Grover's quantum search algorithm for an arbitrary initial mixed state

Eli Biham and Dan Kenigsberg
Computer Science Department, Technion, Haifa 32000, Israel
(Received 16 January 2002; published 4 December 2002)

The Grover quantum search algorithm is generalized to deal with an arbitrary mixed initial state. The probability to measure a marked state as a function of time is calculated, and found to depend strongly on the specific initial state. The form of the function, though, remains as it is in the case of initial pure state. We study the role of the von Neumann entropy of the initial state, and show that the entropy cannot be a measure for the usefulness of the algorithm. We give few examples and show that for some extremely mixed initial states (carrying high entropy), the generalized Grover algorithm is considerably faster than any classical algorithm.

DOI: 10.1103/PhysRevA.66.062301 PACS number(s): 03.67.Lx

I. INTRODUCTION

Grover's search algorithm [1,2] provides an example of the speed-up that would be offered by quantum computers, if and when they are built. The problem solved by Grover's algorithm is finding a sought-after (''marked'') element in an unsorted database of size N. To solve this problem, a classical computer would need $N/2$ database queries on average, and in the worst case it would need $N-1$ queries. Using Grover's algorithm, a quantum computer can find the marked state using only $O(\sqrt{N})$ quantum database queries. The importance of Grover's result stems from the fact that it proves the existence of a gap (albeit a polynomial gap) between the power of quantum computers and classical computers. Moreover, the algorithm may be used to speed up the solution of many problems (such as NP-complete problems), for which no efficient classical algorithms is known.

Along this paper, we assume without loss of generality that $N=2^n$, where n is an integer. The algorithm requires a register of n qubits carrying the computation. When we say it is in a state $|x\rangle$, we mean that its qubits are in states corresponding to the binary representation of the number x. Grover's original quantum search algorithm consists of the following steps: (1) Initialize the register to $H|0\rangle$. That is, reset all the qubits to 0 and apply the Hadamard transform to each of them. (2) Repeat the following operation (named the *Grover iterate* Q) $T=\pi\sqrt{N}/4$ times: (a) Rotate the marked state $|k\rangle$ by a phase of π radians (I_k^π). (b) Apply the Hadamard transform to the register. (c) Rotate the $|0\rangle$ state by a phase of π radians (I_0^π). (d) Apply the Hadamard transform again. (3) Measure the resulting state.

Several generalizations extended the original Grover algorithm. Among these is handling multiple marked states [3], and the initialization of the algorithm in any pure state [4]. Another generalization is the replacement of the Hadamard transform by any other unitary operation [5–7]. In this way, the algorithm may be used to speed up many classical decision algorithms and heuristics. Other generalizations use arbitrary rotation angles [8], replace the $|0\rangle$ state from step (2c) with any other state, or combine all of the above [9]. The rotation angles may be tweaked in order to find a marked state with certainty [10,11].

The original Grover iterate is $Q=-HI_0^\pi HI_k^\pi$. It has been generalized to $Q=-UI_s^\beta U^\dagger I_M^\gamma$, where U is an arbitrary unitary operator, s is an arbitrary state, β and γ are arbitrary angles, and M includes any number of marked states. We now observe that *any* unitary operation Q has a unitary diagonalization. Therefore, it can be represented as $Q=-UI_S^{\vec{\beta}}U^\dagger I_M^\gamma$. This is a further generalization of Grover's algorithm, where the state s is replaced by a set of states S, each of which may have a different rotation angle. Thus, every iterative algorithm is a generalized Grover algorithm.

In this paper, we study the case where the generalized Grover iterate of Ref. [9] is applied to a quantum register that is initialized in an arbitrary mixed state. Our study extends and corrects a result from Ref. [12].

II. ARBITRARY PURE INITIAL STATE

If the above-mentioned search algorithm is used as a procedure by another algorithm, it might be necessary to avoid its first step. Even if the initialization is performed, gate imperfection or external noise might cause the outcome to differ from the exact $H|0\rangle$ state. Rather, it may well be some general pure state $|\psi_0\rangle$, which is a superposition of the marked state and the unmarked states. In addition, the iterate itself may be imperfect: the Hadamard operation might be some other unitary operation U; the rotations of steps (2a) and (2c) may be in angles β and γ (respectively), different of π; and the rotated state of step (2c) may be a nonzero $|s\rangle$. Finally, the set of sought-after items, M, may include multiple items.

When the parameters of the problem are known, we may follow the results of Biham *et al.* [9], and calculate the probability to measure a marked state P_{ψ_0} as a function of the number of Grover iterations t:

$$P_{\psi_0}(t)=\langle P_{\psi_0}\rangle-\Delta P_{\psi_0}\cos(2\omega t+2\phi_{\psi_0}). \tag{1}$$

$\langle P_{\psi_0}\rangle$ and ΔP_{ψ_0} denote the average over time and the amplitude of P_{ψ_0}, respectively. The subscripts ψ_0 denote that the values depend on the initial state. However, ω, which is defined by

$$\cos\omega = \sum_{i\in M} |\langle i|U|s\rangle|^2 \cos\frac{\beta+\gamma}{2} + \sum_{i\notin M} |\langle i|U|s\rangle|^2 \cos\frac{\beta-\gamma}{2}$$

is independent of the initial state. In a large search problem with $N\to\infty$, and with the original Grover iterate, ω may be approximated by $\omega = 2/\sqrt{N}$. With the original initial state $H|0\rangle$ studied by Grover, we reobtain $\langle P_{H|0\rangle}\rangle = \Delta P_{H|0\rangle} = 1/2$ and $\phi_{H|0\rangle} \approx 0$.

III. ARBITRARY MIXED INITIAL STATE

A mixed state arises when one cannot describe the state of a quantum system deterministically, no matter what basis one chooses. Such a condition appears very often when a quantum system is entangled with its environment, while the environment cannot be accessed or manipulated. The state of such a system may be described by a completely positive trace-1 Hermitian density matrix, denoted by ρ. An equivalent description is an ensemble $\mathcal{E}=\{p_\mu,|\psi_\mu\rangle\}$ where $\Sigma_\mu p_\mu = 1$ and $\rho = \Sigma_\mu p_\mu |\psi_\mu\rangle\langle\psi_\mu|$. According to this description, the system is in the pure state $|\psi_\mu\rangle$ with probability p_μ. When a unitary operation V is applied to the mixed state, it transforms the state into $\Sigma_\mu p_\mu V|\psi_\mu\rangle\langle\psi_\mu|V^\dagger$. The mixedness of the state does not change, and it may be thought as if V transforms each of the components of $\mathcal{E}$ independently of the others.

Extending the argument of Sec. II, the initial state of the quantum register might not be pure, due to external noise, decoherence, or previous manipulations. Instead, the initial state may be some general mixed state $\mathcal{E}$. Given the description of $\mathcal{E}$ as an ensemble, all we can say is that the register is in the pure state $|\psi_\mu\rangle$ with probability p_μ (for all i's).

When the Grover algorithm is applied to a register which is in a pure state $|\psi_\mu\rangle$, the probability to measure the marked state is $P_\mu(t)$. The probability for the register to be in $|\psi_\mu\rangle$ is p_μ (considering the ensemble $\mathcal{E}$). Thus, the total probability to measure the marked state is the weighted average

$$\tilde{P}(t) = \sum_\mu p_\mu P_\mu(t) = \sum_\mu p_\mu[\langle P_\mu\rangle - \Delta P_\mu \cos(2\omega t + 2\phi_\mu)]. \quad (2)$$

The functions

$$P_\mu(t) - \langle P_\mu\rangle = -\Delta P_\mu \cos(2\omega t + 2\phi_\mu)$$

share a sinusoidal form, differing in amplitude and phase, but not in frequency. They may be thought of as the projections of vectors rotating in frequency ω, as exemplified by Fig. 1. Therefore, their weighted sum $\Delta\tilde{P}$ (the center of mass of the vectors in the figure) is a sinusoidal function with the same frequency,

$$\tilde{P}(t) = \widetilde{\langle P\rangle} - \widetilde{\Delta P}\cos(2\omega t + 2\tilde{\phi}) \quad (3)$$

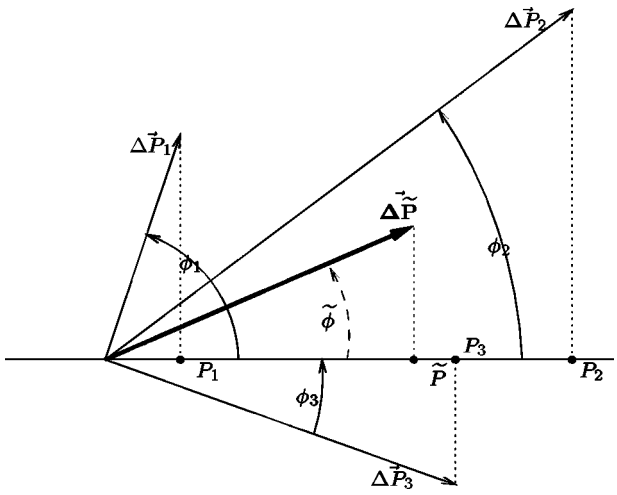

FIG. 1. The change of probabilities as projections of rotating vectors.

while

$$\widetilde{\langle P\rangle} = \sum_\mu p_\mu \langle P_\mu\rangle,$$

$$\widetilde{\Delta P} = \sqrt{\left(\sum_\mu p_\mu \Delta P_\mu \cos 2\phi_\mu\right)^2 + \left(\sum_\mu p_\mu \Delta P_\mu \sin 2\phi_\mu\right)^2}, \quad (4)$$

and

$$\tan 2\tilde{\phi} = \frac{\sum_\mu p_\mu \Delta P_\mu \sin(2\phi_\mu)}{\sum_\mu p_\mu \Delta P_\mu \cos(2\phi_\mu)}. \quad (5)$$

The probability to measure a marked state reaches its maximum value,

$$P_{max} = \langle P\rangle + \widetilde{\Delta P}$$

after $T = (\pi - 2\tilde{\phi})/(2\omega)$ iterations.

If the algorithm is repeated until success with T iterations each time, the expected total time to measure a marked state is

$$\mathcal{T}_Q = \frac{\pi - 2\tilde{\phi}}{2\omega \tilde{P}_{max}},$$

since the number of repetition until success is distributed geometrically with parameter $\tilde{P}_{max}$. When the original iterate is used, and a single item is sought after, this reduces to $\mathcal{T}_Q = (\pi - 2\tilde{\phi})\sqrt{N}/(4\tilde{P}_{max})$. If this value is significantly smaller than the classical expected time $\mathcal{T}_C = N/2$, then the quantum algorithm has an advantage. Quantitatively, the expected number of oracle queries that the quantum algorithm requires is smaller by a factor of

$$\frac{\mathcal{T}_C}{\mathcal{T}_Q} = \frac{N\omega\tilde{P}_{max}}{\pi - 2\tilde{\phi}} = \frac{2\tilde{P}_{max}\sqrt{N}}{\pi - 2\tilde{\phi}}. \quad (6)$$

IV. EXAMPLES

For clarity and simplicity, our examples use the original Grover iterate and single marked state $|k\rangle$, with different initial mixed states.

A. Pure initial state

When the arbitrary mixed state is chosen to be pure, the summations are degenerated and the results of Ref. [4] are achieved. For example, if the initial state is the original $\mathcal{E}=\{p=1,H|0\rangle\}$, the original Grover case is found. If $\mathcal{E}=\{p=1,|k\rangle\}$, then $\widetilde{\langle P\rangle}=\widetilde{\Delta P}=1/2$ and $\tilde{\phi}=\pi/2$. An interesting known property of the Grover algorithm is that for all states orthogonal to both $|k\rangle$ and $H|0\rangle$, $\widetilde{\langle P\rangle}=\widetilde{\Delta P}=0$.

B. Pseudopure initial state

Ensembles, where a state $|\psi\rangle$ appears with probability $\epsilon+(1-\epsilon)/N$ and any state orthogonal to it appears with equal probabilities of $(1-\epsilon)/N$ are called pseudopure mixed states. They are written more conveniently as $\rho_{\epsilon\text{-}pure}=(1-\epsilon)(I/N)+\epsilon|\psi\rangle\langle\psi|$. Notice that $0\leqslant\epsilon\leqslant 1$ is a measure of the purity of ρ: when $\epsilon=0$ it is totally mixed and when $\epsilon=1$ it is totally pure. It is easy to see that in the limit of large N, $\widetilde{\langle P\rangle}=\epsilon\langle P_\psi\rangle$, $\widetilde{\Delta P}=\epsilon\Delta P_\psi$, and $\tilde{\phi}=\phi_\psi$. For example,

$$\rho_{(1/\log_2 N\text{-}pure}=\left(1-\frac{1}{\log_2 N}\right)\frac{I}{N}+\frac{1}{\log_2 N}H|0\rangle\langle 0|H,$$

we obtain $\widetilde{\langle P\rangle}=\widetilde{\Delta P}=1/2\log_2 N$ and $\tilde{\phi}=0$. Notice that although ρ is extremely mixed, the quantum advantage is of factor $2\sqrt{N}/(\pi\log_2 N)$.

C. Initial state where *m* of the qubits are mixed

Let us study the case, where the register is initialized to $\rho_{m\text{-}mix}=2^{-m}\Sigma_{i=0}^{2^m-1}H|i\rangle\langle i|H$. This state may occur if the m least significant qubits of the register are totally mixed before the first Hadamard transform is applied. Since all $H|i\rangle$ are orthogonal to $H|0\rangle$ (except for $H|0\rangle$ itself) and they are almost orthogonal to $|k\rangle$ (since $|\langle k|H|i\rangle|^2=1/N$), the evolution of $\rho_{m\text{-}mix}$ is governed by $\{p=2^{-m},H|0\rangle\}$ and we obtain $\widetilde{\langle P\rangle}=\widetilde{\Delta P}=1/2^{m+1}$ and $\tilde{\phi}=0$. Large m would render the algorithm useless.

V. ALGORITHM USEFULNESS AND ENTROPY

The von Neumann entropy of a mixed state ρ is defined as $S(\rho)=-\mathrm{tr}\rho\log_2\rho$. Bose *et al.* [12] presented a new model for quantum computation and laid out a new proof for the optimality of the Grover algorithm. However, one of their results was the following: if the Grover algorithm is initiated with a mixed state ρ, such that $S(\rho)\geqslant(1/2)\log_2 N$, the algorithm would have no advantage comparing to the classical case. This is in disagreement with our findings [13]. A counterexample to their claim is $\rho_{(1/\log_2 N)\text{-}pure}$ as defined above. The entropy of pseudopure state is

$$\begin{aligned}S(\rho_{\epsilon\text{-}pure})&=S\left(\frac{1-\epsilon}{N}I_N+\epsilon|0\rangle\langle 0|\right)\\&=-\sum_1^{N-1}\frac{1-\epsilon}{N}\log_2\frac{1-\epsilon}{N}\\&\quad-\frac{1+(N-1)\epsilon}{N}\log_2\frac{1+(N-1)\epsilon}{N}\\&=-(N-1)\frac{1-\epsilon}{N}\log_2\frac{1-\epsilon}{N}\\&\quad-\frac{1+(N-1)\epsilon}{N}\log_2\frac{1+(N-1)\epsilon}{N},\end{aligned}$$

and for large N, where $N/(N-1)\approx 1$,

$$\begin{aligned}&\approx-(1-\epsilon)\log_2\frac{1-\epsilon}{N}-\left(\frac{1}{N}+\epsilon\right)\log_2\left(\frac{1}{N}+\epsilon\right)\\&=(1-\epsilon)\log_2 N-(1-\epsilon)\log_2(1-\epsilon)-\left(\frac{1}{N}+\epsilon\right)\log_2\left(\frac{1}{N}+\epsilon\right)\\&=(1-\epsilon)\log_2 N-\ell,\end{aligned}\tag{7}$$

where $\ell=(1-\epsilon)\log_2(1-\epsilon)+(1/N+\epsilon)\log_2(1/N+\epsilon)\in(-1,0.8)$ for any $0\leqslant\epsilon\leqslant 1$ and any $N\geqslant 2$. For $\epsilon=1/\log_2 N$, we obtain $S(\rho_{(1/\log_2 N)\text{-}pure})=(1-1/\log_2 N)\log_2 N+O(1)=\log_2 N+O(1)$. This entropy is almost maximal. However, as noted above, the Grover algorithm outperforms any classical algorithm, even when it is initialized with this state.

Entropy is not a good measure for the usefulness of Grover's algorithm. For practically every value of entropy, there exist states that are good initializers and states that are not. For example, $S(\rho_{(n-1)\text{-}mix})=\log_2 N-1=S(\rho_{(1/\log_2 N)\text{-}pure})$, but when initialized in $\rho_{(n-1)\text{-}mix}$, the Grover algorithm is as bad as guessing the marked state. Another example may be given using the pure states $H|0\rangle\langle 0|H$ and $H|1\rangle\langle 1|H$. With the first, Grover arrives to the marked state with quadratic speed-up, while the second state is practically unchanged by the algorithm.

ACKNOWLEDGMENTS

We thank Tal Mor for valuable discussions and suggestions that made the compiling of this paper possible. The work was partially supported by the European Commission through the IST Program under Contract No. IST-1999-11234. The first author was partially supported by the fund for the promotion of research at the Technion and the Israel MOD Research and Technology Unit.

[1] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1996), pp. 212–219.
[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[3] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998).
[4] E. Biham *et al.*, Phys. Rev. A **60**, 2742 (1999).
[5] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[6] R. M. Gingrich, C. P. Williams, and N. J. Cerf, Phys. Rev. A **61**, 052313 (2000).
[7] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, e-print quant-ph/0005055.
[8] G. L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu, Phys. Rev. A **61**, 042305 (2000).
[9] E. Biham *et al.*, Phys. Rev. A **63**, 012310 (2001).
[10] P. Høyer, Phys. Rev. A **62**, 052304 (2000).
[11] G. L. Long, L. Xiao, and Y. Sun, e-print quant-ph/0107013.
[12] S. Bose, L. Rallan, and V. Vedral, Phys. Rev. Lett. **85**, 5448 (2000).
[13] Bose *et al.* have a mistake regarding the entropy of the *classical* search problem. Just above their Eq. (10), they say that classical search can change entropy by ln $\sqrt{N}$ in $\sqrt{N}$ steps. This is true for a search field of size $\sqrt{N}$, but wrong for the question in matter where the search field is of size N. This mistake does not invalidate the other results in their paper.