

# 修士論文

## 確率的対数領域計算による確率行列の スペクトルギャップ増幅

令和4年度 修了

三重大学 大学院工学研究科 情報工学専攻  
コンピュータソフトウェア研究室

鈴木 健介

## 概 要

近年、量子計算機の研究開発が盛んに行われており、量子計算量クラスに関する理論的な研究も活発に行われている。量子計算機は古典計算機に比べ高速に計算できることが期待されており、すでに実装可能な量子計算機がスーパーコンピュータを上回る性能に達しているという研究結果も存在する [3]。しかし現在実装可能な量子計算機は古典計算機に比べ扱えるビット数が少ないため、量子領域計算クラスに関する困難性を明らかにすることは重要な課題となっている。

また量子計算機はすべての問題において古典計算機より高速に計算できるわけではない。量子ビットは古典ビットに比べ少ない量で多くの情報を保持することが可能だが、保持した情報を一つずつ取り出すといった操作は得意ではない。こういった性質から、量子計算機では行列演算など複数の情報を用いた演算を古典計算機より少ないステップで行い、その結果を出力するという問題に強く、実際に行列に関する様々な問題の量子アルゴリズムが考案されている。こういった量子計算量クラスに関する様々な研究成果が出る中で、古典計算量クラスとの関係性を明らかにすることは量子計算機を活用するうえで重要な指標となる。現在行列問題における古典計算量クラスと量子計算量クラスの違いとして、扱えることのできる行列の種類や、近似を行う際の精度といったことが予想されている。

このような背景より、古典における領域複雑性と行列問題の精度の観点から、Doron らの研究 [6] に注目した。Doron らは確率行列の第二固有値を判定する問題について、逆多項式の精度を要求する場合は BPL 完全であることを示した。しかし彼らの研究において、より簡単な問題である定数精度を要求する第二固有値問題がどれほど困難かについては議論されておらず、定数精度と逆多項式精度の第二固有値問題における困難性が同等かは不明である。そこで本研究では逆多項式精度の第二固有値問題を定数精度に確率的対数領域計算で帰着させることで、定数精度と逆多項式精度の第二固有値問題が確率的対数領域計算において同等の困難性を持つことを示そうと試みた。結果として確率的対数領域計算が可能な状況では、定数精度の第二固有値問題が一部の逆多項式精度の問題より困難であることを示した。

# 目次

<b>第 1 章</b>	<b>序論</b>	<b>4</b>
1.1	研究背景 . . . . .	4
1.2	本研究の成果 . . . . .	5
<b>第 2 章</b>	<b>準備</b>	<b>6</b>
2.1	領域計算量理論 . . . . .	6
2.1.1	領域限定チューリングマシン . . . . .	6
2.1.2	確率的領域計算量クラス . . . . .	6
2.2	量子情報科学の前提知識 . . . . .	7
2.2.1	量子情報科学の概要 . . . . .	7
2.2.2	Dirac の表記法 . . . . .	8
2.2.3	Dirac の表記法による量子ビットの記述 . . . . .	9
2.2.4	量子ビットの測定 . . . . .	10
2.2.5	量子ビットの時間発展 . . . . .	10
2.2.6	多量子ビット . . . . .	10
2.2.7	混合状態 . . . . .	11
2.3	量子領域計算量クラス . . . . .	13
<b>第 3 章</b>	<b>先行研究</b>	<b>15</b>
3.1	Doron らの研究 [6] . . . . .	15
3.1.1	第二固有値問題 . . . . .	15
3.1.2	BPL 完全性 . . . . .	15
3.2	Girish らの研究 [11] . . . . .	20
3.2.1	アルゴリズムの入出力 . . . . .	21
3.2.2	アルゴリズムの概要 . . . . .	21
3.2.3	$BQ_U L = BQ_Q L$ . . . . .	23
<b>第 4 章</b>	<b>本研究の成果</b>	<b>25</b>
4.1	提案手法 . . . . .	25
4.2	確率的対数領域計算における行列冪の近似 . . . . .	25
4.3	定数ギャップ問題への帰着 . . . . .	28
<b>第 5 章</b>	<b>結論</b>	<b>29</b>
5.1	本研究の成果とまとめ . . . . .	29
5.2	今後の課題 . . . . .	29

# 第1章 序論

## 1.1 研究背景

問題を解くのにどれだけの計算資源を必要とするか、もしくは計算機における資源の違いが計算能力にどれほど影響を与えるのかを明らかにすることは、理論計算機科学における重要な課題の一つである。計算資源は具体的に、計算時間や計算時に使用可能な記憶領域などが挙げられる。また計算機に確率性を持たせることで、正確に計算するのではなく近似的な計算を許容するといった問題も存在し、そういった点から確率性の有無にも計算資源の違いが存在する。こういった問題の計算に必要とされる計算資源の違いに対して、それぞれ計算複雑性クラスというもの定義されてきた。そして世の中に存在する問題がどの計算複雑性クラスに属するか、各計算複雑性クラスがどのような関係を持っているのかなどが理論計算機科学では盛んに研究されている。

また、計算機の資源は確率性や計算時間、計算領域だけでなく情報の担い手自身の性質といったところにも存在する。近年盛んに研究開発が行われている量子計算機がそれであり、古典(従来)の計算機理論において情報の担い手として利用される物理系と比べて、より拡張された物理系をもちいて情報処理を行う。これにより量子計算機は古典の計算機より高速に計算することが期待されており、現在すでに実装可能な量子計算機がスーパーコンピュータをも上回る性能に達しているという研究成果も存在する [3]。しかし現在実装可能な量子計算機はスーパーコンピュータなどに比べ扱えるビット数が少ないため、領域効率のよい量子アルゴリズムが必要となる。そういった意味で様々な問題における量子領域計算量の困難性を明らかにすることは量子計算科学における重要な課題となっており、文献 [7] や [15] などの研究が存在する。またすべての問題に対して古典の計算機より高速に計算ができるというわけでもなく、得意不得意な問題が存在する。例えば量子計算機の得意な問題として行列演算が挙げられる。量子計算機で用いられる量子ビットは、古典ビットに比べ少ない量で多くの情報を保持することが可能だが、保持した情報を一つずつ取り出すといった操作は得意ではない。こういった性質から、量子計算機では行列演算など複数の情報を用いた演算を従来の計算機より少ないステップで行い、その結果を出力するといった問題に強く、実際に文献 [10] など行列に関する様々な問題の量子アルゴリズムが考案されている。

そして量子領域計算量の観点からも計算複雑性クラスが定義されており、古典の計算機資源で定義されている計算複雑性クラスとの関係も明らかになりつつある。量子計算は確率的なふるまいを許しているため、主に古典計算複雑性クラスと比較する際には確率的な計算複雑性クラスが用いられる。そして量子と古典での計算複雑性クラスの違いは、近似精度や問題で扱う行列の種類によって区別しようとする研究が存在しており、例えば Gharibian らの研究 [9] が挙げられる。Gharibian らは QSVT と呼ばれる行列操作を定数精度で近似する古典アルゴリズムを提案したが、量子アルゴリズムであれば多項式時間で逆多項式の精度で計算することが可能だという結果を示した。このように量子計算と古典計算の計算複雑性クラスを明らかにする研究が現在盛んに行われている。

こういった背景から私は古典における領域複雑性と行列問題の精度について関心を持ち、Doron らの研究 [6] に注目した。(古典領域複雑性と行列問題に関する研究は、他にも Boix-Adserà らの研究 [1] などが挙げられる。) Doron らは確率行列の第二固有値を判定する問題について、逆多項式の精度を要求する場合は確率的対数領域計算クラスの中で最も困難な問題であることを示した。そこで私は、より簡単な問題である定数精度を要求する第二固有値問題と逆多項式の精度の第二固有値問題との、確率的対数領域計算における関係性について研究した。

## 1.2 本研究の成果

本研究では Doron らが示した第二固有値問題について、行列冪の近似を行うことで、行列がある条件を満たす場合に確率的対数領域計算を用いて  $\frac{1}{n}$  ギャップを定数ギャップに増幅できることを示した。具体的には以下に示す定理を証明し、 $\frac{1}{n}$  ギャップの第二固有値問題を定数ギャップの第二固有値問題へ帰着した。これにより確率的対数領域計算において、定数ギャップ第二固有値問題が一部の  $\frac{1}{n}$  ギャップ第二固有値問題より困難であることを示した。

**定理 4.3.2.** (制限付き  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  の  $\text{Apx-}2\text{ndEV}_{c, 2c}$  への帰着)

インスタンスとして受け取る確率行列が、すべての固有値が重複度 1、もしくは対角化行列の条件数が次数の多項式で抑えられるような  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  のインスタンスは確率的対数領域計算において  $\text{Apx-}2\text{ndEV}_{c, 2c}$  のインスタンスへ帰着可能である。

## 第2章 準備

### 2.1 領域計算量理論

ある問題を計算機で解く際の困難性を議論するうえで、問題の入力長に対して計算機側のコストがどのように変化するかを考えることが一般的である。ここでいう計算機側のコストとは、計算時に必要な記憶領域量や実行時間などが挙げられ、特にどれだけの記憶領域が必要になるかという点に注目するのが領域計算量理論である。また、対象とする計算機の種類によっても領域計算量クラスは細分化されており、動作が決定的に決まるもの、確率的に決まるもの、情報の担い手が量子的なふるまいをするものなどが存在する。

#### 2.1.1 領域限定チューリングマシン

決定的領域限定チューリングマシンとは、入力テープ (読取専用)・ワークテープ (読み書き可)・出力テープ (書込専用) の3つのテープを持っている計算機モデルである。入力長を  $n$  としたとき、ワークテープのサイズを  $S(n)$  とおいて、この入力長に依存して増える使用可能なワークテープのサイズを領域複雑度と呼ぶ。

決定的領域限定チューリングマシンにおける3つのテープだけでなく、ランダムコインテープも使用することができるものを確率的領域限定チューリングマシンと呼ぶ。ここで、ランダムコインテープは一方方向にのみ読み取り可能であり、各ビットはそれぞれ独立に一様ランダムなビットで初期化されている。

#### 2.1.2 確率的領域計算量クラス

ある言語  $L$  が確率的領域限定チューリングマシンで受理可能とは、すべての入力  $x \in L$  と入力  $y \notin L$  に対して以下を満たす確率的領域限定チューリングマシン  $TM$  が存在することをいう。

$$\Pr[TM(x) = 1] \geq \frac{2}{3} \quad (2.1)$$

$$\Pr[TM(y) = 1] \leq \frac{1}{3} \quad (2.2)$$

また、ある言語が領域複雑度  $S(n)$  の確率的領域限定チューリングマシンで受理可能るとき、その言語は確率的領域計算量クラス  $\mathbf{BSPACE}(S(n))$  に含まれるという。本研究において主に扱う確率的対数領域計算量クラス  $\mathbf{BPL}$  は、任意の定数  $c > 0$  に対して以下で定義される。

$$\mathbf{BPL} = \bigcup_{c>0} \mathbf{BSPACE}(c \log n) \quad (2.3)$$

問題と領域計算量クラスの関係性は、単に問題が領域計算量クラスに含まれるという関係性以外にも困難性と完全性が存在する。またこれらを説明するうえで必要となる確率的対数領域計算による帰着という概念も存在する。以下にこれらの定義を示す。定義には文献 [2] を参考にした。

**定義 2.1.1.** (確率的対数領域計算による帰着) 言語  $B$  が確率的対数領域計算のもとで言語  $C$  に帰着可能とは、すべての  $x \in \{0,1\}^n$  に対して、 $\Pr[B(TM(x)) = C(x)] \geq \frac{2}{3}$  となる領域複雑度が  $O(\log n)$  である確率的チューリングマシン  $TM$  が存在することをいう。また  $B \leq_{\text{BPL}} C$  と表記する。

**定義 2.1.2.** (BPL 困難) ある言語  $L$  が BPL 困難であるとは、すべての  $L \in \text{BPL}$  において  $L \leq_{\text{BPL}} L'$  であることを指す。

**定義 2.1.3.** (BPL 完全) ある言語  $L$  が BPL 完全であるとは、 $L \in \text{BPL}$  かつ BPL 困難であることを指す。

## 2.2 量子情報科学の前提知識

従来の計算機 (古典計算機) において、情報の担い手は 0 か 1 のどちらかの状態をとるビット (以降この章では古典ビット) であった。それに対し近年では、この情報の担い手が量子的なふるまいを許す計算機 (量子計算機) の研究開発が盛んにおこなわれており、特定の問題において古典計算機よりも高速に計算できることが期待されている。しかし現在実装可能な量子計算機は古典計算機に比べ使用できる記憶領域が少ない。このことから量子計算理論においても領域計算量について盛んに議論が行われており様々な結果が知られている。これらの結果は古典計算機に対する量子計算機の領域計算量的な優位性を議論するうえでも重要である。ここでは、量子領域計算量クラスを説明するうえで必要となる量子情報科学の前提知識について説明する。本節で紹介する内容は、文献 [14][18] を参考にしてしている。

### 2.2.1 量子情報科学の概要

量子情報科学は量子力学を基にできている。量子情報科学を説明するうえで物理学的な概念が必要となるため、ここで説明する。

まず、自然現象を理解、記述する物理学では対象となるものを定める必要があり、定めた対象のことを物理系と呼ぶ。例えばリンゴや猫、銅線など様々なものが挙げられる。また、特に物理系のなかでも量子力学的な効果が表れる物理系を量子系と呼び、原子系、電子系などが挙げられる。ここでいう量子力学的な効果とは、測定値の予測が確率的にしかできないような場合を指している。

次に物理系を解析する場合を考える。物理系には物理的性質を表す様々な物理量が存在し、それらを測定することで解析が行える。例えば質量や長さ、電圧なども物理量である。様々な物理量を測定することで、リンゴと猫の違いなどを物理学的に議論することが可能になる。ただし物理系が同じ場合でも、状態によって測定した際の物理量は変わってくる。このような議論から、状態は「様々な物理量の測定に対して、測定値を定めるもの」と考えることができる。また、量子系においては同じ状態でも確率的に物理量が決まるため、量子系での状態は「様々な物理量の測定に対して、測定値の確率分布を定めるもの」と拡張して考えることにする。

ここまで物理学の概念的な話を実際に情報科学に当てはめてみる．従来の情報科学 (古典情報科学) においては，例えば電圧の低い高いに対して 0, 1 という古典ビットをラベル付けしていた．つまり回路の銅線という物理系を考えて，出力電圧の低い高いという物理量を測定することで 0, 1 を判定している．そして回路の入力によって出力状態は変わるが，同じ出力状態の銅線の電圧を何度測定したとしても，測定値は同じものである．

それに対し量子情報科学では，量子系を情報の担い手として利用している．そのため，入力状態は物理量の測定値の確率分布であり，出力状態も物理量の測定値の確率分布である．量子情報科学において使用される量子ビットとは「測定を行った際に，2つの測定値が確率的に起こる」量子的現象が現れる物理系を考えている．以降2つの測定値を 0, 1 とラベル付けする．量子ビットを測定することで物理量が決定し，古典ビットを得ることができる．

このように状態を確率的なものと拡張して扱うことで，古典情報科学では行えなかったことができるようになる．例えば古典情報科学において，2ビットの AND 素子に対して  $x \in \{00, 01, 10, 11\}$  であるような  $x$  を入力する．古典ビットの状態は測定値が確定的なものであるため，素子への入力は4つのうちから任意に選ぶことができるが

$\Pr[x = 00] = 0.5, \Pr[x = 11] = 0.5$  であるような不確定な入力  $x$  は受け付けていない．それに対し量子情報科学ではこのような不確定な入力も許し，それらの確率を考慮したうえで情報処理を行う．先ほどの例でいうと， $\Pr[x = 00] = 0.5, \Pr[x = 11] = 0.5$  であるので出力  $y$  は  $\Pr[y = 0] = 0.5, \Pr[y = 1] = 0.5$  となる．このような入力と計算を許すことにより，量子計算科学は特定の計算において高速に計算可能であることが期待されている．

## 2.2.2 Dirac の表記法

量子状態は複素数ベクトルを用いることで記述することができる．量子情報科学において，複素ユークリッド空間  $\mathbb{C}^d$  は Dirac の表記法を用いることが一般的であるため，まずはそれについて解説する．

まず，列ベクトルを表すケットベクトルは以下のように「 $|\cdot\rangle$ 」を使って記述する．ただし， $a, b, c \in \mathbb{C}$  とする．

$$|\psi\rangle = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{C}^3 \quad (2.4)$$

次に，共役な行ベクトルを表すブラベクトルは以下のように「 $\langle\cdot|$ 」を使って記述する．先ほどの  $|\psi\rangle$  に対して

$$\langle\psi| = \begin{pmatrix} \bar{a} & \bar{b} & \bar{c} \end{pmatrix} \quad (2.5)$$

また，ブラベクトルとケットベクトルを組み合わせることで内積や行列を表すことができ



る.  $|\psi\rangle = (a_1, \dots, a_d)^T, |\phi\rangle = (b_1, \dots, b_d)^T$  とすると

$$\langle\psi|\phi\rangle = \begin{pmatrix} \bar{a} & \bar{b} & \bar{c} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \quad (2.6)$$

$$= \sum_{i=1}^d \bar{a}_i b_i \in \mathbb{C} \quad (2.7)$$

$$|\psi\rangle\langle\phi| = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} & \bar{c} \end{pmatrix} \quad (2.8)$$

$$= \begin{pmatrix} a_1 \bar{b}_1 & \cdots & a_1 \bar{b}_d \\ \vdots & \ddots & \vdots \\ a_d \bar{b}_1 & \cdots & a_d \bar{b}_d \end{pmatrix} \quad (2.9)$$

$\langle\psi|\phi\rangle$  のことを複素ユークリッド内積と呼び, 式 (2.7) から分かるように  $\langle\psi|\psi\rangle \geq 0$  であり,

$|\psi\rangle = 0$  の時に等号が成立する. ここから  $|\psi\rangle$  の大きさを

$$\|\psi\| := \sqrt{\langle\psi|\psi\rangle} \quad (2.10)$$

で表すことができる. これをユークリッドノルムと呼ぶ.

また  $a, b \in \mathbb{C}$  であるとき, 内積には以下の式が成立する.

$$\overline{\langle\psi|\phi\rangle} = \langle\phi|\psi\rangle \quad (2.11)$$

$$\langle\psi|a\phi_1 + b\phi_2\rangle = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle \quad (2.12)$$

### 2.2.3 Dirac の表記法による量子ビットの記述

理論的に, 量子ビットはベクトル空間  $\mathbb{C}^2$  を用いて記述することができる. また, そこから状態の変化 (時間発展や量子ビットの操作) を  $\mathbb{C}^{2 \times 2}$  の複素数行列で表現することが可能になる. 以降, 量子ビットを Dirac の表記法を用いて  $|\psi\rangle \in \mathbb{C}^2$  というように表す. 特に古典ビットの 0, 1 を表す量子ビットを以下のように表す.

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \in \mathbb{C}^2 \quad (2.13)$$

このとき  $\{|0\rangle, |1\rangle\}$  はそれぞれユークリッドノルムが 1 であり, 互いの内積が 0 になることから正規直交基底になっている. ここからベクトル空間  $\mathbb{C}^2$  上のすべてのベクトル  $|\psi\rangle$  は  $a, b \in \mathbb{C}$  を用いて

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (2.14)$$

と表すことが可能である. また,  $|\psi\rangle$  は  $|0\rangle$  と  $|1\rangle$  のベクトルが足し合わされた状態であることが分かる. これを重ね合わせ状態と呼ぶ.

ただし, 量子ビットは  $\mathbb{C}^2$  であればなんでもよいわけではなく,  $\|\psi\| = 1$  となるような単位ベクトルのみである.

### 2.2.4 量子ビットの測定

量子ビットは測定したときに、2つの測定値 (例えば 0, 1) がどのような確率で現れるかを状態として記録している。測定を正規直交基底で表すことで、その量子ビットがどのような確率で測定値を出すか記述することができる。例えば量子ビット  $|\psi\rangle = (a, b)^T$ ,  $a, b \in \mathbb{C}$  があるとする。このとき 0, 1 が出る確率は  $\{|0\rangle, |1\rangle\}$  を用いて

$$\Pr[\text{測定値が } 0] = |\langle 0|\psi\rangle|^2 = |a|^2 \quad (2.15)$$

$$\Pr[\text{測定値が } 1] = |\langle 1|\psi\rangle|^2 = |b|^2 \quad (2.16)$$

で表すことが可能である。特にこの基底  $\{|0\rangle, |1\rangle\}$  を計算基底と呼ぶ。

量子ビットは測定されると状態に従って確率的にどちらかの測定値を得ることができる。このとき、 $|\psi\rangle$  の測定値が  $\phi_i$  であったとすると測定によって量子状態は

$$|\psi\rangle \mapsto |\phi_i\rangle \quad (2.17)$$

というように状態は変化する。そのため一般的に量子状態を測定したあとは同じ量子状態を使用することはできない。また、測定による量子状態の変化は不可逆的である。

### 2.2.5 量子ビットの時間発展

量子ビットは時間の経過によって状態が変化する。例えば初期状態を  $|\psi\rangle$ 、最終状態を  $|\psi'\rangle$  とする。これらは  $\mathbb{C}^2$  のベクトルであるため

$$|\psi'\rangle = U |\psi\rangle, \quad U \in \mathbb{C}^{2 \times 2} \quad (2.18)$$

と表すことができる。ただし、どちらの状態も単位ベクトルである必要があるため  $U$  は以下の条件を満たす必要がある。

$$UU^\dagger = U^\dagger U = \mathbb{I} \quad (2.19)$$

ただし  $\mathbb{I}$  は単位行列、 $U^\dagger$  は  $U$  の随伴行列 (転置させて共役した行列) である。式 (2.19) を満たす行列をユニタリ行列と呼び、式 (2.18) をユニタリ発展と呼ぶ。このユニタリ発展を用いて量子ビットの状態を変化させることで量子計算を行う。また式 (2.19) からユニタリ発展は可逆的な変化である。

### 2.2.6 多量子ビット

今までの説明は量子ビットが1つだけの時であった。次に2つの量子ビットをまとめて記述する方法を記述する。1つ目の量子ビットを  $|\psi\rangle = (a_0, a_1)^T \in \mathbb{C}^2$  とし2つ目の量子ビットを  $|\phi\rangle = (b_0, b_1)^T \in \mathbb{C}^2$  とする。このとき2つの量子ビットを合わせて

$$|\psi\rangle \otimes |\phi\rangle := \begin{pmatrix} a_0 |\phi\rangle \\ a_1 |\phi\rangle \end{pmatrix} = \begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{pmatrix} \in \mathbb{C}^4 \quad (2.20)$$

と  $\mathbb{C}^4$  のベクトルとして表現することができる。ここで使われている  $\otimes$  はテンソル積と呼ぶ。ただし、1量子ビットのときと同様に単位ベクトルである必要がある。測定は  $\mathbb{C}^4$  の正規直交基底  $\{|\phi_{i_0, i_1}\rangle\}_{i_0, i_1=\{0,1\}}$  で表される。測定値は4つあり、例えば  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  などがある。ただし  $|0\rangle \otimes |0\rangle$  は  $|00\rangle$  であり、今後はこのように省略して記述する。測定値  $\phi_{i_0, i_1}$  を得る確率は1量子ビットと同じく  $|\langle \phi_{i_0, i_1} | \psi \rangle|^2$  で与えられる。測定による状態変化は測定値  $\phi_{i_0, i_1}$  が得られたとき  $|\phi_{i_0, i_1}\rangle$  に変化する。

時間発展は  $U \in \mathbb{C}^{4 \times 4}$  のユニタリ行列で表すことができる。また、1量子ビット目  $|\psi_1\rangle$  に  $U_1 \in \mathbb{C}^{2 \times 2}$ 、2量子ビット目  $|\psi_2\rangle$  に  $U_2 \in \mathbb{C}^{2 \times 2}$  を作用させるような  $U \in \mathbb{C}^{4 \times 4}$  は以下のように表せる。

$$U |\psi_1 \psi_2\rangle = (U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = U_1 |\psi_1\rangle \otimes U_2 |\psi_2\rangle \quad (2.21)$$

ただし2量子ビットの時間発展は上記のように  $U = U_1 \otimes U_2, U \in \mathbb{C}^{4 \times 4}, U_1, U_2 \in \mathbb{C}^{2 \times 2}$  というように分解できないユニタリ行列も許しており、以下のようなユニタリ行列

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \in \mathbb{C}^{4 \times 4} \quad (2.22)$$

などがある。 $|00\rangle$  に上記の  $U$  を作用させた2量子ビットを  $|\psi\rangle \in \mathbb{C}^4$  とすると

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (2.23)$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad (2.24)$$

この状態である  $|\psi\rangle$  は式 (2.20) のように2つの量子ビットのテンソル積で表すことができない。このような状態のことをエンタングル状態と呼ぶ。これを  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  で測定してみると、 $\Pr[\text{測定値 } 00] = \Pr[\text{測定値 } 11] = 0.5, \Pr[\text{測定値 } 01] = \Pr[\text{測定値 } 10] = 0$  となる。つまり1量子ビット目と2量子ビット目の測定値は必ず同じになり、違う値にはならないという強い相関が存在する。これは古典情報科学にはない性質であり、量子情報科学において重要な性質である。

これまで2量子ビットへの拡張を説明した。次に多量子ビットへの一般化について説明する。 $n$ 量子ビットは  $|\psi\rangle \in \mathbb{C}^{2^n}$ 、 $\|\psi\| = 1$  であるような単位ベクトルで記述できる。量子ビットの合成は式 (2.20) 同様テンソル積で表現可能である。

測定は正規直交基底  $\{|\phi_{i_1, \dots, i_n}\rangle\}_{i_1, \dots, i_n=\{0,1\}}$  で与えられる。特に  $\{|i_1\rangle \otimes \dots \otimes |i_n\rangle\}_{i_1, \dots, i_n=\{0,1\}}$  は計算基底と呼ぶ。測定値  $\phi_{i_1, \dots, i_n}$  が得られる確率は  $|\langle \phi_{i_1, \dots, i_n} | \psi \rangle|^2$  で与えられ、測定後の状態は  $|\phi_{i_1, \dots, i_n}\rangle$  になる。時間発展は  $U \in \mathbb{C}^{2^n \times 2^n}$  であるユニタリ行列で与えられる。

## 2.2.7 混合状態

これまで量子ビットを増やすことを行ってきたが、次は量子ビットを減らす場合について考える。式 (2.20) のように複数量子ビットのテンソル積で表せる状態を積状態と呼び、この場

合は逆の操作で量子ビットを分けることが可能である．それに対して式 (2.24) のようなエンタングル状態から減らす場合は，今までの単位ベクトルで記述することはできない．これを解消するために混合状態というものを考える．混合状態とは，確率的に状態が決まるというものである．例えば  $1/2$  の確率で  $|\psi_1\rangle$ ,  $1/2$  の確率で  $|\psi_2\rangle$  の状態という場合である．エンタングル状態の量子ビットを減らす際はこの混合状態になる．本来であれば量子ビットは確率振幅を持っているが，いらぬ量子ビットは単なる確率として情報を潰すためである．これにより 1 量子ビット目と 2 量子ビット目の相関といった情報が不足する．例えば式 (2.24) の場合で 1 量子ビットだけにすると  $1/2$  の確率で  $|0\rangle$ ,  $1/2$  の確率で  $|1\rangle$  になる．混合状態に対して，そうでないもの (確率 1 で状態が決まるもの) を純粋状態と呼ぶ．

混合状態は，一般的に密度行列を用いて記述される． $i = 1, \dots, n$  について  $\text{Pr}[\text{状態が } |\psi_i\rangle] = p_i$  である混合状態の密度行列  $\rho$  は，以下の式で定義される．ただし  $\sum_{i=1}^n p_i = 1$  である．

$$\rho := \sum_{i=1}^n p_i |\phi_i\rangle\langle\phi_i| \quad (2.25)$$

これは純粋状態の場合でも記述が可能であるため，量子ビットのより一般的な記述になっている．

測定が正規直行基底  $\{|\phi_i\rangle_{i \in \{0,1\}^n}\}$  で与えられるとき， $M_i = |\phi_i\rangle\langle\phi_i|$  を用いて混合状態から  $\phi_i$  が得られる確率は以下の式で表される．

$$\text{Pr}[\text{測定値が } \phi_i] = \text{Tr}(M_i \rho) \quad (2.26)$$

ここで  $\text{Tr}$  はトレース演算子であり，行列の対角成分の総和をとる演算である．トレース演算子は計算基底  $\{|i\rangle_{i \in \{0,1\}^n}\}$  を用いて， $A \in \mathbb{C}^{n \times n}$  について以下のように表される．

$$\text{Tr}(A) = \sum_{i \in \{0,1\}^n} \langle i|A|i\rangle \quad (2.27)$$

式 (2.15) との関係性を見てみると， $M_0 = |0\rangle\langle 0|$ ,  $\rho = |\psi\rangle\langle\psi|$  より

$$\text{Pr}[\text{測定値が } 0] = \text{Tr}(M_0 \rho) \quad (2.28)$$

$$= \sum_{i \in \{0,1\}^n} \langle i|M_0\rho|i\rangle \quad (2.29)$$

$$= \sum_{i \in \{0,1\}^n} \langle i|M_0|\psi\rangle \langle\psi|i\rangle \quad (2.30)$$

$$= \sum_{i \in \{0,1\}^n} \langle\psi|i\rangle \langle i|M_0|\psi\rangle \quad (2.31)$$

$$= \langle\psi| \left( \sum_{i \in \{0,1\}^n} |i\rangle\langle i| \right) M_0 |\psi\rangle \quad (2.32)$$

$$= \langle\psi|0\rangle \langle 0|\psi\rangle \quad (2.33)$$

$$= |\langle 0|\psi\rangle|^2 \quad (2.34)$$

よって式 (2.15) を満たしていることが分かる．

密度演算子  $\rho$  から  $\rho'$  へのユニタリ発展は、ユニタリ行列  $U$  を用いて以下の式で表される。

$$\rho' = \sum_{i=1}^n p_i |\psi'\rangle\langle\psi'| \quad (2.35)$$

$$= \sum_{i=1}^n p_i U |\psi\rangle\langle\psi| U^\dagger \quad (2.36)$$

$$= U \rho U^\dagger \quad (2.37)$$

最後に、不要な量子ビットを減らし混合状態にする操作について説明する。多量子ビットから一部の量子ビットだけになった混合状態を縮約状態と呼ぶ。縮約状態は部分トレースという演算で求めることが可能である。密度演算子  $\rho_{SE}$  で記述された量子ビットを二つのグループ  $S, E$  に分ける場合を考える。このとき  $S$  の量子ビットだけを残したような縮約状態を  $\rho_S$  とすると  $E$  の部分トレースは

$$\rho_S = \text{Tr}_E(\rho_{SE}) \quad (2.38)$$

と記述する。次に具体的な演算方法を説明する。 $n$  量子ビットの密度演算子を  $c_{i_1 \dots i_n, j_1 \dots j_n} \in \mathbb{C}$  として

$$\rho_{SE} = \sum_{\substack{i_1 \dots i_n \in \{0,1\}^n \\ j_1 \dots j_n \in \{0,1\}^n}} c_{i_1 \dots i_n, j_1 \dots j_n} |i_1 \dots i_n\rangle \langle j_1 \dots j_n| \in \mathbb{C}^{2^n \times 2^n} \quad (2.39)$$

と記述する。説明の簡略化のために前半の  $g$  量子ビットを  $E$ 、後半の  $h$  量子ビットを  $S$  として分ける。このとき  $E$  の部分トレースは以下ようになる。

$$\text{Tr}_E(\rho_{SE}) = \sum_{\substack{i_1 \dots i_g \dots i_n \in \{0,1\}^n \\ j_1 \dots j_g \dots j_n \in \{0,1\}^n}} c_{i_1 \dots i_g \dots i_n, j_1 \dots j_g \dots j_n} \langle i_1 \dots i_g | j_1 \dots j_g \rangle |i_{g+1} \dots i_n\rangle \langle j_{g+1} \dots j_n| \quad (2.40)$$

計算基底の正規直交性から

$$\langle i_1 \dots i_g | j_1 \dots j_g \rangle = \begin{cases} 1 & (i_1 \dots i_g = j_1 \dots j_g) \\ 0 & (i_1 \dots i_g \neq j_1 \dots j_g) \end{cases} \quad (2.41)$$

であるので式 (2.40) は

$$\text{Tr}_E(\rho_{SE}) = \sum_{\substack{i_{g+1} \dots i_n \in \{0,1\}^h \\ j_{g+1} \dots j_n \in \{0,1\}^h}} \sum_{k_1 \dots k_g \in \{0,1\}^g} c_{k_1 \dots k_g i_{g+1} \dots i_n, k_1 \dots k_g j_{g+1} \dots j_n} |i_{g+1} \dots i_n\rangle \langle j_{g+1} \dots j_n| \quad (2.42)$$

式 (2.42) から  $\text{Tr}_E(\rho_{SE}) \in \mathbb{C}^{2^h \times 2^h}$  であることが分かる。

## 2.3 量子領域計算量クラス

2.1 節において説明した古典的な領域計算量クラスと同様に、量子版の領域計算量クラスも存在する。Watrous の研究 [17] などでは量子チューリングマシンというものを考え、これの領域複雑度から量子領域計算量クラスを定義している。これは領域計算量クラスにおける古典情報科学から量子情報科学への自然な拡張であるが、考案されている量子アルゴリズムは量子回路モデルで説明されることが多く、現在では量子回路モデルを用いた領域計算量クラスの表現が一般的である。よってここでは Fefferman らの定義 [8] を引用し説明する。

**定義 2.3.1.** (量子領域計算量クラス)  $k(n)$  を  $\Omega(\log(n)) \leq k(n) \leq \text{poly}(n)$  を満たす関数とする. ただし  $\text{poly}(n) = n^{\mathcal{O}(1)}$  とする. このとき問題  $L = (L_{yes}, L_{no})$  が以下を満たすとき, 問題  $L$  は  $\text{Q}_{\text{U}}\text{USPACE}[k(n)](c, s)$  に含まれるという.

実行時間が  $\text{poly}(|x|)$  で領域複雑度が  $\mathcal{O}(k)$  である古典チューリングマシンから生成される量子回路  $\{Q_x\}_{x \in \{0,1\}^*}$  が存在する. ただし量子回路  $Q_x = U_{x,T}U_{x,T-1} \cdots U_{x,1}$  は  $T = 2^{\mathcal{O}(k)}$  個のゲートを持ち,  $\mathcal{O}(k(|x|))$  である  $n_c$  個の量子ビット上で動作する中間測定を含まない量子回路とする. また  $|\phi_i\rangle = |1\rangle \otimes |i\rangle$  としたとき, 出力状態は以下を満たす.  
もし  $x \in L_{yes}$  ならば

$$\sum_{i \in \{0,1\}^{n_c-1}} \langle 0^{n_c} | Q_x^\dagger |\phi_i\rangle \langle \phi_i| Q_x | 0^{n_c} \rangle \geq c \quad (2.43)$$

もし  $x \in L_{no}$  ならば

$$\sum_{i \in \{0,1\}^{n_c-1}} \langle 0^{n_c} | Q_x^\dagger |\phi_i\rangle \langle \phi_i| Q_x | 0^{n_c} \rangle \leq s \quad (2.44)$$

ここで定義 2.3.1 の意味について説明する. チューリングマシンモデルでは入力長が変化しても同じチューリングマシンで動作可能だが, 回路モデルにおいては入力長が変化するたびにそれに合わせた回路を用意する必要がある. よって回路モデルによる領域計算量クラスの定義では, 古典チューリングマシンによって回路を生成する.

次に中間測定について説明する. 中間測定とは, 回路内において途中で測定を行うことである. 2.2.4 節で説明した通り, 測定という操作は量子状態を測定する基底に変化させるものであり, 不可逆的な操作であった. これに対し 2.2.5 節で説明したユニタリ発展は可逆的な変化であるため, 測定による変化と根本的に異なる. 古典計算と異なり, 量子計算においては中間測定がない限り逆の操作が存在し, これを利用した量子アルゴリズムも存在する. よって量子計算量理論において, 中間測定を含む量子回路と含まないものは, 計算資源の異なるものとして分けて考えられている. 中間測定を含む量子回路と含まない量子回路間の関係性に関する研究は, 文献 [12] や [11], [8] などが存在する.

次に式 (2.43) の意味について解説する.  $\langle 0^{n_c} | Q_x^\dagger |\phi_i\rangle$  と  $\langle \phi_i | Q_x | 0^{n_c} \rangle$  は互いに共役であるため, 以下の式変形が成り立つ.

$$\langle 0^{n_c} | Q_x^\dagger |\phi_i\rangle \langle \phi_i| Q_x | 0^{n_c} \rangle = |\langle \phi_i | Q_x | 0^{n_c} \rangle|^2 \quad (2.45)$$

式 (2.15) より, これは  $|0^{n_c}\rangle$  に対して量子回路  $Q_x$  でユニタリ発展させた状態に対して, 測定したとき  $\phi_i$  が得られる確率を示している. また  $\phi_i$  は必ず先頭ビットが 1 であり, 先頭以外のビットパターンすべてに対して総和をとっているため,  $\sum_{i \in \{0,1\}^{n_c-1}} \langle 0^{n_c} | Q_x^\dagger |\phi_i\rangle \langle \phi_i| Q_x | 0^{n_c} \rangle$  は, 量子回路  $Q_x$  にすべてが 0 である量子ビット  $|0^{n_c}\rangle$  を入力した際に, 出力量子ビットの先頭ビットから 1 が得られる確率を示している.

古典における確率的領域計算量クラスと同じく,  $\text{BQ}_{\text{U}}\text{USPACE}[k(n)] = \text{Q}_{\text{U}}\text{USPACE}[k(n)](2/3, 1/3)$  であり,  $k(n)$  が  $\mathcal{O}(\log n)$  のとき  $\text{BQ}_{\text{U}}\text{L}$  である. また, 量子回路に中間測定を含んでいるものを  $\text{BQ}_{\text{Q}}\text{L}$  と呼び, 中間測定の結果を用いて適用させる量子素子を変更するという操作まで許したものを  $\text{BQL}$  と呼ぶ. これらの量子対数領域計算量クラスについて, Girish ら [11] や Fefferman ら [8] によって  $\text{BQ}_{\text{U}}\text{L} = \text{BQ}_{\text{Q}}\text{L} = \text{BQL}$  であることが示されている. つまり量子対数領域計算において, 中間測定の有無は計算能力に関係ないことが分かる.

## 第3章 先行研究

### 3.1 Doron らの研究 [6]

Doron らは確率的対数領域計算量における確率行列の第二固有値近似について、ある条件下において BPL 完全であることを示した [6]。ここで確率行列  $A$  とは、 $A \in \mathbb{R}_{\geq 0}^{n \times n}$  であり、すべての  $0 \leq j \leq n$  に対して  $\sum_{i=0}^n A[i][j] = 1$  を満たす。ただし  $A[i][j]$  は行列  $A$  の  $i$  行  $j$  列の要素とする。この研究により BPL 完全である自然な問題が示された。

#### 3.1.1 第二固有値問題

第二固有値問題は以下で定義される。

**定義 3.1.1.** ( $2\text{ndEV}_{\alpha,\beta}$ ) 入力として  $0 \leq \alpha < \beta < 1$  と、次元が  $n$  であり固有値が  $\lambda_1, \dots, \lambda_n$  である確率行列  $A$  を受け取る。ただし問題の制約として、必ず  $\lambda_2 \in \mathbb{R}$  であり  $|\lambda_n| \leq \dots \leq |\lambda_3| \leq 1 - \beta$  である。このとき Yes/No 各インスタンスは以下で定められる。

**Yes インスタンス :**  $\lambda_2 \leq 1 - \beta$

**No インスタンス :**  $\lambda_2 \geq 1 - \alpha$

ここで確率行列より、必ず  $\lambda_1 = 1$  である。 $\lambda_1, \dots, \lambda_n$  に対応する固有ベクトルを  $v_1, \dots, v_n$  としたとき、任意のベクトル  $w \in \mathbb{R}_{\geq 0}^n$  はある定数  $c_1, \dots, c_n$  を用いて  $w = c_1 v_1 + \dots + c_n v_n$  と書くことができる。ここで  $w$  に対して  $A$  を  $k$  回掛けると  $A^k w = c_1 \lambda_1^k v_1 + \dots + c_n \lambda_n^k v_n$  となり、各固有値の大きさが小さければ小さいほど  $w$  は  $c_1 v_1$  に早く収束することが分かる。よって第二固有値の大きさを判定するこの問題は、確率行列  $A$  に従うランダムウォークがどれだけ早く収束するかを求める際に役に立つ。そういった意味でこの問題は現実における自然な問題であり、この問題がこういった領域計算量クラスに属するのか調べることは重要である。

#### 3.1.2 BPL 完全性

Doron らはこの第二固有値問題  $2\text{ndEV}_{\alpha,\beta}$  に対し、 $\alpha, \beta$  のパラメータを調整することで確率的領域計算量クラスとの関係を示した。ここではその中でも BPL 完全性について説明する。

Doron らはまず、以下の定理を示した。

**定理 3.1.2.**  $\zeta$  を  $0 < \zeta \leq 1/2$  とする。このとき、 $2\text{ndEV}_{\zeta, 2\zeta}$  は領域複雑度  $\mathcal{O}(\log n + \log 1/\zeta)$  である確率的チューリングマシンで、Yes インスタンスを受理する確率が  $2/3$  以上、No インスタンスを受理する確率が  $1/3$  以下であるような確率で解くことができる。

彼らの大まかな証明の流れとしては、確率行列  $A$  の冪乗を計算することで第二固有値問題を BPL に帰着している。  $m$  を  $(1-\zeta)^m = 1/n^2$  となるようなものとする。このとき  $\text{Tr}(A^m)$  の値を考える。確率行列  $A$  はジョルダン標準形を用いて  $A = VJV^{-1}$  と書くことができる。このとき  $J$  は上三角行列であり、対角要素には左上から  $\lambda_1, \dots, \lambda_n$  となっている。すると  $A^m = VJ^mV^{-1}$  となり、  $J$  は上三角行列より対角要素は左上から  $\lambda_1^m, \dots, \lambda_n^m$  となる。  $\text{Tr}$  は行列の対角要素の総和をとる演算なので  $\text{Tr}(A^m) = \sum_{k=1}^n \lambda_k^m$  となる。また、  $A$  は正の実数行列なので  $\text{Tr}(A^m) = |\text{Tr}(A^m)|$  となる。

次に Yes インスタンスの場合に  $\text{Tr}(A^m)$  がどのような値になるかを確認する。

$$\text{Tr}(A^m) = \left| \sum_{k=1}^n \lambda_k^m \right| \leq \sum_{k=1}^n |\lambda_k|^m \leq 1 + n(1-2\zeta)^m \leq 1 + n(1-\zeta)^{2m} = 1 + \frac{1}{n^3} \quad (3.1)$$

これに対し No インスタンスの場合、  $\lambda_2$  が正の実数であることに注意して

$$\text{Tr}(A^m) \geq 1 + \lambda_2^m - \left| \sum_{k=3}^n \lambda_k^m \right| \geq 1 + (1-\zeta)^m - n(1-2\zeta)^m \geq 1 + \frac{1}{n^2} - \frac{1}{n^3} \quad (3.2)$$

よって  $\text{Tr}(A^m)$  を  $1/n^4$  の精度、つまり  $A^m$  の各要素を  $1/n^5$  の精度で計算できればよい。ここで、  $A$  が確率行列であることから、ランダムウォークを用いて以下の補題が加法的チェルノフ限界から導くことができる。

**補題 3.1.3.** 確率行列  $A \in \mathbb{R}_{\geq 0}^{n \times n}$  と  $s, t \in \mathbb{N}_{\leq n}, k \in \mathbb{N}$  を受け取り、  $n$  頂点上における  $s$  番目の頂点から  $A$  の遷移確率に従ってランダムウォークを独立に  $T$  回行う確率的アルゴリズムを考える。また一回のランダムウォークにおける長さを  $k$  とし、一回のランダムウォーク中に頂点  $t$  を通ることができれば 1 を、そうでない場合 0 を出力するとする。このとき  $i$  回目のランダムウォークにおけるアルゴリズムの出力を  $Y_i$  とすると、各  $i$  における  $Y_i$  の期待値は  $A^k[s, t]$  となる。よって加法的チェルノフ限界から

$$\Pr \left[ \left| \frac{1}{T} \sum_{i=1}^T Y_i - A^k[s, t] \right| \geq \epsilon \right] \leq 2e^{-2\epsilon^2 T} \quad (3.3)$$

となる。このときアルゴリズムは  $\mathcal{O}(\log(Tnk))$  の領域を使う。

ここで  $\delta = 2e^{-2\epsilon^2 T}$  とすると

$$T = \frac{\log(2/\delta)}{2\epsilon^2} \quad (3.4)$$

ここでは  $A^m$  の各要素を  $1/n^5$  の精度で計算できればよいので、  $\epsilon = 1/n^5, \delta = 1/3n$  というパラメータで動作するアルゴリズムが存在すれば  $2\text{ndEV}_{\zeta, 2\zeta}$  を解くことができる。このとき、このアルゴリズムの使用する領域は  $\mathcal{O}(\log(nm))$  である。よって定理 3.1.2 を示すことができる。

次に、  $\zeta = 1/n$  であるとき  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  が BPL 完全となることについて説明する。すでに定理 3.1.2 においてこの問題が BPL に含まれていることが分かっているので、BPL 困難性を示すことができればよい。Doron らの大まかな証明の流れとしては、BPL 問題を解く確率的チューリングマシンの出力結果を  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  で模倣するということを考えている。

まず言語  $L$  を受理する、領域複雑度  $c \log n_0$  であり計算時間  $T = n_0^c$  である確率的チューリングマシンを  $M$  とする。入力  $x$  における  $M$  の構成グラフを  $G = (V, E)$  とし、  $s \in V$  を初期頂点、  $t \in V$  を一意の受理頂点とする。



次に  $G$  を層状にしたグラフ  $G' = (V', E')$  を考える.  $V' = V \times \{1, \dots, T+1\}$ ,  $i, j \in V$  としたとき  $(i, j) \in E$  であれば,  $1 \leq l \leq T$  において  $((i, l), (j, l+1)) \in E'$  とする. つまり,  $G'$  は各層  $|v|$  個の頂点を持つ  $T+1$  層状のグラフであり,  $G$  において  $i$  から  $j$  への辺がある場合は  $l$  層の頂点  $i$  から  $l+1$  層の頂点  $j$  への辺が存在するグラフとなっている.

最後に  $G'' = (V'', E'') = G''(M, x)$  というグラフを考える.  $V'' = \{(v', k) | v' \in V', k \in \{1, 2\}\}$  とする. また  $E''$  は以下を満たす辺の集合とする.

- 全ての  $(a, b) \in E'$  と  $k \in \{1, 2\}$  について,  $((a, k), (b, k)) \in E''$
- $r \neq t$  である全ての  $r \in V$  と  $k \in \{1, 2\}$  について,  $((r, T+1), k), ((s, 1), k)) \in E''$
- $((t, T+1), 1), ((s, 1), 2)) \in E''$  かつ  $((t, T+1), 2), ((s, 1), 1)) \in E''$

つまり, グラフ  $G''$  は  $G'$  を二つ持っており, それぞれの最後の層における  $t$  以外の頂点は同じ  $G'$  にある最初の層の頂点  $s$  へ,  $t$  は別の  $G'$  にある最初の層の頂点  $s$  へと辺を追加したものである.

それぞれのグラフの例を図 3.1, 図 3.2, 図 3.3 に示す.

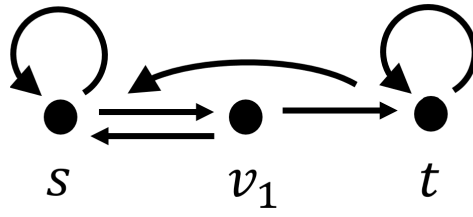


図 3.1: グラフ  $G$  の例

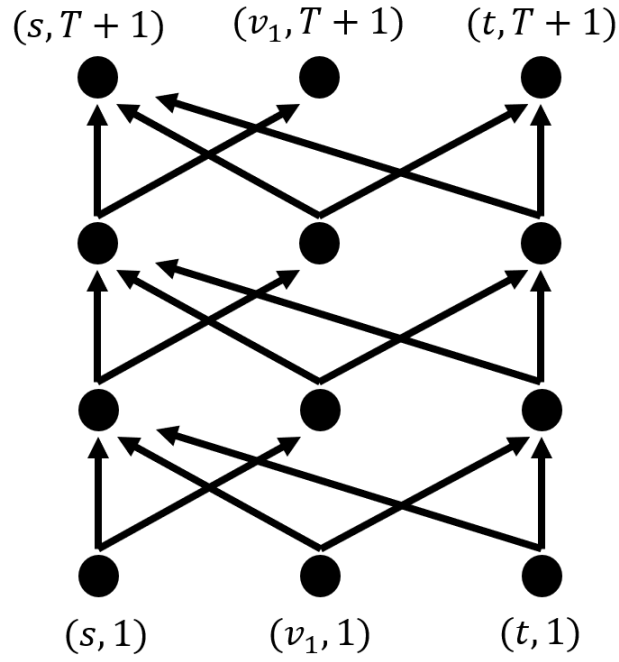


図 3.2:  $T = 3$  の場合におけるグラフ  $G'$  の例

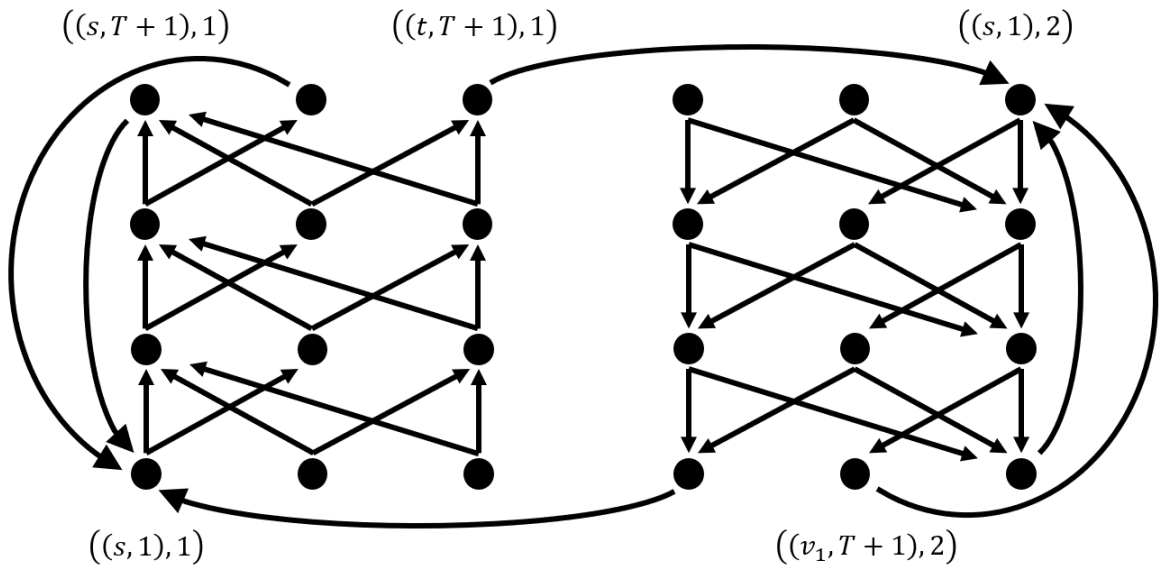


図 3.3: グラフ  $G''$  の例

Doron らは  $G''$  の遷移行列を  $A$  としたとき、以下の補題を示した。

**補題 3.1.4.**  $p = p(M, x) = A^T[s, t]$  を、 $M$  が  $x$  を受理する確率とし、 $\omega$  を 1 の原始  $T+1$  冪根とする。このとき  $A$  の固有値は  $\{0, \omega^k, (1-2p)^{\frac{1}{T+1}}\omega^k | 0 \leq k \leq T\}$  である。

このとき  $A$  は確率行列である。また  $B = \frac{1}{2}A + \frac{1}{2}I_{n \times n}$  とする。このとき  $B$  の任意の固有値と固有ベクトルを  $\lambda, v$  とすると、

$$Bv = \frac{1}{2}Av + \frac{1}{2}Iv \quad (3.5)$$

$$\lambda v = \frac{1}{2}\lambda v + \frac{1}{2}v \quad (3.6)$$

$$= \left(\frac{1}{2} + \frac{1}{2}\lambda\right)v \quad (3.7)$$

となる。ここから  $A$  の第  $i$  固有値を  $\lambda'_i$  とすると  $B$  の第  $i$  固有値は  $\frac{1}{2} + \frac{1}{2}\lambda'_i$  となることが分かる。よって  $B$  の固有値は補題 3.1.4 より  $\{\frac{1}{2}, \frac{1}{2} + \frac{1}{2}\omega^k, \frac{1}{2} + \frac{1}{2}(1-2p)^{\frac{1}{T+1}}\omega^k | 0 \leq k \leq T\}$  である。Doron らは確率的チューリングマシンの受理確率を  $p$  としたとき  $B$  の第二固有値が  $\frac{1}{2} + \frac{1}{2}(1-2p)^{\frac{1}{T+1}}\omega^0$  となることから、一般性を損なわずに受理確率  $p$  を上手く設定することによって、BPL を受理する確率的チューリングマシンの出力結果を  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  で模倣できることを示した。

最後に Doron らが示した補題 3.1.4 の証明について説明する。まず  $W = A^\dagger$  とし、 $\lambda \neq 0$  である  $w$  の固有値に対して、固有ベクトルを  $v$  とする。このとき  $A$  と  $W$  の固有値は同じである。また  $A[i][j] = W[j][i] = a_{i,j}, v[i] = v_i$  とする。

ある頂点を  $z$  としたとき、 $Wv[z]$  は

$$Wv[z] = \sum_{i=1}^n a_{i,z}v_i \quad (3.8)$$

である。ある頂点  $i$  から遷移行列  $A$  に従って 1 ステップランダムウォークした際に頂点  $z$  になる確率は  $a_{i,z}$  であり、 $v[i]$  をランダムウォーク中のあるステップにおける頂点  $i$  に存在する確率としたとき、次のステップで頂点  $z$  にいる確率は  $a_{i,z}v_i$  となる。よって  $Wv[z]$  は、各頂点にいる確率分布が  $v$  であるとき、ランダムウォーク 1 ステップ後に頂点  $z$  にいる確率となる。ここで  $j \neq s$  である頂点  $j \in V$  について、頂点  $((j, 1), 1), ((j, 1), 2)$  の入力辺は存在しないので、 $Wv = \lambda v$  と  $\lambda \neq 0$  から

$$v[((j, 1), 1)] = v[((j, 1), 2)] = 0 \quad (3.9)$$

となる。

$v[((s, 1), 1)] = x, v[((s, 1), 2)] = y$  とし、すべての  $j \in V$  と  $l \geq 0$  に対して、 $W^{l-1}[j, s]$  を頂点  $s$  から遷移行列  $A$  に従って  $l-1$  ステップだけランダムウォークしたときに頂点  $j$  に到達する確率とする。このとき固有ベクトル  $v$  の各要素は以下ようになる。

$$v[((j, l), 1)] = \frac{x}{\lambda^{l-1}}W^{l-1}[j, s] \quad (3.10)$$

$$v[((j, l), 2)] = \frac{y}{\lambda^{l-1}}W^{l-1}[j, s] \quad (3.11)$$

式 (3.10) と式 (3.11) は帰納法から示すことができる。 $l=1$  の場合、 $v[((j, 1), 1)] = xW^0[j, s]$  より成り立つ。 $l$  のとき式 (3.10) が成り立つと仮定すると、 $Wv$  の要素は

$$(Wv)[((j, l+1), 1)] = \sum_{k: (k, j) \in E} v[((k, l), 1)] \cdot \frac{1}{d_{\text{out}}(k)} \quad (3.12)$$

となる．ただし  $d_{\text{out}}(k)$  は頂点  $k$  の出力辺数である．仮定より式 (3.12) は

$$(Wv)[((j, l+1), 1)] = \sum_{k:(k,j) \in E} \frac{x}{\lambda^{l-1}} W^{l-1}[k, s] \cdot \frac{1}{d_{\text{out}}(k)} \quad (3.13)$$

$$= \frac{x}{\lambda^{l-1}} \sum_{k:(k,j) \in E} W^{l-1}[k, s] \cdot \frac{1}{d_{\text{out}}(k)} \quad (3.14)$$

$$= \frac{x}{\lambda^{l-1}} W^l[j, s] \quad (3.15)$$

$Wv = \lambda v$  なので

$$v[((j, l+1), 1)] = \frac{x}{\lambda^l} W^l[j, s] \quad (3.16)$$

よって  $l+1$  でも式 (3.10) が成り立つことが分かる．式 (3.11) に関しても同様に示すことができる．

$Wv[z]$  は、各頂点にいる確率分布が  $v$  であるとき、ランダムウォーク 1 ステップ後に頂点  $z$  にいる確率であったので以下の式が成り立つ．

$$(Wv)[((s, 1), 1)] = \sum_{j \in V: j \neq t} v[((j, T+1), 1)] + v[((t, T+1), 2)] \quad (3.17)$$

$$= \frac{(1-p)x}{\lambda^T} + \frac{py}{\lambda^T} \quad (3.18)$$

$$\lambda x = \frac{(1-p)x}{\lambda^T} + \frac{py}{\lambda^T} \quad (3.19)$$

$(Wv)[((s, 1), 2)]$  に関しても同様に以下式が成り立つ．

$$\lambda y = \frac{(1-p)y}{\lambda^T} + \frac{px}{\lambda^T} \quad (3.20)$$

式 (3.19) と式 (3.20) より

$$\lambda(x+y) = \frac{1}{\lambda^T}(x+y) \quad (3.21)$$

$$x+y = \frac{1}{\lambda^{T+1}}(x+y) \quad (3.22)$$

よって  $x \neq y$  ならば  $\lambda^{T+1} = 1$ ,  $x = -y$  ならば式 (3.19) より

$$\lambda^{T+1}x = (1-2p)x \quad (3.23)$$

$v \neq 0$  であるので,  $x \neq 0$  より

$$\lambda^{T+1} = 1 - 2p \quad (3.24)$$

よって補題 3.1.4 は示された．

## 3.2 Girish らの研究 [11]

本研究と直接関係はないが、量子領域計算量クラスに関する重要な研究成果として Girish らの研究 [11] について説明する．彼らは contraction 行列という特定の性質をもった行列の冪乗を計算する中間測定なしの量子対数領域アルゴリズムを示した．またこれにより、 $\text{BQ}_U\text{L} = \text{BQ}_Q\text{L}$  を示した．

### 3.2.1 アルゴリズムの入出力

Girish らの提案したアルゴリズムでは、入力として  $A \in \mathbb{C}^{n \times n}$  である contraction 行列,  $\|v\| = \|w\| = 1$  であるベクトル  $v, w \in \mathbb{C}^n, T \leq \text{poly}(n)$  を受け取る. そしてアルゴリズムは,  $|w^\dagger A^T v|^2$  を  $n$  の逆多項式的に小さい加法誤差の精度で出力する. ここで contraction 行列とはスペクトルノルム  $\|A\| \leq 1$  を満たすことをいう.

### 3.2.2 アルゴリズムの概要

彼らの提案したアルゴリズムは主に  $|0^n\rangle$  から  $|v\rangle, |w\rangle$  を生成する回路と,  $A$  の冪乗を行う回路から成り立っている. ここで  $A$  はユニタリ行列ではないので, そのまま量子回路として表現することは出来ない. これに対し, 彼らはあるユニタリ行列の中に行列  $A$  を埋め込むという手法で量子計算に落とし込んでいる. この手法はブロックエンコーディングと呼ばれ, 現在様々な量子アルゴリズムに利用されている. ここでは, 彼らの提案したアルゴリズムがどのようにブロックエンコーディングを用いて  $A^T$  を計算しているか説明する. ここでは説明簡略化のため, 各量子回路は誤差なく実装可能であるものとする. また, 実際には量子回路による計算途中で必要となる補助量子ビットが存在するが, ないものとして考える. また, 4 量子ビットにおける  $|0101\rangle$  は  $|5\rangle$  と置くなど, 2 進数表記で書かれた量子ビットを 10 進数で表記するものとする.

まず, この量子回路には 2 つの量子ビット列が存在する. 1 つはカウンタレジスタと呼ばれ,  $\log 2T$  量子ビット存在する. もう 1 つはベクトルレジスタと呼ばれ,  $\log n$  量子ビットである. ただし説明簡略化のため,  $\log 2T, \log n \in \mathbb{N}$  とする. それぞれのレジスタは最初, すべて 0 で初期化されている. また, 行列  $A_1, A_2, U_A, V_A$  を以下のように定義する. ただし  $I_n$  は次元  $n$  の単位行列とする.

$$A_1 = \sqrt{I_n - AA^\dagger} \in \mathbb{C}^{n \times n} \quad (3.25)$$

$$A_2 = \sqrt{I_n - A^\dagger A} \in \mathbb{C}^{n \times n} \quad (3.26)$$

$$U_A = \begin{pmatrix} A & A_1 \\ A_2 & -A^\dagger \end{pmatrix} \in \mathbb{C}^{2n \times 2n} \quad (3.27)$$

$$V_A = |0\rangle\langle 0| \otimes U_A + |1\rangle\langle 1| \otimes U_A^\dagger = \begin{pmatrix} U_A & 0 \\ 0 & U_A^\dagger \end{pmatrix} \in \mathbb{C}^{4n \times 4n} \quad (3.28)$$

$A$  が contraction 行列であるとき,  $U_A, V_A$  はユニタリ行列となる.

次に, 彼らの研究において核となっている,  $|w^\dagger A^T v|^2$  の確率で 1 を出力するアルゴリズムの大まかな流れを示す. このアルゴリズムで用いられる量子回路をパーツとして用いることで, Marriott-Watrous 増幅 [13] から  $|w^\dagger A^T v|^2$  や  $w^\dagger A^T v$  を計算することが出来る. 詳しくは文献 [11] を参考されたい.

---

**アルゴリズム 1** Girish らの提案アルゴリズム

---

- 1:  $Q_v |0\rangle = |v\rangle$  となる量子回路  $Q_v$  をベクトルレジスタに適用
  - 2: **for**  $T$  回繰り返し **do**
  - 3:   カウンタレジスタの下位 2 量子ビットとベクトルレジスタに  $V_A$  を適用
  - 4:    $|0\rangle \mapsto |0\rangle, i = 1, \dots, 2T - 3$  において  $|i\rangle \mapsto |i + 2\rangle$ ,  
 $|2T - 2\rangle \mapsto |1\rangle, |2T - 1\rangle \mapsto |2\rangle$  となる順列をカウンタレジスタに適用
  - 5: **end for**
  - 6:  $Q_w |0\rangle = |w\rangle$  となる量子回路  $Q_w^\dagger$  をベクトルレジスタに適用
  - 7: すべてのレジスタを計算基底で測定し,  $|0\rangle$  であれば 1 を, そうでない場合 0 を出力
- 

このアルゴリズムがどのようにして冪乗の計算を行っているか, 各ステップにおけるレジスタの状態を追うことで説明する. ここでカウンタレジスタを  $|\cdot\rangle_c$ , ベクトルレジスタを  $|\cdot\rangle_v$  とする. レジスタの初期状態は  $|0\rangle_c \otimes |0\rangle_v$  であり, ステップ 1 を行うことで以下の状態に変化する.

$$|0\rangle_c \otimes |0\rangle_v \mapsto |0\rangle_c \otimes |v\rangle_v \quad (3.29)$$

次にステップ 3 を行う.

$$V_A(|00\rangle \otimes |v\rangle_v) = (|0\rangle\langle 0| \otimes U_A + |1\rangle\langle 1| \otimes U_A^\dagger)(|0\rangle \otimes \begin{pmatrix} |v\rangle_v \\ 0 \end{pmatrix}) \quad (3.30)$$

$$= |0\rangle\langle 0| |0\rangle \otimes U_A \begin{pmatrix} |v\rangle_v \\ 0 \end{pmatrix} + |1\rangle\langle 1| |0\rangle \otimes U_A^\dagger \begin{pmatrix} |v\rangle_v \\ 0 \end{pmatrix} \quad (3.31)$$

$$= |0\rangle \otimes \begin{pmatrix} A|v\rangle_v \\ A_2|v\rangle_v \end{pmatrix} + 0 \quad (3.32)$$

$$= |00\rangle \otimes A|v\rangle_v + |01\rangle \otimes A_2|v\rangle_v \quad (3.33)$$

次にステップ 4 を行う.

$$|0\rangle_c \otimes A|v\rangle_v + |1\rangle_c \otimes A_2|v\rangle_v \mapsto |0\rangle_c \otimes A|v\rangle_v + |3\rangle_c \otimes A_2|v\rangle_v \quad (3.34)$$

この状態でもう一度ステップ 3 を行うと以下ようになる.

$$V_A(|00\rangle \otimes A|v\rangle_v + |11\rangle \otimes A_2|v\rangle_v) = |0\rangle \otimes U_A \begin{pmatrix} A|v\rangle_v \\ 0 \end{pmatrix} + |1\rangle \otimes U_A^\dagger \begin{pmatrix} 0 \\ A_2|v\rangle_v \end{pmatrix} \quad (3.35)$$

$$= |00\rangle \otimes A^2|v\rangle_v + |01\rangle \otimes A_2A|v\rangle_v \\ + |10\rangle \otimes A_2^2|v\rangle_v + |11\rangle \otimes -AA_2|v\rangle_v \quad (3.36)$$

このときすべてのレジスタについて状態を見てみると

$$|0\rangle_c \otimes A^2|v\rangle_v + |1\rangle_c \otimes A_2A|v\rangle_v + |2\rangle_c \otimes A_2^2|v\rangle_v + |3\rangle_c \otimes -AA_2|v\rangle_v \quad (3.37)$$

となっており, ステップ 3 では  $|0\rangle_c$  であるような部分空間におけるベクトルレジスタに  $A$  を適用させていることが分かる. また 1 回目のステップ 3 を適用した直後の状態である式

(3.33) にステップ 4 を適用させずにステップ 3 を適用すると以下ようになる。

$$\begin{aligned} |00\rangle \otimes A|v\rangle_v + |01\rangle \otimes A_2|v\rangle_v &\mapsto \\ &|00\rangle \otimes A^2|v\rangle_v + |01\rangle \otimes A_2A|v\rangle_v + \\ &|00\rangle \otimes A_1A_2|v\rangle_v + |01\rangle \otimes -A^\dagger A_2|v\rangle_v \end{aligned} \quad (3.38)$$

$$= |00\rangle \otimes (A^2 + A_1A_2)|v\rangle_v + |01\rangle \otimes (A_2A - A^\dagger A_2)|v\rangle_v \quad (3.39)$$

このとき、 $|0\rangle_c$  であるような部分空間におけるベクトルレジスタには  $A$  以外の行列が適用されてしまうことが分かる。これはステップ 3 の前に  $|1\rangle_c$  の部分空間におけるベクトルレジスタの位相が 0 でないために引き起こされる。よってステップ 4 の操作は  $|1\rangle_c$  の部分空間におけるベクトルレジスタの位相を別の部分空間へ移すことで、 $|0\rangle_c$  であるような部分空間におけるベクトルレジスタへの影響を取り除く意味がある。

ここでステップ 3,4 を  $T$  回行ったときのレジスタの状態は以下になる。ただし  $|\perp\rangle_{cv}$  は、すべてのベクトルレジスタの状態  $|\psi\rangle$  に対して  $\langle 0|_c \langle \psi|_v |\perp\rangle_{cv} = 0$  となるカウンタレジスタとベクトルレジスタの状態である。

$$|0\rangle_c \otimes A^T|v\rangle_v + |\perp\rangle_{cv} \quad (3.40)$$

次にステップ 6 で量子回路  $Q_w^\dagger$  をベクトルレジスタに適用する。このとき、ベクトルの状態は以下になる。

$$(I_{2T} \otimes Q_w^\dagger)(|0\rangle_c \otimes A^T|v\rangle_v + |\perp\rangle_{cv}) \quad (3.41)$$

最後にステップ 7 で計算基底で測定を行う。この時  $|0\rangle_c \otimes |0\rangle_v$  である確率は式 (2.15) より

$$\begin{aligned} &\left| (\langle 0|_c \otimes \langle 0|_v)(I_{2T} \otimes Q_w^\dagger)(|0\rangle_c \otimes A^T|v\rangle_v + |\perp\rangle_{cv}) \right|^2 \\ &= \left| (\langle 0|_c \otimes \langle w|_v)(|0\rangle_c \otimes A^T|v\rangle_v + |\perp\rangle_{cv}) \right|^2 \\ &= \left| 1 \otimes \langle w|A^T|v\rangle_v + 0 \right|^2 \\ &= \left| w^\dagger A^T v \right|^2 \end{aligned} \quad (3.42)$$

よってアルゴリズムは  $|w^\dagger A^T v|^2$  の確率で 1 を出力することが分かる。

### 3.2.3 BQ<sub>U</sub>L = BQ<sub>Q</sub>L

Gilish らは contraction 行列の冪乗を計算できることから BQ<sub>U</sub>L = BQ<sub>Q</sub>L を示した。詳しい内容については、2.2 節で紹介した量子情報科学の基礎的な知識のみでは説明できないため省略する。詳しくは文献 [11] を参考されたい。

大まかな証明のアイデアは、contraction 行列の冪乗を用いて BQ<sub>Q</sub>L の回路を模倣することである。任意のユニタリ行列  $U_1, U_2$  について、 $U_1U_2, U_1 \otimes U_2$  はともにユニタリ行列である。よって中間測定のない量子回路は、回路全体をユニタリ行列として記述することが可能である。しかし 2.3 節で説明したように中間測定を含む量子回路は不可逆的なものであり、ユニタリ行列として表現することはできない。

ここで任意の行列  $A \in \mathbb{C}^{m \times n}$  について、 $\text{vec}(A) \in \mathbb{C}^{mn}$  かつすべての  $i \in \mathbb{N}_{\leq m}, j \in \mathbb{N}_{\leq n}$  に対し  $\text{vec}(A)[i + (j - 1)m] = A[i, j]$  となる  $\text{vec}(\cdot)$  を考える。中間測定を含む量子回路  $\Phi$

に対して、密度行列で表現された任意の量子状態  $\rho \in \mathbb{C}^{m \times m}$  を入力したときの出力状態を  $\Phi(\rho) \in \mathbb{C}^{n \times n}$  とすると、 $\text{vec}(\Phi(\rho)) = K(\Phi)\text{vec}(\rho)$  となるの行列  $K(\Phi) \in \mathbb{C}^{n^2 \times m^2}$  が存在することが知られている。また、量子回路  $\Phi$  が中間測定とユニタリ発展のみから構成される時  $K(\Phi)$  は contraction であることが知られている。このような性質から、中間測定を含む量子回路を contraction 行列として表現し、ユニタリ行列へ埋め込むことで、中間測定を含まない量子回路で模倣することができることを示した。



## 第4章 本研究の成果

本研究ではDoron ら [6] が示した  $1/n$  ギャップ第二固有値問題と定数ギャップ第二固有値問題の、確率対数領域計算における関係性を示すことが目標である．これに対し、定数ギャップ第二固有値問題より  $1/n$  ギャップ第二固有値問題の方が難しいことは自明なので、行列の冪乗を計算することで確率行列のスペクトルギャップを増幅し、 $1/n$  ギャップ第二固有値問題を定数ギャップ第二固有値問題に帰着することを考えた．成果として、条件付きではあるが  $1/n$  ギャップ第二固有値問題を定数ギャップ第二固有値問題に帰着できることを示した．これにより確率的対数領域計算において、定数ギャップ第二固有値問題が一部の  $1/n$  ギャップ第二固有値問題より困難であることを示した．

### 4.1 提案手法

まずは行列冪によってスペクトルギャップが増幅されることを説明する．定義 3.1.1 の  $1/n$  ギャップ第二固有値問題  $2ndEV_{\frac{1}{n}, \frac{2}{n}}$  のインスタンスとして、確率行列  $A$  と  $\frac{1}{n}, \frac{2}{n}$  が与えられるとする．このときインスタンスは以下のどちらかである．

**Yes インスタンス** :  $\lambda_2 \leq 1 - \frac{2}{n}$

**No インスタンス** :  $\lambda_2 \geq 1 - \frac{1}{n}$

次に確率行列を  $T$  乗することを考える．このとき  $\lambda_2^T$  は以下になる．

**Yes インスタンス** :  $\lambda_2^T \leq \sum_{i=0}^T \binom{T}{i} (-2/n)^i$

**No インスタンス** :  $\lambda_2^T \geq \sum_{i=0}^T \binom{T}{i} (-1/n)^i$

より簡単に書くと

**Yes インスタンス** :  $\lambda_2^T \leq 1 - \frac{2T}{n} + \mathcal{O}(\frac{1}{n^2})$

**No インスタンス** :  $\lambda_2^T \geq 1 - \frac{T}{n} + \mathcal{O}(\frac{1}{n^2})$

となり、Yes/No インスタンスのギャップが増幅されていることが分かる．ここから、 $\frac{1}{n}$  ギャップの第二固有値問題として与えられる確率行列を  $\mathcal{O}(n)$  乗することが出来れば定数ギャップの第二固有値に帰着することが可能である．

### 4.2 確率的対数領域計算における行列冪の近似

文献 [5][16] など、領域効率の良い行列冪乗アルゴリズムに関する研究は存在するが、確率行列の冪乗を決定的に対数領域で計算する方法は知られていない．そこで本研究では、確率的対数領域計算で確率行列の冪乗を近似することを考える．このとき補題 3.1.3 より以下の補題が成り立つ．

**補題 4.2.1.** (確率行列の近似) 確率行列  $A \in \mathbb{R}_{\geq 0}^{n \times n}$  と  $s, t \in \mathbb{N}_{\leq n}$  が与えられたとき, 以下を満たす  $B'$  を出力する領域  $\mathcal{O}(\log \log \delta^{-1} + \log \epsilon^{-1} + \log n)$  の乱択アルゴリズムが存在する.

$$\Pr \left[ \left| B' - A^k[s, t] \right| \geq \epsilon \right] \leq \delta \quad (4.1)$$

ここから, 確率的対数領域計算において確率行列  $A$  の  $n$  多項式乗を  $n$  逆多項式の精度で近似することが可能であることが分かる.

しかし補題 4.2.1 では, 近似した冪乗行列の各要素についてのみしか誤差を保証しておらず, 冪乗行列の各固有値の誤差についてはわからない. そこで, 行列の各要素と固有値の誤差の関係について解析する.

文献 [19] の First-order perturbation 定理より, 以下の補題が成立する.

**補題 4.2.2.** (First-order perturbation 定理による確率的対数領域計算における行列冪の固有値誤差) 固有値がすべて重複度 1 の確率行列  $A \in \mathbb{R}_{\geq 0}^{n \times n}$  が与えられる. このときすべての  $s, t, i \in \mathbb{N}_{\leq n}$  について, 以下を満たす行列  $B'$  の各要素を出力する確率的対数領域アルゴリズムが存在する. ただし  $c_1, c_2$  は任意の定数とし,  $\lambda'_i(\lambda_i)$  は  $B'(A^{n^{c_1}})$  とする.

$$\left| B'[s, t] - A^{n^{c_1}}[s, t] \right| \leq \frac{1}{n^{c_2}} \quad (4.2)$$

$$\left| \lambda'_i - \lambda_i \right| \leq \frac{1}{n^{c_2-1}} \quad (4.3)$$

**証明.** 補題 4.2.1 より, 式 4.2 は直ちに証明される.

$B = A^k$  とする. このとき  $A$  の固有値がすべて重複度 1 より,  $B$  の固有値もすべて重複度が 1 となる.  $B$  のある固有値を  $\lambda$  とし,  $v, w^*$  をそれぞれ  $\lambda$  の左, 右固有ベクトルとする. また  $\delta B = B' - B$ ,  $\lambda + \delta\lambda$  が  $B'$  の固有値となるような  $\delta\lambda$ ,  $\delta v$  が  $\lambda + \delta\lambda$  の固有ベクトルとなる  $\delta v$  を考える.

このとき以下の式が成立する. ただし式 (4.12) までの式変形は文献 [19] を引用している.

$$(B + \delta B)(v + \delta v) = (\lambda + \delta\lambda)(v + \delta v) \quad (4.4)$$

$$(\delta B)v + B(\delta v) = (\delta v)\lambda + v(\delta\lambda) \quad (4.5)$$

これに対し右から  $w^*$  を掛け,  $w^*B = \lambda w^*$  を用いて

$$w^*(\delta B)v + w^*B(\delta v) = w^*(\delta v)\lambda + w^*v(\delta\lambda) \quad (4.6)$$

$$w^*(\delta B)v + w^*\lambda(\delta v) = w^*(\delta v)\lambda + w^*v(\delta\lambda) \quad (4.7)$$

$$w^*(\delta B)v = w^*v(\delta\lambda) \quad (4.8)$$

となる. ここで  $\lambda$  は重複度 1 なので  $w^*v \neq 0$  が成り立つ. よって

$$\delta\lambda = \frac{w^*(\delta B)v}{w^*v} \quad (4.9)$$

ここで  $\delta\lambda$  に注目すると

$$|\delta\lambda| = \frac{|w^*(\delta B)v|}{|w^*v|} \quad (4.10)$$

$$\leq \frac{\|w\|_2 \|\delta B\|_2 \|v\|_2}{w^*v} \quad (4.11)$$

$$= \frac{\|\delta B\|_2}{\cos \theta} \quad (4.12)$$

ここで  $\|\cdot\|_2$  はスペクトルノルム,  $\theta$  は  $v$  と  $w$  の成す角度である. ここで  $B$  の固有値がすべて重複度 1 であることから  $B$  は対角化可能であり, 対角化可能から  $\cos \theta = 1$  であることが分かる. よって

$$|\delta\lambda| \leq \|\delta B\|_2 \leq \|\delta B\|_F \quad (4.13)$$

となる. ただし  $\|\cdot\|_F$  はフロベニウスノルムである.  
よってフロベニウスノルムの定義から

$$\|\delta B\|_F = \sqrt{\sum_{s,t=0}^n B[s,t]^2} \leq \sqrt{\frac{n^2}{n^{2c_2}}} = \frac{1}{n^{c_2-1}} \quad (4.14)$$

よって

$$|\delta\lambda| \leq \frac{1}{n^{c_2-1}} \quad (4.15)$$

であり,  $B$  のすべての固有値について成り立つので式 (4.3) は示された.  $\blacksquare$

また, Bauer-Fike の定理 [4] より以下が成り立つ.

**補題 4.2.3.** (Bauer-Fike の定理による確率的対数領域計算における行列冪の固有値誤差)  $X^{-1}AX = \text{diag}(\lambda_1, \dots, \lambda_n)$  と対角化可能な確率行列  $A \in \mathbb{R}_{\geq 0}^{n \times n}$  が与えられる. このとき  $\kappa_p(X) \leq \text{poly}(n)$  であるならばすべての  $s, t, i \in \mathbb{N}_{\leq n}$  について以下を満たす行列  $B'$  の各要素を出力する確率的対数領域アルゴリズムが存在する. ただし,  $c_1$  は任意の定数,  $\lambda'_i$  を  $B'$  の第  $i$  固有値とする.

$$|B'[s,t] - A^{n^{c_1}}[s,t]| \leq \text{poly}(n^{-1}) \quad (4.16)$$

$$\min_{j \in \mathbb{N}_{\leq n}} |\lambda_j^{n^{c_1}} - \lambda'_i| \leq \text{poly}(n^{-1}) \quad (4.17)$$

**証明.** 補題 4.2.1 より, 式 4.2 は直ちに証明される.

Bauer-Fike の定理とは,  $X^{-1}AX = \text{diag}(\lambda_1, \dots, \lambda_n)$  に対して, 摂動行列  $A + E$  の固有値  $\mu$  は以下で上界が決まるというものである.

$$\min_{j \in \mathbb{N}_{\leq n}} |\lambda_j - \mu| \leq \kappa_p(X) \|E\|_p \quad (4.18)$$

ここで  $\|\cdot\|_p$  は行列の  $p$  ノルムを  $\kappa_p(\cdot)$  は  $p$  ノルムによる条件数を指す. これを補題 4.2.3 に当てはめると,

$$\min_{j \in \mathbb{N}_{\leq n}} |\lambda_j^{n^{c_1}} - \lambda'_i| \leq \kappa_p(X) \|B' - A^{n^{c_1}}\|_p \quad (4.19)$$

行列  $A$  の条件より  $\kappa_p(X) \leq \text{poly}(n^{-1})$  である. また  $o$  を要素がすべて 1 の  $n$  次元ベクトルとし,  $\delta B = B' - A^{n^{c_1}}$  とすると

$$\|\delta B\|_p = \max_{\|x\|_p=1} \|\delta Bx\|_p \quad (4.20)$$

$$\leq \|\delta B o\|_p \quad (4.21)$$

$$= \sqrt[p]{\sum_{i=1}^n \left| \sum_{j=1}^n A[i,j] \right|^p} \quad (4.22)$$

$$\leq \text{poly}(n^{-1}) \quad (4.23)$$

よって補題 4.2.3 は示された.  $\blacksquare$

### 4.3 定数ギャップ問題への帰着

定義 3.1.1 を拡張した以下の問題を考える.

**定義 4.3.1.** (Apx-2ndEV<sub>c,2c</sub>) 入力として確率行列  $B''$  と定数  $c \in \mathbb{R}$  が与えられる. ただし  $0 < c < 1/2$  とする. また問題の制約として  $B''$  の第  $i$  固有値を  $\lambda_i''$  とすると,  $|\lambda_n''| \leq \dots \leq |\lambda_3''| \leq 1 - 2c + \text{poly}(n^{-1})$  であり,  $|\text{Im}\{\lambda_2''\}| \leq \text{poly}(n^{-1})$  である. このとき Yes/No 各インスタンスは以下で定められる.

**Yes インスタンス :**  $|\lambda_2''| \leq 1 - 2c + \text{poly}(n^{-1})$

**No インスタンス :**  $|\lambda_2''| \leq 1 - c + \text{poly}(n^{-1})$

このとき, 以下の定理が言える.

**定理 4.3.2.** (制限付き 2ndEV <sub>$\frac{1}{n}, \frac{2}{n}$</sub>  の Apx-2ndEV<sub>c,2c</sub> への帰着)

インスタンスとして受け取る確率行列が, すべての固有値が重複度 1, もしくは対角化行列の条件数が次数の多項式で抑えられるような 2ndEV <sub>$\frac{1}{n}, \frac{2}{n}$</sub>  のインスタンスは確率的対数領域計算において Apx-2ndEV<sub>c,2c</sub> のインスタンスへ帰着可能である.

**証明.** 行列冪近似と正規化の 2 つの構成からなる確率対数領域帰着アルゴリズムを考える. まず行列冪近似を考える. インスタンスとして受け取る確率行列が, すべての固有値が重複度 1, もしくは対角化行列の条件数が次数の多項式で抑えられるような 2ndEV <sub>$\frac{1}{n}, \frac{2}{n}$</sub>  のインスタンスとして, 確率行列  $A \in \mathbb{R}_{\geq 0}^{n \times n}$  を受け取る. 補題 4.2.2 もしくは補題 4.2.3 より, 以下を満たす  $B'$  を対数領域計算において計算可能である. ただし  $B = A^{c_1}$  とし,  $B(B')$  の第  $i$  固有値を  $\lambda_i(\lambda_i')$ ,  $c_1$  を任意の定数とする.

$$|B'[s, t] - B[s, t]| \leq \frac{1}{n^{c_1}} \quad (4.24)$$

$$|\lambda_i' - \lambda_i| \leq \text{poly}(n^{-1}) \quad (4.25)$$

このとき補題 4.2.1 より, 確率的対数領域計算において  $\mathcal{O}(n^n)$  回程度  $B'[s, t]$  を独立に計算しても,  $c_1 \log n$  ビットまでは  $B[s, t]$  と等しいことが保証される.

しかしこのままでは  $B'$  は確率行列ではないので, 以下のように確率行列に正規化することを考える.

$$B''[s, t] = B'[s, t] + \frac{1}{n} \left(1 - \sum_{s=1}^n B'[s, t]\right) \quad (4.26)$$

このとき, 各  $B'[s, t]$  を  $c_1 \log n$  ビットまでで切り捨てて計算するようにすると,  $B''[s, t]$  は  $\mathcal{O}(\log n)$  で計算可能であり, 以下が成り立つ.

$$|B''[s, t] - B[s, t]| \leq \text{poly}(n^{-1}) \quad (4.27)$$

また  $B$  は  $A$  の性質より, すべての固有値が重複度 1, もしくは対角化行列の条件数が次数の多項式で抑えられるため, 補題 4.2.2 もしくは補題 4.2.3 より,

$$|\lambda_i'' - \lambda_i| \leq \text{poly}(n^{-1}) \quad (4.28)$$

となるので,  $B''$  は Apx-2ndEV<sub>c,2c</sub> の条件を満たす. よって定理 4.3.2 は示された. ■

## 第5章 結論

### 5.1 本研究の成果とまとめ

本研究では Doron らが示した第二固有値問題について、行列冪の近似を行うことで限定的ではあるが、確率的対数領域計算において  $\frac{1}{n}$  ギャップを定数ギャップに増幅できることを示した。これにより確率的対数領域計算において、定数ギャップ第二固有値問題が一部の  $\frac{1}{n}$  ギャップ第二固有値問題より困難であることを示した。

### 5.2 今後の課題

本研究の課題として、今回定義した  $\text{Apx-2ndEV}_{c,2c}$  が BPL に含まれているのかを示すことが出来なかったことが挙げられる。Doron らの研究では第二固有値が実数であるという問題設定を用いて BPL に含まれることを示したが、今回の手法では帰着後の確率行列の第二固有値は実数とは限らないため、Doron らの証明における式 (3.2) を用いることが出来なかったためである。しかしながら実数に限りなく近いことは示されているため、 $\text{Apx-2ndEV}_{c,2c}$  が BPL に含まれるのではないかと予想している。この問題について今後明らかにしていきたい。

また本研究における課題として、 $\text{Apx-2ndEV}_{c,2c}$  に帰着可能な  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  のインスタンスが、すべての固有値が重複度 1、もしくは対角化行列の条件数が次数の多項式で抑えられるというものに限られてしまうという強い制限にある。これらの条件は行列冪の近似において、固有値がどれだけ真の値からずれるかを評価する際に必要なものとなっている。よって今後はより一般的な制限の下で固有値のずれを評価する手法を考慮したい。

上記の課題に対する別のアプローチとして、 $2\text{ndEV}_{c,2c}$  が BPL-困難であることを直接示すことも現在考えている。Doron らは確率的チューリングマシンの遷移グラフを  $G''$  にグラフを変換することで  $2\text{ndEV}_{\frac{1}{n}, \frac{2}{n}}$  の問題へ帰着を行っていた。このグラフの変換を工夫することで  $2\text{ndEV}_{c,2c}$  問題へ帰着できないか考えている。現在研究中のアイデアとして、 $G'$  から  $G''$  への変換の際に、Doron らは  $G'$  を 2 つ用いて  $G''$  を構成していたが、複数の  $G'$  から  $G''$  を構成することで  $2\text{ndEV}_{c,2c}$  の問題へ帰着できないかというものがある。具体的な  $G''$  への変換は以下の通りである。ただし  $g \in \mathbb{N}$  としたとき、 $G''$  は  $g$  個の  $G'$  から構成され、 $V'' = \{(v', k) | v' \in V', k \in \mathbb{N}_{\leq g}\}$  とする。

- 全ての  $(a, b) \in E'$  と  $k \in \mathbb{N}_{\leq g}$  について、 $((a, k), (b, k)) \in E''$
- $r \neq t$  である全ての  $r \in V$  と  $k \in \mathbb{N}_{\leq g}$  について、 $((r, T+1), k), ((s, 1), k)) \in E''$
- 全ての  $k \in \mathbb{N}_{\leq g-1}$  について、 $((t, T+1), k), ((s, 1), k+1)) \in E''$  かつ  $((t, T+1), g), ((s, 1), 1)) \in E''$

このとき Doron らと同様に, すべての  $k \in \mathbb{N}_{\leq g}$  とすべての  $j \in V$ ,  $l \leq 0$  に対して式 (3.9) は

$$v[(j, 1), k] = 0 \tag{5.1}$$

と拡張される. 式 (3.10) に関しても同様に,  $v[(s, 1), k] = x_k$  とすると

$$v[(j, l), k] = \frac{x_k}{\lambda^{l-1}} W^{l-1}[j, s] \tag{5.2}$$

となる. ここまでの解析は終わっているが, ここから  $\lambda$  を導出する部分に関しては現在研究中である.

## 謝辞

本研究を進めるにあたり，日頃からご指導して下さいました河内亮周教授，共同研究者として研究に関する助言を下さいました Maharshi Ray 特任助教，研究活動で多くのご支援をしてくださった森岡幸音事務員，研究室の学生の皆様に深く感謝申し上げます．

名古屋大学大学院 多元数理科学研究科の François Le Gall 先生は共同研究者として日頃から研究に関する助言を下さいました．深く感謝申し上げます．

## 参考文献

- [1] Enric Boix-Adserà, Lior Eldar, Saeed Mehraban. Approximating the Determinant of Well-Conditioned Matrices by Shallow Circuits. CoRR, abs/1912.03824, 2019.
- [2] Sanjeev Arora, Boaz Barak. Computational Complexity: A Modern Approach, Cambridge University Press, 2009.
- [3] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor, Nature, 574(7779):505–510, 2019.
- [4] F.L. Bauer, C.T. Fike, Norms and exclusion theorems. Numer. Math. 2, p.137–141, 1960.
- [5] Gil Cohen, Dean Doron, Ori Sberlo. Approximating Large Powers of Stochastic Matrices in Small Space. Electronic Colloquium on Computational Complexity (ECCC), TR22-008, 2022.
- [6] Dean Doron, Amir Sarid, Amnon Ta-Shma. On approximating the eigenvalues of stochastic matrices in probabilistic logspace.computational complexity 26, p.393–420, 2017.
- [7] Bill Fefferman, Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. In 9th Innovations in Theoretical Computer Science Conference (ITCS 2018). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.
- [8] Bill Fefferman, Zachary Remscrem. Eliminating Intermediate Measurements in Space-Bounded Quantum Computation. In Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2021). p.1343 – 1356, 2021.
- [9] Sevag Gharibian, François Le Gall. Dequantizing the Quantum Singular Value Transformation: Hardness and Applications to Quantum Chemistry and the Quantum PCP Conjecture. Proceedings of the 54th ACM Symposium on Theory of Computing (STOC 2022), pp. 19-32, 2022.
- [10] András Gilyén, Yuan Su, Guang Hao Low, Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC 2019), p.193–204, 2019.



- [11] Uma Girish, Ran Raz, Wei Zhan. Quantum Logspace Algorithm for Powering Matrices with Bounded Norm. 48th International Colloquium on Automata, Languages, and Programming (ICALP 2021). pp. 73:1–73:20, 2021.
- [12] Uma Girish, Ran Raz. Eliminating Intermediate Measurements Using Pseudorandom Generators. In Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022), pp.76:1 - 76:18, 2022.
- [13] Chris Marriott, John Watrous. Quantum arthur–merlin games. Computational Complexity, 14(2):122–152, 2005.
- [14] Michael A. Nielsen, Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2010.
- [15] Amnon Ta-Shma. Inverting well conditioned matrices in quantum logspace. In Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC 2013), p.881 - 890, 2013.
- [16] Michael E. Saks, Shiyu Zhou.  $\text{BP}_H\text{SPACE}(S) \subseteq \text{DSPACE}(S^{2/3})$ , Journal of Computer and System Sciences, 58(2):376–403, 1999.
- [17] John Watrous. Space-bounded quantum complexity. Journal of Computer and System Sciences, 59(2):281–326, 1999.
- [18] 石坂智, 小川朋宏, 河内亮周, 木村元, 林正人. 量子計算科学入門. 共立出版株式会社, 2013.
- [19] Cornell 大学 Matrix Computations 2009 年 10 月 23 日分レクチャーノート, <https://www.cs.cornell.edu/bindel/class/cs6210-f09/lec24.pdf> (最終閲覧日 : 2023 年 1 月 29 日)