Quantum Complexity of Noisy IP Query

Kazuo Iwama, Rudy Raymond H.P., Shigeru Yamashita[†] and Tomoyuki Yamakami[‡]
Graduate School of Informatics, Kyoto University/ERATO
{iwama,raymond}@kuis.kyoto-u.ac.jp
[†]NTT/ERATO
[†]ger@kuis.kyoto-u.ac.jp
[‡]Ottawa University
[‡]yamakami@site.uottawa.ca

Abstract

The Goldreich Levin (GL) problem asks to find a from a noisy Inner Product (IP) oracle with bias ϵ and an exact Equality (EQ) oracle which are correlated with a. An interesting question arises on whether we can solve the GL problem without EQ queries. However, it has been known that using IP queries alone, the GL problem cannot be solved in the sense that the solution a is not unique. Here, we investigate the noisy IP problem, that is, given a noisy IP oracle our task is to find all a which are correlated with the noisy IP oracle within bias ϵ. We define *strong solvability* for List Decoding Problem of parity coding and prove its lower bound. This also implies the lower bound of any algorithm which uses *strong solvability* to solve the GL problem.

1 Introduction

The GL problem is given as the following. Let a be a binary string in $\{0,1\}^n$ and ϵ be a positive real number. Let information about a be available only from inner product (IP) and equivalence (EQ) queries. However, the IP query is known to return the correct answers on at least $(\frac{1}{2}+\epsilon)$ of its domain. The task is to determine a.

If $\epsilon = \frac{1}{2}$, a can be determined classically by querying e_i for $i = 1, 2, \ldots, n$, where e_i correspond to string with 1 on the i-th position and 0 elsewhere. This implies that classically it makes n IP queries. On the other hand, Deutsch and Jozsa showed a quantum algorithm which only needs 2 IP queries.

When ϵ is small, Goldreich and Levin implicitly showed classically how to solve this problem with a number of queries and auxiliary operations that is polynomial in n/ϵ. Adcock and Cleve [AC02] also showed that any classical algorithm solving the GL problem with constant probability must use $\Omega(n/\epsilon^2)$ queries. They also showed a quantum algorithm that only makes $O(1/\epsilon)$ queries of the quantum IP and EQ oracles.

Their algorithm uses amplitude amplification method proposed by Brassard et al. That is, they first construct an algorithm $\mathcal{A}$, which only makes IP queries, and apply EQ queries to amplify the amplitude of a in $\mathcal{A}$'s output. Thus, their algorithm is the series of alternating $\mathcal{A}$ and EQ.

Our research is concerned with the number of IP queries in $\mathcal{A}$, that is, the lower bound of IP queries in order to guarantee $\mathcal{A}$ to output a with probability δ. Therefore, it also implies a lower bound for the case when EQ queries are used only in amplitude amplification scheme, such as the one in [AC02]

2 Definitions and Preliminaries

2.1 Inner Product

The definition of classical inner product is given as follows.

Definition 1 *A classical inner product (CIP) oracle with bias ϵ is defined to have input $x \in \{0,1\}^n$ and output a bit $CIP(x)$, where $CIP(x)$ is slightly correlated with $a \cdot x$ s.t.*

$$Prob_x[CIP(x) = a \cdot x] \geq \frac{1}{2} + \epsilon,$$

where the probability is with respect to the uniform distribution.

Note that the above definition includes the case when CIP always returns the false answer for a particular x. Thus, we cannot amplify the success probability for a particular x by repeating queries. Here $a \cdot x = (\sum_i a_i x_i) \bmod 2$, where a_i is the i-th bit of a.

On the other hand, the quantum inner product is defined in [AC02] as follows.

Definition 2 *A quantum inner product (QIP_a) oracle with bias ϵ is defined to have input $x \in \{0,1\}^n$ and some ancilla qubits $|0^m\rangle$ such that*

$$U_{QIP_a} |x\rangle |0^m\rangle = |x\rangle (\alpha_x |v_x\rangle |a \cdot x\rangle + \beta_x |w_x\rangle |\overline{a \cdot x}\rangle),$$

where U_{QIP_a} denotes the unitary transformation of QIP_a, while α_x and β_x are non-negative real numbers. Furthermore, the probability of observing $a \cdot x$ on input x must be equal or more than $\frac{1}{2} + \epsilon$, namely,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \alpha_x^2 \geq \frac{1}{2} + \epsilon.$$

In this paper, we only consider the special case when IP queries have $\alpha_x, \beta_x \in \{0,1\}$, i.e., whether the oracle always returns the right answer for a particular x or always the wrong one.

2.2 Strong Solvability

For any two functions f and g, the error rate is defined as

$$error(f,g) = Prob_x[f(x) \neq g(x)].$$

Let f_a be the inner product function defined as $f_a(x) = a \cdot x$. Clearly, the set of all IP oracles with bias ϵ and $\alpha_x, \beta_x \in \{0,1\}$ is the same with the set F of all Boolean functions with domain $x \in \{0,1\}^n$ such that for any f in F, there exists an f_a satisfying

$error(f_a, f) \leq (\frac{1}{2} - \epsilon)$. However, for a Boolean function f which satisfies $error(f, f_a) \leq (\frac{1}{2} - \epsilon)$, the number of such a could be as large as $O(\frac{1}{\epsilon^2})$.

We define *the noisy IP problem* as follows. Given a noisy IP oracle (denoted by f) with bias ϵ, our task is to determine all a that satisfy $error(f, f_a) \leq \frac{1}{2} - \epsilon$. Strong solvability is defined as follows.

Definition 3 ***Strong Solvability*** *A quantum algorithm $\mathcal{A}$ strongly solves the noisy IP problem using QIP_a with probability $O(\delta)$ iff given QIP_a,ϵ and n, $\mathcal{A}$ halts in a final superposition $|\psi\rangle (\sum_{b \in A} |b\rangle |\xi_b\rangle + \sum_{c \notin A} |c\rangle |\xi_c\rangle)$ such that for any $b \in A$, $||\xi_b\rangle| = c'_b\sqrt{\delta}$ and $\sum_{c \notin A} ||\xi_c\rangle|^2 = o(\delta)$, where $A = \{a|\ error(f_a, QIP_a) \leq \frac{1}{2} - \epsilon\}$ and c'_b is some constant.*

3 Lower Bound of Strong Solvability

The following theorem is by [Amb00].

Theorem 1 *Let $f(x_1, x_2, \ldots, x_N)$ be a function of $N\{0,1\}$-valued variables and X, Y be two sets of inputs such that $f(x) \neq f(y)$ if $x \in X$ and $y \in Y$. Let $R \subset X \times Y$ be such that*

1. *For every $x \in X$, there exist at least m different $y \in Y$ such that $(x, y) \in R$.*
2. *For every $y \in Y$, there exist at least m' different $x \in X$ such that $(x, y) \in R$.*
3. *For every $x \in X$ and $i \in \{1, 2, \ldots, N\}$, there are at most l different $y \in Y$ such that $(x, y) \in R$ and $x_i \neq y_i$.*
4. *For every $y \in Y$ and $i \in \{1, 2, \ldots, N\}$, there are at most l' different $x \in X$ such that $(x, y) \in R$ and $x_i \neq y_i$.*

Then, any quantum algorithm computing f uses $\Omega(\sqrt{\frac{mm'}{ll'}})$ queries.

To solve the noisy IP problem, we need an $\mathcal{A}$ which strongly solves the noisy IP problem. Using Theorem 1, we obtain the following lemma.

Lemma 1 *Let $f : \{0, 1, \ldots, N-1\} \rightarrow \{0, 1\}$ be a Boolean function which is guaranteed to be either :*

1. *$f(x)$ is equal to 0 at exactly $\frac{N}{2}$ points and there exists at least one $b \in \{0,1\}^n$ such that $error(f, f_b) \leq (\frac{1}{2} - \epsilon)$ or*
2. *$f(x)$ is equal to 0 at exactly $N(\frac{1}{2} + \epsilon)$ points.*

Then, any quantum algorithm that determines whether the number of points where $f(x) = 0$ is $\frac{N}{2}$ or $N(\frac{1}{2} + \epsilon)$ uses $\Omega(\frac{1}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$ queries.

Regarding *strong solvability* of the noisy IP problem, we obtain the following theorem.

Theorem 2 *Any quantum algorithm that strongly solves the noisy IP problem with probability δ uses $\Omega(\frac{\sqrt{\delta}}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$ queries.*

Proof Sketch By Lemma 1 and contradiction. Suppose we have an algorithm $\mathcal{A}$ which only makes $o(\frac{\sqrt{\delta}}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$ IP queries to strongly solve the noisy IP problem with probability $O(\delta)$. Then, we can use $\mathcal{A}$ to decide whether the function f in Lemma 1 is equal to 0 at $N/2$ or at $N(\frac{1}{2} + \epsilon)$ points with query complexity $o(\frac{1}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$.

Note that if f in Lemma 1 is 0 at $N/2$ points then if we apply $\mathcal{A}$ to f, the amplitude of $|0\rangle$ in $\mathcal{A}$'s output will be strictly less than $o(\sqrt{\delta})$. On the other hand, if f is 0 at exactly $N(\frac{1}{2}+\epsilon)$ points, then the amplitude of $|0\rangle$ in $\mathcal{A}$'s output will be $O(\sqrt{\delta})$. Thus, using $EQ_0 = I - 2|0\rangle\langle 0|$, we can use the amplitude amplification and finally observe the state $|0\rangle$ to determine the number of 0 points in f. If f is 0 at $N(\frac{1}{2} + \epsilon)$ points then after applying amplitude amplification with EQ_0 $O(\frac{1}{\sqrt{\delta}})$ times, $|0\rangle$ is observed with constant probability. This implies the existence of an algorithm which uses $o(\frac{1}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$ queries and contradicts with the result in Lemma 1. ■

4 Discussion and Concluding Remarks

We have shown that for any algorithm which strongly solves the noisy IP problem makes $\Omega(\frac{\sqrt{\delta}}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$ queries. Thus, if such algorithm is used to solve the GL problem in amplitude amplification scheme, totally it makes $\Omega(\frac{1}{\epsilon} \cdot (\frac{1-10\epsilon+\frac{4}{N}}{3})^{\epsilon N/2})$ IP queries and $\Omega(\frac{1}{\sqrt{\delta}})$ EQ queries.

However, we do not need such a strong solvability algorithm to solve the GL problem. In fact, $\mathcal{A}$ that weakly solves the noisy IP problem with probability $O(\delta)$ makes the same $O(\frac{1}{\sqrt{\delta}})$ EQ queries while it probably makes less IP queries. It is our next topic to explore the property of $\mathcal{A}$ that weakly solves the noisy IP problem.

It should also be noted that the problem in Lemma 1 can be shown to have an upper bound of $O(\frac{1}{\epsilon})$ using the algorithm in [AC02]. Thus, there is still a gap between the lower bound in Lemma 1 with the currently known upper bound.

References

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In *STACS*, 2002. See quant-ph/0108095.

[Amb00] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of STOC*, pages 636–643, 2000. Its journal version at http://www.cs.berkeley.edu/~ambainis.