum conjugate to ϕ. This scalar field model is completely equivalent to the so-called Caldera-Leggett model [6], a common model for an environment in which it is represented by an array of simple harmonic oscillators.

The Heisenberg equations of motion are

$$\dot{\pi} = \partial_x^2\phi \ , \quad (3)$$

$$\dot{\phi} = \pi + \epsilon h(x)\sigma_z \ . \quad (4)$$

The exact solutions for the Heisenberg equations of motion for ϕ are (assuming that σ_z is a function of time)

$$\begin{aligned}\phi(t,x) = \frac{1}{2}\left(\phi(0,x-t) + \phi(0,x+t) + \int_{x-t}^{x+t}\pi(0,y)dy\right) \\ -\frac{\epsilon}{2}\int[\sigma_z(t-|x-y|) - \sigma_z(-|x-y-t|) \\ \times\Theta(x-y-t) - \sigma_z(-|x-y+t|) \\ \times\Theta(-(x-y+t))]h(y)dy \ , \end{aligned} \quad (5)$$

where

$$\Theta(x) = \begin{cases} 0 & \text{if } x < 0 \\ 1 & \text{if } x > 0 \ . \end{cases}$$

Since, in the model I am using, σ_z is a constant of motion (recall that I am not taking into account the effects of the operation of the computer), the solution for ϕ is thus

$$\phi(t,x) = \frac{1}{2}\left(\phi(0,x-t) + \phi(0,x+t) + \int_{x-t}^{x+t}\pi(0,y)dy\right) \quad (6)$$

$$\begin{aligned} -\frac{\epsilon}{2}\sigma_z\int[1 - \Theta(x-y-t) - \Theta(-(x-y+t))] \\ \times h(y)dyh(y)dy \ . \end{aligned} \quad (7)$$

I will, however, be working in the Schrödinger representation in the following.

I assume that the initial state of the environment is a thermal density matrix R_T with temperature T and the initial state of the spin is a density matrix $\rho(0)$. The total state is assumed to be a product state of these two initial states. The reduced state of the spin system at any time t after tracing out over the state of the environment is a density matrix given by

$$\rho(t) = \frac{1}{2}[1 + \vec{\rho}(t)\cdot\vec{\sigma}] \ , \quad (8)$$

where $\vec{\rho}(t)$ is a time-dependent vector of length less than or equal to unity. $\vec{\rho}(t)$ is given by

$$\vec{\rho}(t) = \mathrm{Tr}[\vec{\sigma}e^{iHt}\rho(0)R_T e^{-iHt}] \ , \quad (9)$$

where the trace is over all of the degrees of freedom of spin system and bath.

We can write H as

$$H = e^{i\int\epsilon h(x)\phi(0,x)dx\sigma_z}H_0 e^{-i\int\epsilon h(x)\phi(0,x)dx\sigma_z} \quad (10)$$

since $e^{i\int\epsilon h(x)\phi(0,x)dx\sigma_z}$ is just the translation operator taking $\pi(0,x)$ to $\pi(0,x) + \epsilon\int h(x)\phi(0,x)dx\sigma_z$ and since σ_z commutes with H_0. Thus

$$\begin{aligned}\vec{\rho}(t) = \mathrm{Tr}[\vec{\sigma}e^{i\int\phi(0)\epsilon hdx\sigma_z}e^{-i\int\tilde{\phi}(t)\epsilon hdx\sigma_z}\vec{\rho}(0)\cdot\vec{\sigma} \\ \times e^{iH_0t}R_T e^{-iH_0t}e^{i\int\tilde{\phi}(t)\epsilon hdx\sigma_z}e^{-i\int\tilde{\phi}(0)\epsilon hdx\sigma_z}] \ , \end{aligned} \quad (11)$$

where $\tilde{\phi}(t) = e^{iH_0t}\phi(0,x)e^{-iH_0t}$ is the time development of the *free* field with the same initial conditions $\phi(0)$ and $\pi(0)$, i.e.,

$$\tilde{\phi}(t,x) = \frac{1}{2}\left(\phi(0,x-t) + \phi(0,x+t) + \int_{x-t}^{x+t}\pi(0,x')dx'\right). \quad (12)$$

Using $\sigma_z^2 = 1$ and the fact that R_T is diagonal in the energy representation, we can write $\vec{\rho}(t)$ as

$$\begin{aligned}\vec{\rho}(t) = \mathrm{Tr}(\vec{\sigma}e^{i\int[\phi(0)-\phi(t)]\epsilon hdx\sigma_z}\vec{\rho}(0)\cdot\vec{\sigma} \\ \times R_T e^{i\int[\tilde{\phi}(t)-\phi(0)]\epsilon hdx\sigma_z}) \ . \end{aligned} \quad (13)$$

(Note that the extra terms from the Cambell-Baker-Hausdorf formula cancel out.) This can further be written as

$$\vec{\rho}(t) = \mathrm{Tr}\left(\vec{\sigma}[\vec{\rho}(0)]\cdot\left\{\vec{\sigma} - \left[1 - \cos\left(\int[\tilde{\phi}(t) - \phi(0)]\epsilon hdx\right)\right]\sigma_z\vec{e}_z + \sin\left(\int[\tilde{\phi}(t) - \phi(0)]\epsilon hdx\right)\right\}\vec{e}_z \times \vec{\sigma}R_T\right) \ , \quad (14)$$

where $\vec{e}_z$ is the unit vector in the z direction. Because R_T is symmetric in ϕ and π, the sin term is zero and

$$\begin{aligned} J(t) &\equiv \mathrm{Tr}\left[R_T\cos\left(\int[\tilde{\phi}(t) - \phi(0)]\epsilon hdx\right)\right] \\ &= e^{-\frac{1}{2}\mathrm{Tr}\{R_T(\int[\tilde{\phi}(t)-\phi(0)]\epsilon hdx)^2\}} \ . \end{aligned} \quad (15)$$

We are thus left with

$$\rho_z(t) = \rho_z(0) \ , \quad (16)$$

$$\rho_x(t) = J(t)\rho_x(0) \ , \quad (17)$$

$$\rho_y(t) = J(t)\rho_y(0) \ . \quad (18)$$

Since $J(t)$ will play an important role in what follows, it is worthwhile discussing its physical significance. As we see above, $J(t)$ controls the rate at which a general superposition of the spin states loses coherence for a single

spin. In magnetic resonance studies, one excites a whole ensemble of single spins into some given superposition state and watches the time development of the resultant total magnetization. The total magnetization is just the sum of the individual magnetic moments which are proportional to the individual spins. The off-diagonal terms (perpendicular to the applied magnetic field) of the Bloch vector decay. In most resonance experiments, this decay is dominated by inhomogeneities in the local magnetic fields. This source of decay is reversible and can be compensated by variations of the spin-echo experiment. However, for the irreversible component of that off-diagonal decay, it is $J(t)$ that determines the rate at which those off-diagonal terms in the recurrent spin-echo signal are lost. If $J(t)$ is exponential in t, then $J(T_2) = 1/e$ defines T_2 in the NMR literature [8].

For later use, let us examine $J(t)$ in various regimes. Let us take $h(x)$ such that $h(k)$, the Fourier transform of $h(x)$, is of the form $e^{-\frac{1}{2}\Gamma k}$. Γ is a cutoff parameter typical of interactions with the environment. I will assume that $\Gamma \ll 1/T$. We then get

$$\ln[J(t)] = -\frac{\epsilon^2}{2}\int\left(\frac{1}{\pi k}\coth\left(\frac{k}{2T}\right)[1-\cos(kt)]e^{-\Gamma k}\right)dk \ . \tag{19}$$

We will approximate $\coth(x) \approx 1 + e^{-x}(\frac{1}{x} + \cdots)$. This gives us

$$\ln[J(t)] \approx -\frac{\epsilon^2}{2\pi}\left[\frac{1}{2}\ln\left(\frac{\Gamma^2+t^2}{\Gamma^2}\right) - \frac{1}{2}\ln[1+(2Tt)^2] - iTt\ln\left(\frac{1-i2Tt}{1+i2Tt}\right)\right] . \tag{20}$$

There are essentially three regimes for the time dependence of $J(t)$ given by the conditions $t < \Gamma$, $\Gamma < t < 1/T$, and $t > 1/T$. In the first regime $t < \Gamma$, we have approximately

$$\ln[J(t)] \approx \frac{\epsilon^2 t^2}{4\pi\Gamma^2} \ . \tag{21}$$

For the intermediate regime $\Gamma < t < 1/T$, the quantum regime, we have

$$\ln[J(t)] \approx -\frac{\epsilon^2}{2}\ln\left(\frac{t}{\Gamma}\right) \ . \tag{22}$$

Finally, for the long time regime $t \gg 1/T$, the thermal regime, we have

$$\ln[J(t)] \approx -\epsilon^2 Tt \ . \tag{23}$$

The important feature of these asymptotic formula is that for the intermediate regime, which I call the quantum regime since the behavior is dominated by the vacuum state of the environment, $\ln(J)$ increases only logarithmically with t. In contrast, the third regime, the thermal regime, increases linearly with t. This will be important in determining the ultimate size of a number that can be, say, factored with a quantum computer because of the dependence of the computing time on the length of the number being factored.

This was for the most familiar case of an "Ohmic" coupling to the heat bath. In the case of super-Ohmic coupling ($h[k(\omega)] = \omega^s e(-\Gamma\omega)$ for $s > 0$), the function $\ln[J(t)]$ is essentially constant for times less than $1/T$ and grows as t^{1-s} in the thermal regime for $s < 1$. For $s > 1$, J is constant in both regimes, although it is smaller in the thermal regime than in the quantum regime (and is essentially constant even for such times if $s > 1$). In the sub-Ohmic case, $-1 < s < 0$, on the other hand, $\ln[J(t)]$ grows roughly as t^{-s} in the quantum regime and as t^{1-s} in the thermal regime. Again, in the thermal regime the growth in decoherence is a factor of t larger than in the quantum regime.

The above analysis was carried out for a single bit in the memory of the quantum computer. Let us examine the situation in which our memory has some large number L of bits. Each bit is assumed to couple to its own heat bath of exactly the above type. The question now is, What is the rate of loss of coherence of a coherent sum of numbers stored in the memory? In other words, define the state $|n\rangle = |n_{L-1}\rangle|n_{L-2}\rangle\cdots|n_0\rangle$, where n_i is the ith bit of n. Consider a coherent state

$$|\psi\rangle = \sum_n \alpha_n |n\rangle \ . \tag{24}$$

The probability that after time t the memory remains in the state ψ is given by

$$\begin{aligned} P_\psi &= \langle\psi|\mathrm{Tr}_{\mathrm{environ}}\left[\exp\left(i\sum_i H_i t\right)|\psi\rangle|0\rangle\langle 0|\langle\psi|\exp\left(-i\sum_i H_i t\right)|\psi\rangle\right] \\ &= \sum_{n,n',m,m'} \alpha_n^*\alpha_{n'}\alpha_m\alpha_{m'}^* \prod_i \mathrm{Tr}_{\mathrm{environ}_i}(\langle n_i|e^{iH_i t}|m_i\rangle\langle m_i'|e^{-iH_i t}|n_i'\rangle) \\ &= \sum_{n,n'} |\alpha_n|^2|\alpha_{n'}|^2 \prod_i J_i(t)^{(n_i\otimes n_i')} \ , \end{aligned} \tag{25}$$

where $(n_i \otimes n_i')$ is the XOR of the ith bits of n and n'. (XOR is 0 if both bits are the same and 1 if they are different.)

This expression tells us how the coherent sum over the various states of the memory representing various numbers decoheres as a function of time. As an example, let us choose the completely coherent state in which each of the numbers of length L has an equal probability. This

state is typical of the state required in performing quantum calculations of the sort in which a quantum computer is much faster than a classical computer. In other words, I choose $|\alpha_n|^2 = 2^{-L}$. Furthermore, let me assume that each bit is coupled to the environment in exactly the same way so that $J_i(t) = J(t)$. Then we have the probability P that the coherence will be maintained over time t as

$$P = 2^{-2L} \sum_{n,n'} \prod_i J(t)^{(n_i \otimes n_i')}. \tag{26}$$

To evaluate this, first fix the number n. The number of numbers n' that differ from n in 1 bit is L, the number that differs in 2 bits is $L(L-1)/2$, and the number that differs in r bits is $\frac{L!}{r!(L-r)!}$. Thus the above becomes

$$\begin{aligned} P &= 2^{-2L} \sum_n \sum_r \frac{L!}{r!(L-r)!} J^r \\ &= 2^{-2L} \sum_n (1+J)^L = \left(\frac{J+1}{2}\right)^L . \end{aligned} \tag{27}$$

If we assume that $1-J$ is very small (which is the only case in which the system has any hope at all of acting like a quantum computer), this is well approximated by

$$P \approx e^{-\frac{1}{2}L(1-J)} \tag{28}$$

as long as $L(1-J) < 1/(1-J)$.

The strength of the quantum computer is that the time required to perform the calculation is a polynomial in the length L of the number. This time is designated by $\tau(L)$. Since the quantum calculation is polynomial in L we can write $\tau(L) \approx L^a$ for $a > 1$. We thus have that the probability of maintaining coherence over the time of the calculation is of the order of

$$\ln(P) \approx -O(1)L\epsilon^2 \ln[\tau(N)] \approx -O(1)\epsilon^2 L \ln(L) \tag{29}$$

in the quantum regime, while it is of order

$$\ln(P) \approx -O(1)L^{a+1}\epsilon^2 \tag{30}$$

with a smooth transition between the two regimes. In order to have a reasonable probability of obtaining the correct answer, one needs the probability of obtaining the quantum coherent answer to be of order 1. This implies that one must have a sufficiently small ϵ^2, the coupling parameter between the heat bath and the system. As long as one is in the quantum regime, the relation between the coupling ϵ^2 and the maximum length of the number one can handle is essentially inversely linear, no matter what the polynomial dependence of the calculation. However, once one has entered the thermal regime, a decrease in the coupling buys one only a small increase in the length of the number L that one can use. In other words, in the presence of a coupling to the heat bath, the thermal time scale $\frac{1}{T} \equiv \frac{\hbar}{k_B T}$ plays a crucial role. As long as the calculation can be completed in a time less than this, one can imagine decreasing the coupling to the heat bath for the memory cells so as to achieve the maximum L. If, however, the time for the calculation is longer than the thermal time scale, it becomes very difficult to decrease the coupling to the bath sufficiently to achieve the necessary coherence.

Is it possible to use the computer even if the quantum state loses coherence? I cannot answer this in general, but can show that one strategy does not work. One could imagine trying to make up for the loss of coherence by increasing the number of times the program is run. (This is in fact a crucial factor in the Shor algorithm for factoring, not because of decoherence, but because the calculation itself has a finite probability of not giving the correct outcome.) After a sufficient number of attempts, one should by chance have a system which has maintained coherence. In the factoring problem, one can test ones answer (does it give the factors of the number?) and simply keep repeating the experiment until one gets the right answer. However, in M trials, the probability of never finding a coherent outcome is $(1-P)^M \approx e^{-MP}$. The number of trials required to make this small (i.e., so that one has a high probability of having had a coherent run) is thus the required number of attempts $M \approx 1/P \approx e^{O(1)L\ln(L)}$ in the quantum regime, which is exponential in the length. In the thermal regime, this time scale is even worse. One will thus have lost all advantages of the quantum nature of the computer. We see that one must make sure that coherence is maintained during the calculation.

In order to maintain coherence, one must have a small value for ϵ^2. At first, as one decreases ϵ^2, the gain in the maximum length number one can factor is roughly inversely proportional to the value of ϵ^2. However, once ϵ is sufficiently small that the time scale of computation for the maximum length which can maintain coherence approaches the inverse thermal time $1/T$, one reaches a bottleneck. Further reductions in ϵ^2 now have little effect on the maximum length. The decoherence due to the rapidly increasing time spent in computation cancels out the effect of the smaller ϵ^2. Thus the thermal time scale $1/T$ sets an effective limit to the time of the calculation and thus a weak limit on the maximum length of the numbers one can compute with.

If one imagines factoring a 1000 bit number and one assumes that the quantum factoring time can be made to be of order L^2 (probably the slowest rate imaginable), we find that one must carry out at least 10^6 calculation in the thermal time scale. Since the thermal time scale for a temperature of 1 K is of the order of 10^{-11} sec, this would imply that one would have to use a computer that runs at optical frequencies.

III. OTHER NOISE

The above coupling to the heat bath is "error free" in the sense that if one is in a number eigenstate (i.e., is in a state $|n\rangle$), the system will remain in that state throughout. The environment does not cause spin flips. What about the situation in which there is also some probability of a state flip, i.e., of the system making a transition between the two eigenstates of σ_z? One could approximate this by assuming that the coupling to the heat bath is via, say,

$$\sigma_\theta = \cos(\theta)\sigma_z + \sin(\theta)\sigma_x,$$

with small θ.

The above analysis is exactly the same for this case, where we replace σ_z everywhere by σ_θ. Writing the number eigenstates with respect to σ_θ so that

$$|n\rangle_\theta = |n_{L-1}\rangle_\theta \cdots |n_0\rangle_\theta \ , \tag{31}$$

we have

$$|n\rangle = \sum_m \prod_i \cos(\theta)^{1\otimes n_i \otimes m_i} \sin(\theta)^{n_i \otimes m_i} \times (-1)^{(n_i \otimes m_i)n_i} |m\rangle_\theta \ . \tag{32}$$

The probability of remaining in the state $|n\rangle$ under the coupling to the heat bath is then

$$P = \sum_m \sum_m{}' \cos(\theta)^{2S(n,m)} [J \sin(\theta)^2][L - S(n,m)] \ , \tag{33}$$

where $S(n,m)$ is the number of bits in which n and m are the same. Again using the arguments above as to the number of terms where the S has a given value, we get

$$P = [\cos(\theta)^2 + J \sin(\theta)^2]^L .$$

For small θ this gives

$$P = [1 - (1-J)\theta^2]^L \approx e^{-L\theta^2 J} . \tag{34}$$

Thus θ must be kept very small in order to ensure that the probability of error remains small. However, we note that the probability of error is vastly suppressed with respect to the decoherence probability, which is in accord with the observation that the decoherence effects are in general much larger and more rapid than transition effects.

This has assumed that the process causing spin flips is the same as the one causing loss of coherence in a superposition of the two spin states. In general, the environmental degrees of freedom which cause decoherence are not the same as those causing bit flips. I will therefore look at the alternative situation in which the single bit Hamiltonian is of the form

$$\frac{1}{2}\{[\pi_1 - \epsilon_1 h(x)\sigma_z]^2 + (\partial_x \phi_1)^2 + [\pi_2 - \epsilon_2 h(x)\sigma_x]^2 + (\partial_x \phi_2)^2 + [\pi_3 - \epsilon_2 h(x)\sigma_y]^2 + (\partial_x \phi_3)^2\} \ . \tag{35}$$

Since we want the single bit decoherence and bit flip probabilities to be small (or else the quantum computer is useless from the start), I will assume that the ϵ_k are all sufficiently small. Furthermore, for simplicity I will take $\epsilon_2 = \epsilon_3$, so that the spin flip processes are of equal strength. I cannot solve this problem exactly, but since the probabilities are assumed to be very small, one can calculate the transition probability to lowest order in the various ϵ. The Hamiltonian can be written as

$$H = H_0 - \sum_i \left(\int \epsilon_i \pi_i(x) \sigma_i h(x) dx + \frac{1}{2} \int h(x)^2 dx \right) \ , \tag{36}$$

where $\sigma_i = (\sigma_z, \sigma_x, \sigma_y)$. The reduced density vector $\vec{\rho}(t)$ is given by

$$\vec{\rho}(t) = \mathrm{Tr}[\vec{\sigma} e^{iHt} \vec{\rho}(0) \cdot \sigma R_T e^{-iHt}] \ . \tag{37}$$

To zeroth order, since $H = H_0$ is independent of σ, we have $\rho(t) = \rho(0)$. To first order, one obtains terms that are linear in the π's and the ϕ's. However, in the thermal state, all of these are zero, because the thermal state (of H_0) is symmetric in the fields. To second order the results are nonzero. However, all of the cross terms $\epsilon_i \epsilon_j$ for $i \neq j$ will again be zero because the fields are, by assumption, independent and thus the cross correlations between terms linear in each of the fields will again be zero. Thus the only terms surviving will be the terms proportional to ϵ_i^2. But each of these terms is independent of the other ϵ's, i.e., each of these terms is the same as those obtained by setting the other two ϵ to zero. These are, however, just the same as the second-order terms calculated above in the first part. We thus get

$$\rho(t)_i = \sum_j \left[\delta_{ij} \left(1 - \frac{1}{2} \sum_k \left\{ \epsilon_k^2 \mathrm{Tr} \left[R_T \left(\int [\phi_k(t) - \phi_k(0)] h dx \right)^2 \right] \right\} \right) + \frac{1}{2} \sum_k \epsilon_k^2 \mathrm{Tr} \left[R_T \left(\int [\phi_k(t) - \phi_k(0)] h dx \right)^2 \right] \delta_{ik} \delta_{jk} \right] \rho_j(0) \ . \tag{38}$$

Note that since all of the fields are of the same form and at the same temperature, the $\mathrm{Tr}\{R_T[\int \phi_i(t) - \phi_i(0)]hdx\}^2$ are the same for all i.

The probability of bit flip then becomes

$$P_{\text{no flip}} \approx \{1 - \epsilon_2^2 \langle 0|[\phi(t) - \phi(0)]^2|0\rangle\}^L \ , \tag{39}$$

while the probability of decoherence for a state which is the coherent sum over all the integers of length L is given by

$$P_{\text{decoher}} \approx 1 - \left(\frac{1}{2}(\epsilon_1^2 + \epsilon_2^2) \right) \langle 0|[\phi(t) - \phi(0)]^2|0\rangle \ . \tag{40}$$

If $\epsilon_1 \gg \epsilon_2$, the decoherence will again be much more rapid than the probability of "error" due to bit flip.

IV. CONCLUSION

The above analysis has given a preliminary look at the effects of decoherence on quantum computers. It suggests

that this problem is going to require some serious thought in order to design systems to avoid the disastrous effects that the loss of coherence due to the coupling to the environment can cause.

Quantum computation places the demand on the system that the coherence of the initial state be maintained throughout the computation. In order to maintain this coherence in the presence of a heat bath, the reduction in the coupling to the heat bath results in a proportional increase in the size of the computation only if the computation can be completed within a thermal time scale. For computation times longer than the thermal time scale, a decrease in the coupling causes relatively little change in the size of the possible coherent computation. The thermal time scale thus sets a (weak) limit on the length of time that a quantum calculation can take.

There are a number of areas in which further research is required. One assumption of the above calculation which, as emphasized by Ekert and Lloyd [9], may lead to conclusions more pessimistic than strictly required is the assumption of separate and independent environments for each spin. Especially for the low-frequency components of the real environment (which also have long wavelengths) one might have a number of the spins interacting with the same modes on the environment. This could well lead to a reduction of the effect of the environment on the coherence of the system. However, while I would expect this to be of some help in reducing the effect of the loss of coherence to the environment, I do not expect it to change the above conclusions about the exponential dependence of the loss of coherence on the length of the memory. It could reduce the effective length L by some factor, which would thus reduce the effective size of the coupling ϵ. It would, however, do nothing to change the effect of L on the loss of coherence through the time of the computation t. However, this clearly is an area for further research in the engineering of a quantum computer able to resist the effects studied here.

An assumption which I believe makes the above results more optimistic than is warranted is the assumption that during the course of the computation, the bit flipping produced by the course of the computation has no impact on the decoherence rate. In particular the logarithmic dependence of $J(t)$ on time during the quantum regime is, I suspect, an artifact of this assumption. The very act of allowing the computation to flip a bit will, I suspect, create disturbances in the environment, which will lead to additional loss of coherence. In addition I would expect this to disrupt the long-range coherences in the environment [which lead to the logarithmic growth of $J(t)$] [10].

Quantum computing has now come of age in the sense of demonstration that it is potentially more than just a toy and could have exciting implications for the solution of interesting mathematical or computational problems. However, it now becomes important to examine closely the impediments to the realization of the promise of this new technique. It is only through the recognition of the various impediments, whether in the implementation of reversibility as raised by Landauer or in the loss of coherence as raised here, that those impediments will be overcome.

ACKNOWLEDGMENTS

I would especially like to thank the Santa Fe Institute and the organizers of the conference on Complexity, Entropy, and the Physics of Information held at the Center for the Study of Community, where the issue of quantum computing was a key theme and which incited my interest in the problems thereof.

[1] D. Deutsch and R. Jozsa, Proc R. Soc. London Ser. A **439**, 553 (1992).

[2] Peter W. Shor, in *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, 1994), p. 124.

[3] See papers on the number field sieve in *The Development of the Number Field Sieve*, edited by A.K. Lenstra and H.W. Lenstra, Springer Lecture Notes in Mathematics Vol. 1554 (Springer-Verlag, Berlin, 1993), especially p. 50ff.

[4] See Rolf Landauer, Proc. R. Soc. London Ser. A (to be published), and references cited therein.

[5] The spin-boson problem, of which the model used in this paper is a trivial example, has had a long history of use for trying to understand the effects of decoherence on the development of a quantum two-level system. In particular it demonstrates that a sufficiently strong "decohering" interaction, such as that presented here, can prevent a spin-flip force from being able to effect the spin flip (localization). See the review of A. Leggett *et al.*, Rev. Mod. Phys. **59**, 1 (1987).

[6] A.O. Caldera and A.J. Leggett, Physica **A121**, 587 (1983).

[7] W. Unruh and W. Zurek, Phys. Rev. D **40**, 1071 (1989).

[8] See, for example, C.P. Slichter, *Principles of Magnetic Resonance*, 3rd ed. (Springer-Verlag, Berlin, 1990).

[9] A. Ekert and S. Lloyd (private communication).

[10] J. Pablo Paz (private communication) has carried out calculations which support this view.