複数の量子誤り訂正符号を利用した 2-EDP 構成法及びその評価

佐々木 大地　　指導教員：臼田 毅

1 はじめに

量子情報科学が持つ特有の性質としてエンタングルメント [1] という複数の量子系の間にある非局所的な相関がある．これを用いることで量子テレポーテーション [2] といった量子応用プロトコルの実現が可能となる．ただし，このような応用プロトコルを実行するためには，エンタングルメントを持つ量子状態（エンタングルド状態）を送受信者間で共有する必要がある．状態の共有のために，まず送信者である Alice が最大エンタングルメントを持つ Bell 状態

$$|\Phi^+\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}) \tag{1}$$

を用意して通信路を利用して状態の一方（この場合系 B）を送信することを考える．このとき状態は通信路上の外乱を受けてしまいエンタングルメントが劣化する．これは応用プロトコルの実行が失敗してしまう原因となる．

この問題を扱う方法の一つとしてエンタングルメント抽出（EDP:entanglement distillation protocol）が提案されている [1]. EDP は状態に対する局所操作（例：測定）と古典通信（例：測定結果の伝送）を繰り返し行うことでより高い精度のエンタングルメントを持つ状態を取り出すプロトコルの総称である．EDP には二つのクラス分けがされており，古典通信を常に一方向でのみ行う場合を 1-EDP，一度でも双方向に行うものを 2-EDP と分類されている．本研究では 2-EDP を扱う．先行研究では任意の stabilizer 符号を一つ使った EDP 構成法が示されている [3]. これをもとに本研究では新たに複数の符号を使う 2-EDP 構成法を示し，実際に構成法を適用して 2-EDP を構成しその評価を行うことで有効性を示していく．

2 複数の量子誤り訂正符号を利用した 2-EDP 構成法

本研究で提案する 2-EDP 構成法は，二つ以上の量子誤り訂正符号を使い構成する．ここでは二つの stabilizer 符号 C_1 と C_2 を用意する．ただし，C_1 と C_2 は，それぞれ $[n, k_1]$ 符号と $[n, k_2]$ 符号とし，

$$\begin{aligned} G^{(1)} &= \{g_1^{(1)}, g_2^{(1)}, \cdots, g_{n-k_1}^{(1)}\}, \\ G^{(2)} &= \{g_1^{(2)}, g_2^{(2)}, \cdots, g_{n-k_2}^{(2)}\} \end{aligned} \tag{2}$$

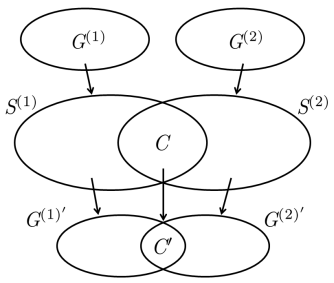

図 1　各作用素集合の関係

をそれぞれスタビライザ符号 C_1 と C_2 の生成作用素の集合とする．さて，各符号のスタビライザは

$$\begin{aligned} S^{(1)} &= \langle g_1^{(1)}, g_2^{(1)}, \cdots, g_{n-k_1}^{(1)}\rangle, \\ S^{(2)} &= \langle g_1^{(2)}, g_2^{(2)}, \cdots, g_{n-k_2}^{(2)}\rangle \end{aligned} \tag{3}$$

であるが，$S^{(1)}$，$S^{(2)}$ 両方に含まれる共通の要素の集合を作る．つまり $C = S^{(1)} \cap S^{(2)}$ を考える．C のある生成作用素の集合を $C' = \{c_1', \cdots, c_l'\}$ とすると，$C' \subset C \subset S^{(1)}, S^{(2)}$ より，C' の要素たちは $S^{(1)}$ と $S^{(2)}$ の生成作用素たちの一部となりうる．このため，各符号の生成作用素を以下のように選ぶことができる．

$$\begin{aligned} G^{(1)'} &= \{g_1^{(1)'}, g_2^{(1)'}, \cdots, g_{n-k_1}^{(1)'}\}, \\ G^{(2)'} &= \{g_1^{(2)'}, g_2^{(2)'}, \cdots, g_{n-k_2}^{(2)'}\} \end{aligned} \tag{4}$$

ただし，

$$g_i^{(1)'} = g_i^{(2)'} = c_i' \ \ (i = 1, \cdots, l). \tag{5}$$

ここまでの各集合の関係は図 1 のようになる．

以上を準備とし，2 つのスタビライザ符号 C_1, C_2 を用いた 2-EDP の手順を説明する (図 2).

- Alice は自身が持つ粒子に対して c_1' から c_l' を測定し測定結果 $\boldsymbol{a}_{C'} = (a_{c_1'}, \cdots, a_{c_l'})$ を得る．
- Bob は自身が持つ粒子に対して c_1' から c_l' を測定し測定結果 $\boldsymbol{b}_{C'} = (b_{c_1'}, \cdots, b_{c_l'})$ を得る．
- Alice は古典通信を使い Bob に $\boldsymbol{a}_{C'}$ を送信し Bob はシンドローム

$$\boldsymbol{s}_{C'} = \boldsymbol{a}_{C'} \oplus \boldsymbol{b}_{C'} = (a_{c_1'} \oplus b_{c_1'}, \cdots, a_{c_l'} \oplus b_{c_l'}) \tag{6}$$

を計算し $\boldsymbol{s}_{C'}$ を Alice に送信する．
- If $\boldsymbol{s}_{C'} \in \mathcal{R}$，Alice と Bob は残りの生成作用素 $g_{l+1}^{(1)'}$ から $g_{k_1}^{(1)'}$ を測定し，測定結果からシンドロームを計算する．すべてのシンドロームによってペアの破棄もしくは誤り訂正及びペアの共有を行う．
- If $\boldsymbol{s}_{C'} \notin \mathcal{R}$，Alice と Bob は残りの生成作用素 $g_{l+1}^{(2)'}$ から $g_{k_2}^{(2)'}$ を測定し，測定結果からシンドロームを計算する．すべてのシンドロームによってペアの破棄もしくは誤り訂正及びペアの共有を行う．

ここで，$\mathcal{R}$ は $\boldsymbol{s}_{C'}$ を測定することで得られる全てのシンドロームの部分集合である．つまりプロトコルの条件分岐は $\mathcal{R} \subset \mathbb{F}_2^l$ について，$\boldsymbol{s}_{C'} \notin \mathcal{R}$ もしくは $\boldsymbol{s}_{C'} \in \mathcal{R}$ の場合において処理が変化する．

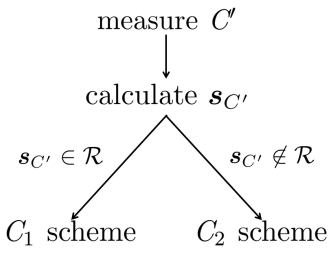

図 2　EDP 実行手順

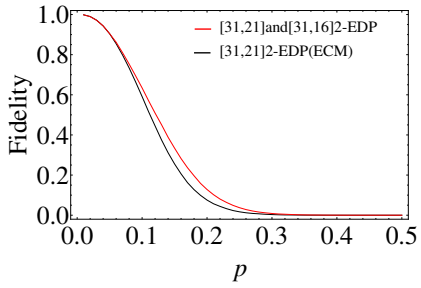

図 3　Fidelity グラフ，赤線：[31, 21]and[31, 16]2-EDP，黒線：[31, 21]2-EDP

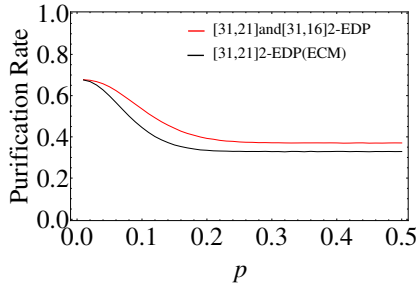

図 4　Purification rate グラフ，赤線：[31, 21]and[31, 16]2-EDP，黒線：[31, 21]2-EDP

3　シミュレーションによる EDP 評価

本節では fidelity，purification rate，fidelity の指数的下界の三つの指標を使い EDP を評価していく．通信路設定には一量子ビット ρ に対する作用を

$$\mathcal{E}_{\mathrm{PD}}(\rho) = (1-p)\rho + pZ\rho Z^{\dagger} \tag{7}$$

のようにした phase-damping 通信路を想定する．尚，式中の Z は状態 ρ に作用する誤りである．

3.1　Fidelity と purification rate の評価

本節で扱う fidelity とは EDP 実行後に出力される状態と，本来共有したい状態との近さを表し，値としては 0 から 1 の間を取り 1 に近いほど抽出性能が高いことを示す．Purification rate は古典理論での符号化率に対応するが，今回は EDP 実行後に状態を共有する確率 P_{S} と設定し，n を用意する状態数，k を最終的に共有する状態数として $(k/n)P_{\mathrm{S}}$ として見ていく．図 3，図 4 はそのプロットである．[31, 21]and[31, 16]2-EDP が本研究の EDP 構成手法であり [31, 21]2-EDP が先行研究で示された EDP 構成手法による EDP である．古典理論には復号誤り率と符号化率の間にはトレードオフの関係がよくみられるが，復号誤り率を fidelity と対応付けるとそれは量子誤り訂正においても同じことが言える．しかし図を見ると [31, 21]2-EDP に対して本研究で示す EDP 構成手法は同じ符号を使って，両方の指標において優位性が見られる結果が得られている．

3.2　Fidelity の指数的下界を利用した評価

ここでは文献 [4] で示されている最良の量子誤り訂正符号を利用した時の fidelity に対する指数的下界 $E(R, P)$ を使い，各種 EDP を見ていく．具体的には EDP の $1-F$ に対して

$$1 - F \leq 2^{-nE(R,P)} \tag{8}$$

とすることで式中の右辺が最良の量子誤り訂正符号に対する $1-F$ の上界となり，EDP の $1-F$ がどれほどの符号長をもつ上界の限界性能に相当するかを見ていく．

図 5 はある R に対する各種 EDP の $1-F$ 及び $1-F$ の上界をプロットしたものである．プロットした EDP は [31, 21]2-EDP，[31, 16]2-EDP，[31, 21]and[31, 16]2-EDP である．また各 EDP のプロットに乗るような形で符号長 n を設定しプロットしている．シャノンによる通信路符号化定理は伝送速度を通信路容量よりも小さく保つことで符号長を長くすると任意に誤り率を小さくできることを示している．また同種の符号ならばより符号長の長い符号に高い性能が期待できる．これを考慮して図を見ると [31, 21]and[31, 16]2-EDP は他の EDP に対してより大きな n の

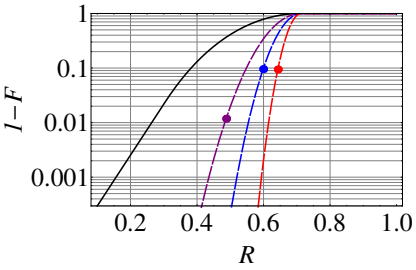

図 5　各 EDP のレート R に対する $1-F$ と $1-F$ の上界，$p = 0.05$，黒実線：$n = 31$ の $1-F$ 上界，紫破線：$n = 137$ の $1-F$ 上界，青破線：$n = 295$ の $1-F$ 上界，赤破線：$n = 795$ の $1-F$ 上界，紫点：[31, 16]2-EDP，青点：[31, 21]2-EDP，赤点：[31, 21]and[31, 16]2-EDP

$1-F$ の上界が示す限界性能に相当しており，その n の差だけ優位性があるといえる．この結果から符号を一つだけ利用して構成した EDP に対して，本手法を適用することでより高い性能を示すことができることがわかったと言える．

4　まとめ

本研究では複数の量子誤り訂正符号を利用した EDP 構成手法を示し，その評価を行った．結果としてその有効性を示すことができたと言えるが，扱ったのはほんの一部の符号に対してのみであり，今回の検証は一例を示したまでになると言える．また図 1 について，扱う符号によって集合 C が空集合になる可能性も考えられ，その C に要素が存在する条件を明らかにすることなどが今後の課題になる．

参考文献

[1] C. H. Bennett, *et al*., Phys. Rev. A54, pp.3824-3851, (1996).
[2] C. H. Bennett, *et al*., Phys. Rev. Lett. 70, pp.1895-1899, (1993).
[3] R. Matsumoto, J. Phys. A: Math. Gen., vol.36, no.29, pp.8113-8127, (2003).
[4] M. Hamada, Phys. Rev. A65, 052305, (2002).

公表論文

A) **D. Sasaki** and T. S. Usuda, Chennai, India, Extended Abstracts of AQIS2013, pp.191-192, (2013.8).
B) 佐々木大地, 臼田毅, 平成 25 年度電気関係学会東海支部連合大会, K2-6, (2013.9).
C) 佐々木大地, 臼田毅, SITA'14, 富山, pp.461-466, (2014.12).