Analysis of generalized Grover quantum search algorithms using recursion equations

Eli Biham,[1] Ofer Biham,[2] David Biron,[2,*] Markus Grassl,[3] Daniel A. Lidar,[4,†] and Daniel Shapira[2]
[1]*Computer Science Department, Technion, Haifa 32000, Israel*
[2]*Racah Institute of Physics, The Hebrew University, Jerusalem 91904, Israel*
[3]*Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, D-76128 Karlsruhe, Germany*
[4]*Department of Chemistry, University of California, Berkeley, California 94720*

(Received 18 August 2000; published 13 December 2000)

The recursion equation analysis of Grover's quantum search algorithm presented by Biham *et al.* [Phys. Rev. A **60**, 2742 (1999)] is generalized. It is applied to the large class of Grover-type algorithms in which the Hadamard transform is replaced by any other unitary transformation and the phase inversion is replaced by a rotation by an arbitrary angle. The time evolution of the amplitudes of the marked and unmarked states, for any initial complex amplitude distribution, is expressed using first-order linear difference equations. These equations are solved *exactly*. The solution provides the number of iterations T after which the probability of finding a marked state upon measurement is the highest, as well as the value of this probability, P_{max}. Both T and P_{max} are found to depend on the averages and variances of the initial amplitude distributions of the marked and unmarked states, but not on higher moments.

DOI: 10.1103/PhysRevA.63.012310 PACS number(s): 03.67.Lx, 89.70.+c

I. INTRODUCTION

Grover's search algorithm [1,2] provides a dramatic example of the potential speedup offered by quantum computers. It also provides an excellent laboratory for the analysis and implementation of quantum algorithms in various hardware media. The problem addressed by Grover's algorithm can be viewed as trying to find a marked element in an unsorted database of size N. To solve this problem, a classical computer would need, on average, $N/2$ database queries and N queries in the worst case. Using Grover's algorithm, a quantum computer can accomplish the same task using merely $O(\sqrt{N})$ queries. The importance of Grover's result stems from the fact that it proves the enhanced power of quantum computers compared to classical ones for a whole class of oracle-based problems, for which the bound on the efficiency of classical algorithms is known.

Grover's algorithm can be represented as searching a pre-image of an oracle-computable Boolean function, which can only be computed forward, but whose inverse cannot be directly computed. Such a function is $F:D\rightarrow\{0,1\}$ where D is a set of N domain values (or states) and the pre-images of the value 1 are called the marked states. The problem is to identify one of the marked states, i.e., some $v\in D$ such that $F(v)=1$. Problems of this type are very common. One important example, from cryptography, is searching for the key K of the data encryption standard (DES) [3], given a known plaintext P and its ciphertext C, where $F=1$ if the pair of plaintext and ciphertext match [i.e., $E_K(P)=C$ where E_K is the encryption function] and $F=0$ otherwise. Other examples are solutions of nondeterministic polynomial time (NP) and NP-complete problems, which include virtually all the difficult computing problems in practice [4].

Let us assume, for simplicity, that $N=2^n$, where n is an integer. We introduce a register $|\overline{x}\rangle=|x_1,\ldots,x_n\rangle$ of n qubits to be used in the computation. Grover's original quantum search algorithm consists of the following steps.

(1) Initialize the register to $|\overline{0}\rangle=|0\cdots00\rangle$, and apply the Hadamard transform to obtain a uniform amplitude distribution.

(2) Repeat the following operation T times

(a) Rotate the marked states by a phase of π radians.

(b) Rotate all states by π radians around the average amplitude of *all* states. This is done by (i) Hadamard transforming every qubit, (ii) rotating the $|\overline{0}\rangle$ state by a phase of π radians, and (iii) again Hadamard transforming every qubit.

(3)Measure the resulting state.

A large number of results followed Grover's discovery. These results include the proof [5] that the algorithm is as efficient as theoretically possible [6]. A variety of applications were developed, in which the algorithm is used in the solution of other problems [7–14]. Recently, experimental implementations of Grover's algorithm were constructed using nuclear magnetic resonance (NMR) [15,16] as well as an optical device [17].

Several generalizations of Grover's original algorithm have been developed. The case in which there are several marked states was studied in Ref. [18]. Let $k(t)$ $[l(t)]$ denote the amplitude of the *marked* [*unmarked*] states after t iterations of the algorithm. It was shown in [18] that the amplitude of the marked states increases as $k(t)=\sin[\omega(t+1/2)]/\sqrt{r}$, while at the same time that of the unmarked states decreases as $l(t)=\cos[\omega(t+1/2)]/\sqrt{N-r}$, where $\omega=2\arcsin(\sqrt{r/N})$ and r is the number of marked states. For $N\gg r$ the optimal time to measure and complete the computation is after $T=O(\sqrt{N/r})$ iterations, when $k(t)$ is maximal.

Recently, the algorithm was further generalized by allowing an arbitrary (but constant) unitary transformation to take the place of the Hadamard transform in the original setting

[*] Present address: Department of Physics of Complex Systems, Weizmann Institute of Science, Rehovot 76100, Israel.

[†] Permanent address: Chemistry Department, University of Toronto, 80 St. George Street, Toronto, ON, Canada M5S 3H6.

[19–21] and an arbitrary phase rotation of the marked and the predefined states instead of the π inversion [22]. Another generalization was obtained by allowing for an *arbitrary complex initial amplitude distribution*, instead of the uniform initial amplitude distribution obtained in step (1) above [23,24].

In this paper we analyze the time evolution of the amplitudes in the most general algorithm, using an arbitrary unitary transformation and phase rotations on an arbitrary complex initial amplitude distribution. Using first-order linear difference equations we obtain an exact solution for the time evolution of the amplitudes under the most general conditions. The solution provides the optimal number of iterations T after which the probability of finding a marked state upon measurement is the highest, as well as the value of this probability, P_{max}. Both T and P_{max} are found to depend on the averages and variances of the initial amplitude distributions of the marked and unmarked states, but not on higher moments.

The paper is organized as follows. In Sec. II we present the generalized algorithm. The analysis based on recursion equations is given in Sec. III. The results are discussed in Sec. IV and summarized in Sec. V. In the Appendix we obtain upper bounds on some weighted averages of the initial amplitudes of the marked and unmarked states which are needed in the analysis.

II. GENERALIZED GROVER ALGORITHM

In the generalized algorithm the initialization step is modified as follows. Instead of initializing the register according to step (1), any initial distribution of marked and unmarked states can be used (e.g., the final state of any other quantum computation). In addition, the π phase rotation of marked states described by $I_f^{\pi}=\Sigma_x e^{i\pi F(x)}|x\rangle\langle x|$ is replaced by rotation by an arbitrary phase γ:

$$I_f^{\gamma}=\sum_x e^{i\gamma F(x)}|x\rangle\langle x|. \tag{1}$$

The rotation about the average, described by $G=-WI_0^{\pi}W^{\dagger}$, where W is the Hadamard transform and $I_0^{\pi}=I-2|0\rangle\langle 0|$, is modified in two ways. First, the rotation of $|0\rangle$ by π is replaced by the rotation of a predefined state $|s\rangle$ by an angle β. Second, the Hadamard transform W is replaced by an arbitrary unitary operator U. In this generalized algorithm, step (2B) above is replaced by

$$G=-UI_s^{\beta}U^{\dagger}, \tag{2}$$

where

$$I_s^{\beta}=I-(1-e^{i\beta})|s\rangle\langle s|. \tag{3}$$

In the generalized algorithm, the geometric interpretation of step (2B) as a rotation around the average amplitude of all states is not straightforward. We will demonstrate below that, in fact, one can return to this interpretation by identifying suitable variables. By inserting I_s^{β} from Eq. (3) into Eq. (2) we obtain that

$$G=(1-e^{i\beta})|\eta\rangle\langle\eta|-I, \tag{4}$$

where $|\eta\rangle=U|s\rangle$.

III. RECURSION EQUATIONS

A. Analysis

We will now analyze the time evolution of the amplitudes in the generalized algorithm with a total of N states, r of which are marked. Let the marked amplitudes at time t be denoted by $k_i(t)$, $i\in M$, and the unmarked amplitudes by $l_i(t)$, $i\in\overline{M}$, where M is the set of marked states ($|M|=r$) and $\overline{M}$ is the set of unmarked states ($|\overline{M}|=N-r$). The initial amplitudes $k_i(0)$, $i\in M$ and $l_i(0)$, $i\in\overline{M}$ at $t=0$ are arbitrary. Without loss of generality we assume that the number of marked states satisfies $1\leqslant r\leqslant N/2$. A general state of the system at time t will now take the form

$$|g(t)\rangle=\sum_{i\in M}k_i(t)|i\rangle+\sum_{i\in\overline{M}}l_i(t)|i\rangle. \tag{5}$$

A single Grover iteration GI_f^{γ} will transform the amplitudes $k_j(t)$, $j\in M$, to $k_j(t+1)=\langle j|GI_f^{\gamma}|g(t)\rangle$ and the amplitudes $l_j(0)$, $j\in\overline{M}$, to $l_j(t+1)=\langle j|GI_f^{\gamma}|g(t)\rangle$. We find that the recursion equations describing such iteration take the form

$$\begin{aligned}k_j(t+1)=&(1-e^{i\beta})e^{i\gamma}\eta_j\sum_{i\in M}k_i(t)\eta_i^*\\&+(1-e^{i\beta})\eta_j\sum_{i\in\overline{M}}l_i(t)\eta_i^*-e^{i\gamma}k_j(t),\end{aligned} \tag{6}$$

$$\begin{aligned}l_j(t+1)=&(1-e^{i\beta})e^{i\gamma}\eta_j\sum_{i\in M}k_i(t)\eta_i^*\\&+(1-e^{i\beta})\eta_j\sum_{i\in\overline{M}}l_i(t)\eta_i^*-l_j(t),\end{aligned} \tag{7}$$

where

$$\eta_i=\langle i|\eta\rangle,\quad i=1,\ldots,N. \tag{8}$$

If $\eta_i=0$ for some i, the Grover iteration GI_f^{γ} changes only the phase of the state $|i\rangle$. Thus the probability to measure a state $|i\rangle$ with $\eta_i=0$ remains constant. Hence we can treat the states with $\eta_i=0$ separately from those with $\eta_i\neq 0$. From now on we assume, without loss of generality, that for the given operator U, the predefined state $|s\rangle$ is chosen such that $|\eta\rangle$ satisfies $\eta_i\neq 0$, $i=1,\ldots,N$. We will now introduce new variables

$$k_j'(t)=\frac{k_j(t)}{\eta_j}, \tag{9}$$

$$l_j'(t)=\frac{l_j(t)}{\eta_j}. \tag{10}$$

With these variables, the recursion equations will take the form

$$k_j'(t+1)=(1-e^{i\beta})e^{i\gamma}\sum_{i\in M}k_i'(t)|\eta_i|^2 +(1-e^{i\beta})\sum_{i\in\bar{M}}l_i'(t)|\eta_i|^2-e^{i\gamma}k_j'(t), \quad (11)$$

$$l_j'(t+1)=(1-e^{i\beta})e^{i\gamma}\sum_{i\in M}k_i'(t)|\eta_i|^2 +(1-e^{i\beta})\sum_{i\in\bar{M}}l_i'(t)|\eta_i|^2-l_j'(t). \quad (12)$$

Let us define

$$2C(t)=(1-e^{i\beta})e^{i\gamma}\sum_{i\in M}k_i'(t)|\eta_i|^2 +(1-e^{i\beta})\sum_{i\in\bar{M}}l_i'(t)|\eta_i|^2. \quad (13)$$

It becomes clear that the time evolution of all the amplitudes (of both marked and unmarked states) can be expressed by

$$k_j'(t+1)=2C(t)-e^{i\gamma}k_j'(t), \quad j\in M, \quad (14)$$

$$l_j'(t+1)=2C(t)-l_j'(t), \quad j\in\bar{M}. \quad (15)$$

One can define the following weights:

$$W_k=\sum_{i\in M}|\eta_i|^2, \quad (16)$$

$$W_l=\sum_{i\in\bar{M}}|\eta_i|^2, \quad (17)$$

quantifying the projections of the state $|\eta\rangle$ on M and $\bar{M}$, respectively. From the normalization of the state $|\eta\rangle$ it is clear that $W_k+W_l=1$. These weights can be used in order to define weighted averages of the new variables, of the form

$$\overline{k'}(t)=\frac{\sum_{i\in M}|\eta_i|^2k_i'(t)}{W_k}, \quad (18)$$

$$\overline{l'}(t)=\frac{\sum_{i\in\bar{M}}|\eta_i|^2l_i'(t)}{W_l}. \quad (19)$$

Using these averages to express $C(t)$ we obtain

$$2C(t)=(1-e^{i\beta})[e^{i\gamma}W_k\overline{k'}(t)+W_l\overline{l'}(t)]. \quad (20)$$

By averaging over all the marked states in Eq. (14) and over all the unmarked states in Eq. (15) we find that the weighted averages $\overline{k'}(t)$ and $\overline{l'}(t)$ obey the following recursion equations:

$$\overline{k'}(t+1)=2C(t)-e^{i\gamma}\overline{k'}(t), \quad (21)$$

$$\overline{l'}(t+1)=2C(t)-\overline{l'}(t). \quad (22)$$

These equations can be solved for $\overline{k'}(t)$ and $\overline{l'}(t)$, and along with the initial distribution this yields the exact solution for the dynamics of all amplitudes. We will proceed to solve the recursion formulas for arbitrary complex initial amplitudes. Let us rewrite Eqs. (21) and (22) in a matrix notation

$$\vec{r}(t+1)=A\vec{r}(t), \quad (23)$$

where

$$\vec{r}(t)=\begin{pmatrix}\overline{k'}(t)\\ \overline{l'}(t)\end{pmatrix} \quad (24)$$

and

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}. \quad (25)$$

The matrix elements of A are given by

$$a=(1-e^{i\beta})e^{i\gamma}W_k-e^{i\gamma}, \quad (26)$$

$$b=(1-e^{i\beta})W_l, \quad (27)$$

$$c=(1-e^{i\beta})e^{i\gamma}W_k, \quad (28)$$

$$d=(1-e^{i\beta})W_l-1. \quad (29)$$

The time evolution of $\overline{k'}(t)$ and $\overline{l'}(t)$ is given by

$$\vec{r}(t)=A^t\vec{r}(0). \quad (30)$$

In order to obtain explicit expressions for $\overline{k'}(t)$ and $\overline{l'}(t)$ we consider the diagonal matrix

$$A_D=S^{-1}AS\equiv\begin{pmatrix}\lambda_+ & 0\\ 0 & \lambda_-\end{pmatrix}. \quad (31)$$

The eigenvalues $\lambda_\pm$ of the matrix A are the solutions of $\det(A-\lambda I)=0$. They can be expressed as

$$\lambda_\pm=e^{i\omega_\pm}, \quad (32)$$

where

$$\omega_\pm=\pi+\frac{\beta+\gamma}{2}\pm\omega \quad (33)$$

and the angular frequency ω is in the range $0<\omega<\pi$, and satisfies

$$\cos\omega = W_k \cos\frac{\beta+\gamma}{2} + W_l \cos\frac{\beta-\gamma}{2}. \tag{34}$$

The matrix *S*, which consists of the corresponding column eigenvectors, takes the form

$$S = \begin{pmatrix} 1 & 1 \\ \dfrac{\lambda_+ - a}{b} & \dfrac{\lambda_- - a}{b} \end{pmatrix}. \tag{35}$$

We will now apply Eq. (31) to reconstruct the matrix *A*, and compute A^t. A simpler expression for the time evolution is obtained:

$$\vec{r}(t) = S A_D^t S^{-1} \vec{r}(0), \tag{36}$$

where

$$A_D^t = \begin{pmatrix} \lambda_+^t & 0 \\ 0 & \lambda_-^t \end{pmatrix}. \tag{37}$$

The time dependence is given by

$$\overline{k'}(t) = z_1 e^{i\omega_+ t} - z_2 e^{i\omega_- t}, \tag{38}$$

$$\overline{l'}(t) = z_3 e^{i\omega_+ t} - z_4 e^{i\omega_- t}, \tag{39}$$

where

$$z_1 = \frac{(\lambda_- - a)\overline{k'}(0) - b\overline{l'}(0)}{\lambda_- - \lambda_+}, \tag{40}$$

$$z_2 = \frac{(\lambda_+ - a)\overline{k'}(0) - b\overline{l'}(0)}{\lambda_- - \lambda_+} \tag{41}$$

and

$$z_3 = \frac{\lambda_+ - a}{b} z_1, \tag{42}$$

$$z_4 = \frac{\lambda_- - a}{b} z_2. \tag{43}$$

We have now completed the solution for the time dependence of the averages $\overline{k'}(t)$ and $\overline{l'}(t)$. However, our aim is to obtain the time evolution of the individual variables $k_i{}'(t)$ and $l_i{}'(t)$ and from them to extract the amplitudes $k_i(t)$ and $l_i(t)$. Subtracting Eq. (21) from Eq. (14), and Eq. (22) from Eq. (15) one finds that

$$k_i'(t+1) - \overline{k'}(t+1) = -e^{i\gamma}[k_i'(t) - \overline{k'}(t)], \tag{44}$$

$$l_i'(t+1) - \overline{l'}(t+1) = -[l_i'(t) - \overline{l'}(t)]; \tag{45}$$

namely, the difference, in absolute value, between each of the variables $k_i{}'(t)$, $l_i{}'(t)$ and the averages of the corresponding sets are time independent. This means that

$$\Delta k_i' \equiv k_i'(0) - \overline{k'}(0), \tag{46}$$

$$\Delta l_i' \equiv l_i'(0) - \overline{l'}(0) \tag{47}$$

are *constants of motion*. Thus, the time dependence of the variables follows:

$$k_i'(t) = \overline{k'}(t) + (-1)^t e^{i\gamma t} \Delta k_i', \tag{48}$$

$$l_i'(t) = \overline{l'}(t) + (-1)^t \Delta l_i'. \tag{49}$$

The time evolution of the amplitudes can now be obtained:

$$k_i(t) = \eta_i[\overline{k'}(t) + (-1)^t e^{i\gamma t} \Delta k_i'], \tag{50}$$

$$l_i(t) = \eta_i[\overline{l'}(t) + (-1)^t \Delta l_i']. \tag{51}$$

In this picture all the marked as well as the unmarked states evolve in unison, so it is sufficient to follow the time evolution of the average in each set. The only feature distinguishing the states from one another is their initial deviation from the average.

B. Results

From Eqs. (48) and (49) it follows immediately that the weighted variances

$$\sigma_k^2(t) = \frac{1}{W_k} \sum_{i \in M} |\eta_i|^2 |k_i'(t) - \overline{k'}(t)|^2, \tag{52}$$

$$\sigma_l^2(t) = \frac{1}{W_l} \sum_{i \in \bar{M}} |\eta_i|^2 |l_i'(t) - \overline{l'}(t)|^2 \tag{53}$$

are time independent and therefore at any time *t* they can be replaced by $\sigma_k^2 = \sigma_k^2(0)$ and $\sigma_l^2 = \sigma_l^2(0)$, respectively. When a measurement is performed at time *t*, the probability that a marked state will be obtained is $P(t) = \Sigma_{i \in M} |k_i(t)|^2$. Since all the operators used are unitary, the variables $k_i{}'(t)$ and $l_i{}'(t)$ satisfy the normalization condition

$$\sum_{i \in M} |\eta_i|^2 |k_i'(t)|^2 + \sum_{i \in \bar{M}} |\eta_i|^2 |l_i'(t)|^2 = 1 \tag{54}$$

at all times. Using the definitions of $k_i'(t)$ and $l_i'(t)$ and their weighted averages $\overline{k'}(t)$ and $\overline{l'}(t)$ given in Eqs. (9), (10) and (18), (19), one can bring Eqs. (52) and (53) to the form

$$\sum_{i \in M} |k_i(t)|^2 = W_k \sigma_k^2 + W_k |\overline{k'}(t)|^2, \tag{55}$$

$$\sum_{i \in \bar{M}} |l_i(t)|^2 = W_l \sigma_l^2 + W_l |\overline{l'}(t)|^2. \tag{56}$$

The first equation provides the probability to measure a marked state at time *t*, while the probability to measure an unmarked state is given by the second equation. We will now try to examine the probability that a measurement at time *t* will yield a marked state, and its dependence on the rotation angles β and γ, the unitary transformation U, the predefined state $|s\rangle$, and the averages and standard deviations of the initial amplitude distributions of the marked and unmarked states. Using Eq. (38) with $z_1=|z_1|e^{i\phi_1}$ and $z_2=|z_2|e^{i\phi_2}$, the probability that a measurement at time t will yield a marked state is given by a sinusoidal function of the form

$$P(t)=P_{av}-\Delta P\cos[2(\omega t+\phi)], \tag{57}$$

where

$$\Delta P=2W_k|z_1||z_2| \tag{58}$$

is the amplitude of the oscillations, π/ω is their period,

$$P_{av}=W_k(|z_1|^2+|z_2|^2+\sigma_k^2) \tag{59}$$

is the average, or reference value of the probability, and

$$2\phi=\phi_1-\phi_2 \tag{60}$$

is the phase. These parameters are found to depend on the unitary operator U which is used in the algorithm, the predefined state $|s\rangle$, and the angle β by which its phase is rotated as well as the angle γ by which the phases of the marked states are rotated. The dependence on the initial amplitudes enters only through the weighted averages of the variables $k_i{}'(0)$ and $l_i{}'(0)$ and their standard deviations.

It is thus observed that $P(t)$ does not depend on any higher moments of the initial amplitude distribution. This is due to the fact that all the transformations in the quantum algorithm are linear. Therefore, $k_i(t)$ and $l_i(t)$ can be expressed as some linear combinations of $k_i(0)$ and $l_i(0)$. The only nonlinearity appears in the expression of $P(t)$ as a sum of squares of the amplitudes of the marked states at time t. Therefore, powers higher than quadratic are excluded in the expression for $P(t)$. Moreover, $P(t)$ does not depend on any other linear combinations of the first and second powers of the initial amplitudes, except for the particular weighted averages that compose the first and second moments. This results from the fact that Grover's iterations maintain a large number of conserved quantities, particularly the variances σ_k^2 and σ_l^2 which are constants of motion. As a result, the time evolution of the amplitudes can be fully described by the time dependence of the averages $\overline{k'}(t)$ and $\overline{l'}(t)$. Due to the linearity of the transformations, $\overline{k'}(t)$ and $\overline{l'}(t)$ can be expressed as linear combinations of $\overline{k'}(0)$ and $\overline{l'}(0)$. The probability $P(t)$ of measuring a marked state at time t is given by Eq. (55) in which the first term on the right hand side, which includes the second moment, is a constant of motion. Therefore, no other quadratic forms can appear. The second term depends on the first moment at time t, which is related to the first moment at $t=0$ through the recursion equations. Thus, the dependence of $P(t)$ on the initial amplitudes is only through the first and second moments of their distribution.

IV. DISCUSSION

In order to examine the performance of the generalized Grover algorithm we will now evaluate the highest possible probability $P_{max}=P_{av}+\Delta P$ that a measurement will yield a marked state. We will also evaluate the optimal number of iterations T after which the probability P_{max} is achieved.

The limit of difficult search problems is obtained when $N\gg r\gg 1$. This is reflected in the fact that in the original Grover algorithm the probability of measuring a marked state immediately after the initialization step is $W_k=r/N$. The assumption that $W_k\ll 1$ carries over to the generalized case discussed here. It is satisfied in all cases except for very unlikely choices of the state $|s\rangle$ from which one Grover iteration with the operator U is sufficient in order to measure a marked state with high probability. In the analysis below W_k will be considered as a small parameter. The highest possible value of the probability to measure a marked state is

$$P_{max}=W_k(|z_1|+|z_2|)^2+W_k\sigma_k^2. \tag{61}$$

Consider the parameters z_1 and z_2 that express the dependence of P_{max} on the initial amplitudes and the phase rotation angles β and γ. The expressions for z_1 and z_2 in Eqs. (40) and (41) include $(\lambda_- - \lambda_+)$ in the denominator. Using Eq. (32) it can be written as

$$\lambda_- - \lambda_+ = 2ie^{i(\beta+\gamma)/2}\sin\omega. \tag{62}$$

Expanding $\sin\omega$ in powers of $W_k\ll 1$, one finds that in case that the angles β and γ are different, and the difference between them satisfies $|\beta-\gamma|=O(1)$ (e.g., in radians):

$$\lambda_- - \lambda_+ = 2ie^{i(\beta+\gamma)/2}\sin\frac{|\beta-\gamma|}{2}+O(W_k); \tag{63}$$

namely, the denominator, in absolute value, is typically of order unity. In case $\beta=\gamma$

$$\lambda_- - \lambda_+ = 4ie^{i\beta}\sin\frac{\beta}{2}W_k{}^{1/2}+O(W_k{}^{3/2}) \tag{64}$$

and the denominator is of order $\sqrt{W_k}\ll 1$. In the following we discuss the search problem in these two cases separately.

A. Different rotation angles: $\beta\neq\gamma$

Here we consider the case when $\beta\neq\gamma$ and the difference between them is fixed and finite, and satisfies $|\beta-\gamma|=O(1)$. In this case, using Eqs. (26), (27), and (32) and the assumption that $W_k\ll 1$, the matrix elements can be approximated by

$$a=-e^{i\gamma}+O(W_k), \tag{65}$$

$$b=1-e^{i\beta}+O(W_k). \tag{66}$$

The eigenvalues are

$$\lambda_+=-e^{i\beta}+O(W_k), \tag{67}$$

$$\lambda_-=-e^{i\gamma}+O(W_k), \tag{68}$$

when $\beta > \gamma$ ($0 < \beta < 2\pi$, $0 < \gamma < 2\pi$), and

$$\lambda_+ = -e^{i\gamma} + O(W_k), \tag{69}$$

$$\lambda_- = -e^{i\beta} + O(W_k), \tag{70}$$

when $\gamma > \beta$. In the Appendix it is shown that the initial amplitude distribution satisfies $|\overline{k'}(0)| = O(W_k^{-1/2})$ and $|\overline{l'}(0)| = O(1)$. From Eqs. (40) and (41) we obtain that $|z_1| = O(1)$ and $|z_2| = O({W_k}^{-1/2})$, in the case $\beta > \gamma$, while in the case $\gamma > \beta$, $|z_1| = O({W_k}^{-1/2})$ and $|z_2| = O(1)$. Therefore, in both cases, using Eq. (58) one obtains

$$\Delta P = O(W_k^{1/2}); \tag{71}$$

namely, the amplitude of the oscillations is negligible. Thus, the probability to measure a marked state after any number of iterations cannot be significantly larger than the probability, given by Eq. (55), to measure a marked state at time $t = 0$. We conclude that in this case the algorithm fails to enhance the probability of measuring a marked state. The angular frequency is $\omega = |\beta - \gamma|/2 + O(W_k)$. Clearly, for such a high frequency, for which the period is of the order of only few steps, it is hard to exploit the oscillations since measurements can be taken only in discrete times and are likely to miss the highest point. The analysis presented above applies as long as $W_k \ll (\beta - \gamma)^2$. The conclusions are in agreement with the results of Refs. [22,25].

B. Identical rotation angles: $\beta = \gamma$

In this case the matrix elements can be approximated according to

$$a = -e^{i\beta} + O(W_k), \tag{72}$$

$$b = 1 - e^{i\beta} + O(W_k), \tag{73}$$

$$\lambda_\pm = -e^{i\beta} \mp i\left[2e^{i\beta}\sin\frac{\beta}{2}\right]{W_k}^{1/2} + O(W_k). \tag{74}$$

This gives rise to

$$z_{1,2} = \frac{1}{2}{W_k}^{-1/2}[i\overline{l'}(0)e^{i\psi} \pm {W_k}^{1/2}\overline{k'}(0)] + O(1), \tag{75}$$

where $\psi = (\pi - \beta)/2$. Inserting Eq. (75) into Eq. (61) we obtain

$$\begin{aligned} P_{max} = \frac{1}{4}[&|i\overline{l'}(0)e^{i\psi} + {W_k}^{1/2}\overline{k'}(0)| \\ &+ |i\overline{l'}(0)e^{i\psi} - {W_k}^{1/2}\overline{k'}(0)|]^2 \\ &+ W_k\sigma_k^2 + O(W_k). \end{aligned} \tag{76}$$

To simplify this expression we will now use the identity $(|a+b| + |a-b|)^2 = 2(|a|^2 + |b|^2 + |a^2 - b^2|)$, where a and b are complex numbers. We will also replace $\overline{l'}(0)$ by ${W_l}^{1/2}\overline{l'}(0)$ [note that ${W_l}^{1/2} = 1 + O(W_k)$] and find that

$$\begin{aligned} P_{max} = 1 - W_l\sigma_l^2 - \frac{1}{2}W_l|\overline{l'}(0)|^2 \\ - \frac{1}{2}W_k|\overline{k'}(0)|^2 + \frac{1}{2}\ \Big|W_l|\overline{l'}(0)|^2 e^{2i(\psi + \alpha_l - \alpha_k)} \\ + W_k|\overline{k'}(0)|^2\Big| + O(W_k), \end{aligned} \tag{77}$$

where $\overline{k'}(0) = |\overline{k'}(0)|e^{i\alpha_k}$ and $\overline{l'}(0) = |\overline{l'}(0)|e^{i\alpha_l}$. This is in agreement with the results of Ref. [20], where the case $\beta = \gamma = \pi$ was studied using a different approach. We observe that P_{max} depends on the statistical properties (averages and variances) of the initial amplitude distribution of the marked and unmarked states. For a given distribution, the probability of measuring a marked state is bounded by $P_{max} = 1 - W_l\sigma_l^2$. This upper bound is reached when $\psi + \alpha_l - \alpha_k = 0$, as well as when $\overline{l'} = 0$ or $\overline{k'} = 0$. This optimization can be achieved by an adjustment of the rotation phases to the value $\beta = \pi - 2(\alpha_k - \alpha_l)$. However, this requires one to know the difference between the phases α_k and α_l, which is not generally available for an arbitrary initial amplitude distribution.

The optimal case of $P_{max} = 1$ can be obtained by using the predefined state $|s\rangle$ and applying on it the operator U, to generate the initial amplitude distribution. In this case the initial unmarked state variance is $\sigma_l = 0$, the weighted initial averages are $\overline{k'}(0) = 1$ and $\overline{l'}(0) = 1$, and the phases $\alpha_k = \alpha_l = 0$. Thus, executing the generalized Grover iterations using the same unitary operator U, the predefined state $|s\rangle$ as the initial state, and a rotation phase of $\beta = \gamma = \pi$ enables one to measure a marked state with the optimal probability $P_{max} = 1$. The original Grover algorithm is a special case in which U is the Hadamard operator and the predefined state $|s\rangle = |0 \cdots 00\rangle$.

Consider an arbitrary initial distribution of r marked and $N - r$ unmarked states, with known averages $\overline{k}(0)$ and $\overline{l}(0)$, respectively. The probability $P(t)$ that a measurement at time t will yield a marked state is a sinusoidal function, given by Eq. (57). The highest value of $P(t)$ is obtained at time T, for which the argument of the cosine function satisfies $2(\omega T + \phi) = \pi$. Thus, the number of iterations T which gives rise to the highest probability of finding a marked state upon measurement is

$$T = \frac{\pi - 2\phi}{2\omega}, \tag{78}$$

where the angular frequency is

$$\omega = 2\sin\frac{\beta}{2}\sqrt{W_k} + O(W_k^{3/2}). \tag{79}$$

An interesting case is the one in which the average and variance of the initial amplitude distribution are *not* known, but different runs of the algorithm use initial amplitudes drawn from the same distribution. Naively, one could pick a random number of iterations T_r and thus find a marked state with probability $P(T_r)$. Correspondingly, the expected number of repetitions of the entire algorithm using the same T_r

would be $1/P(T_r)$ until a marked state is found. However, $P(T_r)$ could be very small. A better strategy is now shown. From Eqs. (34) and (57) it follows that the period of oscillation of $P(t)$ depends only on the unitary operator U and the predefined state $|s\rangle$ as well as on the rotation phase $\beta=\gamma$ used in the algorithm. The phase ϕ depends on the initial amplitude distribution and is thus unknown. Consider the case where one runs the algorithm twice, taking measurements at times T_1 and T_2, respectively, where $T_2-T_1 = \pi/(2\omega)$. From Eq. (57) it is clear that in one of the two measurements the cosine expression will be negative so that $P(T)\geqslant P_{av}$. Since the probability $P(t)$ must be nonnegative at any time, $P_{av}\geqslant \Delta P$. Since $P_{max}=P_{av}+\Delta P$, we also find that $P_{av}\geqslant P_{max}/2$. Therefore, in one of the two measurements one obtains $P(T)\geqslant P_{max}/2$. In this case one needs twice as many repetitions to obtain at least half the success probability compared to the case when the optimal measurement time is known. The slowdown is thus at most by a factor of 4.

V. SUMMARY

In this paper we have generalized the recursion equation analysis of Grover's quantum search algorithm presented in Ref. [24]. We applied it to the large class of Grover-type algorithms in which the Hadamard transform is replaced by any unitary transformation and the phase inversion is replaced by a rotation by an arbitrary angle. We derived recursion equations for the time evolution of the amplitudes of the marked and unmarked states, for any initial complex amplitude distribution. These equations were solved *exactly*. From the solution we obtained an expression for the optimal number of iterations T after which the probability of finding a marked state upon measurement is the highest. The value of this probability, P_{max}, was also obtained. Both T and P_{max} are found to depend on the averages and variances of the initial amplitude distributions of the marked and unmarked states, but not on higher moments. This is due to the linearity of the transformations and the large number of conserved quantities, particularly the (weighted) variances of the distributions of the amplitudes of the marked and unmarked states. The time T and the probability P_{max} also depend on the unitary operator U which is used in the algorithm, the predefined state $|s\rangle$, and the angle β by which its phase is rotated as well as the angle γ by which the phases of the marked states are rotated. Moreover, it was found that in order for the algorithm to apply the two rotation angles must be equal, namely, $\beta=\gamma$.

ACKNOWLEDGMENTS

We thank Dan Kenigsberg for helpful discussions and comments. This work was initiated during the Elsag-Bailey–I.S.I. Foundation research meeting on quantum computation in 1998. It was supported by EU fifth framework program Grant No. IST-1999-11234.

APPENDIX

In this appendix we obtain upper bounds on $|\overline{k'}(0)|$ and $|\overline{l'}(0)|$ in the initial amplitude distribution. According to Eqs. (9) and (18) the initial distribution weighted average of the marked states is

$$\overline{k'}(0)=\frac{\sum_{i\in M}\eta_i^* k_i(0)}{W_k}. \qquad \text{(A1)}$$

From normalization it is clear that $|k_i(0)|\leqslant 1$ for any marked state. Therefore

$$|\overline{k'}(0)|\leqslant\frac{\sum_{i\in M}|\eta_i||k_i(0)|}{W_k}\leqslant\frac{\sum_{i\in M}|\eta_i|}{W_k}\leqslant\frac{r|\eta|}{W_k}, \qquad \text{(A2)}$$

where r is the number of marked states and $|\eta| = \max_{i\in M}|\eta_i|$. Since $|\eta|^2\leqslant\Sigma_{i\in M}|\eta_i|^2=W_k$, one obtains

$$|\overline{k'}(0)|\leqslant\frac{r{W_k}^{1/2}}{W_k}=r{W_k}^{-1/2}. \qquad \text{(A3)}$$

Therefore, typical initial amplitude distributions in large search problems satisfy

$$|\overline{k'}(0)|=O({W_k}^{-1/2}). \qquad \text{(A4)}$$

According to Eqs. (10) and (19) the weighted average of the initial distribution $l_i'(0)$ satisfies

$$\overline{l'}(0)=\frac{\sum_{i\in \bar{M}}\eta_i^* l_i(0)}{W_l}=\sum_{i\in \bar{M}}\eta_i^* l_i(0)+O(W_k). \qquad \text{(A5)}$$

Using Eq. (5) for the initial state of the system $|g(0)\rangle$, the expression for $\overline{k'}(0)$ [given in Eq. (A1)], and $\eta_i^* =\langle s|U^*|i\rangle$, one can bring Eq. (A5) to the form

$$\overline{l'}(0)=\langle s|U^*|g(0)\rangle-W_k\overline{k'}(0)+O(W_k). \qquad \text{(A6)}$$

Using Eq. (A4) one obtains

$$\overline{l'}(0)=\langle s|U^*|g(0)\rangle+O({W_k}^{1/2}). \qquad \text{(A7)}$$

Since $|g(0)\rangle$ is normalized and U^* is unitary, $|\langle s|U^*|g(0)\rangle|<1$. Therefore,

$$|\overline{l'}(0)|<1+O({W_k}^{1/2}), \qquad \text{(A8)}$$

namely,

$$|\overline{l'}(0)|=O(1). \qquad \text{(A9)}$$

[1] L.K. Grover, in *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996), p. 212.

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

[3] D.R. Stinson, *Cryptography: Theory and Practice* (CRC Press, Baton Rouge, FL, 1995).

[4] M.R. Garey and D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, New York, 1979).

[5] C. Zalka, Phys. Rev. A **60**, 2746 (1999).

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

[7] C. Durr and P. Høyer, e-print quant-ph/9607014.

[8] L.K. Grover, e-print quant-ph/9607024.

[9] L.K. Grover, e-print quant-ph/9704012.

[10] B.M. Terhal and J.A. Smolin, Phys. Rev. A **58**, 1822 (1998).

[11] G. Brassard, P. Høyer and A. Tapp, in *Automata, Languages and Programming*, edited by K.G. Larsen, S. Skyum, and G. Winskel (Springer-Verlag, Berlin, 1998), Vol. 1443, p. 820.

[12] N.J. Cerf, L.K. Grover, and C.P. Williams, Phys. Rev. A **61**, 032303 (2000).

[13] L.K. Grover, Phys. Rev. Lett. **85**, 1334 (2000).

[14] A. Carlini and A. Hosoya, e-print quant-ph/9909089.

[15] I.L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).

[16] J.A. Jones, M. Mosca, and R.H. Hansen, Nature (London) **393**, 344 (1998).

[17] P.G. Kwiat, J.R. Mitchell, P.D.D. Schwindt, and A.G. White, J. Mod. Opt. **47**, 257 (2000).

[18] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, in *Proceedings of the fourth workshop on Physics and Computation*, edited by T. Toffoli, M. Biafore, and J. Leao (New England Complex Systems Institute, Boston, 1996), p. 36.

[19] L.K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).

[20] R.M. Gingrich, C.P. Williams, and N.J. Cerf, Phys. Rev. A **61**, 052313 (2000).

[21] R. Jozsa, e-print quant-ph/9901021.

[22] G.L. Long, W.L. Zhang, Y.S. Li, and L. Nui, Commun. Theor. Phys. **32**, 335 (1999).

[23] D. Biron, O. Biham, E. Biham, M. Grassl, and D.A. Lidar, in *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, Lecture Notes in Computer Science (Springer-Verlag, Berlin, 1998); e-print quant-ph/9801066.

[24] E. Biham, O. Biham, D. Biron, M. Grassl, and D. Lidar, Phys. Rev. A **60**, 2742 (1999).

[25] G.L. Long, C.C. Tu, Y.S. Li, W.L. Zhang, and H.Y. Yan, e-print quant-ph/9911004.