

散逸ダイナミクスを用いた量子復号

○下村 光彦（東京大学），大木 健太郎（京都大学），津村 幸治（東京大学）

Quantum Information Decoding using Dissipative Dynamics

*M. Shimomura (The University of Tokyo), K. Ohki (Kyoto University),
K. Tsumura (The University of Tokyo)

Abstract— In this paper, we deal with quantum information decoding. Quantum codes are known as a technique to correct errors of quantum information caused by noise or operational errors and one of the most popular codes is the so-called stabilizer codes. Various implementation methods have been proposed to encode the original information into the stabilizer codes, but there have been few studies on decoding to extract original information from the codes. In this paper, we propose a decoding method of stabilizer codes for noise using dissipation dynamics and show that the original information can be extracted from the code. We furthermore evaluate its effectiveness by demonstrating numerical simulations.

Key Words: quantum information, decoding, error correction

1 はじめに

1.1 背景

量子力学に基づいて動作する量子コンピュータは、古典的なコンピュータでは現実的な時間や規模で解くことが難しい一部の問題に対して、高速に解くことが期待されている。例えば、素因数分解を行う問題に対して、古典コンピュータでは準指数時間で解くアルゴリズムしか知られていないが、量子コンピュータでは Shor のアルゴリズム [1] により多項式時間で解けることが示されている。実際、2001 年には 7 qubits の量子コンピュータで素因数分解に成功した例が報告されている [2]。

一方、汎用的な量子コンピュータの実現はいまだ容易ではない。その最大の要因にノイズに対する量子コンピュータの脆弱性が挙げられる。そのため量子コンピュータでは、計算過程でノイズによって情報に誤りが生じた際に、その誤りを検知および訂正する機能が求められる。そのような方法として、情報に冗長性を持たせる符号化によりこれを実現する量子誤り訂正符号という手法が注目されている。特に誤り訂正符号の一種であるスタビライザ符号 [3] への符号化方法については既に多くの研究 [4, Sec. 10.5][5] がなされてきた。

その一方、これらの研究は種々のユニタリ操作が可能という仮定のもとでの数学的議論に限られており、その実現性については十分検討されていない。さらに、符号から元の情報を取り出す復号方法についてはこれまでほとんど研究されてこなかった。量子情報理論では、情報を取り出すには系にユニタリ演算子を作用させることで仮想空間と呼ばれる空間に符号化されている情報を実 qubit に移してから測定することを想定されるが、この手法では qubit の繊細な制御が必要とされてしまい、実問題においては確実に情報を取り出すことが難しい。情報は復号されなければ意味がないため、確実に復号化する手法の開発が望まれる。

以上を背景に本研究では、物理的実現性を考慮し、先行研究 [5] に倣いマルコフ散逸ダイナミクスを用いた

スタビライザ符号の復号手法を提案する。この方法では系の重ね合わせ状態を崩すことなく量子情報を復号することができる。また、散逸系を用いることで漸近的に目標状態へと収束することが保証されているため、ユニタリ操作のように厳密な時間制御を行う必要がない点も大きな特徴である。

1.2 記号の表記

\mathbb{Z}_2 を 2 を法とする整数の乗法群とし、 X^\top , X^\dagger , $\text{Tr}(X)$ をそれぞれ行列 X の転置、共役転置、トレースとする。また、行列 A, B について交換子 $[A, B] = AB - BA$, 反交換子 $\{A, B\} = AB + BA$ を定める。最後に、 $A \otimes B, A \oplus B$ はそれぞれ A と B のテンソル積と直和を表す。ただし、第 2.2 節のみ \oplus は排他的論理和を表す。

2 基本概念

2.1 量子情報の基本概念

本節の内容は [6, 7] を参考にした。 $i := \sqrt{-1}$ とし複素ヒルベルト空間 $\mathcal{H} = \mathbb{C}^n$ の元を $|\phi\rangle \in \mathcal{H}$ のように表記する。また、その双対空間の元を $\langle\psi| \in \mathcal{H}^*$ のように書き、前者をケット、後者をブラと呼ぶ。ケットとブラの間には $\langle\phi| = |\phi\rangle^\dagger$ の関係がある。ここに $(\cdot)^\dagger$ は共役転置を取る演算子である。 $\langle\psi|\phi\rangle$ は内積を表し、ノルムは $\|\phi\| := \sqrt{\langle\phi|\phi\rangle}$ である。

量子系の状態はヒルベルト空間の単位ベクトル ($\|\phi\| = 1$ なる $|\phi\rangle$) で記述される。また、 $e^{i\theta}|\phi\rangle$ は任意の $\theta \in \mathbb{R}$ について同一の物理状態に対応する。すなわち、状態ベクトル全体にかかるグローバルな位相因子は物理的意味を持たない。

\mathbb{C}^2 の標準基底を古典ビットとのアナロジーから $\{|0\rangle, |1\rangle\}$ のように表記し、量子ビット (qubit) と呼ぶ。

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

同様に n -qubit の系 (\mathbb{C}^2) $^{\otimes n}$ は 2^n 個の標準基底を持ち、それらは $|i_1 i_2 \cdots i_n\rangle, \forall i_k \in \{0, 1\}$ と表される。ここに

$|i_1 i_2 \cdots i_n\rangle$ は $|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle$ を略記したものである。以降、特に断らない限り行列表示の基底には標準基底を選ぶものとする。

実際の物理系においては、観測者の情報不足により物理系の状態が確率的に混合する場合がある。このような状態は状態ベクトルで記述できないため、密度演算子というものを導入して記述する。いま系が確率 p_i で状態 $|\phi_i\rangle$ にあったとする。このとき、この系の状態を表す密度演算子は

$$\rho = \sum_i p_i |\phi_i\rangle \langle \phi_i|$$

で定められる。密度演算子は次の性質を満たすことが知られている。

$$\rho = \rho^\dagger, \quad \rho \geq 0, \quad \text{Tr}(\rho) = 1.$$

また、状態 ρ の下で物理量 A を測定したときに得られる結果の期待値は

$$\langle A \rangle = \text{Tr}(A\rho) \quad (2.1)$$

によって与えられる。系が確率 1 でただ一つの状態にあるとき系は純粋状態にあるといい、確率 $\{p_i\}_i$ で混合しているとき系は混合状態にあるという。この状態を判別する方法に純粋度と呼ばれる $\text{Tr}(\rho^2)$ で与えられる量を調べる方法があり、

$$\text{Tr}(\rho^2) = 1 \Leftrightarrow \text{系は純粋状態にある}$$

$$\text{Tr}(\rho^2) < 1 \Leftrightarrow \text{系は混合状態にある}$$

の関係が成り立つことが知られている。

次に示す 3 つの複素正方行列 X, Y, Z に単位行列 I を加えた 4 つの行列 $\{I, X, Y, Z\}$ をパウリ行列と呼ぶ。

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

任意の行列 A について、

$$A = c_0 I + c_1 X + c_2 Y + c_3 Z \quad (2.2)$$

なる複素係数の組 $c_0, c_1, c_2, c_3 \in \mathbb{C}$ が存在することが知られている。

2.2 スタビライザ符号

まず、パウリ群を導入する。パウリ行列 X, Y, Z はその自乗が単位行列に等しく

$$X^2 = Y^2 = Z^2 = I,$$

また、相異なる行列同士の積は次の関係式を満たす。

$$XY = -YX = iZ,$$

$$YZ = -ZY = iX,$$

$$ZX = -XZ = iY$$

したがって、

$$\mathcal{P} := \{\pm 1, \pm i\} \times \{I, X, Y, Z\}$$

は群をなす。一般にパウリ行列の n 重テンソル積を取った

$$\mathcal{P}_n := \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}$$

を n -qubits のパウリ群と呼ぶ。また、下付きの添字により作用先の qubit を表すことにする。すなわち、 X_j, Y_j, Z_j はそれぞれ j 番目の qubit にのみ X, Y, Z として作用し、他の qubit には I として作用する。

パウリ群 \mathcal{P}_n の部分群 \mathcal{S} であって、全ての要素が互いに可換であるような \mathcal{S} をスタビライザ群と呼ぶ。すなわち、

$$\forall S_i, S_j \in \mathcal{S} \subset \mathcal{P}_n, \quad [S_i, S_j] = 0$$

が成り立つ。スタビライザ群 \mathcal{S} の独立な元の最大集合を \mathcal{S} の生成子と呼ぶ。ここに独立であるとは他の元の積で表せないことを意味する。

生成子 $\{S_i\}_{i=1}^r$ で生成されるスタビライザ群を $\langle S_1, S_2, \dots, S_r \rangle$ で表す。また、

$$S_i |\phi\rangle = |\phi\rangle \text{ for all } S_i \in \mathcal{S}$$

を満たす状態 $|\phi\rangle$ を \mathcal{S} によってスタビライズされる状態と呼ぶ。

次に論理演算子を導入する。スタビライザ群 $\mathcal{S} = \langle \{S_i\}_{i=1}^r \rangle$ に対して、次のような性質を満たす論理演算子 $\{\bar{X}_k, \bar{Z}_k\}_{k=1}^{n-r} \subset \mathcal{P}_n$ を定める。

$$[\bar{X}_k, S_i] = [\bar{Z}_k, S_i] = 0, \quad \text{for all } i, k$$

$$\{\bar{X}_k, \bar{Z}_k\} = 0, \quad \text{for all } k$$

$$[\bar{X}_k, \bar{Z}_l] = 0, \quad \text{for all } k \neq l$$

$$[\bar{X}_k, \bar{X}_l] = [\bar{Z}_k, \bar{Z}_l] = 0, \quad \text{for all } k, l$$

スタビライザ符号 \mathcal{C} はスタビライザ群 \mathcal{S} と論理演算子 $\{\bar{X}_k, \bar{Z}_k\}_{k=1}^{n-r}$ の組に対して定められる。一般に互いに可換でかつ独立な n 個の元を \mathcal{P}_n から取ると、その固有値 $+1$ の同時固有状態は一意に決定される。そこで \mathcal{C} の各符号語を次のように定める。

$\langle S_1, \dots, S_r, (-1)^{i_1} \bar{Z}_1, (-1)^{i_2} \bar{Z}_2, \dots, (-1)^{i_{n-r}} \bar{Z}_{n-r} \rangle$ によってスタビライズされる状態を、論理基底 $|i_1 i_2 \cdots i_{n-r}\rangle_L$ として定める。このとき、定義から

$$\bar{Z}_k |i_1 i_2 \cdots i_{n-r}\rangle_L = (-1)^{i_k} |i_1 i_2 \cdots i_{n-r}\rangle_L$$

を満たし、さらに

$$\begin{aligned} & \bar{Z}_k (\bar{X}_k |i_1 i_2 \cdots i_{n-r}\rangle_L) \\ &= -\bar{X}_k \bar{Z}_k |i_1 i_2 \cdots i_{n-r}\rangle_L \\ &= (-1)^{i_k \oplus 1} (\bar{X}_k |i_1 i_2 \cdots i_{n-r}\rangle_L) \end{aligned}$$

から

$$\bar{X}_k |i_1 \cdots i_k \cdots i_{n-r}\rangle_L = |i_1 \cdots (i_k \oplus 1) \cdots i_{n-r}\rangle_L$$

を満たす。ただし、 \oplus は排他的論理和を表す。これより \bar{X}_k, \bar{Z}_k は論理基底上でパウリ演算子のように振る舞うことが確認できる。スタビライザ群と論理演算子

によって定められる量子誤り訂正符号をスタビライザ符号という。

最後に生成子 $\{S_i\}_{i=1}^r$ の効果的な表現方法として検査行列 [4, Sec. 10.5] を導入する。これは $r \times 2n$ 型の行列で、 i 行目は生成子 S_i に対応している。いま $S_i = P_{i1} \otimes \cdots \otimes P_{in}$, $P_{ij} \in \{I, X, Y, Z\}$ であるとすると、検査行列 M の要素は

$$\begin{aligned} M_{i,j} &= 0, & M_{i+n,j} &= 0 & (P_{ij} &= I) \\ M_{i,j} &= 1, & M_{i+n,j} &= 0 & (P_{ij} &= X) \\ M_{i,j} &= 1, & M_{i+n,j} &= 1 & (P_{ij} &= Y) \\ M_{i,j} &= 0, & M_{i+n,j} &= 1 & (P_{ij} &= Z) \end{aligned}$$

となる。また、次のような行列 Λ を定める。

$$\Lambda = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$$

このとき、パウリ群 g_1, g_2 が可換であるとは、それぞれの対応する検査行列 G_1, G_2 が $G_1 \Lambda G_2^\top = 0$ を満たすことと同値である。

検査行列において、行の置換は生成子のラベルの付け直しを、列の置換は qubit のラベルの付け直しを、行同士の加算は生成子同士の積による生成子の取り直しを意味する。よって、検査行列に行基本変形および列の置換を施しても、対応するスタビライザ群は変化しない。この性質を利用した検査行列の標準形が存在し、任意の検査行列は

$$S = \left[\begin{array}{ccc|ccc} A_1 & A_2 & I_k & B & 0 & C \\ 0 & 0 & 0 & D & I_{r-k} & E \end{array} \right]$$

の形に変形できる。ここに各ブロック行列は $A_1 \in \mathbb{Z}_2^{k \times n-r}$, $A_2 \in \mathbb{Z}_2^{k \times r-k}$, $B \in \mathbb{Z}_2^{k \times n-r}$, $C \in \mathbb{Z}_2^{k \times k}$, $D \in \mathbb{Z}_2^{r-k \times n-r}$, $E \in \mathbb{Z}_2^{r-k \times r-k}$ の形状をしたバイナリ行列である。

3 先行研究

3.1 マルコフ散逸ダイナミクス

本章では F. Ticozzi らによるマルコフ散逸ダイナミクスを用いた符号化手法 [5] についてまとめる。対象となる符号空間は $\mathcal{C} \simeq \mathcal{H}_L \otimes \mathcal{H}_F \oplus \mathcal{H}_R$ と分解できる [8]。ここに \mathcal{H}_L は符号化された論理情報に対応するヒルベルト空間を、 \mathcal{H}_F は符号による冗長項に対応するヒルベルト空間を、 \mathcal{H}_R はこれらに直交するヒルベルト空間をそれぞれ表す。同様に、物理系に対応するヒルベルト空間も $\mathcal{H}_P = \mathcal{H}_{L'} \otimes \mathcal{H}_{F'} \oplus \mathcal{H}_{R'}$ のように分解できる。ここで $\mathcal{H}_{L'}$ は \mathcal{H}_L に等長であるが、 $\mathcal{H}_{F'}$ は \mathcal{H}_F に等長である必要はない。このように表せば、符号化は \mathcal{H}_P から \mathcal{C} への写像として構成することができる。

量子系における連続時間のマルコフ散逸ダイナミクスは GKS-Lindblad マスター方程式 [9] により記述さ

れる。

$$\begin{aligned} \dot{\rho} &= \mathcal{L}(\rho) \\ &= -i[H, \rho] \\ &\quad + \sum_k \left(L_k \rho L_k^\dagger - 1/2 \{L_k^\dagger L_k, \rho\} \right) \end{aligned} \quad (3.1)$$

ここに ρ は系の状態を記述する密度演算子であり、 H は系のハミルトニアンを表すエルミート行列、 L_k は散逸項を表す任意の行列である。

3.2 連続時間符号化

先行研究 [5] では、この散逸項を適切に設計することで任意の情報の符号化が可能であることを示した。以下、その手法について簡単にまとめる。

符号空間 \mathcal{C} に対応するスタビライザ群 $S = \langle S_1, S_2, \dots, S_r \rangle \subset \mathcal{P}_n$ が与えられたとき、第 2.2 節の手順により生成子の検査行列は次のように表せる。

$$S = \left[\begin{array}{ccc|ccc} A_1 & A_2 & I_k & B & 0 & C \\ 0 & 0 & 0 & D & I_{r-k} & E \end{array} \right]$$

このとき、次の行列 G_X, G_Z を定める。

$$\begin{aligned} G_X &= \left[\begin{array}{ccc|ccc} I_{n-r} & D^\top & 0 & 0 & 0 & B \\ 0 & 0 & 0 & I_{n-r} & 0 & A_1^\top \end{array} \right] \\ G_Z &= \left[\begin{array}{ccc|ccc} I_{n-r} & D^\top & 0 & 0 & 0 & B \\ 0 & 0 & 0 & I_{n-r} & 0 & A_1^\top \end{array} \right] \end{aligned}$$

これは $S \Lambda G_X^\top = S \Lambda G_Z^\top = 0$, $G_X \Lambda G_Z^\top = I$ を満たすので、 G_X, G_Z がそれぞれの検査行列になるように、論理演算子 $\{\bar{X}_k\}_{k=1}^{n-r}, \{\bar{Z}_k\}_{k=1}^{n-r}$ を取ることができる。

次に訂正行列 $\{C_k\}_{k=1}^r$ を以下の手順により構成する。まず、次のような行列 \bar{S} を取る。

$$\bar{S} := \begin{bmatrix} S \\ G_Z \\ G_X \end{bmatrix} \in \mathbb{Z}_2^{(2n-r) \times 2n}$$

この \bar{S} に対して、 $\bar{S} \Lambda x_k = e_k$ (e_k は k 番目の要素のみが 1 で他の要素が 0 の単位ベクトル) なる $\{x_k\}_{k=1}^r$ が取れる [4, Prop. 10.4]。このようにして取った x_k が検査行列となるように対応する C_k を取ると、訂正行列 $\{C_k\}_{k=1}^r$ が構成できる。 $\{C_k\}_{k=1}^r$ は次の性質を満たす。

$$\begin{aligned} [C_k, \bar{X}_i] &= [C_k, \bar{Z}_i] = 0, \quad \forall i, k \\ [C_k, S_k] &= 0, \quad \forall k \\ [C_k, S_i] &= 0, \quad \forall i \neq k \end{aligned}$$

最後にスタビライザ群の生成子 $\{S_k\}_{k=1}^r$ と上で構成した訂正行列 $\{C_k\}_{k=1}^r$ を用いて、連続時間散逸エンコーダ (Continuous-time Dissipative Encoder, CDE) を構成する。次に示す Φ_k を用いて、写像 $\Phi := \Phi_r \circ \cdots \circ \Phi_1$ を定める。

$$\Phi_k(\rho) = A_{+,k} \rho A_{+,k}^\dagger + A_{-,k} \rho A_{-,k}^\dagger, \quad k = 1, \dots, r$$

ただし、 $A_{+,k}, A_{-,k}$ は次式で与えられる。

$$A_{+,k} = \frac{1}{2}(I + S_k), \quad A_{-,k} = \frac{1}{2}C_k(I - S_k)$$

このとき CDE は

$$\mathcal{L}(\rho) = \Phi(\rho) - \rho \quad (3.2)$$

で与えられ、これが GKS-Lindblad 方程式の特別な場合になっていることが確認できる (補題 1)。

F. Ticozzi らは式 (3.2) で与えられる CDE について、いくつかの定理を示し、これによって符号化が可能であることを示している。まず、系を式 (3.2) にしたがって時間発展させたとき、系が漸近的に収束すること [10, Prop. 43]。次に、その収束先が符号空間 \mathcal{C} 上であり、さらに \mathcal{C} 上の元を不変に保つこと [5, Prop. 1]。最後に、符号化にあたって付随する冗長化項 ($\mathcal{H}_{F'}$ の元) の初期値を上手く取ることで、元の情報と対応する符号語に適切に写されることを示した [5, Thm. 2]。

4 散逸系による復号化

4.1 復号空間

この章では第 3 章の手法により符号化した状態に対して、マルコフ散逸ダイナミクスを用いて復号する手法を示す。対象となる符号空間 \mathcal{C}_E に対応するスタビライザ群 S の生成子、 \mathcal{C}_E の論理演算子 $\{\bar{X}_k, \bar{Z}_k\}_{k=1}^{n-r}$ が

$$S = \left[\begin{array}{ccc|ccc} A_1 & A_2 & I_k & B & 0 & C \\ 0 & 0 & 0 & D & I_{r-k} & E \end{array} \right] \quad (4.1)$$

$$G_X = [I_{n-r} \quad D^\top \quad 0 \quad | \quad 0 \quad 0 \quad B] \quad (4.1)$$

$$G_Z = [0 \quad 0 \quad 0 \quad | \quad I_{n-r} \quad 0 \quad A_1^\top] \quad (4.2)$$

で与えられていたとする。このとき、次のような生成子 S' で生成されるスタビライザ群 S_D を考える。

$$S' = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 0 & I_k \\ 0 & I_{r-k} & 0 & 0 & 0 & 0 \end{array} \right] \quad (4.3)$$

これらは

$$S' \Lambda G_X^\top = S' \Lambda G_Z^\top = 0 \quad (4.4)$$

を満たすので、スタビライザ群 S_D と論理演算子 $\{\bar{X}_k, \bar{Z}_k\}_{k=1}^{n-r}$ で構成される符号空間 \mathcal{C}_D を考えることができる。本手法では \mathcal{C}_E から \mathcal{C}_D への適切な写像を構成し、それによりスタビライザ符号の復号が行えることを示す。

以降、特に断らない限り S_D の生成子を $\{S'_k\}_{k=1}^r$, \mathcal{C}_D の論理演算子を $\{\bar{X}'_k, \bar{Z}'_k\}_{k=1}^{n-r}$ で表す。当然

$$\bar{X}_k = \bar{X}'_k, \bar{Z}_k = \bar{Z}'_k, \quad k = 1, \dots, n-r \quad (4.5)$$

である。

4.2 提案手法

まず、第 3.2 節と同様にして訂正行列 $\{C'_k\}_{k=1}^r$ を構成する。すなわち、

$$\bar{S}' := \begin{bmatrix} S' \\ G_Z \\ G_X \end{bmatrix} \in \mathbb{Z}_2^{(2n-r) \times 2n}$$

に対して $\bar{S}' \Lambda x'_k = e_k$ なる x'_k から C'_k を定める。このとき $\{C'_k\}_{k=1}^r$ は次の性質を満たす。

$$[C'_k, \bar{X}'_i] = [C'_k, \bar{Z}'_i] = 0, \quad \forall i, k \quad (4.6)$$

$$\{C'_k, S'_k\} = 0, \quad \forall k \quad (4.7)$$

$$[C'_k, S'_i] = 0, \quad \forall i \neq k \quad (4.8)$$

また、 $\Phi' := \Phi'_r \circ \dots \circ \Phi'_1$ についても同様に定める。

$$\Phi'_k(\rho) = A'_{+,k} \rho A'_{+,k}^\dagger + A'_{-,k} \rho A'_{-,k}^\dagger, \quad k = 1, \dots, r \quad (4.9)$$

$$A'_{+,k} = \frac{1}{2}(I + S'_k), \quad A'_{-,k} = \frac{1}{2}C'_k(I - S'_k) \quad (4.10)$$

これを用いて連続時間散逸デコーダ (Continuous-time Dissipative Decoder, CDD) を次のように構成する。

$$\mathcal{L}'(\rho) = \Phi'(\rho) - \rho \quad (4.11)$$

定理 1

式 (4.11) で表される CDD によって系を時間発展させると、系は符号空間 \mathcal{C}_D 上に収束し、また \mathcal{C}_D 上の状態を不変に保つ。

証明。 まず、不変性について示す。 \mathcal{C}_D 上の任意の状態は論理演算子の線形結合で表されるため、CDD が論理演算子を不変に保つことを示せば十分である。これは式 (4.4), (4.6) より論理演算子が S'_k, C'_k と可換であることと、 $PP^\dagger = I, \forall P \in \mathcal{P}_n$ が成り立つことから直ちにわかる。

次に収束性について示す。CDD が何らかの集合に漸近的に収束することは示されている [10, Prop. 43] ので、それが符号空間 \mathcal{C}_D 上であることを示せば十分である。 Φ' は次のように変形できる。

$$\begin{aligned} \Phi'(\rho) &= \Phi'_r \circ \dots \circ \Phi'_1(\rho) \\ &= \sum_{s_1, \dots, s_r \in \{+, -\}} A'_{s_r, r} \cdots A'_{s_1, 1} \rho A'_{s_1, 1}^\dagger \cdots A'_{s_r, r}^\dagger \end{aligned}$$

ここで、式 (4.7) より

$$A'_{-,k} = \frac{1}{2}C'_k(I - S'_k) = \frac{1}{2}(I + S'_k)C'_k$$

とできる。これと式 (4.8), および $(I + S'_k)/2$ が S'_k の固有値 +1 の固有空間への射影演算子になっていることに注意すると、 $A'_{s_r, r} \cdots A'_{s_1, 1}$ は任意の $s_1, \dots, s_r \in \{+, -\}$ について $\Pi_{\mathcal{C}_D} \bar{C}$ と表せる。ここに $\Pi_{\mathcal{C}_D}$ はスタビライザ空間への射影演算子で、 \bar{C} は訂正行列 $\{C'_k\}_{k=1}^r$ の適当な結合である。したがって、CDD の収束先は符号空間 \mathcal{C}_D 上に存在する。 \square

定理 1 より、復号元の空間 \mathcal{C}_E の状態から CDD にしたがって時間発展させると復号先の空間 \mathcal{C}_D 上の何れかの点に収束することがわかった。次に、その収束先が元の符号語と対応する適切な符号語になっていることを示す。

定理 2

任意の $\bar{\rho} \in \mathcal{C}_E$ に対して

$$\begin{aligned} & \text{Tr} \left(\bar{X}'_1{}^{p_1} \bar{Z}'_1{}^{q_1} \dots \bar{X}'_{n-r}{}^{p_{n-r}} \bar{Z}'_{n-r}{}^{q_{n-r}} \lim_{t \rightarrow +\infty} e^{\mathcal{L}'t} [\bar{\rho}] \right) \\ &= \text{Tr} \left(\bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}} \bar{\rho} \right) \end{aligned} \quad (4.12)$$

が全ての $p_i, q_i \in \{0, 1\}$ の組み合わせについて成り立つ。

証明.

$$\begin{aligned} & \text{Tr} \left(\bar{X}'_1{}^{p_1} \bar{Z}'_1{}^{q_1} \dots \bar{X}'_{n-r}{}^{p_{n-r}} \bar{Z}'_{n-r}{}^{q_{n-r}} \lim_{t \rightarrow +\infty} e^{\mathcal{L}'t} [\bar{\rho}] \right) \\ &= \text{Tr} \left(\lim_{t \rightarrow +\infty} e^{\mathcal{L}'t} \left[\bar{X}'_1{}^{p_1} \bar{Z}'_1{}^{q_1} \dots \bar{X}'_{n-r}{}^{p_{n-r}} \bar{Z}'_{n-r}{}^{q_{n-r}} \right] \bar{\rho} \right) \\ &= \text{Tr} \left(\bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}} \bar{\rho} \right) \\ &= \text{Tr} \left(\bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}} \bar{\rho} \right) \end{aligned}$$

二行目への変形は Schrödinger 表示から Heisenberg 表示への切り替え、三行目への変形は論理演算子が CDD によって不変であること、最後の変形は式 (4.5) を用いた。

式 (2.2) の一般化により、論理 qubits に作用する任意の行列は論理演算子のテンソル積の線形結合によって表すことができることと、式 (2.1) に注意すると、定理 2 より、CDD は \mathcal{C}_E 上の符号語を対応する \mathcal{C}_D 上の適切な符号語に移していることが確かめられる。最後に CDD によりスタビライザ符号が復号されていることを示す。

定理 3

任意の $|i_1 i_2 \dots i_r\rangle_L \in \mathcal{C}_D$ に対して

$$|i_1 i_2 \dots i_r\rangle_L = |i_1 i_2 \dots i_r\rangle \otimes |\psi_i\rangle$$

が成り立つ。

証明. 式 (4.3) より、 \mathcal{C}_D 上の任意の符号語の後ろ r -qubits は

$$|\psi\rangle := (|+\rangle)^{\otimes r-k} \otimes (|0\rangle)^{\otimes k}$$

と一意に定まる。このとき式 (4.2) から \bar{Z}'_k は

$$\bar{Z}' : \overbrace{I \dots I}^{n-r} \overbrace{Z I \dots I}^{r-k} \overbrace{I (I \text{ or } Z) \dots (I \text{ or } Z)}^k$$

となっているので、後ろ r -qubits に注目すると

$$\overbrace{I \dots I}^{r-k} \overbrace{I (I \text{ or } Z) \dots (I \text{ or } Z)}^k |\psi\rangle = |\psi\rangle$$

が成り立つ。ただし、 \otimes を省略した。さらに、前 $(n-r)$ -qubits に注目すると \bar{Z}'_k は Z_k に一致し、生成子 S'_k は単位行列 I に一致するから、

$$\begin{aligned} \bar{Z}'_k &= Z_k \otimes \tilde{Z}_k \\ S'_k &= I \otimes \tilde{S}_k \end{aligned}$$

とかける。

スタビライザ符号の定義より $|i_1 i_2 \dots i_r\rangle_L$ は $\langle S'_1, \dots, S'_r, (-1)^{i_1} \bar{Z}'_1, (-1)^{i_2} \bar{Z}'_2, \dots, (-1)^{i_{n-r}} \bar{Z}'_{n-r} \rangle$ によってスタビライズされる状態である。まず、生成子 $\{S'_k\}_{k=1}^r$ にスタビライズされることから、 $|i_1 i_2 \dots i_r\rangle_L = |\phi_i\rangle \otimes |\psi\rangle$ とかける。次に

$$\begin{aligned} (-1)^{i_k} \bar{Z}'_k |i_1 i_2 \dots i_r\rangle_L &= (-1)^{i_k} (Z_k |\phi_i\rangle) \otimes (\tilde{Z}_k |\psi\rangle) \\ &= (-1)^{i_k} (Z_k |\phi_i\rangle) \otimes |\psi\rangle \\ &= ((-1)^{i_k} Z_k |\phi_i\rangle) \otimes |\psi\rangle \end{aligned}$$

と、 $(-1)^{i_k} \bar{Z}'_k$ によってスタビライズされることから

$$(-1)^{i_k} Z_k |\phi_i\rangle = |\phi_i\rangle, \quad k = 1, \dots, n-r$$

が成り立つ。このような $|\phi_i\rangle$ は $|i_1 i_2 \dots i_r\rangle$ に限られる。□

さらに、CDE と CDD はともに変換の前後で状態の純粋度を変化させないことが確認できている。証明手順は同様であるため、ここでは CDD についてのみ示す。

定理 4

$\lim_{t \rightarrow +\infty} e^{\mathcal{L}'t} [\bar{\rho}] = \bar{\rho}' \in \mathcal{C}_D$ とする。

$$\text{Tr}(\bar{\rho}'^2) = \text{Tr}(\bar{\rho}'^2)$$

が成り立つ。

証明. \mathcal{C}_D 上の任意の状態は論理演算子の線形結合で表せるから、

$$\bar{\rho}' = \sum_{p,q} c'_{p,q} \bar{X}'_1{}^{p_1} \bar{Z}'_1{}^{q_1} \dots \bar{X}'_{n-r}{}^{p_{n-r}} \bar{Z}'_{n-r}{}^{q_{n-r}}$$

なる複素係数 $\{c'_{p,q}\}_{p,q}$ が取れる。このときトレースの線形性と $\bar{X}'_k = \bar{X}_k, \bar{Z}'_k = \bar{Z}_k$ 、および定理 2 から次式が成り立つ。

$$\begin{aligned} \text{Tr}(\bar{\rho}'^2) &= \text{Tr} \left(\sum_{p,q} c'_{p,q} \bar{X}'_1{}^{p_1} \bar{Z}'_1{}^{q_1} \dots \bar{X}'_{n-r}{}^{p_{n-r}} \bar{Z}'_{n-r}{}^{q_{n-r}} \bar{\rho}' \right) \\ &= \sum_{p,q} c'_{p,q} \text{Tr} \left(\bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}} \bar{\rho}' \right) \\ &= \sum_{p,q} c'_{p,q} \text{Tr} \left(\bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}} \bar{\rho} \right) \\ &= \text{Tr} \left(\sum_{p,q} c'_{p,q} \bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}} \bar{\rho} \right) \\ &= \text{Tr}(\bar{\rho}' \bar{\rho}) \\ &= \text{Tr}(\bar{\rho} \bar{\rho}') \end{aligned}$$

再び論理演算子による分解から

$$\bar{\rho} = \sum_{p,q} c_{p,q} \bar{X}_1{}^{p_1} \bar{Z}_1{}^{q_1} \dots \bar{X}_{n-r}{}^{p_{n-r}} \bar{Z}_{n-r}{}^{q_{n-r}}$$

なる複素係数 $\{c_{p,q}\}_{p,q}$ が取れて,

$$\begin{aligned} \text{Tr}(\bar{\rho} \bar{\rho}') &= \text{Tr} \left(\sum_{p,q} c_{p,q} \bar{X}_1^{p_1} \bar{Z}_1^{q_1} \dots \bar{X}_{n-r}^{p_{n-r}} \bar{Z}_{n-r}^{q_{n-r}} \bar{\rho}' \right) \\ &= \sum_{p,q} c_{p,q} \text{Tr} \left(\bar{X}_1^{p_1} \bar{Z}_1^{q_1} \dots \bar{X}_{n-r}^{p_{n-r}} \bar{Z}_{n-r}^{q_{n-r}} \bar{\rho}' \right) \\ &= \sum_{p,q} c_{p,q} \text{Tr} \left(\bar{X}_1^{p_1} \bar{Z}_1^{q_1} \dots \bar{X}_{n-r}^{p_{n-r}} \bar{Z}_{n-r}^{q_{n-r}} \bar{\rho} \right) \\ &= \text{Tr}(\bar{\rho}^2) \end{aligned}$$

が成り立つ. \square

全く同様の手順により, CDE による変換の前後においても状態の純粋度は変化しないことが証明できる. これにより CDE による符号化や CDD による復号化を行っても, 元の状態の純粋度は変化しないことがわかる.

5 数値実験

5.1 実験設定

適当に取った初期状態に対して, CDE を用いて \mathcal{C}_E 上に符号化し, その後 CDD を用いて \mathcal{C}_D 上へ復号する数値実験を行った. 1-qubit の情報の符号化を考える. まず, 符号化先の \mathcal{C}_E は $\langle Z_1 Z_2, Z_1 Z_3 \rangle$ で生成されるスタビライザ符号とする. 第 3.2 節に従って訂正行列を取ると, $C_1 = X_2, C_2 = X_3$ となる. なお, \mathcal{C}_E は反復符号と呼ばれるもので, 論理基底は $|0\rangle_L = |000\rangle, |1\rangle_L = |111\rangle$ となっている. 次に, 第 4 章の手順に従って復号先の \mathcal{C}_D を構成すると, \mathcal{C}_D は $\langle X_2, X_3 \rangle$ で生成されるスタビライザ符号であり, その訂正行列は $C_1 = Z_1 Z_2, C_2 = Z_1 Z_3$ となる.

次に示す三つの初期状態に対して数値実験を行った.

- Case 1: 純粋状態

$$\rho = |0\rangle\langle 0|$$

- Case 2: 混合状態

$$\rho = \frac{1}{4} |0\rangle\langle 0| + \frac{3}{4} |1\rangle\langle 1|$$

- Case 3: 重ね合わせ状態の混合状態

$$\begin{aligned} \rho &= \frac{2}{3} |\phi_1\rangle\langle \phi_1| + \frac{1}{3} |\phi_2\rangle\langle \phi_2|, \\ |\phi_1\rangle &= \frac{1}{2} |0\rangle + \frac{\sqrt{3}}{2} |1\rangle, \\ |\phi_2\rangle &= \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \end{aligned}$$

各初期状態ごとに CDE と CDD をそれぞれ 10,000 ステップずつ実行した. その際, 各ステップの時間幅は $dt = 0.001$ とした.

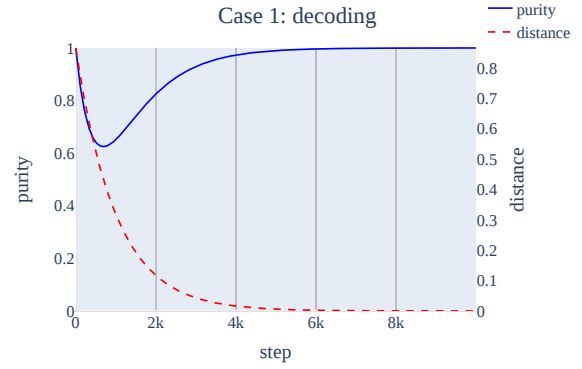
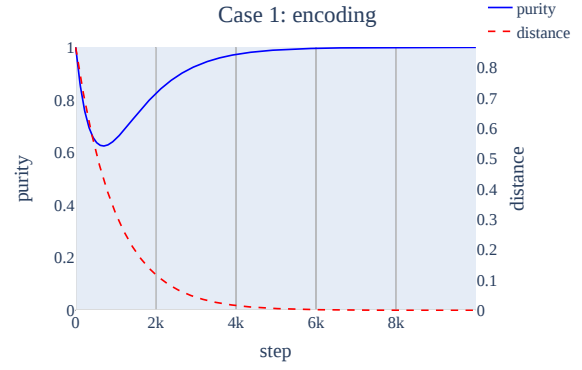


Fig. 1: Case 1 での符号化 (上) と復号化 (下) における純粋度の変化および目標状態との距離の変化

5.2 結果と考察

横軸に時間ステップ, 左縦軸に純粋度, 右縦軸に目標状態との距離を取り, 各初期状態から始めたときの符号化と復号化の様子を Fig. 1-3 にプロットした. ここに目標状態 ρ^* との距離は $\|\rho - \rho^*\|_2 = \sigma_{\max}(\rho - \rho^*)$ で与えられる. また, 初期状態と復号後の最終状態についても距離を計算した. その結果を Table 1 に示す.

Table 1: 初期状態と復号後の最終状態との距離

初期状態	初期状態と最終状態との距離
Case 1	4.120×10^{-5}
Case 2	2.900×10^{-5}
Case 3	3.860×10^{-5}

全ての場合において, 純粋度 (purity) は始め減少した後ある時刻から増加し, 最終的に変換前の純粋度に収束していることがわかる. また, 目標状態との距離はいずれの場合においても短調に減少していることが確認できる. さらに Table 1 から初期状態と復号後の最終状態の差は十分小さく, 数値誤差を除いて元の状態を正しく復号できていることがわかる.

6 おわりに

6.1 本研究のまとめ

本論文では, まず第 3 章で, 先行研究によるスタビライザ符号への符号化方法をまとめ, 続く第 4 章にて, それに対する散逸ダイナミクスを用いた復号化手法を

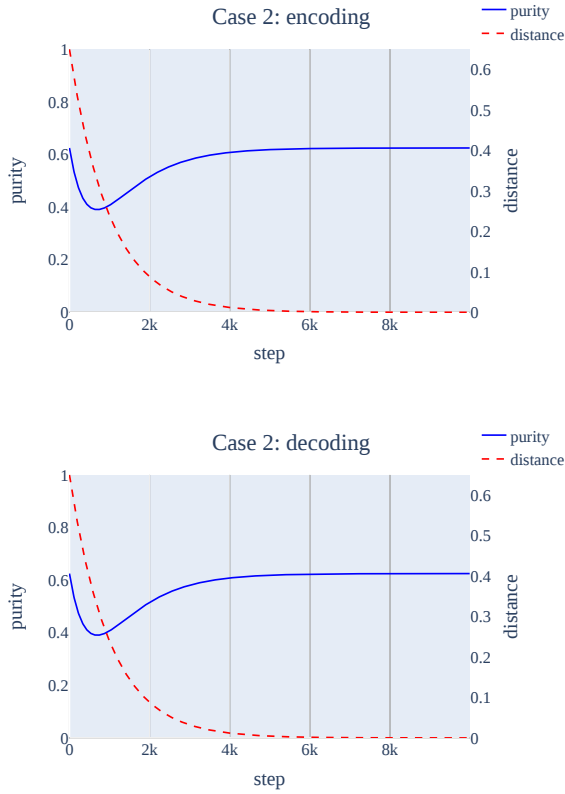


Fig. 2: Case 2での符号化 (上) と復号化 (下) における純粋度の変化および目標状態との距離の変化

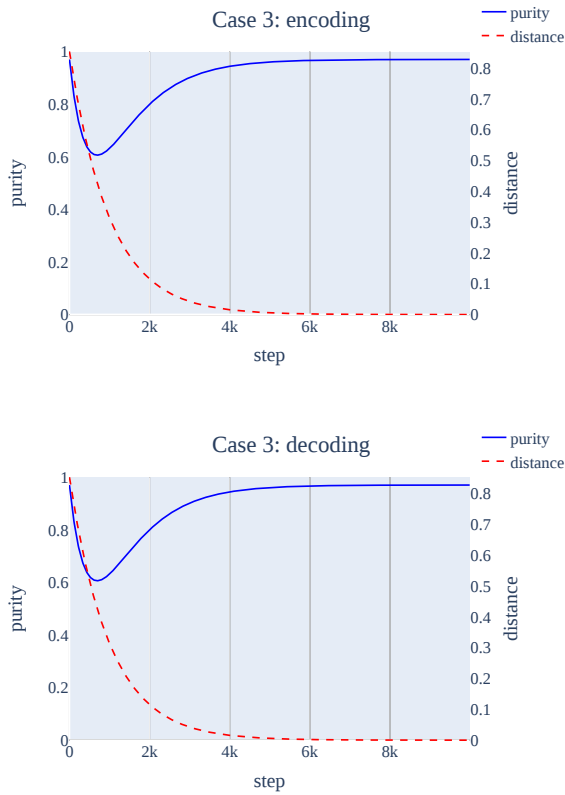


Fig. 3: Case 3での符号化 (上) と復号化 (下) における純粋度の変化および目標状態との距離の変化

提案した. 証明においては, 始めに CDD の平衡点の集合が復号先の符号空間 \mathcal{C}_D 上にあることを示し, 次に, もとの符号空間 \mathcal{C}_E 上の符号語を CDD に従って時間発展させると, 対応する \mathcal{C}_D 上の符号語へ適切に写されることを示した. そして, \mathcal{C}_D 上では先頭 $n-r$ 個の実 qubits に情報が格納されていることを示し, これによって復号が行われていることを確認した. さらに, 散逸ダイナミクスを用いた CDE や CDD による時間発展においては, 系の純粋度が変化しないことを示した.

これを元に第 5 章では, 適当にとった初期状態を先行研究の手法で符号化し, さらにそれを提案手法により復号化する数値実験を行った. 初期状態として純粋状態と混合状態のいずれを取った場合においても, 最終的には初期状態に十分近い状態へ復号されることが確認できた. また, 変換の前後において純粋度が変化していないことも確認できた.

6.2 今後の課題

本研究では, 復号の過程において雑音が入らない理想的な条件下での復号方法を考えた. 一方, 実問題においては計算過程だけでなく複合過程においても雑音が入ることが考えられる. 計算過程においては, 情報が符号空間上に存在するので雑音由来の誤りを訂正することができるが, 復号過程においては符号空間から外れるので, そのままの手法では誤りを訂正できない. そのため, 理論をさらに発展させ, 雑音が入る場合でも正確に復号が行えるような手法を考える必要がある.

また, 実際の量子コンピュータではコヒーレンス時間といって, 量子的な重ね合わせ状態を維持できる時間が決まっている. コヒーレンス時間を過ぎると, 重ね合わせが解けて古典的な情報へと落ちてしまう, デコヒーレンス [11] という現象が確認されている. コヒーレンス時間は量子コンピュータの物理的な実現方法に強く依存するが, 長くても 10^{-6} s ほどであることが知られている [12]. 本研究で提案した手法は目標状態へ漸近的に収束することを保証しているが, デコヒーレンスの影響を考慮すると, 一連の復号過程をコヒーレンス時間内に終える必要がある. そのため, 復号手続きを高速に行えるように手法の改善を行うことが, 今後の課題として挙げられる.

A 補足の証明

補題 1

CDE(3.2) や CDD(4.11) は GKS-Lindblad 方程式の形式を満たす.

証明. 証明手順は同様なので CDE についてのみ示す.

$$\begin{aligned} \Phi(\rho) &= \Phi_r \circ \dots \circ \Phi_1(\rho) \\ &= \sum_{s_1, \dots, s_r \in \{+, -\}} A_{s_r, r} \dots A_{s_1, 1} \rho A_{s_1, 1}^\dagger \dots A_{s_r, r}^\dagger \end{aligned}$$

より,

$$L_k = A_{s_r, r} \dots A_{s_1, 1}$$

$k = (s_1, \dots, s_r), \forall s_i \in \{+, -\}$ とすると

$$\Phi(\rho) = \sum_k L_k \rho L_k^\dagger$$

とかける。このとき、 $\sum_k L_k^\dagger L_k = I$ となることを帰納法により示す。

$$A_{+,k} = \frac{1}{2}(I + S_k), \quad A_{-,k} = \frac{1}{2}C_k(I - S_k)$$

より、

$$\begin{aligned} A_{+,k}^\dagger A_{+,k} &= \frac{1}{2}(I + S_k), & A_{-,k}^\dagger A_{-,k} &= \frac{1}{2}(I - S_k), \\ A_{+,k}^\dagger A_{+,k} + A_{-,k}^\dagger A_{-,k} &= I, \\ A_{+,k}^\dagger A_{-,k} &= A_{-,k}^\dagger A_{+,k} = 0 \end{aligned}$$

が成り立つことに注意して証明を行う。

• $r = 1$ のとき

$$\begin{aligned} \sum_k L_k^\dagger L_k &= A_{+,1}^\dagger A_{+,1} + A_{-,1}^\dagger A_{-,1} \\ &= I \end{aligned}$$

より成り立つ。

• $r + 1$ のとき

$$\begin{aligned} &\sum_{k(r+1)} L_k^\dagger L_k \\ &= \sum_{k(r)} \{(A_{+,r+1} + A_{-,r+1}) L_k\}^\dagger \{(A_{+,r+1} + A_{-,r+1}) L_k\} \\ &= \sum_{k(r)} L_k^\dagger \left(A_{+,r+1}^\dagger A_{+,r+1} + A_{-,r+1}^\dagger A_{-,r+1} \right) L_k \\ &= \sum_{k(r)} L_k^\dagger L_k \end{aligned}$$

となるので、帰納法の仮定より成り立つ。

さて、 $\sum_k L_k^\dagger L_k = I$ に注意すれば、CDE は

$$\begin{aligned} \mathcal{L}(\rho) &= \Phi(\rho) - \rho \\ &= \sum_k L_k \rho L_k^\dagger - \frac{1}{2} \sum_k L_k^\dagger L_k \rho - \frac{1}{2} \rho \sum_k L_k^\dagger L_k \end{aligned}$$

とかけるので、これは式 (3.1) で $H = 0$ とした場合に一致する。□

References

- [1] P. W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.
- [2] L. M. Vandersypen et al. “Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance”. In: *Nature* 414.6866 (2001), pp. 883–887.
- [3] D. Gottesman. “Stabilizer codes and quantum error correction”. In: *quant-ph/9705052, Caltech Ph.D. thesis* (1997).
- [4] M. A. Nielsen and I. Chuang. “Quantum Computation and Quantum Information.” American Association of Physics Teachers, 2002.
- [5] F. Ticozzi, G. Baggio, and L. Viola. “Quantum Information Encoding from Stabilizing Dynamics”. In: *2019 IEEE 58th Conference on Decision and Control (CDC)*. 2019, pp. 413–418.
- [6] G. Nannicini. “An Introduction to Quantum Computing, without the Physics”. In: *SIAM Review* 62.4 (2020), pp. 936–981.
- [7] 沙川貴大 and 上田正仁. “量子測定と量子制御 (数理科学 SGC ライブラリ 123).” サイエンス社, 2016.
- [8] E. H. Knill. “Protected realizations of quantum information”. In: *Phys. Rev. A* 74 (4 Oct. 2006), p. 042301.
- [9] R. Alicki and K. Lendi. “Quantum Dynamical Semigroups and Applications.” Vol. 717. Springer, 2007.
- [10] P. D. Johnson, F. Ticozzi, and L. Viola. “Exact stabilization of entangled states in finite time by dissipative quantum circuits”. In: *Phys. Rev. A* 96 (1 July 2017), p. 012308.
- [11] M. Schlosshauer. “Quantum decoherence”. In: *Physics Reports* 831 (2019). Quantum decoherence, pp. 1–57. ISSN: 0370-1573.
- [12] V. Salari et al. “Quantum decoherence time scales for ionic superposition states in ion channels”. In: *Phys. Rev. E* 91 (3 Mar. 2015), p. 032704.