量子誤り訂正符号覚え書き*

松本 隆太郎
東京工業大学 電気電子工学科 坂庭研究室
Email: ryutaroh@ss.titech.ac.jp

初版: 2000 年 8 月 2 日
最終更新: 2000 年 11 月 20 日

1 前書き

近年, 量子力学的現象を利用することによりそれらを利用しなかった場合に比べてある種の計算を非常に高速に実行したり, 計算量的な仮定に基づかず安全性を証明できる暗号方式が存在することがわかり, 注目を集めている. 例えば, Shor (1994, 1997) はほとんどの公開鍵暗号の基礎になっている素因数分解問題と離散対数問題を高速に解く量子アルゴリズムを提案し, Bennett and Brassard (1984) は安全性の仮定を量子力学的な物理法則だけに置く鍵共有方式を提案している.

量子アルゴリズムの実行には量子コンピュータが必要だが, 量子コンピュータは通常のディジタルコンピュータに比べて周囲の雑音に非常に弱いので, 雑音を抑圧する必要がある. これらのニーズに答えるのが量子誤り訂正符号である.

量子誤り訂正符号の研究は主に二元の場合を対象に行われてきたが, 雑音の性質によっては多元符号を用いた方が良い場合もあると思われる. 本稿では多元の量子誤り訂正符号に関する研究成果の紹介を行う.

2 量子力学の形式的構造

本稿の 3 節以降の内容を理解するのに最低限必要な量子力学の基礎について説明する. この節に述べることは量子力学の教科書にはどれでも書いてあるようなことである. 数学的に厳密な量子力学の教科書には例えば (Ballentine, 1998) がある.

外部との相互作用が無い物理系があるとせよ. この物理系の状態は数学的にはある複素 Hilbert 空間 H の長さ 1 の要素として表される. 複素数倍して同じになる H の要素は同じ物理状態を表すとする. これ以降, 量子誤り訂正符号では H が有限次元の場合しか扱わないので, H は有限次元とする[1].

この物理系がどの状態にあるかを厳密にしることはできない. 状態に関して知ることができるのは以下のようなことで, 知ることにより物理系の状態には以下のような変化が起きる.

---

*この文書は http://tsk-www.ss.titech.ac.jp/~ryutaroh/qecc.html から入手可能. 間違いを見つけた場合御連絡いただけると有難いです.

[1]無限次元の場合は数学的に厳密な取り扱いが若干面倒になる. どう面倒かは (Ballentine, 1998, Chapter 1) を参照せよ.

物理系の状態に関して情報を得ることを測定 (measurement) と言い, 測定ではかるものを観測量 (observable) と言い, すべての観測量は H のエルミート作用素に対応する. A を H に作用するエルミート作用素とせよ. A の固有値を $\lambda_1, \ldots, \lambda_s \in \mathbb{R}$ とし[2], $\boldsymbol{v}_{i,1}, \boldsymbol{v}_{i,2}, \ldots$ を λ_i に属する固有ベクトルとする. $\{\boldsymbol{v}_{i,j}\}$ は正規直交基底になっているとする. 今測定の前の物理系の状態を $\boldsymbol{v} \in H$ とし

$$\boldsymbol{v} = \sum_{i,j} a_{i,j} \boldsymbol{v}_{i,j}$$

とする. このとき $\boldsymbol{v}$ が長さ 1 であることより

$$\sum_{i,j} |a_{i,j}|^2 = 1$$

である.

観測量 A を測定すると状態 $\boldsymbol{v}$ は s 個の状態

$$\left\{ \sum_j a_{i,j} \boldsymbol{v}_{i,j} \;\middle|\; i = 1, \ldots, s \right\}$$

のどれかを長さ 1 に正規化した状態に確率的に移行する. 状態 $\sum_j a_{i,j} \boldsymbol{v}_{i,j}$ (を正規化したもの) に移る確率は $\sum_j |a_{i,j}|^2$ で与えられ, このとき測定を行った観測者は固有値 λ_i を得る. もし λ_i の固有空間の次元が 1 ならば観測者は測定後の物理状態を一意的に知ることができる.

測定は物理系の外部との相互作用の一種だが, 外部との相互作用の無いときの物理系の変化は H のユニタリー作用素として表される.

また, Hilbert 空間 H_1, H_2 で表される 2 つの物理系が有る場合, 2 つの物理系を合わせた物理系はテンソル積 $H_1 \otimes H_2$ で表される. このとき H_1 の観測量 A を測定することは $H_1 \otimes H_2$ の観測量 $A \otimes I$ を測定することと同じである.

3 量子誤り訂正符号

3.1 量子誤り訂正符号の問題設定

これ以降 H を ℓ (≥ 2) 次元線形空間とする. H が 1 個の光子や電子の物理状態に対応していると考えていただきたい. $H^{\otimes k}$ (H の k 重テンソル積) で表される物理状態を送りたいとする. これをこのまま送ると送っている途中で外部の環境から影響を受けて, 受け取ったときに送ったときの状態と違う状態になってしまう. このようなことを防ぐために, 元の状態を (巧みに構成した) $H^{\otimes n}$ の ℓ^k 次元部分空間 Q の要素に対応させて送ると, ある程度誤りが発生しても元の情報を復元できるようになる. 本稿ではそのような Q の構成法を紹介する.

量子通信路を介して送られる情報は $H^{\otimes n}$ の要素として表せる量子状態である. このような状態に生じるエラーは以下のように表せる. H_{env} を通信路の周りの物理状態を表す Hilbert 空間とし, 送信した状態は $\boldsymbol{v} \in Q$ でそのとき周りの環境の物理状態は $\boldsymbol{v}_{\mathrm{env}}$ であったとする. H_{env} を適当に取ることにより $H^{\otimes n} \otimes H_{\mathrm{env}}$ で表される物理系は外部との相互作用が無いようにできる. このとき生じるエラーは $H^{\otimes n} \otimes H_{\mathrm{env}}$ のユニタリー作用素 U で表すことができる. つまり受信したときの物理系の状態が $U(\boldsymbol{v} \otimes \boldsymbol{v}_{\mathrm{env}}) \in H^{\otimes n} \otimes H_{\mathrm{env}}$ であるということである. このとき $U(\boldsymbol{v} \otimes \boldsymbol{v}_{\mathrm{env}})$ は必ずしも $H^{\otimes n}$ のベクトルと H_{env} のベクトルのテンソル積では書けないことに注意せよ.

[2] エルミート作用素の固有値はすべて実数である. 線形代数の教科書を参照.

$0 \le \tau \le n$ を整数として U を, $H^{\otimes n}$ の中の H の順番を入れ換えることにより,

$$U = I_{n-\tau} \otimes J \tag{1}$$

と表すことができる. 但し, $I_{n-\tau}$ は H で表される物理系のうち $n-\tau$ 個の系に作用する恒等作用素で, J は残りの系に作用するユニタリー作用素である. 式 (1) が $U = J$ としか書けないときは $\tau = n$ とする. τ がなるべく小さくなるように $I_{n-\tau}$ と J を選んだときの τ の値を**エラーの数**と呼ぶ.

起こりうるすべてのエラーを訂正できるような量子誤り訂正符号は構成できないので, エラーの数がある値以下のエラーをすべて訂正できる Q の構成法を考える. 多くの量子誤り訂正符号の論文でこのような形のエラーを訂正対象とする量子誤り訂正符号が扱われている. 構成する量子誤り訂正符号 Q は $n-k$ (余分に必要な量子システム H の数) が小さく訂正できるエラーの数が多ければ良い符号であると考えられる. 次節では Q の構成法について説明する.

3.3 節ではエラーの数があまり大きく無いときに $U(\boldsymbol{v} \otimes \boldsymbol{v}_{\rm env})$ から $\boldsymbol{v}$ を復元する方法を示す. 具体的には, $H^{\otimes n}$ の幾つかの観測量を測定することにより $U(\boldsymbol{v} \otimes \boldsymbol{v}_{\rm env})$ は $H^{\otimes n}$ のユニタリー作用素の有限集合 E の要素 A とある $\boldsymbol{v}'_{\rm env} \in H_{\rm env}$ を用いて $(A\boldsymbol{v}) \otimes \boldsymbol{v}'_{\rm env}$ と表せる状態に射影されることを示し, さらに測定の結果から $A'A\boldsymbol{v}$ が $\boldsymbol{v}$ のスカラー倍になるような $A' \in E$ を決定できることを示す.

量子誤り訂正符号では大抵の場合 H で表される $n-\tau$ 個の物理系にはまったく変化が生じていないという仮定の下で誤り訂正を論じている. このような仮定が非現実的だと感じる読者は Knill and Laflamme (1997, Section 5.4) および Matsumoto (2000) の議論が参考になると思う.

3.2 量子誤り訂正符号 Q の構成法

λ を 1 の複素原始 ℓ 乗根[3]とし, $\ell \times \ell$ 複素ユニタリー行列 C_ℓ, D_λ を $(C_\ell)_{ij} = \delta_{i-1,j \bmod \ell}$, $(D_\lambda)_{ij} = \lambda^{i-1}\delta_{i,j}$ で定義する. $\ell = 2$ のとき C_2, D_{-1} は Pauli spin 行列 σ_x, σ_z になることに注意せよ. ほとんどの量子誤り訂正の論文は $\ell = 2$ の場合しか扱っていないが, $\ell = 2$ の場合にしか興味が無い読者は $\ell = 2$ と限定することにより補題 1 と 2 は容易に理解できるようになる. その他の部分は $\ell = 2$ でも一般の場合でも理解の容易さは変わらない. C_ℓ, D_λ は以下の性質を持つ.

補題 1 a, b, a', b' を整数とすると,

$$(C_\ell^a D_\lambda^b)(C_\ell^{a'} D_\lambda^{b'}) = \lambda^{a'b-ab'}(C_\ell^{a'} D_\lambda^{b'})(C_\ell^a D_\lambda^b).$$

証明: 単位ベクトル $\boldsymbol{e}_i$ $(i = 0, \ldots, \ell-1)$ を

$$\boldsymbol{e}_i = (\overbrace{0, \ldots, 0}^{i}, 1, 0, \ldots, 0)^T$$

とする. このとき $C_\ell \boldsymbol{e}_i = \boldsymbol{e}_{i+1 \bmod \ell}$, $D_\lambda \boldsymbol{e}_i = \lambda^i \boldsymbol{e}_i$ である. 従って

$$\begin{aligned}(C_\ell^a D_\lambda^b)(C_\ell^{a'} D_\lambda^{b'})\boldsymbol{e}_i &= \lambda^{ib+ib'+a'b}\boldsymbol{e}_{i+a+a' \bmod \ell}, \\ (C_\ell^{a'} D_\lambda^{b'})(C_\ell^a D_\lambda^b)\boldsymbol{e}_i &= \lambda^{ib+ib'+ab'}\boldsymbol{e}_{i+a+a' \bmod \ell}\end{aligned}$$

を得る. これらの式を比較することにより補題の主張を確認できる. ■

[3] $\lambda^\ell = 1$ かつすべての $j = 1, \ldots, \ell-1$ について $\lambda^j \ne 1$ のとき λ を 1 の原始 ℓ 乗根であると言う. 例えば $\exp(2\pi i/\ell)$ は 1 の原始 ℓ 乗根である.

補題 2 集合 $\{C_\ell^a D_\lambda^b \mid a = 0, \ldots, \ell-1, b = 0, \ldots, \ell-1\}$ は $\ell \times \ell$ 複素行列のなす線形空間の基底をなす.

証明: $D_\lambda^0, \ldots, D_\lambda^{\ell-1}$ の対角成分を並べて作った行列は Vandermonde 行列なので, $D_\lambda^0, \ldots, D_\lambda^{\ell-1}$ の適当な線形結合で (j,j) 成分だけが 1 の $\ell \times \ell$ 行列を作ることができる. この行列に $C_\ell^{\ell+i-j \bmod \ell}$ を左から掛けると (i,j) 成分だけが 1 の行列を作ることができる. 従って $\{C_\ell^a D_\lambda^b \mid a = 0, \ldots, \ell-1, b = 0, \ldots, \ell-1\}$ の適当な線形結合で任意の $\ell \times \ell$ 複素行列を表すことが可能で, この集合の要素数は $\ell \times \ell$ 複素行列のなす線形空間の次元に等しいので補題を証明できた. ■

誤り群 $E = \{\lambda^i C_\ell^{a_1} D_\lambda^{b_1} \otimes \cdots \otimes C_\ell^{a_n} D_\lambda^{b_n} \mid a_1, \ldots, a_n, b_1, \ldots b_n, i \text{ は整数 }\}$, および E の可換部分群 S を考える. 補題 1 より集合 E は群演算に関して閉じている. ここで E は $H^{\otimes n}$ に作用する線形変換 (行列) の集合だが, 群演算として線形変換の合成 (つまり行列の積) を考えている.

今後 S の固有空間として量子誤り訂正符号 Q を構成するが, その前に必要になる線形代数の事実を確認する. $\ell \times \ell$ 行列 A が対角化可能であるとは, $\mathbb{C}^\ell$ の基底 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell\}$ で, 各々のベクトル $\boldsymbol{v}_i$ が固有ベクトルになっているものが存在することである. 対角化可能な $\ell \times \ell$ 行列 A, B に対し A と B が同時に対角化可能であるとは, $\mathbb{C}^\ell$ の基底 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell\}$ で各々の $\boldsymbol{v}_i$ が A と B 両方の固有ベクトルになっているものが存在することを言う. もし A, B が対角化可能な $\ell \times \ell$ 行列で $AB = BA$ ならば, A と B は同時に対角化可能である. この段落で述べた事実の証明は例えば (Ballentine, 1998, Thm. 5, Chap. 1) に見つけることができる.

S は可換な行列のなす群なので, $H^{\otimes n} = \mathbb{C}^{\ell^n}$ の基底 $B = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\ell^n}\}$ で各々の $\boldsymbol{v}_i$ が S に属するすべての行列の固有ベクトルになっているものが存在する. $\boldsymbol{v}_i$ を基底 B に含まれる任意のベクトルとする. S の固有空間とは $\boldsymbol{v}_i$ を適当に選ぶことによって, 集合 $\{\boldsymbol{v} \in B \mid S$ に含まれるすべての行列 A について $\boldsymbol{v}$ と $\boldsymbol{v}_i$ は A の同じ固有値に属する $\}$ によって張られる線形空間としてえられる $H^{\otimes n}$ の線形部分空間である. したがって 1 つの S の固有空間は S に属する各々の行列の属する固有値によって識別される. S は群であるので, S の固有空間を識別するには S の生成元になっている行列のどの固有値に属するかだけがわかれば十分である. 量子誤り訂正符号 Q を S の固有空間の 1 つとして構成する. 以下 Q の次元と訂正可能な誤りの数を検討する.

まず E に含まれる行列が Q に対してどのように作用するか検討する. $H^{\otimes n}$ に含まれるベクトルを複素数倍しても同じ量子状態を表すので, S に含まれる行列は Q に含まれる量子状態に影響を与えない.

E の部分群 S' を

$$S' = \{A \in E \mid \forall B \in S,\ AB = BA\}$$

で定義する. 以下の補題により S' に含まれるエラーは検出できないことがわかる.

補題 3 $A \in E, \boldsymbol{v} \in Q \setminus \{\boldsymbol{0}\}$ とすると, $A\boldsymbol{v} \in Q \iff A \in S'$ である.

証明: 最初に $A \in S' \Longrightarrow A\boldsymbol{v} \in Q$ を証明する. 主張ををを証明するためには, 任意の $B \in S$ に対し, $\boldsymbol{v}$ と $A\boldsymbol{v}$ が B の同じ固有値に属することを示せばよい. $\boldsymbol{v}$ が B の固有値 η に属しているとする. $BA\boldsymbol{v} = AB\boldsymbol{v} = \eta A\boldsymbol{v}$ より $A\boldsymbol{v}$ も B の固有値 η に属する.

次に $A \notin S' \Longrightarrow A\boldsymbol{v} \notin Q$ を証明する. $A \notin S'$ なので, 補題 1 より $BA = \tau AB, \tau \neq 1$ を満たす $B \in S$ が存在する. $\boldsymbol{v}$ が B の固有値 η に属するとすると, $BA\boldsymbol{v} = \tau AB\boldsymbol{v} = \eta\tau A\boldsymbol{v}$ より, $A\boldsymbol{v}$ は $\boldsymbol{v}$ と異なる B の固有値に属する. 従って $\boldsymbol{v} \notin Q$. ■

補題 4 $A \in E$ に対し $AQ := \{A\boldsymbol{v} \mid \boldsymbol{v} \in Q\}$ と定義する. このとき AQ は S の固有空間である.

証明: $\boldsymbol{v} \in Q$, $B \in S$, $B\boldsymbol{v} = \eta\boldsymbol{v}$ とすると補題を証明するには $A\boldsymbol{v}$ の属する B の固有値が $\boldsymbol{v}$ に依存しないことを示せばよいが, 補題 1 より $BA = \tau AB$ とすると $BA\boldsymbol{v} = \tau AB\boldsymbol{v} = \eta\tau A\boldsymbol{v}$ より明らかである. ■

補題 5 S の固有空間からなる集合は $\{AQ \mid A \in E\}$ に等しい.

証明: $A \in E$ に対し $A\boldsymbol{v}$ は S のどの行列に対しても固有ベクトルになるので, 集合 $\{AQ \mid A \in E\}$ は S の固有空間からなる集合に含まれることがわかる.

$\boldsymbol{v} \in Q$ を非零なベクトルとする. 補題 2 とテンソル積の性質より, 集合 E は $\ell^n \times \ell^n$ 複素行列のなす線形空間を張る. 従って集合 $\{A\boldsymbol{v} \mid A \in E\}$ は $H^{\otimes n}$ を張る. 従って $\{AQ \mid A \in E\}$ は $H^{\otimes n}$ の直交分解になっているので補題を証明できた. ■

次に剰余類群 E/S' を考えるために以下の補題を導入する.

補題 6 S' は E の正規部分群である.

証明: S' は 集合 $\{\lambda^i I \mid i$ は整数 $\}$ を含んでいる. 但しここで I は $H^{\otimes n}$ の恒等写像である. $A \in E$, $B \in S'$ とすると, AB は剰余類 AS' に含まれる. $AB = \lambda^i BA$ とする. $\lambda^i IB \in S'$ なので $AB \in S'A$ である. ■

補題 6 より E/S' は群である. 補題 3 と補題 4 より群 E/S' の S の固有空間からなる集合への作用を定義することができる.

補題 7 $A_1S', A_2S' \in E/S'$ とする. もし $A_1S' \neq A_2S'$ ならば $(A_1S')Q \neq (A_2S')Q$ である.

証明: $A_3 = A_2A_1^{-1}$ とおくと $(A_1S')Q \neq (A_2S')Q \Longleftrightarrow Q \neq A_3Q$ である. 補題 3 と $A_3 \notin S'$ より $Q \neq A_3Q$ である. ■

定理 8

$$\dim Q = \frac{\ell^n}{\sharp(E/S')}.$$

但し $\sharp$ は集合の要素数を表す.

証明: 補題 7 と補題 5 より S の固有空間の数と E/S' の要素数が等しいことがわかる. 補題 5 より S の固有空間はすべて同じ次元を持つことがわかる. 従って $\dim Q = \dim H^{\otimes n}/\sharp(E/S')$ である. ■

3.3 誤り訂正の方法

これ以降 Q の要素を符号語として送り誤りが発生した場合どのように起きた誤りを訂正するか考える. $A = \lambda^i C_p^{a_1} D_\lambda^{b_1} \otimes \cdots \otimes C_p^{a_n} D_\lambda^{b_n} \in E$ に対し, A の重み $w(A)$ を

$$\sharp\{j \mid (a_j, b_j) \neq (0,0)\} \tag{2}$$

と定義する. これは A をエラーと見たときのエラーの数に等しい. また

$$d = \min\{w(A) \mid A \in S' \setminus S\}$$

と定義し, 量子誤り訂正符号 Q の最小距離と呼ぶ. 符号長 n, 次元 ℓ^k, 最小距離 d の量子誤り訂正符号を $[[n,k,d]]_\ell$ 符号と記す.

生じた誤りの数が $d-1$ 個以下なら, 補題 3 より誤りが生じたことを検出できる. $\lfloor (d-1)/2 \rfloor$ 個までの誤りを訂正する手続きを以下に示す. 式 (1) のようなエラーが生じたと仮定し, エラーを U で表す. 送信した符号語は $\boldsymbol{v} \in Q$ で, そのときの周りの環境の状態は $\boldsymbol{v}_{\rm env} \in H_{\rm env}$ で表されるとする.

$\boldsymbol{a} = (a_1, \ldots, a_n)$ $(a_i \in \{0, \ldots, p-1\})$ に対し

$$\begin{aligned} X(\boldsymbol{a}) &= C_p^{a_1} \otimes \cdots \otimes C_p^{a_n}, \\ Z(\boldsymbol{a}) &= D_\lambda^{a_1} \otimes \cdots \otimes D_\lambda^{a_n} \end{aligned}$$

と定義する. このとき補題 2 より集合 $\{X(\boldsymbol{a})Z(\boldsymbol{b})\boldsymbol{v} \mid \boldsymbol{a}, \boldsymbol{b} \in \{0, \ldots, \ell-1\}^n\}$ は $H^{\otimes n}$ の基底になる. 従って $U(\boldsymbol{v} \otimes \boldsymbol{v}_{\rm env})$ を

$$U(\boldsymbol{v} \otimes \boldsymbol{v}_{\rm env}) = \sum_{\boldsymbol{a},\boldsymbol{b}} \alpha_{\boldsymbol{a},\boldsymbol{b}} (X(\boldsymbol{a})Z(\boldsymbol{b})\boldsymbol{v}) \otimes \boldsymbol{v}_{{\rm env},\boldsymbol{a},\boldsymbol{b}} \tag{3}$$

という形の線型結合で書くことができる. 但し, $\boldsymbol{v}_{{\rm env},\boldsymbol{a},\boldsymbol{b}}$ は $H_{\rm env}$ のベクトルである. もし生じたエラーの数 τ が $\lfloor (d-1)/2 \rfloor$ 以下なら線型結合の中に現れるすべての $X(\boldsymbol{a})Z(\boldsymbol{b})$ の重みを $\lfloor (d-1)/2 \rfloor$ 以下にすることができる.

$A_1, A_2 \in E$ かつ $w(A_1), w(A_2) \leq \lfloor (d-1)/2 \rfloor$ とする. このとき d の定義から

$$A_1 S' \neq A_2 S' \tag{4}$$

または

$$A_1 S = A_2 S \tag{5}$$

が必ず成立する. 式 (4) が成立した場合, 補題 7 より $A_1\boldsymbol{v}$ および $A_2\boldsymbol{v}$ は S の異なる固有空間に属し, 従って直交する. 式 (5) が成立した場合 $A_1\boldsymbol{v} = A_2\boldsymbol{v}$ である.

式 (3) と前段落の議論から,

$$U(\boldsymbol{v} \otimes \boldsymbol{v}_{\rm env}) = \sum_{\boldsymbol{a},\boldsymbol{b}} \alpha_{\boldsymbol{a},\boldsymbol{b}} (X(\boldsymbol{a})Z(\boldsymbol{b})\boldsymbol{v}) \otimes \boldsymbol{v}_{{\rm env},\boldsymbol{a},\boldsymbol{b}}$$

と表し, なおかつ $\sum$ の中に現れる $X(\boldsymbol{a})Z(\boldsymbol{b})\boldsymbol{v}$ はお互いに異なる S の固有空間に属するようにできる. $G_1, \ldots, G_r$ を S の生成元とすると, $G_1, \ldots, G_r$ と同じ固有空間を持つ r 個の $H^{\otimes n}$ の観測量を測定することにより, $U(\boldsymbol{v} \otimes \boldsymbol{v}_{\rm env})$ は適当な $A \in E$ を用いて $(A\boldsymbol{v}) \otimes \boldsymbol{v}'_{\rm env}$ と表せる状態に射影される. 但し, $\boldsymbol{v}'_{\rm env} \in H_{\rm env}$ である.

誤りを訂正するには剰余類 AS を調べ, $B^{-1} \in AS$ となるユニタリー変換 B を $A\boldsymbol{v}$ に作用させれば $\boldsymbol{v}$ を復元できる. 以下測定の結果から剰余類 AS を決定する方法について述べる.

補題 9 剰余類 AS' の中に, $A'S \subset AS'$, $AS \neq A'S$, かつ $w(A') \leq \lfloor (d-1)/2 \rfloor$ となる剰余類 $A'S$ は存在しない.

証明: そのような A' が存在したとすると, $w(A'^{-1}) = w(A') \leq \lfloor (d-1)/2 \rfloor$ かつ $A'^{-1}A \in S' \setminus S$ なので, d の定義に矛盾する. ■

従って AS を知るためには AS' を知ることが出来ればよい. 補題 7 より $A\boldsymbol{v}$ が S のどの固有空間に属しているかわかれば AS' がわかる. $A\boldsymbol{v}$ が属している固有空間は $A\boldsymbol{v}$ が属している S の生成元 $G_1, \ldots, G_r$ の固有値からわかるが, それは前に行った測定の結果からわかる.

ここで 測定の結果から剰余類 AS を求める計算は予め測定結果と S の剰余類の対応を表にしておき, その表を探索することにより行う. 表の大きさは n と d に関して指数関数的に増えるので n と d が大きくなると測定の結果から AS を求める計算が困難になる. より効率の良い誤り AS の計算方法は Matsumoto and Uyematsu (2000) を参照せよ. また, 命題 12 で述べる CSS 符号の場合測定結果から従来の符号理論の意味でのシンドロームを直ちに求めることが可能で, 従来の符号理論でシンドロームから誤りベクトルを求めるアルゴリズムを用いて AS を求めることができる.

3.4 次元が素数冪の場合への帰着

前節では H の次元 ℓ が 2 以上の自然数の場合を取り扱ったが ℓ の素因数分解が $p_1^{m_1}\cdots p_s^{m_s}$ であるとき, 量子誤り訂正符号 $Q \subset H^{\otimes n}$ は基本になる物理系の自由度が小さい系のための量子誤り訂正符号 $Q_i \subset H_i^{\otimes n}$ $(i = 1, \ldots, s)$ のテンソル積 $Q = Q_1 \otimes \cdots \otimes Q_s$ と書くことができ, Q の次元と誤り訂正能力は $Q_1, \ldots, Q_s$ から直ちに評価することができる. 但し H_i は $p_i^{m_i}$ 次元 Hilbert 空間である.

また, このとき H, H_i に作用するユニタリー作用素の基底の取り方は補題 2 の取り方とは違い, H_i のユニタリー作用素の基底は $\{C_{p_i}^a D_{\lambda_i}^b \mid a = 0, \ldots, p_i - 1, b = 0, \ldots, p_i - 1\}$ (λ_i は 1 の 原始 p_i 乗根) の m_i 重テンソル積としてとり, H のユニタリー作用素の基底は H_i のユニタリー作用素の基底 $(i = 1, \ldots, s)$ のテンソル積としてとる. このように基底をとっても 3.2 節と 3.3 節の議論は若干修正を加えた上ですべて成り立つ. 従って量子誤り訂正符号の構成においては H の次元として素数冪の場合だけ考えれば良い.

4 直交幾何を用いた問題の変形

H の次元を素数 p とする. H の次元が素数冪の場合は記述が煩雑になるので省略する. 3.2 節で述べた良い量子誤り訂正符号を構成する問題は以下のようなものであった.

問題 10 誤り群 E の可換部分群 S で $\sharp(E/S')$ が小さく最小距離 $\min\{w(A) \mid A \in S' \setminus S\}$ が大きいものを探す.

この節ではこの問題をもう少し見やすい形に変形する.

集合 $\{\lambda^i I \mid i = 0, \ldots, p-1\}$ は E の正規部分群である. $\overline{E} = E/\{\lambda^i I \mid i = 0, \ldots, p-1\}$ とし, これ以降 E の要素や部分群に上線を付けたものはその $\overline{E}$ での像とする. $\overline{E}$ は可換群になることに注意せよ.

$\mathbf{F}_p$ を要素数 p の有限体とし, ベクトル $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbf{F}_p^n$ に対し, $(\boldsymbol{a}|\boldsymbol{b})$ で $\boldsymbol{a}$, $\boldsymbol{b}$ を連接したベクトル $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ を表すことにする. 以下の写像

$$\begin{array}{ccc} \mathbf{F}_p^{2n} & \longrightarrow & \overline{E} \\ (\boldsymbol{a}|\boldsymbol{b}) & \longmapsto & \overline{X(\boldsymbol{a})Z(\boldsymbol{b})} \end{array}$$

は可換群の同型写像を与える. 但し $\mathbf{F}_p^{2n}$ の群演算はベクトルの加算だが, $\overline{E}$ の群演算は行列の乗算である. これ以降 $\overline{E}$ と $\mathbf{F}_p^{2n}$ を同一視する.

$(\boldsymbol{a}|\boldsymbol{b})$, $(\boldsymbol{a}'|\boldsymbol{b}') \in \mathbf{F}_p^{2n}$ に対し交代的 (alternating または symplectic) かつ非退化 (nondegenerate)[4] な内積を

$$\langle \boldsymbol{a}, \boldsymbol{b}' \rangle - \langle \boldsymbol{a}', \boldsymbol{b} \rangle \tag{6}$$

[4]内積が交代的であること及び非退化であることの説明は代数の教科書 (例えば Lang (1993)) に見つけることができる.

で定義する. 但し $\langle,\rangle$ は通常の $\mathbf{F}_p^{2n}$ での内積を表す. このとき $X(\boldsymbol{a})Z(\boldsymbol{b})X(\boldsymbol{a}')Z(\boldsymbol{b}') = \lambda^i X(\boldsymbol{a}')Z(\boldsymbol{b}')X(\boldsymbol{a})Z(\boldsymbol{b})$ とすると $-i$ は補題 1 より $(\boldsymbol{a}|\boldsymbol{b})$ と $(\boldsymbol{a}'|\boldsymbol{b}')$ の内積に等しい.

$E \supseteq S$ を必ずしも可換とは限らない E の部分群とする. このとき $\overline{S}$ は線形空間 $\mathbf{F}_p^{2n}$ の部分空間になる. $\overline{S}^{\perp}$ を $\overline{S}$ の内積 (6) に関する直交空間とする. このとき S が可換になることと $\overline{S} \subseteq \overline{S}^{\perp}$ は同値である.

また $\overline{S'}$ は $\overline{S}^{\perp}$ に等しい. $\{\lambda^i I \mid i = 0, \ldots, p-1\} \subset S'$ なので $\sharp(E/S') = \sharp(\overline{E}/\overline{S'}) = \sharp(\overline{E}/\overline{S}^{\perp})$ である. このとき内積 (6) は非退化なので $\dim \overline{S} = n - k$ とすると $\dim \overline{S}^{\perp} = n + k$, $\sharp(\overline{E}/\overline{S}^{\perp}) = p^{n-k}$ となるので量子誤り訂正符号 Q の次元は $\dim H^{\otimes n}/\sharp(\overline{E}/\overline{S}^{\perp}) = p^k$ となる.

また, $(\boldsymbol{a}|\boldsymbol{b}) = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathbf{F}_p^{2n}$ に対し重みを

$$w(\boldsymbol{a}|\boldsymbol{b}) = \sharp\{i \mid (a_i, b_i) \neq (0,0)\}$$

とすると, E の可換部分群 S に対し

$$\min\{w(A) \mid A \in S' \setminus S\} = \min\{w(\boldsymbol{a}|\boldsymbol{b}) \mid (\boldsymbol{a}|\boldsymbol{b}) \in \overline{S}^{\perp} \setminus \overline{S}\}$$

が成り立つ. 従って良い量子誤り訂正符号を構成する問題は以下のように言い直すことができる.

問題 11 $C \subset \mathbf{F}_p^{2n}$ を線形部分空間とし, $C^{\perp}$ を内積 (6) に関する直交空間とする. このとき $C \subseteq C^{\perp}$ で $\dim C$ が小さく $\min\{w(\boldsymbol{a}|\boldsymbol{b}) \mid (\boldsymbol{a}|\boldsymbol{b}) \in C^{\perp} \setminus C\}$ が大きい C を探す.

以上の問題は更に代数的符号理論の問題に帰着できるがそれについては Matsumoto and Uyematsu (2000) または Ashikhmin and Knill (2000) と Bierbrauer and Edel (2000) を参照せよ.

自己直交な部分空間 $C \subseteq \mathbf{F}_p^{2n}$ から得られる量子誤り訂正符号のパラメータは $[[n, n - \dim C, d]]_p$ である. 但し $d = \min\{w(\boldsymbol{a}|\boldsymbol{b}) \mid (\boldsymbol{a}|\boldsymbol{b}) \in C^{\perp} \setminus C\}$ である.

本稿で紹介した量子誤り訂正符号の構成法は Calderbank and Shor (1996) および Steane (1996) が提案した構成法 (CSS 符号) の一般化である. CSS 符号は単純な構造を持ち量子メモリの誤り訂正などでよく使われるので, 以下に紹介する.

命題 12 (CSS 符号) (Calderbank and Shor, 1996; Steane, 1996) $C_1 \subseteq C_2 \subset \mathbf{F}_p^n$ を線形符号, $C_1^{\perp}$, $C_2^{\perp}$ を C_1, C_2 の標準内積に関する双対符号とする.

$$C = \{(\boldsymbol{x}|\boldsymbol{y}) \mid \boldsymbol{x} \in C_1,\ \boldsymbol{y} \in C_2^{\perp}\}$$

とすると C は内積 (6) に関して自己直交しているので C から量子誤り訂正符号 Q を構成することができる. このとき Q は $[[n, k_2 - k_1, d]]_p$ 符号である. 但し d は $C_2 \setminus C_1$ および $C_1^{\perp} \setminus C_2^{\perp}$ の最小ハミング重みの小さいほうに等しい. ■

この節では p 元量子誤り訂正符号の構成問題を $\mathbf{F}_p^{2n}$ のある種の部分空間を探す問題に帰着した. しかし基本になる量子系 H の次元が素数冪 p^m のとき同様の問題の変形ができるかどうかは自明ではない. Ashikhmin and Knill (2000) はこの節の結果を拡張し以下の結果を導いている. 証明は省略する.

命題 13 $(\boldsymbol{a}|\boldsymbol{b})$, $(\boldsymbol{a}'|\boldsymbol{b}') \in \mathbf{F}_{p^m}^{2n}$ に対し交代的かつ非退化な $\mathbf{F}_p$-bilinear form を以下のように定義する:

$$\mathrm{Tr}_p^{p^m}(\langle \boldsymbol{a}, \boldsymbol{b}' \rangle - \langle \boldsymbol{a}', \boldsymbol{b} \rangle), \tag{7}$$

但し $\mathrm{Tr}_p^{p^m}$ は $\mathbf{F}_{p^m}$ から $\mathbf{F}_p$ へのトレース写像である. $\mathbf{F}_p$ 線形空間 $C \subset \mathbf{F}_{p^m}^{2n}$ の (7) に関する直交空間を $C^{\perp}$ とし, $d = \min\{w(\boldsymbol{a}|\boldsymbol{b}) \mid (\boldsymbol{a}|\boldsymbol{b}) \in C^{\perp} \setminus C\}$ とする. もし $C \subseteq C^{\perp}$ なら C を用いて $[[n, n - (\dim_{\mathbf{F}_p} C)/m, d]]_{p^m}$ 量子謝り訂正符号を構成できる. ■

5 Bibliographic Notes

3.2 節の結果は $\dim H = 2$ の場合を Gottesman (1996); Calderbank et al. (1997, 1998) が明らかにし, $\dim H$ が一般の場合は Knill (1996a,b); Rains (1999) が明らかにした. Gottesman (1996); Calderbank et al. (1997, 1998) は誤り訂正の過程を明示的に論文中に書かなかったが, 3.3 節に述べた過程は量子誤り訂正符号の一般論 Bennett et al. (1996, Appendix B), Ekert and Macchiavello (1996); Knill and Laflamme (1997) から導くことができる.

3.4 節で述べた量子誤り訂正符号の構成が $\dim H$ が素数冪の場合だけ考えれば十分であることは Rains (1999, p.1831, Remarks) が指摘した.

4 節の結果は Calderbank et al. (1997, 1998) が $\dim H = 2$ の場合に明らかにした. $\dim H$ が 2 以外の素数の場合への拡張は自明である.

参考文献

Ashikhmin, A. and E. Knill (2000, May). Nonbinary quantum stabilizer codes. LANL eprint[5] `quant-ph/0005008`.

Ballentine, L. E. (1998). *Quantum Mechanics: A Modern Development*. Singapore: World Scientific.

Bennett, C. H. and G. Brassard (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Intl. Conf. on Computers, Systems, and Signal Processing*, pp. 175–179.

Bennett, C. H., D. P. DiVicenzo, J. A. Smolin, and W. K. Wootters (1996, Nov.). Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54**(5), 3824–3851. LANL eprint `quant-ph/9604024`.

Bierbrauer, J. and Y. Edel (2000, Apr.). Quantum twisted codes. *Journal of Combinatorial Designs* **8**(3), 174–188.

Calderbank, A. R., E. M. Rains, P. W. Shor, and N. J. A. Sloane (1997, Jan.). Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* **78**(3), 405–408. LANL eprint `quant-ph/9605005`.

——— (1998, July). Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory* **44**(4), 1369–1387. LANL eprint `quant-ph/9608006`.

Calderbank, A. R. and P. W. Shor (1996). Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098–1105. LANL eprint `quant-ph/9512032`.

Ekert, A. and C. Macchiavello (1996, Sept.). Quantum error correction for communication. *Phys. Rev. Lett.* **77**(12), 2585–2588. LANL eprint `quant-ph/9602022`.

Gottesman, D. (1996, Sept.). Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* **54**(3), 1862–1868. LANL eprint `quant-ph/9604038`.

Knill, E. (1996a, Aug.). Non-binary unitary error bases and quantum codes. LANL eprint `quant-ph/9608048`.

——— (1996b, Aug.). Group representations, error bases and quantum codes. LANL eprint `quant-ph/9608049`.

[5] LANL eprint は `http://xxx.lanl.gov/` から入手可能.

Knill, E. and R. Laflamme (1997, Feb.). Theory of quantum error-correcting codes. *Phys. Rev. A* **55**(2), 900–911. LANL eprint `quant-ph/9604034`.

Lang, S. (1993). *Algebra* (third ed.). Addison-Wesley.

Matsumoto, R. (2000). Fidelity of a t-error correcting quantum code with more than t errors. LANL eprint `quant-ph/0011047`.

Matsumoto, R. and T. Uyematsu (2000, Oct.). Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes. *IEICE Trans. Fundamentals* **E83-A**(10), 1878–1883. LANL eprint `quant-ph/9911011`.

Rains, E. M. (1999, Sept.). Nonbinary quantum codes. *IEEE Trans. Inform. Theory* **45**(6), 1827–1832. LANL eprint `quant-ph/9703048`.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134.

——— (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509. LANL eprint `quant-ph/9508027`.

Steane, A. M. (1996). Multiple particle interference and quantum error correction. *Proc. Roy. Soc. London Ser. A* **452**, 2551–2577. LANL eprint `quant-ph/9601029`.