数理解析研究所講究録
第1752巻 2011年 7-21

誤り訂正符号を用いた量子力学的性質の保護 -量子誤り訂正符号入門-

萩原学*

1 はじめに

本稿は量子誤り訂正符号の基礎事項を綴ったものである。内容は、京都大学数理解析研究所の共同事業として開催された「諸分野との協働による数理科学のフロンティア（研究代表者：坂上貴之氏）」の講演「誤り訂正符号を用いた量子力学的性質の保護」を基にしている。本稿では、数学の立場として量子誤り訂正符号理論を学ぶ為に必要な基礎事項をまとめている。これは共同事業のテーマを意識した為である。

2 量子誤り訂正符号理論とは

量子誤り訂正符号理論とは、量子力学の視点から誤り訂正符号理論を一般化した理論体系を指す。本稿を読み進めるには量子力学の知識も誤り訂正符号理論の知識も必要ない。もし、誤り訂正符号理論を知っていれば量子誤り訂正符号理論の理解が進みやすいであろう。誤り訂正符号理論は１９９０年以降に飛躍的な進化を遂げた分野である。興味を持たれた読者は文献 [1] や文献 [2] を参考にすると良い。特に、後者は大学２年生以上を対象に書かれており、予備知識が殆どなくとも読み進められる。量子誤り訂正符号と誤り訂正符号を区別するために、誤り訂正符号を古典誤り訂正符号と呼ぶ慣習がある。本稿でもその慣習に従うことにする。

古典誤り訂正符号とはデータの損失や読み取りミスを機械的に補正する為の技術である。そして古典誤り訂正符号理論とは、そのような技術の為の理論体系である。古典誤り訂正符号の研究は、純粋理論として発展しているのみならず、実装も進んでいる。一般家庭における家電において古典誤り訂正

*独立行政法人産業技術総合研究所: e-mail: hagiwara.hagiwara@aist.go.jp, University of Hawaii, 中央大学研究開発機構, ブログ: http://manau.jp/blog/sub/ 研究ホームページ: http://staff.aist.go.jp/hagiwara.hagiwara/,

符号の技術が導入された最初の対象はCD（コンパクトディスク）に関するものであろう。特に、CDのデータ形式と読み取り時の処理であろう。CDには小さい面積に多くのデータが書きこまれる。そして、CDや読み取り機器についた傷やホコリなどが原因となりデータの損失や読み取りミスが生じる恐れがある。それにも関わらず美しい音楽が再生されるのは古典誤り訂正符号技術により自動的にデータが復元される賜と言える。他にも例を挙げれば、無線LAN、無線MAN、有線LAN、衛星放送、携帯電話などの通信機器およびハードディスク、フラッシュメモリ、DVD、Blu-ray Discなどの記録機器に古典誤り訂正符号の技術が組み込まれている。物理装置の精度を向上させて誤りの発生を防ぐよりも、符号理論に基づく処理によって誤りを訂正するほうが便利と考えられている。

他方、量子誤り訂正符号の実装は、原稿執筆時点において、実用的と言えるまで発展していない。それどころか、量子誤り訂正符号が一般家庭で用いられるには数十年、数百年以上かかると考える研究者もいる。これは（後述する）量子情報や量子回路の実装が困難であることに起因する。では、量子誤り訂正符号の研究は無意味なのだろうか。このことについては歴史を振り返ると良い。現在、日常生活において不可欠となった古典符号の技術でさえも、CDが登場するまでは同様の意見が持たれていた。量子誤り訂正符号が実用的と考えられる日は突然やってくるかも知れない。

量子誤り訂正符号の定義を把握するために、量子通信路モデルを導入する。通信路モデルは、古典符号理論においても大変重要な概念とされている。

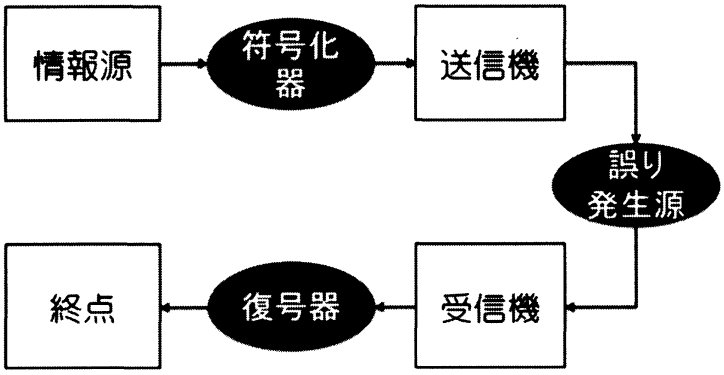

図 1: 通信路モデル

上の図を見ながら、下記で述べる例により「情報源」「符号化器」などの用語を直感的に感じ取って頂きたい。

友人と待ち合わせをしていると仮定する。約束の１２：１５になってもその友人が現れない。既に１０分が経過している。周りを見渡すと、自分から３０mほど離れたところに友人を発見した。どうやら、待ち合わせ場所の目

印を勘違いしたようだ。そこで自分が移動するのではなく、声をかけることにした。

- 「自分がここにいる」ことを伝えたい。(情報源)
- やや距離があるため「(大きな声で) おーい、おーい、おれはこっちだよーん」と呼ぶことにする。(符号化器)
- はじらいながらも大きな声で「おーい、おーい、おれはこっちだよーん」と声高らかに叫ぶ。(送信機)
- １２：３０を告げるチャイムが「ゴーン」と響く。(誤り発生)
- 友人の耳に「おーい、おーい、おれはこっちだゴーン」と伝わる (受信機)
- 友人は「何者かが自分の居場所を伝えている」のだろうと推測する (復号器)
- 「自分がここにいる」という情報が伝わり、友人が振り向いた。(終点)

ここでは「誤り」の意味を「声が別の音に変換される」という意味で用いた。誤りとは日常生活においてごく自然に発生するものだと意識すると良い。

符号理論では、伝えたい情報や読み取りたい情報があるテイで話を進める。そして、「誤りが発生すると考えられる (誤り発生源)」という状況に対して、「誤りが発生しても推測できるように情報を変換する (符号化器)」かつ「誤った情報から、即座に元来の情報を推測する (復号器)」という二つの操作がどれだけ効率よく精度良く行えるかを研究する。量子誤り訂正符号では伝えたい情報が複素数として表される。さらに、符号化や復号などの処理に対して量子力学に基づく制約が付けられる。

次節では量子誤り訂正符号の数学的な記述を述べていく。つまり、量子誤り訂正符号における「符号化器」「誤り発生源」「復号器」とはどのように記述されるかを述べていく。

3　量子誤り訂正符号の定義

k を正整数、$\mathbb{C}$ を複素数体とする。$\mathbb{C}^{2\otimes k}$ を

$$\mathbb{C}^{2\otimes k} := \overbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{k}$$

と定義する。このとき $\mathbb{C}^{2\otimes k}$ は 2^k 次元の複素ベクトル空間である。ただし $\otimes$ はテンソル積を表し、$\mathbb{C}^2$ は行ベクトルからなる 2 次元複素ベクトル空間とする。

量子情報 $|m\rangle$ とは $\mathbb{C}^{2\otimes k}$ の元であって長さが 1 であるものを表す。ただし、長さは $\mathbb{C}^{2\otimes k}$ に対するエルミート内積 $\langle , \rangle$ によって

$$\sqrt{\langle\, |m\rangle, |m\rangle\, \rangle}$$

と定義される。[1]

先の通信路モデル図 1 と照らし合わせると、情報源から $\mathbb{C}^{2\otimes k}$ に含まれる量子情報が発生する。整数 k を明記したい時には k 量子ビット q の持つ量子情報と言う。

以下、k 量子ビットのもつ量子情報を n 量子ビットのもつ量子情報へ符号化しよう。ただし n は正整数であり $n \geq k$ とする。符号化写像 f（もしくは符号化器）は二つの写像 $\mathrm{pad}^{k,n} : \mathbb{C}^{2\otimes k} \to \mathbb{C}^{2\otimes n}$ と $\mathrm{enc} : \mathbb{C}^{2\otimes n} \to \mathbb{C}^{2\otimes n}$ の合成写像 $\mathrm{enc} \circ \mathrm{pad} : \mathbb{C}^{2\otimes k} \to \mathbb{C}^{2\otimes n}$ として表される。ここまでの用語と異なり、f を符号化写像と呼んで符号化器と呼ばなかった理由を一言述べよう。前者では数学的な概念を想定し、後者では実装された機器を想定する。であるからモデル上では符号化器と書くが、この文脈では符号化写像と呼ぶ。ここから、これら $\mathrm{pad}^{k,n}, \mathrm{enc}$ の定義を述べる。

k, n を正整数とし、大小関係 $k < n$ にあるとする。そして、$|m\rangle$ を k 量子ビット q の持つ量子情報とする。写像 $\mathrm{pad}^{k,n} : \mathbb{C}^{2\otimes k} \to \mathbb{C}^{2\otimes n}$ を

$$\mathrm{pad}^{k,n}(|m\rangle) := |m\rangle \otimes \overbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}^{n-k}$$

と定義する。ただし $|0\rangle := (1,0)^T \in \mathbb{C}^2$ とし、T は転置記号を表す。続いて写像 enc を $\mathbb{C}^{2\otimes n}$ に作用するユニタリ変換として定義しよう。符号化写像により量子情報の所属する次元が 2^k から 2^n へ変化した。それにあわせて量子ビットの記号 q を q' としておく。つまり n 量子ビット q' の量子情報 $\mathrm{enc} \circ \mathrm{pad}^{k,n}(|m\rangle)$ と表す。符号化後の量子ビット数 n を符号長と呼ぶ。

ここで記号 $|1\rangle$ および $|c_1 c_2 \ldots c_n\rangle$ を導入しておこう。ただし $c_1, c_2, \ldots, c_n \in \{0,1\}$ とする。この記号を以下で定義する。

$$|1\rangle := (0,1)^T$$

$$|c_1 c_2 \ldots c_n\rangle := |c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle$$

符号化写像の像 $Q := \mathrm{Im}\,\mathrm{enc} \circ \mathrm{pad}^{k,n}$ を量子誤り訂正符号空間と呼ぶ。符号化写像 $\mathrm{enc} \circ \mathrm{pad}^{k,n}$ は元来の量子情報の空間 $\mathbb{Q}^{2\otimes k}$ と量子誤り訂正符号空間 Q の間に一対一対応を与える。

計算理論、情報理論、符号理論などの分野では、0 と 1 からなる系列の構成要素である「0」と「1」をビットと呼ぶ。上の記法 $|c_1 c_2 \ldots c_n\rangle$ は量子情報とビットを関連付ける。量子情報に対して「量子ビット」と冠をつける気持ちが伝わっただろうか。

[1] 量子情報 $|m\rangle, |m'\rangle$ の内積 $\langle |m\rangle, |m'\rangle \rangle$ の表記として、一般的には $\langle m|m'\rangle$ を用いる。

量子誤りとはユニタリ変換を表す。ここまでの流れを組むと、発生した量子誤りによって影響を受ける量子情報は n 量子ビットの持つ量子情報である。であるから、量子誤りを表すユニタリ変換として $\mathbb{C}^{2\otimes n}$ に作用するユニタリ変換を想定しよう。どのような量子誤りを想定するかは、量子通信の実験結果と照らし合わせるほうが、現実的な意味を感じられて面白い。ところが、実験はなかなか難しいと聞いている。そこで、量子誤り訂正符号の理論では量子誤りのうち「古典誤りの拡張と捉えられるもの」や「理論的に扱いやすいもの」を研究する傾向がある。詳しくは次節以降で述べる。

復号器 dec は次のアルゴリズムとして定義される。まず $\bigoplus_{s\in\{0,1\}^{n-k}} V_s$ を $\mathbb{C}^{2\otimes n}$ の直交直和であり各複素ベクトル空間 V_s の次元を 2^k とする。そして $\mathrm{rec} : \{0,1\}^{n-k} \to U_{2^n}(\mathbb{C})$ を写像とし、特に $\mathrm{rec}(s)$ に対する V_s への定義域の制限 $\mathrm{rec}(s)_{V_s}$ が

$$\mathrm{rec}(s)_{V_s} : V_s \to Q$$

を満たすとする。ただし Q は量子誤り訂正符号空間を表し、$U_{2^n}(\mathbb{C})$ は $\mathbb{C}^{2\otimes n}$ に作用するユニタリ変換全体を表す。

* 入力：n 量子ビット q' の持つ量子情報 $|y\rangle$

* 出力：k 量子ビット q の持つ量子情報 $|m'\rangle$

(1) n 量子ビット q' の量子情報 $|y\rangle$ に基づき $s \in \{0,1\}^{n-k}$ を得る。ただし s を得る確率は $|y\rangle$ を複素ベクトル空間 V_s に射影したベクトルの長さの２乗と等しい。

(2) n 量子ビット q' の量子情報にユニタリ変換 $\mathrm{rec}(s)$ を作用させる。[2]その結果を $|c'\rangle$ とする。

(3) n 量子ビット q' の量子情報 $|c'\rangle$ に符号化写像の逆写像を作用させる。その結果を $|m'\rangle$ とする。

(4) k 量子ビット q の量子状態 $|m'\rangle$ を出力する。

上記の復号器のステップ 1 には s を得る確率的操作が含まれる。これは量子力学における観測と呼ばれる物理現象に基づく事情がある。このステップの確率的操作を嫌う場合には、s によらず出力が一致する復号アルゴリズムを構築すれば良い。そうすれば入力に対して出力が一意に定まる。

量子誤り訂正符号では、元来の量子情報 $|m\rangle$ と復号器が出力した量子情報 $|m'\rangle$ がどれだけ近い量子状態にできるかを焦点として研究する。ここで近いというのは内積の絶対値 $|\langle m|m'\rangle|$ の期待値がどれだけ 1 に近づけるかを意味する。この期待値は忠実度もしくは復号成功確率と呼ばれる。また “1 − 忠実度” は復号失敗確率と呼ばれる。この評価基準は古典誤り訂正符号の評価基準とあ

[2]この量子情報だけ明記されていない理由は後ほど述べる。今は復号アルゴリズムの流れを把握することを優先しよう。

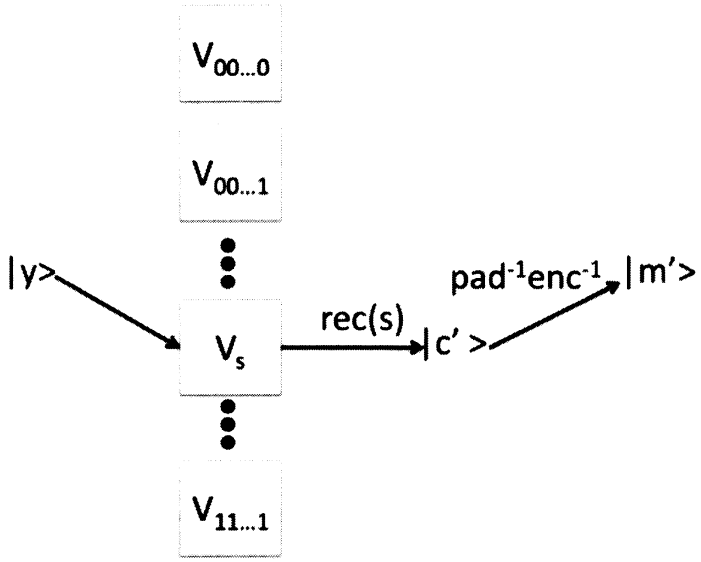

図 2: 復号器の過程

る意味で同じと言える。古典誤り訂正符号では元来のメッセージ $m \in \{0,1\}^k$ と復号器の出力の $m' \in \{0,1\}^k$ がどれだけ高い確率で一致するかを焦点として研究されてきた。この確率が先の期待値と同様の意味を持つ。

復号器のアルゴリズムのうち、最後の計算において「符号化写像の逆写像」ではなく「写像 enc の逆写像」とする研究もある。この場合、出力される量子状態は n 量子ビットの量子状態 $|c'\rangle$ となる。この時の量子誤り訂正符号の評価基準は $|\langle c|c'\rangle|$ の期待値となる。

いずれにせよ、元来の量子情報と復号器が出力する量子情報が一致する確率を挙げるためには、符号長 n を十分大きくすることが望まれる。というのも、符号長が小さな量子誤り訂正符号では 1 に十分近い復号成功確率は得られない。これは古典符号理論の一般論として知られた事実である。逆に符号の性能は n を大きくすればするほど、量子情報が一致する確率を高められると期待できる。ただしその際には別の問題が生じる。それは、計算量の小さい復号アルゴリズムの構成が困難なことにある。つまり量子誤り訂正符号の研究とは「(定義は曖昧であるが) 必要十分に大きな符号長を持ち」「計算量の小さな復号アルゴリズムが存在し」「復号成功確率が 1 に近い、つまり復号失敗確率が非常に小さい」という 3 つの条件を同時に達成できる符号を構成することと言える。これらの用語で「必要十分に長い」「小さな」「近い」[3] というのは数学的には曖昧である。この曖昧さを短所と考えずに、自由度が

[3] 古典符号でもこれらの用語は曖昧なまま用いられる。何故なら、実装環境に応じて「十分長い」とか「計算量の小さな」などの意味が変化する為である。例えば、１０年前の携帯電話と現在のスマートフォンでは計算処理の速さや記憶領域のサイズに差異がある。それぞれの機器で実現できる範囲で誤り訂正符号を設計する必要がある。かと言って、これらの機器を開発している人たちが「こんな条件の符号が欲しい」という情報を公開することは殆ど無い。そういう背景を踏まえ、機器を開発している人たちが思わず飛びついてしまうほど簡単で性能のよい「符号化写像」「復号器」の両方を同時に提案すると良い。

高いと前向きに考えるほうが楽しい研究ができる。

4 パウリ行列を用いて記述される量子誤り訂正符号とその関連事項

パウリ行列とは次で定義される4つのユニタリ行列を意味する。

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

ただし i は虚数単位を表す。

上の行列のうち X は古典誤り訂正符号における誤りの量子版と例えられることが多い。古典誤り訂正符号の誤りとして「ビット0がビット1へと誤る」「ビット1がビット0へと誤る」という二つの誤りを想定することがある。この古典誤りはビット反転誤りと呼ばれる。

パウリ行列 X はこれに似ている。1量子ビットをもつ量子情報 $|0\rangle$ および $|1\rangle$ に対して X を作用させれば

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$$

が従う。記号 $|\rangle$ 内に着目すれば、古典誤り訂正符号の誤りとの類似性を感じられる。

もう一つ例を述べる。次のユニタリ変換 $I \otimes X \otimes I \otimes I \otimes I$ を量子情報 $|c_1c_2c_3c_4c_5\rangle$ に作用させよう。二つ目のパウリ行列のみが X である。結果として

$$(I \otimes X \otimes I \otimes I \otimes I)|c_1c_2c_3c_4c_5\rangle = |c_1\bar{c}_2c_3c_4c_5\rangle$$

を得る。つまり左辺の c_2 が右辺では $\bar{c}_2$ に変わっている。ここで $\bar{c}_2$ はビット c_2 に対してビット誤りを施したビットを表す。これはビット列 $c_1c_2c_3c_4c_5$ のうち2番目のビット c_2 にのみビット反転が起こった状況と似ている。加えて、行列 I に対応する位置の c_i はビット反転しないことも注意しておこう。

$E_1, E_2, \ldots, E_n$ をパウリ行列とする。$E_{n_0} \neq I$ である添字 $1 \leq n_0 \leq n$ の総数を t としよう。ユニタリ行列 $E := E_1 \otimes E_2 \otimes \cdots \otimes E_n$ を量子誤りとみなしたとき、この誤りを t 重誤りと呼ぶ。

量子誤り訂正符号の研究で導入される量子通信路のうち代表的なものの1つが **depolarizing** 通信路である。この定義はパウリ行列の言葉で表される。定義を述べよう。上の誤りにおいて、E_{n_0} が I, X, Y, Z となる生起確率が独立であり、それぞれの値が $1-q, q/3, q/3, q/3$ である通信路を depolarizing 通

信路と呼ぶ。ちなみにこの表記のもと、depolarizing 通信路において上で定めた t 重誤り E の生起確率は $q^t(1-q)^{n-t}$ と表せる。depolarizing 通信路は量子誤り訂正符号で記述したい性質を表しやすい特徴を持つ。

パウリ行列は誤りを記述する以外にも、量子誤り訂正符号化写像の像や復号アルゴリズムに登場した直交直和を与えることにも利用される。ところで直交直和と相性の良い考え方の一つとして、線形変換に対する固有空間分解が知られる。パウリ行列と固有空間分解を結びつけよう。パウリ行列 X, Z, Y の固有値は $1, -1$ であり、I の固有値は 1 である。これは各パウリ行列に対して直接計算して確かめれば良い。その系としてパウリ行列をいくつかテンソル積でかけ合わせて作られる行列の固有値もまた $1, -1$ となる。もし n 個のパウリ行列をテンソル積で掛けあわせ、そのうちに X, Y, Z が一つでも含まれれば（つまり I 以外の行列がテンソル積で掛け合わされていれば）、固有値 $1, -1$ に対応する固有空間の次元は一定となり、2^{n-1} と等しい。

n 個のパウリ行列のテンソル積を m 個つくり、それぞれを $M_1, M_2, \ldots, M_m$ と表そう。これら M_{m_0} は全てユニタリ行列である。ただし $1 \leq m_0 \leq m$ とする。このユニタリ行列が全て "可換" であれば同時固有空間分解ができる。さらにこれらの固有空間は全て次元が等しいという特徴を持つ。[4]この時、集合 $\{M_1, M_2, \ldots, M_m\}$ をパリティ検査観測と呼ぶ。そしてこのように構成された符号空間をスタビライザ符号と呼ぶ [3]。

固有空間による直交直和分解を復号アルゴリズムでの分解とする。そして、全ての M_{m_0} に対して固有値 1 の固有空間を量子誤り訂正符号空間 Q とする。このように構成した量子誤り訂正符号の中には理論的に面白く振る舞うものがある。次節以降で述べていく。

スタビライザ符号を構成する際、スタビライザ符号以外の固有空間が 2^m 個得られたことに注目しよう。2^m 個の固有空間のうち、一つの固有空間 Q' を定よう。空間 Q' の任意の量子情報 $|y\rangle, |y'\rangle$ に対して各観測 M_{m_0} に対する固有値 t_{m_0} は一致する。つまり

$$M_{m_0}|y\rangle = t_{m_0}|y\rangle, \quad M_{m_0}|y'\rangle = t_{m_0}|y'\rangle,$$

が成立する。[5]この固有値 t_{m_0} は $1, -1$ のどちらかである。そこで $t_{m_0} = 1$ のときに $s_{m_0} := 0$ と定義し、$t_{m_0} = -1$ のときに $s_{m_0} := 1$ と定義して得られる 01 系列 $(s_1, s_2, \ldots, s_m)$ を固有空間 Q' のパリティ検査観測 $\{M_{m_0}\}_{1 \leq m_0 \leq m}$ に対するシンドロームと呼ぶ。スタビライザ符号とはシンドロームが $(0, 0, \ldots, 0)$ の固有空間として特徴付けられる。

定理 4.1. $\{M_{m_0}\}_{1 \leq m_0 \leq m}$ をパリティ検査観測、Q をスタビライザ符号とする。E をパウリ行列のテンソル積で与えられる量子誤りとする。

---

[4] X, Y, Z の固有値が $1, -1$ をそれぞれ 1 つづつ持つことに注目すれば、直接的な計算で確かめられる。

[5] これは同じ固有空間 Q' から元を選んでいるために従う。

この時、次の集合

$$EQ := \{E|c\rangle \mid |c\rangle \in Q\}$$

はパリティ検査観測 $\{M_{m_0}\}_{1\leq m_0\leq m}$ の固有空間である。

Proof. 行列 M_{m_0} および誤り E がパウリ行列で構成されていることに注目する。特に二つのパウリ行列 P_1, P_2 には

$$P_1P_2 = P_2P_1$$

もしくは

$$P_1P_2 = -P_2P_1$$

のどちらかが従う。この事実から、任意の M_{m_0} に対してある $t_{m_0} \in \{1, -1\}$ によって

$$M_{m_0}E = t_{m_0}EM_{m_0}$$

が従う。この事実を用いて EQ の元が固有ベクトルであることを示そう。EQ の定義から、任意の元 $|y\rangle \in EQ$ に対してある量子情報 $|c\rangle \in Q$ が存在して

$$|y\rangle = E|c\rangle$$

と表せる。この事実と、上で注意した t_{m_0} を用いれば

$$\begin{aligned} M_{m_0}|y\rangle &= M_{m_0}E|c\rangle \\ &= t_{m_0}EM_{m_0}|c\rangle \end{aligned}$$

と表せる。ところで $|c\rangle$ がスタビライザ符号 Q の元であることから M_{m_0} に対する固有値は 1 である。つまり $|M_{m_0}|c\rangle = |c\rangle$ が従う。よって右辺を変形して

$$\begin{aligned} M_{m_0}|y\rangle &= t_{m_0}E|c\rangle \\ &= t_{m_0}|y\rangle \end{aligned}$$

を得た。とくに量子情報 $|y\rangle \in EQ$ の選び方によらず同一の固有値 t_{m_0} を取る。つまり EQ は固有値 s_{m_0} を持つ固有空間 Q' に含まれる。他方、EQ は線形空間であり、その次元は Q の次元と等しい。また、パリティ検査観測の固有空間の次元は全て Q の次元と一致する。

まとめると $EQ \subset Q'$ かつ $\dim EQ = \dim Q'$ が従う。これは EQ と Q' が等しいことを意味する。 □

5　5量子ビット符号

パリティ検査観測の元 M_1, M_2, M_3, M_4 をそれぞれ

$$\begin{aligned} M_1 &:= Z \otimes X \otimes I \otimes X \otimes Z \\ M_2 &:= Z \otimes Z \otimes X \otimes I \otimes X \\ M_3 &:= X \otimes Z \otimes Z \otimes X \otimes I \\ M_4 &:= I \otimes X \otimes Z \otimes Z \otimes X \end{aligned}$$

と定義する。

このスタビライザ符号 Q の性質を考察しよう。このスタビライザ符号は5量子ビット符号と呼ばれる。

定理 5.1. Q を5量子ビット符号とする。五つのパウリ行列のテンソル積で表される1重量子誤り、および単位行列のみで表される量子誤り全体を $\mathcal{E}$ とする。

この時、どの $E \in \mathcal{E}$ に対する EQ のシンドロームも異なる。

Proof. 1つ1つ計算して確かめれば良い。その作業はそれほど大変ではない。定理4.1で見たとおり、誤り $E \in \mathcal{E}$ と M_{m_0} を交換したときの係数を調べるだけで良い。例えば誤り $X \circ I \circ I \circ I \circ I \in \mathcal{E}$ に対して、

$$\begin{aligned} M_1 E &= -E M_1 \\ M_2 E &= -E M_2 \\ M_3 E &= E M_3 \\ M_4 E &= E M_4 \end{aligned}$$

が従う。よって EQ のシンドロームは $(1,1,0,0)$ である。

残りは読者に計算していただきたい。 □

定理5.1で定義した $\mathcal{E}$ の濃度は16である。他方、パリティ検査観測が4つの行列で構成されることから、シンドロームの種類は $2^4 = 16$ である。全ての $\mathcal{E}$ に対して異なるシンドロームが得られることから、シンドロームの集合と $\mathcal{E}$ の間に一対一対応が得られた。この対応によって rec を定義する。$\mathcal{E}$ の元 E はすべて $E^2 = I$ という性質を有する。このことは、復号アルゴリズムの出力が元来の量子情報と一致することを意味する。実際、5量子ビット符号 Q の元 $|c\rangle$ に対し、量子誤り E が発生した結果の量子情報 $E|c\rangle$ を復号アルゴリズムに入力すればどうなるか確かめよう。シンドロームを s とすれば rec の定義から、$\mathrm{rec}(s) = E$ が従う。よって $\mathrm{rec}(s)E|c\rangle = |c\rangle$ が従う。これは

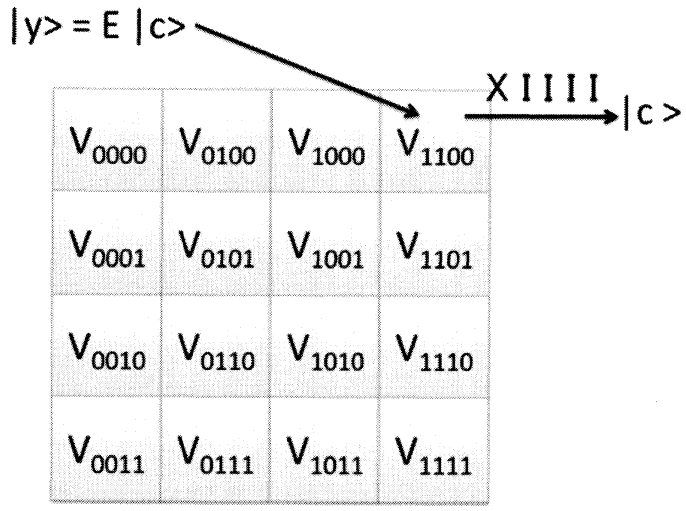

図 3: 5 量子ビット符号の復号過程

誤りが発生する前の Q の元と一致している。あとは $\mathrm{pad}^{1,5}$ の逆写像を作用させれば原来の量子情報が得られる。

5 量子ビット符号のシンドロームの総数 16 は情報機器（計算機等）が扱う数としては小さな値である。復号アルゴリズムの処理にかかる時間は少ないと見込める。シンドロームが 16 通りしかないことを読者が確かめるために要した時間はそれほどかからなかったのと同じ理由である。これは計算時間の少ない復号アルゴリズムが構成できることを意味する。

他方、符号化も簡単である。その理由はスタビライザ符号 Q の次元が 2 次元と小さいことにある。[6]そこで符号化写像の構成要素 $\mathbb{C}^2 \otimes |000\rangle \to Q$ を力づくで構成してしまえば良い。しかもそれはそんなに複雑ではない。

量子誤り訂正符号の定義の際に用いた正整数 n や k が小さい時には、力づくで符号化や復号ができてしまう。その為、性質を調べ上げたとしても、インパクトのある結果として主張しづらいことが懸念される。

5 量子ビット符号が注目された背景には、スタビライザ符号の登場という理由だけでなく、1 重以下の全ての誤りを訂正できる量子誤り訂正符号のうち最小の符号長を持つという理由もある。特別な最適性を発見することで「高い複合成功確率」とは異なる利点を主張できる。量子誤り訂正符号とは異なる意味付けが得られるのは非常に興味深いと言える。

5 量子ビット符号の復号成功確率を求めておこう。通信路を depolarizing 通信路とすればその確率は

$$(1-3q)^5 + 15q(1-3q)^4$$

[6]これはシンドロームが 16 通りであり、すべての固有空間の次元が等しく、全体の空間が $2^5 = 32$ 次元であることから従う。

と表せる。これはdepolarizing通信路における$\mathcal{E}$の生起確率として得られる。

具体的に復号成功確率を求めよう。例として$q = 0.022$とする。このとき上の成功確率は約0.962である。つまり失敗確率は0.038程度である。$n = 5$と小さい値を取るため、極端によい復号成功確率はそもそも期待できない。[7]

量子誤りとはユニタリ変換を指す言葉である。中にはパウリ行列で表せない誤りもある。例えば

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

などがあげられる。これらの誤りとIのテンソル積で表される1重量子誤りは5量子ビット符号では訂正できるだろうか。下記の定理により肯定的な結論が得られる。

定理 5.2. Qをスタビライザ符号（符号化写像と復号器の組の意味）とする。$\mathcal{E}$をパウリ行列のテンソル積として得られる誤りであって、スタビライザ符号Qが訂正できる誤りの集合とする。

この時、

$$\sum_{E \in \mathcal{E}} \alpha_E E$$

と表される誤りもQで訂正できる。ただしα_Eは複素数を表す。

この定理の証明には量子力学の概念「観測」を導入する必要がある。その為、本紙面では割愛する。興味のある読者は量子情報の専門書を参考にされると良い。実は観測の考え方は、復号アルゴリズムの定義中の（2）で暗に用いた。[8]

ちなみに任意の$(2,2)$型の行列はパウリ行列の一次結合として表されることを注意しておく。例えば、回転などのユニタリ変換も表される。この事実を上の定理とあわせれば、任意の1重誤りが5量子ビット符号によって訂正されることを得た。

5量子ビット符号は任意の1重以下の量子誤りに対して、上の復号アルゴリズムが出力する量子情報が元来の量子情報と一致するという性質を有した。このことを以て、5量子ビット符号は1重誤り訂正符号と呼ぶ。より一般的な表現として、t重以下の誤りであれば復号アルゴリズムによって訂正できる符号をt重誤り訂正符号と呼ぶ。こう言った性質をもつ符号は20世紀の符号理論において非常に活発に研究された。ちなみに、特定のしきい値までの誤り訂正を保証する性質は暗号プロトコルへの応用に適している[5][4]。

---

[7] ちなみに後述する量子LDPC符号の中には、同じ通信路の条件に対して失敗確率が0.0001未満を達成する符号が存在する。

[8] 量子情報を明記しなかった理由がそれである。

6 量子ハミング符号

$M_1, M_2, M_3, M_4, M_5, M_6$ をそれぞれ

$$
\begin{aligned}
M_1 &= I \otimes I \otimes I \otimes Z \otimes Z \otimes Z \otimes Z \\
M_2 &= I \otimes Z \otimes Z \otimes I \otimes I \otimes Z \otimes Z \\
M_3 &= Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z \\
M_4 &= I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X \\
M_5 &= I \otimes X \otimes X \otimes I \otimes I \otimes X \otimes X \\
M_6 &= X \otimes I \otimes X \otimes I \otimes X \otimes I \otimes X
\end{aligned}
$$

とする。このとき、対応するスタビライザ符号を量子ハミング符号もしくは7量子ビット符号と呼ぶ。

この符号も1重量子誤り訂正符号である。証明は、先程の5量子ビット符号と同様に、1重以下の誤りが全て異なるシンドロームを与えることを確かめれば良い。

この符号のシンドロームは面白い。1重誤りにおける I 以外のパウリ行列 P の位置を m_0 番目としよう。ただし $1 \leq m_0 \leq 7$ を表す。

$P = X$ の時を考察しよう。M_4, M_5, M_6 に対応するシンドローム $s_4 s_5 s_6$ は0のみで構成される。続いて M_1, M_2, M_3 に対応するシンドローム $s_1 s_2 s_3$ に注目する。この時、シンドロームを2進数とみなせば m_0 と一致する。つまり誤り X の示している。

次に $P = Z$ の時を考察しよう。今度は M_1, M_2, M_3 に対応するシンドロームは0のみで構成される。そして M_4, M_5, M_6 に対応するシンドロームを2進数とみなせば、やはり誤りの位置と一致する。

今後は $P = Y$ の時を考察しよう。このとき M_1, M_2, M_3 に対応するシンドロームと M_4, M_5, M_6 に対応するシンドロームが一致することが確かめられる。更に、上と同様に誤りの位置を表す。

この事実から、計算量の少ない復号アルゴリズムが構成できる。

ところで量子ハミング符号は、ハミング符号と呼ばれる古典誤り訂正符号を量子誤り訂正符号に拡張したものと言われている。ハミング符号とは二元体上の行列

$$
A = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}
$$

の核として定義される二元体上のベクトル空間を表す。この行列 H と量子ハミング符号のパリティ検査観測との類似性を探していただきたい。

7 量子LDPC符号

この節では筆者の成果を踏まえた専門的な話題を扱うことにする。ここで取り上げる量子 **LDPC** 符号とはスタビライザ符号もしくは CSS 符号であって、「疎」と呼ばれる構造を導入したパリティ検査観測をもつものとして定義される。復号法として sum-product 復号法と呼ばれるアルゴリズムを用いるのが特徴である。量子 LDPC 符号を理解するには古典誤り訂正符号の LDPC 符号の理解が不可欠である。残念であるが、理論面や技術面のことは本紙面では書ききれない。幾つか特徴を紹介するに留める。

古典 LDPC 符号の符号長として数十〜数十万などの様々な値が扱える。ここまでの量子誤り訂正符号では符号長が非常に小さな値を取った。しかし、理論的に興味深いのは符号長がある程度大きな場合である。量子誤り訂正符号へ LDPC 符号の理論を拡張することでそのような大きい符号長を扱える。

古典 LDPC 符号は符号長が数万程度であっても復号アルゴリズム（sum-product 復号法）が高速に動作するという特徴を持つ。さらに復号成功確率が非常に高いことも特徴である。フラッシュメモリや衛星放送などに実装されるなど、実用的に優れている。

2007 年頃は、量子誤り訂正符号に対して古典 LDPC 符号の理論を導入する動きが非常に活発だった。最近でも非常に興味深い成果が得られている。笠井らは文献 [8] において拡大体を経由した LDPC 符号の構成に成功している。この符号は文献 [9] のアイデアを巧みに利用したものである。現在知られる量子 LDPC 符号のなかで最も高い復号成功確率を持っている。

さらに小柳らは文献 [10] において笠井らのアイデアを一般化することに成功している。笠井らの方法では符号長の種類が制限されていた。しかし、小柳らの方法ではその制限を外すことに成功している。それでいて笠井らの符号と同等の復号成功確率を実現しているところが興味深い。しかも、次のことは数学的に面白い。小柳らの手法では、笠井らのアイデアを組合せ論の視点で捉える。それにより、連立２次多変数方程式の解法と組合せ論の関連を簡潔に記述している。

8 まとめ

量子誤り訂正符号の基礎を数学的な視点から整理した。古典誤り訂正符号が自然に拡張された理論であることを感じて頂ければ幸いである。

筆者が専門的に研究を行った量子 LDPC 符号の理論では、「LDPC 符号」と「組合せ論」と「連立２次多変数方程式」を考察することで理論的に面白く、かつ、復号成功確率の高い符号の構成が発見できた。数学者が活躍できるフィールドとして、量子誤り訂正符号は魅力的な分野の１つと言えるだろう。

参考文献

[1] Modern Coding Theory, T.Richardson and R.Urbanke, Cambridge University Press, 2008.

[2] 符号理論～コミュニケーションのための数学～（仮）, 萩原学, 日本評論社, 2011 発売予定.

[3] Stabilizer Codes and Quantum Error Correction, D. Gottesman, Ph.D. thesis, Calif. Inst. Technol., Pasadena, 1997.

[4] A Public-Key Cryptosystem Based On Algebraic Coding Theory R. J. McEliece, DSN Progress Report 42-44: 114, 1978.

[5] Safeguarding cryptographic keys, G. R. Blakley, AFIPS 1979 Nat. Computer Conf., vol. 48, pp. 313- 317, 1979.

[6] Good quantum error-correcting codes exist, A.R.Calderbank and P.W.Shor, Phys. Rev. A 54, pp.1098-1105, 1996.

[7] Error Correcting Codes in Quantum Theory, A.M.Steane, Phys. Rev. Lett. 77, pp.793-797, 1996.

[8] Quantum Error Correction beyond the Bounded Distance Decoding Limit, K.Kasai, M.Hagiwara, H.Imai, K.Sakaniwa, arXiv:1007.1778, 2010.

[9] Quantum quasi-cyclic LDPC codes, M. Hagiwara and H. Imai, in Proceedings of ISIT 2007. Nice, pp. 806-811, 2007.

[10] 2準位量子 QC-LDPC 符号を GF(2) の拡大体の同伴行列で拡張するための十分条件, 小　裕嵩, 萩原学, 今井秀樹.