RAPID COMMUNICATIONS

PHYSICAL REVIEW A

ATOMIC, MOLECULAR, AND OPTICAL PHYSICS

THIRD SERIES, VOLUME 52, NUMBER 4 OCTOBER 1995

RAPID COMMUNICATIONS

The Rapid Communications section is intended for the accelerated publication of important new results. Since manuscripts submitted to this section are given priority treatment both in the editorial office and in production, authors should explain in their submittal letter why the work justifies this special handling. A Rapid Communication should be no longer than 4 printed pages and must be accompanied by an abstract. Page proofs are sent to authors.

Scheme for reducing decoherence in quantum computer memory

Peter W. Shor*

AT&T Bell Laboratories, Room 2D-149, 600 Mountain Avenue, Murray Hill, New Jersey 07974

(Received 17 May 1995)

Recently, it was realized that use of the properties of quantum mechanics might speed up certain computations dramatically. Interest has since been growing in the area of quantum computation. One of the main difficulties of quantum computation is that decoherence destroys the information in a superposition of states contained in a quantum computer, thus making long computations impossible. It is shown how to reduce the effects of decoherence for information stored in quantum memory, assuming that the decoherence process acts independently on each of the bits stored in memory. This involves the use of a quantum analog of error-correcting codes.

PACS number(s): 03.65.Bz, 89.70.+c

I. INTRODUCTION

Recently, interest has been growing in an area called *quantum computation*, which involves computers that use the ability of quantum systems to be in a superposition of many states. These computations can be modeled formally by defining a quantum Turing machine [1,5], which is able to be in the superposition of many states. Instead of considering the computer itself to be in a superposition of states, it is sufficient to assume that the contents of the memory cells are in a superposition of different states and that the computer performs deterministic unitary transformations on the quantum states of these memory cells [2]. This model resembles a quantum circuit [3] more than a quantum Turing machine. After Schumacher [4], we will call a two-state memory cell that can be part of such a superposition a quantum bit, or *qubit*. Whereas k classical two-state memory cells can take on 2^k states, thereby requiring k bits to describe them, k quantum bits require 2^k-1 complex numbers to completely represent their state. Even though most of these numbers must be small, and only the most significant digits of these numbers are important, there still appears to be too much information contained in k qubits to represent in a polynomial number of classical bits. Although only k bits of classical information can be extracted from k qubits, the presence of extra unextractable quantum information is a barrier to efficient simulation of a quantum computer on a classical computer.

It now appears that, at least theoretically, quantum computation may be much faster than classical computation for solving certain problems [5–7], including prime factorization. However, it is not yet clear whether quantum computers are feasible to build. One reason that quantum computers will be difficult, if not impossible, to build is *decoherence*. In the process of decoherence, some qubit or qubits of the computation become entangled with the environment, thus in effect "collapsing" the state of the quantum computer. The conventional assumption has been that once one qubit has decohered, the entire computation of the quantum computer is corrupted, and the result of the computation will no longer be correct [8,9]. We believe that this may be too conservative an assumption. This paper gives a way to use software to reduce the rate of decoherence in quantum memory. Berthiaume, Deutsch, and Jozsa [10] have similarly proposed a way of partially correcting errors in a quantum computer by taking many copies of the computation and continually projecting the computation into the symmetric subspace of these many copies. The degree to which their method corrects errors will depend on the type of errors that the computers are likely to make. Unfortunately, a mathematical analysis of the efficiency of their error-correction scheme has not yet been accomplished.

Assuming that the decoherence process affects the differ-

*Electronic address: shor@research.att.com

ent qubits in memory independently, we show how to store an arbitrary state of n qubits using $9n$ qubits in a decoherence-resistant way. That is, even if one of the qubits decoheres, the original superposition can be reconstructed perfectly. In fact, we map each qubit of the original n qubits into nine qubits, and our process will reconstruct the original superposition if at most one qubit decoheres in each of these groups of nine qubits. We thus show that the identity computation can be performed in a more decoherence resistant manner than the naive implementation.

The classical analog of our problem is the transmission of information over a noisy channel; in this situation, error-correcting codes can be applied so as to recover with high probability the transmitted information even after corruption of some percentage of the transmitted bits, where the percentage depends on the Shannon entropy of the channel. We give a quantum analog of the most trivial classical coding scheme: the repetition code, which provides redundancy by duplicating each bit several times [11]. This encoding scheme might be useful when storing qubits in the internal memory of the quantum computer; so that while qubits are in storage they avoid (or at least undergo reduced) decoherence, leaving decoherence to occur mainly in qubits actively involved in the computation.

II. QUANTUM COMPUTATION

In our model of quantum computation (the *gate array* model) we assume that we have s qubits. These qubits start in some specified initial configuration, which we may take to be $|0,0,0,\ldots,0\rangle$. They are then acted on by a sequence of the following operations, which manipulate the state of these s qubits in the corresponding 2^s-dimensional Hilbert space.

(1) Measurement. One qubit is measured in some basis, and the result is recorded classically. This corresponds to a projection operation in the Hilbert space.

(2) Entanglement. Two qubits are entangled according to some four-by-four unitary matrix. The corresponding Hilbert space operation describing the entire s qubits is the tensor product of this four by four unitary matrix with the 2^{s-2} by 2^{s-2} identity matrix. Entanglements of three or more qubits can always be accomplished by a sequence of two-bit entanglements [12].

The sequence of operations can be arbitrary, and there is no reason to assume that it does not depend on the input to the computer. However, in comparing quantum computation with classical computation, in order to prevent the programmer from "cheating" by using the sequence of operations to give the computer information which might otherwise be impossible or difficult to compute, we require that this sequence of operations be generated by a classical computer in polynomial time (in computer science terminology, this keeps the class of problems solvable by a quantum computer *uniform).* The result of the computation is extracted from the computer by measuring the values of the qubits.

We must also initialize the computer by putting its memory in some known state. This could be done by postulating a separate operation, initialize, which sets a qubit to a predetermined value. However, we can also initialize a qubit by first measuring it and then performing a rotation to put it in the proper state [rotations are a special case of operation (2), even though there is no actual entanglement of different qubits taking place].

III. ENCODING

Our encoding is as follows. Suppose we have k qubits that we wish to store. We have our quantum computer encode each of these qubits into nine qubits as follows:

$$|0\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle),$$

$$|1\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle). \tag{3.1}$$

Consider what happens when the nine qubits containing the encoding are read. We will actually read them in a quantum fashion using an ancilla, i.e., by entangling them with other qubits [as in process (2) above] and then measuring some of these other qubits, and not by measuring them directly [as in process (1)]. However, for explanatory purposes, it is best to first consider what happens if the qubits are measured using a Bell basis. This same basis will later be used to "read" them by entangling them with qubits that will then be measured.

Suppose that no decoherence has occurred, and that the first three qubits are in state $|000\rangle+|111\rangle$. This means that the other two sets are also in state $|000\rangle+|111\rangle$. Similarly, if the first three are in state $|000\rangle-|111\rangle$, the other two triplets must also be in this state. Thus, even if one qubit has decohered, when we measure the nine qubits (measuring each triple in the Bell basis $|000\rangle\pm|111\rangle,|001\rangle\pm|110\rangle,|010\rangle\pm|101\rangle,|100\rangle\pm|011\rangle$) we can deduce what the measurement should have been by taking the majority of the three triples, and thus we can tell whether the encoded bit was 0 or a 1. This, however, does not let us restore the first qubit to any superposition or entanglement that it may have been in, because by measuring the nine qubits, we are in effect projecting all the qubits onto a subspace. This process also projects the original encoded bit onto a subspace, and so does not let us recover a superposition of an encoded 0 and an encoded 1.

To preserve the state of superposition of the encoded qubit, what we do in effect is to measure the decoherence without measuring the state of the qubits. This allows us in effect to reverse the decoherence. To explain in detail, we must first examine the decoherence process more fully. The critical assumption here is that decoherence only affects one qubit of our superposition, while the other qubits remain unchanged. It is not clear how reasonable this assumption is physically, but it corresponds to the assumption in classical information theory of the independence of noise.

By quantum mechanics, decoherence must be a unitary process that entangles a qubit with the environment. We can describe this process by describing what happens to two basis states of the qubit undergoing decoherence, $|0\rangle$ and $|1\rangle$. Considering the environment as well, these must be taken to orthogonal states, but if the environment is neglected, they can get taken to any combination of states.

Let us describe more precisely what happens to the qubit that decoheres. We assume that this is the first qubit in the encoding, but the procedure works equally well if any of the

other eight qubits is the one that decoheres. Because $|0\rangle$ and $|1\rangle$ form a basis for the first qubit, we need only consider what happens to these two states. In general, the decoherence process must be

$$|e_0\rangle|0\rangle \rightarrow |a_0\rangle|0\rangle + |a_1\rangle|1\rangle$$
$$|e_0\rangle|1\rangle \rightarrow |a_2\rangle|0\rangle + |a_3\rangle|1\rangle, \tag{3.2}$$

where $|a_0\rangle$, $|a_1\rangle$, $|a_2\rangle$, and $|a_3\rangle$ are states of the environment (not generally orthogonal or normalized). Let us now see what happens to an encoded 0, that is, to the superposition $(1/\sqrt{2})(|000\rangle + |111\rangle)$. After decoherence, it goes to the superposition

$$(1/\sqrt{2})[(|a_0\rangle|0\rangle + |a_1\rangle|1\rangle)|00\rangle + (|a_2\rangle|0\rangle + |a_3\rangle|1\rangle)|11\rangle]. \tag{3.3}$$

We now write this in terms of a Bell basis, obtaining

$$\frac{1}{2\sqrt{2}}(|a_0\rangle + |a_e\rangle)(|000\rangle + |111\rangle)$$
$$+ \frac{1}{2\sqrt{2}}(|a_0\rangle - |a_3\rangle)(|000\rangle - |111\rangle)$$
$$+ \frac{1}{2\sqrt{2}}(|a_1\rangle + |a_2\rangle)(|100\rangle + |011\rangle)$$
$$+ \frac{1}{2\sqrt{2}}(|a_1\rangle - |a_2\rangle)(|100\rangle - |011\rangle). \tag{3.4}$$

Similarly, the vector $|000\rangle - |111\rangle$ goes to

$$\frac{1}{2\sqrt{2}}(|a_0\rangle + |a_3\rangle)(|000\rangle - |111\rangle)$$
$$+ \frac{1}{2\sqrt{2}}(|a_0\rangle - |a_3\rangle)(|000\rangle + |111\rangle)$$
$$+ \frac{1}{2\sqrt{2}}(|a_1\rangle + |a_2\rangle)(|100\rangle - |011\rangle)$$
$$+ \frac{1}{2\sqrt{2}}:(|a_1\rangle - |a_2\rangle)(|100\rangle + |011\rangle). \tag{3.5}$$

The important thing to note is that the state of the environment is the same for corresponding vectors from the decoherence of the two quantum states encoding 0 and encoding 1. Further, we know what the original state of the encoded vector was by looking at the other two triples. Thus, we can restore the original state of the encoded vector and also keep the evolution unitary by creating a few ancillary qubits which tell which qubit decohered and whether the sign on the Bell superposition changed. By measuring these ancillary qubits, we can restore the original state. We still maintain any existing superposition of basis Bell states because the coefficients are the same whether the original vector decohered from the state $|000\rangle + |111\rangle$ or $|000\rangle - |111\rangle$. By measuring the ancillary qubits that tell which qubit was decohered, we in effect restore the original state.

We now describe this restoration process more fully. This restoration consists first of a unitary transformation which we can regard as being performed by a quantum computer, and then a measurement of some of the qubits of the outcome. What the computer first does is compare all three triples in the Bell basis. If these triples are the same, it outputs (in the ancillary qubits) "no decoherence," and leaves the encoded qubits alone. If these triplets are not the same, it outputs which triple is different, and how it is different. The computer must then restore the encoded qubits to their original state. For example, in Eqs. (3.4) and (3.5), the output corresponding to the second line would mean "wrong sign," and the output corresponding to the third line would mean "first qubit wrong, but right sign." These outputs are expressed by some quantum state of the ancilla, which then is measured. Because the coefficients on the corresponding vectors in Eqs. (3.4) and (3.5) are the same, the superposition of states after the measurement and the subsequent corrections will be the same as the original superposition of states before the decoherence. Further, the correction of errors is now a unitary transformation because we are not just correcting the error, but also "measuring" the error, in that we measure what and where the error was, so we do not have to combine two quantum states into one.

If more than one qubit of a nine-tuple decoheres, the encoding scheme does not work. However, the probability that this happens is proportional to the square of the probability that one qubit decoheres. That is, if each qubit decoheres with a probability p, then the probability that k qubits do not decohere is probability $(1-p)^k$. In our scheme, we replace each qubit by nine. The probability that at least two qubits in any particular nine-tuple decohere is $1-(1+8p)\times(1-p)^8 \approx 36p^2$, and the probability that our $9k$ qubits can be decoded to give the original quantum state is approximately $(1-36p^2)^k$. Thus, for a probability of decoherence less than $\frac{1}{36}$, we have an improved storage method for quantum-coherent states of large numbers of qubits. Since p generally increases with storage time the watchdog effect could be used to store quantum information over long periods by using the decoherence restoration scheme to frequently reset the quantum state. If the decoherence time for a qubit is t_d, the above analysis implies that use of the watchdog effect will be advantageous if the quantum state is reset at time intervals $t_r \ll \frac{1}{36} t_d$.

It seems that we are getting something for nothing, in that we are restoring the state of the superposition to the exact original predecoherence state, even though some of the information was destroyed. The reason we can do this is that we expand one qubit to nine encoded qubits, providing some sort of redundancy. Our encoding scheme stores information in the entanglement between qubits, so that no information is stored in any one specific qubit; i.e., measuring any one of the qubits gives no information about the encoded state. Essentially, what we are doing is putting all of the information in the signal into dimensions of the signal space that are unlikely to be affected by decoherence. We can then measure the effect of the decoherence in the other dimensions of this space, which contain no information about our signal, and use this measurement to restore the original signal.

There is a cost for using this scheme. First, the number of qubits is expanded from k to $9k$. Second, the machinery that implements the unitary transformations will not be exact. Thus, getting rid of the decoherence will introduce a small extra amount of error. This may cause problems if we wish to store quantum information for long periods of time by repeatedly using this decoherence reduction technique. If our unitary transformations were perfect, we could keep the information for large times using the watchdog effect by repeatedly measuring the state to eliminate the decoherence. However, each time we get rid of the decoherence (or even check whether there was decoherence) we introduce a small extra amount of error. We must therefore choose the rate at which we measure the state so as to balance the error introduced by decoherence with the error introduced by the restoration of decoherence.

The assumption that the qubits decohere independently is crucial. This is not completely unreasonable physically, and may in many cases be a good approximation of reality, but the effects of changing this assumption on the accuracy of the encoding must be investigated. This assumption corresponds to independence of errors between different bits in classical information theory; even though this does not always hold in practice for classical channels, classical error-correcting codes can still be made to work very well. This is done by exploiting the fact that errors in bits far enough apart from each other are, in fact, nearly independent. It is not clear what the corresponding property would be in a quantum channel, or whether it would hold in practice.

There are clearly improvements that can be made to the above scheme. What this scheme does is use the three-repetition code twice: once in an outer layer (repeating the triplet of qubits three times) and once in an inner layer (using $|000\rangle \pm |111\rangle$ for each triplet). In classical information theory, repetition codes are extremely inefficient. The outer layer of our quantum code can be replaced by a classical error-correcting code to produce a more efficient scheme; this reduces the cost of encoding k qubits from $9k$ qubits to a function that approaches $3k$ qubits asymptotically as k grows. The inner layer of our quantum code, however, needs to have more properties than a classical error-correcting code because it needs to be able to correct errors coherently. While longer repetition codes can be used for this inner layer, it is not immediately clear how to improve on repetition codes for this mechanism, but I believe it should be possible.

This scheme is a step toward the quantum analog of channel coding in classical information theory. Whereas the quantum analog of Shannon's source coding theorem is already known [4,13], it is not even clear how a noisy quantum channel should properly be defined. Other steps in this direction have also recently been taken in [14,15], which deal with transmitting classical information over a quantum channel, and in [16], which deals with transmitting quantum information over a quantum channel, given an auxiliary two-way classical channel. The ultimate goal would be to define the quantum analog of the Shannon capacity for a quantum channel, and find encoding schemes which approach this capacity. An intermediate goal would be to find schemes for faithfully encoding k qubits that use $k+\epsilon k$ qubits, where ϵ approaches 0 as the channel's error rate goes to 0, as in classical information theory.

[1] D. Deutsch, Proc. R. Soc. London Ser. A **400**, 96 (1985).

[2] A. Yao, in *Proceedings of the 34th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1993), p. 352.

[3] D. Deutsch, Proc. R. Soc. London Ser. A **425**, 73 (1989).

[4] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[5] E. Bernstein and U. Vazirani, in *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing* (Association for Computing Machinery, New York, 1993), p. 11.

[6] D. Simon, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 116.

[7] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (Ref. [6]), p. 124.

[8] R. Landauer (unpublished).

[9] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).

[10] A. Berthiaume, D. Deutsch, and R. Jozsa, in *Proceedings of the Workshop on Physics and Computation, PhysComp 94* (IEEE Computer Society, Los Alamitos, CA, 1994), p. 60.

[11] See any information theory textbook for these concepts; for example, T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

[12] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[13] R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994).

[14] A. Fujiwara and H. Nagaoka, Mathematical Engineering Technical Report No. 94-22, University of Tokyo, 1994 (unpublished).

[15] P. Hausladen, B. Schumacher, M. Westmoreland, and W. K. Wooters (unpublished).

[16] C. H. Bennett, G. Brassard, B. Schumacher, J. Smolin, and W. K. Wooters (unpublished).