社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－AL－96 (1)
2004／7／27

オラクル同定問題に対する頑健な量子アルゴリズム

河内 亮周*†, 山下 茂‡, 岩間 一雄*†
* 京都大学大学院 情報学研究科
† 独立行政法人 科学技術振興機構 今井量子計算機構プロジェクト
‡ 奈良先端科学技術大学院大学 情報科学研究科

要旨 オラクル同定問題とは n ビット入力1ビット出力のオラクルの集合 $S = \{f_1, ..., f_M\}$ と S に属する未知のオラクル f_i が与えられたとき，未知のオラクル f_i を S の中から同定する問題であり，数多くの問題の一般化になっている．本稿では，与えられた未知のオラクルクエリーの結果が正しい値と誤った値が重ね合わせ状態として出力される場合のオラクル同定問題（但し，誤った計算結果が得られる確率は1/2より小さい定数確率，例えば1/10以下とする.）に対して以下を示す．(i) 与えられたオラクル集合のサイズが $N = 2^n$ の場合（すなわち $M = N$.），エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N})$ で少なくとも定数確率で解く量子アルゴリズムが構成できる．(ii) 与えられたオラクル集合のサイズが N の場合，各 $x \in \{0,1\}^n$ で $f_i(x) = 1$ を満たす i の数に関するパラメータ K に関してある条件を満たすとき，エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N/K})$ で少なくとも定数確率で解く量子アルゴリズムが構成できる．

Robust Quantum Algorithms for Oracle Identification

Akinori Kawachi*†, Shigeru Yamashita‡, Kazuo Iwama*†
*School of Infomatics, Kyoto University, Kyoto, Japan
†Graduate School of Information Science,
Nara Institute of Science and Technology, Nara, Japan
‡Quantum Computation and Information Project, ERATO,
Japan Science and Technology Agency

Abstract The oracle identification problem (OIP) is, given an oracle $f_i : \{0,1\}^n \to \{0,1\}$ and a candidate set $S = \{f_1, ..., f_M\}$, to determine which oracle in S is given. In this paper, we consider an oracle that outputs a superposition of the correct and the incorrect values, where the probability of measuring the incorrect value is a constant less than 1/2. For this OIP, we show that (i) if $|S| = N(= 2^n)$, i.e., $M = N$, then we can construct a robust quantum algorithm for the OIP by $O(\sqrt{N})$ queries with at least constant probability, and (ii) if $|S| = N$ and S satisfies a certain condition of a parameter K that depends on the number of i's such that $f_i(x) = 1$ for every $x \in \{0,1\}^n$, then we can construct a robust quantum algorithm for the OIP by $O(\sqrt{N/K})$ queries with at least constant probability.

1 はじめに

Høyer らは，以下のようなアルゴリズム的なエラーに対して頑健な量子探索アルゴリズムを構成した [6]．彼らのアルゴリズムは，N 個の量子アルゴリズム $A_1, ..., A_N$（計算結果は 0 または 1 となるサブルーチン）が与えられた時に，その中から 1 を出力する A_i を $O(\sqrt{N})$ 回の A_i の呼び出し（クエリー）により，高い確率で発見するものである．

ここで，A_i は誤りを含む量子アルゴリズムであり，正しい解を返す確率は 1 ではない．つまり，古典計算における確率アルゴリズムに相当する量子アルゴリズムで，その計算結果は正しい計算結果と誤った計算結果が量子的な重ね合わせ状態となっているものである．(ここで誤った計算結果が得られる確率は $1/2$ より小さい定数確率とする．以下同様とする.)

古典計算では，同じ設定の場合には，素朴なアルゴリズムを用いた場合，入力アルゴリズムのエラーを減らすために $O(\log N)$ の余分な繰り返し回数が必要となるため，誤り確率が $1/2$ より小さい定数確率の場合には全体では $O(N \log N)$ 回のクエリーが必要となる．また量子計算においても Grover の探索アルゴリズム [5] を素朴に利用しただけでは $O(\sqrt{N} \log N)$ 回のクエリーが必要となり，やはりこの場合においても $O(\log N)$ の項が必要となってしまう．しかし，彼らの量子アルゴリズムは，サブルーチンのエラーを減らすための余分な繰り返しが不要であるということを意味している．(但しこの探索問題に関しては非自明な $O(N)$ の古典アルゴリズムが知られている [4]．)

さらに最近，Buhrman らは [6] のアルゴリズムを一般化して，エラー付きの $A_1, ..., A_N$ の出力を $O(N)$ 回呼ぶだけで，$A_1, ..., A_N$ の出力の任意の関数を計算することができる量子アルゴリズムを構成した [3]．一方古典ではエラー付きアルゴリズムの出力からパリティを少なくとも定数確率で正しく計算するためには，入力アルゴリズムを $\Omega(N \log N)$ 回呼び出さなければならないという結果が知られているため [4]，古典では達成できない高速化が量子アルゴリズムで達成できていることを意味する．

本稿ではさらに彼らの問題を一般化したオラクル同定問題 [1] について頑健なアルゴリズムの構成について議論する．オラクル同定問題とは n ビット入力 1 ビット出力のオラクルの集合 $S = \{f_1, ..., f_M\}$ と S に属する未知のオラクル f_i が与えられたとき，未知のオラクル f_i を S の中から同定する問題であり，例えば Grover 探索 [5] や Bernstein-Vazirani の問題 [2] といった量子計算で扱われている多くの問題の一般化になっていることが知られている．

このオラクル同定問題で与えられる未知のオラクルが Høyer らのエラー付きモデルで与えられるとした場合に対して，本稿では以下の二つの量子アルゴリズムを示す．(i) 与えられたオラクル集合のサイズが $N = 2^n$ の場合（すなわち $M = N$.），エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N})$ で少なくとも定数確率で解く量子アルゴリズムが構成できる．(ii) 与えられたオラクル集合のサイズが N の場合，各 $x \in \{0,1\}^n$ で $f_i(x) = 1$ を満たす i の数に関するパラメータ K に関してある条件を満たすとき，エラー付きオラクル同定問題をクエリー回数 $O(\sqrt{N/K})$ で少なくとも定数確率で解く量子アルゴリズムが構成できる．

なお，エラー無しオラクルで $|S| = N$ の場合でも $\Theta(\sqrt{N})$ 回のクエリーの最適な量子アルゴリズムが知られており [1]，本稿の結果はエラー付きオラクルの場合でもその定数倍程度の

クエリー回数の増加で済むような頑健な量子アルゴリズムを示していることになる.

2 準備

本節では，本稿に必要な概念である，エラーを持つ量子オラクルのモデルおよびオラクル同定問題のそれぞれの定義を述べる.

2.1 エラーを持つ量子オラクル

Høyer らは実質的に以下のような「エラーを持つオラクル」に対して定義された探索問題をエラー無しの場合の定数倍程度のクエリー回数により定数確率で解を発見する頑健な量子探索アルゴリズムを示している [6].

エラー付き探索問題

入力： N 個の以下の条件を満たす量子アルゴリズム $A_1, ..., A_N$:

$$A_i|0\rangle|0\rangle = \sqrt{p_x}|\phi_i\rangle|b\rangle + \sqrt{1-p_x}|\psi_i\rangle|\neg b\rangle .$$

ここで ϕ_i, ψ_i は A_i の計算過程のゴミ，b は A_i の正しい出力ビットを表し，定数 $1/2 < \varepsilon < 1$ に対して $1/2 + \varepsilon \leq p_x \leq 1$ である.

出力： 1 を高い確率で出力する量子アルゴリズム A_i のインデックス i.

通常，量子アルゴリズムは正しい計算結果と誤った計算結果を重ね合わせで出力することが一般的であるので，誤りを含むサブルーチンを利用する状況を考えればこのエラーモデルは自然であると言える.

2.2 オラクル同定問題

Grover の探索アルゴリズムなどのオラクルを用いて解く問題の一般化として，[1] では以下のような問題を定義し，それに対する効率の良いアルゴリズムを与えている.

オラクル同定問題

入力： M 個のオラクル集合 $S = \{f_1, ..., f_M\}$ とその中のオラクル $f_i : \{0,1\}^n \to \{0,1\}$, $f_i \in S$.

出力： オラクル f_i のインデックス i.

例えば解が一つの場合の探索問題，つまりオラクル $f_i(i) = 1, f_i(j) = 0\ (j \neq i)$ から i を求める問題 [5] はオラクル同定問題 EQ となり (図 1)，ビット毎の積の論理和（内積）$f_i(j) = i \cdot j$ から i を求める問題 [2] はオラクル同定問題 IP となる（図 2）. オラクル同定問題は，M 個のオラクルの動作がわかっているという条件で，ブラックボックスにその内の一つが隠されている時に，オラクルへのクエリーを用いてどのオラクルがブラックボックスに隠されているかを決定する問題である. これは，図 1 や図 2 のような $M \times N$ 行列 $(N = 2^n, N \leq M \leq 2^N)$ が与えられ、現在のオラクル（ブラックスボックスに隠されたオラクル）がどの行であるかを同定する問題と見ることもできる. そのため，以下では，「$M \times N$ 行列に対するオラクル同定問題」と呼ぶことにする.

3 $N \times N$ 行列に対する頑健なオラクル同定量子アルゴリズム

本節では，オラクル同定問おいて，オラクルが前節で定義したようなエラーを持つ場合に，

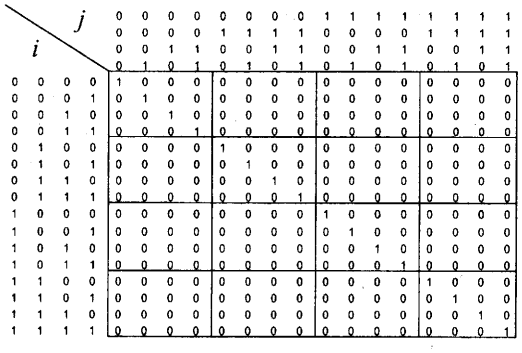

図 1: EQ $(f_i(j) = 1 \quad \text{iff} \quad i = j)$

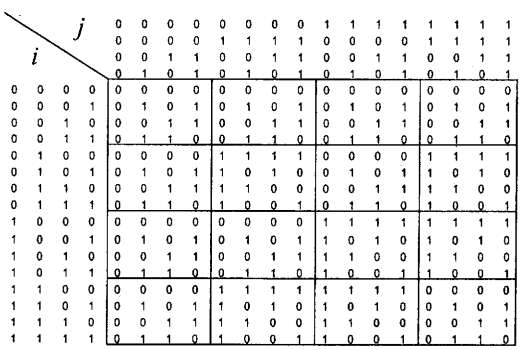

図 2: IP $(f_i(j) = i \cdot j = \sum_x i_x \cdot j_x \mod 2)$

エラー除去のために増加するクエリー回数が定数倍程度で済む量子アルゴリズムについて述べる．ここでは，$M = N$，すなわちオラクル候補の数がオラクル入力の長さと一致する場合を考える．(Grover の探索アルゴリズムの問題もこの場合に相当する.)

エラー付きオラクル同定問題

入力： M 個のオラクル集合 $S = \{f_1, ..., f_M\}$ とその中のある一つのオラクル $f_i \in S$ を計算するユニタリ変換 U_{f_i}:

$$U_{f_i} |x\rangle |0\rangle |0\rangle =$$

$$\sqrt{p_x} |x\rangle |\phi_i\rangle |f_i(x)\rangle + \sqrt{1-p_x} |i\rangle |\psi_i\rangle |\neg f_i(x)\rangle,$$

但しある定数 $0 < \varepsilon < 1/2$ に対して，$1/2 + \varepsilon \leq p_x^2 \leq 1$ である．

出力： オラクル f_i のインデックス i.

エラー無しの場合は [1] のアルゴリズムで $O(\sqrt{N})$ 回のオラクルクエリーにより解けることが知られている．しかし，このアルゴリズムは古典的なオラクルクエリーを数多く利用しているために単純に [6] のアルゴリズムを利用するするだけでは，$O(\log N)$ 倍のオラクルクエリーが避けられない．そのため，エラーがあるオラクルの同定問題をエラーのない場合に対して定数倍程度のクエリー回数の増加で解く量子アルゴリズムは自明でない．しかし，実際には以下の定理が成り立つ．

Theorem 3.1 $N \times N$ 行列に対するエラー付きオラクル同定問題を $O(\sqrt{N})$ 回のオラクルクエリーにより少なくとも定数確率で解くアルゴリズムが構成可能である．

Proof. まず最初に我々のアルゴリズムを述べる．

1. 以下の 2.–6. をオラクル候補 Z が一つになるまで繰り返す．最初 は Z を与えられた N 個のオラクル候補全てとする．

2. 以下の操作では，Z の各列に対して**列反転** (column flip)[1] を行う．ここで列反転とは Z の各列において，もし 1 が 0 の数より少なければ，その列の 0, 1 を反転し，そうでなければそのままにしておく，という操作である．この操作で各列での 1 の数が 0 の数よりも少ない行列として常に扱うようにする．(この操作にはクエリーを全く用いないことに注意する.)

3. 以下の 4. を選択された列によって**被覆**された行が $|Z|/3$ を超えるまで，あるいは選択する列がなくなるまで繰り返す．ここで列 j が行 i を被覆するとは $f_i(j) = 1$ を満たす，つまり i 行 j 列が 1 であることを意味する．最初，選択された列の集合 T は空集合とする．

4. T に属する列で被覆されていない行において 1 の数が最大の列を選び，T で被覆されてない行のうち $\sqrt{|Z|}/\log N$ 行を被覆しているならば，それを T に含める (図 3)．

5. T に属する列に対して [6] のアルゴリズムを $O(\log N)$ 回適用する．1 が発見できれば T が被覆する行を新たに Z とおいて 2. へ戻る．

6. 5. で 1 が発見できなかった場合，以下のいずれかを行なう．

6.a T で被覆する行数が $|Z|/3$ 以上だった場合，T が被覆する行を除外したものを新たに Z として 2. に戻る．

6.b T で被覆する行数が $|Z|/3$ 未満だった場合，T が被覆する行を除外した行列に対して 7.-9. を実行する．(なお，以下の処理は [1] の $N \times N$ 行列に対するアルゴリズムを素朴に頑健化したアルゴリズムである.)

7. T に属さない列に対して [6] のアルゴリズムを適用する．

8. T に被覆されていない列の中で，7. で得られた列に 1 を持つ行を選ぶ．選ばれた行の集合を S' とする．

9. T に被覆されていない列の中で，S' 中に 0 と 1 両方含んだ列を探し，$\log N$ 回の古典的クエリーでその列の値を決定し，その結果に矛盾する行を Z から削除する．7.–9. を $|Z| = 1$ になるまで繰り返す．

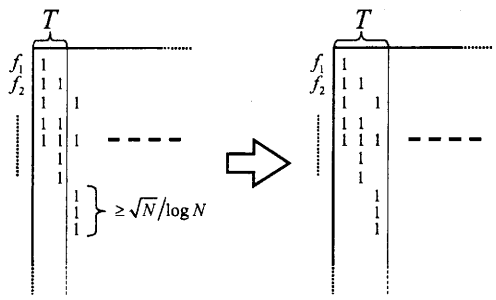

図 3: T の構成

上記のアルゴリズムに対して，オラクルのクエリー回数を評価する．5. で必要なクエリー回数は $O(\sqrt{|T|}\log N)$ であるが，$|T| \leq |Z|/(\sqrt{|Z|}/\log N) = \sqrt{|Z|}\log N$ より，5. で 1 が発見できた場合にはクエリー回数 $O(|Z|^{1/4}\log^{3/2} N)$ で確率 $1-O(1/N)$ でオラクル候補の総数を 1/2 以下に絞り込むことができることになる．一方，5. で 1 が発見できなかった場合には，確率 $1-O(1/N)$ 以上でオラクルは T に属さないことになる．従って，T が被覆する行数が $|Z|/3$ 以上だった場合には，オラクル候補の総数を 2/3 以下に絞り込むことができる．また，T が被覆する行数が $|Z|/3$ 未満だった場合には T で被覆された行を除外した後の各列に含まれる 1 の数が $\sqrt{N}/\log N$ という事実に注目すると 7.–9. で $\log N$ 回のクエリーをせいぜい $\sqrt{N}/\log N$ 回繰り返せばよい．よってこのときのクエリー回数は $O(\sqrt{N})$ 回である．従って全体でせいぜい $O(N^{1/4}\log^{5/2} N + \sqrt{N}) = O(\sqrt{N})$ のクエリー回数でオラクル同定が定数確率で可能である． □

4 $N \times N$ 行列の1の数とそのオラクル同定問題のクエリー回数

$N \times N$ 行列のオラクル同定問題に関して，行列の列方向の1の数の最大値を K とした時，オラクルがエラーを持たない場合には，オラクル同定に必要なクエリー数が $\Omega(\sqrt{N/K})$ であり，またほとんどの場合において $O(\sqrt{N/K})$ であることが示されている [1].

以下の定理は，オラクルがエラーを持つ場合においても，やはりほとんどの場合で，$O(\sqrt{N/K})$ でオラクル同定が可能であることを示している.

Theorem 4.1 $N \times N$ 行列に対するエラー付きオラクル同定問題に関して，与えられた行列の任意の行を N/K 以上選択して生成される行列の列方向の1の数の割合が K/N 以上かつ $1-K/N$ 以下ならば，$O(\sqrt{N/K})$ 回のクエリーでオラクル同定が可能である．ただし，任意の定数 $0 < \delta < 1$ に対して，$K < N^{\delta}$ とする.

Proof. まず最初に我々のアルゴリズムを述べる.

1. 以下の 2.–7. をオラクル候補 Z が一つの要素になるまで繰りす．最初は Z を与えられた N 個のオラクル候補全てとする.

2. 以下の操作では，Z の各列に対して列反転 [1] を行うことで各列での1の数が0の数よりも少ない行列として常に扱うようにする.

3. 以下の 4. を選択された列によって被覆された行が $|Z|/3$ を超えるまで，あるいは選択する列がなくなるまで繰り返す．ここで列 j が行 i を被覆するとは $f_i(j) = 1$ を満たす，つまり i 行 j 列が1であることを意味する．最初，選択された列の集合 T は空集合とする.

4. T に属する列で被覆されていない行において1の数が最大の列を選び，T で被覆されてない行のうち $\frac{K}{N \log^4 N}$ 以上の1の割合の行を被覆しているならば，それを T に含める.

5. T に属する列に対して [6] のアルゴリズムを $O(\log N)$ 回適用する．1が発見できれば T が被覆する行を新たに Z とおいて 2. へ戻る.

6. 5. で1が発見できなかった場合，以下のいずれかを行なう.

6.a T で被覆する行数が $|Z|/3$ 以上だった場合，T が被覆する行を除外したものを新たに Z として 2. に戻る.

6.b T で被覆する行数が $|Z|/3$ 未満だった場合，T が被覆する行を除外した行列の集合を Y として，7. 以下を行なう.

7. オラクルの1となっている列を [6] のアルゴリズムを用いて見つける．ここでそのような解の濃度が K/N 以上であると仮定して探索を行なう.

8. 7. で1が発見できれば，Y は列方向の1の数が $N\frac{K}{N}\log^4 N = K \log^4 N$ 以下になる．この発見された1の列に注目して，矛盾する行を候補から取り除き，Z を更新する．さらに Z 内のオラクル同定に不要な列を取り除くことで $|Z| \times |Z|$ 部分行列を作成し，以下のいずれかを行う.

8.a もし $|Z| \leq N/K$ ならば，この部分行列に定理 3.1 のアルゴリズムを適用する．

8.b もし $|Z| > N/K$ ならば，この部分行列にこのアルゴリズムの 2.–9. を再帰的に適用する．

9. 7. で 1 が発見できない場合は，定数確率で同定すべきオラクルの行方向の 1 の数が K 以下であると断定できる．この場合，問題の仮定よりそのようなオラクルの数は，N/K 以下なので，あとは N/K 以下の候補に対して，定理 3.1 のアルゴリズムを適用する．

上記のアルゴリズムに対して，オラクルのクエリー回数を評価する．5. で必要なクエリー回数は $O(\sqrt{|T|}\log N)$ であるが，$|T| \leq |Z|/(|Z| \times K/N\log^4 N) = \frac{N}{K\log^4 N}$ より，5. で 1 が発見できた場合にはクエリー回数 $O(\sqrt{\frac{N}{K\log^2 N}})$ で確率 $1 - O(1/N)$ でオラクル候補の総数を 1/2 以下に絞り込むことができることになる．一方，5. で 1 が発見できなかった場合には，確率 $1 - O(1/N)$ 以上でオラクルは T に属さないことになる．従って，T が被覆する行数が $|Z|/3$ 以上だった場合には，オラクル候補の総数を 2/3 以下に絞り込むことができる．また，T が被覆する行数が $|Z|/3$ 未満だった場合には，7. 以下の手順を行なうが，7., 8.a および 9. で必要なクエリー回数はそれぞれ，$O(\sqrt{N/K})$ となる．さらに 8.b により 1 回再帰的に呼ばれる毎に 8. で作成される部分行列の大きさは $\frac{K\log^4 N}{N}$ 倍以下になっているので，r 回呼ばれたときの部分行列のサイズはせいぜい $N\left(\frac{K\log^4 N}{N}\right)^r$ となる．この部分行列のサイズが N/K 以下になるには，定数 δ に対して $K < N^\delta$ より，繰り返し回数 r はせいぜい定数である．以上より，全体で必要なオラクルのクエリー回数は $O(\sqrt{N/K})$ となる． □

5 まとめと今後の方針

本稿では，オラクル同定問題 [1] に関して，オラクルがエラーを持つ場合について、$N \times N$ 行列の場合に対する頑健な量子アルゴリズを与えた．エラーがない場合の $N \times N$ のオラクル同定問題のアルゴリズム [1] は古典的なオラクルクエリーを一部で用いていたため，オラクルにエラーのある場合の量子探索アルゴリズム [6] を単純に利用することはできず，本稿で述べたようなアルゴリズム的な工夫により，定数倍程度のオーバーヘッドの量子アルゴリズムが構築できた．

一方で [1] における最も一般化された問題の $M \times N$ 行列に対する量子アルゴリズムは古典的オラクルクエリーを本質的に利用しておらず，Grover の探索アルゴリズムを用いている部分に関して [6] のアルゴリズムを利用するだけで定数倍程度のオーバーヘッドの頑健なアルゴリズムを構成できる．ただし，$M \times N$ 行列に対する [1] のアルゴリズムのクエリー回数は $O(\sqrt{N\log M\log N}\log\log M)$ であるため，例えば $2^N \times N$ の場合には $\log^2 N$ といった余分なクエリーを必要としており，この場合には [3] のアルゴリズムよりもクエリー回数が大きくなってしまう．従って今後の目標としてはエラー付きオラクルについて $M \times N$ 行列オラクル同定問題を解く $O(\sqrt{N\log M})$ のクエリー回数のアルゴリズムを設計することが挙げられる．この目標の達成は [1] の改良及び [3] の一般化アルゴリズムを与えることに相当する．

参考文献

[1] 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.

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

[3] 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.

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

[5] 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.

[6] 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.