量子断熱計算を用いた古典最適復号に関する研究

西野 祐太　　指導教員：臼田 毅

1　はじめに

量子断熱計算（Adiabatic Quantum Computation,AQC）は，組み合わせ最適化問題を高速に解くアルゴリズムとして，Farhi ら [1] らによって提案された．この計算アルゴリズムは，1998 年に門脇と西森によって考案された量子アニーリング（Quantum Annealing,QA）[2] の理論を基にしたものである．現在では，D-Wave 社によってこれらのアルゴリズムを実装した量子計算機が商品化されており，そのアプリケーションを探す研究が活発になっている．しかし，量子アニーリングマシンの高速性を発揮できるアプリケーションがまだ多く見つかっていないのが現状である．そこで本稿では，量子断熱計算（量子アニーリング）のアプリケーションを探すことを目的として研究を行う．特に応用先として，ディジタル通信の分野での問題である古典最適復号を考える．古典最適復号とは，軟判定と最尤復号をもちいる復号法であり，誤る確率がもっとも小さい復号法である．古典最適復号では，ある受信語を受け取ったときに，送信された可能性がもっとも高い符号語を探しだし，その符号語で符号化された元のメッセージへと復号を行う．符号語は，情報記号数 k に対して，2^k 個存在し，復号を行うためにはこれら一つ一つに対して評価関数を計算する必要があるため，指数回の計算が必要となる．一部の符号では，効率的に最適復号を行うアルゴリズムは存在するが，任意の符号に対して効率的なアルゴリズムは存在しない．量子暗号 Keyed Communication in Quantum Noise(KCQ) プロトコルでは，性能評価のために盗聴者と正規受信者の復号誤り率を求める必要があるが，古典最適復号の膨大な計算量により，厳密な誤り率ではなく，近似値や上界，下界などを用いて評価している [3]．そのため，古典最適復号の計算量を削減することは非常に重要な問題である．

本稿では，AQC によって効率的に古典最適復号を行うことができる可能性を探る．そのためにまず，古典最適復号のためのハミルトニアンを構成する．そして，最良でどの程度の計算量となるのか確認するために，アニーリングスケジュールと呼ばれるパラメータを最適化する．

2　量子断熱計算

2.1　量子断熱計算のハミルトニアン

AQC では，次のハミルトニアンによって定まるエネルギー最小の状態（基底状態）を見つけることで問題を解く．

$$H(t) = \big(1 - q(t)\big)H_0 + q(t)H_1 \tag{1}$$

ここで，$q(t)$ はアニーリングスケジュールと呼ばれるものであり，$q(0) = 0, q(1) = 1$ を満たすような単調増加関数である．AQC のアルゴリズムでは，t を 0 から 1 へと変化させることで実行される．H_1 はアルゴリズム終了時のハミルトニアンであり，問題の評価関数の働きをするように構成する．そのため，H_1 の最小エネルギー状態である基底状態が問題の評価関数の最小値に対応しており，この基底状態を見つけることで最適解を得る．しかし，H_1 の基底状態は非自明なものであるため，これを簡単に見つけることはできない．そこで，H_1 とは別に，基底状態が自明な H_0 を用意する．アルゴリズムの初期状態 $t = 0$ のときには，式 (1) の第一項のみであり，さらに H_0 の基底状態は自明であるので，その基底状態から計算をスタートすることができる．そして，t を 0 から 1 まで適切な速度で状態を変化させ，その各瞬間で基底状態をたどり続けることにより，最終的には $t = 1$ で H_1 の基底状態へと辿り着くことができ，問題の解を得ることができる．

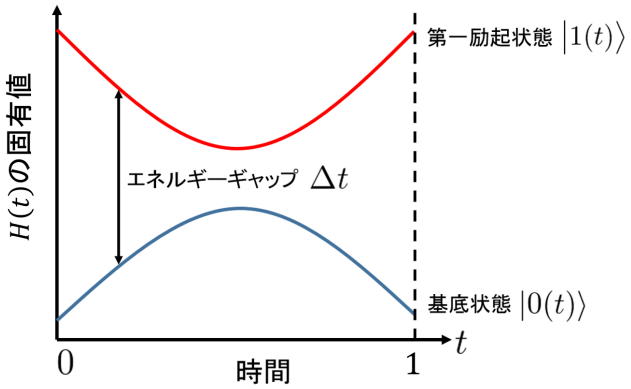

図 1　基底状態と第一励起状態の固有値の例．基底状態と第一励起状態の固有値の差は，エネルギーギャップ Δ_t であらわされる．

2.2　断熱定理

式 (1) の基底状態をたどるための，状態の適切な変化の速度は，次の断熱定理によって与えられる．

$$\tau \propto \frac{1}{\delta \min \Delta_t^2} \tag{2}$$

ここで，Δ_t は図 1 で示されているような，基底状態と第一励起状態の固有値の差であり，$1 - \delta^2$ は基底状態へと到達する確率となる．また，最小値は $0 \le t \le 1$ の範囲で考える．

2.3　アニーリングスケジュール

通常，$q(t)$ は線形スケジュール（一定）で変化させるが，効率的にアルゴリズムを実行するためには，非線形にすることが望ましい．なぜならば，第一励起状態への遷移のしやすさは，基底状態と第一励起状態の固有値の差によって定まるが，その差はアルゴリズムの各瞬間で変わるからである．そのため，固有値の差が大きいところでは状態を素早く変化させ，小さいところでは慎重に変化させるのが好ましい．このように，アニーリングスケジュールを最適なものにすることで計算時間を削減することができる．しかし，最適なアニーリングスケジュールは非自明なものであるため，これを見つける必要がある．

3　古典最適復号

本研究では，二元線形符号で符号化された binary-phase-shift-keying(BPSK) 信号を用いる．また通信路として，無記憶の加法的白色ガウス通信路を仮定し，符号として単一パリティ検査符号を用いる．古典最適復号では，次の条件付確率を最大にす

る符号語に復号を行う．

$$P(\boldsymbol{y}|\boldsymbol{w}_i) = \prod_{j=1}^{n} p(y_j|w_{i,j}) \tag{3}$$

ここで，$\boldsymbol{y} = (y_1, y_2, \ldots, y_n), y_i \in \mathbb{C}$ は通信路の出力，$\mathbb{C}$ は複素数全体の集合，$\boldsymbol{w}_i, (i = 1, 2, \ldots, 2^k)$ は符号語，k は情報記号数であり，n は符号語長である．各出力に対する条件付確率 $p(y_j|w_{i,j})$ は次のように計算される．

$$p(y_j|w_{i,j}) = \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\{(\mathrm{Re}[y_j]-\mathrm{Re}[w_{i,j}])^2+(\mathrm{Im}[y_j]-\mathrm{Im}[w_{i,j}])^2\}/2\sigma^2} \tag{4}$$

ここで，$w_{i,j} \in \{-A, A\}$ は BPSK 信号の振幅であり，σ^2 は雑音の分散である．受信者は，式 (3) の条件付確率を最大にする符号語 $\boldsymbol{w}_i$ に復号を行う．本稿では BPSK 変調を用いるため，式 (4) の虚数部分を省略することができる．さらに，符号語間での評価関数の大小関係に影響がない定数を省略し，式 (3) の対数尤度をとった次の式が最終的な評価関数となる．

$$\log P(\boldsymbol{y}|\boldsymbol{w}_i) = \sum_{j=1}^{n} 2y_j w_{i,j} + \mathrm{const.} \tag{5}$$

4　古典最適復号のためのハミルトニアンの構成

本章では，古典最適復号のためにハミルトニアンの構成を考える．初めに，初期状態のハミルトニアン H_0 は次のように構成される．

$$H_0 = I_{2^n} - |\psi(0)\rangle\langle\psi(0)| \tag{6}$$

ここで，

$$|\psi(0)\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=1}^{2^k} |\boldsymbol{w}_i\rangle, \quad |\boldsymbol{w}_i\rangle = \bigotimes_{j=1}^{n} |w_{i,j}\rangle \tag{7}$$

である．また，$|w_{i,j} = A\rangle = (1, 0)^{\mathrm{T}}$，$|w_{i,j} = -A\rangle = (0, 1)^{\mathrm{T}}$ であり，I_M は $M \times M$ の単位行列である．明らかに，H_0 の基底状態は $|\psi(0)\rangle$ であることがわかる．

次に，終状態のハミルトニアン H_1 はその固有値が問題の評価関数となるように，式 (5) の正負の符号を反転させたものと，単一パリティ検査符号の特徴を基に，次のように構成される．

$$H_1 = \sum_{j=1}^{n} \lambda_j - c(n) \bigotimes_{j=1}^{n} (\sigma_z - I_2) \tag{8}$$

ここで，$c(n)$ はペナルティ関数であり，λ_j は次のようなものである．

$$\lambda_j = I_2 \otimes I_2 \otimes \cdots \otimes \underbrace{-2Ay_j\sigma_z}_{j\mathrm{th}} \otimes \cdots \otimes I_2 \tag{9}$$

ここで，σ_z はパウリ行列であり，次のように定義される．

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{10}$$

5　数値シミュレーション

5.1　問題設定

AQC による古典最適復号のシミュレーションの簡単化のため，符号語長を $n = 6$，通信路の出力を $\boldsymbol{y} = (1, 1, 1, 1, 1, 1)$，BPSK 信号の振幅を $A = 1$，雑音の分散を $\sigma^2 = 1/2$ と設定する．また，ペナルティ関数を符号語長と振幅が大きくなるに従って増えるようにするため，$c(n) = nA^n$ と設定する．

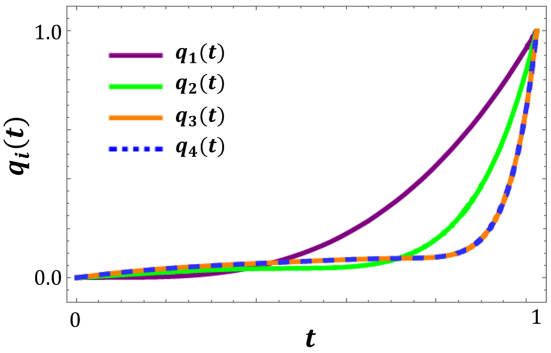

図 2　スケジュール q_i の変化 (i=1,2,3,4).

5.2　数値シミュレーション結果

AQC による，単一パリティ検査符号を用いた古典最適復号のための最適なスケジュールを見つけるために，まず初めに，式 (1) において $q(t) = t$ を用いた場合の各瞬間の固有値のふるまいに対して最適になるようなスケジュール $q_1(t)$ を求める．次に，スケジュールを $q_1(t)$ に置き換えた式 (1) に対して，最適なスケジュール $q_2(t)$ を求める．同様に $q_3(t)$ 以降も求める．これらを繰り返して，最終的にスケジュールがある一定のカーブに収束することを確かめたものが，図 2 である．縦軸はスケジュール $q_i(t)$ の値であり，横軸は経過時間 t を意味している．図 2 からスケジュール $q_i(t)$ が $q_3(t)$ 以降で一定のカーブに収束していることがわかる．数値実験では $i = 5, 6$ の場合も収束していることを確かめたが，図の見易さのために省略した．収束を確かめることができたことにより，AQC による単一パリティ検査符号を用いた古典最適復号における最適なスケジュールが存在すること，またその形を確かめることができた．

6　おわりに

本稿では，AQC の単一パリティ検査符号を用いた古典最適復号への適用について考察した．古典最適復号のためのハミルトニアンを構成し，さらに計算量削減の鍵となるアニーリングスケジュールの最適化を行った．今後の課題として，本稿で求めたスケジュールを用いた場合の計算量を見積もることや，収束を視覚的にではなく，数値的に確かめることなどが挙げられる．

参考文献

[1] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, Science **292**, pp. 472-474, (2001).

[2] T. Kadowaki and H. Nishimori, Phys. Rev. **E58**, pp. 5355-5363, (1998).

[3] A. Kadoya, Y. Umemura, S. Asano, N. Iwata, and T.S. Usuda, Proc. of AQIS2015, pp.161-162, (2015).

公表論文

[A] **Y. Nishino**, S. Takahira, A. Ohashi, and T.S. Usuda, Extd. Abst. of AQIS2016, pp.102-103, (2016).

[B] **Y. Nishino**, S. Takahira, A. Kadoya, and T.S. Usuda, Proc. of ISITA2016, p.563, (2016).

[C] **Y. Nishino**, S. Takahira, and T.S. Usuda, Proc. of AQIS2017, pp. 202-204, (2017).

他 2 件 (筆頭著者)，5 件 (第二以降著者)