Family of Grover's quantum-searching algorithms

A. Galindo and M. A. Martín-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040-Madrid, Spain
(Received 14 June 2000; published 8 November 2000)

We introduce the concepts of Grover operators and Grover kernels to systematically analyze Grover's searching algorithms. Then we investigate a one-parameter family of quantum searching algorithms of Grover type and we show that the standard Grover algorithm is a distinguished member of this family. We show that all the algorithms of this class solve the searching problem with an efficiency of order $O(\sqrt{N})$, with a coefficient which is class-dependent. The analysis of this dependence is a test of the stability and robustness of the algorithms. We show the stability of this constructions under perturbations of the initial conditions and extend them to a very general class of Grover operators.

PACS number(s): 03.67.Lx

I. INTRODUCTION

The problem of searching for an element in a list of N unsorted elements when this number becomes very large is known to be one of the basic problems of computational science. Classically, one may devise many strategies to perform that search, but if the elements in the list are distributed with equal probability, then we shall need to make $O(N)$ trials in order to have a high level of confidence of finding the desired element, also called the marked element. The formulation of quantum computation as a well-established theoretical discipline for storing and processing information [1] has opened the possibility of designing new searching algorithms with no classical analogue. The familiar Grover quantum searching algorithm takes advantage of the quantum mechanical properties to perform the searching problem with an efficiency of order $O(\sqrt{N})$ [2,3].

In classical computation there exist design techniques that provide general directions for algorithmic problem solving. In quantum computation, however, the list of quantum algorithms is very short. It seems we are lacking the basic principles underlying the quantum algorithmic design. Under these circumstances, it is a good choice to put to the test the currently known quantum algorithms. In this work, our aim is to follow this goal with Grover's quantum searching algorithm by trying to understand the relevant pieces of this algorithm and questioning to what extent they allow for generalization [4–10].

Let us state the searching problem in terms of a list $\mathcal{L}[0,1,\ldots,N-1]$ with a number N of unsorted elements. We shall denote by x_0 the marked element in $\mathcal{L}$ that we are searching for. The quantum mechanical solution of this searching problem goes through the preparation of a quantum register in a quantum computer to store the N items on our list. This is how quantum parallelism is realized. Thus, let us assume that our quantum registers are made of n qubits so that the total elements we have are $N=2^n$. Let us denote by $|x\rangle$, $x=0,1,\ldots,N-1$ the ket states of the computational basis which are orthonormalized. Any state $|\Psi\rangle$ of the quantum register is a linear superposition of the computational states. In the beginning of the algorithm the quantum register is initialized to a given quantum state $|\Psi\rangle=|x_{\text{in}}\rangle$.

The second component of the algorithm is to design a quantum operation that will be repeatedly applied to $|x_{\text{in}}\rangle$ in order to find the marked element. This strategy is similar to the classical counterpart algorithm. The difference is the fact that the quantum operation is realized in terms of a unitary operator that implements the reversible quantum computation. It is this quantum operation that has been so neatly designed by Grover [2]. With Grover's choice we may say that the quantum evolution is such that the constructive interference of quantum amplitudes is directed towards the marked state one looks for.

II. GROVER OPERATORS

In order to set up our analysis we shall need to introduce some definitions.

Definition 1. A Grover operator G is any unitary operator with at most two different eigenvalues; i.e., G is a linear superposition of two orthogonal projectors P and Q:

$$G=\alpha P+\beta Q, \quad P^2=P, \quad Q^2=Q, \quad P+Q=1, \tag{1}$$

where $\alpha,\beta\in\mathbb{C}$ are complex numbers of unit norm.

Definition 2. A Grover kernel K is the product of two Grover operators:

$$K=G_2G_1. \tag{2}$$

Some elementary properties follow immediately from these definitions.

Property 1. Any Grover kernel K is a unitary operator and, therefore, it can be used to implement the unitary evolution in a quantum computer.

Property 2. Let the Grover operators G_1,G_2 be chosen such that

$$G_1=\alpha P_{x_0}+\beta Q_{x_0}, \quad P_{x_0}=|x_0\rangle\langle x_0|, \quad P_{x_0}+Q_{x_0}=1, \tag{3}$$

$$G_2=\gamma\overline{P}+\delta\overline{Q}, \quad \overline{P}+\overline{Q}=1, \tag{4}$$

with $\overline{P}$ given by the rank 1 matrix

$$\overline{P}=\frac{1}{N}\begin{pmatrix}1 & \cdots & 1\\ \vdots & & \vdots\\ 1 & \cdots & 1\end{pmatrix}. \tag{5}$$

This is clearly a projector $\overline{P}=|k_0\rangle\langle k_0|$ on the subspace spanned by the state $|k_0\rangle=\frac{1}{\sqrt{N}}(1,\ldots,1)^{\mathrm{t}}$, where the superscript denotes the transpose. Then, if we take the following set of parameters,

$$\alpha=-1,\quad \beta=1,\quad \gamma=-1,\quad \delta=1, \tag{6}$$

the Grover kernel (2) reproduces the original Grover choice. This property follows immediately by construction. In fact, we have in this case $G_1=1-2P_{x_0}=:G_{x_0}$ while the operator $G_2=1-2\overline{P}$ coincides with the diffusion operator introduced by Grover to implement the inversion about the average [2].

One can also show the following property, which provides a geometrical meaning for the Grover kernels.

Property 3. Let $\mathcal{K}_{\mathrm{G}}$ denote the set of all the Grover kernels for fixed $\{|x_0\rangle,|k_0\rangle\}$. Then $\mathcal{K}_{\mathrm{G}}$ can be viewed as a three-dimensional (3D) subset of the group U(2), which is of the form $S^1\times\mathcal{K}'_{\mathrm{G}}$, where $\mathcal{K}'_{\mathrm{G}}$ is a 2D submanifold of SU(2) (Fig. 1).

The content of this property is illustrated in Fig. 1. It follows from the fact that the two parameters of a Grover kernel in Definition 2 with the fixing (6) can be used to parametrize a subset of the unitary group U(2) of complex 2×2 matrices. This 3D subset has a factorized form $S^1\times\mathcal{K}'_{\mathrm{G}}$, where S^1 is the unit circle [the group U(1)], and we call $\mathcal{K}'_{\mathrm{G}}$ a certain 2D submanifold of the group of special unitary matrices SU(2) whose construction we explain in the following and plot in Fig. 1. This figure is constructed by parametrizing the two elements $\pm iG_{1,2}$ of SU(2) as follows: $\pm iG_{1,2}=e^{i\alpha_{1,2}\mathbf{n}_{1,2}\cdot\boldsymbol{\sigma}}$, where $\boldsymbol{\sigma}$ are the Pauli matrices and $\mathbf{n}_{1,2}$ are unit vectors which are kept fixed. Likewise, we parametrize the corresponding Grover kernel (2) as $K=e^{i\alpha\mathbf{n}\cdot\boldsymbol{\sigma}}$. Then, upon varying the parameters $\alpha_{1,2}$ we obtain the surface depicted in Fig. 1. Let us point out the following interpretation of the Grover operators. Let us think of the computational basis $\{|x\rangle\}$ as a coordinate basis in quantum mechanics and introduce the quantum discrete Fourier transform in the standard fashion, $|\hat{x}\rangle:=U_{\mathrm{DFT}}|x\rangle=(1/\sqrt{N})\Sigma_{y=0}^{N-1}e^{2\pi ix\cdot y/N}|y\rangle$. The transformed basis $\{|\hat{x}\}$ can then be seen as the dual momentum basis. Then, it is easy to see that in such a basis the projector operator $\overline{P}$ takes the following form:

$$U_{\mathrm{DFT}}^{-1}\overline{P}U_{\mathrm{DFT}}=|0\rangle\langle0|=:P_0. \tag{7}$$

This means that the Grover operator G_2 takes the same matrixlike form in the momentum basis as the Grover operator G_1 in the coordinate basis. They are somehow dual of each other. The original Grover kernel takes then the form

$$K=U_{\mathrm{DFT}}G_{x=0}U_{\mathrm{DFT}}^{-1}G_{x_0}, \tag{8}$$

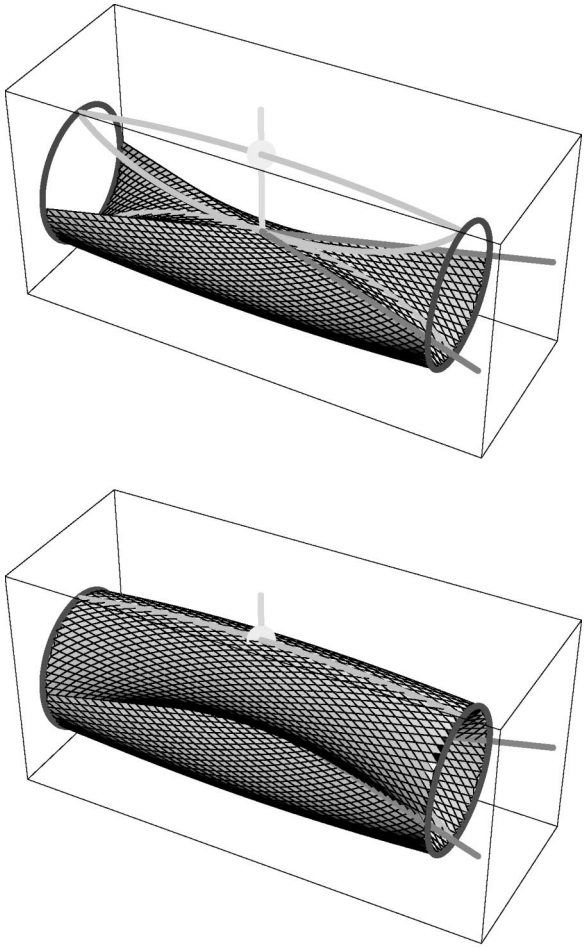

FIG. 1. Top: half of the surface $\mathcal{K}'_G$ for $N=10$. Bottom: the whole surface $\mathcal{K}'_G$ for $N=10$. The straight lines represent the rotation axes corresponding to $iG_{1,2}\in\mathrm{SU}(2)$ and the normal to their plane. The dot signals the original Grover kernel. The front circle curves are the border $\alpha=\pi,3\pi$, where α is the rotation angle. The rest of the curves represent the locus of kernels K with factors i$G_{1,2}$ with the same rotation angles mod 2π.

which shows that a Grover kernel has a part local in coordinate space and another part which is local in momentum space. This ''momentum'' interpretation of the search algorithm stems from a quantum mechanical analogy between the computational basis and its Fourier-transformed states that enter into the definition of the Grover operators. We would like to point out that similar analogies have been used in connection with alternative formulations of the quantum searching algorithm, namely, the analog analogue of a digital quantum computation with Grover's algorithm [10] which is based on a Hamiltonian formulation.

III. THE SEARCHING ALGORITHMS

A. The basic formalism

Next, the third part of the algorithms corresponds to applying the Grover kernel K to the initial state $|x_{\mathrm{in}}\rangle$ a number of times m, seeking a final state $|x_{\mathrm{f}}\rangle$ given by

$$|x_f(m)\rangle=K^m|x_{\mathrm{in}}\rangle \tag{9}$$

such that the probability $\mathcal{P}(x_0)$ of finding the marked state is above a given threshold value. We shall take this value to be 1/2, meaning that we choose a probability of success of 50% or larger. Thus, we are seeking to determine under which circumstances the following condition,

$$\mathcal{P}(x_0)=|\langle x_0|K^m|x_{\rm in}\rangle|^2>1/2, \tag{10}$$

holds true.

The analysis of this probability is simplified if we realize that the evolution associated with the searching problem can be mapped onto a reduced 2D space spanned by the vectors

$$\left\{|x_0\rangle,|x_\perp\rangle:=\frac{1}{\sqrt{N-1}}\sum_{x\neq x_0}|x\rangle\right\}. \tag{11}$$

Then we can easily compute the projections of the Grover operators G_1, G_2 in the reduced basis with the result

$$G_1=\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}, \tag{12}$$

$$G_2=\begin{pmatrix}\delta & 0\\ 0 & \gamma\end{pmatrix}+(\gamma-\delta)\begin{pmatrix}\frac{1}{N} & \sqrt{\frac{N-1}{N}}\\ \sqrt{\frac{N-1}{N}} & \frac{-1}{N}\end{pmatrix}. \tag{13}$$

From now on, we shall fix two of the phase parameters using the freedom we have to define each Grover factor in Eq. (2) up to an overall phase. Then we fix them as follows:

$$\alpha=\gamma=-1. \tag{14}$$

With this choice, the Grover kernel (2) takes the following form in this basis:

$$K=\frac{1}{N}\begin{pmatrix}1+\delta(1-N) & -\beta(1+\delta)\sqrt{N-1}\\ (1+\delta)\sqrt{N-1} & \beta(1+\delta-N)\end{pmatrix}. \tag{15}$$

We shall fix the initial conditions using the same initial state $|x_{\rm in}\rangle$ as in the original Grover algorithm [2], i.e., we choose the uniform state corresponding to zero momentum and find its components in the reduced basis to be

$$|x_{\rm in}\rangle=\frac{1}{\sqrt{N}}|x_0\rangle+\sqrt{\frac{N-1}{N}}|x_\perp\rangle. \tag{16}$$

In order to compute the probability amplitude in Eq. (10), we introduce the spectral decomposition of the Grover kernel K in terms of its eigenvectors $\{|\kappa_1\rangle,|\kappa_2\rangle\}$, with eigenvalues $e^{i\omega_1}, e^{i\omega_2}$. Thus we have

$$\begin{aligned}\mathcal{A}(x_0):&=\langle x_0|K^m|x_{\rm in}\rangle\\ &=\frac{1}{\sqrt{N}}\sum_{j=1}^{2}\{|\langle x_0|\kappa_j\rangle|^2\\ &\quad+\sqrt{N-1}\langle x_0|\kappa_j\rangle\langle\kappa_j|x_\perp\rangle\}e^{im\omega_j}.\end{aligned} \tag{17}$$

This, in turn, can be cast into the following closed form:

$$\langle x_0|K^m|x_{\rm in}\rangle=e^{im\omega_1}\left(\frac{1}{\sqrt{N}}+(e^{im\Delta\omega}-1)\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{\rm in}\rangle\right), \tag{18}$$

with $\Delta\omega=\omega_2-\omega_1$.

In terms of the matrix invariants

$$\mathrm{Det}\,K=\beta\delta,\quad \mathrm{Tr}\,K=-(\beta+\delta)+(1+\beta)(1+\delta)\frac{1}{N}, \tag{19}$$

the eigenvalues $\zeta_{1,2}=e^{i\omega_{1,2}}$ are given by

$$\zeta_{1,2}=(\mathrm{Tr}\,K)/2\mp\sqrt{-\mathrm{Det}\,K+(\mathrm{Tr}\,K/2)^2}. \tag{20}$$

The corresponding unnormalized eigenvectors are

$$|\kappa_{1,2}\rangle\propto\begin{pmatrix}\frac{A\mp\sqrt{-4(\mathrm{Det}\,K)N^2+A^2}}{2(1+\delta)\sqrt{N-1}}\\ 1\end{pmatrix}, \tag{21}$$

with

$$A:=(\beta-\delta)N+(1-\beta)(1+\delta). \tag{22}$$

Although we could work out all the expressions for a generic value N of elements in the list, we shall restrict our analysis to the case of a large number of elements, $N\to\infty$, and we shall leave for a numerical simulation the effect of arbitrary N. Thus, in this asymptotic limit we need to know the behavior for $N\gg 1$ of the eigenvector $|\kappa_2\rangle$, which turns out to be

$$|\kappa_2\rangle\propto\begin{pmatrix}\frac{\beta-\delta}{1+\delta}\sqrt{N}+O\left(\frac{1}{\sqrt{N}}\right)\\ 1\end{pmatrix}. \tag{23}$$

Thus, for generic values of β,δ we observe that the first component of the eigenvector dominates over the second one, meaning that asymptotically $|\kappa_2\rangle\sim|x_0\rangle$ and then $\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{\rm in}\rangle=O(1/\sqrt{N})$. This implies that the probability of success in Eq. (18) will never reach the threshold value (10). Then we are forced to tune the values of the two parameters in order to have a well-defined and nontrivial algorithm and we demand

$$\beta=\delta\neq-1. \tag{24}$$

Now the asymptotic behavior of the eigenvector changes and is given by a balanced superposition of marked and unmarked states, as follows:

$$|\kappa_2\rangle\sim\frac{1}{\sqrt{2}}\begin{pmatrix}i\,\delta^{1/2}\\ 1\end{pmatrix}. \tag{25}$$

This is normalized and we see that none of the components dominates. When we insert this expression into Eq. (18) we find

$$|\langle x_0|K^m|x_{\rm in}\rangle| \sim \frac{|\delta|}{2}|e^{im\Delta\omega}-1| \sim \left|\sin\left(\frac{m\Delta\omega}{2}\right)\right|. \quad (26)$$

This expression means that we have succeeded in finding a class of algorithms that are appropriate for solving the quantum searching problem. Now we need to find out how efficient they are. To do this let us denote by M the values of the time step m at which the probability becomes maximum; then

$$M = \lfloor |\pi/\Delta\omega| \rfloor, \quad (27)$$

where $\lfloor\ \rfloor$ denotes the ''floor'' of a number, i.e., the closest integer from below. As it happens, we are interested in the asymptotic behavior of this optimal period of time M. From Eq. (20) we find the following behavior as $N\to\infty$:

$$\Delta\omega \sim \frac{4}{\sqrt{N}}\mathrm{Re}\sqrt{\delta}. \quad (28)$$

Thus, if we parametrize $\delta = e^{i\phi}$, we finally obtain the expression

$$M \sim \left\lfloor \frac{\pi}{4\cos\dfrac{\phi}{2}}\sqrt{N} \right\rfloor \quad (29)$$

Therefore, we conclude that the Grover algorithm of the class parametrized by ϕ is a well-defined quantum searching algorithm with an efficiency of order $O(\sqrt{N})$ and with a subdominant behavior that depends on each element of the family. Within this class, the original Grover algorithm is a distinguished element for which the coefficient in Eq. (29) achieves its optimal value at $\phi = 0$. Moreover, the worst value occurs for $\phi\to\pi$; in this limit M is not well defined, and it corresponds to the trivial case where the Grover kernel is just the identity operator, $K = 1$.

The expression (29) for M can also be given another meaning regarding the stability of the Grover case $\phi = 0$. It is plain that under a small perturbation $\delta\phi$ around this value, its optimal nature is not spoiled in first-order approximation for we find a behavior which is quadratic in the perturbation, namely, $M \sim (\pi/4)[1 + 0.125(\delta\phi)^2]\sqrt{N}$. This stability considered here is with respect to perturbations in eigenvalues (or eigenvectors) in the reduced 2D subspace specified by the quantum searching problem (11). We also require these type of perturbations to hold in all iterations.

However, if we happen to choose a Grover kernel with a ϕ far from 0 we may end up with a searching algorithm for which the leading behavior order $O(\sqrt{N})$ is masqueraded by the big value of the coefficient and the time needed to achieve a succeeding probability becomes very long. For instance, we may have a Grover kernel with a behavior $M \sim 10^3\sqrt{N}$ and for a value of $N = 10^6$ it would turn out to be as efficient as a classical algorithm of order $O(N) = 10^6$. Thus,

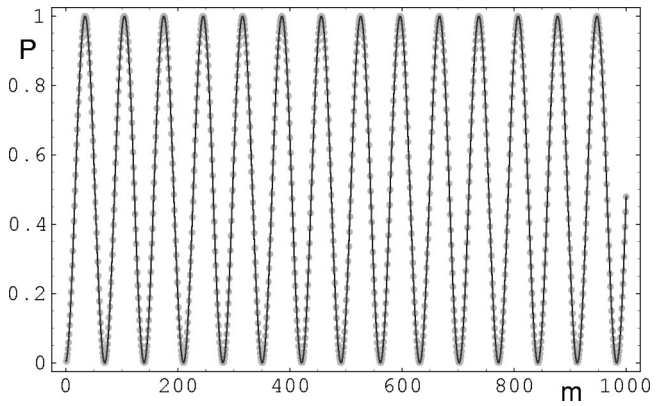

FIG. 2. Probability of success $\mathcal{P}$ as a function of the time step for $N = 1000$ and $\beta = \delta = e^{i\pi/2}$.

the limit $\phi\to\pi$ behaves as a sort of classical limit where the quantum properties disappear. In Fig. 2 we have plotted the probability of success as a function of the time step m for a list of $N = 1000$ elements and a choice of parameters $\beta = \delta = \mathrm{e}^{\mathrm{i}\pi/2}$ satisfying condition (24). We observe how the algorithm is fully efficient in achieving the maximum probability possible. Despite the fact that $\phi = \pi/2$ is not close to Grover's optimal value of 0, we find an excellent behavior. The main difference with the optimal case is that here the number of maxima is 14 while for Grover's it is 20, as implied by 29. This looks like a pattern of fully constructive interference.

In Fig. 3 we have plotted the same function but with a

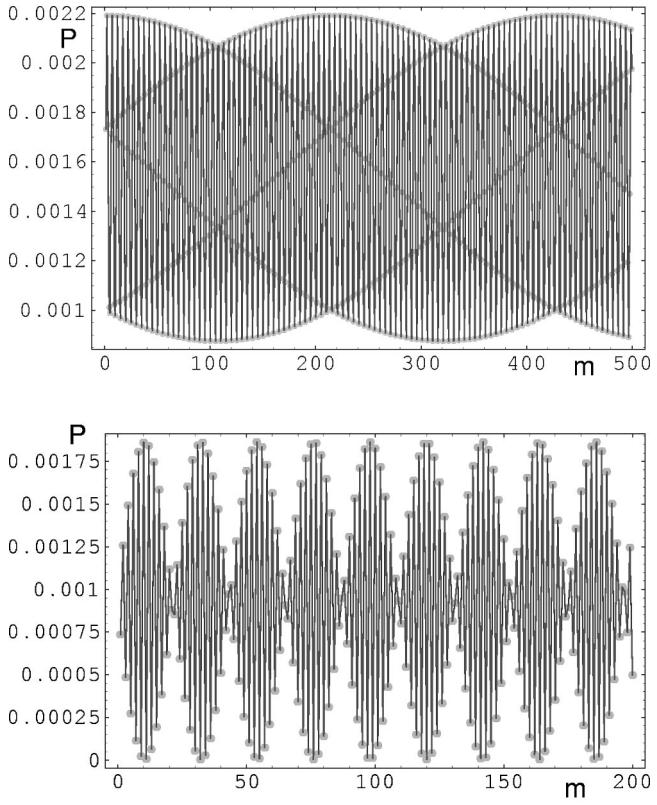

FIG. 3. Probability of success $\mathcal{P}$ as a function of the time step for $N = 1000$ and $\beta = i, \delta = ie^{i5/4}$ (up), $\beta = i, \delta = e^{i3}$ (down).

choice of parameters $\beta=i, \delta=ie^{i5/4}$ ($\beta=i, \delta=ie^{i3}$), violating condition (24). We observe how the algorithm becomes inefficient and the maximum it takes is less than 0.002 192 3 (0.001 864) for any time step. This looks like a pattern of partially constructive interference.

We find this behavior to be reminiscent of a quantum phase transition where the transition is driven by quantum fluctuations instead of standard thermal fluctuations. In this type of transition each quantum phase is characterized by a ground state which is different in each phase. It is the variation of a coupling constant in the Hamiltonian of the quantum many-body problem, which controls the occurrence of one quantum phase or another in the same manner as the temperature does in thermal transitions. In our case we may consider the two different asymptotic behaviors of the eigenvector $|\kappa_2\rangle$ as playing the role of two ground states. Following this analogy, we may see our family of algorithms parametrized by a torus $\mathcal{T}=S^1\times S^1$ where the parameters β and δ take their values and the difference $g:=\beta-\delta$ is a sort of coupling constant that governs in which of the two phases we are. When $g\neq 0$ we fall into a sort of disordered phase where the efficiency of this class of Grover's algorithms is spoiled. However, when $g=0$ we are located precisely at one equal superposition of the principle cycles of the torus which defines a one-parameter family of efficient algorithms.

B. The influence of initial conditions

Next we shall address the issue of the extent to which this one-parameter family of algorithms depends on the choice of initial conditions for the initial state $|x_{\text{in}}\rangle$. We would like to check that the stable behavior we have found is not disturbed under perturbations of initial conditions.

Let us consider a more general initial state $|x_{\text{in}}\rangle$ which is not the precise one used in the original Grover algorithm [2] but instead it is chosen as

$$|x_{\text{in}}\rangle=\frac{a}{\sqrt{N}}|x_0\rangle+b\sqrt{\frac{N-1}{N}}|x_\perp\rangle, \tag{30}$$

where a and b are chosen to satisfy a normalization condition. Then, it is possible to go over the previous analysis and find that the probability amplitude is now given by

$$\langle x_0|K^m|x_{\text{in}}\rangle=e^{im\omega_1}\left(\frac{a}{\sqrt{N}}+(e^{im\Delta\omega}-1)\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{\text{in}}\rangle\right), \tag{31}$$

where now $|x_{\text{in}}\rangle$ is the new initial state (30). We have to distinguish two cases: (i) The coefficient a of the marked state is order 1, and (ii) it is order bigger than 1, say, of order $O(\sqrt{N})$. In the latter case (ii), it means that the initial state is so peaked around the marked state that we do not even need to resort to a searching algorithm, but instead measure directly on the initial state to find the marked state successfully. Thus, we shall restrict ourselves to case (i) in the following. Now, the key point is to realize that all the previous asymptotic analyses are dominated by the behavior of the eigenvector $|\kappa_2\rangle$ given by expression (23), which is something intrinsic to the Grover kernel and independent of the initial conditions. Thus, if condition (24) is not satisfied, then as we are in case (i) the first term an the right-hand side of Eq. (31) is not relevant and we are led again to the conclusion that the algorithm is not efficient. On the contrary, if condition (24) is satisfied, the same mechanism based on Eq. (25) operates again and the algorithm has a probability of success measured by

$$|\langle x_0|K^m|x_{\text{in}}\rangle|\sim|b|\sin\left(\frac{m\Delta\omega}{2}\right), \tag{32}$$

with $\Delta\omega$ also given by Eq. (28). Then we may conclude that the class of algorithms is stable under perturbations of the initial conditions.

C. Extended formalism

Finally, we would like to check how general construction is this in terms of projection operators of the type used in Eq. (5) for $\overline{P}$. Toward this end, let us recall that $\overline{P}$ can be interpreted as the projector $|\hat{0}\rangle\langle\hat{0}|$. Thus, a natural generalization is to consider a projector on a different momentum state, say, $|\hat{y}_0\rangle$, with $y_0\neq 0$. The matrix elements of this projection operator in the coordinate basis are

$$(\overline{P})_{x,x'}=\frac{1}{N}e^{2\pi i(x'-x)y_0/N}, \quad x,x'=0,1,\ldots,N-1. \tag{33}$$

We can go even further and consider a general form for the states $|x_0\rangle,|x_\perp\rangle,|k_0\rangle$ as follows:

$$|x_0\rangle=(1,0,\ldots,0)^t,$$

$$|x_\perp\rangle=\frac{1}{\sqrt{1-\alpha_1^2}}(0,\alpha_2,\ldots,\alpha_N)^t, \tag{34}$$

$$|k_0\rangle=(\alpha_1,\alpha_2,\ldots,\alpha_N)^t,$$

where there is no loss of generality by choosing $|x_0\rangle$ in this way; $\alpha_1,\ldots,\alpha_N$ is a given and normalized set of arbitrary complex amplitudes, with $\alpha_1>0$. We will assume that $||\alpha||^2>\alpha_1^2$.

The projector $\overline{P}$ is chosen to be

$$\overline{P}=|k_0\rangle\langle k_0| \tag{35}$$

and it admits Eq. (33) as a particular case.

Now in the reduced 2D basis spanned by $\{|x_0\rangle,|x_\perp\rangle\}$ the Grover kernel has the following expression:

$$K=\begin{pmatrix}-\delta+\Delta\alpha_1^2 & -\beta\Delta\alpha_1\sqrt{1-\alpha_1^2}\\ \Delta\alpha_1\sqrt{1-\alpha_1^2} & \beta(\Delta\alpha_1^2-1)\end{pmatrix}, \tag{36}$$

with $\Delta:=1+\delta$. Thus all the dynamics depends on the relative strength of the real amplitude α_1 with respect to the rest

of the amplitudes. If we set $\alpha_i = 1/\sqrt{N}\ \forall i$, then we recover the same expression as in Eq. (15). Moreover, the initial condition is taken as

$$|x_{\rm in}\rangle = \alpha_1 |x_0\rangle + \sqrt{1-\alpha_1^2}\,|x_\perp\rangle. \tag{37}$$

In order to perform our analysis, we shall assume that the unknown amplitude α_1 behaves generically as $\alpha_1 \sim 1/\sqrt{N}$, and consequently $\sqrt{1-\alpha_1^2} \sim \sqrt{1-1/N}$. Under these circumstances, we find the following asymptotic behavior for the eigenvector $|\kappa_2\rangle$ of the Grover kernel: if $\beta \neq \delta$ and $\delta \neq -1$,

$$|\kappa_2\rangle \propto \begin{pmatrix} \dfrac{\beta-\delta}{1+\delta}\,\dfrac{1}{\alpha_1} \\ 1 \end{pmatrix}, \tag{38}$$

and if $\beta = \delta$,

$$|\kappa_2\rangle \sim \frac{1}{\sqrt{2}} \begin{pmatrix} i\,\delta^{1/2} \\ 1 \end{pmatrix}. \tag{39}$$

This latter case is again the only one favorable to obtaining an efficient algorithm and the behavior of the time M for achieving maximum probability of success takes the following form:

$$M \sim \frac{\pi \alpha_1^{-1}}{4\cos\dfrac{\phi}{2}}. \tag{40}$$

We conclude then that our construction of quantum searching algorithms of Grover's type are general enough under different choices of Grover operators G_1, G_2 and that the analysis performed with the simplest choice of these operators captures the essential properties of the class of algorithms we have presented.

IV. CONCLUSIONS

We have introduced the notion of Grover operators and Grover kernels that lead to a systematic study of Grover's quantum searching algorithms. These notions facilitate the generalization of Grover's algorithms in several directions. We have characterized the basic features of this algorithm in terms of these operators whose main properties we have established in Sec. II. Using these operators, we have investigated a family of Grover kernels whose qualities as efficient algorithms depend on the range of parameters entering the construction of their associated Grover operators. When the algorithms are efficient, they also perform the searching task with order $O(\sqrt{N})$, and the original Grover's choice gives the optimum value in the one-parameter family of algorithms. Moreover, we have extended this study to incorporate initial conditions different than the standard uniform initial states and we have checked that aside from exceptional cases, the basic algorithms of Sec. III maintain their efficiency. Finally, we have also addressed the issue of considering quite general Grover operators and found that the basic efficiency properties of the simplest choices for Grover's algorithm remain unchanged.

ACKNOWLEDGMENTS

We would like to thank J. I. Cirac and L. K. Grover for carefully reading the manuscript and suggesting references. This work was partially supported by the CICYT through Project No. AEN97-1693 (A.G.) and by the DGES through Grant No. PB97-1190 (M.A.M.-D.).

[1] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985); P. Benioff, Phys. Rev. Lett. **48**, 1581 (1982); R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); , Optics News **11**, 11 (1985); A. Yao (unpublished); P. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.

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

[3] A. Yao, in *Proceedings of the 34th Annual Symposium on the Foundations of Computer Science* (IEEE, Computer Society Technical Committee on Mathematical Foundations of Computing, Los Alamitos, CA, 1993), pp. 352–360.

[4] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998); e-print quant-ph/9605034.

[5] C. Zalka, Phys. Rev. A **60**, 2746 (1999); e-print quant-ph/9711070.

[6] D. Biron, O. Biham, E. Biham, M. Grassl, and D. A. Lidar, e-print quant-ph/9801066.

[7] O. Biham, E. Biham, D. Biron, M. Grassl, and D. A. Lidar, e-print quant-ph/9801066.

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

[9] M. Mussinger, A. Delgado, and A. Alber, e-print quant-ph/0003141.

[10] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403 (1998); e-print quant-ph/9612026.