2023 年度 芝浦工業大学 工学部 情報工学科

卒　　業　　論　　文

虚時間発展法を用いた励起状態探索の
最短ベクトル問題への応用

学籍番号　　**AL20013**

氏　　名　　水野　航太

指導教員　　渡部　昌平

目 次

第1章　序論

1.1　背景

量子コンピュータは，量子重ね合わせや量子もつれといった量子力学特有の現象を用いて動作するコンピュータである．基本単位である量子ビットは，古典的ビットとは異なり，0と1の両方の値を重ね合わせという形で表現することができる．この量子ビットを用いて並列計算を行うことで，特定の問題を高速に解くことができると期待されている [1].

量子コンピュータの応用分野の１つとして有力視されているのが暗号分野である．量子技術の発展に伴い，現在一般的に用いられている暗号技術が将来的に破られてしまう恐れがあるため，量子コンピュータによる攻撃に耐性のある耐量子計算機暗号 (PQC) の研究開発・規格標準化が進んでいる [2]．複数ある暗号の中で有力視されているのが格子暗号であり，数学的背景である格子問題が効率的に解けていないことを安全性の根拠としている．

暗号技術の進展において，安全性の確保は重要な要素である．安全な暗号を実現するためには，その暗号が解読されないことが必要不可欠であり，その検証は解読アルゴリズムの研究によって行われる．さまざまな攻撃手法に対して継続的な解読アルゴリズムの研究が必要であり，これによって新たな脅威に対処し，信頼性を維持することが可能となる．特に格子暗号に対する解読アルゴリズムの研究は，その耐量子計算機暗号としての安全性を保証するために重要である．

1.2 関連研究

Ura らは，格子問題の 1 つである最短ベクトル問題に対して，量子アニーリングを用いた解の探索手法を提案した [3]．しかし，ドライバハミルトニアンの第一励起状態を初期状態として用意する必要があり，実装において課題が残る．また，エネルギーギャップ小さい場合，断熱条件を満たすために，系のサイズに対して指数関数的に長いアニーリング時間がかかってしまう場合がある．

1.3 目的

暗号技術の開発・発展は現代社会において不可欠な要素であり，その安全性を確保するためには様々な解読アルゴリズムに対する検証が必要である．そこで本研究では，最短ベクトル問題に焦点を当て，虚時間発展法を用いた解の探索手法を提案し，その性能評価を行う．そこで，実際に提案手法の有用性を確認した上で，計算時間や精度の問題サイズ依存性・基底ベクトルの角度依存性を検証する．

1.4 構成

本論文の構成は以下の通りである．第 2 章では，量子コンピュータとその基礎である量子ビット・量子アルゴリズムについて述べる．第 3 章では，本研究で扱う最短ベクトル問題について述べる．第 4 章では，提案手法とその評価方法について述べ，第 5 章で数値実験の結果と考察を述べる．第 6 章では，本研究のまとめと今後の課題について述べる．

第2章　量子コンピュータ

2.1　量子コンピュータとは

量子コンピュータとは，波と粒子の 2 面性を持つ「量子」の性質を用いて情報処理を行うコンピュータである．粒子の性質に由来する量子もつれと，波の性質に由来する干渉という現象を巧妙に用いて情報処理を削減することを基本指針としている [4].

量子コンピュータは，方式によって量子ゲート方式と量子アニーリング方式の 2 つに分類される．量子ゲート方式は，量子ビットに対してゲート操作を行う量子回路を構成し計算を行う方式である．古典コンピュータが AND や OR などの論理ゲートを用いて計算を行うのと同様に，量子ゲート方式ではアダマールゲート (H) や制御ノットゲート (CNOT) という基本ゲートの組み合わせで演算を行う．多くの量子アルゴリズムは量子ゲート方式によって実現されるが，現状では比較的小規模な問題にしか対応ができない．量子ビットの表現において，超電導やイオントラップなど様々な実現手法が提案されている．量子アニーリング方式は，1998 年に西森・門脇によって発表された [5]，組み合わせ最適化問題を量子効果を用いて解くことに特化した量子コンピュータである．焼きなまし法と呼ばれる組合せ最適化問題に対する汎用的近似解法から着想を得ており，熱揺らぎの代わりに量子揺らぎを用いて，よりエネルギーの低い解を探索する．アニーリングのスケジュールを調整することにより，長時間極限において，確率 1 でハミルトニアンの基底状態に到達できることがわかっている [6].

2.2 量子ビット

従来の古典コンピュータは情報の最小単位としてビットを用いるのに対し，量子コンピュータはその単位として量子ビット (quantum bit，qubit) を用いる．古典ビットは 0 か 1 のどちらかの状態しか取らないのに対し，量子ビットは，0 と 1 という状態に加えて，その重ね合わせという状態を表現することができる．

量子ビット系の状態は，$\mathbb{C}^2$ の単位ベクトルで記述される．特に，古典ビットの 0 と 1 に対応する状態は，それぞれ $\mathbb{C}^2$ の単位ベクトル

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

となる [7]．これらは正規直交基底 $\{|0\rangle, |1\rangle\}$ を形成し，計算基底と呼ばれる．

一般の量子状態は，$|0\rangle$ と $|1\rangle$ を用いて以下の式で与えられる．

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \alpha, \beta \in \mathbb{C} \tag{2.2}$$

ここで，α, β は確率振幅と呼ばれ，規格化条件 $|\alpha|^2 + |\beta|^2 = 1$ を満たす．α, β はそれぞれ，状態 $|\psi\rangle$ における 0 と 1 の重みを表している．この量子状態に対し測定を行うと，測定の結果に対応する状態に変化する．具体的には，測定結果が 0 の場合は $|0\rangle$ に，1 の場合は $|1\rangle$ に変化する．確率規則より，$|0\rangle, |1\rangle$ を得る確率をそれぞれ p_0, p_1 とすると，

$$p_0 = |\langle 0|\psi\rangle|^2 = |\langle 0| (\alpha |0\rangle + \beta |1\rangle)|^2 = |\alpha|^2 \tag{2.3}$$

$$p_1 = |\langle 1|\psi\rangle|^2 = |\langle 1| (\alpha |0\rangle + \beta |1\rangle)|^2 = |\beta|^2 \tag{2.4}$$

となる．規格化条件は，全確率が 1 であることを表している．

また，量子状態は 2 つの変数 $\theta, \phi \in \mathbb{R}$ を用いて，

$$|\psi\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle \tag{2.5}$$

と表すこともできる（グローバル位相は省略）．これは，量子状態を単位球面上の点としてプロットしたものである．

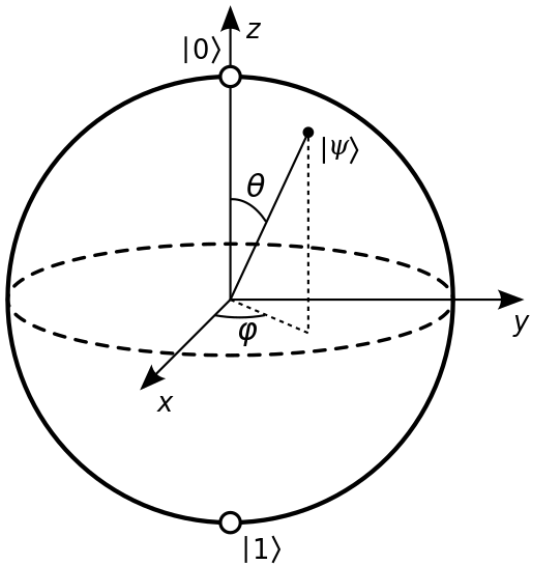

図 2.1: 量子状態のブロッホ球による表現

次に，量子ビットが複数存在する場合の振る舞いについて述べる．例として 2 量子ビットの場合を考える．2 つの量子状態を以下のように用意する．

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \tag{2.6}$$

対応する 2 量子ビットの状態は，これらのテンソル積によって記述される．これは以下のように定義される．

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \\ \\ \beta \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} \tag{2.7}$$

$|\psi\rangle, |\phi\rangle$ がそれぞれ 2 次元の時，それらのテンソル積 $|\psi\rangle \otimes |\phi\rangle$ は 4 次元となる．

一般に n 個の量子ビットからなる量子状態については，2^n 個の状態がどのよう

な重みで重なり合っているか，という複素確率振幅によって記述される．

$$|\psi\rangle = c_{0\cdots00}\,|0\cdots00\rangle + \cdots + c_{1\cdots11}\,|1\cdots11\rangle = \begin{pmatrix} c_{0\cdots00} \\ \vdots \\ c_{1\cdots11} \end{pmatrix} \tag{2.8}$$

ここで $|0\cdots00\rangle, \cdots, |1\cdots11\rangle$ は基底であり，状態はそれらの基底の線形結合で表現される．各基底は 2^n 次元であるので，n 量子ビットの状態は 2^n 次元の複素ベクトルで記述される．ここで，確率振幅は $\sum_{i_1,\cdots,i_n} |c_{i_1,\cdots,i_n}|^2 = 1$ と規格化されている．この状態 $|\psi\rangle$ を測定すると，確率 $p_{i_1,\cdots,i_n} = |c_{i_1,\cdots,i_n}|^2$ で状態 $i_1, \cdots, i_n$ が得られる．また，2 量子ビットの場合と同様に，n 量子ビットの状態は $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ のようなテンソル積でも記述され，その次元は 2^n となる．

2.3 量子アルゴリズム

量子コンピュータは，重ね合わせの性質を用いて高速な並列計算が可能である．しかし，計算結果を取得するために測定を行うと，計算結果のうちどれか 1 つの状態がランダムで得られるのみとなり，これが正解である保証はない．そのため，所望の解が高確率で得られるように設計された，量子コンピュータ専用のアルゴリズムが必要であり，これを量子アルゴリズムという．例として，Shor の素因数分解アルゴリズム [8]，Grover の探索アルゴリズム [9] 等がある．

その中で，本研究で用いた量子アルゴリズムである「虚時間発展法」と「Folded-Spectrum Method」を紹介する．

2.3.1 虚時間発展法

虚時間発展法は，実時間 t の代わりに虚時間 $\tau = it$ で系を時間発展させることで，状態をハミルトニアンの基底状態に収束させるというアルゴリズムである．

量子状態の時間発展は，以下のシュレディンガー方程式に従う．

$$i\frac{\partial}{\partial t}\left|\psi(t)\right\rangle = \hat{H}\left|\psi(t)\right\rangle \tag{2.9}$$

これを解くと，

$$\left|\psi(t)\right\rangle = e^{-i\hat{H}t}\left|\psi(0)\right\rangle . \tag{2.10}$$

$\tau = it$ とすると，

$$\left|\psi(\tau)\right\rangle = e^{-\hat{H}\tau}\left|\psi(0)\right\rangle . \tag{2.11}$$

ここで，時間に依存しないシュレディンガー方程式の解

$$\hat{H}\left|E_i\right\rangle = E_i\left|E_i\right\rangle \quad (i = 0, 1, \cdots \infty) \tag{2.12}$$

を用いて，初期状態を展開する．ここで，$i < j$ のとき, $E_i < E_j$ である．この状態を虚時間発展させると，

$$e^{-\hat{H}\tau}\left|\psi(0)\right\rangle = \sum_{i=0}^{\infty} e^{-\hat{H}\tau}E_i\left|E_i\right\rangle \tag{2.13}$$

$$= E_0 e^{-E_0\tau}\left|E_0\right\rangle + \sum_{i=1}^{\infty} e^{-E_i\tau}E_i\left|E_i\right\rangle . \tag{2.14}$$

よって

$$e^{(E_0-\hat{H})\tau}\left|\psi(0)\right\rangle = E_0\left|E_0\right\rangle + \sum_{i=1}^{\infty} e^{(E_0-E_i)\tau}E_i\left|E_i\right\rangle . \tag{2.15}$$

$i \geq 1$ において，$E_0 - E_i < 0$ であるので，

$$(\text{右辺第 2 項}) = \sum_{i=1}^{\infty} e^{(E_0-E_i)\tau}E_i\left|E_i\right\rangle \to 0 \quad (\tau \to \infty). \tag{2.16}$$

したがって，

$$\left|\psi(\infty)\right\rangle A(\infty) = \left|E_0\right\rangle . \tag{2.17}$$

これは，任意の状態を十分に長い時間虚時間発展させると，ハミルトニアンの基底状態に収束することを表す．ここで，虚時間発展演算子 $e^{-\hat{H}\tau}$ はユニタリ演算子ではないので，規格化定数 $A(\tau)$ を用いて量子状態を規格化している．励起状態となる確率は指数関数的に小さくなるので，効率的に基底状態に収束することが特徴である．虚時間発展におけるエネルギーの遷移を図 2.2 に示す．

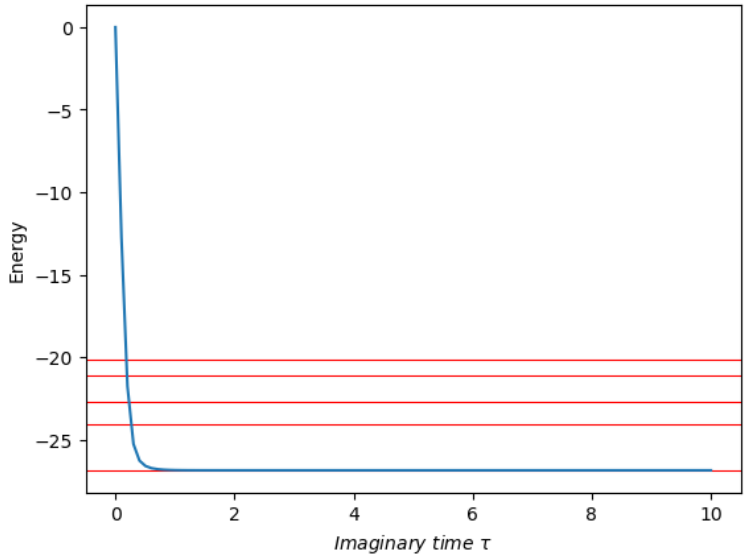

図 2.2: 虚時間発展のエネルギー遷移

図の横軸は虚時間 τ，縦軸はエネルギーの値を示している．赤線は下から基底エネルギーと第 1~4 励起エネルギーを表す直線である．τ を十分長い時間 (今回は T=10) 虚時間発展させると，適当な状態がハミルトニアンの基底状態に高速に収束していることがわかる．

2.3.2 Folded-Spectrum Method

単純な虚時間発展法では，基底状態の探索しかできない．励起状態の探索手法として，量子化学計算や VQE の領域で研究されている Folded-Spectrum Method(FS

法) がある [10, 11]．これは，パラメータ ω を用いて，ハミルトニアンを,

$$\hat{H}' = (\hat{H} - \omega I)^{2m} \tag{2.18}$$

のように変換する手法である．FS 演算子 $\hat{H}$ と元のハミルトニアン $\hat{H}$ は同じ固有状態を共有するが，固有値の並び替えが起こる．これは，エネルギー値 ω まわりの折り返しに対応する．変換を行った H' では，基底状態は元のハミルトニアン $\hat{H}$ の固有値のうち ω に最も近いものに対応する [12]．これにより，適当な初期状態に対して H' を用いて虚時間発展を行えば，$\hat{H}$ の基底状態，すなわち ω 近傍のエネルギー固有値に対応する状態に収束する (図 2.3)．

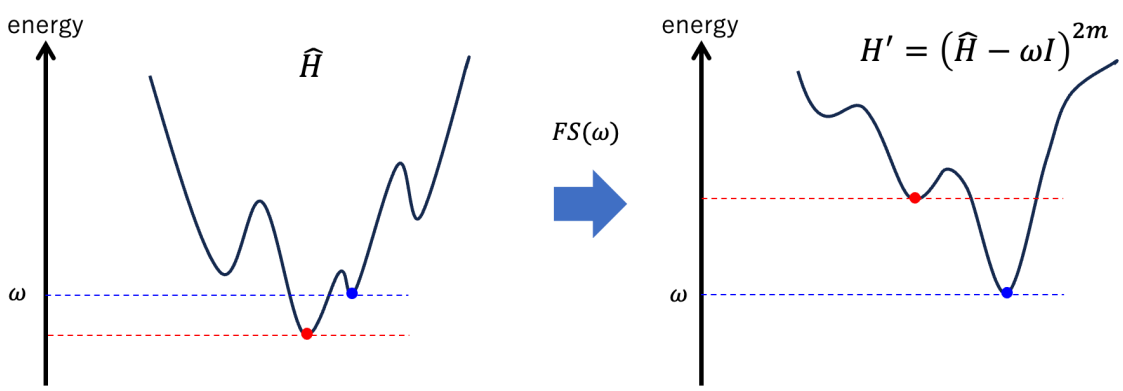

図 2.3: FS 法のイメージ

左は $\hat{H}$，右は $\hat{H}' = (\hat{H} - \omega I)^{2m}$ の固有エネルギー分布を表している．左の分布において，エネルギー値が ω となる励起状態を考える．この値を用いてハミルトニアンを $\hat{H}' = (\hat{H} - \omega I)^{2m}$ とすると，エネルギーが ω 以外をとる時に値が大きくなるようにエネルギー分布が変化する．すなわち，変換後の $\hat{H}'$ では，エネルギー ω が基底エネルギーとなる．このように変換した $\hat{H}'$ を用いて量子状態を虚時間発展させることで，もとのハミルトニアン $\hat{H}$ の ω に対応する励起状態に収束する．

第3章　最短ベクトル問題

3.1　格子

ベクトル空間 $\mathbb{R}^m$ の n 個のベクトル $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ の整数係数の線型結合全体の集合を，

$$\mathcal{L}(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) := \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b_i} \in \mathbb{R}^m : x_i \in \mathbb{Z} \right\} \tag{3.1}$$

と表す．$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \mathbb{R}^m$ が一次独立な時，これらのベクトルの整数の線型結合全体の集合 $L = \mathcal{L}(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ を $\mathbb{R}^m$ の格子という．格子の元を格子点または格子ベクトルという．また，格子 L を生成する一次独立な n 個のベクトルの組 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ を格子基底といい，各 $\boldsymbol{b}_i$ を基底ベクトルという．本稿では，基底ベクトルの個数である整数 n を格子の次元という．

上記の定義において，各基底ベクトル $\boldsymbol{b}_i = (b_{i_1}, \cdots, b_{i_m})^T$ を横に並べた $n \times m$ 行列

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{b}_1 & \cdots & \boldsymbol{b}_n \end{pmatrix} = \begin{pmatrix} b_{1_1} & \cdots & b_{m_1} \\ \vdots & \ddots & \vdots \\ b_{1_n} & \cdots & b_{m_n} \end{pmatrix} \tag{3.2}$$

を格子 L の格子基底行列という．これを用いて，$\mathcal{L}(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) = \mathcal{L}(\boldsymbol{B})$ と表現する．

また，格子 L の格子基底行列 $\boldsymbol{B}$ を用いて表される行列

$$\boldsymbol{G} := \boldsymbol{B}^T \boldsymbol{B} = \begin{pmatrix} \langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle & \cdots & \langle \boldsymbol{b}_1, \boldsymbol{b}_n \rangle \\ \vdots & \ddots & \vdots \\ \langle \boldsymbol{b}_n, \boldsymbol{b}_1 \rangle & \cdots & \langle \boldsymbol{b}_n, \boldsymbol{b}_n \rangle \end{pmatrix} \tag{3.3}$$

をベクトル $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ のグラム行列という．$\langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle = \langle \boldsymbol{b}_j, \boldsymbol{b}_i \rangle$ より，$\boldsymbol{G}$ は対称行列である．

一般に，格子点ベクトル $\boldsymbol{v}$ は，それぞれの基底ベクトルに対応する整数係数のベクトル $\boldsymbol{x} = (x_1, \cdots, x_n)$ を用いて，

$$\boldsymbol{v} = \boldsymbol{x} \cdot \boldsymbol{B} = x_1\boldsymbol{b}_1 + \cdots + x_n\boldsymbol{b}_n \in \mathcal{L}(\boldsymbol{B}) \tag{3.4}$$

で与えられる．

3.2 最短ベクトル問題

格子暗号の安全性は，格子問題と呼ばれる，計算困難と考えられる数学問題に基づいている．本稿では，格子問題の 1 つである最短ベクトル問題 (Shortest Vector Problem，SVP) に焦点を当てる．

3.2.1 定義

最短ベクトル問題は，格子基底行列 $\boldsymbol{B} = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ が与えられた時，この $\boldsymbol{B}$ から成る格子点ベクトル $\boldsymbol{v}$ の中で，ノルムが最小となる非零ベクトルを求める問題である（図 3.1).

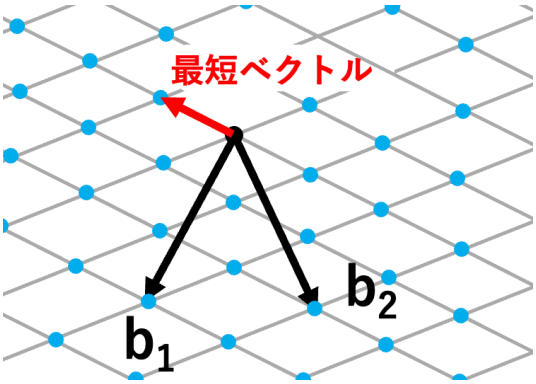

図 3.1: 2 次元格子空間における最短ベクトル問題

3.2.2 NP 困難性

最短ベクトル問題に付随する問題として，次のような問題が考えられている [13]. 以下，格子 L における各格子点ベクトルのノルムの集合を $\{\lambda_i\}$ とする．例えば，λ_1 が最短ベクトルのノルムを表し，λ_2 はその次に大きい格子ベクトルのノルムを表す.

- γ-近似最短ベクトル問題
  - $\gamma \geq 1$ とする．格子 L の格子基底行列 $\boldsymbol{B}$ が与えられた状況で，$\|\boldsymbol{v}\| \leq \gamma \cdot \lambda_1$ を満たす $\boldsymbol{v} \in L \backslash \{\boldsymbol{0}\}$ を計算する問題.
- γ-一意最短ベクトル問題
  - $\gamma \geq 1$ とする．$\lambda_2 > \gamma \cdot \lambda_1$ を満たす格子 L の基底 $\boldsymbol{B}$ が与えられた状況で，L の最短ベクトルを計算する問題.

これらと最短ベクトル問題の間には，最短ベクトル問題が解ければ $\gamma-$ 近似最短ベクトル問題が解け，γ-近似最短ベクトル問題が解ければ，γ-一意最短ベクトルが解けるという関係がある [13]．最短ベクトル問題と，ある程度小さな γ(例として$\gamma = \sqrt{2}$ など) に対する γ-近似最短ベクトル問題は NP 困難であることが知られている [14, 15]．現在，最短ベクトル問題を多項式時間で求めるアルゴリズムは知られていない.

3.2.3 古典的アプローチ

最短ベクトル問題に対する多くの効率的なアルゴリズムは，最短ベクトル問題を基底簡約問題に帰着させることで解を求めている．一般に，格子暗号などに用いられる格子の基底は，最短ベクトルを計算しにくいような「悪い」基底であることが多い [13]．このような「悪い」基底を,「良い」基底に変換する操作を基底

簡約という．ここで「良い」基底とは，基底のノルムができるだけ小さいものであったり，基底同士が直交かそれに近くなっているものを指す．

基底簡約アルゴリズムの代表的な例として，A.Lenstra，H.Lenstra，L.Lovász が開発したアルゴリズムである LLL アルゴリズムがある [16]．これは，与えられた格子において複数存在する基底の中で，ノルムの和が最小となる基底を近似的に求めるアルゴリズムであり，近似的な最短ベクトル問題であれば多項式時間で解けることが特徴である．格子の次元が低いときは，基底簡約によって最小基底の厳密解が求まることが多い．しかし，得られる解の近似率は，理論上次元に関する指数関数になることも知られている．

3.3 イジング形式への写像

3.3.1 目的関数

最短ベクトル問題を量子アルゴリズムを用いて解くために，イジング形式での定式化を行う必要がある．イジング形式とは，$\{-1, 1\}$ のいずれかの値をとるスピンから構成されるモデルである．最短ベクトル問題は，非零ベクトルのノルムを最小化することが目的であるため，目的変数はノルムである．格子点ベクトル $\boldsymbol{v}$ のノルムの二乗は，以下の式で与えられる．

$$\|\boldsymbol{v}\|^2 = \sum_{i,j=1}^{n} x_i x_j \langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle \tag{3.5}$$

$$= \sum_{i,j=1}^{n} x_i x_j G_{ij} \tag{3.6}$$

$G_{ij} = \langle \boldsymbol{b}_i, \boldsymbol{b}_j \rangle$ は格子基底ベクトルのグラム行列 $\boldsymbol{G}$ の要素である．ここで，各基底ベクトルの整数係数 x_i の範囲を $-k \leq x_i \leq k$ に限定すると，量子ビットは各基底ごとに $2k+1$ 個必要であるので，合計で $(2k+1)n$ 個必要である．この時，ノルム

に対応するハミルトニアンは，次のように書ける [17].

$$\hat{H}_p = J \sum_{i,j=1}^{n} G_{ij} \hat{Q}^{(i)} \hat{Q}^{(j)} \tag{3.7}$$

ここで，$\hat{Q}^{(i)}$ は $\hat{Q}^{(i)} = \frac{1}{2} \sum_{p=0}^{2k} (-k+p) \hat{\sigma}_z^{(p,i)}$ で定義される変数であり，$\hat{\sigma}_z$ はパウリ Z 演算子である．$(-k+p)$ は基底ベクトルの係数である．本稿では，係数は $J = 1$ とした．$\hat{H}_p$ の基底状態は，$\|\boldsymbol{v}\|^2 = 0$，すなわち零ベクトルに対応するため，最短ベクトル問題の解に対応するのは $\hat{H}_p$ の第一励起状態である．

3.3.2 数式との対応

ある基底ベクトル $\boldsymbol{b}_i$ について考える．各基底ベクトルの整数係数 x_i の範囲を $-k \leq x_i \leq k$ に限定しているため，$\boldsymbol{b}_i$ の整数係数は $-k \sim k$ の $2k+1$ 個ある．この $2k+1$ 個の量子ビットで，$-k \sim k$ の係数のうちどれを採択するか，を表現する．ここで，量子ビットは 1(up スピン) か -1(down スピン) の二値をとり，j 番目の量子ビットの値が 1 ならば係数 x_j が採択される (図 3.2).

さらに，各量子ビットに係数の情報を加える必要がある．実装上はインデックスは $0 \sim 2k$ であり，それぞれが係数 $-k \sim k$ に対応する．係数をインデックスを用いて表すには，ループ変数を p として $(-k+p)$ とし，その和を取れば良い．これが，$\hat{Q}^{(i)} = \frac{1}{2} \sum_{p=0}^{2k} (-k+p) \hat{\sigma}_z^{(p,i)}$ に対応する．

以上を各次元について考えることで，n 次元の基底ベクトル・係数を二値変数を用いて表現することができる．

3.3.3 制約項

本研究における目的関数では，それぞれの量子ビットが対応する整数係数の存在の有無を表す．そのため,「各次元において整数係数は 1 つだけ」という制約条件を問題ハミルトニアンに追加する必要がある．

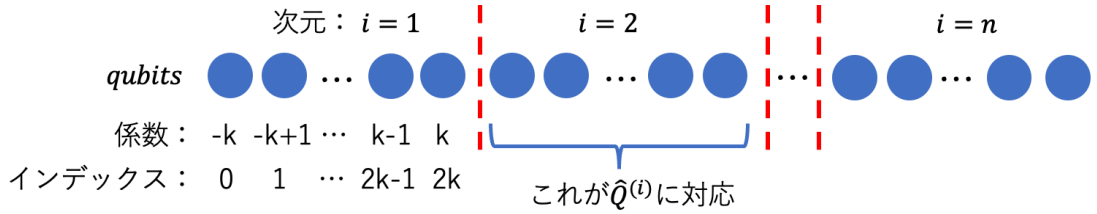

図 3.2: 基底ベクトルの整数係数と対応する量子ビットのイメージ

ある基底ベクトル $\boldsymbol{b}_i$ について考える．この基底における整数係数 x_i はただ 1 つに定まって欲しいので，1 つの量子ビットだけ 1 をとり，他の量子ビットは -1 になるような制約条件が必要である．基底 $\boldsymbol{b}_i$ における整数係数は全部で $-k \sim k$ の $2k+1$ 個であり，全てが $\{-1, 1\}$ の二値のいずれかをとることから，量子ビットの値の和が $2k-1$ になればよい．この制約条件を定式化すると，

$$J_i = \left(\sum_{p=0}^{2k} \hat{\sigma}_z^{(i,p)} - (-2k+1) \right)^2 \tag{3.8}$$

となる．これは，各量子ビットの値の和が $-2k+1$ の時に 0 となり，そのほかの時は正の値をとる．図 3.3 は，$k=2$ の場合の，ある基底における各スピンのイメージである．このとき，$2 \cdot 2 + 1 = 5$ 個の量子ビットを用いて，$-2 \sim 2$ までの各係数を表す．このうち 1 つが $+1$，4 つが -1 であればいいので，制約条件は $\sum_{p=0}^{4} \hat{\sigma}_z^{(i,p)} = -2 \cdot 2 + 1 = -3$ となる．

イジングモデルは，特定のスピンの形状をとらない，というような制約条件を課すことはできないので，条件を満たさない時にエネルギーを大きくする，というペナルティの形で制約条件を表現する．

以上を各次元について考える．具体的には，以下の制約項

$$H_{penalty} = \lambda \sum_{i=1}^{n} \left(\sum_{p=0}^{2k} \hat{\sigma}_z^{(i,p)} - (-2k+1) \right)^2 \tag{3.9}$$

を問題ハミルトニアンに追加する．ここで，λ は正の値をとる重み係数である．

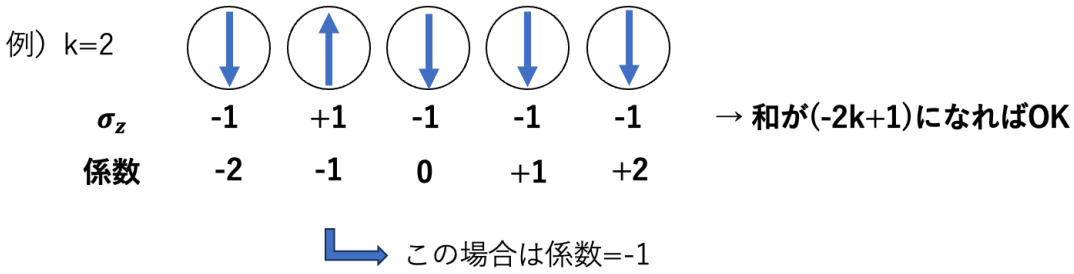

図 3.3: 各基底における制約条件のイメージ (k=2)

最終的に，最短ベクトル問題に対応する問題ハミルトニアンは以下の形である．

$$\hat{H}_{SVP} = J \sum_{i,j=1}^{n} G_{ij} \hat{Q}^{(i)} \hat{Q}^{(j)} + \lambda \sum_{i=1}^{n} \left(\sum_{p=0}^{2k} \hat{\sigma}_z^{(i,p)} - (-2k+1) \right)^2 \tag{3.10}$$

第4章　提案手法と評価方法

4.1　提案手法

最短ベクトル問題の解は，問題ハミルトニアンの非自明な第一励起状態に対応する．本研究では，虚時間発展法を用いた最短ベクトル問題の解の探索手法を提案する．虚時間発展法による励起状態探索には，量子化学計算の分野で研究されている FS 法を用いる．FS 法を用いた第一励起状態探索には，ハミルトニアンの第一励起状態のエネルギー固有値 E_1 近傍のパラメータが必要である．そこで，二分法を拡張した，パラメータの絞り込み手法も併せて提案する．

最短ベクトル問題において，ハミルトニアンのエネルギーは格子ベクトルのノルムに対応する．ハミルトニアンの基底状態は零ベクトルに対応するため，基底エネルギーは $E_0 = 0$ である．ここで，ある実数 $\alpha, \beta (\alpha < \beta)$ を用いて，m 個のエネルギー固有値が $\alpha < E_{i_1,\cdots,i_m} < \beta$ となる状況を考える．適当な実数 $\omega \in [\alpha, \beta]$ を選び FS 法を実行すると，ω に応じて，エネルギーが $E_{i_1,\cdots,i_m}$ である固有状態の中のいずれかの状態に収束する．

本手法では，α は十分小さい正実数 ε を用いて $\alpha = \varepsilon$ で固定しておく．これは，$E_0 = 0, E_1 > E_0$ であるため，$E_1 > \varepsilon$ と仮定しているためである．β は第一励起状態のエネルギーより十分大きい値で初期化する．この初期範囲内で FS 法を行うと，$[\alpha, \beta]$ に含まれるエネルギー固有状態の集合が得られる．次のループでは，得られた固有値を用いて β を小さな値へ更新する．このループを繰り返し，区間の

上限値である β を更新していくことで，最終的に

$$(0 <)\alpha < E_1 < \beta < E_2 < \cdots \tag{4.1}$$

を満たす α, β を見つけることができれば，解の探索が完了する (図 4.1).

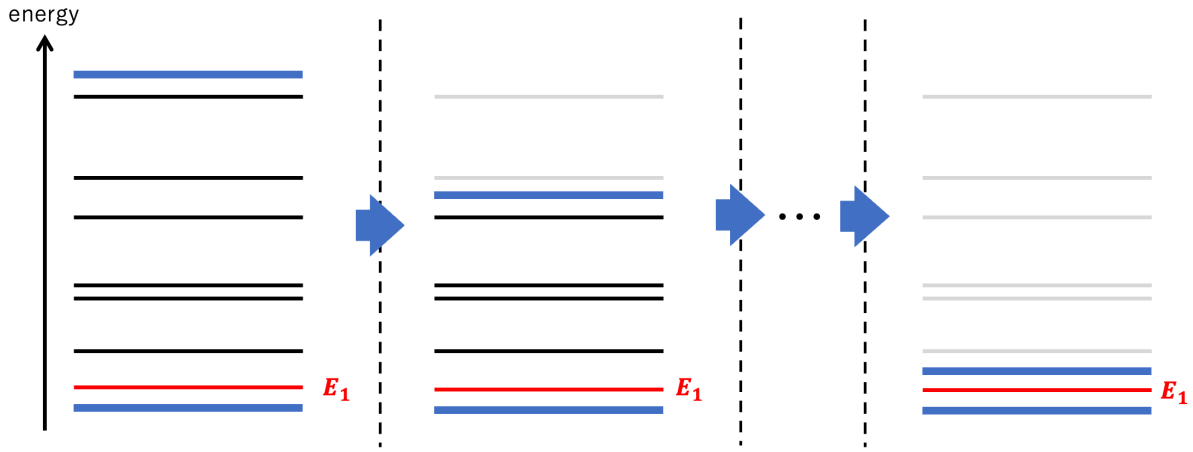

図 4.1: 第一基底エネルギー E_1 の絞り込み手法のイメージ

具体的な $[\alpha, \beta]$ の更新方法について述べる．あるループにおいて，パラメータ ω を $[\alpha, \beta]$ の範囲内で小さいステップ単位で動かしながら逐次 FS 法を実行すると，$\alpha < E'_{i_1,\cdots,i_{m'}} < \beta$ を満たすエネルギー固有値の集合 $\{E'_{i_j}\}_{j=1}^{m'}$ が得られる．なお，実際に $[\alpha, \beta]$ に含まれるすべてのエネルギー固有値の集合を $\{E_{i_j}\}_{j=1}^{m}$ とすると，FS 法によって得られた集合 $\{E'_{i_j}\}_{j=1}^{m'}$ はすべてのエネルギーを探索できていない可能性があるので，$\{E'_{i_j}\}_{j=1}^{m'}$ は $\{E_{i_j}\}_{j=1}^{m}$ の部分集合である．すなわち，$\{E'_{i_j}\}_{j=1}^{m'} \subseteq \{E_{i_j}\}_{j=1}^{m}$, $m' \leq m$ である．これは ω を動かすステップの値に起因する．上記の操作により求めた集合 $\{E'_{i_j}\}_{j=1}^{m'}$ のうち，最小のエネルギー値 E'_{i_1} と十分小さい正実数 x を用いて，$\beta \leftarrow E'_{i_1} + x$ として次の範囲を更新する．この x は，$E'_{j_1} = E_1$ となったときに，次の探索で E_1 が範囲に含まれない可能性を排除するためである．

このループを繰り返し行い，最終的に，FS 法によって得たエネルギー固有値が 1 つ (すなわち $m' = 1$) となったとき，得られたエネルギーの値こそが E_1 であると期待される．最終的にはこの E_1 を用いて再度虚時間発展を行い，収束した状態を

解として出力する．

実装上は，イテレーション回数の上限を設定し，途中で $m' = 1$ となったらループを抜け終了するようにした．実際にはイテレーションが上限まで行っても $m' = 1$ とならない場合が存在する．この場合は，得られた固有値 $\{E'_{i_j}\}_{j=1}^{m'}$ の最小値を近似的な第一励起エネルギーとし，その値を FS 法のパラメータとして虚時間発展を行う．

4.2 実験環境

実験で用いた計算機環境は以下の通りである．

表 4.1: 実験に用いた計算機環境

CPU	Apple M1
OS	macOS Sonoma 14.1.1
メモリ	16[GB]

なお，シミュレーションのプログラムについては Python の量子計算ライブラリである Qutip を用いた．量子状態の時間発展には，Qutip の mesolve メソッドを用いた．

4.3 評価方法

$(n, k) = \{(1,1), (1,2), (1,3), (2,1), (2,2), (3,1)\}$ とし，規格化された基底 $\{\boldsymbol{b}_i\}_{i=1}^{n}$ をランダムに設定してシミュレーションを行った．計算時間・正答率に関しては，各 (n, k) の組に対し，それぞれ 30 回の計算実験を行い，その平均値を用いた．その他の条件は以下の通りである．

- 実験において，FS 演算子は $\hat{H}' = (\hat{H} - \omega I)^2$ とした

– 一般に FS 演算子の指数は $2m$ であるが，計算量の観点から 2 とした．なお，古典コンピュータ上のシミュレーションの範囲では，$\hat{H} - \omega I$ の各成分の絶対値をとったものを $\hat{H}'$ とすることで，解の探索を行うことも可能である．しかし，異なるエネルギー固有値の差が拡大・縮小するなどの差異が発生するので，$(\hat{H} - \omega I)^2$ の場合と同様の結果とはならない．具体的には，指数が 2 の場合，サイズが $2^{(2k+1)n} \times 2^{(2k+1)n}$ の行列同士の積を計算する必要がある．また，パラメータ ω との差が 1 未満であるエネルギー固有値については，2 乗することでその差がさらに小さくなってしまい．求解が困難になってしまう可能性がある．

- 初期探索範囲は ε を十分小さい正実数として $[\varepsilon, 100]$ とした

  – 探索範囲の分割数は 100 とした．範囲の初期上限値を 100 と設定したのは，シミュレーションの範囲ではノルムの値は 100 以下となり，すべての解の探索が可能であるためである．

- ハミルトニアンにおける制約項の重み係数は $\lambda = 2.5$ とした

  – λ の値はヒューリスティックに決定した．具体的には，制約条件を満たさない解のエネルギーが，各格子ベクトルのノルムの 2 乗の値の最大値を超えるように決定した．

- 虚時間発展における時間は $T = 50$，分割数は 100 とした

  – 発展時間である T は，状態が十分に収束する時間であり，かつ探索が現実的な時間で終わりるような値をヒューリスティックに決定した．分割数においても同様である．この分割数が小さいと，量子状態の時間発展を計算する際に ODE エラーが発生する．これは時間のステップ数が減少することで，離散ステップで近似的に計算を行う ODE 積分の精度が

低下するためである．一方，分割数を大きくし過ぎると，1 回のループあたりの計算量が大きくなり，結果として計算時間の増大が発生する．

また，正答率に対する第一励起エネルギーおよび基底ベクトル間の角度依存性を調査するため，$(n, k) = (2, 1)$ において，基底ベクトル間のなす角 θ を $(0, \pi)$ で変化させながら解の探索を行った (図 4.3).

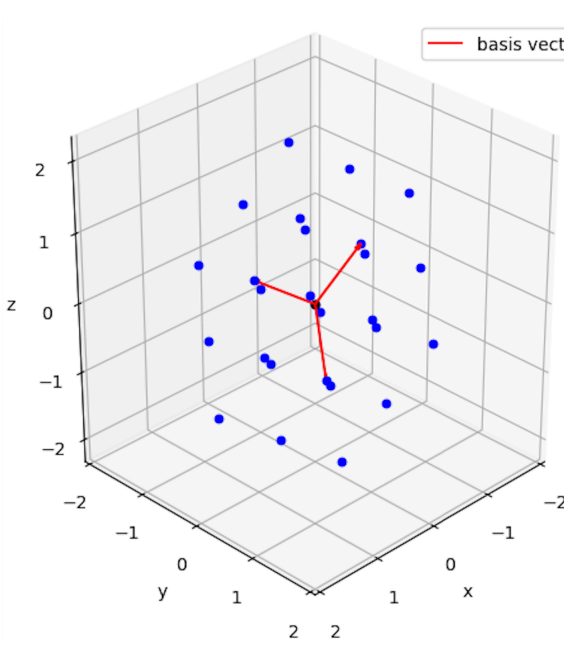

図 4.2: $(n, k) = (3, 1)$ の例

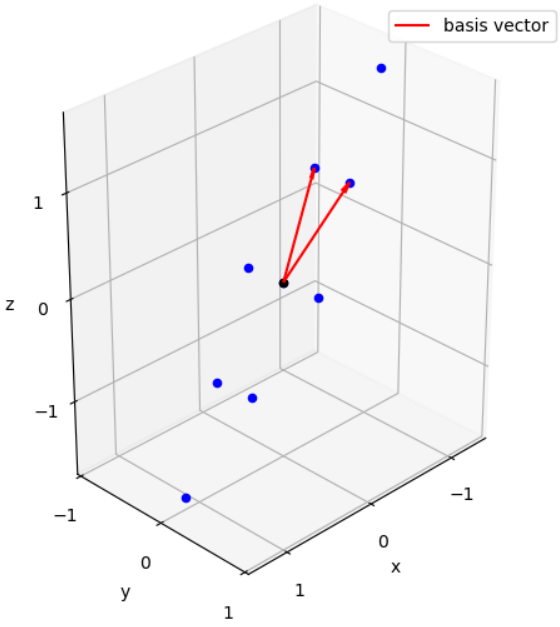

図 4.3: $(n, k) = (2, 1)$ の例

第5章　結果と考察

5.1　実行結果

結果として，実験を行った範囲 (量子ビット数が 10 以下) では，提案手法によって解の探索に成功した (表 5.1)．ここでは,「解の探索に成功すること」を,「提案手法によって求めた解と古典ライブラリによって求めた厳密解が一致する」と定義する．また，図 5.1 に量子ビット数と正答率の関係，図 5.2 に第一励起エネルギーと正答率の関係を示す.

表 5.1: (n, k) と正答率・計算時間の関係

(n, k)	qubit	Acc	Time[s]
$(1, 1)$	3	1.0	$5.7(7) \times 10^1$
$(1, 2)$	5	1.0	$8(1) \times 10^2$
$(2, 1)$	6	0.91	$5(3) \times 10^2$
$(1, 3)$	7	1.0	$10(2) \times 10^3$
$(3, 1)$	9	0.53	$5(2) \times 10^3$
$(2, 2)$	10	0.78	$7(1) \times 10^4$

ここで，Acc は正答率，Time は最終的に解を出力するまでにかかる時間の平均を表している．また，必要な量子ビット数 qubit は $(2k + 1)n$ で計算される．量子ビット数が 7 以下の範囲では，0.9 以上の正解率で解を求めることができた．量子ビットが 9,10 のサイズにおいては，正答率が下がったものの，0.5 以上の正答率となった.

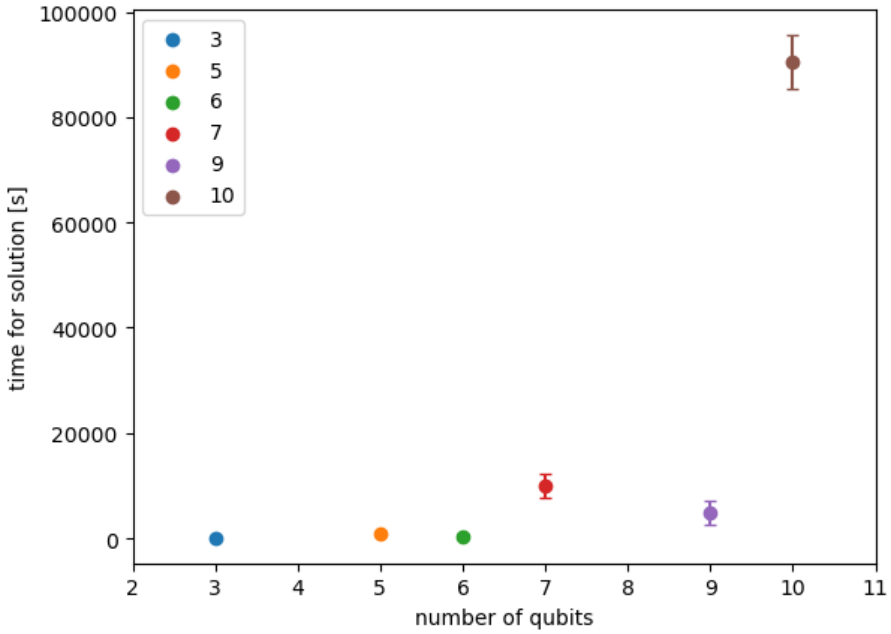

図 5.1: 量子ビット数と計算時間の関係

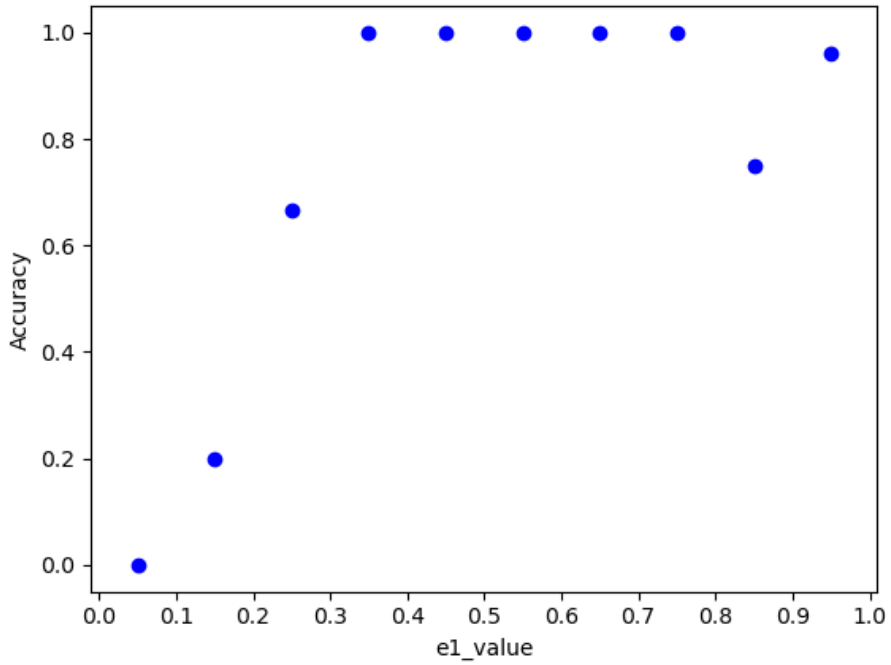

図 5.2: 第一励起エネルギーと正答率の関係

5.2 考察

5.2.1 正答率・計算時間

正答率については，量子ビット数が7以下，すなわち $(n,k)=\{(1,1),(1,2),(1,3),(2,1)\}$ の範囲では9割以上，量子ビットが9以上，$(n,k)=\{(3,1),(2,2)\}$ の範囲では $5\sim7$ 割という結果になった．系のサイズの増加に伴い，解の候補であるエネルギー固有値の値も増加するため，正答率が低下したと考えられる．

また，次元の増加により，近いエネルギー値を持つ状態が多くなると，正答率が低下すると考えられる．これは，FS 法によるエネルギー固有値探索の際に，エネルギー同士のギャップが小さいと，計算スケールの増大や計算精度の問題によって，正しい解が得られない可能性があるためである．実験結果より，第一励起エネルギーが 0 に近い値をとる時，$E_0=0$ であることから，基底エネルギーとのエネルギーギャップが小さくなり，正答率が下がっている．また第一励起エネルギーが 1 に近い場合でも，基底ベクトルに対応する状態とのエネルギーギャップが小さくなり，正答率が低下している．逆に，第一励起エネルギーが $0.4\sim0.7$ の範囲では，他の状態のエネルギーとある程度離れており，正答率が高くなっている (図 5.2)．これは主に次元 n の増加によって起こるため，係数の範囲 k が増加しても正答率の低下の割合は小さい．

計算時間については，量子ビット数の増加に伴い指数関数的に増加した (図 5.1)．これは，初期探索範囲における解の候補数が，$(2k+1)^n$ で表されるため，n の累乗のオーダーで大きくなるためだと考えられる．n,k を比較すると，k の増加の方が,n よりも計算時間の増加に寄与している結果となった．これは単純に，量子ビット数が $(2k+1)n$ で計算されるためだと考えられる．

以上より，提案手法を最短ベクトル問題に適用させると，次元数 n が増加するにつれ問題の正答率が下がり，係数の範囲 k が増加するにつれ計算時間が増加すると結論づけられる．

5.2.2　角度依存性

最短ベクトル問題における入力は格子基底行列 $\boldsymbol{B}$ のみであるため，問題の難易度は $\boldsymbol{B}$ に依存する．本研究において，各基底ベクトルのノルムは $\|\boldsymbol{b}_i\| = 1$ と正規化しているため，問題ごとに異なるのは基底ベクトル間のなす角 θ である．正答率の角度依存性の検証のため，二次元格子である $(n, k) = (2, 1)$ において，2 基底ベクトル $\boldsymbol{b}_1, \boldsymbol{b}_2$ のなす角 θ を開区間 $(0, \pi)$ で変化させながら実験を行った (図 5.3)．図の横軸はなす角 θ であり，縦軸は第一励起エネルギーの値である．各条件において，解の探索に成功した例を青，失敗した例を赤でプロットした．

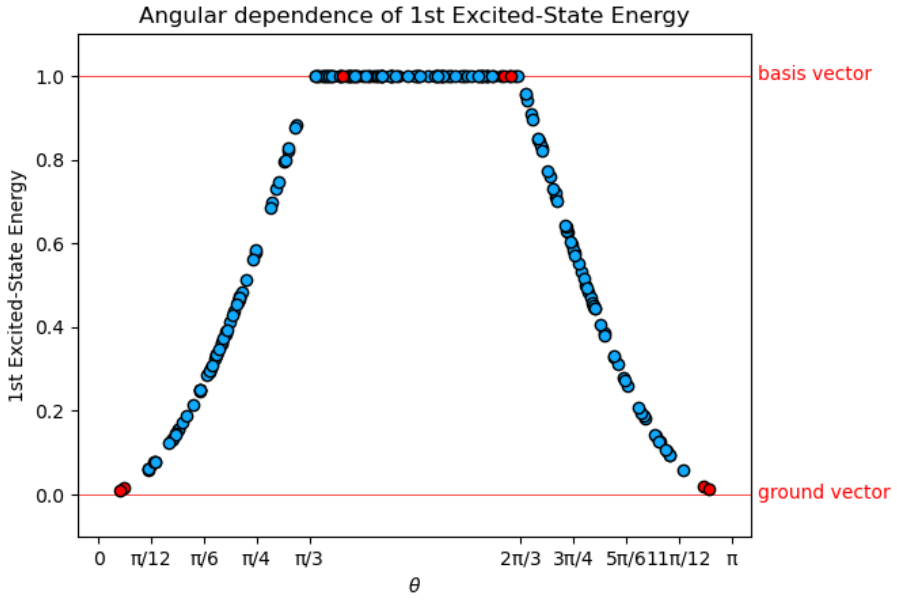

図 5.3: $(n, k) = (2, 1)$ における第一励起エネルギーの角度依存性

零ベクトルと基底ベクトルのノルムはそれぞれ $0, 1$ であるので，第一励起エネルギーは閉区間 $[0, 1]$ に含まれる．5.2.1 の議論により，第一励起エネルギーが 0 または 1 に近いと，エネルギーギャップが小さくなり，正答率が下がる．ここで，第一励起エネルギーが 0 に近くなる θ の条件を考えると，簡単な計算により，$\theta \approx 0$ または $\theta \approx \pi$ となることがわかる．実際，$\theta \approx 0, \pi$ 付近の問題設定では失敗した例が多くなっている．次に，第一励起エネルギーが 1 に近くなる条件は，$\theta \approx \frac{\pi}{3}$ また

は $\theta \approx \frac{2\pi}{3}$ となる．これも，$\theta \approx \frac{\pi}{3}, \frac{2\pi}{3}$ 付近に失敗した例が存在することがわかる．なお，$\frac{\pi}{3} < \theta < \frac{2\pi}{3}$ の範囲においては，2 つの基底ベクトルによって作られる格子点のノルムが 1 を超えるため，基底ベクトルとその (-1) 倍のベクトル自身に対応する状態が第一励起状態となる．

5.2.3 求解困難なケースの考察

ここで，探索した解が厳密解と一致しなかったケースについて考察する．求解ができなかった要因として，以下の要因が考えられる．

1. 第一励起エネルギーと他のエネルギー固有値とのギャップが小さい

    - 5.2.2 で示したように，問題となる格子の設定によって，エネルギー固有値同士の差が小さくなる場合がある．特に第一励起エネルギーと他のエネルギー固有値の差が小さい場合，多くの状態が，正解でない固有状態に収束してしまい，それを解として出力してしまう可能性がある．

2. 状態の発展時間 T が小さい

    - 原理的には，適切な ω を用いて FS 法を実行し虚時間発展を行えば，所望の状態に収束する．しかし，これはあくまで虚時間 $\tau \to \infty$ の場合である．実装上は，τ を有限時間 T で打ち止めにしてその時点での固有状態を判別しているので，厳密解と比較してエネルギー固有値に対して誤差が発生する可能性がある．一方，この有限時間 T を大きくすると．固有値計算におけるステップ数を大きくしなければならず，これも計算時間の増加に寄与してしまう．収束性と計算ステップの増大はトレードオフであるため，適切なパラメータを判断する必要がある．

第6章　まとめと展望

6.1　まとめ

本研究では，格子問題の 1 つである最短ベクトル問題について，虚時間発展法を用いた解の探索手法を提案した．最短ベクトル問題の解は問題ハミルトニアンの非自明な第一励起状態に対応する．そのため，基底状態探索手法である虚時間発展法を単純に適用することはできない．そこで，励起状態探索手法として FS 法を用い，その際のパラメータの絞り込み手法についても提案を行った．検証実験として，$(2k+1)n \leq 10$ を満たす (n,k) において，解の探索可能性の検証を行った．シミュレーションの結果，実際に提案手法が最短ベクトル問題の解の探索に有用であることを示した．また，実験における正答率・計算時間において．それらの問題サイズ依存性．および基底ベクトルの角度依存性について議論を行った．

6.2　今後の展望

今後の展望として，11 量子ビット以上のさらに大きい系でのシミュレーションや，3 次元以上の際の基底ベクトルの角度依存性について議論する必要がある．実際に格子暗号として使用されるレベルは次元 $n > 400$ ほどであるので，次元の増加に対する正答率の低下・計算時間の増加に耐性のある手法の議論は重要である．また，第一励起エネルギー E_1 の絞り込みの際のパラメータについて，問題サイズによるエネルギースケールを考慮した検討を行う．

謝辞

本研究を進めるにあたり，多くのご指導をいただいた渡部昌平准教授に深く感謝致します．また，OIST の比屋根芳周氏，研究室の先輩・同期のみなさまには大変お世話になりました．ありがとうございます．

参考文献

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[2] 高木剛. 暗号と量子コンピュータ -耐量子計算機暗号入門-. オーム社, 2019.

[3] Katsuki Ura, Takashi Imoto, Tetsuro Nikuni, Shiro Kawabata, and Yuichiro Matsuzaki. Analysis of the shortest vector problems with the quantum annealing to search the excited states. *Japanese Journal of Applied Physics*, Vol. 62, No. SC, 8 2022.

[4] 嶋田義皓. 量子コンピューティング：基本アルゴリズムから量子機械学習まで. オーム社, 2020.

[5] Tadashi Kadowaki and Hidetoshi Nishimori. Quantum annealing in the transverse ising model. *Phys. Rev. E*, Vol. 58, pp. 5355–5363, Nov 1998.

[6] 宇都宮聖子. 量子コンピュータの新潮流：量子アニーリングと d-wave. 人工知能, Vol. 29, No. 2, pp. 190–194, 2014.

[7] 石坂智, 小川朋宏, 河内亮周, 木村元. 量子情報科学入門. 共立出版, 2012.

[8] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, Vol. 41, No. 2, pp. 303–332, 1999.

[9] Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996.

[10] George H Booth and Garnet Kin-Lic Chan. Communication: Excited states, dynamic correlation functions and spectral properties from full configuration interaction quantum monte carlo. *The Journal of chemical physics*, Vol. 137, No. 19, 11 2012.

[11] Takashi Tsuchimochi, Yoohee Ryo, Seiichiro L. Ten-no, and Kazuki Sasasako. Improved algorithms of quantum imaginary time evolution for ground and excited states of molecular systems. *Journal of Chemical Theory and Computation*, Vol. 19, No. 2, 1 2023.

[12] Jarrod R McClean, Jonathan Romero, Ryan Babbush, Al ├ínAspuru-Guzik. The theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*, Vol. 18, No. 2, p. 023023, feb 2016.

[13] 縫田光司. 耐量子計算機暗号. 森北出版, 2020.

[14] Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM Journal on Computing*, Vol. 30, No. 6, pp. 2008–2035, 2001.

[15] S. Khot. Hardness of approximating the shortest vector problem in lattices. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pp. 126–135, 2004.

[16] A.K.Lenstra, H.W.Lenstra, and L.Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 1982.

[17] Joseph David, Callison Adam, Ling Cong, et al. Two quantum ising algorithms for the shortest-vector problem. *Phys. Rev. A*, Vol. 103, p. 032433, Mar 2021.