Impossibility of a Quantum Speed-up with a Faulty Oracle

Oded Regev* Liron Schiff†

Abstract

We consider Grover's unstructured search problem in the setting where each oracle call has some small probability of failing. We show that no quantum speed-up is possible in this case.

1 Introduction

Unstructured search problem: The unstructured search problem, also known as the unordered search problem or as Grover's search problem, is the most basic problem in the query model. The goal is to find a marked entry out of N possible entries. In this model the entries are accessible only through a black box (the oracle), and the complexity of the algorithm is measured in terms of the number of oracle queries. In the classical world, it is easy to see that solving this search problem requires $\Theta(N)$ queries, even if we allow randomization. In the quantum world, however, one can find a marked item with only $O(\sqrt{N})$ queries, as was shown in Grover's seminal paper [8]. Moreover, it is known that this is optimal (see, e.g., [4, 5, 1]). This remarkable quadratic improvement is considered one of the biggest successes of quantum computing, and has sparked a huge interest in the quantum query model (see [2] for a recent survey).

Searching with a faulty oracle: In this paper we consider the unstructured search problem in the *faulty oracle model*, a question originally presented to us by Harrow [9]. In this model, each oracle call succeeds with some probability $1-p$, and with the remaining probability p the state given to the oracle remains unchanged. More formally, each oracle call maps an input state ρ into $(1-p)\cdot O\rho O^\dagger + p\cdot\rho$ where O is the original (unitary) oracle operation. We note that this model can be seen to be equivalent to other, seemingly more realistic, models of faults, such as the model considered in Shenvi et al. [19] in which the oracle's operation is subject to small random phase fluctuations.

Our motivation for considering the faulty oracle model is twofold. First, we believe that since the unstructured search problem is such a basic question, it is theoretically interesting to consider it in different settings, as this might shed more light on the strengths and weaknesses of quantum query algorithms. A second motivation is related to implementation aspects of quantum query algorithms, as one can expect any future implementation of a Grover oracle to be imperfect (see [19] for a further discussion of the physical significance of the model).

*School of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel. Supported by the Binational Science Foundation, by the Israel Science Foundation, and by the European Commission under the Integrated Project QAP funded by the IST directorate as Contract Number 015848.

†School of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel.

To motivate our main result and to get some intuition for the model, let us consider the behavior of Grover's original algorithm in this setting. Recall that Grover's algorithm can be seen as a sequence of two alternating reflections, $OUOUOU \cdots OU$ where U is the reflection given by Grover's algorithm and O is the reflection representing the oracle call. In the analysis of Grover's algorithm, one observes that the state of the system is restricted to a two-dimensional subspace, inside which lie the initial state and the target state. The angle between these two states is essentially $\pi/2$. Furthermore, the combined operation OU of two consecutive reflections can be seen a rotation by an angle of essentially $1/\sqrt{N}$ inside this two dimensional subspace. Hence the total number of oracle calls required to get to the target state is $O(\sqrt{N})$.

In the faulty oracle model, each oracle call O has some constant probability of not doing anything. Hence, the sequence of reflections might look like $OUOUOUUOUOUOUO$. The effect of this is that after a sequence of rotations OU by $1/\sqrt{N}$, we instead obtain a sequence of rotations $UO = (OU)^\dagger$ by $-1/\sqrt{N}$ which cancel the previous ones. The cancellation can also be seen by noting that $U^2 = O^2 = I$. The end result is that instead of rotating towards the target, our rotation behaves like a random walk, alternating between steps of $1/\sqrt{N}$ and steps of $-1/\sqrt{N}$. Using known properties of random walks on a line, the number of steps required for this walk to reach the target is $\Theta(N)$, which shows that Grover's algorithm is no better than the naive classical search algorithm.

But can there be another, more sophisticated algorithm that copes better with the faults? Our main result shows that the answer is essentially 'no'.

Our result: Our main result shows that there is essentially no quantum advantage when searching with a faulty oracle.

Theorem 1. *Any algorithm that solves the p-faulty Grover problem must use* $T > \frac{p}{10(1-p)}N$ *queries.*

In particular, for any constant $p > 0$, this gives a lower bound of $\Omega(N)$.

Notice that the above statement holds for *any* quantum algorithm, and not just for Grover's algorithm. In particular, it shows that some natural approaches, like fault-tolerant quantum computation [14], cannot help in this setting. Note, however, that this impossibility result applies only in case that the oracle is truly a black-box oracle; if, instead, the oracle is given as a faulty circuit, then fault-tolerant schemes *can* be used to achieve a quantum speed-up by applying them to the circuit obtained by taking Grover's algorithm and replacing the oracle calls with their circuit implementation.

Related work: There has been a considerable amount of work dedicated to analyzing Grover's algorithm in all kinds of faulty settings (see, e.g., [15, 19, 18]). All these works concentrate on Grover's algorithm (or variants thereof) and none of them give a general statement that applies to all algorithms. In particular, Shenvi et al. [19] analyze the behavior of Grover's algorithm in a physically motivated model that is equivalent to ours. Our result answers the main open question presented in their paper.

There has also been a significant amount of work on searching with an imperfect, but still unitary, oracle (see, e.g., [6, 11, 7, 12, 20]). Such oracles are sometimes known as *noisy* oracles. The motivation for this model is algorithmic, and is related to what is known as amplitude amplification. Typically in this case, the quantum speed-up of $O(\sqrt{N})$ is still achievable. Very roughly speaking, this is because a unitary operation (even an imperfect one) is reversible and does not

lead to decoherence. There has also been some recent work on analyzing the case of an imperfect unitary implementation of Grover's algorithm (as opposed to an imperfect *oracle*) [16], again showing that a speed-up of $O(\sqrt{N})$ is achievable.

Open problems: One interesting open question is to extend our result to other physically interesting fault models. We believe that our proof technique should be applicable in a more general setting. One natural fault model suggested to us by Nicolas Cerf is the one in which each oracle query has probability p of turning the state into the completely mixed state. Also, is there *any* reasonable fault model for which a quantum speed-up *is* achievable? We suspect that the answer is no.

Another open question is to extend our result to other search problems (see [2] for a recent survey). Is there *any* search problem for which a quantum speed-up is achievable with a faulty oracle? Can one extend our lower bound to a more general lower bound in the spirit of the adversary method (see [1, 10])? It is also worth investigating whether the polynomial method [3] can be used to derive lower bounds in the faulty oracle case; our attempts to do so were unsuccessful. We should emphasize, however, that our faulty oracle model is not necessarily so natural for other search problems, and before approaching the above open questions, some thought should be given to the choice of the faulty oracle model.

2 Preliminaries

We assume familiarity with basic notions of quantum computation (see [17]).

Definition 1 (Grover oracle)**.** *For each $k \in \{1, \ldots, N\}$ where N is an integer, the* perfect oracle $\hat{O}^k$ *is the unitary transformation acting on an N-dimensional register that maps $|k\rangle$ to $-|k\rangle$ and $|i\rangle$ to $|i\rangle$ for each $i \neq k$, i.e.,*

$$\hat{O}^k = -|k\rangle\langle k| + \sum_{i \neq k} |i\rangle\langle i|.$$

We also extend the definition to $k = 0$ by defining $\hat{O}^0$ to be the 'null' oracle, given by the identity matrix I.

Definition 2. *The p-*faulty oracle O_p^k *is defined as the operation that with probability $1 - p$, acts as the perfect oracle $\hat{O}^k$ and otherwise does nothing, i.e., for any density matrix ρ,*

$$O_p^k(\rho) = (1 - p) \cdot \hat{O}^k \rho \hat{O}^{k\dagger} + p \cdot \rho.$$

We note that instead of our phase-flipping oracle, one could also consider a bit-flipping oracle. Since it is not difficult to construct the latter from the former (see, e.g., [13, Chapter 8]), our lower bound also applies to the bit-flipping case.

Definition 3. *Let $0 < p < 1$ be some constant. In the p-*faulty Grover problem*, we are given oracle access to the p-faulty oracle O_p^k for some unknown $k \in \{0, \ldots, N\}$ and our goal is to decide whether $k = 0$ or not with success probability at least $\frac{9}{10}$.*

Note that the choice of success probability is inconsequential, as one can easily increase it by repeating the algorithm a few times. Also note that we consider here the decision problem, as opposed to the search problem of recovering k from O_p^k. Since we are interested in lower bounds, this makes our result stronger.

3 Proof

We start by giving a brief outline of the proof. For simplicity, we consider the case $p = 1/2$. The proof starts with a simple, yet crucial, observation (Claim 2) which gives an alternative description of the faulty oracle. In the case $p = 1/2$, it says that the oracle O_p^k is essentially performing the two-outcome measurement given by $\{|k\rangle, |k\rangle^\perp\}$. Then, in Lemma 3, we 'approximate' the mixed states that arise during the algorithm with (unnormalized) pure states. This is done by assuming that the measurements done by the oracle all end up in the $|k\rangle^\perp$ subspace. The rest of the proof is similar in structure to previous lower bounds. Using the pure state description, we define a progress measure H_t^k, which is initially zero. We show that at the end of the algorithm it must be high (Lemma 4), and that it cannot increase by too much at each step (Lemma 5). This yields the desired lower bound on the number of queries T. We now proceed with the proof.

Let A be an algorithm for the p-faulty Grover problem on N elements that uses T queries. Assume the algorithm is described by the unitary operations $U_0, U_1, U_2, \ldots, U_T$ acting on an NM-dimensional system, composed of an N-dimensional query register used as oracle input, and an M-dimensional ancillary register. Let $\widetilde{\rho}_0$ denote the initial state of the system, which we assume without loss of generality to be a pure state $\widetilde{\rho}_0 = |\widetilde{\phi}_0\rangle\langle\widetilde{\phi}_0|$. For $k \in \{0, \ldots, N\}$, we let $\widetilde{\rho}_0^k = \widetilde{\rho}_0$, $\rho_0^k = U_0\widetilde{\rho}_0^k U_0^\dagger$, $\widetilde{\rho}_1^k = O_p^k(\rho_0^k)$, $\rho_1^k = U_1\widetilde{\rho}_1^k U_1^\dagger, \ldots, \rho_T^k = U_T\widetilde{\rho}_T^k U_T^\dagger$ be the intermediate states of the algorithm when run with oracle O_p^k (see Figure 1). In other words, ρ_t^k is the state of the system right after applying U_t, and $\widetilde{\rho}_{t+1}^k$ is the state of the system right after applying O_p^k on ρ_t^k.

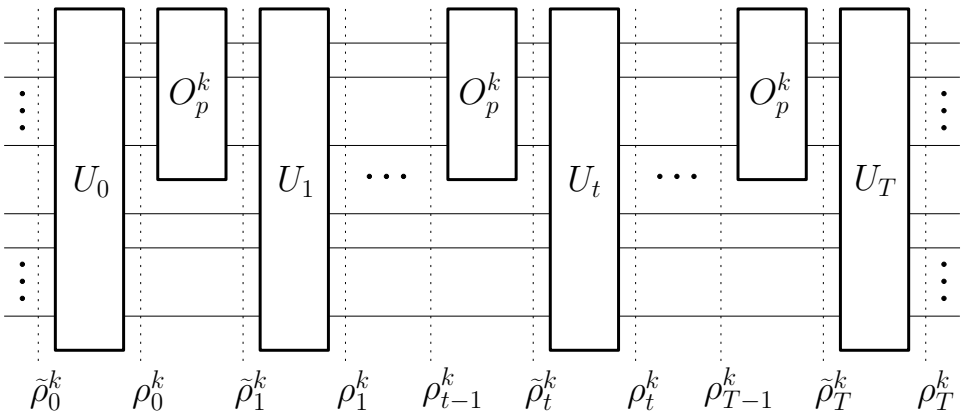

Figure 1: State evolution.

First we show a different way to decompose the outcome of O_p^k.

Claim 2. *Let $|\phi\rangle \in \mathbb{C}^{N\cdot M}$ be an arbitrary vector and let $|\beta_i\rangle \in \mathbb{C}^M$ be such that $|\phi\rangle = \sum_{i=1}^N |i, \beta_i\rangle$. Then*

$$O_p^k(|\phi\rangle\langle\phi|) = |\widetilde{\phi}\rangle\langle\widetilde{\phi}| + 4p(1-p)|k, \beta_k\rangle\langle k, \beta_k|$$

where

$$|\widetilde{\phi}\rangle := \sum_{i=1}^N |i, \beta_i\rangle - 2(1-p)|k, \beta_k\rangle.$$

Proof: By Definition 2 we have

$$O_p^k(|\phi\rangle\langle\phi|) = p|\phi\rangle\langle\phi| + (1-p)|\psi\rangle\langle\psi|$$

where $|\psi\rangle = \sum_{i\neq k} |i,\beta_i\rangle - |k,\beta_k\rangle$. Therefore

$$\begin{aligned}
O_p^k(|\phi\rangle\langle\phi|) &= \sum_{i\neq k}\sum_{j\neq k} |i,\beta_i\rangle\langle j,\beta_j| - (1-2p)\sum_{j\neq k}|k,\beta_k\rangle\langle j,\beta_j| - (1-2p)\sum_{i\neq k}|i,\beta_i\rangle\langle k,\beta_k| + |k,\beta_k\rangle\langle k,\beta_k| \\
&= \left(\sum_{i\neq k}|i,\beta_i\rangle - (1-2p)|k,\beta_k\rangle\right)\left(\sum_{j\neq k}\langle j,\beta_j| - (1-2p)\langle k,\beta_k|\right) \\
&\quad + (1-(1-2p)^2)|k,\beta_k\rangle\langle k,\beta_k|.
\end{aligned}$$

■

We will use the following vectors to track the progress of the algorithm.

Definition 4. *For $k \in \{0,\ldots,N\}$ and $t \in \{0,\ldots,T\}$ we define the vectors $|\phi_t^k\rangle, |\widetilde{\phi}_t^k\rangle \in \mathbb{C}^{N\cdot M}$ and $|\alpha_{t,i}^k\rangle \in \mathbb{C}^M$ as follows. First,*

$$\begin{aligned}
|\widetilde{\phi}_0^k\rangle &:= |\widetilde{\phi}_0\rangle, \\
|\phi_t^k\rangle &:= U_t|\widetilde{\phi}_t^k\rangle
\end{aligned}$$

and $|\alpha_{t,i}^k\rangle$ are given by

$$|\phi_t^k\rangle = \sum_{i=1}^N |i,\alpha_{t,i}^k\rangle.$$

Finally, for $k \in \{1,\ldots,N\}$ and $t \in \{0,\ldots,T-1\}$ we define

$$|\widetilde{\phi}_{t+1}^k\rangle := |\phi_t^k\rangle - 2(1-p)|k,\alpha_{t,k}^k\rangle = \sum_{i=1}^N |i,\alpha_{t,i}^k\rangle - 2(1-p)|k,\alpha_{t,k}^k\rangle$$

and for $k=0$ we define $|\widetilde{\phi}_{t+1}^0\rangle := |\phi_t^0\rangle$.

Lemma 3. *For all $t \in \{0,\ldots,T\}$ and $k \in \{1,\ldots,N\}$, we can write*

$$\rho_t^k = |\phi_t^k\rangle\langle\phi_t^k| + \sigma_t^k$$

for some positive semidefinite matrix σ_t^k.

Proof: Fix some $k \in \{1,\ldots,N\}$. The lemma clearly holds for $t=0$ (with $\sigma_0^k = 0$). Suppose the lemma holds for t and let us prove it for $t+1$. By the induction hypothesis,

$$\widetilde{\rho}_{t+1}^k = O_p^k(\rho_t^k) = O_p^k(|\phi_t^k\rangle\langle\phi_t^k|) + O_p^k(\sigma_t^k). \tag{1}$$

By Claim 2 and the definition of $|\widetilde{\phi}_t^k\rangle\langle\widetilde{\phi}_t^k|$

$$O_p^k(|\phi_t^k\rangle\langle\phi_t^k|) = |\widetilde{\phi}_{t+1}^k\rangle\langle\widetilde{\phi}_{t+1}^k| + 4p(1-p)|k,\alpha_{t,k}^k\rangle\langle k,\alpha_{t,k}^k|.$$

By combining this with Eq. (1) we get

$$\widetilde{\rho}_{t+1}^k = |\widetilde{\phi}_{t+1}^k\rangle\langle\widetilde{\phi}_{t+1}^k| + 4p(1-p)|k,\alpha_{t,k}^k\rangle\langle k,\alpha_{t,k}^k| + O_p^k(\sigma_t^k).$$

We apply U_{t+1} and obtain

$$\begin{aligned}\rho_{t+1}^k &= U_{t+1}\widetilde{\rho}_{t+1}^k U_{t+1}^\dagger \\ &= U_{t+1}|\widetilde{\phi}_{t+1}^k\rangle\langle\widetilde{\phi}_{t+1}^k|U_{t+1}^\dagger + U_{t+1}\left(4p(1-p)|k,\alpha_{t,k}^k\rangle\langle k,\alpha_{t,k}^k| + O_p^k(\sigma_t^k)\right)U_{t+1}^\dagger \\ &= |\phi_{t+1}^k\rangle\langle\phi_{t+1}^k| + U_{t+1}\left(4p(1-p)|k,\alpha_{t,k}^k\rangle\langle k,\alpha_{t,k}^k| + O_p^k(\sigma_t^k)\right)U_{t+1}^\dagger.\end{aligned}$$

The second term is clearly positive semidefinite, as required. ■

We now define our progress measure H_t^k.

Definition 5. *For $t \in \{0,\ldots,T\}$ and $k \in \{1,\ldots,N\}$ we define*

$$H_t^k := \left\||\phi_t^0\rangle - |\phi_t^k\rangle\right\|^2.$$

Notice that $H_0^k = 0$. The following lemma shows that at the end of the algorithm, the progress measure must be not too small. Intuitively, this holds since if H_T^k is small, then $|\phi_T^k\rangle$ is close to $|\phi_T^0\rangle$ and since the latter is a unit vector, the former must be of norm close to 1. This, in turn, implies that ρ_T^k is close to $|\phi_T^k\rangle\langle\phi_T^k|$, which is close to $|\phi_T^0\rangle\langle\phi_T^0| = \rho_T^0$ and thus the algorithm cannot distinguish between ρ_T^k and ρ_T^0 in contrast to our assumption about the algorithm. We proceed with the formal proof.

Lemma 4. *For all $k \in \{1,\ldots,N\}$, $H_T^k > \frac{1}{10}$.*

Proof: By our assumption on the correctness of the algorithm,

$$\begin{aligned}\frac{9}{10} \le \left\|\rho_T^k - \rho_T^0\right\|_{\mathrm{tr}} &= \left\|\rho_T^k - |\phi_T^0\rangle\langle\phi_T^0|\right\|_{\mathrm{tr}} \\ &\le \sqrt{1 - \langle\phi_T^0|\rho_T^k|\phi_T^0\rangle} \\ &= \sqrt{1 - \langle\phi_T^0|(|\phi_T^k\rangle\langle\phi_T^k| + \sigma_T^k)|\phi_T^0\rangle} \\ &\le \sqrt{1 - |\langle\phi_T^0|\phi_T^k\rangle|^2}\end{aligned}$$

where our definition of trace norm is normalized to be in $[0,1]$ and in the second inequality we used that for a (normalized) pure state $|\varphi\rangle$ and a mixed state ρ, we have $\|\rho - |\varphi\rangle\langle\varphi|\|_{\mathrm{tr}} \le \sqrt{1 - \langle\varphi|\rho|\varphi\rangle}$ (see, e.g., [17, Chapter 9]). Therefore,

$$\begin{aligned}H_T^k &= \left\||\phi_T^0\rangle - |\phi_T^k\rangle\right\|^2 \\ &= \langle\phi_T^0|\phi_T^0\rangle + \langle\phi_T^k|\phi_T^k\rangle - 2\mathrm{Re}(\langle\phi_T^0|\phi_T^k\rangle) \\ &\ge 1 - 2|\langle\phi_T^0|\phi_T^k\rangle| > \frac{1}{10},\end{aligned}$$

where the next to last inequality uses the fact that $\langle\phi_T^0|\phi_T^0\rangle = 1$ and $\langle\phi_T^k|\phi_T^k\rangle \ge 0$. ■

The following lemma bounds the amount by which the progress measure H_t^k can increase in each step.

Lemma 5. *For all $k \in \{1, \ldots, N\}$ and any $0 \leq t < T$,*

$$H_{t+1}^k - H_t^k \leq \frac{1-p}{p} \cdot \|\alpha_{t,k}^0\|^2.$$

Proof: By the definition of the progress measure,

$$\begin{aligned}
H_{t+1}^k &= \left\| |\phi_{t+1}^k\rangle - |\phi_{t+1}^0\rangle \right\|^2 \\
&= \left\| U_{t+1}|\widetilde{\phi}_{t+1}^k\rangle - U_{t+1}|\phi_t^0\rangle \right\|^2 \\
&= \left\| |\widetilde{\phi}_{t+1}^k\rangle - |\phi_t^0\rangle \right\|^2 \\
&= (\langle\phi_t^k| - 2(1-p)\langle k, \alpha_{t,k}^k| - \langle\phi_t^0|)(|\phi_t^k\rangle - 2(1-p)|k, \alpha_{t,k}^k\rangle - |\phi_t^0\rangle) \\
&= H_t^k - 4(1-p)\|\alpha_{t,k}^k\|^2 + 2(1-p)\langle\alpha_{t,k}^k|\alpha_{t,k}^0\rangle + 2(1-p)\langle\alpha_{t,k}^0|\alpha_{t,k}^k\rangle + 4(1-p)^2\|\alpha_{t,k}^k\|^2 \\
&\leq H_t^k - 4p(1-p)\|\alpha_{t,k}^k\|^2 + 4(1-p)\|\alpha_{t,k}^k\|\|\alpha_{t,k}^0\| \\
&\leq H_t^k + \frac{1-p}{p}\|\alpha_{t,k}^0\|^2
\end{aligned}$$

where the last inequality follows by maximizing the quadratic expression over $\|\alpha_{t,k}^k\|$. ∎

Theorem 1. *Any algorithm that solves the p-faulty Grover problem must use $T > \frac{p}{10(1-p)}N$ queries.*

Proof: By Lemma 5, for all $k \in \{1, \ldots, N\}$,

$$H_T^k \leq \frac{1-p}{p} \sum_{t=0}^{T-1} \|\alpha_{t,k}^0\|^2.$$

Since for any t, $|\phi_t^0\rangle$ is a unit vector,

$$\sum_{k=1}^{N} H_T^k \leq \frac{1-p}{p} \sum_{k=1}^{N} \sum_{t=0}^{T-1} \|\alpha_{t,k}^0\|^2 = \frac{1-p}{p}T.$$

To complete the proof, note that by Lemma 4, $\sum_{k=1}^{N} H_T^k > \frac{1}{10}N$. ∎

Acknowledgments

We thank Aram Harrow for presenting us with the faulty Grover problem and for useful discussions. We also thank Nicolas Cerf, Frédéric Magniez, and the anonymous referees for useful comments.

References

[1] A. Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the ACM Symposium on Theory of Computing*, pages 636–643, New York, 2000.

[2] A. Ambainis. Quantum search algorithms. *SIGACT News*, 35(2):22–35, 2004. quant-ph/0504012.

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

[4] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

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

[6] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum computation and information*, volume 305 of *Contemp. Math.*, pages 53–74. Amer. Math. Soc., Providence, RI, 2002.

[7] H. Buhrman, I. Newman, H. Röhrig, and R. de Wolf. Robust polynomials and quantum algorithms. *Theory Comput. Syst.*, 40(4):379–395, 2007. Preliminary version in STACS 2005.

[8] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the ACM Symposium on the Theory of Computing*, pages 212–219, 1996.

[9] A. Harrow. Personal communication, 2006.

[10] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proceedings of the ACM Symposium on the Theory of Computing*, pages 526–535, 2007. quant-ph/0611054.

[11] P. Høyer, M. Mosca, and R. de Wolf. Quantum search on bounded-error inputs. In *Proceedings of ICALP 2003*, volume 2719 of *Lecture Notes in Comput. Sci.*, pages 291–299. Springer, Berlin, 2003.

[12] K. Iwama, R. Raymond, and S. Yamashita. General bounds for quantum biased oracles. *IPSJ Journal*, 46(10):1234–1243, 2005.

[13] P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford University Press, Oxford, 2007.

[14] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279(5349):342–345, 1998.

[15] G. L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu. Dominant gate imperfection in Grover's quantum search algorithm. *Physical Review A*, 61:042305, 2000. quant-ph/9910076.

[16] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk. In *Proceedings of the ACM Symposium on the Theory of Computing*, pages 575–584, New York, 2007.

[17] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[18] D. Shapira, S. Mozes, and O. Biham. Effect of unitary noise on Grover's quantum search algorithm. *Phys. Rev. A*, 67(4):042301, 2003.

[19] N. Shenvi, K. R. Brown, and K. B. Whaley. Effects of a random noisy oracle on search algorithm complexity. *Phys. Rev. A*, 68(5):052313, 2003.

[20] T. Suzuki, S. Yamashita, M. Nakanishi, and K. Watanabe. Robust quantum algorithms with ϵ-biased oracles. In *Computing and combinatorics*, volume 4112 of *Lecture Notes in Comput. Sci.*, pages 116–125. Springer, Berlin, 2006.