Quantum-circuit model of Hamiltonian search algorithms

Jérémie Roland and Nicolas J. Cerf
Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, 1050 Brussels, Belgium

(Received 19 February 2003; published 15 December 2003)

We analyze three different quantum search algorithms, namely, the traditional circuit-based Grover's algorithm, its continuous-time analog by Hamiltonian evolution, and the quantum search by local adiabatic evolution. We show that these algorithms are closely related in the sense that they all perform a rotation, at a constant angular velocity, from a uniform superposition of all states to the solution state. This makes it possible to implement the two Hamiltonian-evolution algorithms on a conventional quantum circuit, while keeping the quadratic speedup of Grover's original algorithm. It also clarifies the link between the adiabatic search algorithm and Grover's algorithm.

DOI: 10.1103/PhysRevA.68.062311 PACS number(s): 03.67.Lx, 89.70.+c

I. INTRODUCTION

While the standard paradigm of quantum computation uses quantum gates (i.e., unitary operators) applied sequentially on a quantum register, recent developments have introduced a new type of quantum algorithm where the state of the quantum register evolves continuously in time under the action of some Hamiltonian. It includes, for instance, the ''analog analogue'' of Grover's algorithm [1] or the quantum algorithms by adiabatic evolution that have been intensively studied lately [2,3]. It has been shown that these Hamiltonian algorithms are genuinely quantum in the sense that they reproduce the quadratic speedup of Grover's algorithm (see, in particular, the *local* adiabatic version of Grover's algorithm [3,4]). The purpose of this paper is, on one hand, to clarify the link between these Hamiltonian algorithms and their conventional discrete equivalents, and, on the other hand, to show how they can be implemented on a traditional quantum circuit. This second issue is important because it was never shown how to do so while keeping the quadratic speedup of Grover's algorithm. It appears that all these algorithms take a very similar form in the high dimension limit, which is particularly unexpected for the case of the adiabatic search algorithm. Specifically, we see that the mixing parameter (which measures the mixing between the initial and final Hamiltonians in the adiabatic search algorithm) has to evolve in such a way that the instantaneous ground state rotates at a constant rate from the initial to the final ground state. This makes the link fully explicit with Grover's original algorithm.

II. TRADITIONAL GROVER'S ALGORITHM

First of all, let us briefly recall the principle of Grover's algorithm [5,6]. It is designed to solve the problem of finding the values x for which a function $f(x)$, usually called the ''oracle,'' is equal to 1 (while it vanishes everywhere else). As quantum gates have to be reversible, the quantum oracle must take the form

$$O_f:\mathcal{H}_N\otimes\mathcal{H}_2\rightarrow\mathcal{H}_N\otimes\mathcal{H}_2,$$

$$|x\rangle\otimes|y\rangle\mapsto|x\rangle\otimes|y\oplus f(x)\rangle, \tag{1}$$

where the N candidate solutions $|x\rangle$ are taken as the basis states of the Hilbert space $\mathcal{H}_N$, while $\oplus$ stands for the addition modulo 2. By considering the second register $\mathcal{H}_2$ as an ancilla and preparing it in the state $(1/\sqrt{2})[|0\rangle-|1\rangle]$, the application of O_f on both registers is equivalent to the following unitary operation on the first one:

$$U_f:\mathcal{H}_N\rightarrow\mathcal{H}_N,$$

$$|x\rangle\mapsto(-1)^{f(x)}|x\rangle. \tag{2}$$

To clarify the notations, we will restrict ourselves to the case where there is only one solution $x=m$ throughout this article (our results may easily be generalized to the case of M solutions, roughly speaking by replacing N with N/M in all the formulas below). In this case, $f(m)=1$ while $f(x)=0$ ($\forall\ x\neq m$) so that U_f may be rewritten as

$$U_f=I-2|m\rangle\langle m|. \tag{3}$$

Initially, we have no idea of what the solution could be, so we prepare the system in a uniform superposition of all possible solutions

$$|\sigma\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle. \tag{4}$$

This state may easily be obtained by applying a Hadamard transform H on each of the $n=\log_2 N$ qubits realizing the quantum register $\mathcal{H}_N$, initially prepared in state $|0\rangle$ (we assume here that N is an integer power of 2). The algorithm will also require the operation

$$U_0=H^{\otimes n}(I-2|0\rangle\langle 0|)H^{\otimes n}=I-2|\sigma\rangle\langle\sigma|, \tag{5}$$

which is simply the oracle operation when the solution is $m=0$, rotated in the Hadamard basis.

Let us define the operator $G=-U_0U_f$ as the Grover iteration. Throughout this article, we will always assume that $N\gg 1$ for simplicity reasons and because the link between the different versions of the algorithm will then appear more clearly. In that limit, it may be shown that the Grover iteration becomes a simple rotation of angle $2/\sqrt{N}$ in the two-dimensional subspace spanned by $|\sigma\rangle$ and $|m\rangle$. More pre-

 ©2003 The American Physical Society

cisely, successive applications of G on the initial state $|\sigma\rangle$ progressively rotate it onto the solution state $|m\rangle$:

$$|\psi_j^{\mathrm{dis}}\rangle = G^j|\sigma\rangle = \left(\cos\alpha_j^{\mathrm{dis}} - \frac{1}{\sqrt{N-1}}\sin\alpha_j^{\mathrm{dis}}\right)|\sigma\rangle + \sqrt{\frac{N}{N-1}}\sin\alpha_j^{\mathrm{dis}}|m\rangle = [\cos\alpha_j^{\mathrm{dis}} + O(N^{-1/2})]|\sigma\rangle + [\sin\alpha_j^{\mathrm{dis}} + O(N^{-1})]|m\rangle, \tag{6}$$

where

$$\alpha_j^{\mathrm{dis}} = j\left(\arcsin 2\frac{\sqrt{N-1}}{N}\right) = \frac{2j}{\sqrt{N}}[1 + O(N^{-1})]. \tag{7}$$

Thus, by applying the Grover iteration $R^{\mathrm{dis}} \approx (\pi/4)\sqrt{N}$ times, we obtain the solution state $|m\rangle$ with a probability close to 1 with a quadratic speedup with respect to a classical search, which would necessarily require a number of calls to the oracle $f(x)$ of order N.

Let us notice that as $(\pi/4)\sqrt{N}$ is generally not an integer we have to round it, for instance, to the nearest lower integer, so that $R^{\mathrm{dis}} = \lfloor(\pi/4)\sqrt{N}\rfloor$. This results in an error

$$\| |\psi_{R^{\mathrm{dis}}}^{\mathrm{dis}}\rangle - |m\rangle \| < \sin\frac{2}{\sqrt{N}} \in O(N^{-1/2}), \tag{8}$$

which tends to zero for $N \to \infty$.

III. HAMILTONIAN VERSION OF THE ORACLE

In the two Hamiltonian-evolution quantum search algorithms discussed below, we will need the Hamiltonian

$$H_f = I - |m\rangle\langle m|. \tag{9}$$

Let us show why it can be considered as equivalent to the oracle U_f. If we apply this Hamiltonian on a basis state $|x\rangle$ during a time t, it yields

$$e^{-iH_f t}|x\rangle = \begin{cases} |x\rangle, & x = m, \\ e^{-it}|x\rangle & \forall\ x \neq m, \end{cases} = e^{-i(1-f(x))t}|x\rangle. \tag{10}$$

We immediately see that by taking $t = \pi$ we reproduce the operation $-U_f$, that is,

$$e^{-iH_f\pi} = -U_f. \tag{11}$$

Conversely, it is possible to simulate the application of H_f during a time t with a quantum circuit using a one-qubit ancilla prepared in state $|0\rangle$, two calls to the oracle O_f, and an additional phase gate

$$U_t = e^{-it}|0\rangle\langle 0| + |1\rangle\langle 1|. \tag{12}$$

Considering the circuit represented in Fig. 1, we have

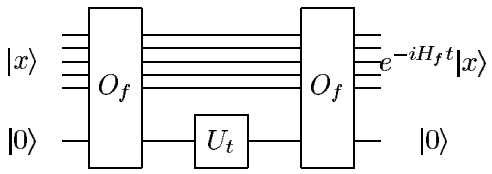

FIG. 1. Circuit for implementing the evolution of a Hamiltonian H_f during a time t by using twice the corresponding oracle O_f.

$$\begin{aligned} O_f[|x\rangle\otimes|0\rangle] &= |x\rangle\otimes|f(x)\rangle, \\ I\otimes U_t[|x\rangle\otimes|f(x)\rangle] &= e^{-i(1-f(x))t}|x\rangle\otimes|f(x)\rangle, \\ O_f[e^{-i(1-f(x))t}|x\rangle\otimes|f(x)\rangle] &= e^{-i(1-f(x))t}|x\rangle\otimes|0\rangle, \\ &= e^{-itH_f}|x\rangle\otimes|0\rangle, \end{aligned} \tag{13}$$

which indeed coincides with the result of evolving $|x\rangle$ with H_f during time t.

IV. ANALOG QUANTUM SEARCH

Let us now consider the "analog" algorithm introduced by Farhi *et al.* in [1]. In addition to the oracle Hamiltonian H_f, we will need a second Hamiltonian

$$H_0 = H^{\otimes n}(I - |0\rangle\langle 0|)H^{\otimes n} = I - |\sigma\rangle\langle\sigma|, \tag{14}$$

which is related to U_0 as defined in Eq. (5) in the same way as H_f is related to U_f. The algorithm consists in preparing the system in the starting state $|\psi^{\mathrm{an}}(t=0)\rangle = |\sigma\rangle$ and then let it evolve under the time-independent Hamiltonian $H^{\mathrm{an}} = H_0 + H_f$. A simple calculation shows that

$$|\psi^{\mathrm{an}}(t)\rangle = e^{-itH^{\mathrm{an}}}|\sigma\rangle = e^{-it}\left[\cos\frac{t}{\sqrt{N}}|\sigma\rangle + i\sin\frac{t}{\sqrt{N}}|m\rangle\right] = e^{-it}[\cos\alpha^{\mathrm{an}}(t)|\sigma\rangle + i\sin\alpha^{\mathrm{an}}(t)|m\rangle], \tag{15}$$

where

$$\alpha^{\mathrm{an}}(t) = \frac{t}{\sqrt{N}}. \tag{16}$$

Thus, the quantum search simply works via a rotation from $|\sigma\rangle$ to $|m\rangle$, just as in the traditional algorithm. However, here the rotation is continuous and follows a different path because of the presence of i in the second term of Eq. (15). The solution state is thus obtained with probability 1 if we apply H^{an} during a time $T^{\mathrm{an}} = (\pi/2)\sqrt{N}$. Let us also notice that

$$\alpha^{\mathrm{an}}(2j) = \alpha_j^{\mathrm{dis}}[1 + O(N^{-1})], \tag{17}$$

which shows that the application of H^{an} during a time $T^{\mathrm{an}}/R^{\mathrm{dis}} = 2$ corresponds roughly to one Grover iteration.

Suppose now that we want to implement this analog algorithm on a quantum circuit. We showed in the previous section how to reproduce the application of H_f with a circuit,

but this does not allow us to directly apply $H^{\mathrm{an}}=H_0+H_f$. In order to achieve this, we need to cut the evolution time T^{an} into R^{an} small intervals $\Delta T=T^{\mathrm{an}}/R^{\mathrm{an}}=(\pi/2)\sqrt{N}/R^{\mathrm{an}}$ such that we may approximate

$$U(\Delta T)=e^{-i(H_0+H_f)\Delta T} \tag{18}$$

by

$$U'_{\Delta T}=e^{-iH_0\Delta T}e^{-iH_f\Delta T}. \tag{19}$$

Using the Campbell-Baker-Hausdorff approximation, which states that $|||e^{A+B}-e^Ae^B|||_2\in O(|||[A,B]|||_2)$ with $|||A|||_2=\max_{|x\rangle:\||x\rangle\|=1}\|A|x\rangle\|$ denoting the operator norm of A, we have

$$|||U(\Delta T)-U'_{\Delta T}|||_2\in O(|||[H_0,H_f]|||_2\Delta T^2). \tag{20}$$

Since

$$|||[H_0,H_f]|||_2=\sqrt{\frac{1}{N}}\sqrt{1-\frac{1}{N}}\in O\left(\frac{1}{\sqrt{N}}\right), \tag{21}$$

the error introduced in each step is

$$|||U(\Delta T)-U'_{\Delta T}|||_2\in O\left(\frac{\sqrt{N}}{(R^{\mathrm{an}})^2}\right). \tag{22}$$

Since there are R^{an} successive steps, the total error made by this discretized version of the analog algorithm is

$$|||U(T^{\mathrm{an}})-(U'_{\Delta T})^{R^{\mathrm{an}}}|||_2\in O\left(\frac{\sqrt{N}}{R^{\mathrm{an}}}\right). \tag{23}$$

This simply results from the property that if the condition $|||U_j-U'_j|||_2\ll 1$ is satisfied $\forall\ j$, then

$$\left|\left|\left|\prod_j U_j-\prod_j U'_j\right|\right|\right|_2\leqslant\sum_j |||U_j-U'_j|||_2. \tag{24}$$

We thus observe that for a number of steps $R^{\mathrm{an}}=\lfloor\sqrt{N}/\epsilon\rfloor$ (of the same order in N as in Grover's algorithm), we get the solution state with an error of order ϵ.

Furthermore, using the result of the previous section, we see that each step has the same form $e^{-iH_0\Delta T}e^{-iH_f\Delta T}$ as a Grover iteration $G=-U_0U_f$ and therefore requires two calls to the oracle O_f if it is implemented on a quantum circuit.

V. QUANTUM SEARCH BY LOCAL ADIABATIC EVOLUTION

For this third algorithm, exposed in [3] and [4], we once more need the Hamiltonians H_0 and H_f, and initially prepare our system in a uniform superposition of all possible solutions $|\psi^{\mathrm{ad}}(t=0)\rangle=|\sigma\rangle$. This time, however, we apply a time-dependent Hamiltonian

$$\tilde{H}(s)=(1-s)H_0+sH_f, \tag{25}$$

where the mixing parameter $s=s(t)$ is a monotonic function with $s(0)=0$ and $s(T^{\mathrm{ad}})=1$. As $|\sigma\rangle$ is the ground state of $\tilde{H}(0)=H_0$, the adiabatic theorem [7] tells us that the system will stay near the instantaneous ground state of $\tilde{H}(s)$ as long as the evolution of $\tilde{H}(s)$ imposed by $s(t)$ is "slow enough." If this condition is satisfied, the system will thus end up in the ground state of $\tilde{H}(1)=H_f$, which is the solution state $|m\rangle$. Let us recall that, following [4], we use the term *local* adiabatic evolution when the evolution rate is optimized at each time, whereas for a *global* adiabatic evolution the adiabatic condition is applied globally on the whole time interval, using a linear $s(t)$.

Let us first study the path followed by $|\psi^{\mathrm{ad}}(t)\rangle$ during the time evolution. As $\tilde{H}(s)$ acts only on the subspace spanned by $|\sigma\rangle$ and $|m\rangle$ and, as we start from $|\sigma\rangle$, the path followed by $|\psi^{\mathrm{ad}}(t)\rangle$ will remain in this subspace so that the problem may again be studied in this two-dimensional space. By calculating the eigenstates of $\tilde{H}(s)$, we find

$$|E_0;s\rangle=\frac{\sqrt{N}[E_1(s)-s]|\sigma\rangle+s|m\rangle}{\sqrt{E_1(s)^2+(N-1)[E_1(s)-s]^2}}, \tag{26}$$

$$|E_1;s\rangle=\frac{\sqrt{N}[E_0(s)-s]|\sigma\rangle+s|m\rangle}{\sqrt{E_0(s)^2+(N-1)[E_0(s)-s]^2}}, \tag{27}$$

where

$$E_0(s)=\frac{1}{2}\left[1-\sqrt{1-4\frac{N-1}{N}s(1-s)}\right], \tag{28}$$

$$E_1(s)=\frac{1}{2}\left[1+\sqrt{1-4\frac{N-1}{N}s(1-s)}\right]. \tag{29}$$

The adiabatic theorem states that if the adiabatic condition is obeyed *locally* (see [4] for details), that is, if

$$\frac{ds}{dt}\leqslant\epsilon g^2(t)\quad\forall\ t\in[0,T^{\mathrm{ad}}], \tag{30}$$

where $g(t)=E_1[s(t)]-E_0[s(t)]$ is the gap between the two eigenvalues, then we have

$$|\psi^{\mathrm{ad}}(s)\rangle=\sqrt{1-\eta^2(s)}|E_0;s\rangle+\eta(s)e^{i\phi(s)}|E_1;s\rangle, \tag{31}$$

where $\eta^2(s)\leqslant\epsilon^2$ is the error probability and $\phi(s)$ is a relative phase appearing during the evolution. Note that, here and throughout the rest of the paper, we omit an irrelevant global phase in front of $|\psi^{\mathrm{ad}}(s)\rangle$, assuming that the phase has been modified such that the amplitude of the first term is real. As expected, $|\psi^{\mathrm{ad}}(s)\rangle$ stays close to the ground state $|E_0;s\rangle$, which may be rewritten as

$$\begin{aligned}|E_0;s\rangle=&[\cos\alpha^{\mathrm{ad}}(s)+O(N^{-1/2})]|\sigma\rangle\\&+[\sin\alpha^{\mathrm{ad}}(s)+O(N^{-1})]|m\rangle\end{aligned} \tag{32}$$

with

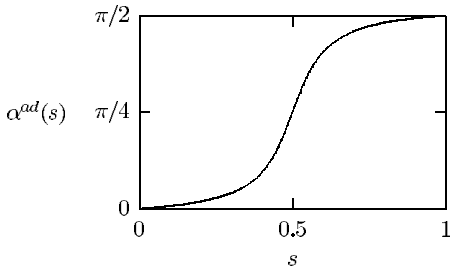

FIG. 2. Rotation angle $\alpha^{\mathrm{ad}}(s)$ for the adiabatic quantum search algorithm with $N=32$.

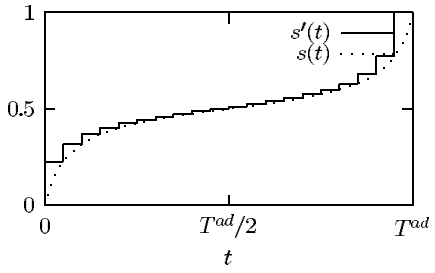

FIG. 3. $s(t)$ and its discrete approximation $s'(t)$ (using $R^{\mathrm{ad}}=20$ steps) for the local adiabatic algorithm with $N=32$.

$$\alpha^{\mathrm{ad}}(s)=\frac{1}{2}\arctan\left[\frac{2\sqrt{N-1}s}{N-2(N-1)s}\right] \tag{33}$$

$$=\frac{1}{2}\arctan\left[\frac{2s}{\sqrt{N}(1-2s)}[1+O(N^{-1})]\right] \tag{34}$$

in analogy to Eq. (6).

The function $\alpha^{\mathrm{ad}}(s)$ is plotted in Fig. 2. We see that the evolution is once again a rotation from $|\sigma\rangle$ to $|m\rangle$, but it is *not* performed at a constant angular velocity if $s(t)$ is chosen to be linear in t, which corresponds to the quantum search by *global* adiabatic evolution originally described in [2]. The observed angular velocity is indeed greater for s close to 1/2 while it is smaller at the beginning and the end of the time evolution. Let us also notice that at discrete values $s(t)=s_k$, the continuous path $|\psi^{\mathrm{ad}}(s)\rangle$ coincides with the states $|\psi_j^{\mathrm{dis}}\rangle$ of Grover's traditional algorithm. Thus, in the global adiabatic search algorithm, the system exactly follows the path of Grover's algorithm, but at a varying rate. This suggests that this algorithm is not the correct adiabatic equivalent to Grover's algorithm. Moreover, we note that if $s(t)=t/T^{\mathrm{ad}}$, then the adiabatic theorem imposes that $T^{\mathrm{ad}}\in\Omega(N)$, so that we lose the quadratic speedup of Grover's algorithm (see [4]).

In order to circumvent this problem, we must perform a *local* adiabatic evolution according to Eq. (30), as shown in [4]. Then, we get the solution state with an error probability less than ϵ^2

$$\|\,|\psi^{\mathrm{ad}}(T^{\mathrm{ad}})\rangle-|m\rangle\|^2\leqslant\epsilon^2, \tag{35}$$

provided that we evolve at a rate such that

$$t(s)=\frac{N}{2\epsilon\sqrt{N-1}}\{\arctan[\sqrt{N-1}(2s-1)]+\arctan\sqrt{N-1}\}$$

$$=\frac{N}{2\epsilon\sqrt{N-1}}\arctan\left[\frac{2\sqrt{N-1}s}{N-2(N-1)s}\right]$$

$$=\frac{\sqrt{N}}{2\epsilon}\arctan\left[\frac{2s}{\sqrt{N}(1-2s)}[1+O(N^{-1})]\right] \tag{36}$$

in the limit $N\gg 1$. Thus, for a local adiabatic evolution,

$$\alpha^{\mathrm{ad}}(t)=\frac{\epsilon\sqrt{N-1}t}{N} \tag{37}$$

$$=\frac{\epsilon t}{\sqrt{N}}[1+O(N^{-1})]. \tag{38}$$

This is now a rotation at a constant rate, which yields the solution state after a time $T^{\mathrm{ad}}=(\pi/2\epsilon)\sqrt{N}$, so that we may consider this local adiabatic evolution as the proper equivalent to Grover's algorithm.

Let us study the implementation of this algorithm on a quantum circuit (we will closely follow the lines of the development exposed in [3]). As for the analog quantum search, we discretize the evolution by cutting the time T^{ad} into R^{ad} intervals $\Delta T=T^{\mathrm{ad}}/R^{\mathrm{ad}}$. During each interval $[t_{j-1},t_j]$ $(t_j=j\Delta T)$, we approximate the varying Hamiltonian $\tilde{H}(s(t))$ by the constant one $H_j=(1-s_j)H_0+s_jH_f$ $[s_j=s(t_j)]$, which is equivalent to replacing the actual Hamiltonian $H(t)=\tilde{H}(s(t))$ by $H'(t)=\tilde{H}(s'(t))$ where $s'(t)$ is a monotonic function approaching $s(t)$ but varying at times t_j only (see Fig. 3)

In order to evaluate the error introduced by this approximation, we will use a straightforward generalization of a lemma introduced in [3]. Considering two time-dependent Hamiltonians $H(t)$ and $H'(t)$ such that $|||H(t)-H'(t)|||_2\leqslant\delta(t)$ for $0\leqslant t\leqslant T$, the goal will be to find an upper bound on the distance between the unitaries induced by them. The difference with the lemma in [3] is that here the Hamiltonian difference $\delta(t)$ may vary in time. This will be crucial in order to keep the quadratic speedup of Grover's search after this discretization procedure (this is reminiscent to the distinction between the global and the local adiabatic evolution). Let $|\psi(t)\rangle$ and $|\psi'(t)\rangle$ be the trajectories induced by $H(t)$ and $H'(t)$ starting from a common initial state $|\psi(0)\rangle=|\psi'(0)\rangle=|\psi_0\rangle$. We have

$$\frac{d}{dt}\langle\psi(t)|\psi'(t)\rangle=-i\langle\psi(t)|H(t)-H'(t)|\psi'(t)\rangle \tag{39}$$

and

TABLE I. Summary of the properties of the three quantum search algorithms. Here $\delta t_{0,j}$ and $\delta t_{f,j}$ are the times during which H_0 and H_f have to be applied in step j. Notice that we have omitted some irrelevant global phases in front of $|\psi_j\rangle$ and $|\psi_R\rangle$

	Grover	Analog	Adiabatic
No. of steps R	$\lfloor(\pi/4)\sqrt{N}\rfloor$	$\lfloor\sqrt{N}/\epsilon\rfloor$	$\lfloor\sqrt{N}/\epsilon^3\rfloor$
Step j	$\delta t_{0,j}=\delta t_{f,j}=\pi$	$\delta t_{0,j}=\delta t_{f,j}=\epsilon\pi/2$	$\begin{cases}\delta t_{0,j}=(1-s_j)\epsilon^2\pi/2\\ \delta t_{f,j}=s_j\epsilon^2\pi/2\end{cases}$
State $\lvert\psi_j\rangle$	$\cos\alpha_j\lvert\sigma\rangle+\sin\alpha_j\lvert m\rangle$	$\cos\alpha_j\lvert\sigma\rangle+i\sin\alpha_j\lvert m\rangle$	$\cos\alpha_j\lvert\sigma\rangle+\sin\alpha_j\lvert m\rangle$
Angle α_j	$2j/\sqrt{N}$	$(\epsilon j/\sqrt{N})\pi/2$	$(\epsilon^3 j/\sqrt{N})\pi/2$
Error $\|\lvert\psi_R\rangle-\lvert m\rangle\|$	$O(1/\sqrt{N})$	$O(\epsilon)$	$O(\epsilon)$

$$\left|\frac{d}{dt}|\langle\psi(t)|\psi'(t)\rangle|^2\right|\leqslant 2|\langle\psi(t)|H(t)-H'(t)|\psi'(t)\rangle| \tag{40}$$

$$\leqslant 2\,\delta(t), \tag{41}$$

which gives after integration, with the initial condition $\langle\psi(0)|\psi'(0)\rangle=1$,

$$|\langle\psi(T)|\psi'(T)\rangle|^2\geqslant 1-2\int_0^T\delta(t)dt. \tag{42}$$

Introducing the unitary evolutions $U(T)$ and $U'(T)$ induced by the application of these Hamiltonians from $t=0$ to $t=T$, this last equation may be rewritten

$$\|U(T)|\psi_0\rangle-U'(T)|\psi_0\rangle\|\leqslant\sqrt{2\int_0^T\delta(t)dt}. \tag{43}$$

As $|\psi_0\rangle$ is arbitrary, we find the following upper bound on the error introduced by replacing $H(t)$ by $H'(t)$:

$$|||U(T)-U'(T)|||_2\leqslant\sqrt{2\int_0^T\delta(t)dt}. \tag{44}$$

This concludes the generalization of the lemma in [3].

In our problem, the approximation of $H(t)$ by $H'(t)$ is such that

$$\begin{aligned}|||H(t)-H'(t)|||_2&=|||\tilde{H}(s(t))-\tilde{H}(s'(t))|||_2\\&=|s'(t)-s(t)|\,|||H_0-H_f|||_2\\&\leqslant|s(t+\Delta T)-s(t)|\,|||H_0-H_f|||_2\\&\leqslant|s(t+\Delta T)-s(t)|,\end{aligned} \tag{45}$$

where we have assumed that $s(t)=1$ for $t>T^{\mathrm{ad}}$ and used the fact that

$$|||H_0-H_f|||_2=|||\,|m\rangle\langle m|-|\sigma\rangle\langle\sigma|\,|||_2=\sqrt{1-\frac{1}{N}}\leqslant 1. \tag{46}$$

We may now use Eq. (44) with $\delta(t)=s(t+\Delta T)-s(t)$, and

$$\begin{aligned}\int_0^{T^{\mathrm{ad}}}\delta(t)dt&=\int_0^{T^{\mathrm{ad}}}[s(t+\Delta T)-s(t)]dt\\&=\Delta T-\int_0^{\Delta T}s(t)dt\leqslant\Delta T.\end{aligned} \tag{47}$$

Finally, we get

$$|||U(T^{\mathrm{ad}})-U'(T^{\mathrm{ad}})|||_2\leqslant\sqrt{2\Delta T}=\sqrt{2\frac{T^{\mathrm{ad}}}{R^{\mathrm{ad}}}}, \tag{48}$$

so that in order to keep an error of constant order ϵ for growing N, we must choose a number of steps proportional to T^{ad}, that is, $R^{\mathrm{ad}}=\lfloor\sqrt{N}/\epsilon^3\rfloor$.

For each step, we have to apply H_j during a time $\Delta T=T^{\mathrm{ad}}/R^{\mathrm{ad}}$, that is, the unitary operation

$$U_j'=e^{-iH_j\Delta T}=e^{-i(1-s_j)H_0\Delta T-is_jH_f\Delta T}. \tag{49}$$

As for the analog algorithm, we use the Campbell-Baker-Hausdorff approximation and replace U_j' by

$$U_j''=e^{-i(1-s_j)H_0\Delta T}e^{-is_jH_f\Delta T}. \tag{50}$$

The error introduced at each step by this approximation will be

$$|||U_j'-U_j''|||_2\in O(s_j(1-s_j)\Delta T^2|||[H_0,H_f]|||_2) \tag{51}$$

$$\in O\left(s_j(1-s_j)\frac{\sqrt{N}}{(\epsilon R^{\mathrm{ad}})^2}\right). \tag{52}$$

For the R^{ad} steps we have $U'(T^{\mathrm{ad}})=\Pi_jU_j'$, so that using Eq. (24) gives

$$|||U'(T^{\mathrm{ad}})-\prod_j U_j''|||_2\in O\left(\frac{\sqrt{N}}{\epsilon^2R^{\mathrm{ad}}}\right). \tag{53}$$

Consequently, the number of steps $R^{\mathrm{ad}}=\lfloor\sqrt{N}/\epsilon^3\rfloor$ required in the previous approximation [i.e., replacing $H(t)$ by $H'(t)$] results in an error of order ϵ.

VI. CONCLUSION

We have shown that, in spite of their different original formulations, the three quantum search algorithms that have been found so far are very closely related. They all perform a rotation from the uniform superposition of all states to the solution state at a constant angular velocity, even though a slightly different path is followed by the analog quantum search algorithm. Their similarities become even more obvious when they are implemented on a quantum circuit as they all require a number of steps of order $\sqrt{N}$, each step having the same form $e^{-iH_0\delta t_0}e^{-iH_f\delta t_f}$. Note that the ''duty cycle'' $\delta t_f/(\delta t_0+\delta t_f)$ varies along the evolution according to a specific law in the case of the local adiabatic search algorithm, while it is 50% for the traditional Grover's algorithm as well as its Hamiltonian analog. Finally, we have shown how one can realize these basic steps on a quantum circuit by using two calls to the quantum oracle. This will be helpful to use these algorithms as building blocks to solve more advanced structured search problems (see [8]). These results are summarized in Table I.

ACKNOWLEDGMENTS

J.R. acknowledges financial support from the Belgian FRIA foundation. We also acknowledge funding from the European Union under the project RESQ (Grant No. IST-2001-37599) in the IST-FET-QIPC program, from the Communauté Française de Belgique under the ''Action de Recherche Concertée'' Grant No. 00/05-251, and from the IAP program of the Belgian federal government under Grant No. V-18.

[1] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403 (1998).
[2] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, e-print quant-ph/0001106.
[3] W. van Dam, M. Mosca, and U. Vazirani, in *Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, New York, 2001), pp. 279–287.
[4] J. Roland and N.J. Cerf, Phys. Rev. A **65**, 042308 (2002).
[5] L.K. Grover, in *Proceedings of the 28th Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996), pp. 212–219.
[6] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[7] L.I. Schiff, *Quantum Mechanics* (McGraw-Hill, Singapore, 1955).
[8] J. Roland and N.J. Cerf, following paper, Phys. Rev. A **68**, 062312 (2003).