数理解析研究所講究録 1426 巻 2005 年 219-224

Robust Quantum Algorithms for Oracle Identification

Kazuo Iwama[†,‡] Akinori Kawachi[*]
Rudy Raymond[†,‡] Shigeru Yamashita[§]

[†]Quantum Computation and Information Project, ERATO,
Japan Science and Technology Corporation (JST)
[‡]Graduate School of Informatics, Kyoto University
{iwama, raymond}@kuis.kyoto-u.ac.jp
[*] Graduate School of Information Science and Engineering, Tokyo Institute of Technology
kawachi@is.titech.ac.jp
[§]Graduate School of Information Science, Nara Institute of Science and Technology
ger@is.aist-nara.ac.jp

Abstract

The oracle identification problem (OIP) was introduced by Ambainis et. al. [4], which is given as a set S of M oracles and a hidden oracle f. Our task is to figure out which oracle in S is equal to the hidden f by doing queries to f. OIP includes several problems such as Grover Search as special cases. In this paper, we design *robust* algorithms, i.e., those which are tolerant against noisy oracles, for OIP. Our results include: (*i*) For any oracle set S such that $|S|$ is polynomial in N, $O(\sqrt{N})$ queries are enough to identify the hidden oracle, which is obviously optimal since this OIP includes Grover Search as a special case. (*ii*) For the case that $|S| \leq 2^{N^d}$ $(d < 1)$, we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$ and matches the lower bound proved in [4]. (*iii*) We can furthermore design a robust algorithm whose complexity changes smoothly between the complexity of (*ii*) and the complexity of recovering all information about the hidden oracle whose complexity is $O(N)$ as showed by Buhrman et. al. in [11]. Thus our new algorithms are not only robust but also their query complexities are even better than the previous noiseless case [4].

1 Introduction

When we solve some problem over an input data of N bits, $a_1, \ldots, a_n$, we usually need to know all the values of these N bits. This specific N-bit data are frequently called an *oracle* and we can get the value of bit a_i by making a query to the oracle by specifying the $(\log N)$-bit index i of the target bit. In the case of classical computation, we usually need all the N bits, which in turn forces us to make at least N queries to the oracle. (There are rare but interesting exceptions including [12].) By contrast, we need much fewer queries in the case of quantum computation. For instance, we need only $O(\sqrt{N})$ queries to find an index i such that $a_i = 1$ (Grover Search [17]). This is one of the major examples of quantum superiority.

Recently, two papers, by Høyer et. al. [20] and Buhrman et. al. [11], raised the question of how to cope with "imperfect" oracles for the quantum case. This question is not new in the classical case, where the natural model for such an oracle is the one which returns a wrong value (i.e., returns 0 when 1 is correct and vice versa) with some probability less than 1/2. Note that we can get all the values of N bit with high probability by querying each a_i $O(\log N)$ times instead of once. Thus, we can make any algorithm *robust*, i.e., resilient against imperfect oracles at the cost of an $O(\log N)$-factor overhead. In some cases, this factor of $O(\log N)$ is

actually needed: Feige et. al. [15] proved that any classical *robust* algorithm to compute the parity of the N bits needs $\Omega(N \log N)$ queries. On the other hand, the same paper also gives a non-trivial classical algorithm which computes OR of the N bits with $O(N)$ queries.

For the quantum setting, both papers [20, 11] are based on the following model: The oracle returns, for the query to bit a_i, a quantum pure state from which we can measure the correct value of a_i with a constant probability. This noise model naturally fits the motivation that a similar mechanism should apply when we use bounded-error quantum subroutines. In [20] Hoyer et. al. gave a quantum algorithm that robustly computes the Grover's problem with $O(\sqrt{N})$ queries, which is only a constant factor worse than the noiseless case. Buhrman et. al. [11] also gave a robust quantum algorithm to output all the N bits by using $O(N)$ queries. This obviously implies that $O(N)$ queries are enough to compute the parity of the N bits, which contrasts with the classical $\Omega(N \log N)$ lower bound mentioned earlier. Thus, robust quantum computation does not need a serious overhead at least for several important problems.

Now the natural question is whether this assersion is true more generally. Against this question, we study in this paper the *oracle identification problem* (OIP) introduced by Ambainis et. al. [4]. Recall that a single oracle is given as an N-bit string $f = a_1 \cdots a_N$. Let $f(i)$ denote a_i. Then the original Grover Search can be viewed as the following problem: Given the sets of N oracles $f_1, ..., f_N$ such that $f_i(j) = 1$ if $i = j$ and 0 otherwise, answer which oracle in S is now hidden in the black box through queries to the hidden oracle. As a natural generalization, the OIP is given as a set S of oracles which we know in advance and a hidden oracle f which we do not know in advance. Our task is to identify the oracle f, i.e., to decide which oracle in S is equal to f through queries to f. The Bernstein-Vazirani problem [6] is also an OIP, i.e., the set S now contains $f_1, ..., f_N$ such that $f_i(j) = i \cdot j$ (inner product modulo two). The problem of getting all the N bits is also an OIP where S consists of all the 2^N oracles. OIP can also be translated into problems in the learning theory as treated in, e.g., [16]. Thus OIP is quite general, for which Ambainis et. al. [4] proves that: (i) $O(\sqrt{N})$ queries are enough for *any* OIP if $|S| = N$. (ii) For the case that $|S| > N$, they obtained an $O(\sqrt{N \log M \log N} \log \log M)$ upper bound for its query complexity.

Our Contribution. This paper shows that we can design *robust* algorithms for (general) OIP which are mostly optimal. (i) If $|S|$ is polynomial in N, $O(\sqrt{N})$ queries are enough to identify the hidden oracle with high probability. This is obviously optimal within a constant factor since this problem includes Grover Search as a special case. (ii) If $|S| = M \leq 2^{N^d}$ for a constant d (< 1), $O(\sqrt{N \log M / \log N})$ queries are enough. Note that this bound matches the lower bound proven in [4]. (iii) For the range between (i.e., $2^{N^d} < |S| \leq 2^N$), we can design a robust algorithm whose query complexity changes smoothly between the bound in (ii) and the bound $O(N)$ in recovering all information of the hidden oracle.

Thus our new algorithms are not only robust but also their query complexity is even better than the previous noiseless case. They fully depend on the robust Grover Search by Hoyer et. al. but we also need a careful treatment of several parameter values troughout the algorithm. Thus our result is a yet another evidence claiming that Grover Search is really powerful if used repeatedly and carefully.

Previous Work. Quantum query complexity has been intensively studied as a central issue of quantum quantum computation. The most remarkable result is due to Grover [17], which provided a number of applications and extensions, e.g., [7, 8, 13, 18, 19]. Recently quite many results on efficient quantum algorithms are shown by sophisticated ways of using Grover Search. Brassard et. al. [9] showed a quantum counting algorithm that gives an approximate counting method by combining the Grover search with the quantum Fourier transformation. Quantum algorithms for the claw-finding and the element distinctness problems given by Buhrman et. al. [10] also exploited classical random and sorting methods with Grover Search. (Ambainis [3] developed an optimal quantum algorithm with $O(N^{2/3})$ queries for element distinctness problem, which makes use of quantum walk and matches to the lower bounds shown by Shi [23].) Ambainis and Aaronson [1] constructed quantum search algorithms for spatial regions by combining Grover Search with the divided-and-

conquer method. Magniez, Santha and Szegedy [22] showed efficient quantum algorithms to find a triangle in a given graph by using combinatorical techniques with Grover Search. Dürr, Heiligman, Høyer and Mhalla [14] also investigated quantum query complexity of several graph-theoretic problems. In particular, they exploited Grover Search on some data structures of graphs for their upper bounds.

2 Problem Formulation and Useful Tools

Before describing our results, we need some definitions and previous results which will be used in our algorithms.

Definition 1 *Oracle Identification Problem (OIP) is defined as follows.*

- **Input :** *A set $S = \{f_1, \ldots, f_M\}$ of oracles where each oracle f_i is a string of length N over $\{0,1\}$, and a black-box oracle $f \in S$ which is not known in advance.*
- **Output :** *Index i of the oracle $f_i \in S$ which is equal to the unknown f.*

Thus OIP is a premise problem for which the candidate set of oracles are known in advance. In this paper, we consider that the candidates are given as an $M \times N$ 0-1 matrix where the element at (i,j) denotes the value of $f_i(j)$. Namely, the i-th row corresponds to the f_i (the i-th oracle), and the j-th column corresponds to the output of oracles on input j. For short, we refer to the problem as $M \times N$ OIP.

Ambainis et. al. [4] previously considered OIP in the setting where oracles are perfect, i.e., the oracle f_i inside the black-box behaves according to the unitary matrix U_{f_i} such that:

$$U_{f_i} |x\rangle |0\rangle |0\rangle = |x\rangle |\phi_{i,x}\rangle |f_i(x)\rangle ,$$

where x in denotes the input to the oracle, and $|\phi_{i,x}\rangle$, the content of the working register after calling the oracle.

In this paper, we will be considering an imperfect oracle f_i where the corresponding unitary transformation is as follows.

$$U_{f_i} |x\rangle |0\rangle |0\rangle = \sqrt{p_x} |x\rangle |\phi_{i,x}\rangle |f_i(x)\rangle + \sqrt{1-p_x} |x\rangle |\psi_{i,x}\rangle |\neg f_i(x)\rangle ,$$

where $2/3 \leq p_x \leq 1$ denotes the probability that f_i returns the correct answer. This oracle is called *a biased oracle*. Although this error model cannot deal with all kinds of physical noises unlike the classical case, the model has been adopted in the literature. It is considered that any bounded error (quantum) algorithm can be formulated as this model. Indeed, [11, 20] used the same model as the one assumed in this paper.

Considering the OIP corresponding to Grover Search with an imperfect oracle, a straightforward algorithm would be by first amplifying the success probability of f_i on each input x to $1 - O(1/N)$ and then applying Grover Search on top of it. The amplification procedure costs $O(\log N)$ queries, therefore the total number of queries is $O(\sqrt{N} \log N)$. However, Høyer et. al. [20] showed a robust quantum algorithm which is worse only by a constant factor compared to the original Grover Search. Their result is summarized in the following lemma.

Lemma 1 (Robust Quantum Search [20]) *Given a quantum algorithm A with input $i \in \{1, \ldots, N\}$ such that*

$$A |i\rangle |0\rangle |0\rangle = \sqrt{p_i} |i\rangle |\phi_i\rangle |b_i\rangle + \sqrt{1-p_i} |i\rangle |\psi_i\rangle |\neg b_i\rangle ,$$

where $b_i \in \{0,1\}$ and $2/3 \leq p_i \leq 1$, there exists a quantum algorithm outputting j such that $b_j = 1$ (when there is such b_j) with probability more than $2/3$ and the algorithm uses $O(\sqrt{N})$ queries to A.

Furthermore, when the number of i such that $b_i = 1$ is t, the above query complexity can be reduced to $O(\sqrt{N/t})$ by modifying the algorithm as done in [8]. We refer to this modified algorithm as *Multi-Target Robust Quantum Search*.

Buhrman et. al. [11] showed a robust quantum algorithm which retrieves all the values of the imperfect quantum algorithms with $O(N)$ queries. In this paper, we will use a modified version of their algorithm which is described as follows.

Lemma 2 (Robust Quantum Find-Ones Algorithm) *Given a quantum algorithm A with input $i \in \{1,\ldots,N\}$ such that*

$$A|i\rangle|0\rangle|0\rangle = \sqrt{p_i}|i\rangle|\phi_i\rangle|b_i\rangle + \sqrt{1-p_i}|i\rangle|\psi_i\rangle|\neg b_i\rangle,$$

where $b_i \in \{0,1\}$ and $2/3 \leq p_i \leq 1$, there exists a quantum algorithm outputting all the values of b_i with probability more than $2/3$ and the algorithm uses $O(\sqrt{Nt})$ queries of A if the number of i such that $b_i = 1$ is less than t.

3 Robust Quantum Algorithms for OIP

In this section we design three robust algorithms for the cases that the column size of the given matrix is small, medium and large. Before proving the theorems, we introduce some convenient techniques.

Column Flip. Suppose that Z is any $M \times N$ 0-1 matrix (a set of M oracles). Then any quantum computation for Z can be transformed into a quantum computation for an $M \times N$ matrix Z' such that the number of 1's is less than or equal to the number of 0's in every column. (We say that such a matrix is 1-*sensitive*.)

Row-Cover. *Row-Cover(Z,r)* is the basic procedure in our algorithms to construct a set T that covers at least $M/4$ rows of Z, if there exists such one. Note that T is constructed such that the new element added to it covers at least r part of uncovered ones in Z. Row-Cover could fail, i.e., it returns T which does not cover at least $M/4$ rows of Z; this case will be treated specifically in our algorithms. Note also that these procedures do not need any query to oracles.

We often use Robust Quantum Search (Lemma 1) to find an index k of the oracle and need to verify its value by $O(\log N)$ classical queries. This verification is formalized by *Majority(k,m,f)*, where m is the number of classical queries to the hidden oracle f on input k.

Now we are ready to introduce our results. The first algorithm is for the case that the matrix is small, i.e., when the number of possible oracles is poly(N). Due to the space limitation, we only give results without proving them. Interested readers are directed to quant-ph/0411204 for full details.

Theorem 1 *The $M \times N$ OIP can be solved with a constant success probability by querying the blackbox oracle for $O(\sqrt{N})$ times if $M = poly(N)$.*

Now we show the case for a larger range of M where we still have an optimal algorithm. For ease of notation, let us define $\log^{(n)} x = \log\log^{(n-1)} x$.

Theorem 2 *The $M \times N$ OIP can be solved with a constant success probability by querying the blackbox oracle for $O(\sqrt{N\frac{\log M}{\log N}})$ times if poly(N) $\leq M \leq 2^{N^d}$ for some constant d $(0 < d < 1)$.*

Next, we consider the case when $M > 2^{N^d}$. Note that when $M = 2^{d'N}$, for a constant d' less or equal to 1, the lower bound of the number of queries is $\Omega(N)$ instead of $\Omega(\sqrt{N\log M/\log N})$. Therefore, it is natural to expect the increase on the number of queries as M becomes close to $2^{d'N}$. Indeed, when poly(N) $< M < 2^{N/\log^3 N}$, the number of queries of ROIPL is bigger than $O(\sqrt{N\log M/\log N})$ but still better than $O(N)$.

Corollary 1 *The $M \times N$ OIP can be solved with a constant success probability by querying the blackbox oracle for $O(\frac{\sqrt{N\log N\log M}}{\log\frac{2N}{\log M(\log^{(2)} M)^2\log N}})$ times if $2^{N^d} \leq M \leq 2^{N/\log^3 N}$.*

Remarks. The query complexity of the above corollary changes smoothly from $O(\sqrt{\frac{N\log M}{\log N}})$ when $M = 2^{N^d}$ to $O(N/\log N)$ when $M = 2^{N/\log^3 N}$.

What can be expected when $M \geq 2^{N/\log^3 N}$? Assume that we can design an algorithm such that at each round the Grover Search spends a constant number of queries to reduce the size of the oracle candidate set by at least 1/4 fraction. Since the success probability of the Grover Search is only guaranteed to be constant, it has to be repeated for $O(\log N)$ times at each round. Therefore, this procedure, which is used in ROIPS, ROIPM and ROIPL, needs at least $O((O(1) + \log N) \cdot \log N \cdot \log M)$ number of queries, where the first $\log N$ comes from the queries used in Majority and the second one from the repetition of the Grover Search to boost the success probability. Therefore, we can only expect the algorithm using this procedure to be more efficient than (the worst case of) Robust Quantum Find-Ones Algorithm when $M < 2^{N/\log^2 N}$.

Indeed, we can design a more efficient algorithm when $2^{N/\log^3 N} \leq M < 2^{N/\log^2 N}$ as shown in the following theorem.

Theorem 3 *The $M \times N$ OIP can be solved with a constant success probability by querying the blackbox oracle for $O(N/\log^\delta N)$ times if $2^{N/\log^3 N} \leq M = 2^{N/\log^{2+\delta} N} \leq 2^{N/\log^2 N}$.*

4 Concluding Remarks

We have showed that for a large range of $\text{poly}(N) \leq M \leq 2^{N^d}$, we can construct an optimal algorithm to identify the hidden oracle. This results matches the lower bound showed in [4]. Moreover, from the quantum learning point of view, our results answer affirmatively the question posed by Hunziker et.al. [21] who conjectured that there is a quantum learning algorithm which learns any concept class of size M with at most $O(\sqrt{M})$ queries. In fact, our algorithms are much better for large M and resilient to error. It should also be noted that independent to our work, Atici and Servedio [5] showed a quantum algorithm, which resembles ROIPS, for resolving another conjecture in [21] .

The next interesting topics are, e.g., to extend the range of M to get the optimal algorithms and to design algorithms which are not only have small query complexities but also small circuits or execution time.

References

[1] S. Aaronson and A. Ambainis. Quantum search of spatial regions. In *Proceedings of the 44th Symposium on Foundations of Computer Science*, pages 200-209, 2003.

[2] M. Adcock and R. Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science*, LNCS 2285, pages 323-334, 2002.

[3] A. Ambainis. Quantum walk algorithm for element distinctness. In *Proceedings of the 45th Symposium on Foundations of Computer Science*, pages 22-31, 2004.

[4] A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R. H. Putra, and S. Yamashita. Quantum identification of boolean oracles. In *Proceedings of the 21st Annual Symposium on Theoretical Aspects of Computer Science*, LNCS 2996, pages 105-116, 2004.

[5] A. Atici and R. A. Servedio. Improved Bounds on Quantum Learning Algorithms. arXiv:quant-ph/0411140

[6] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[7] D. Biron, O. Biham, E. Biham, M. Grassl, and D. A. Lidar. Generalized Grover Search Algorithm for Arbitrary Initial Amplitude Distribution. In *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication, LNCS, Vol. 1509, Springer-Verlag*, pages 140–147, 1998.

[8] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, vol. 46(4-5), 493-505, 1998.

[9] G. Brassard, P. Høyer, M. Mosca, A. Tapp. Quantum Amplitude Amplification and Estimation. In *AMS Contemporary Mathematics Series Millennium Volume entitled "Quantum Computation & Information"*.

[10] H. Buhrman, C. Dürr, M. Heiligman, P. Høyer, F. Magniez, M. Santha and R. de Wolf. Quantum Algorithms for Element Distinctness. In *Proceedings of the 16th IEEE Annual Conference on Computational Complexity (CCC'01)*, pages 131–137, 2001.

[11] H. Buhrman, I. Newman, H. Röhrig, and R. de Wolf. Robust quantum algorithms and polynomials. LANL preprint, http://xxx.lanl.gov/archive/quant-ph/0309220, 2003. To appear in *STACS* 2005.

[12] B. Chazelle, D. Liu and A. Magen. Sublinear geometric algorithms. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, 531-540, pages 531-540, 2003.

[13] D. P. Chi and J. Kim. Quantum Database Searching by a Single Query. In *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication, LNCS, Vol. 1509, Springer-Verlag*, pages 148–151, 1998.

[14] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum query complexity of some graph problems. In *Proceedings of the 31st International Colloquium on Automata, Languages and Programming*, LNCS 3142, pages 481-493, 2004.

[15] U. Feige, P. Raghavan, D. Peleg, and E. Upfal. Computing with noisy information. *SIAM Journal on Computing*, 23(5):1001–1018, 1994.

[16] S. Gortler and R. Servedio. Quantum versus classical learning learnability. In *Proceedings of the 16th Annual Conference on Computational Complexity*, pages 138-148, 2001.

[17] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th ACM Symposium on Theory of Computing*, pages 212–218, 1996.

[18] L. K. Grover. A framework for fast quantum mechanical algorithms. In *Proceedings of the 30th ACM Symposium on Theory of Computing*, pages 53–62, 1998.

[19] L. K. Grover. Rapid sampling through quantum computing. In *Proceedings of the 32th ACM Symposium on Theory of Computing*, pages 618–626, 2000

[20] P. Høyer, M. Mosca, and R. de Wolf. Quantum search on bounded-error inputs. In *Proceedings of the 30th International Colloquium on Automata, Languages and Programming*, LNCS 2719, pages 291–299, 2003.

[21] M. Hunziker, D. A. Meyer, J. Park, J. Pommersheim and M. Rothstein The Geometry of Quantum Learning. arXiv:quant-ph/0309059, to appear in Quantum Information Processing

[22] F. Magniez, M. Santha and M. Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms*, 2005. To appear.

[23] Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. In *Proceedings of the 43rd IEEE Symposium on the Foundation of Computer Science*, pages 513–519, 2002.