Adiabatic quantum oracles

2004 J. Phys. A: Math. Gen. 37 L421

(http://iopscience.iop.org/0305-4470/37/34/L01)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **37** (2004) L421–L427 PII: S0305-4470(04)82207-8

LETTER TO THE EDITOR

Adiabatic quantum oracles

M Andrecut and M K Ali

Department of Physics, University of Lethbridge, Lethbridge, AB, T1K 3M4, Canada

E-mail: mircea.andrecut@uleth.ca and ali@uleth.ca

Received 16 June 2004
Published 11 August 2004
Online at stacks.iop.org/JPhysA/37/L421
doi:10.1088/0305-4470/37/34/L01

Abstract
In this letter we discuss the adiabatic quantum implementation of some well-known standard quantum oracles.

PACS numbers: 03.67.Lx, 89.70.+c

1. Introduction

Usually, for quantum computational purposes, a Boolean function

$$f(x) : \{0, 1\}^n \to \{0, 1\} \tag{1}$$

is considered a 'black box' and its implementation is often neglected [1]. A convenient way of computing this function in the standard quantum approach is to consider a two qubit computer which starts in the state $|x, y\rangle$. It can be shown that with an appropriate sequence of logic gates it is possible to transform this state into $|x, y \oplus f(x)\rangle$, where $\oplus$ indicates addition modulo 2. If $y = 0$, then the final state of the second qubit is just the value $f(x)$. In general, it can be shown that given a classical circuit for computing f there is a quantum circuit of comparable efficiency which computes (in polynomial time) the unitary transformation

$$|x, y\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle, \tag{2}$$

on a quantum computer [1].

What makes quantum Boolean function evaluation really interesting is its action on a superposition of different inputs x. For example, quantum parallel evaluation of f, produces $f(x)$ for all x in a single run. However, this parallelism is not immediately useful since the measurement of the state $\sum_x |x, f(x)\rangle$ would give only $f(x)$ for a single value of x.

Here, we give a theorem which shows that any Boolean function can be computed using the adiabatic quantum method. Also, we discuss the adiabatic quantum implementation of some well-known standard quantum oracles.

2. The adiabatic theorem

The adiabatic quantum computation method uses the language of ground states, spectral gaps and Hamiltonians, instead of the standard unitary transformation language. In the adiabatic quantum computation model, a computational procedure is described by the continuous time evolution of a time dependent Hamiltonian $\widehat{H}(t)$ [2–4]. To state the adiabatic theorem, it is convenient and traditional to work with a re-scaled time $s = t/T$ where T is the total time (or *delay schedule*). For the sake of simplicity we shall suppose the spectrum of $\widehat{H}(s)$ to be entirely discrete. Also, we assume that the quantum system corresponds to a set of n qubits. In addition we suppose that:

1. the eigenvalues $E_j(s)$ and the associated eigenstates $|\xi_j(s)\rangle$, $j = 0, \ldots, N$, of $\widehat{H}(s)$ are continuous and derivable functions of $s \in (0, 1)$;
2. the eigenvalues of $\widehat{H}(s)$ remain distinct throughout the transition period $s \in (0, 1)$: $E_0(s) < E_1(s) < \cdots < E_N(s)$.

We say that $|\xi_0(s)\rangle$ is the groundstate, $|\xi_1(s)\rangle$ is the first excited state and $|\xi_N(s)\rangle$ is the Nth excited state of the system ($N = 2^n - 1$). The Hamiltonian of the system is therefore given by:

$$\widehat{H}(s) = \sum_{j=0}^{N} E_j(s)\widehat{P}_j(s), \tag{3}$$

where $\widehat{P}_j(s) = |\xi_j(s)\rangle\langle\xi_j(s)|$ is the projector onto the subspace of $E_j(s)$. The Hamiltonian evolution from $\widehat{H}(0)$ to $\widehat{H}(1)$ induces the unitary transformation $\widehat{U}_T$ (the evolution operator). The adiabatic theorem states that $\widehat{U}_T(s)$ has the following asymptotic property:

$$\lim_{T\to\infty} \widehat{U}_T(s)\widehat{P}_j(0) = \widehat{P}_j(s) \lim_{T\to\infty} \widehat{U}_T(s), \qquad j = 0, \ldots, N. \tag{4}$$

Thus, if $|j\rangle = |\xi_j(0)\rangle$ is an eigenvector of $\widehat{H}(0)$ belonging to the eigenvalue $E_j(s)$, then the vector $\widehat{U}_T(s)\widehat{P}_j(0)\,|j\rangle = \widehat{U}_T(s)\,|j\rangle$ tends toward a vector of the subspace of $E_j(s)$ when $T \to \infty$ [5, 6].

It is useful to estimate the minimum delay schedule T, that it takes for this evolution to be adiabatic [7]. The crucial quantities for this transformation to be adiabatic are the minimum gap between the eigenstates

$$\delta_{\min} = \min_{j\neq k} \min_{0\leqslant s\leqslant 1} [E_j(s) - E_k(s)], \tag{5}$$

and the maximum rate at which the Hamiltonian can be modified

$$\Delta_{\max} = \max_{s\in[0,1]} \left\| \frac{\mathrm{d}}{\mathrm{d}s}\widehat{H}(s) \right\|_2. \tag{6}$$

It can be shown that a minimum delay schedule T with

$$T = \frac{\Delta_{\max}}{\varepsilon\delta_{\min}^2}, \tag{7}$$

where $0 < \varepsilon \ll 1$, is sufficiently slow for the adiabatic evolution from $\widehat{H}(0)$ to $\widehat{H}(1)$.

3. Boolean functions

Theorem. *Given a n-bit Boolean function,*

$$f(x) : \{0, 1\}^n \to \{0, 1\}, \tag{8}$$

there exists an adiabatic Hamiltonian

$$\widehat{H}(s) = \sum_{x=0}^{2^n-1} \widehat{H}_x(s), \tag{9}$$

$s \in [0, 1]$, *such that the superposition*

$$|\psi(0)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), \tag{10}$$

can be transformed adiabatically into

$$|\psi(1)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), \tag{11}$$

($\oplus$ is the modulo 2 addition) with a minimum delay schedule of

$$T = 4\varepsilon^{-1}, \tag{12}$$

where $0 < \varepsilon \ll 1$.

Proof. Let us consider the following Hamiltonians:

$$\widehat{H}_x(s) = (1-s)\widehat{H}_{0x} + s\widehat{H}_{1x} + s(1-s)\widehat{H}_{01x}, \tag{13}$$

$$\widehat{H}_{0x} = E_x^0 \, |x, 0\rangle \, \langle x, 0| + E_x^1 \, |x, 1\rangle \, \langle x, 1| \, , \tag{14}$$

$$\widehat{H}_{1x} = \big[(1 - f(x))E_x^0 + f(x)E_x^1\big]|x, 0\rangle\langle x, 0| + \big[f(x)E_x^0 + (1 - f(x))E_x^1\big]|x, 1\rangle\langle x, 1|, \tag{15}$$

$$\widehat{H}_{01x} = f(x)\big(E_x^1 - E_x^0\big)(|x, 0\rangle\langle x, 1| + |x, 1\rangle\langle x, 0|). \tag{16}$$

The computation is done by switching between the eigenstates $|x, 0\rangle$ and $|x, 1\rangle$ corresponding to the eigenvalues E_x^0 and E_x^1 respectively. The switching depends on the values of the Boolean function f. The intermediate Hamiltonian $\widehat{H}_{01x}$ makes sure that this switching is done without crossing the eigenvalues during the adiabatic evolution. Thus we have:

$$\begin{aligned} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) &\xrightarrow{\widehat{H}_x(s)} |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) \\ &= |x\rangle \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} \right) = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \end{aligned} \tag{17}$$

Now, let us calculate the minimum delay schedule. Assuming that

$$E_0^0 = 0, \, E_0^1 = 1, \, E_1^0 = 2, \ldots, \, E_{2^n-1}^0 = 2^{n+1} - 2, \, E_{2^n-1}^1 = 2^{n+1} - 1, \tag{18}$$

we obtain the following eigenvalues:

$$E_x^{0,1}(s) = \frac{E_x^0 + E_x^1}{2} \mp \frac{1}{2}\sqrt{1 - 4f(x)s + 4f(x)s^2(1 - 2s + s^2)}. \tag{19}$$

Thus, the gaps are:

$$\delta_x^{0,1}(1/2) = \big|E_x^0(1/2) - E_x^1(1/2)\big| = \sqrt{1 - \frac{3}{4}f(x)} > 0. \tag{20}$$

For $f(x) = 1, \forall x \in \{0, 1\}^n$, we have $\delta_{\min} = 1/2$. Also, it can be easily shown that the matrix elements are

$$\Delta_{x,y}^{i,j} = \begin{cases} 1, & x = y, i \neq j \\ 0, & x \neq y, \end{cases} \tag{21}$$

where $x, y \in \{0, 1, \ldots, 2^n - 1\}$ and $i, j \in \{0, 1\}$. Thus, the minimum delay schedule for the adiabatic computation of the n-bit Boolean function f is $T = 4\varepsilon^{-1}$. □

4. Adiabatic quantum oracles

Oracles are devices, which are used to answer questions with a simple *yes* or *no*. The oracles we are going to study are:

- The Deutsch oracle. This oracle answers the following question. Suppose we have a function $f(x) : \{0, 1\} \to \{0, 1\}$, which can be either constant $f(0) = f(1)$, or balanced $f(0) \neq f(1)$. Classically it would take two evaluations of the function to tell whether it is one or the other. Using the standard quantum method, we can answer this question in one evaluation. The reason for this is that we can create a superposition of all the values of x at the same time and evaluate the function f in parallel.
- The Deutsch–Josza oracle. This oracle generalizes the Deutsch oracle to a function $f(x) : \{0, 1\}^n \to \{0, 1\}$. We ask the same question: is the function constant or balanced? Here balanced means that the function is 0 on half of its arguments and 1 on the other half. Of course in this case the function may be neither constant nor balanced. In this case the oracle doesn't work: it may say yes or no and the answer will be meaningless. In the worst classical case, the best deterministic algorithm needs to query the function f at least $2^{n-1} + 1$ times, in order to solve the problem. Using the standard quantum method, we can answer this question in one evaluation. The reason for this is that we can create a superposition of all the values of x at the same time and evaluate the function f in parallel.
- The Bernstein–Vazirani oracle. Suppose you have a function $f(x) : \{0, 1\}^n \to \{0, 1\}$ of the form $f(x) = a \cdot x$ where $a \in \{0, 1\}^n$ is a constant vector and $a \cdot x$ is the bitwise inner product of a and x, modulo 2. How many measurements are required to find a? Classically one has to perform measurements for all possible arguments and then solve a system of linear equations for a. Using the standard quantum method, a is delivered in one computational step.

4.1. The adiabatic Deutsch oracle

The first step, in the standard quantum algorithm implementation of the Deutsch oracle, is to apply the Hadamard gate, W, to the initial state

$$|\varphi_0\rangle = |0\rangle|1\rangle, \tag{22}$$

to obtain the state

$$|\varphi_0\rangle \xrightarrow{\widehat{H}_W^{\otimes 2}(s)} |\varphi_1\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle). \tag{23}$$

Recently, we have shown that the Hadamard gate can be implemented in the framework of the adiabatic quantum computation method using the following Hamiltonian [8]:

$$\widehat{H}_W(s) = (1 - s)\widehat{H}_{W,0} + s\widehat{H}_{W,1}, \tag{24}$$

where

$$\widehat{H}_{W,0} = -E|0\rangle\langle 0| + E|1\rangle\langle 1| \tag{25}$$

and

$$\widehat{H}_{W,1} = -\frac{E}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) + \frac{E}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|). \tag{26}$$

Also, by choosing $E = 1$, we have obtained the following minimum delay schedule $T_W = \frac{1}{\sqrt{2}}\varepsilon^{-1}$ [8].

Now, one can apply the Boolean function $f(x) : \{0, 1\} \rightarrow \{0, 1\}$, implemented by the adiabatic Hamiltonian, $\widehat{H}(s)$, given in the above theorem. In this particular case we have $n = 1$ and after a delay $T_f = 4\varepsilon^{-1}$, we obtain the following state:

$$|\varphi_1\rangle \xrightarrow{\widehat{H}(s)} |\varphi_2\rangle = \tfrac{1}{2}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle](|0\rangle - |1\rangle). \tag{27}$$

The last step of the algorithm applies the adiabatic Hadamard gate to the first qubit:

$$\begin{aligned} |\varphi_2\rangle \xrightarrow{\widehat{H}_W(s)} |\varphi_3\rangle &= \tfrac{1}{2}[(-1)^{f(0)}W|0\rangle + (-1)^{f(1)}W|1\rangle](|0\rangle - |1\rangle) \\ &= \tfrac{1}{2}\{[(-1)^{f(0)} + (-1)^{f(1)}]|0\rangle \\ &\quad + [(-1)^{f(0)} - (-1)^{f(1)}]|1\rangle\}\left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \end{aligned} \tag{28}$$

The minimum delay schedule for this step is $T_W = \frac{1}{\sqrt{2}}\varepsilon^{-1}$.

Now, one observes that if $f(x)$ is constant, $f(0) = f(1)$, then $(-1)^{f(0)} - (-1)^{f(1)} = 0$ and the value of the first qubit evaluates to $\pm|0\rangle$. If $f(x)$ is balanced, $f(0) \neq f(1)$, then $(-1)^{f(0)} + (-1)^{f(1)} = 0$ and the value of the first qubit evaluates to $\pm|1\rangle$. Consequently, in order to find whether the function $f(x) : \{0, 1\} \rightarrow \{0, 1\}$ is constant or balanced all that is required is to measure the first qubit. If it is $|0\rangle$, then $f(x)$ is constant, $|1\rangle$ then $f(x)$ is balanced. The minimum delay schedule for the adiabatic quantum Deutsch oracle is therefore given by:

$$T_D = \tfrac{1}{\sqrt{2}}\varepsilon^{-1} + 4\varepsilon^{-1} + \tfrac{1}{\sqrt{2}}\varepsilon^{-1} = (4 + \sqrt{2})\varepsilon^{-1}. \tag{29}$$

4.2. The adiabatic Deutsch–Josza oracle

This oracle generalizes the Deutsch oracle to a function $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}$. Recently, it has been conjectured that the adiabatic quantum computation solution of the Deutsch–Jozsa problem does not match the $O(1)$ time that is achievable using standard quantum computational techniques [11]. In their approach, Das *et al* [11] have considered the Hamiltonian:

$$\widehat{H}_D(s) = (1 - s)\widehat{H}_0 + s\widehat{H}_1, \tag{30}$$

where

$$\widehat{H}_0 = \widehat{I} - |\psi_0\rangle\langle\psi_0|, \tag{31}$$

$$\widehat{H}_1 = \widehat{I} - |\psi_1\rangle\langle\psi_1|. \tag{32}$$

Also, they have considered the following initial and final states:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle, \tag{33}$$

$$|\psi_1\rangle = \alpha|0\rangle + \frac{\beta}{\sqrt{2^n - 1}}\sum_{x=1}^{2^n-1}|x\rangle, \tag{34}$$

with

$$\alpha = \frac{1}{2^n}\left|\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|, \tag{35}$$

$$\beta = 1 - \alpha. \tag{36}$$

One can see that if f is constant, then $\alpha = 1$ and $\beta = 0$ and vice-versa, if f is balanced then $\alpha = 0$ and $\beta = 1$. Thus, after the required running time, if a measurement of the final state yields $|0\rangle$, then f is constant and if it does not yield $|0\rangle$, then it is balanced. With these choices of the initial and final states, they have obtained the following minimum running time:

$$T \geqslant \sqrt{2^n - 1}\varepsilon^{-1}, \tag{37}$$

which is only a quadratic improvement over the classical result. This result is far from the $O(1)$ time that is achievable using the standard quantum computational approach.

Contrary to the above conjecture, here we show that every step in the standard Deutsch–Jozsa oracle can be efficiently implemented in the framework of the adiabatic quantum computation method.

The initial state of the quantum system:

$$|\varphi_0\rangle = |0\rangle^{\otimes n}|1\rangle, \tag{38}$$

is sent through $n + 1$ adiabatic Hadamard gates to give

$$|\varphi_0\rangle \xrightarrow{\widehat{H}_W^{\otimes(n+1)}(s)} |\varphi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{39}$$

Now, one can apply the Boolean function $f(x) : \{0, 1\}^n \to \{0, 1\}$, implemented by the adiabatic Hamiltonian given in the above theorem, and we obtain:

$$\begin{aligned} |\varphi_1\rangle \xrightarrow{\widehat{H}(s)} |\varphi_2\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \end{aligned} \tag{40}$$

Finally, we apply the adiabatic Hadamard transform to the first n qubits again to obtain

$$|\varphi_2\rangle \xrightarrow{\widehat{H}_W^{\otimes n}(s)} |\varphi_3\rangle = \left[\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle \right] \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), \tag{41}$$

where, $x \cdot y$ is the bitwise inner product of x and y, modulo 2.

Let us note that the amplitude of the state $|y\rangle = |0 \ldots 0\rangle$ is

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}. \tag{42}$$

If the function $f(x)$ is constant then the amplitude of the state $|y\rangle = |0 \ldots 0\rangle$ is ± 1. If the function $f(x)$ is balanced then the amplitude of the state $|y\rangle = |0 \ldots 0\rangle$ is 0. In summary, if $f(x)$ is constant then measuring the first n qubits on exit must return the value $|0\rangle$ for all of them. If this is not the case, then $f(x)$ must be balanced. The minimum delay schedule for the adiabatic quantum Deutsch–Josza oracle is also given by: $T_{DJ} = (4 + \sqrt{2})\varepsilon^{-1}$. The obtained value is independent of 2^n , and it is of the same order $O(1)$ that is achievable using standard quantum computational techniques.

4.3. The adiabatic Bernstein–Vazirani oracle

The Bernstein–Vazirani oracle is the Deutsch–Josza oracle with [12]:

$$f(x) = x \cdot a, \tag{43}$$

where, $x, a \in \{0, 1\}^n$, $x \cdot a$ is the bitwise inner product of x and a, modulo 2. The final state of the oracle is:

$$|\varphi_3\rangle = \left[\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{x\cdot a}(-1)^{x\cdot y}|y\rangle\right]\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{44}$$

The amplitude of $|y\rangle = |a\rangle$ is given by

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot a}(-1)^{x\cdot a} = \frac{1}{2^n}\sum_{x=0}^{2^n-1}1 = 1. \tag{45}$$

Thus measuring the first n qubits on exit must return the value $|1\rangle$ for $y = a$ and $|0\rangle$ for $y \neq a$. Obviously, the minimum delay schedule for the adiabatic quantum Bernstein–Vazirani oracle is also given by: $T_{BV} = (4 + \sqrt{2})\varepsilon^{-1}$.

5. Conclusions

We have shown that any Boolean function can be easily implemented using a simple adiabatic Hamiltonian. Also, we have applied this result to the adiabatic quantum implementation of some well-known standard oracles. The presented examples show how a quantum algorithm can outperform a classical one, by combining the essential properties of quantum computing: first it shows the power of quantum parallelism, then it shows the importance of entanglement and non-locality in quantum computing. Also, we would like to note that our results give a different proof of the recent work of Aharonov *et al* [13], showing that the model of adiabatic computation with sparse Hamiltonians is polynomially equivalent to the standard model of quantum computation.

Acknowledgment

This work was supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Farhi E, Goldstone J, Gutmann S and Sipser M 2000 *Preprint* quant-ph/0001106
[3] van Dam W, Mosca M and Vazirani U 2001 *Proc. 42nd Annual Symposium on Foundations of Computer Science* pp 279–87
[4] Roland J and Cerf N J 2002 *Phys. Rev.* A **65** 042308
[5] Messiah A 1976 *Quantum Mechanics* vol 2 (New York: Wiley)
[6] Bransden B H and Joachain C J 2000 *Quantum Mechanics* (Englewood, NJ: Prentice Hall)
[7] Andrecut M and Ali M K 2004 *J. Phys. A: Math. Gen.* **37** L157
[8] Andrecut M and Ali M K 2004 *J. Phys. A: Math. Gen.* **37** L267
[9] Deutsch D 1985 *Proc. R. Soc.* A **400** 97
[10] Deutsch D and Josza R 1992 *Proc. R. Soc.* A **439** 553
[11] Das S, Kobes R and Kunstatter G 2002 *Phys. Rev.* A **65** 062310
[12] Bernstein E and Vazirani U 1997 *SIAM J. Comput.* **26** 1411
[13] Aharonov D, van Dam W, Kempe J, Landau Z, Lloyd S and Regev O 2004 *Preprint* quant-ph/0405098