Quantum Computers Can Search Rapidly by Using Almost Any Transformation

Lov K. Grover*

3C-404A Bell Labs, 600 Mountain Avenue, Murray Hill, New Jersey 07974

(Received 4 December 1997)

A quantum computer has a clear advantage over a classical computer for exhaustive search. The quantum mechanical algorithm for exhaustive search was originally derived by using subtle properties of a particular quantum mechanical operation called the Walsh-Hadamard (W-H) transform. This paper shows that this algorithm can be implemented by replacing the W-H transform by almost any quantum mechanical operation. This leads to several new applications where it improves the number of steps by a square root. It also broadens the scope for implementation since it demonstrates quantum mechanical algorithms that can adapt to available technology. [S0031-9007(98)06052-9]

PACS numbers: 03.67.Lx, 89.70.+c

Quantum mechanical systems can be in a superposition of computational states and hence simultaneously carry out multiple computations in the same computer. In the last few years there has been extensive research on how to use this quantum parallelism to carry out meaningful computations. In any quantum mechanical computation the system is initialized to a state that is easy to prepare and caused to evolve unitarily, the answer to the computational problem is deduced by a final measurement that projects the system onto a unique state. The amplitude (and hence probability) of reaching a specified final state depends on the interference of all paths that take it from the initial to the final state—the system is thus very sensitive to any magnitude of phase disturbances that affect any of the paths leading to the desired final state. As a result, quantum mechanical algorithms are very delicate, and it is generally believed that an actual implementation would need elaborate procedures for correcting errors [1].

This paper shows that the quantum search algorithm is surprisingly robust to certain kinds of perturbations. It was originally derived by using the Walsh-Hadamard (W-H) transform and appeared to be a consequence of the special properties of this transform; this paper shows that similar results are obtained by substituting almost *any* unitary transformation in place of the W-H transform. Since all quantum mechanical operations are unitary, this means that almost *any* quantum mechanical system can be used—all that is needed is a valid quantum mechanical operation and a way of selectively inverting the phase of states. Meaningful computation can hence be carried out on the basis of universal properties of quantum mechanical operations; this is somewhat similar in spirit to [2], where circuit behavior of a certain class of neural networks was independent of the precise nature of the nonlinearity in each neuron.

1. Quantum operations.—In a quantum computer, the logic circuitry and time steps are essentially classical, only the memory *bits* that hold the variables are in quantum superpositions—these are called *qubits*. There is a set of distinguished computational states in which all the bits are definite 0s or 1s. In a quantum mechanical algorithm, the quantum computer consisting of a number of qubits is prepared in some simple initial state, and caused to evolve unitarily for some time, and is then measured. The algorithm is the design of the step-by-step unitary evolution of the system. Operations that can be carried out in a controlled way are unitary operations that act on a small number of qubits in each step. Two elementary unitary operations presented in this section are the W-H transformation and the selective inversion of the amplitudes of certain states.

A basic operation in quantum computing is the operation M performed on a single qubit—this is represented by the following matrix:

$$M \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

—where the state 0 is transformed into a superposition: $(1/\sqrt{2}, 1/\sqrt{2})$. Similarly, state 1 is transformed into the superposition $(1/\sqrt{2}, -1/\sqrt{2})$. In a system in which the states are described by n qubits (it has $N = 2^n$ possible states) we can perform the transformation M on each qubit independently in sequence thus changing the state of the system. The state transition matrix representing this operation will be of dimension $2^n \times 2^n$. Consider a case when the starting state is one of the 2^n basis states, i.e., a state described by a general string of n binary digits composed of some 0s and some 1s. The result of performing the transformation M on each qubit will be a superposition of states consisting of all possible n bit binary strings with amplitude of each state being $\pm 2^{-n/2}$. This transformation is referred to as the W-H transformation [3] and denoted by W. For $n = 2, N = 4$:

$$W = \frac{1}{\sqrt{4}}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Make note of the following three points: (i) Each of the terms of the first row and first column are $1/\sqrt{N}$, (ii) each of the other terms is $\pm 1/\sqrt{N}$, and (iii) the various columns are orthonormal.

The other transformation that we will need is the selective inversion of the phase of the amplitudes in certain states. Unlike the W-H transformation and other state transition matrices [4], the probability in each state stays the same since the square of the absolute value of the amplitude in each state stays the same. Its realization is particularly straightforward; based on [5], the following paragraph gives a realization.

Assume that there is a binary function $f(x)$ that is either 0 or 1. Given a superposition over states x, it is possible to design a quantum circuit that will selectively invert the amplitudes in all states where $f(x) = 1$. This is achieved by appending an ancilla bit b and considering the quantum circuit that transforms a state $|x, b\rangle$ into $|x, f(x)\text{XOR}b\rangle$ (such a circuit exists since, as proved in [6], it is possible to design a quantum mechanical circuit to evaluate any function $f(x)$ that can be evaluated classically). If the bit b is initially placed in a superposition $1/\sqrt{2}\,(|0\rangle - |1\rangle)$, this circuit will selectively invert the amplitudes in the states for which $f(x) = 1$ [5].

2. Amplitude amplification.—A function $f(x)$, $x = 1, 2, \ldots, N$, is given which is known to be nonzero at a single (unknown) value of x, say at $x = \tau$—the goal is to find τ. If there is no other information about $f(x)$ and one is using a classical computer, it is easy to see that on the average it will take $N/2$ function evaluations to solve this problem successfully. However, quantum mechanical systems can explore multiple states simultaneously, and there is no clear lower bound on how fast this can be done. Reference [7] showed by using subtle arguments about unitary transforms that it cannot be done in fewer than $O(\sqrt{N})$ steps—subsequently an algorithm was discovered that took precisely $O(\sqrt{N})$ steps [8].

The basic idea of [8] is to consider an N state quantum mechanical system and map each value of x in the domain to a basis state of the system. The system is initialized so that there is an equal amplitude in each basis state, then by a series of unitary operations, the amplitude in the state corresponding to $x = \tau$ is increased (the corresponding basis state is denoted by $|\tau\rangle$). A measurement is then made due to which the system collapses to a basis state; the observed basis state then gives the solution to the problem. This algorithm is based on subtle properties of the W-H transform. The analysis in this section shows that very similar results are obtained by replacing the W-H transform by any arbitrary unitary operation. Some consequences of this are presented in the next section.

Assume that we have at our disposal a unitary operation U and we start with the system in a basis state that is easy to prepare, say $|\gamma\rangle$. If we apply U to $|\gamma\rangle$, the amplitude of reaching state $|\tau\rangle$ is $U_{\tau\gamma}$, if we were to observe the system at this point, the probability of getting the right state would be $|U_{\tau\gamma}|^2$—according to the notation, $|\gamma\rangle$ denotes the initial basis state and $|\tau\rangle$ the target basis state. It will therefore take at least $O(1/|U_{\tau\gamma}|^2)$ repetitions of this experiment before a single success. This section shows how it is possible to reach state $|\tau\rangle$ in only $O(1/|U_{\tau\gamma}|)$ steps. This leads to a sizable improvement in the number of steps if $|U_{\tau\gamma}| \ll 1$.

Denote the unitary operation that inverts the amplitude in a single basis state $|x\rangle$ by I_x. In matrix notation this is the diagonal matrix with all diagonal terms equal to 1, except the xx term which is -1—a quantum mechanical implementation of this was presented at the end of section 1.

Consider the following unitary operator: $Q \equiv -I_\gamma U^{-1} I_\tau U$—note that since U is unitary, U^{-1} is equal to the *adjoint* (the complex conjugate of the transpose) of U. We first show that Q preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$ (note that in the situation of interest, when $|U_{\tau\gamma}|$ is small, these two vectors are almost orthogonal).

First consider $Q|\gamma\rangle$. By the definition of Q, this is $-I_\gamma U^{-1} I_\tau U|\gamma\rangle$. Note that $|x\rangle\langle x|$, where $|x\rangle$ is a basis state, is an $N \times N$ square matrix all of whose terms are zero, except the xx term which is 1. Therefore $I_\tau \equiv I - 2|\tau\rangle\langle\tau|$ and $I_\gamma \equiv I - 2|\gamma\rangle\langle\gamma|$, it follows:

$$\begin{aligned} Q|\gamma\rangle &= -(I - 2|\gamma\rangle\langle\gamma|)U^{-1}(I - 2|\tau\rangle\langle\tau|)U|\gamma\rangle \\ &= -(I - 2|\gamma\rangle\langle\gamma|)U^{-1}U|\gamma\rangle \\ &\quad + 2(I - 2|\gamma\rangle\langle\gamma|)U^{-1}|\tau\rangle\langle\tau|U|\gamma\rangle. \end{aligned} \tag{1}$$

Using the facts: $U^{-1}U \equiv I$ and $\langle\gamma|\gamma\rangle \equiv 1$, it follows that

$$Q|\gamma\rangle = |\gamma\rangle + 2(I - 2|\gamma\rangle\langle\gamma|)U^{-1}(|\tau\rangle\langle\tau|)U|\gamma\rangle. \tag{2}$$

Simplifying the second term of (2) by the following identities: $\langle\tau|U|\gamma\rangle \equiv U_{\tau\gamma}$ and $\langle\gamma|U^{-1}|\tau\rangle \equiv U^*_{\tau\gamma}$ (as mentioned previously, U is unitary and so U^{-1} is equal to the complex conjugate of its transpose);

$$Q|\gamma\rangle = |\gamma\rangle(1 - 4|U_{\tau\gamma}|^2) + 2U_{\tau\gamma}(U^{-1}|\tau\rangle). \tag{3}$$

Next consider the action of the operator Q on the vector $U^{-1}|\tau\rangle$. Using the definition of Q (i.e., $Q \equiv -I_\gamma U^{-1} I_\tau U$), and carrying out the algebra as in (3):

$$\begin{aligned} Q(U^{-1}|\tau\rangle) &\equiv -I_\gamma U^{-1} I_\tau U(U^{-1}|\tau\rangle) \\ &= -I_\gamma U^{-1} I_\tau|\tau\rangle = I_\gamma U^{-1}|\tau\rangle. \end{aligned} \tag{4}$$

Writing I_γ as $I_\gamma \equiv I - 2|\gamma\rangle\langle\gamma|$ and as in (3), $\langle\gamma|U^{-1}|\tau\rangle \equiv U^*_{\tau\gamma}$:

$$\begin{aligned} Q(U^{-1}|\tau\rangle) &= U^{-1}|\tau\rangle + |\gamma\rangle\langle\gamma|(U^{-1}|\tau\rangle) \\ &= U^{-1}|\tau\rangle - 2U^*_{\tau\gamma}|\gamma\rangle. \end{aligned} \tag{5}$$

The operator Q hence transforms any superposition of the vectors $|\gamma\rangle$ and $U^{-1}|\tau\rangle$ into another superposition of the same two vectors. (3) and (5) may be written as

$$Q\begin{bmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{bmatrix} = \begin{bmatrix} (1 - 4|U_{\tau\gamma}|^2) & 2U_{\tau\gamma} \\ -2U^*_{\tau\gamma} & 1 \end{bmatrix}\begin{bmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{bmatrix}. \tag{6}$$

It follows from (6) that Q preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$. Q rotates any

vector in this space by approximately $2|U_{\tau\gamma}|$ radians as shown in Fig. 1.

In the situation of interest, $|\gamma\rangle$ and $U^{-1}|\tau\rangle$ are almost orthogonal (or else $|\tau\rangle$ may be trivially obtained by applying U to $|\gamma\rangle$ and repeating the experiment a few times). Therefore the angle between the two vectors $|\gamma\rangle$ and $U^{-1}|\tau\rangle$ is approximately $\pi/2$.

The number of applications of Q required to transform $|\gamma\rangle$ into $U^{-1}|\tau\rangle$ is obtained by dividing the angle between the two vectors (which is $\pi/2$) by the rotation achieved in each application of Q [which is $(2|U_{\tau\gamma}|)$]; therefore in $\pi/4|U_{\tau\gamma}|$ applications, Q transforms $|\gamma\rangle$ into $U^{-1}|\tau\rangle$. From this, with a single application of U, we can get $|\tau\rangle$. Therefore in $O(1/|U_{\tau\gamma}|)$ steps, we can start with $|\gamma\rangle$ and reach the target state $|\tau\rangle$ with certainty.

The above derivation easily extends to the case when the amplitudes in states $|\gamma\rangle$ and $|\tau\rangle$, instead of being inverted by I_γ and I_τ, are rotated by arbitrary phases. However, the number of operations required to reach $|\tau\rangle$ will be greater. Given a choice, it will be clearly better to use the inversion rather than a different phase rotation. Also the analysis can be extended to include the case where I_τ is replaced by $V^{-1}I_\tau V$, V is an arbitrary unitary matrix. The analysis is the same as before except that the operation U is replaced by VU.

3. Examples of quantum mechanical algorithms.—The interesting feature of this paper is that U can be *any* unitary transformation. Clearly, it can be used to design algorithms where U is a transformation on the qubits in a quantum computer—this paper gives a few search-related applications; further search-related applications are discussed in [9]. This technique also extends to problems not immediately connected with search [10]. The $N = 2^n$ states to be searched are represented by n qubits. According to the framework of section 2, a search of these N states can be carried out quantum mechanically by using a unitary operation U which has a finite amplitude $U_{\tau\gamma}$ to go from the starting state $|\gamma\rangle$ to the target state $|\tau\rangle$. Such a search will take $O(1/|U_{\tau\gamma}|)$ steps. The following analyses calculate $U_{\tau\gamma}$ and thus the number of steps required for the search.

(i) Exhaustive search starting from the $|\bar{0}\rangle$ state.—In case the starting state $|\gamma\rangle$ is the $|\bar{0}\rangle$ state and the unitary transformation U is chosen to be W (the W-H transformation as discussed in section 1), then $U_{\tau\gamma}$ for any target state τ is $1/\sqrt{N}$. The algorithm of section 2 requires

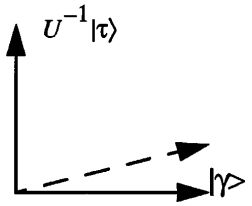

FIG. 1. The operator $Q \equiv -I_\gamma U^{-1} I_\tau U$ preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$; it rotates each vector in the space by approximately $2|U_{\tau\gamma}|$ radians.

$O(1/|U_{\tau\gamma}|)$, i.e., $O(\sqrt{N})$ steps. This algorithm would carry out repeated operations of Q; with $U^{-1} = U = W$, Q becomes $Q \equiv -I_{\bar{0}} W I_\tau W$; the operation sequence is hence $\ldots(-I_{\bar{0}} W I_\tau W)(-I_{\bar{0}} W I_\tau W)(-I_{\bar{0}} W I_\tau W)\ldots$. By rearranging parentheses and shifting minus signs, this may be seen to consist of alternating repetitions of $-W I_{\bar{0}} W$ and I_τ.

The operation sequence $-W I_{\bar{0}} W$ is simply the inversion-about-average operation [8]. To see this, write $I_{\bar{0}}$ as $I - 2|\bar{0}\rangle\langle\bar{0}|$. For any superposition $|x\rangle$, it follows: $-W I_{\bar{0}} W|x\rangle = -W(I - 2|\bar{0}\rangle\langle\bar{0}|)W|x\rangle = -|x\rangle + 2W|\bar{0}\rangle\langle\bar{0}|W|x\rangle$. It is easily seen that $W|\bar{0}\rangle\langle\bar{0}|W|x\rangle$ is another vector each of whose components is the same and equal to A where $A \equiv 1/N \sum_{i=1}^{N} x_i$ (the average value of all components). Therefore the ith component of $-W I_{\bar{0}} W|x\rangle$ is simply $(-x_i + 2A)$. This may be written as $A + (A - x_i)$, i.e., each component is as much above (below) the average as it was initially below (above) the average—this is precisely the definition of the inversion-about-average [8].

(ii) Search when an item near the desired state is known.—Problem: Assume that an n bit word is specified—the desired word differs from this in exactly k bits. *Solution:* The proximity to the specified word is a constraint whose effect is to reduce the size of the solution space. One way of making use of this constraint, would be to map to another problem which exhaustively searches the reduced space using (i). However, such a mapping would involve additional overhead. This section presents a different approach which also carries over to more complicated search-related situations as discussed in [9].

Instead of choosing U as the W-H transform, in this algorithm U is tailored to the problem under consideration. The starting state $|\gamma\rangle$ is chosen to be the specified word. The operation U consists of the transformation

$$\begin{bmatrix} \sqrt{1-\alpha} & \sqrt{\alpha} \\ \sqrt{\alpha} & -\sqrt{1-\alpha} \end{bmatrix},$$

applied to each of the n qubits (α is a variable parameter yet to be determined)—note that if α is $\frac{1}{2}$, we obtain the W-H transform of section 1. Calculating $U_{\tau\gamma}$ it follows that $|U_{\tau\gamma}| = (1-\alpha)^{(n-k)/2}\alpha^{k/2}$, this is maximized when α is chosen to be k/n; then $\ln|U_{\tau\gamma}| = n/2\ln[(n-k)/n] - k/2\ln[(n-k)/k]$. The procedure of section 2 can now be used—as in (i), this consists of repeating the sequence of operations $-I_\gamma U^{-1} I_\tau U$, $O(1/|U_{\tau\gamma}|)$ times.

The size of the space being searched in this problem is $\binom{n}{k}$, which is equal to $n!/(n-k!\,k!)$. Using Stirling's approximation: $\ln n! \approx n\ln n - n$, from this it follows that $\ln\binom{n}{k} \approx n\ln[n/(n-k)] - k\ln[k/(n-k)]$, comparing this to the number of steps required by the algorithm, we find that the number of steps in this algorithm, as in (i), varies approximately as the square root of the size of the solution space being searched.

4. Sensitivity.—In order to achieve isolation, quantum computational devices generally have to be designed to

be microscopic—however, it is extremely difficult to exert precise control over microscopic individual entities. As a result, a serious problem in implementing quantum mechanical computers is their extreme sensitivity to perturbations. This paper synthesizes algorithms in terms of unitary matrices—as shown in section 3 this framework can always be specialized to a quantum computer based on qubits; however, it can also be applied directly to more physical situations, hopefully reducing the need for error correction [1].

For example, consider a hypothetical implementation of the quantum search algorithm where the qubits are the spin states of electrons and the W-H transform is achieved by a pulsed external magnetic field. The results of sections 2 and 3 tell us that it does not significantly alter the working of the algorithm if the axes of the magnets, or the periods of the pulse, are slightly perturbed from what is required for the W-H transform. Any unitary transform U which is *close* to the W-H transform, will work provided both U and U^{-1} are consistently applied as specified.

5. Limitation.—As discussed in [5], it is possible to express several important computer science problems in such a way so that a quantum computer can solve them efficiently by an exhaustive search. Even in physics, several important problems can be looked upon as searches of domains. Many spectroscopic analyses are essentially searches—a rather dramatic example of a recent search was that for the top quark [11]. The framework of this paper could equally well be used there. All that is needed is a means to repeatedly apply a specified Hamiltonian that produces various phase inversions and state transitions. For example, it took about 10^{12} repetitions of a certain experiment, consisting of interacting a proton and antiproton at high energies, to obtain 12 observations of the top quark [11]. Denoting the desired state with the top quark by $|\tau\rangle$ and the initial proton-antiproton state by $|\gamma\rangle$, it implies that $|U_{\tau\gamma}|^2$ is approximately 12×10^{-12}. Therefore if it was possible to apply the operation $-I_\gamma U^{-1} I_\tau U$ repetitively m times, it would boost the success probability by approximately m^2 (assuming m to be a small number), and it would take m^2 fewer experiments; in case it were possible to apply the operations $-I_\gamma U^{-1} I_\tau U$, about 10^6 times, *one could achieve success in a single experiment.*

In principle it is possible to synthesize U^{-1} for any unitary operation U, since the adjoint of a unitary operator is unitary and can hence be synthesized quantum mechanically. For controlled operations on a few qubits, synthesizing the adjoint is no harder than synthesizing the original operation. However, the adjoint of the time evolution operation is the reversed evolution operation—this may not be easy to synthesize when the states are nondegenerate and there is significant time evolution. This is especially true if the time evolution is due to the internal dynamics of the system. That is the main reason this procedure, at least in its present form, could not be used to isolate the top quark.

Another limitation is that the framework of section 2 demands that U and U^{-1} stay the same at all time steps. What happens if there are small perturbations in these? It seems plausible that these will not create much of an impact if they are small and average out to zero; however, that is something still to be proved.

In conclusion, designing a useful quantum computer has been a daunting task for two reasons. First, because the physics to implement this is different from what most known devices use and so it is not clear what its structure should be like. The second reason is that once such a computer is built, few applications for this are known where it will have a clear advantage over existing computers. This paper has given a general framework for the synthesis of a category of algorithms where the quantum computer would have an advantage. See Refs. [9,10] for further applications developed using this framework. It is expected that this formalism will also be useful in the physical design of quantum computers, since it demonstrates that quantum algorithms can be implemented through general properties of unitary transformations and can thus adapt to available technology.

We thank Norm Margolus and Charles Bennett for spending the time and effort to comment on several versions of this paper.

*Electronic address: lkgrover@bell-labs.com

[1] P. W. Shor, in *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, California, 1996), pp. 56–65.

[2] J. Hopfield, in *Proceedings of the National Academy of Sciences* (National Academy of Sciences, Washington, DC, 1992), Vol. 79, p. 2554.

[3] D. Deutsch and R. Jozsa, in Proceedings of the Royal Society of London, 1992, A400, pp. 73–90.

[4] P. Shor, in *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science* (IEEE Computer Society Press, Los Alamitos, California, 1994), pp. 124–134.

[5] M. Boyer *et al.*, in Proceedings of the 4th Workshop on Physics and Computation–PhysComp'96, 1996 (lanl e-print quant-ph/9605034) [Fortschr. Phys. (to be published)].

[6] C. H. Bennett, SIAM J. Comput. **18**, 766–776 (1989).

[7] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510–1524 (1997).

[8] L. K. Grover, Phys. Rev. Lett. **78**, 325–328 (1997).

[9] L. K. Grover, in Proceedings of the 1st NASA Conference on Quantum Computation and Quantum Communication, 1998 (lanl e-print quant-ph/9802035; Special Issue on Quantum Computing [Int. J. Nonlinear Sci. (to be published)].

[10] L. K. Grover, in Proceedings of the 30th Annual ACM Symposium on the Theory of Computing (STOC), 1998 (lanl e-print quant-ph/9711043).

[11] T. M. Liss and P. L. Tipton, Sci. Am. **277**, No. 3, 54–59 (1997).