Quantum search by measurement

Andrew M. Childs,* Enrico Deotto,† Edward Farhi,‡ and Jeffrey Goldstone§

Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Sam Gutmann‖

Department of Mathematics, Northeastern University, Boston, Massachusetts 02115

Andrew J. Landahl¶

Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125

We propose a quantum algorithm for solving combinatorial search problems that uses only a sequence of measurements. The algorithm is similar to quantum computation by adiabatic evolution, in that the goal is to remain in the ground state of a time-varying Hamiltonian. Indeed, we show that the running times of the two algorithms are closely related. We also show how to achieve the quadratic speedup for Grover's unstructured search problem with only two measurements. Finally, we discuss some similarities and differences between the adiabatic and measurement algorithms.

I. INTRODUCTION

In the conventional circuit model of quantum computation, a program for a quantum computer consists of a discrete sequence of unitary gates chosen from a fixed set. The memory of the quantum computer is a collection of qubits initially prepared in some definite state. After a sequence of unitary gates is applied, the qubits are measured in the computational basis to give the result of the computation, a classical bit string.

This description of a quantum computer has been used to formulate quantum algorithms that outperform classical methods, notably Shor's factoring algorithm [1] and Grover's algorithm for unstructured search [2]. Subsequent development of quantum algorithms has focused primarily on variations of the techniques introduced by Shor and Grover. One way to motivate new algorithmic ideas is to consider alternative (but, in general, equivalent) descriptions of the way a quantum computer operates. For example, the technique of quantum computation by adiabatic evolution [3] is most easily described by a quantum computer that evolves continuously according to a time-varying Hamiltonian. With this approach, the state of the quantum computer remains close to the instantaneous ground state of the time-varying Hamiltonian, which is engineered so that the ground state of the final Hamiltonian encodes the solution to a computational problem.

Another model of quantum computation allows measurement at intermediate stages. Indeed, recent work has shown that *measurement alone* is universal for quantum computa-

tion: one can efficiently implement a universal set of quantum gates using only measurements (and classical processing) [4–7]. In this paper, we describe an algorithm for solving combinatorial search problems that consists only of a sequence of measurements. Using a straightforward variant of the quantum Zeno effect (see, for example, [8–10]), we show how to keep the quantum computer in the ground state of a smoothly varying Hamiltonian $H(s)$. This process can be used to solve a computational problem by encoding the solution to the problem in the ground state of the final Hamiltonian just as in adiabatic quantum computation.

The organization of the paper is as follows. In Sec. II, we present the algorithm in detail and describe how measurement of $H(s)$ can be performed on a digital quantum computer. In Sec. III, we estimate the running time of the algorithm in terms of spectral properties of $H(s)$. Then, in Sec. IV, we discuss how the algorithm performs on Grover's unstructured search problem and show that, by a suitable modification, Grover's quadratic speedup can be achieved by the measurement algorithm. Finally, in Sec. V, we discuss the relationship between the measurement algorithm and quantum computation by adiabatic evolution.

II. THE MEASUREMENT ALGORITHM

Our algorithm is conceptually similar to quantum computation by adiabatic evolution [3], a general method for solving combinatorial search problems using a quantum computer. Both algorithms operate by remaining in the ground state of a smoothly varying Hamiltonian $H(s)$ whose initial ground state is easy to construct and whose final ground state encodes the solution to the problem. However, whereas adiabatic quantum computation uses Schrödinger evolution under $H(s)$ to remain in the ground state, the present algorithm uses *only* measurement of $H(s)$.

In general, we are interested in searching for the minimum of a function $h(z)$ that maps n-bit strings to nonnegative real numbers. Many computational problems can be

————
*Electronic address: amchilds@mit.edu
†Electronic address: deotto@mitlns.mit.edu
‡Electronic address: farhi@mit.edu
§Electronic address: goldston@mit.edu
‖Electronic address: sgutm@neu.edu
¶Electronic address: alandahl@caltech.edu

cast as minimizations of such functions; for specific examples and their relationship to adiabatic quantum computation, see [3,11]. We restrict our attention to the case where the global minimum of $h(z)$ is unique. Associated with this function, we can define a *problem Hamiltonian* H_P through its action on computational basis states:

$$H_P|z\rangle = h(z)|z\rangle. \tag{1}$$

Finding the global minimum of $h(z)$ is equivalent to finding the ground state of H_P. If the global minimum is unique, then this ground state is nondegenerate.

To reach the ground state of H_P, we begin with the quantum computer prepared in the ground state of some other Hamiltonian H_B, the *beginning Hamiltonian*. Then we consider a one-parameter family of Hamiltonians $H(s)$ that interpolates smoothly from H_B to H_P for $s \in [0,1]$. In other words, $H(0) = H_B$ and $H(1) = H_P$, and the intermediate $H(s)$ is a smooth function of s. One possible choice is linear interpolation,

$$H(s) = (1-s)H_B + sH_P. \tag{2}$$

Now we divide the interval $[0,1]$ into M subintervals of width $\delta = 1/M$. So long as the interpolating Hamiltonian $H(s)$ is smoothly varying and δ is small, the ground state of $H(s)$ will be close to the ground state of $H(s+\delta)$. Thus, if the system is in the ground state of $H(s)$ and we measure $H(s+\delta)$, the postmeasurement state is very likely to be the ground state of $H(s+\delta)$. If we begin in the ground state of $H(0)$ and successively measure $H(\delta), H(2\delta), \ldots, H((M-1)\delta), H(1)$, then the final state will be the ground state of $H(1)$ with high probability, assuming δ is sufficiently small.

To complete our description of the quantum algorithm, we must explain how to measure the operator $H(s)$. The technique we use is motivated by von Neumann's description of the measurement process [8]. In this description, measurement is performed by coupling the system of interest to an ancillary system, which we call the *pointer*. Suppose that the pointer is a one-dimensional free particle and that the system-pointer interaction Hamiltonian is $H(s) \otimes p$, where p is the momentum of the particle. Furthermore, suppose that the mass of the particle is sufficiently large that we can neglect the kinetic term. Then the resulting evolution is

$$e^{-itH(s) \otimes p} = \sum_a \left[|E_a(s)\rangle\langle E_a(s)| \otimes e^{-itE_a(s)p} \right], \tag{3}$$

where $|E_a(s)\rangle$ are the eigenstates of $H(s)$ with eigenvalues $E_a(s)$, and we have set $\hbar = 1$. Suppose we prepare the pointer in the state $|x=0\rangle$, a narrow wave packet centered at $x=0$. Since the momentum operator generates translations in position, the above evolution performs the transformation

$$|E_a(s)\rangle \otimes |x=0\rangle \to |E_a(s)\rangle \otimes |x=tE_a(s)\rangle. \tag{4}$$

If we can measure the position of the pointer with sufficiently high precision that all relevant spacings $x_{ab} = t|E_a(s) - E_b(s)|$ can be resolved, then measurement of the

position of the pointer—a fixed, easy-to-measure observable, independent of $H(s)$—effects a measurement of $H(s)$.

Von Neumann's measurement protocol makes use of a continuous variable, the position of the pointer. To turn it into an algorithm that can be implemented on a fully digital quantum computer, we can approximate the evolution (3) using r quantum bits to represent the pointer [12,13]. The full Hilbert space is thus a tensor product of a 2^n-dimensional space for the system and a 2^r-dimensional space for the pointer. We let the computational basis of the pointer, with basis states $\{|z\rangle\}$, represent the basis of momentum eigenstates. The label z is an integer between 0 and $2^r - 1$, and the r bits of the binary representation of z specify the states of the r qubits. In this basis, the digital representation of p is

$$p = \sum_{j=1}^{r} 2^{-j} \frac{1 - \sigma_z^{(j)}}{2}, \tag{5}$$

a sum of diagonal operators, each of which acts on only a single qubit. Here $\sigma_z^{(j)}$ is the Pauli z operator on the jth qubit. As we will discuss in the next section, we have chosen to normalize p so that

$$p|z\rangle = \frac{z}{2^r}|z\rangle, \tag{6}$$

which gives $\|p\| \sim 1$. If $H(s)$ is a sum of terms, each of which acts on at most k qubits, then $H(s) \otimes p$ is a sum of terms, each of which acts on at most $k+1$ qubits. As long as k is a fixed constant independent of the problem size n, such a Hamiltonian can be simulated efficiently on a quantum computer [14]. Expanded in the momentum eigenbasis, the initial state of the pointer is

$$|x=0\rangle = \frac{1}{2^{r/2}} \sum_{z=0}^{2^r - 1} |z\rangle. \tag{7}$$

The measurement is performed by evolving under $H(s) \otimes p$ for a total time τ. We discuss how to choose τ in the next section. After this evolution, the position of the simulated pointer could be measured by measuring the qubits that represent it in the x basis, i.e., the Fourier transform of the computational basis. However, note that our algorithm only makes use of the postmeasurement state of the system, not of the measured value of $H(s)$. In other words, only the reduced density matrix of the system is relevant. Thus it is not actually necessary to perform a Fourier transform before measuring the pointer, or even to measure the pointer at all. When the system-pointer evolution is finished, one can either reprepare the pointer in its initial state $|x=0\rangle$ or discard it and use a new pointer, and immediately begin the next measurement.

As an aside, note that the von Neumann measurement procedure described above is identical to the well-known phase estimation algorithm for measuring the eigenvalues of a unitary operator [15,16], which can also be used to produce eigenvalues and eigenvectors of a Hamiltonian [17]. This connection has been noted previously in [13], and it has been

pointed out that the measurement is a nondemolition measurement in [18]. In the phase estimation problem, we are given an eigenvector $|\psi\rangle$ of a unitary operator U and asked to determine its eigenvalue $e^{-i\phi}$. The algorithm uses two registers, one that initially stores $|\psi\rangle$ and one that will store an approximation of the phase ϕ. The first and last steps of the algorithm are Fourier transforms on the phase register. The intervening step is to perform the transformation

$$|\psi\rangle \otimes |z\rangle \rightarrow U^z |\psi\rangle \otimes |z\rangle, \qquad (8)$$

where $|z\rangle$ is a computational basis state. If we take $|z\rangle$ to be a momentum eigenstate with eigenvalue z [i.e., if we choose a different normalization from that in Eq. (6)] and let $U = e^{-iHt}$, this is exactly the transformation induced by $e^{-i(H \otimes p)t}$. Thus we see that the phase estimation algorithm for a unitary operator U is exactly von Neumann's prescription for measuring $i \ln U$.

III. RUNNING TIME

The running time of the measurement algorithm is the product of M, the number of measurements, and τ, the time per measurement. Even if we assume perfect projective measurements, the algorithm is guaranteed to keep the computer in the ground state of $H(s)$ only in the limit $M \rightarrow \infty$, so that $\delta = 1/M \rightarrow 0$. Given a finite running time, the probability of finding the ground state of H_P with the last measurement will be less than 1. To understand the efficiency of the algorithm, we need to determine how long we must run as a function of n, the number of bits on which the function h is defined, so that the probability of success is not too small. In general, if the time required to achieve a success probability greater than some fixed constant (e.g., $\frac{1}{2}$) is poly(n), we say the algorithm is efficient, whereas if the running time grows exponentially, we say it is not.

To determine the running time of the algorithm, we consider the effect of the measurement process on the reduced density matrix of the system. Here, we simply motivate the main result; for a detailed analysis, see Appendix A.

Let $\rho^{(j)}$ denote the reduced density matrix of the system after the jth measurement; its matrix elements are

$$\rho_{ab}^{(j)} = \langle E_a(j\delta)|\rho^{(j)}|E_b(j\delta)\rangle. \qquad (9)$$

The interaction with the digitized pointer effects the transformation

$$|E_a(s)\rangle \otimes |z\rangle \rightarrow e^{-iE_a(s)zt/2^r}|E_a(s)\rangle \otimes |z\rangle. \qquad (10)$$

Starting with the pointer in the state (7), evolving according to (10), and tracing over the pointer, the quantum operation induced on the system is

$$\rho_{ab}^{(j+1)} = \kappa_{ab}^{(j+1)} \sum_{c,d} U_{ac}^{(j)} \rho_{cd}^{(j)} U_{bd}^{(j)*}, \qquad (11)$$

where the unitary transformation relating the energy eigenbases at $s=j\delta$ and $s=(j+1)\delta$ is
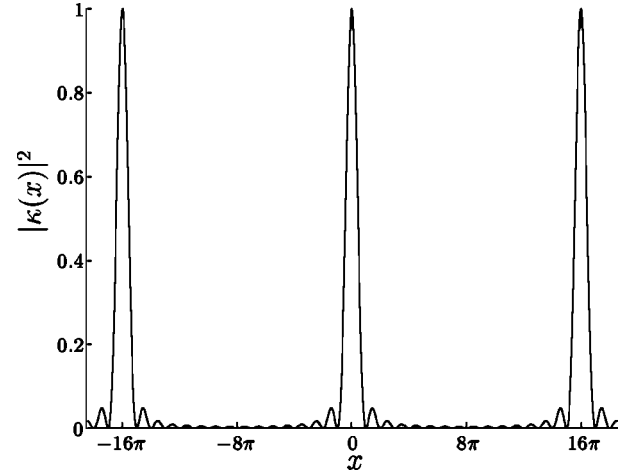

FIG. 1. The function $|\kappa(x)|^2$ for $r=4$.

$$U_{ab}^{(j)} = \langle E_a((j+1)\delta)|E_b(j\delta)\rangle \qquad (12)$$

and

$$\kappa_{ab}^{(j)} = \frac{1}{2^r} \sum_{z=0}^{2^r-1} e^{i[E_b(j\delta)-E_a(j\delta)]zt/2^r}. \qquad (13)$$

Summing this geometric series, we find

$$|\kappa_{ab}^{(j)}|^2 = |\kappa([E_b(j\delta)-E_a(j\delta)]t/2)|^2, \qquad (14)$$

where

$$|\kappa(x)|^2 = \frac{\sin^2 x}{4^r \sin^2(x/2^r)}. \qquad (15)$$

This function is shown in Fig. 1 for the case $r=4$. It has a sharp peak of unit height and width of order 1 at the origin, and identical peaks at integer multiples of $2^r\pi$.

If the above procedure were a perfect projective measurement, then we would have $\kappa_{ab}=0$ whenever $E_a \neq E_b$. Assuming (temporarily) that this is the case, we find

$$\rho_{00}^{(j+1)} \geqslant |U_{00}^{(j)}|^2 \rho_{00}^{(j)} \qquad (16)$$

with the initial condition $\rho_{00}^{(0)}=1$ and $\rho_{ab}^{(0)}=0$ otherwise. Perturbation theory gives

$$|U_{00}^{(j)}|^2 = 1 - \delta^2 \sum_{a \neq 0} \frac{|\langle E_a(s)|(dH/ds)|E_0(s)\rangle|^2}{[E_0(s)-E_a(s)]^2}\bigg|_{s=j\delta} + O(\delta^3) \qquad (17)$$

$$\geqslant 1 - \frac{\Gamma(j\delta)^2\delta^2}{g(j\delta)^2} + O(\delta^3), \qquad (18)$$

where

$$\Gamma(s)^2 = \langle E_0(s)|(dH/ds)^2|E_0(s)\rangle$$
$$- \langle E_0(s)|(dH/ds)|E_0(s)\rangle^2 \qquad (19)$$

and

$$g(s) = E_1(s) - E_0(s) \tag{20}$$

is the energy gap between the ground and first excited states. If we let

$$\Gamma = \max_{s \in [0,1]} \Gamma(s), \tag{21}$$

$$g = \min_{s \in [0,1]} g(s), \tag{22}$$

then according to Eq. (16) the probability of being in the ground state after the last measurement is at least

$$\rho_{00}^{(M)} \geq \left[1 - \frac{\Gamma^2}{M^2 g^2} + O(M^{-3}) \right]^M \tag{23}$$

$$= \exp\left(-\frac{\Gamma^2}{M g^2} \right) + O(M^{-2}). \tag{24}$$

The probability of success is close to 1 provided

$$M \gg \frac{\Gamma^2}{g^2}. \tag{25}$$

When H_B and H_P are both sums of poly(n) terms, each of which acts nontrivially on at most a constant number of qubits, it is easy to choose an interpolation such as Eq. (2) so that Γ is only poly(n). Thus we are mainly interested in the behavior of g, the *minimum gap* between the ground and first excited states. We see that, for the algorithm to be successful, the total number of measurements must be much larger than $1/g^2$.

In fact, the simulated von Neumann procedure is not a perfect projective measurement. We must determine how long the system and pointer should interact so that the measurement is sufficiently good. The analysis in Appendix A shows that $|\kappa_{01}^{(j)}|^2$ should be bounded below 1 by a constant for all j. In other words, to sufficiently resolve the difference between the ground and first excited states, we must decrease the coherence between them by a fixed fraction per measurement. The width of the central peak in Fig. 1 is of order 1, so it is straightforward to show that to have $|\kappa(x)|^2$ less than, say, 1/2, we must have $x \geq O(1)$. This places a lower bound on the system-pointer interaction time of

$$\tau \geq \frac{O(1)}{g} \tag{26}$$

independent of r, the number of pointer qubits. (Note that the same bound also holds in the case of a continuous pointer with a fixed resolution length.)

Putting these results together, we find that the measurement algorithm is successful if the total running time $T = M\tau$ satisfies

$$T \gg \frac{\Gamma^2}{g^3} \quad \text{(measurement)}. \tag{27}$$

This result can be compared to the corresponding expression for quantum computation by adiabatic evolution,

$$T \gg \frac{\Gamma}{g^2} \quad \text{(adiabatic)}. \tag{28}$$

Note that the same quantity appears in the numerator of both expressions; in both cases, Γ accounts for the possibility of transitions to all possible excited states.

The adiabatic and measurement algorithms have qualitatively similar behavior: if the gap is exponentially small, neither algorithm is efficient, whereas if the gap is only polynomially small, both algorithms are efficient. However, the measurement algorithm is slightly slower: whereas adiabatic evolution runs in a time that grows as $1/g^2$, the measurement algorithm runs in a time that grows as $1/g^3$. To see that this comparison is fair, recall that we have defined the momentum in Eq. (5) so that $\|p\| \sim 1$, which gives $\|H(s)\| \sim \|H(s) \otimes p\|$. Alternatively, we can compare the number η of few-qubit unitary gates needed to simulate the two algorithms on a conventional quantum computer. Using the Lie product formula

$$e^{A+B} \simeq (e^{A/m} e^{B/m})^m, \tag{29}$$

which is valid provided $m \gg \|A\|^2 + \|B\|^2$, we find $\eta = O(1/g^4)$ for adiabatic evolution and $\eta = O(1/g^6)$ for the measurement algorithm, in agreement with the previous comparison.

The argument we have used to motivate Eq. (27) is explained in greater detail in Appendix A. There, we also consider the number of qubits r that must be used to represent the pointer. We show that if the gap is only polynomially small in n, it is always sufficient to take $r = O(\log n)$. However, we argue that generally a single qubit will suffice.

IV. THE GROVER PROBLEM

The unstructured search problem considered by Grover is to find a particular unknown n-bit string w (the marked state, or the *winner*) using only queries of the form "Is z the same as w?" [2]. In other words, one is trying to minimize a function

$$h_w(z) = \begin{cases} 0, & z = w, \\ 1, & z \neq w. \end{cases} \tag{30}$$

Since there are 2^n possible values for w, the best possible classical algorithm uses $\Theta(2^n)$ queries. However, Grover's algorithm requires only $\Theta(2^{n/2})$ queries, providing a (provably optimal [19]) quadratic speedup. In Grover's algorithm, the winner is specified by an *oracle* U_w with

$$U_w |z\rangle = (-1)^{h_w(z)} |z\rangle. \tag{31}$$

This oracle is treated as a black box that one can use during the computation. One call to this black box is considered to be a single query of the oracle.

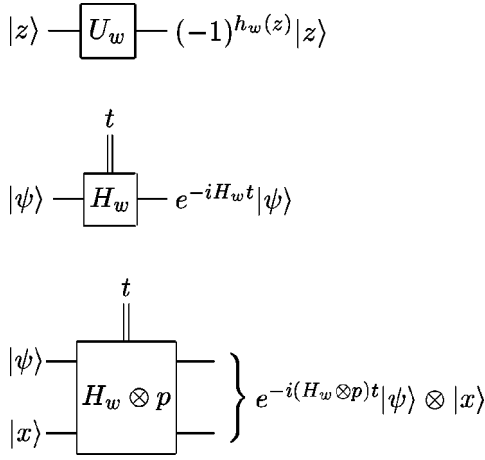In addition to Grover's original algorithm, quadratic speedup can also be achieved in a time-independent Hamil-

FIG. 2. Oracles for the Grover problem. (a) Top: Grover's original oracle. (b) Center: An oracle that performs evolution according to H_w. The double line indicates a classical control parameter, the time for which the Hamiltonian is applied. (c) Bottom: An oracle that allows one to measure H_w.

tonian formulation [20] or by adiabatic quantum computation [21,22]. In either of these formulations, the winner is specified by an "oracle Hamiltonian"

$$H_w = 1 - |w\rangle\langle w| \tag{32}$$

whose ground state is $|w\rangle$ and that treats all orthogonal states (the nonwinners) equivalently. One is provided with a black box that implements H_w, where w is unknown, and is asked to find w. Instead of counting queries, the efficiency of the algorithm is quantified in terms of the total time for which one applies the oracle Hamiltonian.

Here, we show that if we are given a slightly different black box, we can achieve quadratic speedup using the measurement algorithm. We let the problem Hamiltonian be $H_P = H_w$ and we consider a one-parameter family of Hamiltonians $H(s)$ given by Eq. (2) for some H_B. Because we would like to *measure* this Hamiltonian, it is not sufficient to be given a black box that allows one to evolve the system according to H_w. Instead, we will use a black box that evolves the system and a pointer according to $H_w \otimes p$, where p is the momentum of the pointer. This oracle is compared to the previous two in Fig. 2. By repeatedly alternating between applying this black box and evolving according to $H_B \otimes p$, each for small time, we can produce an overall evolution according to the Hamiltonian $[sH_B + (1-s)H_P] \otimes p$, and thus measure the operator $H(s)$ for any s.

Now consider the beginning Hamiltonian

$$H_B = \sum_j \frac{1 - \sigma_x^{(j)}}{2}, \tag{33}$$

where $\sigma_x^{(j)}$ is the Pauli x operator acting on the jth qubit. This beginning Hamiltonian is a sum of local terms, and has the easy-to-prepare ground state $|E_0(0)\rangle = 2^{-n/2}\Sigma_z|z\rangle$, the uniform superposition of all possible bit strings in the computational basis. If we consider the interpolation (2), then one can show [3] that the minimum gap occurs at

$$s^* = 1 - \frac{2}{n} + O(n^{-2}), \tag{34}$$

where the gap takes the value

$$g(s^*) = 2^{1-n/2}[1 + O(n^{-1})]. \tag{35}$$

Naively applying Eq. (27) gives a running time $T = O(2^{3n/2})$, which is even worse than the classical algorithm.

However, since we know the value of s^* independent of w, we can improve on this approach by making fewer measurements. We observe that in the limit of large n, the ground state of $H(s)$ is close to the ground state $|E_0(0)\rangle$ of H_B for $s \lesssim s^*$ and is close to the ground state $|E_0(1)\rangle = |w\rangle$ of H_P for $s \gtrsim s^*$, switching rapidly from one state to the other in the vicinity of $s = s^*$. In Appendix B, we show that up to terms of order $1/n$, the ground state $|\psi_+\rangle$ and the first excited state $|\psi_-\rangle$ of $H(s^*)$ are the equal superpositions

$$|\psi_\pm\rangle \simeq \frac{1}{\sqrt{2}}[|E_0(0)\rangle \pm |E_0(1)\rangle] \tag{36}$$

of the initial and final ground states (which are nearly orthogonal for large n). If we prepare the system in the state $|E_0(0)\rangle$ and make a perfect measurement of $H(s^*)$ followed by a perfect measurement of $H(1)$, we find the result w with probability $\frac{1}{2}$. The same effect can be achieved with an imperfect measurement, even if the pointer consists of just a single qubit. First consider the measurement of $H(s^*)$ in the state $|E_0(0)\rangle$. After the system and pointer have interacted for a time t according to Eq. (10) with $r=1$, the reduced density matrix of the system in the $|\psi_+\rangle, |\psi_-\rangle$ basis is approximately

$$\frac{1}{2}\begin{pmatrix} 1 & e^{ig(s^*)t/4}\cos[g(s^*)t/4] \\ e^{-ig(s^*)t/4}\cos[g(s^*)t/4] & 1 \end{pmatrix}. \tag{37}$$

If we then measure $H(1)$ (i.e., measure in the computational basis), the probability of finding w is approximately

$$\frac{1}{2}\sin^2[g(s^*)t/4]. \tag{38}$$

To get an appreciable probability of finding w, we choose $t = \Theta(2^{n/2})$.

This approach is similar to the way one can achieve quadratic speedup with the adiabatic algorithm. Schrödinger time evolution governed by Eq. (2) does not yield quadratic speedup. However, because s^* is independent of w, we can change the Hamiltonian quickly when the gap is big and more slowly when the gap is small. Since the gap is only of size $\sim 2^{-n/2}$ for a region of width $\sim 2^{-n/2}$, the total oracle time with this modified schedule need only be $O(2^{n/2})$. This has been demonstrated explicitly by solving for the optimal schedule using a different beginning Hamiltonian H_B' that is not a sum of local terms [21,22], but it also holds using the beginning Hamiltonian (33).

Note that measuring $H(s^*)$ is not the only way to solve the Grover problem by measurement. More generally, we can start in some w-independent state, measure the operator

$$\tilde{H} = H_w + K, \tag{39}$$

where K is also independent of w, and then measure in the computational basis. For example, suppose we choose

$$K = 1 - |\psi\rangle\langle\psi|, \tag{40}$$

where $|\psi\rangle$ is a w-independent state with the property $|\langle w|\psi\rangle| \sim 2^{-n/2}$ for all w. (If we are only interested in the time for which we use the black box shown in Fig. 2(c), i.e., if we are only interested in the oracle query complexity, then we need not restrict K to be a sum of local terms.) In Eq. (40), the coefficient of -1 in front of $|\psi\rangle\langle\psi|$ has been fine tuned so that $|\psi\rangle + |w\rangle$ is the ground state of $\tilde{H}$ (choosing the phase of $|w\rangle$ so that $\langle w|\psi\rangle$ is real and positive). If the initial state has a large overlap with $|\psi\rangle$, then the measurement procedure solves the Grover problem. However, the excited state $|\psi\rangle - |w\rangle$ is also an eigenstate of $\tilde{H}$, with an energy higher by of order $2^{-n/2}$. Thus the time to perform the measurement must be $\Omega(2^{n/2})$.

The measurement procedures described above saturate the well-known lower bound on the time required to solve the Grover problem. Using an oracle like the one shown in Fig. 2(a), Bennett *et al.* showed that the Grover problem cannot be solved on a quantum computer using fewer than of order $2^{n/2}$ oracle queries [19]. By a straightforward modification of their argument, an equivalent result applies using the oracle shown in Fig. 2(c). Thus every possible $\tilde{H}$ as in Eq. (39) that can be measured to find w must have a gap between the energies of the relevant eigenstates of order $2^{-n/2}$ or smaller.

V. DISCUSSION

We have described a way to solve combinatorial search problems on a quantum computer using only a sequence of measurements to keep the computer near the ground state of a smoothly varying Hamiltonian. The basic principle of this algorithm is similar to quantum computation by adiabatic evolution, and the running times of the two methods are closely related. Because of this close connection, many results on adiabatic quantum computation can be directly imported to the measurement algorithm—for example, its similarities and differences with classical simulated annealing [23]. We have also shown that the measurement algorithm can achieve quadratic speedup for the Grover problem using knowledge of the place where the gap is smallest, as in adiabatic quantum computation.

One of the advantages of adiabatic quantum computation is its inherent robustness against error [24]. In adiabatic computation, the particular path from H_B to H_P is unimportant as long as the initial and final Hamiltonians are correct, the path is smoothly varying, and the minimum gap along the path is not too small. Exactly the same considerations apply to the measurement algorithm. However, the adiabatic algorithm also enjoys robustness against thermal transitions out of the ground state: if the temperature of the environment is much smaller than the gap, then such transitions are suppressed. The measurement algorithm might not possess this kind of robustness, since the Hamiltonian of the quantum computer during the measurement procedure is not simply $H(s)$.

Although it does not provide a computational advantage over quantum computation by adiabatic evolution, the measurement algorithm is an alternative way to solve general combinatorial search problems on a quantum computer. The algorithm can be simply understood in terms of measurements of a set of operators, without reference to unitary time evolution. Nevertheless, we have seen that to understand the running time of the algorithm, it is important to understand the dynamical process by which these measurements are realized.

APPENDIX A: THE MEASUREMENT PROCESS

In Sec. III, we discussed the running time of the measurement algorithm by examining the measurement process. In this appendix, we present the analysis in greater detail. First, we derive the bound on the running time by demonstrating Eqs. (25) and (26). We show rigorously that these bounds are sufficient as long as the gap is only polynomially small and the number of qubits used to represent the pointer is $r = O(\log n)$. Finally, we argue that $r=1$ qubit should be sufficient in general.

Our goal is to find a bound on the final success probability of the measurement algorithm. We consider the effect of the measurements on the reduced density matrix of the system, which can be written as the block matrix

$$\rho = \begin{pmatrix} \mu & \nu^\dagger \\ \nu & \chi \end{pmatrix}, \tag{A1}$$

where $\mu = \rho_{00}$, $\nu_a = \rho_{a0}$ for $a \neq 0$, and $\chi_{ab} = \rho_{ab}$ for $a, b \neq 0$. Since $\text{tr}\rho = 1$, $\mu = 1 - \text{tr}\chi$. For ease of notation, we suppress j, the index of the iteration, except where necessary. The unitary transformation (12) may also be written as a block matrix. Define $\epsilon = \Gamma \delta/g$. Using perturbation theory and the unitarity constraint, we can write

$$U = \begin{pmatrix} u & -w^\dagger V + O(\epsilon^3) \\ w & V + O(\epsilon^2) \end{pmatrix}, \tag{A2}$$

where $|u|^2 \geqslant 1 - \epsilon^2 + O(\epsilon^3)$, $\|w\|^2 \leqslant \epsilon^2 + O(\epsilon^3)$, and V is a unitary matrix. We let $\|\cdot\|$ denote the l_2 vector or matrix norm as appropriate. Furthermore, let

$$\kappa = \begin{pmatrix} 1 & k^\dagger \\ k & J \end{pmatrix}. \qquad (A3)$$

From Eq. (11), the effect of a single measurement may be written

$$\rho' = (U\rho U^\dagger) \circ \kappa, \qquad (A4)$$

where $\circ$ denotes the elementwise (Hadamard) product. If we assume $\|\nu\| = O(\epsilon)$, we find

$$\mu' = |u|^2 \mu - w^\dagger V \nu - \nu^\dagger V^\dagger w + O(\epsilon^3), \qquad (A5)$$

$$\nu' = [V\nu + \mu w - V\chi V^\dagger w + O(\epsilon^2)] \circ k. \qquad (A6)$$

Now we use induction to show that our assumption always remains valid. Initially, $\nu^{(0)} = 0$. Using the triangle inequality in Eq. (A6), we find

$$\|\nu'\| \leqslant [\|\nu\| + \epsilon + O(\epsilon^2)]\tilde{k}, \qquad (A7)$$

where

$$\tilde{k} = \max_{j,a} |k_a^{(j)}|. \qquad (A8)$$

So long as $\tilde{k} < 1$, we can sum a geometric series, extending the limits to go from 0 to ∞, to find

$$\|\nu^{(j)}\| \leqslant \frac{\epsilon}{1 - \tilde{k}} + O(\epsilon^2) \qquad (A9)$$

for all j. In other words, $\|\nu\| = O(\epsilon)$ so long as $\tilde{k}$ is bounded below 1 by a constant.

Finally, we put a bound on the final success probability $\mu^{(M)}$. Using the Cauchy-Schwartz inequality in Eq. (A5) gives

$$\mu' \geqslant (1 - \epsilon^2)\mu - \frac{2\epsilon^2}{1 - \tilde{k}} + O(\epsilon^3). \qquad (A10)$$

Iterating this bound M times with the initial condition $\mu^{(0)} = 1$, we find

$$\mu^{(M)} \geqslant 1 - \frac{\Gamma^2}{Mg^2}\left(1 + \frac{2}{1 - \tilde{k}}\right) + O(M\epsilon^3). \qquad (A11)$$

If $\tilde{k}$ is bounded below 1 by a constant (independent of n), we find the condition (25) as claimed in Sec. III.

The requirement on $\tilde{k}$ gives the bound (26) on the measurement time τ, and also gives a condition on the number of pointer qubits r. To see this, we must investigate properties of the function $|\kappa(x)|^2$ defined in Eq. (15) and shown in Fig. 1. It is straightforward to show that $|\kappa(x)|^2 \leqslant 1/2$ for $\pi/2 \leqslant x \leqslant \pi(2^r - 1/2)$. Thus, if we want $\tilde{k}$ to be bounded below 1 by a constant, we require

$$\pi/2 \leqslant [E_a(s) - E_0(s)]t/2 \leqslant \pi(2^r - 1/2) \qquad (A12)$$

for all s and for all $a \neq 0$. The left hand bound with $a = 1$ gives $t \geqslant \pi/g$, which is Eq. (26). Requiring the right hand bound to hold for the largest energy difference gives the additional condition $2^r \gtrsim (E_{2^n - 1} - E_0)/g$. Since we only consider Hamiltonians $H(s)$ that are sums of poly(n) terms of bounded size, the largest possible energy difference must be bounded by a polynomial in n. If we further suppose that g is only polynomially small, this condition is satisfied by taking

$$r = O(\log n), \qquad (A13)$$

as claimed at the end of Sec. III. Thus we see that the storage requirements for the pointer are rather modest.

However, the pointer need not comprise even this many qubits. Since the goal of the measurement algorithm is to keep the system close to its ground state, it would be surprising if the energies of highly excited states were relevant. Suppose we take $r = 1$; then $|\kappa(x)|^2 = \cos^2(x/2)$. As before, Eq. (26) suffices to make $|\kappa_{01}|^2$ sufficiently small. However, we must also consider terms involving $|\kappa_{0a}|^2$ for $a > 1$. The algorithm will fail if the term $\mu w \circ k$ in Eq. (A6) accumulates to be $O(1)$ over M iterations. This will only happen if, for $O(M)$ iterations, most of $\|w\|$ comes from components w_a with $(E_a - E_0)t$ close to an integer multiple of 2π. In such a special case, changing t will avoid the problem. An alternative strategy would be to choose t from a random distribution independently at each iteration.

APPENDIX B: EIGENSTATES IN THE GROVER PROBLEM

Here, we show that the ground state of $H(s^*)$ for the Grover problem is close to Eq. (36). Our analysis follows Sec. 4.2 of [3].

Since the Grover problem is invariant under the choice of w, we consider the case $w = 0$ without loss of generality. In this case, the problem can be analyzed in terms of the total spin operators

$$S_a = \frac{1}{2} \sum_{j=1}^{n} \sigma_a^{(j)}, \qquad (B1)$$

where $a = x, y, z$ and $\sigma_a^{(j)}$ is the Pauli a operator acting on the jth qubit. The Hamiltonian commutes with $\vec{S}^2 = S_x^2 + S_y^2 + S_z^2$, and the initial state has $\vec{S}^2 = (n/2)((n/2) + 1)$, so we can restrict our attention to the $(n+1)$-dimensional subspace of states with this value of $\vec{S}^2$. In this subspace, the eigenstates of the total spin operators satisfy

$$S_a |m_a = m\rangle = m |m_a = m\rangle \qquad (B2)$$

for $m = -n/2, -n/2 + 1, \ldots, n/2$. Written in terms of the total spin operators and eigenstates, the Hamiltonian is

$$H(s) = (1-s)\left(\frac{n}{2} - S_x\right) + s\left(1 - \left|m_z = \frac{n}{2}\right\rangle\left\langle m_z = \frac{n}{2}\right|\right).$$
(B3)

The initial and final ground states are given by $|E_0(0)\rangle = |m_x = n/2\rangle$ and $|E_0(1)\rangle = |m_z = n/2\rangle$, respectively.

Projecting the equation $H(s)|\psi\rangle = E|\psi\rangle$ onto the eigenbasis of S_x, we find

$$\left\langle m_x = \frac{n}{2} - r \middle| \psi \right\rangle = \frac{s}{1-s}\sqrt{\frac{P_r}{r - \lambda}}\left\langle m_z = \frac{n}{2} \middle| \psi \right\rangle, \quad \text{(B4)}$$

where we have defined $\lambda = (E-s)/(1-s)$ and $P_r = 2^{-n}\binom{n}{r}$. Now focus on the ground state $|\psi_+\rangle$ and the first excited state $|\psi_-\rangle$ of $H(s^*)$. By Eq. (4.39) of [3], these states have $\lambda_\pm = \mp(n/2)2^{-n/2}[1 + O(1/n)]$. Putting $r = 0$ in Eq. (B4) and taking $s = s^*$ from Eq. (34), we find

$$\left\langle m_x = \frac{n}{2} \middle| \psi_\pm \right\rangle = \pm\left\langle m_z = \frac{n}{2} \middle| \psi_\pm \right\rangle[1 + O(1/n)]. \quad \text{(B5)}$$

For $r \neq 0$, we have

$$\left\langle m_x = \frac{n}{2} - r \middle| \psi_\pm \right\rangle = \frac{n}{2}\sqrt{\frac{P_r}{r}}\left\langle m_z = \frac{n}{2} \middle| \psi_\pm \right\rangle[1 + O(1/n)].$$
(B6)

Requiring that $|\psi_\pm\rangle$ be normalized, we find

$$1 = \sum_{r=0}^{n}\left|\left\langle m_x = \frac{n}{2} - r \middle| \psi_\pm \right\rangle\right|^2 \quad \text{(B7)}$$

$$= \left|\left\langle m_z = \frac{n}{2} \middle| \psi_\pm \right\rangle\right|^2\left(1 + \frac{n^2}{4}\sum_{r=1}^{n}\frac{P_r}{r^2}\right)[1 + O(1/n)] \quad \text{(B8)}$$

$$= \left|\left\langle m_z = \frac{n}{2} \middle| \psi_\pm \right\rangle\right|^2[2 + O(1/n)], \quad \text{(B9)}$$

which implies $|\langle m_z = (n/2)|\psi_\pm\rangle|^2 = \frac{1}{2} + O(1/n)$. From Eq. (B5), we also have $|\langle m_x = (n/2)|\psi_\pm\rangle|^2 = \frac{1}{2} + O(1/n)$. Thus we find

$$|\psi_\pm\rangle \simeq \frac{1}{\sqrt{2}}\left(\left|m_x = \frac{n}{2}\right\rangle \pm \left|m_z = \frac{n}{2}\right\rangle\right) \quad \text{(B10)}$$

up to terms of order $1/n$, which is Eq. (36).

---

[1] P.W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE, Los Alamitos, CA, 1994), p. 124.

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

[3] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, e-print quant-ph/0001106.

[4] M.A. Nielsen, e-print quant-ph/0108020.

[5] S.A. Fenner and Y. Zhang, e-print quant-ph/0111077.

[6] D.W. Leung, e-print quant-ph/0111122.

[7] R. Raussendorf and H.J. Briegel, e-print quant-ph/0010033.

[8] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955).

[9] Y. Aharonov and M. Vardi, Phys. Rev. D **21**, 2235 (1980).

[10] L.S. Schulman, A. Ranfagni, and D. Mugnai, Phys. Scr. **49**, 536 (1993).

[11] A.M. Childs, E. Farhi, J. Goldstone, and S. Gutmann, Quantum Inf. Comput. **2**, 181 (2002).

[12] S. Wiesner, e-print quant-ph/9603028.

[13] C. Zalka, Proc. R. Soc. London, Ser. A **454**, 313 (1998).

[14] S. Lloyd, Science **273**, 1073 (1996).

[15] A.Yu. Kitaev, e-print quant-ph/9511026.

[16] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. London, Ser. A **454**, 339 (1998).

[17] D.S. Abrams and S. Lloyd, Phys. Rev. Lett. **83**, 5162 (1999).

[18] B.C. Travaglione, G.J. Milburn, and T.C. Ralph, e-print quant-ph/0203130.

[19] C.H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510 (1997).

[20] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403 (1998).

[21] J. Roland and N. Cerf, Phys. Rev. A **65**, 042308 (2002).

[22] W. van Dam, M. Mosca, and U. Vazirani, in *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, CA, 2001), p. 279.

[23] E. Farhi, J. Goldstone, and S. Gutmann, e-print quant-ph/0201031.

[24] A.M. Childs, E. Farhi, and J. Preskill, Phys. Rev. A **65**, 012322 (2002).