HIGHLIGHTS OF QUANTUM SEARCH BY MEASUREMENT

ANDREW M. CHILDS, ENRICO DEOTTO
EDWARD FARHI, JEFFREY GOLDSTONE
Center for Theoretical Physics, MIT, Cambridge, MA 02139, USA

SAM GUTMANN
Department of Mathematics, Northeastern University, Boston, MA 02115, USA

ANDREW J. LANDAHL
Center for Bits and Atoms, MIT, Cambridge, MA 02139, USA
Institute for Quantum Information, Caltech, Pasadena, CA 91125, USA
E-mail: alandahl@mit.edu

We describe a quantum algorithm for solving combinatorial search problems that uses only a sequence of measurements. The algorithm is similar in spirit to quantum computation by adiabatic evolution, in that the goal is to remain in the ground state of a time-varying Hamiltonian. Indeed, we show that the running times of the two algorithms are closely related. We also show how to achieve the quadratic speedup for Grover's unstructured search problem with only two measurements.

A promising way to develop new quantum algorithmic ideas is to explore alternative formulations of quantum computation. In a previous paper[1], we explored measurement back-action as a way to simulate adiabatic evolution. In so doing, we developed a generic quantum measurement algorithm for solving combinatorial optimization problems as well as a specific algorithm for solving Grover's search problem[2] with quadratic speedup using only two measurements. In this article, we review these algorithms and highlight some key points of their analysis.

An adiabatic algorithm finds the minimum of a function by applying a slowly changing Hamiltonian to the ground state of the initial Hamiltonian H_B. The final Hamiltonian H_P is chosen so that its ground state encodes the minimum of the function. The adiabatic theorem states that if the evolution is smooth, without level crossings, and applied over a total time $T \gg \Gamma/g^2$, the final state will be the ground state of H_P with high probability, where

$$\Gamma^2 \equiv \max_s \left[\langle E_0(s)|(\tfrac{\mathrm{d}H}{\mathrm{d}s})^2|E_0(s)\rangle - \langle E_0(s)|\tfrac{\mathrm{d}H}{\mathrm{d}s}|E_0(s)\rangle^2\right] \quad (1)$$

$$g \equiv \min_s |E_1(s) - E_0(s)|, \quad (2)$$

and where $E_i(s)$ represents the i^{th} largest energy eigenstate of the interpolating Hamiltonian $H(s)$, with $0 \leq s \leq 1$.

We define the corresponding M-measurement algorithm to be the sequence of M measurements of the interpolating Hamiltonian's value at equally spaced times. No Hamiltonian acts during the measurement algorithm; evolution is generated solely by backaction. For projective measurements, the

Zeno effect predicts that the system will remain in the (changing) ground state with high probability when M is large, resulting in a final ground state population of $\exp(-\Gamma^2/Mg^2)+\mathcal{O}(M^{-2})$, and therefore a successful algorithm when $M \gg \Gamma^2/g^2$.

The running time of the M-measurement algorithm is the product of M and the time τ it takes to perform each measurement of $H(s)$. We calculate this time using von Neumann's measurement model: a Hamiltonian interaction $H(s) \otimes p$ with a pointer followed by a measurement of the pointer's momentum p. To implement this process as a quantum circuit, we digitize the pointer to r qubits, identifying its momentum eigenbasis with the computational basis. We further normalize p as $p\,|z\rangle = 2^{-r} z\,|z\rangle$ so as not to artificially hide algorithmic strength in a growing system-pointer interaction. Finally, we use standard techniques to simulate the interaction Hamiltonian $H(s) \otimes p$ by a quantum circuit[3,4]. In our more detailed paper[1], we show that this model is equivalent to the quantum phase-estimation algorithm.

This quantum circuit approximates a projective measurement, generating a state whose matrix elements are $|\langle E_a|\,\rho\,|E_b\rangle|^2 \cdot |\kappa(x)|^2$, where $x \equiv (E_b - E_a)\tau/2$ and

$$|\kappa(x)|^2 = \frac{\sin^2 x}{4^r \sin^2(x/2^r)}\,. \tag{3}$$

Fig. 1 depicts this function for $x = 4$. It has a sharp peak of unit height and width of order 1 at the origin, and identical peaks at integer multiples of $2^r\pi$. For this approximation to be sufficiently good, $|\kappa(x)|^2$ must be bounded below 1 by a constant for all relevant energy separations x, and in particular for $x = g\tau/2$. Because the width of the central peak is of order 1, this condition is satisfied when $\tau \geq \mathcal{O}(1)/g$, and therefore the M-measurement algorithm succeeds with high probability whenever its running time $T = M\tau \gg \Gamma^2/g^3$. Finally, this approximation is space-efficient—we show in our more detailed paper[1] that r need be no larger than $\mathcal{O}(\log n)$.

One can use a variant of the M-measurement algorithm to solve Grover's unstructured search problem faster than the best possible classical algorithm. The Grover problem[2] is to find a particular unknown n-bit string w using only queries of the form "Is z the same as w?". This is equivalent to the problem of minimizing the oracle function

$$h_w(z) = \begin{cases} 0 & z = w \\ 1 & z \neq w \end{cases}\,. \tag{4}$$

The best possible classical algorithm for solving this problem requires $\Theta(2^n)$ queries to h_w, whereas the best possible quantum algorithm requires only $\Theta(2^{n/2})$ queries for both the unitary ($U_w|z\rangle = (-1)^{h_w(z)}|z\rangle$) and Hamiltonian ($H_w = 1 - |w\rangle\langle w|$) formulations of the oracle[5,6,7,8]. We propose an

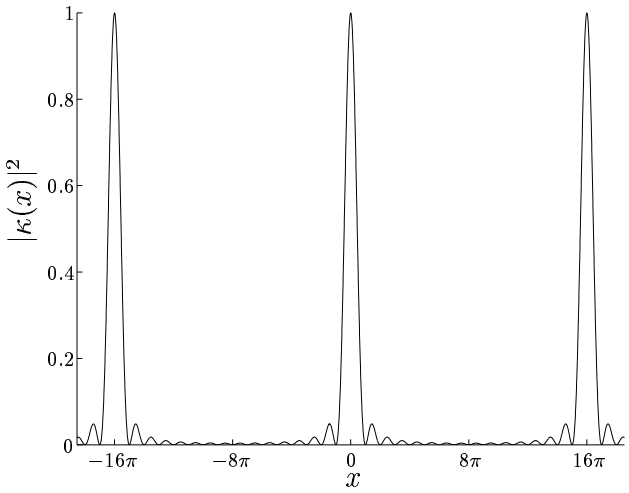

Figure 1. The function $|\kappa(x)|^2$ for $r = 4$.

analogous *measurement oracle* for this problem: the interaction Hamiltonian $H_w \otimes p$. This proposal is motivated by the fact that repeated alternation of $H_w \otimes p$ and $H_B \otimes p$ can generate any Hamiltonian of the form $[sH_B + (1-s)H_w] \otimes p$, which is our model for approximating projective measurement of $H(s)$.

For $H_B = \sum_j (1 - \sigma_x^{(j)})/2$, and linear interpolation to H_w, the minimum gap $g \sim 2^{1-n/2}$ and the $s = s^*$ at which it occurs are known and are independent of w.[9] Furthermore, up to terms of order $1/n$, the $H(s^*)$ eigenstates are equal superpositions of the beginning and final ground states, $|\psi_\pm\rangle \simeq [|E_0(0)\rangle \pm |E_0(1)\rangle]/\sqrt{2}$. Hence, a two-measurement algorithm will solve this problem: prepare the system in the state $|E_0(0)\rangle$, measure $H(s^*)$, then measure $H(1)$. This algorithm finds w with probability $\frac{1}{2}$, which can be boosted as close to unity as desired by repetition. This is not a constant-time algorithm, however. Because the $H(1)$ measurement takes constant time and the $H(s^*)$ measurement takes time $\tau = \mathcal{O}(1)/g$, its complexity is $\Theta(2^{n/2})$, the most efficient possible quantum mechanically[5].

We have shown that an adiabatic algorithm requiring time $T \gg \Gamma/g^2$ can be simulated by a corresponding measurement algorithm requiring time $T \gg \Gamma^2/g^3$. Thus, the measurement algorithm is efficient whenever the adiabatic algorithm is efficient. Moreover, we have presented a measurement algorithm that can achieve quadratic speedup for the Grover problem by using knowledge of the place where the gap g is smallest. Finally, we have argued that it is important to use an explicit dynamical process to model the measurement of complicated observables when they are called for in quantum

algorithms. Without a measurement model, the analysis of such algorithms can give misleading results.

Acknowledgments

This work was supported in part by the Department of Energy under cooperative research agreement DE-FC02-94ER40818, by the National Science Foundation under grant EIA-0086038, and by the National Security Agency and Advanced Research and Development Activity under Army Research Office contract DAAD19-01-1-0656. AMC received support from the Fannie and John Hertz Foundation, and ED received support from the Istituto Nazionale di Fisica Nucleare (Italy).

References

1. A. M. Childs, E. Farhi, E. Deotto, J. Goldstone, S. Gutmann, and A. Landahl. Quantum search by measurement. *Phys. Rev. A*, 66:032314, 2002. quant-ph/0204013.
2. L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325, 1997.
3. S. Wiesner. Simulations of many-body quantum systems by a quantum computer, 1996. quant-ph/9603028.
4. C. Zalka. Efficient simulation of quantum systems by quantum computers. *Proc. Roy. Soc. London A*, 454:313, 1998.
5. C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26:1510, 1997.
6. E. Farhi and S. Gutmann. Analog analogue of a digital quantum computation. *Phys. Rev. A*, 57:2403, 1998.
7. J. Roland and N. Cerf. Quantum search by local adiabatic evolution, 2001. quant-ph/0107015.
8. W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? In B. Werner, editor, *Proceedings, 42th Annual Symposium on Foundations of Computer Science*, pages 279–287, Los Alamitos, CA, 2001. IEEE Press. quant-ph/0206003.
9. E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution, 2000. quant-ph/0001106.