An Information-Theoretic Analysis of Grover's Algorithm

Erdal Arıkan
Bilkent University
Department of Electrical Engineering
Ankara, 06800, Turkey
e-mail: arikan@ee.bilkent.edu.tr

I. Introduction

Grover [1] discovered a quantum algorithm for identifying a target element in an unstructured search universe of N items in approximately $\pi/4\sqrt{N}$ queries to a quantum oracle. For classical search using a classical oracle, the search complexity is clearly of order $N/2$. It has been proven that this square-root speed-up is the best attainable performance gain by any quantum algorithm [2], [3], [4]. In this talk we present an information-theoretic analysis of Grover's algorithm and give a tight lower bound on the complexity of search algorithms using Grover's oracle.

II. Grover's algorithm

A quantum search may be viewed as a quantum system consisting of a target subsystem X and a computer subsystem C. The target state is fixed throughout and is given by $\rho_T = \sum_{x=0}^{N-1}(1/N)|x\rangle\langle x|$, where $\{|x\rangle\}$ is an orthonormal set. The joint state of the target and the computer at time k is given by

$$\rho_{TC}(k) = \sum_{x=0}^{N-1}(1/N)|x\rangle\langle x| \otimes \rho_x(k), \tag{1}$$

where $\rho_x(k)$ is the state of the computer at time k, conditional on the target value being x.

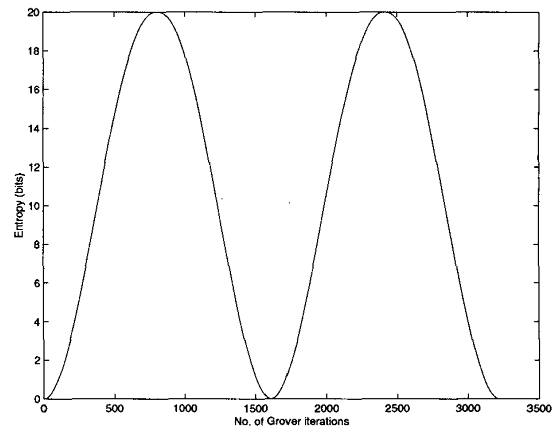
The computer begins in a fixed initial state $\rho_C(0)$ and evolves to a state of the form $\rho_C(k) = \sum_{x=0}^{N-1}(1/N)\rho_x(k)$ at time k, under control of the algorithm. The computation terminates at a prespecified time K, when a measurement is taken on $\rho_C(K)$ and an output Y is obtained. An error is said to occur if Y differs from the target value. Each computational step consists of the application of an operator of the form $\sum_x |x\rangle\langle x| \otimes G_x$, which transforms the joint state $\rho_{TC}(k)$ to

$$\rho_{TC}(k+1) = \sum_x (1/N)|x\rangle\langle x| \otimes G_x\rho_x(k)G_x^\dagger. \tag{2}$$

In particular, Grover's algorithm consists of $K = (\pi/4)\sqrt{N}$ successive applications of the operator $G_x = U_sO_x$ where $O_x = I-2|x\rangle\langle x|$, $U_s = 2|s\rangle\langle s|-I$, and $|s\rangle = \sum_{x=0}^{N-1}(1/\sqrt{N})|x\rangle$. The initial state in Grover's algorithm is $\rho_C(0) = |s\rangle\langle s|$. Each use of $\{O_x\}$ is counted as one call to 'Grover's oracle.'

III. Information flow in Grover's algorithm

Clearly, the von Neumann entropy of the joint state remains fixed at $S(\rho_{TC}(k)) = \log N$ throughout the algorithm, whereas the entropy of the computer state $S(\rho_C(k))$ changes as information is transferred by the oracle between the target and the computer. This is illustrated in the figure, which shows the entropy of $\rho_C(k)$ for $N = 2^{20}$. The period equals $\pi/\theta \approx (\pi/2)\sqrt{N}$.



This figure suggests that a bound on the complexity of any oracle-based search algorithm may be obtained by giving an upper bound on the amount of information transfer per oracle call. The following result is based on this idea.

Proposition 1 *Any quantum search algorithm that uses Grover's oracle $\{O_x\}$ must call the oracle at least*

$$K \geq \left(\frac{1-P_e}{2\pi} + \frac{1}{\pi \log N}\right)\sqrt{N} \tag{3}$$

times to achieve a probability of error P_e.

The proof uses Holevo's bound and Fano's inequality and may be found in the full version of the paper [5].

The bound (3) captures the $\sqrt{N}$ complexity of Grover's algorithm. Lower-bounds on Grover's algorithm have been known before; and, in fact, the present bound is not as tight as e.g. the one in [4]. The significance of the present bound is that it is largely based on information-theoretic concepts. Also worth noting is that the probability of error P_e appears explicitly in (3), unlike other bounds known to us.

References

[1] L. K. Grover, 'A fast quantum mechanical algorithm for database search,' *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, May 1996, pp. 212-219. (quant-p/9605043)

[2] C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani, 'Strength and weaknesses of quantum computing,' *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510-1523, Oct. 1997. (quant-ph/9701001)

[3] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, 'Tight bounds on quantum computing,' *Proceedings 4th Workshop on Physics and Computation*, pp. 36-43, 1996. Also *Fortsch. Phys.* 46(1998) 493-506. (quant-ph/9605034)

[4] C. Zalka, 'Grover's quantum searching is optimal,' *Phys. Rev. A*, 60, 2746 (1999). (quant-ph/9711070v2)

[5] E. Arikan, 'An information-theoretic analysis of Grover's algorithm,' Oct, 2002. (quant-ph/0210068)

0-7803-7728-1/03/$17.00 ©2003 IEEE.