Good Dynamics versus Bad Kinematics: Is Entanglement Needed for Quantum Computation?

Noah Linden[1] and Sandu Popescu[2]

[1]*Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom*
[2]*HH Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom*
and BRIMS, Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, United Kingdom

(Received 24 June 1999; published 10 July 2001)

We study the role of entanglement in quantum computation. We consider the case of a pure state contaminated by "white noise." This framework arises, for example, in pseudopure state implementations of quantum computing using NMR. We analyze quantum computational protocols which aim to solve exponential classical problems with polynomial resources and ask whether or not entanglement of the pseudopure states is needed to achieve this aim. We show that, for a large class of such protocols, including Shor's factorization, entanglement is necessary. We also show that achieving entanglement is not sufficient: If the state is sufficiently noisy, exponential resources are needed even if entanglement is present.

DOI: 10.1103/PhysRevLett.87.047901 PACS numbers: 03.67.Lx, 76.60.–k, 89.20.Ff

In a beautiful example of how technology can stimulate fundamental physics, the proposals for implementing quantum computing via liquid-state NMR [1–4] have sparked a debate recently on the very nature of quantum computing [5–9]. More precisely, doubts have been raised as to whether entanglement is a necessary requirement for a quantum computer to be able to speed-up a computation (exponentially) relative to a classical computer.

The proposal to use liquid-state NMR with pseudopure states for quantum computing has two important aspects.

(i) Bad kinematics.—On the one hand, liquid-state NMR quantum computing has a great disadvantage: One cannot prepare pure states. This situation is different from the original quantum computation protocols which considered the quantum computer in a pure state $|\Psi\rangle$. Instead, in the NMR protocol, one prepares "pseudopure" states, i.e., mixed states of the form

$$\rho = (1 - \epsilon)M + \epsilon|\Psi\rangle\langle\Psi|, \qquad (1)$$

where M is the maximally mixed state (i.e., the identity density matrix normalized to have trace 1). In other words, in quantum information theory, one says that (1) represents the pure state $|\Psi\rangle$ contaminated with noise. We note that we use the term pseudopure to mean any state of the form (1) without restriction as to how it arises. In liquid-state NMR, states of this form are produced from a thermal density matrix by suitable manipulations leading to a certain scaling of ϵ with the number of qubits. However, we do not assume any behavior of ϵ initially; we consider any state of the form (1).

In addition to the fact that, in liquid-state NMR, one prepares states of the form (1), rather than pure states, it has been shown [6] that in all experiments until now the noise is so large that the pseudopure state ρ is *nonentangled* even if the pure-state component $|\Psi\rangle$ is entangled. Since entanglement is widely considered to be the main ingredient in quantum computing, these results lead to the question as to whether the NMR scheme is a "true" quantum computation [6].

(ii) Good dynamics.—On the other hand, the NMR experiments have a great advantage: one can produce *correct dynamics;* that is, the interactions between the spins are exactly as required in the theoretical quantum computational protocols. Thus if the initial state of the spins would be pure instead of pseudopure, NMR experiments would completely implement the original quantum computation protocols.

Furthermore, the noise in the pseudopure state looks quite benign—it averages to zero (without loss of generality we can consider our observables to be traceless). Thus the expectation value of any operator A when the quantum system is in a given pure state $|\Psi\rangle$ is the same, up to normalization, as the average in the corresponding pseudopure state $\rho = (1 - \epsilon)M + \epsilon|\Psi\rangle\langle\Psi|$, i.e.,

$$\mathrm{Tr}(A\rho) = \epsilon\langle\Psi|A|\Psi\rangle. \qquad (2)$$

Given the good dynamics, some authors have suggested that in fact liquid-state NMR computing is nonetheless a true quantum computation, capable of speeding-up computations relative to classical computers. As a corollary, it was suggested that perhaps entanglement is *not* a *sine-qua-non* requirement for quantum computing [7].

Whether or not entanglement is a necessary condition for quantum computation is a question of fundamental importance. In the present Letter, we study this question for the pseudopure-state quantum computing. Although the particular scheme we study is inspired by liquid-state NMR, its importance goes far beyond NMR since the state we consider (1) is the canonical example of a noise-contaminated state, namely, a pure state contaminated with "white noise."

We analyze quantum computational protocols which aim to solve exponential classical problems with polynomial resources and ask whether or not entanglement of the pseudopure states is needed to achieve this aim. We show that, for a large class of such protocols, including Shor's factorization [10], entanglement of the pseudopure states is necessary: unless the pseudopure state (1) of the quantum computer becomes entangled during the computation, the aim of transforming exponential problems to polynomial ones cannot be achieved.

We will first consider the general effect of noise on the computation, then the relationship between separability and noise.

Consider then a pure-state computational protocol in which the computer starts in the state $|\Psi_0\rangle$ and ends in the state $|\Psi_f\rangle = U|\Psi_0\rangle$, where U is the unitary time evolution operator which describes the computation. The corresponding computation starting with pseudopure state

$$\rho = (1 - \epsilon)M + \epsilon|\Psi_0\rangle\langle\Psi_0| \tag{3}$$

ends up in the state

$$\rho = (1 - \epsilon)M + \epsilon|\Psi_f\rangle\langle\Psi_f|. \tag{4}$$

Upon reaching the final state, a measurement is carried out and the result of the computation is inferred from the result of the measurement.

We will assume the most favorable case that the pure-state protocol gives the correct answer with certainty with a single repetition of the protocol and that, if the result of the computation is found, one can check it with polynomial overhead. We will then show that the pseudopure-state protocol requires of the order of $\frac{1}{\epsilon}$ repetitions. Thus if ϵ becomes exponentially small with N, the number governing the scaling of the classical problem (in other words the noise becomes exponentially large with N), the protocol requires an exponential number of repetitions to get the correct answer. So, for this amount of noise, the quantum protocol with a pseudopure state cannot transform an exponential problem into a polynomial one: even in the best possible case that the pure-state protocol takes one computational step, the protocol with noise takes exponentially many steps. We emphasize that this conclusion applies quite generally to pseudopure-state quantum computing and is independent of the discussion of separability which follows later.

In the state (4) there is a probability ϵ of finding the computer in the "correct" final state $|\Psi_f\rangle$ arising from the term

$$\epsilon|\Psi_f\rangle\langle\Psi_f|, \tag{5}$$

in (4). As stated above, we will assume here the most favorable case, that if the state is $|\Psi_f\rangle$ then, from the outcome of the final measurement, one can infer the solution to the computational problem with certainty with one repetition. We note that in general protocols, such as Shor's algorithm, for example, a single repetition of the protocol is not sufficient to find the correct answer.

There is also the probability $(1 - \epsilon)$ of finding the computer in the maximally mixed state M. In this case, there *is* a possibility that the correct answer will be found, since the noise term contains all possible outcomes with some probability. However, the probability of finding the correct answer from the noise term must be at least exponentially small with N. Otherwise, there would be no need to prepare the computer at all: one could find the correct answer from the noise term simply by repeating the computation a polynomial number of times. In fact, if the probability of finding the correct answer from the noise term did not become exponentially small with N, we could dispense with the computer altogether. For using a classical probabilistic protocol which selected from all the possibilities at random, we would get the correct answer with probability of the order of one with only a polynomial number of trials.

Thus, we may say that the probability of finding the correct answer from the state (4) is essentially ϵ and so the computation must be repeated $\frac{1}{\epsilon}$ times on average to find the correct answer with probability of order one.

We now consider whether reaching entangled states during the computation is a *necessary* condition for exponential speed-up. We address this by investigating what can be achieved with *separable* states. Specifically, we impose the condition that the pseudopure state remains separable during the entire computation. For an important class of computational protocols, we show that this condition implies an exponential amount of noise.

The protocols which we consider use $n = n_1 + n_2$ qubits of which n_1 are considered to be the input registers, and the remaining n_2 the output registers. We assume that n_1 and n_2 are polynomial in the number N which describes how the classical problem scales. As stated earlier, we consider problems in which the quantum protocol gives an exponential speed-up over the classical protocol, specifically the classical protocol is exponential in N whereas the quantum protocol is polynomial in N. (For example, in the factorization problem, the aim is to factor a number of the order of 2^N. The classical protocol is exponential in N and, in Shor's algorithm, n_1 and n_2 are linear in N.)

We first describe the protocols as applied to pure states. The first steps are as follows:

(1) Prepare system in the initial state:

$$|\Psi_0\rangle = |00\cdots0\rangle \otimes |00\cdots0\rangle. \tag{6}$$

(2) Perform a Hadamard transform on the input register, so that the state becomes

$$|\Psi_1\rangle = \frac{1}{2^{n_1/2}} \sum_{x=0}^{2^{n_1}-1} |x\rangle \otimes |00\cdots0\rangle. \tag{7}$$

(3) Evaluate the function $f\colon \{0,1\}^{n_1} \rightarrow \{0,1\}^{n_2}$. The state becomes

$$|\Psi_2\rangle = \frac{1}{2^{n_1/2}} \sum_{x=0}^{2^{n_1}-1} |x\rangle \otimes |f(x)\rangle. \tag{8}$$

Now consider the protocol when applied to a mixed state input. Thus, the initial state ρ_0 is

$$\rho_0 = (1 - \epsilon)M_{2^n} + \epsilon|\Psi_0\rangle\langle\Psi_0|, \tag{9}$$

where $|\Psi_0\rangle$ is given in (6), and M_{2^n} is the maximally mixed state in the 2^n dimensional Hilbert space. After the second computational step the state is

$$\rho_0 = (1 - \epsilon)M_{2^n} + \epsilon|\Psi_2\rangle\langle\Psi_2|. \tag{10}$$

Consider now protocols in which the function $f(x)$ is not constant. Let x_1 and x_2 be values of x such that $f(x_1) \neq f(x_2)$. Thus we may write the state $|\Psi_2\rangle$ as

$$|\Psi_2\rangle = \frac{1}{2^{n_1/2}}(|x_1\rangle|f(x_1)\rangle + |x_2\rangle|f(x_2)\rangle + |\Psi_r\rangle), \tag{11}$$

where $|\Psi_r\rangle$ has no components in the subspace spanned by $|x_1\rangle|f(x_1)\rangle$, $|x_1\rangle|f(x_2)\rangle$, $|x_2\rangle|f(x_1)\rangle$, $|x_2\rangle|f(x_2)\rangle$. It is convenient to relabel these states and write

$$|\Psi_2\rangle = \frac{1}{2^{n_1/2}}(|1\rangle|1\rangle + |2\rangle|2\rangle + |\Psi_r\rangle), \tag{12}$$

where $|\Psi_r\rangle$ has no components in the subspace spanned by $|1\rangle|1\rangle$, $|1\rangle|2\rangle$, $|2\rangle|1\rangle$, $|2\rangle|2\rangle$.

We now derive a necessary condition on ϵ for the state of the system to be separable throughout the computation. For consider projecting each particle onto the subspace spanned by $|1\rangle$ and $|2\rangle$. The state after projection is

$$\begin{aligned}\rho_2' &= \frac{1}{A}\left[\frac{4(1-\epsilon)}{2^{n_1+n_2}}M_4 + \frac{2\epsilon}{2^{n_1}}\left(\frac{|1\rangle|1\rangle + |2\rangle|2\rangle}{\sqrt{2}}\right)\left(\frac{\langle 1|\langle 1| + \langle 2|\langle 2|}{\sqrt{2}}\right)\right] \\ &= (1-\epsilon')M_4 + \epsilon'\left(\frac{|1\rangle|1\rangle + |2\rangle|2\rangle}{\sqrt{2}}\right)\left(\frac{\langle 1|\langle 1| + \langle 2|\langle 2|}{\sqrt{2}}\right),\end{aligned} \tag{13}$$

where

$$A = \left(\frac{4(1-\epsilon)}{2^{n_1+n_2}} + \frac{2\epsilon}{2^{n_1}}\right) \tag{14}$$

is the normalization factor, M_4 is the maximally mixed state in the four-dimensional Hilbert space spanned by $|1\rangle|1\rangle$, $|1\rangle|2\rangle$, $|2\rangle|1\rangle$, $|2\rangle|2\rangle$, and

$$\epsilon' = \frac{2\epsilon}{2^{n_1}A} = \frac{\epsilon}{(1-\epsilon)2^{-n_2+1} + \epsilon}. \tag{15}$$

Now a two qubit state of the form

$$(1-\delta)M_4 + \delta\left(\frac{|1\rangle|1\rangle + |2\rangle|2\rangle}{\sqrt{2}}\right)\left(\frac{\langle 1|\langle 1| + \langle 2|\langle 2|}{\sqrt{2}}\right) \tag{16}$$

is entangled for $\delta > 1/3$. Therefore the original state (10) must have been entangled unless

$$\epsilon' \leq 1/3 \Rightarrow \epsilon \leq \frac{1}{1 + 2^{n_2}}, \tag{17}$$

since local projections cannot create entangled states from unentangled ones.

Therefore we conclude that, if we have a computational protocol (for nonconstant f) starting with a mixed state of the form (9) and if we require that the state remains separable throughout the protocol, then we certainly need

$$\epsilon \leq \frac{1}{1 + 2^{n_2}}. \tag{18}$$

However, we have shown earlier that, even in favorable circumstances, a computation with noise ϵ takes of the order of $1/\epsilon$ repetitions to get the correct answer with probability of the order of one.

Thus, we reach our main result that computational protocols of the sort we have considered require exponentially many repetitions. So no matter how efficient the original pure-state protocol is, the mixed-state protocol, which is sufficiently noisy that it remains separable for all N, will *not* transform an exponential classical problem into a polynomial one.

We note that, while we have considered protocols of a specific form, many of the details are unimportant. As long as the number of qubits n_1 and n_2 in the output register is polynomial in the number N which governs the classical problem, and the pure-state protocol goes through a state which has a non-negligible amount of entanglement, similar conclusions can be drawn.

We repeat here that our conclusions apply only to separable states of pseudopure-state form (1). We have nothing to say at this stage about separable states of other forms. We have also considered only exponential speed-up so that our results do not apply to Grover's algorithm, for example [11]. Furthermore, we cannot rule out the possibility of the future discovery of more efficient algorithms of Shor type to which our results do not apply.

We have shown earlier that having entanglement is a necessary condition. Is it sufficient? Our earlier results show that it is not. As long as the noise is exponential (i.e., ϵ decreases exponentially with n), the computation has to be repeated an exponential number of times, even if entangled states are reached during the computation (we note that it is known that there are entangled states with an exponential amount of noise [6]).

Finally, let us return to NMR quantum computation which gave rise to the issues we have been discussing. In our previous discussion we had in mind that one has a single quantum computer and $1/\epsilon$ then gives the number of times the computation has to be repeated. In NMR, each molecule in the sample is considered to be a quantum computer. Here, rather than repeating the computation on the same computer, one treats a large number of computers in parallel. Thus, $1/\epsilon$ would be the number of individual molecular computers one would need in the sample.

However, the NMR scheme has a number of difficulties beyond those we have discussed above concerning the measurement of the final state of the system. In fact, rather than being able to address each molecule individually, as we have assumed in our discussion above, one can measure only bulk properties of the sample.

For example, suppose the computational protocol requires measuring the first qubit in the computational basis. In the discussion above, we supposed that such a measurement can be performed. In NMR the first qubit is realized as the spin of, say, the first nucleus in the molecule. But we cannot measure the spin of each molecule. Rather, we can measure only the total spin of this nucleus (i.e., over all molecules in the sample). Furthermore, of course, we cannot measure this total spin exactly; we can make only macroscopic measurements; i.e., we can find only the value of this total spin with a broad resolution.

Overall, these factors mean that NMR has a far less favorable situation than we have assumed in the general discussion above. Thus, $1/\epsilon$ is a lower bound on the sample scaling required.

The usual construction of pseudopure states in NMR has $\epsilon \sim \frac{n}{2^n}$. In light of the discussion in the previous paragraph, the sample size would therefore have to grow exponentially with n. Thus, this framework does not allow one to convert exponential classical problems into polynomial ones via Shor-type protocols.

Of course, other ways of using liquid-state NMR as a quantum computer might be found with more favorable scaling than current techniques. Whether or not this is possible is obviously beyond the scope of this paper.

We are grateful to Sam Braunstein, Carlton Caves, Richard Jozsa, and Ruediger Schack for many illuminating discussions and to David Collins for pointing out an error in an earlier draft.

[1] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).

[2] D. G. Cory, M. D. Price, and T. F. Havel, Physica (Amsterdam) **120D**, 82 (1998).

[3] N. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).

[4] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung, Proc. R. Soc. London A **454**, 447 (1998).

[5] W. Warren, Science **277**, 1688 (1997).

[6] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).

[7] R. Laflamme, review of "Separability of very noisy mixed states and implications for NMR quantum computing," by S. Braunstein *et al.,* in *Quick Reviews in Quantum Computation and Information,* http://quantum-computing.lanl.gov/qcreviews/qc/.

[8] T. F. Havel, S. S. Somaroo, C.-H. Tseng, and D. G. Cory, quant-ph/9812086.

[9] R. Schack and C. M. Caves, quant-ph/9903101.

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

[11] L. Grover, Phys. Rev. Lett. **79**, 325 (1997).