Scaling considerations in ground-state quantum computation

Ari Mizel, M. W. Mitchell, and Marvin L. Cohen
Department of Physics, University of California at Berkeley, Berkeley, California 94720
and Materials Sciences Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720
(Received 2 September 1999; published 15 January 2002)

We study design challenges associated with realizing a ground-state quantum computer. In such a computer, it is necessary that the energy gap between the ground state and first excited state be sufficiently large to prevent disruptive excitations. Here, an estimate of this gap is provided as a function of computer size. We then address the problem of detecting the output of a ground-state quantum computer. It is shown that the exponential detection difficulties that appear to be present at first can be overcome by small design changes.

DOI: 10.1103/PhysRevA.65.022315 PACS number(s): 03.67.Lx

I. INTRODUCTION

Recently, there has been intense interest among researchers in the possibility of designing quantum computers [1] that calculate using the remarkable properties of quantum mechanics [2–4]. Although the potential power of quantum-computation algorithms is enticing, there is great difficulty associated with actually fabricating a quantum computer in the laboratory. A variety of schemes have been suggested [5–18] and progress has been encouraging, but the feasibility of realizing a useful quantum computer is still unclear.

In a recent paper, we proposed a ground-state quantum-computation approach that could circumvent some of the main problems suffered by traditional quantum-computer designs [19]. This approach replaces the progress of a usual, time-dependent quantum computation with a single, time-independent state. To see how this works, let us suppose that a quantum-computation algorithm consists of the evolution of M qubits through N steps defined by $2^M \times 2^M$ unitary matrices $\mathcal{U}_j$, $j=1,\ldots,N$. To define the state of M qubits at one step of the algorithm requires 2^M amplitudes. To describe the M qubits at every step of the algorithm, from before it begins until after it ends, requires $(N+1)\times 2^M$ amplitudes. If we do not demand that the qubits evolve simultaneously from step to step, allowing qubit 1 be at step 2 while qubit 3 is at step 6, then $[2(N+1)]^M$ amplitudes are required to map out the development of the qubits. Let us suppose that we collect these $[2(N+1)]^M$ amplitudes into a state $|\Psi\rangle$ defined on a Hilbert space of dimension $[2(N+1)]^M$. This state will contain all the information in a time-dependent quantum computation, but the state itself will be completely time independent. Instead of developing through time in accordance with an algorithm, the state will develop through Hilbert space in accordance with the algorithm.

How can we explicitly describe this development through Hilbert space? The projection of $|\Psi\rangle$ onto some 2^M-dimensional subspace will contain the 2^M amplitudes necessary to describe the state of the M qubits when they are all at step 0 and have undergone no unitary evolution. Let us call this projection $P_0|\Psi\rangle$. More generally, let us call $P_j|\Psi\rangle$ the projection onto the 2^M-dimensional subspace that describes the state of the M qubits when they are at step j, $j=0,\ldots,N$. Suppose that we define an operator $A_{j,0}$ that carries the 2^M basis vectors of the subspace associated with P_0 into the 2^M basis vectors of the subspace associated with P_j. Then, $|\Psi\rangle$ develops in accordance with a quantum-computation algorithm if and only if

$$P_j|\Psi\rangle = \mathcal{U}_j\mathcal{U}_{j-1}\cdots\mathcal{U}_1 A_{j,0}P_0|\Psi\rangle \tag{1}$$

for $j=1,\ldots,N$.

This formal notion makes it possible to propose a ground-state approach to quantum computation. In ground-state quantum computation, we do not make a register of qubits evolve in time by subjecting it to a series of time-dependent Hamiltonians. Instead, we perform calculations by manufacturing a Hamiltonian H whose ground state satisfies Eq. (1). This is described precisely in Ref. [19]. In that paper, an appropriate Hamiltonian H is found. It is comprised of a sum of (i) one-body terms denoted like $h_a^k(U_{a,k})$ where $U_{a,k}$ indicates the unitary evolution of qubit a at algorithmic step k of the calculation and (ii) two-body terms designated $h_{a,b}^j$ (CNOT), where CNOT represents a controlled-NOT operation, associated with a controlled-NOT operation of qubit b by qubit a at step j. In [19], a hypothetical physical realization of H is suggested using states localized on quantum dots to comprise the $[2(N+1)]^M$, dimensional Hilbert space.

This ground-state, time-independent approach has the attractive characteristic that it can defend against time-dependent environmental decoherence problems associated with time evolution. However, it does have its own challenging aspects that need to be addressed. Many of these challenges concern the scaling of a ground-state quantum computer—the feasibility of making such a computer larger and larger. In this paper, we address two of the most important considerations involved in increasing the size of a ground-state quantum computer. First, we study how the energy gap between the ground state and first excited state of the Hamiltonian H will depend on N and M. Clearly, if a ground-state quantum computer is to function properly the gap must be large enough in energy that the computer will reliably remain in its ground state. (Of course, we are assuming here that the computer can be placed in its ground state to begin with. The problem of cooling a system to the ground state is the subject of an extensive simulated annealing literature [20] that has been applied to classical ground-state computation in cellular automata [21,22]. In implementing a quantum ground-state computer, it is essential to address the

issue of cooling time; one approach might be to turn on gradually the tunneling matrix elements in the Hamiltonian. The cooling strategy is best addressed in connection with a specific computer implementation; here we are concerned instead with general properties of the formalism [19].) Second, we investigate the problem of measuring the outcome of a ground-state quantum computation. In its most naive form, a ground-state quantum computer seems very difficult to probe as it grows in size. We propose several means of addressing this difficulty.

II. GAP

In order to compute correctly, a ground-state quantum computer must reside in its ground state. This condition is to be achieved, not by isolating the computer from the environment and waiting for it to decay spontaneously, but by directly cooling the system through contact with a bath. For the system to remain in its ground state once put there, it is necessary that the temperature k_BT of the bath be well below the energy gap between the ground state of the computer and the first excited state. (In fact, this is necessary, but not sufficient. A large number g of low-lying excited states would reduce the required temperature by a factor of $\ln g$. However, we expect this g to grow roughly linearly in M, so the $\ln g$ factor should be relatively unimportant.)

Of course, it is not possible to achieve arbitrarily low temperatures, so we need to study the size of the energy gap between ground state and first excited state. One might worry that the energy gap will decrease quickly as the computer grows in size, severely limiting the length of practical computations. Here, we address this concern by studying the size dependence of the gap of the Hamiltonian described in [19]. We argue that the gap shrinks approximately like $1/(N+1)^2$ and prove the existence of a lower bound that scales as $1/(N+1)^4$.

A. Single qubit

To obtain these quantitative estimates of the gap, we first consider the case of a single qubit computer. Here, the Hamiltonian is simply $H=\Sigma_{i=1}^{N}h^i(U_i)$, where [19]

$$h^i(U)\equiv\epsilon[C_{i-1}^{\dagger}C_{i-1}+C_i^{\dagger}C_i-(C_i^{\dagger}UC_{i-1}+\text{H.c.})] \quad (2)$$

is associated with the development of the single qubit from step $i-1$ to step i of the calculation. (Note that the energy scale ϵ and the C operators are independent of M, N [19].) It is convenient to make a unitary transformation from the C_i operators to new operators $(\Pi_{j=1}^{i}U_j^{\dagger})C_i$. This changes the form of the Hamiltonian to $H=\Sigma_{i=1}^{N}h^i(I)$, where every U_i that appears in H has been replaced by the 2×2 identity matrix I. To determine the eigenspectrum of this new H, we solve the determinantal equation $\det(H-E)=0$. The determinant is evaluated by deriving and solving a recursion relation on matrices of increasing size. We find that

$$\det(H-E)=\epsilon^{2(N+1)}\frac{k-2+1/k}{k-1/k}\left(k^{2(N+1)}-\frac{1}{k^{2(N+1)}}\right), \quad (3)$$

where $k=(1-E/2\epsilon)+\sqrt{(1-E/2\epsilon)^2-1}$. Setting the determinant (3) to zero yields eigenenergies $E=E_m\equiv2\epsilon(1-\cos[\pi m/2(N+1)])$, where m is an integer between 0 and $2N+1$. The ground state has energy $E=E_0=0$, and the first excited state has energy $E=E_1=2\epsilon(1-\cos[\pi/2(N+1)])\rightarrow\epsilon\pi^2/[2(N+1)]^2$ for large N. Thus, the gap decreases as $1/(N+1)^2$. This is true for a single qubit, and also for any number of noninteracting qubits.

B. One controlled-NOT gate

Of course, a useful quantum computer must have interactions among qubits, so the behavior of the gap must be examined when interactions are present. To begin, we address the case of exactly two qubits interacting through exactly one controlled-NOT gate. The full Hamiltonian includes single qubit $h^j(U_i)$ terms and one $h^j(\text{CNOT})$ interaction term at stage j.

We begin by examining the Hamiltonian with the h^j (CNOT) term omitted. Without the $h^j(\text{CNOT})$ term, the computer has two disjoint regions for each qubit, one ''upstream'' of the omitted controlled-NOT gate consisting of stages 0 to $j-1$ and one ''downstream'' of the omitted controlled-NOT gate consisting of stages j to N. Since an electron in one of the disjoint regions will possess the eigenspectrum of a single, noninteracting qubit, the first excited state in such a region will have an amount of energy of order $1/(N+1)^2$. If we neglect such ''high-energy'' states, only the (doubly degenerate) ground states of the two regions make important contributions to the electronic state of each qubit. This means that each qubit has four available states, leading to an effective 16-dimensional Hilbert space for the two qubit system.

It is straightforward to diagonalize the interaction Hamiltonian $h^j(\text{CNOT})$ analytically in this 16×16 basis. The result is a (fourfold degenerate) ground state of the computer with zero energy, an (eightfold degenerate) first excited state with energy $\epsilon/(j)(N-j+1)$, and a (fourfold degenerate) second excited state with energy $\epsilon/(N-j+1)^2+\epsilon/(j)(N-j+1)+\epsilon/(j)^2$. So, the energy of the gap in the 16-dimensional Hilbert space scales as $\epsilon/(j)(N-j+1)\sim1/N^2$.

What relationship does the gap in this 16-dimensional Hilbert space have to the exact gap of the system? The (fourfold degenerate) ground state in this 16-dimensional Hilbert space is, in fact, the exact ground state in the whole Hilbert space. Hence, the (eightfold degenerate) first excited state in the 16-dimensional Hilbert space is actually orthogonal to the exact ground state of the system. It follows that the quantity $\epsilon/(j)(N-j+1)$ represents a rigorous variational upper bound to the exact first excited state energy of the system.

The variational upper bound should provide a reasonable estimate of the true value of the gap. However, for our purposes we are perhaps more interested in having a guaranteed lower bound to the gap. Such a lower bound would ensure that, when less than a specified amount of energy is available, the computer will not experience a disruptive excitation. As it turns out, it is possible to show that the gap has a rigorous lower bound of $\alpha/(N+1)^4$ for some real positive α. The following is an argument by contradiction.

We know the ground state of the Hamiltonian H has energy zero. Suppose that $|\psi\rangle$ is some state of the two-particle system that is orthogonal to the ground state of H. Assume that the expectation value $\langle\psi|H|\psi\rangle$ satisfies

$$\langle\psi|H|\psi\rangle < \alpha/(N+1)^4 \equiv E_{\text{lower}}. \tag{4}$$

To evaluate the left-hand side and draw a contradiction, we split the Hamiltonian H into H_0, which consists of only single-body terms, and $H_1 = h^j(\text{CNOT})$, which consists of only interaction terms. Both H_0 and H_1, it is straightforward to show, are positive semidefinite. Consider the form of $|\psi\rangle$ in a basis of eigenstates of H_0,

$$|\psi\rangle = \sum_{n,i} c_{n,i}|\phi_{n,i}\rangle, \tag{5}$$

where the i labels the degenerate eigenstates with the nth eigenenergy. Saying that $|\psi\rangle$ is orthogonal to the (fourfold degenerate) ground state of H essentially means that $|\psi\rangle$ has no contribution from the four states $|\phi_{n,i}\rangle$ for which $H_0 + H_1|\phi_{n,i}\rangle = 0$. Therefore, $|\psi\rangle$ can consist of a superposition of eigenstates of H_0 with eigenenergies greater than zero and the 12 zero-energy eigenstates of H_0 that are orthogonal to the (fourfold degenerate) ground state of the system.

Further reflection shows that $|\psi\rangle$ cannot involve exclusively the 12 zero-energy eigenstates of H_0 because then $\langle\psi\rangle H|\psi\rangle$ would go like $1/(N+1)^2$, as we showed above, violating the assumption (4). The state must, therefore, possess some contributions from excited eigenstates of H_0. These states have eigenenergies of at least $\epsilon\pi^2/[2(N+1)]^2$, as we saw in our single qubit analysis, so assumption (4) limits the contribution from such states to $\Sigma_{n>0,i}|c_{n,i}|^2 < E_{\text{lower}}/(\epsilon\pi^2/[2(N+1)]^2)$. This limit exists even though H_1 is present since H_1 is positive semidefinite and cannot decrease the expectation value produced by H_0. Hence we find that

$$\begin{aligned}
\langle\psi|H|\psi\rangle = &\sum_{i,j} c^*_{n=0,i}c_{n=0,j}\langle\phi_{n=0,i}|H_0+H_1|\phi_{n=0,j}\rangle \\
&+ \sum_{n>0,m>0,i,j} c^*_{n,i}c_{m,j}\langle\phi_{n,i}|H_0+H_1|\phi_{m,j}\rangle \\
&+ \sum_{m>0,i,j} (c^*_{m,i}c_{n=0,j}\langle\phi_{m,i}|H_1|\phi_{n=0,j}\rangle \\
&+ c^*_{n=0,i}c_{m,j}\langle\phi_{n=0,i}|H_1|\phi_{m,j}\rangle)
\end{aligned} \tag{6}$$

$$\begin{aligned}
> &\frac{\epsilon}{(N+1)^2}\left(1-\sum_{n>0,i}|c_{n,i}|^2\right) \\
&+ \frac{\epsilon\pi^2}{[2(N+1)]^2}\sum_{n>0,i}|c_{n,i}|^2 \\
&- 2\left|\sum_i c_{n=0,i}\right|\left|\sum_{m>0,i} c_{m,i}\right|\frac{\mu}{(N+1)^2}
\end{aligned} \tag{7}$$

$$\begin{aligned}
> &\frac{\epsilon}{(N+1)^2} + 0 - 2|\sqrt{12}| \\
&\times\left|\sqrt{4(N+1)^2-16}\left(\frac{E_{\text{lower}}}{\epsilon\pi^2/[2(N+1)]^2}\right)^{1/2}\right| \\
&\times\frac{\mu}{(N+1)^2},
\end{aligned} \tag{8}$$

where $-\mu/(N+1)^2$ is less than the most negative value of $\langle\phi_{m>0,i}|H_1|\phi_{n=0,j}\rangle$. (The parameter μ can be chosen so that it does not increase with N or M.) This last inequality contradicts the assumption (4), however, since

$$\begin{aligned}
&\frac{\epsilon}{(N+1)^2} + 0 - 2|\sqrt{12}| \\
&\quad\times\left|\sqrt{4(N+1)^2-16}\left(\frac{E_{\text{lower}}}{\epsilon\pi^2/[2(N+1)]^2}\right)^{1/2}\right|\frac{\mu}{(N+1)^2} \\
&= \frac{1}{(N+1)^2}\left(\epsilon - 2|\sqrt{12}|\right. \\
&\quad\left.\times\left|\left(\frac{4(N+1)^2-16}{(N+1)^2}\right)^{1/2}\left(\frac{\alpha}{\epsilon\pi^2/4}\right)^{1/2}\right|\mu\right)
\end{aligned} \tag{9}$$

$$> E_{\text{lower}} \tag{10}$$

provided that α is chosen to be sufficiently small. This contradiction shows that the assumption (4) is not valid. Since the ground state has energy zero, and any state orthogonal to the ground state has energy at least E_{lower}, we have a lower bound E_{lower} on the value of the gap.

C. Arbitrary computer

It is straightforward to apply these results to the case of M qubits interacting via an arbitrary number of controlled-NOT gates. First of all the variational upper bound on the gap of $\epsilon/(j)(N-j+1)$ still holds. This is because different controlled-NOT Hamiltonians $h^j_{a,b}(\text{CNOT})$ commute with one another, so we can treat each separately when diagonalizing in a basis of zero energy, M-particle eigenstates of H_0.

The lower bound on the gap of order $1/(N+1)^4$ also still holds, which we demonstrate in the following way. The Hamiltonian consists of H_0, that governs the single qubit development between controlled-NOT gates and the controlled-NOT gate terms $h^j_{a,b}(\text{CNOT})$ themselves. We begin by dividing H_0 into parts labeled $(H_0)^j_{a,b}$ where the index j, a,b suggests proximity to the controlled-NOT gate controlled by Hamiltonian $h^j_{a,b}(\text{CNOT})$. Let $(H_0)^j_{a,b}$ consist of terms that control the single qubit development of qubit a between controlled-NOT gate j,a,b and the previous controlled-NOT operation experienced by qubit a, terms that control the single qubit development of qubit a between controlled-NOT gate j,a,b and the next controlled-NOT operation experienced by qubit a, terms that control the single qubit development of qubit b between controlled-NOT gate j,a,b and the previous controlled-NOT operation experienced

by qubit b, and terms that control the single qubit development of qubit b between controlled-NOT gate j,a,b and the next controlled-NOT operation experienced by qubit b. By this definition of the $(H_0)^j_{a,b}$, we have $H_0=\frac{1}{2}\Sigma_{j,a,b}(H_0)^j_{a,b}$ plus extra positive semi-definite one body terms that are near the first or last stages of the computer.

Now, with this division described, we are in a position to demonstrate the lower bound of order $1/(N+1)^4$. Suppose that some M-particle state $|\psi\rangle$ is orthogonal to the (2^M-fold degenerate) ground state of the system. It is possible to write $|\psi\rangle$ in the form

$$|\psi\rangle=\sum_{n,i} c_{n,i}|\phi_{n,i}\rangle, \tag{11}$$

where the $|\phi_{n,i}\rangle$ are M-particle eigenstates of H_0. Because $|\psi\rangle$ is orthogonal to the ground state of the system, each term $|\phi_{n,i}\rangle$ that appears in $|\psi\rangle$ must satisfy $(H_0)^j_{a,b}+h^j_{a,b}(\mathrm{CNOT})|\phi_{n,i}\rangle\neq 0$ for some controlled-NOT gate j, a, b. Let us call $|\psi^j_{a,b}\rangle$ the sum of the components $c_{n,i}|\phi_{n,i}\rangle$ that satisfy $(H_0)^j_{a,b}+h^j_{a,b}(\mathrm{CNOT})|\phi_{n,i}\rangle\neq 0$. If any $|\phi_{n,i}\rangle$ could belong in more than one $|\psi^j_{a,b}\rangle$, we include it in every possible $|\psi^j_{a,b}\rangle$. Then,

$$\langle\psi|H|\psi\rangle\geqslant\sum_{j,a,b}\langle\psi^j_{a,b}|\tfrac{1}{2}(H_0)^j_{a,b}+h^j_{a,b}(\mathrm{CNOT})|\psi^j_{a,b}\rangle \tag{12}$$

$$\geqslant\tfrac{1}{2}\sum_{j,a,b}\langle\psi^j_{a,b}|\psi^j_{a,b}\rangle\frac{\alpha}{(N+1)^4} \tag{13}$$

$$\geqslant\frac{\alpha}{2(N+1)^4}\sim\frac{1}{(N+1)^4}, \tag{14}$$

where we have made use of the lower bound $\alpha/(N+1)^4$ derived in Sec. I. The last inequality holds because every component of $|\psi\rangle$ appears in at least one of the $|\psi^j_{a,b}\rangle$. This result shows that a lower bound $\sim 1/(N+1)^4$ holds for an arbitrary number of qubits and controlled-NOT gates.

III. DETECTION

The task of detecting the result of a ground-state computation seems daunting at first. It seems that each qubit in the computer must be measured in the final stage [19], which it only visits with probability $1/(N+1)$. Since there are M qubits, the probability of making a successful measurement seems to scale as $1/(N+1)^M$, which quickly goes to zero as the computer increases in size. In fact, this assessment is too much pessimistic.

If the final state output by a quantum algorithm is classical in form, it is actually possible to obtain a successful measurement with certainty. This is very significant, since it is known how to modify Grover's algorithm and other important algorithms so that they fall into this category [8,23,24]. Even Shor's algorithm can be modified to produce output that is almost classical in form.

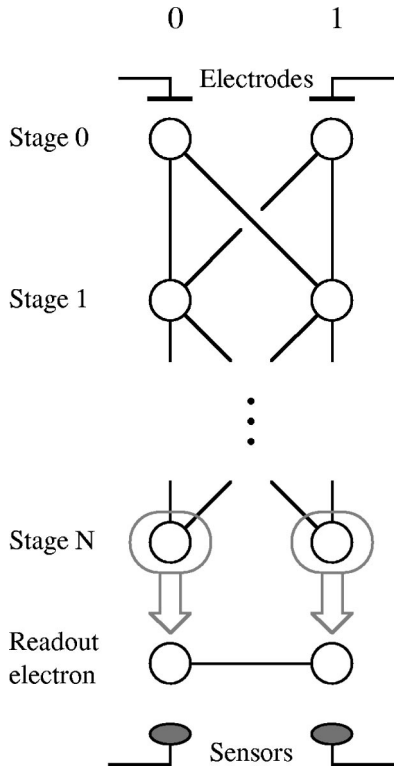

FIG. 1. Additional readout electrons are placed after the final stage of each qubit. The position of these additional electrons indicates the outcome of the algorithm.

How can a successful measurement be guaranteed in the case of classical output? For concreteness, consider the quantum dot implementation of [19]. In this implementation, classical output implies that an electron in the ground state either reaches the left dot of the final stage and never the right dot or the right dot of the final stage and never the left dot. In other words, the ground-state charge density vanishes at half of the dots of the final stage. It is, therefore, possible to obtain the result of the calculation (without disturbing the ground state) by measuring the electric field produced by each electron near the final stage. For example, an additional readout electron could be placed just after the final stage of each qubit, as in Fig. 1. Since the qubit electron will only reach one of its two dots in the final stage, the readout electron will be forced to stay in one of its two possible locations by the Coulomb interaction. That is, the readout electron will be localized to the left (right) if its qubit is in the right (left) at the final stage. The ground state of the entire system, qubit electrons and readout electrons included, will be a product of the ground state of the qubit electrons and a classical state of the readout electrons. The outcome of the algorithm can always be determined by detecting the position of the readout electrons, even though the qubit electrons have only a small probability of residing at the final stage.

Although this readout electron method is guaranteed to work for an algorithm for which the final state of the qubits is classical, it will not work otherwise since the readout electrons will become entangled with the qubit electrons and spoil Eq. (1). An approach that applies to the general case

involves the adjusting the Hamiltonian at the final stage N for each qubit a [19]. Suppose that the operator $C^{\dagger}_{a,N}$ is replaced by $(1/\lambda)C^{\dagger}_{a,N}$ everywhere it appears in the Hamiltonian and $C_{a,N}$ by $(1/\lambda)C_{a,N}$, where $1/\lambda$ is a small fraction. All algorithms will still work just as before, but we are ''tipping'' the computer toward the final stage so that the qubits reside there more often. Then, it follows that in the ground state of the system, each qubit has λ times greater amplitude on the final stage than on the previous stages. The probability of detecting all qubits on the final stage is of order $1/(1+N/\lambda^2)^M$. If $1/\lambda$ is set to be of order, say $1/\sqrt{MN}$, we find that the probability of all qubits being at the final stage goes as approximately $1/(1+1/M)^M$, which approaches $\exp(-1)$. For this very extreme choice of λ, it only takes two or three attempts to catch all of the qubits at the final stage.

Of course, the change in the Hamiltonian will affect the gap. If the final operators are scaled by a factor $1/\lambda$ then the quantity $\det(H-E)$ of noninteracting qubits will change to

$$\det(H-E)=\epsilon^{2(N+1)}\frac{k-2+1/k}{k-1/k}\left[k^{2(N+1)}-\frac{1}{k^{2(N+1)}}+[(1/\lambda)^2-1]\left(k^{2N+1}-\frac{1}{k^{2N+1}}\right)\right]. \qquad (15)$$

Setting this determinant to zero, we find that the gap of noninteracting qubits still scales roughly as $1/(N+1)^2$ for $1/\lambda$ between zero and one. Once controlled-NOT gates are included, however, the gap will have a variational upper bound of order $1/(N+1)(N+\lambda^2)$ and a lower bound of $E_{\text{lower}}=\alpha/(N+1)^2(N+\lambda^2)^2$. If $1/\lambda=1/\sqrt{MN}$, then the upper bound is $1/(NM+N)(N+1)$ and the lower bound $E_{\text{lower}}=\alpha/(N+1)^2(NM+N)^2$.

Another technique for alleviating measurement problems is to ''synchronize'' the arrival of the qubits at the final stage. In our controlled-NOT gate, the target electron cannot proceed beyond the gate until the control electron has. A controlled ''identity'' gate could be constructed that would function similarly, preventing a target electron from proceeding beyond the gate until after a control electron, but always subjecting the target qubit to an identity operation and never a NOT operation. With this gate, the arrival of the qubits at the final stage could be ''synchronized.'' Suppose that each qubit controls the entry of the next qubit to a ground-state quantum computer's final stages, using a controlled identity gate. Then, whenever qubit M is found in the final stage, all qubits are in the final stage. This could be useful for detection schemes, although it would not enhance the overall probability of finding the qubits at the final stage of the computer.

IV. CONCLUSION

In this paper, we have explored some important challenges to constructing a ground-state quantum computer. First, we found upper and lower bounds for the energy gap between the computer's ground state and first excited state. The bounds provide guidelines to making a computer of a specified size that can be relied upon to remain in its ground state. Next, several schemes were presented for easing qubit detection difficulties. These schemes indicate how to design a ground-state quantum computer so that it will yield output with certainty, for some of the most important algorithms, or at least high probability, for general algorithms. It is hoped that the analysis of energy gap and detection in this paper complements our initial proposal and eases the task of designing and fabricating a ground-state quantum computer in the laboratory.

ACKNOWLEDGMENTS

We gratefully thank D. A. Lidar, V. J. Mizel, and M. Mosca for helpful comments and references. This work was supported by National Science Foundation Grant No. DMR-9520554, the Director, Office of Energy Research, Office of Basic Energy Services, Materials Sciences Division of the U.S. Department of Energy under Contract No. DE-AC03-76SF00098, and the Office of Naval Research Grant No. N000149610034.

[1] D. Deutsch and A. Ekert, Phys. World **11**(3), 47 (1998).
[2] P. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE, New York, 1994), p. 124.
[3] L. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation* (ACM, New York, 1996), pp. 212–219.
[4] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[5] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[6] C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995).
[7] Q. A. Turchette *et al.*, Phys. Rev. Lett. **75**, 4710 (1995).
[8] N. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
[9] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).
[10] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).
[11] G. Burkhard, D. Loss, and D. P. DiVincenzo, Phys. Rev. B **59**, 2070 (1999).
[12] A. Shnirman, G. Schon, and Z. Hermon, Phys. Rev. Lett. **79**, 2371 (1997).
[13] Y. Makhlin, G. Schon, and A. Shnirman, Nature (London) **398**, 305 (1999).
[14] D. V. Averin, Solid State Commun. **105**, 659 (1998).
[15] Y. Nakamura, Yu. A. Pashkin, J. S. Tsai, Nature (London) **398**, 786 (1999).
[16] J. E. Mooij *et al.*, Science **285**, 1036 (1999).
[17] B. Kane, Nature (London) **393**, 133 (1998).
[18] L. B. Ioffe, V. B. Geshkenbein, M. V. Feigel'man, A. L. Fauchere, and G. Blatter, Nature (London) **398**, 679 (1999).
[19] A. Mizel, M. W. Mitchell, and M. L. Cohen, Phys. Rev. A **63**, 040302(R) (2001).

[20] S. Kirkpatrick, C. D. Gelatt, Jr., and M. P. Vecchi, Science **220**, 671 (1983).
[21] M. Akazawa, Y. Amemiya, and N. Shibata, J. Appl. Phys. **82**, 5176 (1997).
[22] M. Macucci, G. Iannaccone, S. Francaviglia, and B. Pellegrini, Int. J. Circ. Theor. Appl. **29**, 37 (2001).
[23] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, e-print quant-ph/0005055.
[24] G. Brassard and P. Hoyer, e-print quant-ph/9704027.