Exact quantum lower bound for Grover's problem*

Cătălin Dohotaru† Peter Høyer†

October 19, 2008

Abstract

One of the most important quantum algorithms ever discovered is Grover's algorithm for searching an unordered set. We give a new lower bound in the query model which proves that Grover's algorithm is exactly optimal. Similar to existing methods for proving lower bounds, we bound the amount of information we can gain from a single oracle query, but we bound this information in terms of angles. This allows our proof to be simple, self-contained, based on only elementary mathematics, capturing our intuition, while obtaining at the same an exact bound.

Keywords. Quantum computing. Lower bound. Grover's algorithm. Decision trees.

1 Introduction

Grover's algorithm [13] is one of the most celebrated quantum algorithms ever devised. The algorithm and its many extensions demonstrate that quantum computers can speed up many search-related problems by a quadratic factor over classical computers. The algorithm is based on some of the most fundamental properties of quantum mechanics and has consequently found uses in a very wide range of situations, including unordered searching [13, 9], communication complexity [11], counting [10], cryptography [2], learning theory [19], network flows [5], zero-knowledge [20], and random walks [18], just to name a few. The underlying principles of the algorithm are very versatile and are readily amendable to a number of variations in applications. By clever insight into its basic principles, it has been adapted to for instance local searching of spatial structures [1], searching erroneous data [15], and searching structures with variable search costs [4]. Grover's algorithm and its generalizations are in conclusion one of the most successful frameworks ever discovered for quantum information processing.

Given these overwhelmingly many positive applications of Grover's search algorithm, it is natural to ask if Grover's algorithm is optimal, or if an even faster routine could take its place in the above applications. The unanimous answer is that no better algorithm exists for searching unordered structures on a quantum computer. Grover's algorithm is in other words optimal. The optimality of the algorithm has been established through many different approaches, including adversarial arguments [3], degree of polynomials [7], hybrid arguments [8], Kolmogorov complexity [17], and spectral decompositions [6].

Common for all the above lower bounds is, however, that they do not show that Grover's algorithm is exactly optimal, but only asymptotically optimal. The above lower bound results on quantum searching do not exclude the possibility that there might be another quantum algorithm that solves Grover's search problem say 10% faster than Grover's own algorithm.

Fortunately we do know that Grover's algorithm is exactly optimal through the singular work of Zalka [21]. By carefully inspecting each step in Grover's algorithm, Zalka is able to argue that it is exactly optimal. Zalka's proof involves defining a certain function g and proving it has some appropriate behaviour, including $g' > 0$ and $g'' < 0$, using Lagrange multiplies to solve constrained extremum problems, and eventually concluding that four different inequalities are saturated by Grover's algorithm. Zalka's construction seems

*This work has been supported by Canada's NSERC, the Canadian Institute for Advanced Research (CIFAR), and MITACS.

†Department of Computer Science, University of Calgary, 2500 University Drive N.W., Calgary, Alberta, Canada T2N 1N4. Email: {dcatalin,hoyer}@ucalgary.ca.

to require an intimate understanding of Grover's algorithm and fluency in finding extrema for various multivariate functions.

Grover and Radhakrishnan [14] make several simplifications to Zalka's proof and construct a more explicit and rigorous proof that allows them to give a near-tight lower bound for Grover's problem. Their near-optimal theorem applies without modifications to success probabilities of at least 0.9, whereas Zalka's original proof applies to any choice of success probability and any size of search space.

The aim of the present paper is to give a new tight lower bound for the unordered search problem that is as simple and transparent as possible, using only elementary mathematics, and that does not presume any knowledge of Grover's algorithm or any other upper bound. Our proof applies, as Zalka's, to any choice of success probability and any size of search space.

2 Proving lower bounds for quantum algorithms

In the unordered search problem, we are given a bitstring x as input. The input is given to us as an oracle so that the only knowledge we can gain about the input is in asking queries to the oracle. We are interested in solving the unordered search problem with the least number of queries to the oracle. We model the oracle

$$\mathsf{O}_x|i;\, w\rangle = \begin{cases} (-1)^{x_i}|i;\, w\rangle & \text{if } 1 \leq i \leq N \\ |i;\, w\rangle & \text{if } i = 0. \end{cases}$$

Definition 1 (Unordered search problem) *We are given a bitstring $x \in \{0,1\}^N$ as an oracle, and promised that there exists a unique index $1 \leq i \leq N$ for which $x_i = 1$. We want to output an index $1 \leq j \leq N$ such that $i = j$ with probability at least p.*

In the following, we identify the N possible inputs with the set $y \in \{1, 2, \ldots, N\}$ so that for instance input $y = 7$ denotes the input bitstring x in which bit 7 is 1 ($x_7 = 1$) and the $N-1$ other bits are 0 ($x_i = 0$ for $i \neq 7$).

The most straightforward classical *deterministic* algorithm for solving the unordered search problem would be to simply query the oracle for the $N-1$ bits $x_1, x_2, \ldots, x_{N-1}$. If any of these $N-1$ bits equals 1, we output the corresponding index, and otherwise, we output the unqueried index N. This algorithm always outputs the correct answer, uses $N-1$ queries, and is optimal. An optimal *probabilistic* algorithm is to pick a set of $T = \lceil pN - 1 \rceil$ distinct indices uniformly at random, and query the oracle on those T indices. If any of the T bits equals 1, we output the corresponding index, and otherwise, we output one of the remaining $N - T$ indices, picked again uniformly at random. The probability we output the correct index is $\frac{T+1}{N} \geq p$. Grover's algorithm is the best known *quantum* algorithm for the unordered search problem. It uses of order $\sqrt{pN}$ queries and outputs the correct index with probability at least p.

Any quantum algorithm in the oracle model starts in a state that is independent of the oracle x. For convenience, we take the start state to be $|0\rangle$ in which all qubits are initialized to 0. It then evolves by applying arbitrary unitary operators U to the system, alternated by queries O_x to the oracle x, followed by a conclusive measurement of the final state, the outcome of which is the result of the computation. We assume (without loss of generality) that the final measurement is a von Neumann measurement represented by a finite set of orthogonal projectors $\{\Pi_y\}$ that sum to the identity. In symbols, a quantum algorithm A that uses T queries to the oracle, computes the final state

$$|\Psi_x^T\rangle = \mathsf{U}_T \mathsf{O}_x \mathsf{U}_{T-1} \cdots \mathsf{U}_1 \mathsf{O}_x \mathsf{U}_0 |0\rangle$$

which is then measured, yielding the answer y with probability $\left\| \Pi_y |\Psi_x^T\rangle \right\|^2$.

A more detailed and excellent introduction to the query model is given in [12], and a discussion of lower bounds for the model in [16].

3 Exact lower bound for quantum searching

In the unordered search problem, we are given one of N possible inputs x, and we produce one of N possible outputs $y \in \{1, 2, \dots, N\}$. For the algorithm to succeed with probability at least p, we require that $\left\|\Pi_x |\Psi_x^T\rangle\right\|^2 \geq p$ for all $x \in \{1, 2, \dots, N\}$. Let $\Psi^t = \mathsf{U}_t \mathsf{O}_u \mathsf{U}_{t-1} \cdots \mathsf{U}_1 \mathsf{O}_u \mathsf{U}_0 |0\rangle$ denote the state after t queries when the oracle $u = 00\cdots0$ is the all-zero bitstring, in which case, the oracle O_u acts as the identity. Let $\Psi_y^{i,T} = \mathsf{U}_T \mathsf{O}_u \cdots \mathsf{O}_u \mathsf{U}_{i+1} \mathsf{O}_u \mathsf{U}_i \mathsf{O}_y \cdots \mathsf{U}_1 \mathsf{O}_y \mathsf{U}_0 |0\rangle$ denote the final state after T queries, where we use oracle y for the first i oracle queries and the identity for the latter $T - i$ oracle queries.

We now give our new exactly optimal lower bound for the unordered search problem. We present our proof in parallel with the standard (asymptotically optimal) hybrid argument lower bound derived from [8] which seems to be the simplest of the existing lower bounds. Both proofs require three steps, and we present each of these steps in a form so that the two proofs resemble each other as closely as possible and are as simple as possible.

The key to our new lower bound is the use of angles as opposed to distances as in the standard proof in [8]. We define the *quantum angle* between two non-zero vectors as

$$\measuredangle(\psi, \psi') = \arccos \frac{\left|\langle\psi|\psi'\rangle\right|}{\|\psi\|\|\psi'\|}. \tag{1}$$

This seems to be the most appropriate definition of angles for quantum computing and can be readily generalized to mixed states through fidelity and satisfies, in particular, the triangle inequality.

3.1 First step

The first step in the proof is to establish a Cauchy-Schwarz-like inequality (for each of our two measures, distances and angles) which will allow us to bound the amount of information we can learn by each individual query.

Lemma 2 (Cauchy–Schwarz — distance version)

$$\max\left\{\sum_{i=1}^N a_i \mid 0 \leq a_i \text{ and } \sum_{i=1}^N a_i^2 \leq 1\right\} = \sqrt{N}. \tag{2}$$

Proof First note that when all a_i's are equal, the maximum value of the sum is $\sqrt{N}$. Now, assume that $\sqrt{N}$ is not the maximum value of the sum. Then there exist N numbers $b_1, \dots, b_N$ for which the maximum is attained. At least two of the b_i's are not equal, denote them by x and y. Replacing both x and y with their average, the sum we want to maximize remains unchanged, while the sum of squares strictly decreases since

$$x^2 + y^2 - 2\left(\frac{x+y}{2}\right)^2 = \frac{1}{2}(x-y)^2 > 0.$$

We can thus increase all b_i's by a tiny amount while keeping the sum of squares at most 1, contradicting the assumption that the b_i's attain the maximum. It follows the maximum is attained when all a_i's are equal. □

Lemma 3 (Cauchy–Schwarz — angle version)

$$\max\left\{\sum_{i=1}^N \theta_i \mid 0 \leq \theta_i \leq \frac{\pi}{2} \text{ and } \sum_{i=1}^N \sin^2\theta_i \leq 1\right\} = N \arcsin \frac{1}{\sqrt{N}}. \tag{3}$$

Proof First note that when all a_i's are equal, the maximum value of the sum is $N \arcsin \frac{1}{\sqrt{N}}$. Now, assume that this is not the maximum value of the sum. Then there exist N angles $\varphi_1, \dots, \varphi_N$ for which the maximum is attained. At least two of the φ_i's are not equal, denote them by u and v. Replacing both u and v with their average, the sum we want to maximize remains unchanged, while the sum of squares strictly decreases since[1]

$$\sin^2 u + \sin^2 v - 2\sin^2\left(\frac{u+v}{2}\right) = 2\sin^2\left(\frac{u-v}{2}\right)\cos(u+v) > 0.$$

We can thus increase all φ_i's by a tiny amount while keeping the sum of squares at most 1, contradicting the assumption that the φ_i's attain the maximum. It follows the maximum is attained when all θ_i's are equal. □

3.2 Second step

The second step is then to show that the amount of information we learn by each of the T query can only add up linearly (with respect to our two measures, distances and angles).

Lemma 4 (Increase in distance by T queries) *The average distance after T queries is at most $2T\frac{1}{\sqrt{N}}$.*

Proof We have, using the triangle inequality,

$$\begin{aligned}\frac{1}{N}\sum_{y=1}^{N}\left\|\Psi^T - \Psi_y^T\right\| &= \frac{1}{N}\sum_{y=1}^{N}\left\|\Psi_y^{T,T} - \Psi_y^{0,T}\right\| \le \frac{1}{N}\sum_{y=1}^{N}\sum_{i=0}^{T-1}\left\|\Psi_y^{i+1,T} - \Psi_y^{i,T}\right\| \\ &= \frac{1}{N}\sum_{i=0}^{T-1}\sum_{y=1}^{N}\left\|\mathsf{O}_y\Psi^i - \Psi^i\right\| = \frac{1}{N}\sum_{i=0}^{T-1}\sum_{y=1}^{N}2\left\|\Pi_y\Psi^i\right\| \\ &\le 2\sum_{i=0}^{T-1}\frac{1}{\sqrt{N}} = 2T\frac{1}{\sqrt{N}},\end{aligned}$$

where the last inequality follows from the inequality proven in Lemma 2. □

Lemma 5 (Increase in angle by T queries) *The average angle after T queries is at most $2T\Theta$, where $\Theta = \arcsin(\frac{1}{\sqrt{N}})$.*

Proof We have, using the triangle inequality for angles,

$$\begin{aligned}\frac{1}{N}\sum_{y=1}^{N}\measuredangle\big(\Psi^T, \Psi_y^T\big) &= \frac{1}{N}\sum_{y=1}^{N}\measuredangle\big(\Psi_y^{T,T}, \Psi_y^{0,T}\big) \le \frac{1}{N}\sum_{y=1}^{N}\sum_{i=0}^{T-1}\measuredangle\big(\Psi_y^{i+1,T}, \Psi_y^{i,T}\big) \\ &= \frac{1}{N}\sum_{i=0}^{T-1}\sum_{y=1}^{N}\measuredangle\big(\mathsf{O}_y\Psi^i, \Psi^i\big) = \frac{1}{N}\sum_{i=0}^{T-1}\sum_{y=1}^{N}\arccos\left(\left|\cos(2\theta_y^i)\right|\right) \\ &\le \frac{1}{N}\sum_{i=0}^{T-1}\sum_{y=1}^{N}2\theta_y^i \le 2\sum_{i=0}^{T-1}\Theta = 2T\Theta,\end{aligned}$$

where the last inequality follows from the inequality for angles proven in Lemma 3. □

3.3 Third step

The third and final step is then to show that by the end of the algorithm, after all T queries, our measure (distance or angle, respectively) is large.

Lemma 6 (Distinguishability of final states — distance version) *Suppose that the algorithm correctly outputs y with probability at least p after T queries, given oracle O_y. Then the average distance is at least*

$$\frac{1}{N}\sum_{y=1}^{N}\left\|\Psi^T - \Psi_y^T\right\| \ge \frac{1}{\sqrt{2}}\Big(1 + \sqrt{p} - \sqrt{1-p} - \frac{2}{\sqrt{N}}\Big). \tag{4}$$

[1] The equality can be proven by showing that both sides are equal to $\cos(u+v) - \frac{1}{2}\cos(2u) - \frac{1}{2}\cos(2v)$, or by applying Euler's formula.

Proof The distance after T queries is at least

$$\begin{aligned}
\big\|\Psi^T - \Psi_y^T\big\| &\geq \frac{1}{\sqrt{2}}\Big(\big\|\Pi_y\Psi_y^T - \Pi_y\Psi^T\big\| + \big\|\Pi_y^\perp\Psi^T - \Pi_y^\perp\Psi_y^T\big\|\Big)\\
&\geq \frac{1}{\sqrt{2}}\Big(\big\|\Pi_y\Psi_y^T\big\| - \big\|\Pi_y\Psi^T\big\| + \big\|\Pi_y^\perp\Psi^T\big\| - \big\|\Pi_y^\perp\Psi_y^T\big\|\Big)\\
&\geq \frac{1}{\sqrt{2}}\Big(\sqrt{p} - \big\|\Pi_y\Psi^T\big\| + \big\|\Pi_y^\perp\Psi^T\big\| - \sqrt{1-p}\Big)\\
&\geq \frac{1}{\sqrt{2}}\Big(\sqrt{p} - \sqrt{1-p} + 1 - 2\big\|\Pi_y\Psi^T\big\|\Big),
\end{aligned}$$

where the first inequality follows from the inequality $(a-b)^2 \geq 0$, the second-last inequality from the success probability being at least p, and the other two from the triangle inequality. The average distance after T queries is thus at least

$$\begin{aligned}
\frac{1}{N}\sum_{y=1}^{N}\big\|\Psi^T - \Psi_y^T\big\| &\geq \frac{1}{N}\sum_{y=1}^{N}\frac{1}{\sqrt{2}}\Big(1 + \sqrt{p} - \sqrt{1-p} - 2\big\|\Pi_y\Psi^T\big\|\Big)\\
&= \frac{1}{\sqrt{2}}\Big(1 + \sqrt{p} - \sqrt{1-p} - \frac{2}{N}\sum_{y=1}^{N}\big\|\Pi_y\Psi^T\big\|\Big)\\
&\geq \frac{1}{\sqrt{2}}\Big(1 + \sqrt{p} - \sqrt{1-p} - \frac{2}{\sqrt{N}}\Big),
\end{aligned}$$

where the last inequality follows from the inequality proven in Lemma 2. □

Lemma 7 (Distinguishability of final states — angle version) *Suppose that the algorithm correctly outputs y with probability at least p after T queries, given oracle O_y. Then the average angle is at least*

$$\frac{1}{N}\sum_{y=1}^{N}\measuredangle\big(\Psi^T, \Psi_y^T\big) \geq \Theta^T - \Theta, \tag{5}$$

where $\sin^2(\Theta^T) = p$ *and* $\sin^2(\Theta) = \frac{1}{N}$.

Proof The angle difference after T queries is at least

$$\begin{aligned}
\measuredangle\big(\Psi^T, \Psi_y^T\big) &= \arccos\big(\big|\langle\Psi^T|\Psi_y^T\rangle\big|\big)\\
&= \arccos\big(\big|\langle\Psi^T|(\Pi_y + \Pi_y^\perp)|\Psi_y^T\rangle\big|\big)\\
&\geq \arccos\big(\big\|\Pi_y\Psi^T\big\|\cdot\big\|\Pi_y\Psi_y^T\big\| + \big\|\Pi_y^\perp\Psi^T\big\|\cdot\big\|\Pi_y^\perp\Psi_y^T\big\|\big)\\
&= \arccos\big(\sin\theta_y^T\sin\phi_y^T + \cos\theta_y^T\cos\phi_y^T\big)\\
&= \arccos\big(\cos(\phi_y^T - \theta_y^T)\big)\\
&= \big|\phi_y^T - \theta_y^T\big|,
\end{aligned}$$

where $\sin(\phi_y^T) = \|\Pi_y\Psi_y^T\|$ and $\sin(\theta_y^T) = \|\Pi_y\Psi^T\|$. The average angle difference after T queries is thus at least

$$\frac{1}{N}\sum_{y=1}^{N}\measuredangle\big(\Psi^T, \Psi_y^T\big) \;\geq\; \frac{1}{N}\sum_{y=1}^{N}\big(\phi_y^T - \theta_y^T\big) \;\geq\; \Theta^T - \frac{1}{N}\sum_{y=1}^{N}\theta_y^T \;\geq\; \Theta^T - \Theta,$$

where the second-last inequality follows from the success probability being at least p, and the last inequality from the inequality for angles proven in Lemma 3. □

3.4 Concluding the proof

Since each of our two measures is 0 initially, is large by the end of the algorithm, and can only increase modestly by each query, we can conclude that a large number of queries is required.

Theorem 8 (Asymptotic lower bound for searching — distance version) *The unordered search problem with success probability $p > 0$ requires at least $T \geq \frac{\sqrt{N}}{2\sqrt{2}}\left(1+\sqrt{p}-\sqrt{1-p}-\frac{2}{\sqrt{N}}\right)$ queries.*

Theorem 9 (Tight lower bound for searching — angle version) *The unordered search problem with success probability $p = \sin^2(\Theta^T) > 0$ requires at least $T \geq \frac{\Theta^T - \Theta}{2\Theta}$ queries.*

In the case of distances, we conclude that Grover's algorithm is asymptotically optimal, and in the case of angles, that Grover's algorithm is exactly optimal. No other algorithm can achieve even a constant additive improvement with respect to the number of queries required for a given success probability. Compared to other lower bounds, and even to the hybrid argument, our proof seems surprisingly simple. It would be interesting to extend our method to obtain both simpler and better lower bounds for other problems, and also to find other uses of quantum angles.

References

[1] S. Aaronson and A. Ambainis. *Quantum search of spatial regions.* Theory of Computing, 1(1):47–79, 2005.

[2] M. Adcock, R. Cleve, K. Iwama, R. Putra, and S. Yamashita. *Quantum lower bounds for the Goldreich-Levin problem.* Information Processing Letters, 97(5):208–211, 2006.

[3] A. Ambainis. *Quantum lower bounds by quantum arguments.* Journal of Computer and System Sciences, 64:750–767, 2002.

[4] A. Ambainis. *Quantum search with variable times.* Proceedings of the 25th Annual Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science 49–61, 2008.

[5] A. Ambainis and R. Špalek. *Quantum algorithms for matching and network flows.* Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science 3884:172–183, 2006.

[6] H. Barnum, M. Saks, and M. Szegedy. *Quantum decision trees and semidefinite programming.* Proceedings of the 18th IEEE Conference on Computational Complexity, pp. 179–193, 2003.

[7] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. *Quantum lower bounds by polynomials.* Journal of the ACM, 48(4):778–797, 2001.

[8] H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. *Strengths and weeknesses of quantum computing.* SIAM Journal on Computing, 26(5):1510–1523, 1997.

[9] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. *Tight bounds on quantum searching.* Fortschritte Der Physik, 46(4–5):493–505, 1998.

[10] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. *Quantum amplitude amplification and estimation.* In Quantum Computation and Quantum Information: A Millennium Volume, AMS Contemporary Mathematics Series, Volume 305, 2002.

[11] H. Buhrman, R. Cleve, and A. Wigderson. *Quantum vs. classical communication and computation.* Proceedings of the 30th ACM Symposium on Theory of Computing, pp 63–65, 1998.

[12] H. Buhrman and R. de Wolf. *Complexity Measures and Decision Tree Complexity: A Survey.* Theoretical Computer Science, 288(1):21–43, 2002.

[13] L. K. Grover. *Quantum mechanics helps in searching for a needle in a haystack.* Physical Review Letters, 79(2):325–328, 1997.

[14] L. K. Grover and J. Radhakrishnan. *Is partial quantum search of a database any easier?* Proceedings of the 17th Annual ACM Symposium on Parallelism in Algorithms and Architectures, pp 186–194, 2005.

[15] P. Høyer, M. Mosca, and R. de Wolf. *Quantum search on bounded-error inputs.* Proceedings of the 30th International Colloquium on Automata, Languages, and Programming, Lecture Notes in Computer Science 2719:291–299, 2003.

[16] P. Høyer and R. Špalek. *Lower bounds on quantum query complexity.* Bulletin of the European Association for Theoretical Computer Science, 87:78–103, 2005.

[17] S. Laplante and F. Magniez. *Lower bounds for randomized and quantum query complexity using Kolmogorov arguments.* SIAM Journal on Computing, 38(1):46–62, 2008.

[18] F. Magniez, A. Nayak, J. Roland, and M. Santha. *Search via quantum walk.* Proceedings of the 39th ACM Symposium on Theory of Computing, pp 575–584, 2007.

[19] R. Servedio and S. Gortler. *Equivalences and separations between quantum and classical learnability.* SIAM Journal on Computing, 33(5):1067–1092, 2004.

[20] J. Watrous. *Zero-knowledge against quantum attacks.* To appear in SIAM Journal on Computing, 2008.

[21] Ch. Zalka. *Grover's quantum searching is exactly optimal.* Physical Review A, 60:2746–2751, 1999.