Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER

Electronic Notes in Discrete Mathematics 21 (2005) 231–232

Electronic Notes in DISCRETE MATHEMATICS

www.elsevier.com/locate/endm

An upper bound on the rate of information transfer by Grover's oracle

Erdal Arikan

*Electrical-Electronics Engineering Department, Bilkent University, 06533 Ankara, Turkey,*arikan@ee.bilkent.edu.tr

Abstract

Grover 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 of order $N/2$ queries since on average half of the items must be searched. In work preceding Grover's, Bennett et al. had shown that no quantum algorithm can solve the search problem in fewer than $O(\sqrt{N})$ queries. Thus, Grover's algorithm has optimal order of complexity. Here, we present an information-theoretic analysis of Grover's algorithm and show that the square-root speed-up by Grover's algorithm is the best possible by any algorithm using the same quantum oracle.

Grover [1], [2] 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 $N/2$ queries since on average half of the items must be searched. It has been proven that this square-root speed-up is the best attainable performance gain by any quantum algorithm. In work preceding Grover's, Bennett et al. [4] had shown that no quantum algorithm can solve the search problem in fewer than $O(\sqrt{N})$ queries. Following Grover's work, Boyer et al. [5] showed that Grover's algorithm is optimal asymptotically, and that square-root speed-up cannot be improved even if one allows, e.g., a 50% probability of error. Zalka [3] strengthened these results to show that Grover's algorithm is optimal exactly (not only asymptotically). In this correspondence we present an information-theoretic analysis of Grover's algorithm and show the optimality of Grover's algorithm from a different point of view.

1571-0653/$ – see front matter
doi:10.1016/j.endm.2005.07.031

References

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

[2] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Letters, 78, 2, 325-328, 1997.

[3] C. Zalka, Grover's quantum searching is optimal, Phys. Rev. A, 60, 2746, 1999.

[4] 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, 1510-1523, 1997.

[5] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, Tight bounds on quantum computing, Proceedings 4th Workshop on Physics and Computation, 36-43, 1996; Fortsch. Phys. 46, 493-506, 1998.

[6] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[7] J. Stoer and R. Bulirsch, Introduction to Numerical Analysis, Springer, NY, 1980.