修士論文

Grover アルゴリズムの最適性のより簡潔な証明

岡﨑 崚

主指導教員 藤﨑 英一郎

北陸先端科学技術大学院大学
先端科学技術研究科
（情報科学）

令和 6 年 3 月

Abstract

In recent years, there has been a lot of research on quantum computers. If a large-scale and error-correcting quantum computer is realized, many of the popular cryptosystems, such as RSA and elliptic curve cryptography, will be compromised. Therefore, it is important to consider quantum computers in cryptography.

In cryptography, the random oracle model is an idealized version of the cryptographic hash function, and is widely used to discuss the security of cryptographic schemes. In 2011, Boneh et al. proposed the quantum random oracle model, which is a quantum version of the random oracle model. The two differ in many points due to their quantum property. One of these is random oracle can easily record queries, whereas quantum random oracle are difficult to record queries. To address this problem, Zhandry proposed a way for quantum random oracle to record queries at CRYPTO 2019.

Zhandry introduces applications of quantum random oracle that can record queries, one of which is a proof of the optimality of Grover's algorithm. In this paper, we show that Zhandry's proof is simpler and easier to verify by transforming the oracle basis into a Fourier basis.

目次

第 1 章　序論

1.1　背景

近年，量子コンピュータに関する研究が盛んに行われている．量子コンピュータとは，量子の持つ性質を用いて情報処理を行う，従来のコンピュータ (古典コンピュータと呼ばれる) とは異なる動作原理のコンピュータである．現時点で実現されている量子コンピュータは NISQ(Noisy Intermediate-Scale Quantum Computer) と呼ばれるもので，量子誤り訂正をできない中規模なものである．一方で，量子誤り訂正を備えた量子コンピュータを FTQC(Fault-Tolerant Quantum Computer) といい，これは現時点において実現されていない．しかしながら，大規模な FTQC が実現された場合は様々な分野で大きな影響があると考えられている．その 1 つが暗号分野への影響である．例えば，Shor のアルゴリズム [Sho97] は FTQC 上で素因数分解問題や離散対数問題を入力長の 3 乗の多項式時間で解くことができるため，現在主流である RSA 暗号や楕円曲線暗号は危殆化し，利用できなくなる．このようなこともあり，暗号分野では量子コンピュータの実現を見据えた研究が盛んに行われている．

暗号理論においてランダムオラクルモデルとは，暗号学的ハッシュ関数を理想化したモデルであり，暗号方式の安全性を議論する際に広く用いられているモデルである．Boneh 等により提案された量子ランダムオラクルモデル (QROM)[BDF+11] は，ランダムオラクルモデル (ROM)[BR93] の量子版であり，攻撃者はランダムオラクルに量子クエリを質問できる．量子ランダムオラクルモデルは古典のランダムオラクルモデルと多くの点で異なり，古典では容易であったことがしばしば容易で無くなる．そのうちの一つがオラクル側にクエリを記録する問題である．その主な理由は量子状態の複製が不可能であること，また量子状態の観測は全体の系に変化を与えてしまうからである．この問題に対して，Zhandry はオラクル側がクエリを記録する方法をを示した [Zha19]．この手法は Zhandry の recording technique と呼ばれている．

Zhandry[Zha19] はクエリを記録できる QROM の応用を幾つか紹介しているが，その 1 つに Grover アルゴリズム [Gro96] の最適性の証明がある．これにより，従来の証明よりも簡潔かつ検証容易な証明ができる．

1.2 本研究の成果

本研究の成果は，オラクルの基底をフーリエ基底でみることにより定理 1.2.1 の証明がより簡潔かつ検証容易になることを示したことである．

クエリを記録できる QROM を用いて Grover アルゴリズムの最適性の証明をするには，任意の量子アルゴリズムで量子ランダムオラクルにクエリを q 回行い random function の逆像を求めるとき，その確率は最大で $O(q^2/N)$ であることを示せばよい (系 1.2.3)．この証明は定理 1.2.1 を示したのち，補題 1.2.2 を用いて系 1.2.3 を証明するという流れで行われる．

定理 1.2.1. 攻撃者がランダムオラクル cO に q 回クエリする状況を考える．q 回のクエリを行った後に D を測定するとき，$0^n \in D$ である確率は高々 $O\left(q^2/N\right)$ である．

補題 1.2.2 ([Zha19, Lemma 5])．ランダムオラクル H にクエリし，タプル $(x_1, \cdots, x_k, y_1 \cdots, y_k)$ を出力する量子アルゴリズム A を考える．R を前述したようなタプルの集合とする．A は確率 p で次のようなタプルを出力するとする．(1) 出力されたタプルが R に含まれる．(2) 任意の i に対して $H(x_i) = y_i$. いま A はオラクル cO にクエリし，タプルを出力した後に D が測定されるとする．p' を A が次のようなタプルを出力する確率とする．(1) 出力されたタプルが R に含まれる．(2) 任意の i に対して $D(x_i) = y_i$（ただし，$D(x_i) \neq \perp$）である．このとき，$\sqrt{p} \leq \sqrt{p'} + \sqrt{k/2^n}$ となる．

系 1.2.3. 攻撃者がランダムオラクルに q 回のクエリをした後にデータベースから 0 を見つけることができる確率は $O\left(q^2/N\right)$ である．

まず前提知識として，Grover アルゴリズムは関数の逆像を $O(\sqrt{N})$ のクエリ回数で高い確率で求める量子アルゴリズムであり，任意の関数の逆像を見つける問題はランダム関数の逆像を見つける問題に帰着できる．次に補題 1.2.3 は，量子アルゴリズム A が $H(x_i) = y_i$ を出力する確率 p は，データベースを測定して $D(x_i) = y_i$ となる確率 p' とほとんど変わらないことを意味している．定理 1.2.1 で示される確率は補題 1.2.2 の $p'(= O(q^2/N))$ に対応している．よって補題 1.2.2 より $p = O(q^2/N)$ となる．このことから系 1.2.3 が示される．Grover アルゴリズムのクエリ数は $O(\sqrt{N})$ であるため，系 1.2.3 より，これは最適なクエリ回数であることがわかる．

[Zha19] では random function と worst-case function の逆像を求める場合の難しさは等価であるから，この証明は worst-case についての証明になると主張している．しかし，それについては十分検証できなかったため本研究は average-case の最適性の証明とする．

第 2 章　準備

2.1　量子計算

この節では量子計算の基礎を紹介する．より詳しい内容については [NC11] を参照するとよい．

2.1.1　Dirac の記法

$|\psi\rangle \in \mathbb{C}^k$ は列ベクトルを表し，$\langle\psi| := |\psi\rangle^\dagger$ である．ただし，$\dagger$ は共役転置を取るという記号である．代表的なものとしては $|0\rangle, |1\rangle \in \mathbb{C}^2$ があり，次のように定義されている．

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

$|0\rangle, |1\rangle$ は $\mathbb{C}^2$ の正規直交基底ある．量子計算では $|0\rangle, |1\rangle$ を計算基底と呼ぶ．

$\langle\psi|\varphi\rangle$ は $|\psi\rangle, |\varphi\rangle$ の内積であり，$|\psi\rangle$ のノルムは $\| |\psi\rangle \| := \sqrt{\langle\psi|\psi\rangle}$ である．

2.1.2　量子ビット系

量子計算において古典ビットの $0, 1$ に対応するものが $|0\rangle, |1\rangle$ である．また $\mathbb{C}^2$ 上の単位ベクトルのことを量子ビットという．古典ビットは 0 か 1 の 2 状態しかとらないが，量子ビット $|\psi\rangle$ は計算基底を用いて以下のように書ける．これを重ね合わせ状態と呼ぶ．

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{2.2}$$

ただし，α, β は $|\alpha|^2 + |\beta|^2 = 1$ を満たす複素数である．

2.1.3　測定

量子ビットから物理量についての情報を得るためには測定と呼ばれる操作を行う必要がある．射影測定は最も一般的な測定方法であり次のように行われる．射影演算子の集合 $\{P_i\}_i$ は $\sum_i P_i = I$ を満たしている．このとき量子状態 $|\psi\rangle$ を測定し，測定値 m を得る確率 $p(m)$ は次のようになる．

$$p(m) = \| P_m |\psi\rangle \|^2 \tag{2.3}$$

例として $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ の測定を考える．射影演算子 $P_0 = |0\rangle\langle 0|, P_1 = |1\rangle\langle 1|$ を用いて $|\psi\rangle$ を測定すると次のようになり，係数の絶対値の 2 乗が確率に対応していることが分かる．

$$p(0) = \| P_0|\psi\rangle \|^2 = |\alpha|^2$$
$$p(1) = \| P_1|\psi\rangle \|^2 = |\beta|^2$$

2.1.4 時間発展

量子状態は時間発展により変化する．時間発展は量子状態にユニタリー演算子 U を作用させることで表現される．ただし，ユニタリー演算子 U とは $UU^\dagger = U^\dagger U = I$ を満たす線形写像である．始状態を $|\psi\rangle$，終状態を $|\psi\rangle'$ とすると $|\psi\rangle' = U|\psi\rangle$ となる．

2.1.5 合成系

量子ビットは $\mathbb{C}^2$ 上の単位ベクトルだったが，これをテンソル積 $\otimes$ で拡張して多量子ビットを考えることができる．量子計算ではテンソル積はクロネッカー積で定義される．クロネッカー積は，$|\psi\rangle = (a_1, \ldots, a_m)^\top \in \mathbb{C}^m, |\varphi\rangle = (b_1, \ldots, b_n)^\top \in \mathbb{C}^n$ に対して以下のように定義される．

$$|\psi\rangle \otimes |\varphi\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} := \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ \vdots \\ a_m \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{pmatrix}$$

n 量子ビットを考えるとき，量子状態は $(\mathbb{C}^2)^{\otimes n} := \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ 上の単位ベクトルである．また計算基底のテンソル積 $\{|i_1\rangle \otimes \ldots \otimes |i_n\rangle\}_{i_1,\ldots,i_n=0,1}$ は合成系の計算基底 $\{|j\rangle\}_{j=0}^{2^n-1}$ となる．

第 3 章　関連研究

3.1　Grover アルゴリズム

3.1.1　概要

Grover アルゴリズム [Gro96] は Grover の探索問題を解くための量子アルゴリズムであり，量子計算の分野では著名かつ汎用的であるため盛んに研究が行われている．端的に言えば，Grover アルゴリズムは関数の逆像を見つける量子アルゴリズムである．Grover アルゴリズムは暗号分野への応用も考えられており，例えば，ハッシュ値 $H(m)$ から m を見つけるなどがある．

定義 3.1.1 (Grover の探索問題)**.** 関数 $f : \{0,1\}^n \to \{0,1\}$ が与えられる．ただし，$f(s) = 1$ となる $s \in \{0,1\}^n$ は唯一つ存在し，これを解と呼ぶ．このとき解 s を見つける問題を Grover の探索問題という．

関数 f はオラクルとして与えられており，クエリ x を送ると $f(x)$ を返す．またこれ以外の方法で f に関する情報を得ることはできない．オラクルが与えられる計算のとき，オラクルへのクエリ回数が計算量の指標としてよく考えられ，質問計算量 (query complexity) と呼ばれる．

$N = |\{0,1\}^n|$ とする．古典計算で決定性のアルゴリズムを用いて Grover の探索問題を解くとき，オラクル (f) に $N-1$ 回クエリする必要がある．一方で，Grover アルゴリズムはクエリ回数が $O(\sqrt{N})$ で高い確率で正しい解 s を出力する．

3.1.2　アルゴリズム

まずはアルゴリズムで使用するオラクルについて説明する．

定義 3.1.2 (Grover アルゴリズムのオラクル)**.** Grover アルゴリズムのオラクルは次のように定義されるユニタリー演算子 O_g である．ただし，$|x\rangle$ はクエリであり，$|q\rangle$ はオラクルの状態である．また $\oplus$ は bitwiseXOR である．

$$O_g |x\rangle |q\rangle := |x\rangle |q \oplus f(x)\rangle$$

例えば，$q = 0$ とおけば $O_g |x\rangle |0\rangle = |x\rangle |0 \oplus f(x)\rangle$ となる．これはクエリ x が解でないと

きはオラクルは $|x\rangle|0\rangle$ を返し，クエリ x が解のときオラクルは $|x\rangle|1\rangle$ を返すため，クエリが解となっているかどうかがわかる．

Grover アルゴリズムでは $|q\rangle$ は次のようにする．

$$|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

このようにすることで，オラクルは次のような振る舞いをすることがわかる．

$$O_g|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

つまり，オラクルは x が解のときに符号を反転させ，それ以外では何もしないという操作を行う．

次にアルゴリズムを紹介する．

1. 初期状態として一様な重ね合わせ状態 $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$ を用意する．
2. オラクル O_g に $|\psi\rangle$ を作用させる．
3. $2|\psi\rangle\langle\psi| - I$ を作用させる．
4. 2,3 を繰り返す．
5. 測定する．

2,3 は合わせて Grover iteration と呼ばれる．Grover アルゴリズムは幾何学的な考察により，直感的な理解が得られる．

3.1.3 幾何学的な説明

$A = \{x \in \{0,1\}^n \mid f(x) = 0\},\ B = \{x \in \{0,1\}^n \mid f(x) = 1\}$ とする．解が M 個あるとし，解の重ね合わせ状態 $|\alpha\rangle$ と解でないものの重ね合わせ状態 $|\beta\rangle$ で張られる 2 次元平面を考える．

$$|\alpha\rangle := \frac{1}{\sqrt{N-M}}\sum_{x\in A}|x\rangle$$
$$|\beta\rangle := \frac{1}{\sqrt{M}}\sum_{x\in B}|x\rangle$$

初期状態 $|\psi\rangle$ は次のように $|\alpha\rangle$, $|\beta\rangle$ の重ね合わせで書けるため，この 2 次元平面上のベクトルである．

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$

さらに $\cos\frac{\theta}{2}=\sqrt{\frac{N-M}{N}}$, $\sin\frac{\theta}{2}=\sqrt{\frac{M}{N}}$ とおき，アルゴリズムの各段階でどのように変化するかを説明する．

$$|\psi\rangle=\cos\frac{\theta}{2}|\alpha\rangle+\sin\frac{\theta}{2}|\beta\rangle \tag{3.1}$$

まずはアルゴリズムの 2 では，式 3.1 で表される $|\psi\rangle$ に O_g を作用させるので

$$O_g|\psi\rangle=\cos\frac{\theta}{2}|\alpha\rangle-\sin\frac{\theta}{2}|\beta\rangle$$

次にアルゴリズムの 3 において，$2|\psi\rangle\langle\psi|-I$ は $|\varphi\rangle=a|\psi\rangle+b|\psi_\perp\rangle$ と表される状態に作用して $|\varphi\rangle=a|\psi\rangle-b|\psi_\perp\rangle$ という状態にする．ただし，$\langle\psi|\psi_\perp\rangle=0$ である．つまり，$2|\psi\rangle\langle\psi|-I$ は $|\psi\rangle$ を軸にしてベクトルを反転させる操作であるためアルゴリズムの 2 と合わせると次のようになる．

$$(2|\psi\rangle\langle\psi|-I)O_g|\psi\rangle=\cos\frac{3\theta}{2}|\alpha\rangle+\sin\frac{3\theta}{2}|\beta\rangle$$

これら一連の操作は図 3.1 のように幾何学的に考えることができる．そうすることで，アルゴリズムの 2,3 を繰り返すことは $|\psi\rangle$ を $|\beta\rangle$(解のベクトル) に近づけていく操作をしていると理解できる．また，アルゴリズムを k 回繰り返した場合の状態 $|\psi'\rangle$ は次のようになっている．

$$\begin{aligned}|\psi'\rangle&=((2|\psi\rangle\langle\psi|-I)O_g)^k|\psi\rangle\\&=\cos\left(\frac{2k+1\theta}{2}\right)|\alpha\rangle+\sin\left(\frac{2k+1\theta}{2}\right)|\beta\rangle\end{aligned}$$

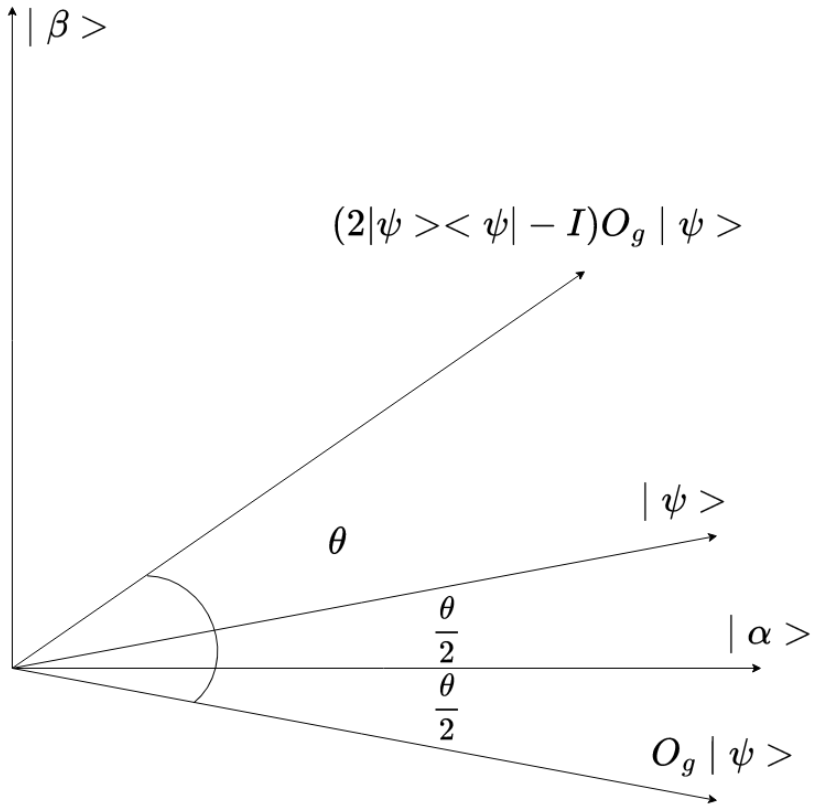

fig3.1　Grover アルゴリズムの幾何学的な理解

3.1.4　計算量

最後に Grover アルゴリズムの繰り返し回数 k の最適な値を解析する．最適な k とは $|\psi'\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$ における $|\beta\rangle$ の係数が最も 1 に近づくときである．つまり $\frac{2k+1}{2}\theta = \frac{\pi}{2}$ となる k を求めれば良い．等式が成り立つとき k が整数とは限らないため，$\mathrm{CI}(\cdot)$ を $\cdot$ に最も近い整数として，$R := \mathrm{CI}(\frac{\pi}{2\theta} - \frac{1}{2})$ を求める．$\frac{\theta}{2} \geq \sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$ に注意すると

$$\begin{aligned} \frac{\theta}{2} &\geq \sqrt{\frac{M}{N}} \\ \Longrightarrow \frac{2}{\theta} &\leq \sqrt{\frac{N}{M}} \\ \Longrightarrow \frac{\pi}{2\theta} &\leq \frac{\pi}{4}\sqrt{\frac{N}{M}} \end{aligned}$$

したがって，

$$R = \mathrm{CI}\left(\frac{\pi}{2\theta} - \frac{1}{2}\right) \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil$$

つまり $R = O(\sqrt{N/M})$ となる．また解が 1 つのときは $M = 1$ なので $R = O(\sqrt{N})$ である．

3.2 Zhandry の recording technique

この節では量子ランダムオラクルモデルにおいてオラクルが攻撃者のクエリ情報を記録する方法，Zhandry's recording technique について述べる．Zhandry の recording technique における記法は [CFHL21] を参考にした．

3.2.1 フーリエ基底

定義 3.2.1. (フーリエ基底). 計算基底 $\{|j\rangle\}_{j=0}^{N-1}$ を次のように変換した基底 $\{|\hat{j}\rangle\}_{j=0}^{N-1}$ をフーリエ基底という．

$$|\hat{j}\rangle := \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle$$

ただし，$\omega_N \in \mathbb{C}$ は 1 の N 乗根である．

本論文で用いるフーリエ基底の重要な性質を紹介する．ユニタリー演算子 U が $U|y\rangle|y'\rangle = |y+y'\rangle|y'\rangle$ と作用するものとすると，$U|\hat{y}\rangle|\hat{y'}\rangle = |\hat{y}\rangle|\hat{y'-y}\rangle$ となる．また，$\hat{y'} \pm \hat{y} = \widehat{y' \pm y}$ が成り立つ．

3.2.2 Zhandry の recording technique

$\mathcal{Y}$ を濃度 N の有限集合とするとき，$\mathbb{C}^N$ を $\mathbb{C}[\mathcal{Y}]$ と書く．$\mathcal{L}(\mathbb{C}^k)$ は $\mathbb{C}^k$ 上の線形写像全体の集合を表す．また $|\mathcal{X}| = M,\ |\mathcal{Y}| = N$ とする．

定義 3.2.2 (ランダム関数とその量子状態). $H : \mathcal{X} \to \mathcal{Y}$ をランダム関数とし，$\mathcal{H} := \{H : \mathcal{X} \to \mathcal{Y}\}$ を取りうるすべてのランダム関数の集合族とする．H を真理値表 $(H(0), \ldots, H(M-1)) \in \mathcal{Y}^M$ として考えるとき，この量子状態を $|H\rangle := \bigotimes_x |H(x)\rangle$ と書く．

定義 3.2.3 (データベースとその量子状態). $D : \mathcal{X} \to \overline{\mathcal{Y}} := \mathcal{Y} \cup \{\perp\}$ を H のデータベースという．データベース D において，$D(x) = \perp$ は $D(x)$ が未定義であることを意味する．$\mathcal{D} := \{D : \mathcal{X} \to \overline{\mathcal{Y}}\}$ を取りうるすべてのデータベースの集合族とする．$D \in \mathcal{D}$ は量子状態で $|D\rangle := \bigotimes_x |D(x)\rangle$ と書く．D の初期状態はすべて $\perp$，つまり $|D\rangle = |\perp, \ldots, \perp\rangle$ とする．

定義 3.2.4. (Oracle) $\mathrm{O} \in \mathcal{L}(\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}] \otimes \mathbb{C}[\mathcal{H}])$ は次のように定義されるユニタリー演算

子である．

$$\mathrm{O}\,|x\rangle\,|y\rangle\,|H\rangle := |x\rangle\,|y + H(x)\rangle\,|H\rangle$$

補題 3.2.5. O に対して次が成り立つ．

$$\mathrm{O}\,|x\rangle\,|\hat{y}\rangle\,|\hat{H}\rangle := |x\rangle\,|\hat{y}\rangle\,|\hat{H} - \hat{y}\cdot\delta_x\rangle$$

ただし $\delta_x : \mathcal{X} \to \{0,1\}$ であり，$x = x'$ のとき $\delta_x(x') = 1$，それ以外で $\delta_x(x') = 0$ である．これは $\hat{H}$ の x の位置に $-\hat{y}$ を加えることを意味する．また $|\hat{H}\rangle := \bigotimes_x |\widehat{H(x)}\rangle$ である．

ユニタリー演算子 O は $D(x) = \perp$ のとき $\mathrm{O}\,|x\rangle\,|y\rangle\,|D\rangle := |x\rangle\,|y\rangle\,|D\rangle$ と定義することで $\mathrm{O} \in \mathcal{L}(\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}] \otimes \mathbb{C}[\mathcal{D}])$ に自然に拡張できる．

定義 3.2.6. (Comp_x)．ユニタリー演算子 $\mathrm{Comp}_x : \mathbb{C}[\overline{\mathcal{Y}}] \to \mathbb{C}[\overline{\mathcal{Y}}]$ は $\mathbb{C}[\mathcal{D}] = \bigotimes_x \mathbb{C}[\overline{\mathcal{Y}}]$ の x の位置に作用するユニタリー演算子で次のように定義される．

$$\mathrm{Comp}_x := |\perp\rangle\langle\hat{0}| + |\hat{0}\rangle\langle\perp| + \sum_{\hat{z}\neq\hat{0}} |\hat{z}\rangle\langle\hat{z}|$$

定義 3.2.7. (Comp)．Comp は次のように定義されるユニタリー演算子である．

$$\mathrm{Comp}\,|x\rangle\,|y\rangle\,|D\rangle := |x\rangle\,|y\rangle \otimes \mathrm{Comp}_x\,|D\rangle$$

定義 3.2.8. (Compressed Oracle (cO))．cO は次のように定義されるユニタリー演算子である．

$$\mathrm{cO} := \mathrm{Comp} \circ \mathrm{O} \circ \mathrm{Comp}^\dagger \in \mathcal{L}(\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}] \otimes \mathbb{C}[\mathcal{D}])$$

補題 3.2.9 (Zhandry's recording technique)．cO に対して次が成り立つ．

$$\mathrm{cO}\,|x\rangle\,|\hat{y}\rangle\,|\hat{D}\rangle := |x\rangle\,|\hat{y}\rangle\,|\hat{D} - \hat{y}\cdot\delta_x\rangle$$

ただし $\delta_x : \mathcal{X} \to \{0,1\}$ であり，$x = x'$ のとき $\delta_x(x') = 1$，それ以外で $\delta_x(x') = 0$ である．これは $\hat{D}$ の x の位置に $-\hat{y}$ を加えることを意味する．また $|\hat{D}\rangle := \bigotimes_x |\widehat{D(x)}\rangle$ である．

例として，compressed オラクルを用いたときにクエリがデータベースに記録される様子を示す．$|\hat{D}\rangle := \bigotimes_x |\widehat{D(x)}\rangle$ は初期状態ではすべて $\perp$ とする．つまり $|\hat{D}\rangle = |\perp,\ldots,\perp\rangle$ となっている．このとき，最初のクエリは以下のようにしてデータベースの x の位置に $-\hat{y}$ が記録される．

$$\begin{aligned}
\mathrm{cO}\,|x\rangle\,|\hat{y}\rangle\,|\hat{D}\rangle &= \mathrm{Comp}\cdot\mathrm{O}\cdot\mathrm{Comp}^\dagger\,|x\rangle\,|\hat{y}\rangle\,|\perp,\ldots,\perp\rangle \\
&= \mathrm{Comp}\cdot\mathrm{O}\,|x\rangle\,|\hat{y}\rangle\,|\perp,\ldots,\hat{0},\ldots,\perp\rangle \\
&= \mathrm{Comp}\,|x\rangle\,|\hat{y}\rangle\,|\perp,\ldots,-\hat{y},\ldots,\perp\rangle \\
&= |x\rangle\,|\hat{y}\rangle\,|\perp,\ldots,-\hat{y},\ldots,\perp\rangle
\end{aligned}$$

続いて 2 回目のクエリ $\mathrm{cO}\,|x\rangle\,|\hat{y}'\rangle\,|\hat{D}\rangle$ を行うとする．

$$\begin{aligned}
\mathrm{cO}\,|x\rangle\,|\hat{y}'\rangle\,|\hat{D}\rangle &= \mathrm{Comp}\cdot\mathrm{O}\cdot\mathrm{Comp}^{\dagger}\,|x\rangle\,|\hat{y}'\rangle\,|\perp,\ldots,-\hat{y},\ldots,\perp\rangle \\
&= \mathrm{Comp}\cdot\mathrm{O}\,|x\rangle\,|\hat{y}'\rangle\,|\perp,\ldots,-\hat{y},\ldots,\perp\rangle \\
&= \mathrm{Comp}\,|x\rangle\,|\hat{y}'\rangle\,|\perp,\ldots,\widehat{-y-y'},\ldots,\perp\rangle \\
&= |x\rangle\,|\hat{y}'\rangle\,|\perp,\ldots,\widehat{-y-y'},\ldots,\perp\rangle
\end{aligned}$$

このように，$-\hat{y}$ は $\widehat{-y-y'}$ に書き換えられる．またこのとき 2 つの場合が考えられる．

1. $-y-y'=0$ のとき，$-y$ は $D(x)=\perp$ に書き換えられる．
2. $-y-y'\neq 0$ のとき，$-y$ は $-y-y'$ に書き換えられる．

1 の場合はデータベースの x の位置に記録されていたデータを消去することを意味する．
2 の場合はデータベースの x の位置に記録されていたデータをアップデートすることを意味する．

第 4 章　研究結果

この節では，研究成果である定理 4.0.1 のより簡潔かつ検証容易な証明を行う．定理の主張は，ランダムオラクルに対して任意のクエリを q 回行うアルゴリズムがあるとき，データベース D から所望のデータを見つけることができる確率は高々 $O\left(q^2/N\right)$ だというものである．今回は所望のデータを 0 としたが，固定の値ならば何でも良い．また $0 \in D$ と書くとき，$|D\rangle$ に $|D(x) = 0\rangle$ が存在することを意味する．

定理 4.0.1. 攻撃者がランダムオラクル cO に q 回クエリする状況を考える．q 回のクエリを行った後に D を測定するとき，$0 \in D$ である確率は高々 $O\left(q^2/N\right)$ である．

先行研究 [Zha19] の証明方針は次のとおりである．まず，攻撃者とオラクルの合成系の量子状態 $|\psi\rangle$ を $P,\ Q,\ R,\ S$ で射影する．それぞれ次を満たす空間への射影である．

$$
\begin{aligned}
&P : 0 \in D \\
&Q : 0 \notin D,\ y \neq 0,\ D(x) = \perp \\
&R : 0 \notin D,\ y \neq 0,\ D(x) \neq \perp \\
&S : 0 \notin D,\ y = 0
\end{aligned}
$$

P, Q, R, S はそれぞれ直交した空間への射影になっている．また $P + Q + R + S = I$ であり，$\| P|\psi\rangle \|^2$ がデータベースに所望のデータが含まれている確率である．次に $P|\psi\rangle, Q|\psi\rangle\ , R|\psi\rangle, S|\psi\rangle$ にオラクルを作用させた後，P で射影する．最後に $\|P|\psi\rangle\|$ と $\|P \cdot \mathrm{cO}|\psi\rangle\|$ を比較し，1 回のクエリで $0 \in D$ となるベクトルのノルムがどれほど増加したかを評価するという流れである．具体的には次の不等式が成り立つことを示すことで，クエリ前後のノルムを比較する．

$$
\begin{aligned}
\|P \cdot \mathrm{cO}|\psi\rangle\| &= \|P \cdot \mathrm{cO} \cdot (P + Q + R + S)|\psi\rangle\| \quad (\because P + Q + R + S = I) \\
&\leq \|P \cdot \mathrm{cO} \cdot P|\psi\rangle\| + \|P \cdot \mathrm{cO} \cdot Q|\psi\rangle\| \\
&\quad + \|P \cdot \mathrm{cO} \cdot R|\psi\rangle\| + \|P \cdot \mathrm{cO} \cdot S|\psi\rangle\| \quad (\because \text{三角不等式}) \\
&\leq \|P|\psi\rangle\| + \frac{1}{\sqrt{N}}
\end{aligned}
$$

ここからは本論文での研究成果であるより簡潔かつ検証容易な証明を行う．

証明　一度のオラクルアクセスで $0 \in D$ となる確率が最大でどれだけ増えるかを示す．データベースは初期状態で空であり，このとき所望のデータが含まれる確率は 0 である．

いま，オラクルアクセスが $q-1$ 回行われた後とし，このときの攻撃者とオラクルの合成系の量子状態 $|\psi\rangle$ が次のようになっているとする．

$$\begin{aligned}|\psi\rangle &= \sum_{x,\hat{y},\hat{D}} \alpha_{x,\hat{y},D} \,|x,\hat{y}\rangle \otimes |D\rangle \\ &= \sum_{x,\hat{y},s,D'} \alpha_{x,\hat{y},s,D'} \,|x,\hat{y}\rangle \otimes |s\rangle_x \,|D'\rangle_{\bar{x}}\end{aligned}$$

2 行目の式で $|s\rangle_x$ は $|D\rangle$ の x の位置を陽に書いたものであり，$|D'\rangle_{\bar{x}}$ は x 以外の位置を表したものである．次に $|x,\hat{y}\rangle \otimes |D\rangle$ が張る空間への射影 $P,\ Q,\ R,\ S$ を次のように定義する．

$$\begin{aligned}&P : 0 \in D \\ &Q : 0 \notin D,\ \hat{y} \neq \hat{0},\ D(x) = \perp \\ &R : 0 \notin D,\ \hat{y} \neq \hat{0},\ D(x) \neq \perp \\ &S : 0 \notin D,\ \hat{y} = \hat{0}\end{aligned}$$

P, Q, R, S はそれぞれ直交した空間への射影になっており，$P+Q+R+S=I$ である．ここからは簡単のため，射影した空間の基底を次のように 1 つに固定して考える．

$$\begin{aligned}P\,|\psi\rangle &= |x\rangle\,|\hat{y}\rangle\,|s\rangle_x\,|D'\rangle_{\bar{x}} \\ Q\,|\psi\rangle &= |x\rangle\,|\hat{y}\rangle\,|\perp\rangle_x\,|D'\rangle_{\bar{x}} \\ R\,|\psi\rangle &= |x\rangle\,|\hat{y}\rangle\,|s\rangle_x\ \,|D'\rangle_{\bar{x}} \\ S\,|\psi\rangle &= |x\rangle\,|\hat{0}\rangle\,|s\rangle_x\,|D'\rangle_{\bar{x}}\end{aligned}$$

これらに cO を作用させた後に P で射影することで，$0 \in D$ となるノルムの変化を調べる．

$P\,|\psi\rangle$ に cO を作用させたとき，cO はユニタリーであるからノルムを保存することに注意すると，

$$\|P \cdot \mathrm{cO} \cdot P\,|\psi\rangle\,\| \leq \|\mathrm{cO} \cdot P\,|\psi\rangle\,\| = \|P\,|\psi\rangle\,\|$$

したがって，

$$\|P \cdot \mathrm{cO} \cdot P\,|\psi\rangle\,\| \leq \|P\,|\psi\rangle\,\| \tag{4.1}$$

$Q\,|\psi\rangle$ に cO を作用させたとき，

$$\begin{aligned}\mathrm{cO} \cdot Q\,|\psi\rangle &= \mathrm{cO}\,|x\rangle\,|\hat{y}\rangle\,|\perp\rangle_x\,|D'\rangle_{\bar{x}} \\ &= |x\rangle\,|\hat{y}\rangle\,|-\hat{y}\rangle_x\,|D'\rangle_{\bar{x}}\end{aligned}$$

よって，P で射影すると次のようになる．

$$P \cdot \mathrm{cO} \cdot Q \left|\psi\right\rangle = \left|x\right\rangle \left|\hat{y}\right\rangle \frac{1}{\sqrt{N}} \left|0\right\rangle_x \left|D'\right\rangle_{\bar{x}}$$

したがって，

$$\| P \cdot \mathrm{cO} \cdot Q \left|\psi\right\rangle \| = \frac{1}{\sqrt{N}} \| Q \left|\psi\right\rangle \| \tag{4.2}$$

$R\left|\psi\right\rangle$ に cO を作用させたとき，

$$\begin{aligned}
\mathrm{cO} \cdot R \left|\psi\right\rangle &= \mathrm{cO} \left|x\right\rangle \left|\hat{y}\right\rangle \left|s\right\rangle_x \left|D'\right\rangle_{\bar{x}} \\
&= \mathrm{cO} \left|x\right\rangle \left|\hat{y}\right\rangle \frac{1}{\sqrt{N}} \sum_d \omega_N^{s \cdot d} \left|\hat{d}\right\rangle_x \left|D'\right\rangle_{\bar{x}} \\
&= \left|x\right\rangle \left|\hat{y}\right\rangle \frac{1}{\sqrt{N}} \sum_d \omega_N^{s \cdot d} \left|\widehat{d-y}\right\rangle_x \left|D'\right\rangle_{\bar{x}} \\
&= \left|x\right\rangle \left|\hat{y}\right\rangle \frac{1}{\sqrt{N}} \sum_{d'} \omega_N^{s \cdot (d'+y)} \left|\hat{d'}\right\rangle_x \left|D'\right\rangle_{\bar{x}}
\end{aligned}$$

ただし，$\left|\hat{d'}\right\rangle = \frac{1}{\sqrt{N}} \sum_k \omega_N^{d' \cdot k} \left|k\right\rangle$ とした．これより，

$$\begin{aligned}
P \cdot \mathrm{cO} \cdot R \left|\psi\right\rangle &= \left|x\right\rangle \left|\hat{y}\right\rangle \frac{1}{\sqrt{N}} \sum_{d'} \omega_N^{s \cdot (d'+y)} \frac{1}{\sqrt{N}} \left|0\right\rangle_x \left|D'\right\rangle_{\bar{x}} \\
&= 0
\end{aligned}$$

最後の等式は $\sum_\alpha \omega_N^{s \cdot \alpha} = 0$ を用いた．したがって，

$$\| P \cdot \mathrm{cO} \cdot R \left|\psi\right\rangle \| = 0 \tag{4.3}$$

$S\left|\psi\right\rangle$ に cO を作用させたとき，

$$\begin{aligned}
\mathrm{cO} \cdot S \left|\psi\right\rangle &= \left|x\right\rangle \left|\hat{0}\right\rangle \left|s\right\rangle_x \left|D'\right\rangle_{\bar{x}} \\
&= S \left|\psi\right\rangle
\end{aligned}$$

したがって，

$$\| P \cdot \mathrm{cO} \cdot S \left|\psi\right\rangle \| = 0 \tag{4.4}$$

式 (4.1),(4.2),(4.3),(4.4) より，

$$\begin{aligned}\|P\cdot \mathrm{cO}\,|\psi\rangle\,\| &\le \|P\cdot \mathrm{cO}\cdot P\,|\psi\rangle\,\| + \|P\cdot \mathrm{cO}\cdot Q\,|\psi\rangle\,\| \\ &\quad + \|P\cdot \mathrm{cO}\cdot R\,|\psi\rangle\,\| + \|P\cdot \mathrm{cO}\cdot S\,|\psi\rangle\,\| \\ &\le \|P\,|\psi\rangle\,\| + \frac{1}{\sqrt{N}}\|Q\,|\psi\rangle\,\| \\ &\le \|P\,|\psi\rangle\,\| + \frac{1}{\sqrt{N}}\end{aligned}$$

したがって，1 回のクエリで $0 \in D$ となるノルムは最大で $1/\sqrt{N}$ だけ増加するので，q 回のクエリ後に $0 \in D$ であるノルムは最大で $q/\sqrt{N}$ だけ増加する．よって q 回のクエリ後に $0 \in D$ である確率は最大で q^2/N である．

□

第 5 章　結論

Grover アルゴリズムの最適性の証明をオラクルの基底をフーリエ基底で考えることで証明が簡潔かつ検証容易になることを示した．本研究ではランダム関数の逆像を見つけるのに最低必要な量子クエリ数を評価したが，任意の関数の逆像を見つける問題は，ランダム関数の逆像を見つける問題に帰着できるため，本証明が Grover アルゴリズム [Gro96] の最適性を証明したことになるのは Zhandry [Zha19] と全く同じである．

謝辞

藤﨑先生には研究活動だけにとどまらず，ありとあらゆる面でお世話になりました．私は研究室配属の当初から学力的に不足しており，研究活動についても右も左もわからない状態でしたが，先生は辛抱強くご指導ご鞭撻下さいました．また個人的な悩みなどをご相談したときは，真摯にお話を聞いてくださり温かい言葉や助言を頂きました．研究活動においては，研究テーマの考案や学会に提出する論文の添削，および学会発表のスライド作成まで様々な面で終始適切な助言をして頂きました．深く感謝しております．

研究室メンバーの工藤君，谷君には研究をはじめ，自主ゼミやセキュリティーコンテストを通して日頃より刺激的な議論をさせていただきました．ありがとうございます．

参考文献

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security*, ASIACRYPT'11, page 41–69, Heidelberg, 2011. Springer.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, page 62–73, New York, NY, USA, 1993. Association for Computing Machinery.

[CFHL21] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In *Advances in Cryptology – EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II*, page 598–629, Berlin, Heidelberg, 2021. Springer-Verlag.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, oct 1997.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 239–268. Springer International Publishing, 2019.