量子誤り訂正とエンタングルメント純粋化[1]
Quantum Error-Correction and Entanglement Distillation

松本 隆太郎
Ryutaroh Matsumoto
〒 152-8552 東京工業大学 大学院理工学研究科 集積システム専攻
Dept. of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, 152-8552 Japan
Email: ryutaroh@rmatsumoto.org

Abstract 量子通信の様々な局面において空間的に離れた二者間で量子エンタングルメントを共有することが必要不可欠である. しかし, 二者間で利用できる通信路に雑音が有る場合単純にエンタングルメントを構成する系の片方を送ることではエンタングルメントの共有ができない. このように雑音の有る通信路しか利用できない場合でもエンタングルメントの共有を可能にする手法が量子誤り訂正符号と量子エンタングルメント純粋化プロトコルである. またエンタングルメント純粋化は高密度符号化の前処理として使うことで完全な秘話通信を実現できる点でも重要である. 本稿ではこれらの手法を量子通信で普通に用いる基礎的な量子論の知識だけを用いて解説する.

キーワード: 量子誤り訂正符号, エンタングルメント純粋化プロトコル, スタビライザー符号, 忠実度

1 前書き

量子テレポーテーション [2] や 量子高密度符号化 [4] などの量子通信の様々な手法において, 離れた二者間が量子エンタングルメントを共有することが必要不可欠である. もし雑音の無い通信路が利用できる場合エンタングルメントの片方を通信路を介して送ることにより, エンタングルメントの共有は容易に実現できる. しかし, 雑音のある通信路を用いて共有したエンタングルメントは一般にエンタングルメントの度合が低く, テレポーテーションや高密度符号化の性能に悪影響を及ぼす. 従って, 雑音のある通信路を用いて完全な量子エンタングルメントを共有する方法が求められていた. 通信路を介して共有したエンタングルメントから雑音の悪影響を取り除く代表的な手法が量子誤り訂正符号と量子エンタングルメント純粋化プロトコルである. また, エンタングルメント純粋化は高密度符号化の前処理として用いることで完全な秘話通信を実現できる点でも重要である. 本稿ではこれらの手法の目的, 問題設定, 具体的な実現方法について量子通信に使われる基本的な概念だけを用いて説明する. 本稿で説明しない基礎的概念は本特集の他の記事に解説があるはずである.

[1]電子情報通信学会誌 vol. 85, no. 8, pp. 591–595, Aug. 2002

2 量子誤り訂正符号

2.1 問題設定と目的

本小節の内容は図 1 で視覚的に要約されているので適宜参照していただきたい. 本稿では $\mathcal{H}$ は常に何らかの二準位系に対応する 2 次元複素線形空間とする. 量子誤り訂正符号の目的は k 個の二準位系の任意の未知の状態 $|\varphi\rangle \in \mathcal{H}^{\otimes k}$ を雑音のある通信路を介して送ることである. 状態 $|\varphi\rangle$ をそのまま送ると雑音による変化を元に戻すことができないので, n 個の二準位系の状態空間 $\mathcal{H}^{\otimes n}$ のある状態 $|\psi\rangle$ に $|\varphi\rangle$ を対応させて送る. この対応関係はユニタリ作用素で通常記述される. 従って送られる可能性のある符号語 $|\psi\rangle$ の集合は $\mathcal{H}^{\otimes n}$ の 2^k 次元線形部分空間 Q に含まれる. この Q を符号空間と呼ぶ.

さて次に $|\psi\rangle$ を通信路を介して送ることを考える. 通常の古典通信路では入力信号に対して出力信号の確率分布が定まり, この確率分布によって通信路は完全に記述される. 量子通信路も入力状態に対して出力状態の確率分布が定まる. 状態の確率分布は混合状態 (密度作用素) で記述され, また通信路に混合状態を入力することも可能なので, 結局量子通信路は混合状態から混合状態への写像として記述される. 但し任意の混合状態から混合状態への写像が量子通信路に対応する訳ではなく, 完全正写像 (CP 写像) と呼ばれる写像のクラスが有り得る量子通信路と一対一に対応するという仮説が現在広く受け入

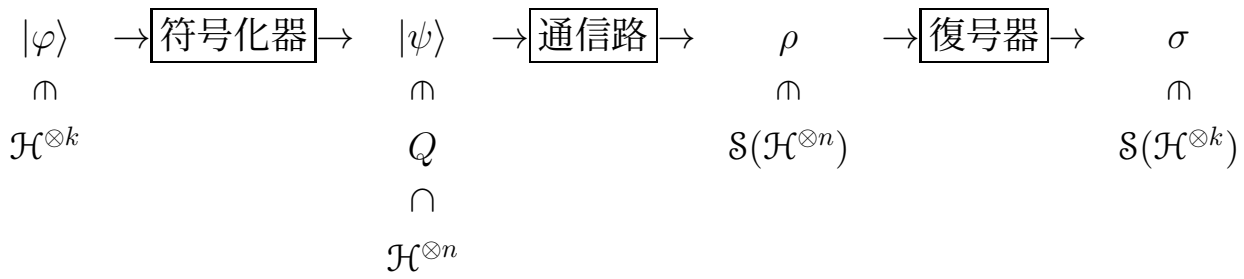

図 1: 量子誤り訂正の概念図: 純粋状態 $|\varphi\rangle$ を送りたい場合, まず符号化器により冗長性を付加する. 通信路を通って雑音が乗った状態 ρ を復号器でなるべく元の状態 $|\varphi\rangle$ に近い状態 σ に復元する. 但しここで $\mathcal{S}(\mathcal{H}^{\otimes n})$ は $\mathcal{H}^{\otimes n}$ 上の混合状態を表す.

れられている. この仮説は Holevo [8] により 1972 年に提唱された.

さて $|\psi\rangle$ を量子通信路を介して送り, $\mathcal{H}^{\otimes n}$ の混合状態 ρ が得られたとする. この状態 ρ を復号器で処理して状態 σ が得られたとする. 量子誤り訂正符号の目的は σ をなるべく $|\varphi\rangle$ に近くすることであるが, 量子状態は複素ベクトルまたは複素行列で表されある意味で連続的だから, 受信状態 σ が完全に送信状態 $|\varphi\rangle$ に一致することは稀である. そこで σ と $|\varphi\rangle$ の状態の近さを評価し, 状態が近ければ満足することにする.

このために状態の近さを評価する尺度が必要になるが, 量子誤り訂正符号で良く使われる尺度は Uhlmann [14] により提案され Jozsa [9] により様々な性質が明らかにされた忠実度 (fidelity) である. 純粋状態 $|\varphi\rangle$ と混合状態 σ の忠実度は

$$\langle\varphi|\sigma|\varphi\rangle \tag{1}$$

により定義される.

忠実度は以下のように解釈することができる. 観測量 $|\varphi\rangle\langle\varphi|$ を測定し結果 1 を得ることはある量子系が状態 $|\varphi\rangle$ にあるかどうか測定し系の状態が $|\varphi\rangle$ であるという結果を得ることに等しい. 忠実度 (1) は状態 σ にある系の観測量 $|\varphi\rangle\langle\varphi|$ を測定し結果 1 を得る確率に等しい. 従って σ が $|\varphi\rangle$ に近いほど忠実度が大きいと考えられる.

今までは純粋状態を送ることだけを考えて来たが, 前書きで述べた高密度符号化などに必要なエンタングルメントの共有ではエンタングルメントを構成する物理系の片方だけを送るので, 送信状態を $\mathcal{H}^{\otimes k}$ の純粋状態として表せない. しかし符号空間 Q の任意の純粋状態をある程度高い忠実度で送ることができる場合エンタングルメントを Q を用いて高い忠実度で送ることができることが知られているので [10], 純粋状態を送る場合に問題設定を限定しても差し支えない.

古典のブロック誤り訂正符号の性能評価は符号化率と最悪誤り確率によって行うことが多いが, 量子誤り訂正符号も同様に符号化率 k/n と最悪忠実度

$$\min_{\substack{|\varphi\rangle\in\mathcal{H}^{\otimes k}\\ \langle\varphi|\varphi\rangle=1}} \langle\varphi|\sigma|\varphi\rangle$$

によって性能評価を行うことが多い. 次の節では復号器をより具体的に紹介し, その後最悪忠実度の評価法を説明する.

2.2 具体的な復号法

図 1 において符号化器の実現は概念的には自明であろう. ただ $|\varphi\rangle$ に補助的な系を付加してユニタリ作用素を作用させるだけである. この節では復号法について見ていく.

復号の概略は以下の通りである: 受信者は受信状態 ρ にある系を測定してどのような誤りが生じたのか推測する. 測定により状態 ρ は別の状態 ρ' に変化する. 次に受信者は推測した誤りの逆作用素を ρ' に作用させる. 逆作用素を作用させた状態を ρ'' とすると, もし誤りを比較的良く推測していれば ρ'' は送信状態 $|\psi\rangle$ に近いはずである. その後 ρ'' に対し符号化の逆を行って σ を得る.

上記の手続きでまだ明らかでない点はどのような測定を行うかということと, 測定結果から生じた誤りを推定する部分である. これらの点についてこれから解説する.

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

という行列と

$$\mathcal{B} = \{M_1 \otimes \cdots \otimes M_n \,:\, M_i \in \{I, X, Y, Z\}\}$$

という集合を考える. X, Y, Z はユニタリ行列でかつエルミート行列である. 今 $\mathcal{B}$ の部分集合 $\mathcal{B}_{\rm c}$ が「もし M, $N \in \mathcal{B}_{\rm c}$ が $M \neq N$ ならば $MQ \perp NQ$ が成り立つ」という条件を満たしているとする. 但し「$MQ \perp NQ$」とはあらゆる $|\psi\rangle$, $|\psi'\rangle \in Q$ について $M|\psi\rangle$ と $N|\psi'\rangle$ が直交することを表す.

復号器は受信状態が $\mathcal{H}^{\otimes n}$ の混合状態 ρ であったときに以下のような復号手続きを実行する. まず $\{MQ : M \in \mathcal{B}_{\rm c}\}$ を固有空間とするような観測量を測定し, 測定後の混合状態を ρ' とする. もしある $M \in \mathcal{B}_{\rm c}$ について ρ' が MQ に属する状態の混合として表せるならば $M^{-1}\rho'(M^{-1})^\dagger$ を復号後の状態とする.

以上の復号手続きから $\mathcal{B}_c$ に属するユニタリ行列が誤りとして生じた場合には完全に送信状態を復元できることがわかる．しかし実際に起きる誤りは $\mathcal{B}_c$ の要素として表せない場合がほとんどである．2.1 節で述べたように量子通信路は完全正写像を用いて記述される．量子通信路の完全正写像から上に述べた復号手続きによる最悪忠実度の下界を評価する方法を次に述べる．

2.3 最悪忠実度の評価

量子通信路を記述する完全正写像とは大雑把に言えば $\mathcal{H}^{\otimes n}$ 上の混合状態の集合 $\mathcal{S}(\mathcal{H}^{\otimes n})$ からそれ自身への線形写像である．通信路を記述する写像を $\Gamma_n : \mathcal{S}(\mathcal{H}^{\otimes n}) \to \mathcal{S}(\mathcal{H}^{\otimes n})$ とすると式 (2) で表されるように Γ_n は通信路と環境の相互作用の通信路の部分だけに注目したものと見なすことができる．ある 2^{2n} 次元線形空間 $\mathcal{H}_n$, 長さ 1 のベクトル $|e_n\rangle \in \mathcal{H}_n$, $\mathcal{H}^{\otimes n} \otimes \mathcal{H}_n$ のユニタリ作用素 U_n が存在して

$$\Gamma_n(\rho) = \mathrm{Tr}_{\mathcal{H}_n}[U_n(\rho \otimes |e_n\rangle\langle e_n|)U_n^\dagger] \tag{2}$$

がすべての $\rho \in \mathcal{S}(\mathcal{H}^{\otimes n})$ について成り立つことが知られている．但し $\mathrm{Tr}_{\mathcal{H}_n}$ は $\mathcal{H}_n$ 上の部分トレースを取ることを表している．

以上のような通信路の表現を用いて最悪忠実度の下界を求めることができる．$\mathcal{H}^{\otimes n}$ 上の線形作用素全体は線形空間をなすが, 集合 $\mathcal{B}$ はこの線形空間の基底になっている．従って式 (2) の U_n を

$$U_n = \sum_{M \in \mathcal{B}} M \otimes L_M$$

と展開することができる．但し L_M は $\mathcal{H}_n$ 上の線形作用素である．Preskill は [12] の 7.4 節で, $|\psi\rangle \in Q$ を送り復号後の状態が $\mathcal{H}^{\otimes n}$ の混合状態 ρ'' であったときの $|\psi\rangle$ と ρ'' の忠実度が

$$1 - \left\| \sum_{M \in \mathcal{B} \setminus \mathcal{B}_c} M|\psi\rangle \otimes L_M|e_n\rangle \right\|^2 \tag{3}$$

以上であることを明らかにしている．但し $\mathcal{B} \setminus \mathcal{B}_c$ は $\mathcal{B}$ の要素で $\mathcal{B}_c$ に属さないものからなる集合である．

2.4 無記憶通信路と t 誤り訂正

古典の誤り率 p の二元対称通信路において符号長 n の二元線形ブロック符号を用いて誤り訂正を行う場合, もし t 個までの誤りを用いる符号が訂正できるならば正しく復号できる確率は

$$1 - \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

以上であることが良く知られている．このため二元対称通信路では誤り確率の代わりに訂正可能誤り数 t を符号の性能の指標として用いることができる．量子誤り訂正符号においても, 同様に無記憶通信路と呼ばれる通信路のクラスでは訂正可能誤り数によって最悪忠実度の下界が定まることを紹介する．

通信路を表す完全正写像 $\Gamma_n : \mathcal{S}(\mathcal{H}^{\otimes n}) \to \mathcal{S}(\mathcal{H}^{\otimes n})$ がある $\mathcal{S}(\mathcal{H})$ の完全正写像 $\Gamma_1 : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ が存在して

$$\Gamma_n = \Gamma_1^{\otimes n}$$

と表せるならば, その通信路は無記憶であると言われる．また行列

$$M_1 \otimes M_2 \otimes \cdots \otimes M_n \in \mathcal{B}$$

の重みを $M_i \neq I$ であるような添え字 i の数とする．$\mathcal{B}$ の重みが t 以下の行列がすべて $\mathcal{B}_c$ に含まれるときに, 符号 Q は t 誤り訂正可能であると言う．訂正可能誤り数 t と最悪忠実度の間には以下のような関係がある．

まず, ある 4 次元線形空間 $\mathcal{H}_1$, $|e_1\rangle \in \mathcal{H}_1$, $\mathcal{H} \otimes \mathcal{H}_1$ 上のユニタリ作用素 U_1 を用いて

$$\Gamma_1(\rho) = \mathrm{Tr}_{\mathcal{H}_1}[U_1(\rho \otimes |e_1\rangle\langle e_1|)U_1^\dagger]$$

と Γ_1 を表す．次に, $\{I, X, Y, Z\}$ は $\mathcal{H}$ の線形作用素からなる線形空間の基底をなすから, U_1 を

$$U_1 = I \otimes L_I + X \otimes L_X + Y \otimes L_Y + Z \otimes L_Z$$

と展開することができる．但し $L_?$ は $\mathcal{H}_1$ の線形作用素である．ここで

$$p = \|L_X|e_1\rangle\| + \|L_Y|e_1\rangle\| + \|L_Z|e_1\rangle\|$$

とおくと, $|\psi\rangle \in Q$ を送ったときの $|\psi\rangle$ と復号後の混合状態の間の忠実度は少なくとも

$$1 - \left[\sum_{i=t+1}^{n} \binom{n}{i} p^i \right]^2$$

であることが, 式 (3) から導くことができる．

2.5 代数的な量子誤り訂正符号の構成法

今まで量子誤り訂正符号の一般的な枠組みを述べてきたが, 具体的な符号の構成法には触れなかった．この節では Gottesman [7] および Calderbank ら [5, 6] によって独立に提案されたスタビライザー符号について紹介する．スタビライザー符号は現在知られている量子誤り訂正符号の構成法で最も一般的なもので, 今まで発見された符号のほとんどすべてがスタビライザー符号として構成できる．

まず前節で導入した行列の集合 $\mathcal{B}$ によって生成される非可換群 E を考える．具体的には

$$E = \{\pm M, \pm iM : M \in \mathcal{B}\}$$

である．ここで E の群演算として行列の乗算を考えている．次に E の可換部分群 S を考える．ここで符号空間 Q として各々の行列 $M \in S$ のある一つの固有空間の共通集合として得られる $\{\vec{0}\}$ ではない線形空間を考える．各々の行列 M のどの固有空間の共通部分を取るかによって Q は異なるが, いつでも Q の次元は同じで式 (4) で与えられる．

一応符号空間の定義ができたので, これから符号化率および復号手続きについて考える．非可換群 E の中で S のどの行列とも可換な行列からなる集合

$S' = \{M \in E : \text{すべての } N \in S \text{ について } MN = NM\}$

を考える．集合 S' の要素数は常に 2 のべき乗になることが示せるが, S' の要素数が 2^{n+k+2} であるならば

$$\dim Q = 2^k \tag{4}$$

である. 従って k 個の $\mathcal{H}$ で表される二準位系を n 個の二準位系に符号化するので符号化率は k/n である.

次に復号手続きについて述べる. 二つの行列 $M, N \in E$ が有るとき, 常に $MQ = NQ$ または $MQ \perp NQ$ のどちらかが必ず成り立つ. また集合

$$\{MQ : M \in E\} \tag{5}$$

は $\mathcal{H}^{\otimes n}$ の直交分解になっているので, 式 (5) と同じ固有空間を持つ $\mathcal{H}^{\otimes n}$ の観測量を考えることができる. 受信状態が $\mathcal{H}^{\otimes n}$ の混合状態 ρ であった場合, まず式 (5) から定まる観測量を測定する. 測定後の状態を ρ' とし ρ' がある観測量の固有空間 Q' の状態の混合で表せるとする. このとき生じた誤りが $\mathcal{B}$ の要素として表せるという仮定の下で, 生じた誤りは集合

$$\{M \in \mathcal{B} : MQ = Q'\} \tag{6}$$

の要素のどれかである. 受信者が持っている通信路に関する知識から集合 (6) の中で最も有り得そうな誤り M_E を決定し, $M_E^{-1}\rho'(M_E^{-1})^\dagger$ を復号後の状態とする.

もし通信路が無記憶である種の対称性がある場合, 集合 (6) の中で最も重みが小さい行列を M_E とすると忠実度が最も大きくなる. これは古典の二元対称通信路で最小距離復号が最尤復号になることに対応している.

この節で紹介したことだけでは良い符号を構成するために可換部分群 S をどのように選べばよいのかまったくわからない. 実は良い可換部分群 S の構成には古典符号を構成するための代数的符号理論が威力を発揮するが, その話題は次の浜田充氏の記事で解説されるはずなのでここでは紹介しない.

3 量子エンタングルメント純粋化プロトコル

今まで量子誤り訂正符号について紹介してきたが, この節では量子誤り訂正符号と並び雑音のある通信路を介してエンタングルメントを共有するための代表的手法である, Bennett ら [3] により提案された量子エンタングルメント純粋化プロトコル (entanglement purification protocol または entanglement distillation protocol) について説明する. 最初に問題設定と目的を説明し, 次に 2.5 節で紹介したスタビライザー符号を用いてエンタングルメント純粋化プロトコルを構成する方法について述べる.

3.1 問題設定と目的

$\mathcal{H}_A$, $\mathcal{H}_B$ を 2 次元線形空間とする. 今 Alice と Bob という空間的に離れた人または装置があるとし, Alice は $\mathcal{H}_A^{\otimes n}$ で表される n 個の二準位系を所有し, Bob は $\mathcal{H}_B^{\otimes n}$ で表される n 個の二準位系を所有しているとする. $\{|0_A\rangle, |1_A\rangle\}$ を $\mathcal{H}_A$ の正規直交基底とし, $\{|0_B\rangle, |1_B\rangle\}$ を $\mathcal{H}_B$ の正規直交基底とする.

高密度符号化やテレポーテーションを行うためには Alice と Bob の系を

$$\frac{|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle}{\sqrt{2}} \tag{7}$$

という状態に準備する必要がある. もし Alice と Bob の間に雑音の無い通信路が存在する場合には Alice または Bob が 2 つの二準位系にまたがる状態 (7) を準備して片方の二準位系を相手に送ればよい. しかし現実には通信路に雑音があるので, 通信路を通った後の状態は $\mathcal{H}_A \otimes \mathcal{H}_B$ の混合状態になる. 一般に n 個の状態 (7) を準備した後 n 個の二準位系を送った場合には $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ の混合状態 ρ を共有することになる.

共有している混合状態 ρ からなるべく多くの (7) に近い状態を取り出したいが, Alice と Bob は空間的に離れているので可能な操作は

- Alice が所有している $\mathcal{H}_A^{\otimes n}$ で表される系への操作・測定
- Bob が所有している $\mathcal{H}_B^{\otimes n}$ で表される系への操作・測定
- Alice または Bob による測定結果の古典的通信路を介した相手への伝達

に限られる. エンタングルメント純粋化プロトコルとは上記の限られた操作だけを用いて ρ から状態 (7) に近い状態を取り出すための手法の総称である.

3.2 スタビライザー符号を用いた構成法

Bennett ら [1] が早くから量子誤り訂正符号とエンタングルメント純粋化プロトコルの関係を論じていたが, これから述べるように量子誤り訂正符号から直接エンタングルメント純粋化プロトコルを構成する方法を示したのは Shor と Preskill [13] が最初である. Shor らはいわゆる CSS 符号から構成する方法だけを具体的に記述したが, 彼らの方法をスタビライザー符号に拡張することは自明で, [11] の 12 章にもスタビライザー符号を用いたエンタングルメント純粋化プロトコルの構成法が書いてある.

説明を短くするために問題設定をかなり簡略化する. まず Alice は状態 (7) を n 個準備し, 状態が $\mathcal{H}_B^{\otimes n}$ で表される n 個の二準位系を Bob に送る. このとき Alice は $\mathcal{H}_A^{\otimes n}$ のベクトルで表される送らなかった n 個の二準位系を手元に持っている. ここで通信路は $\mathcal{B}$ の要素がある確率で誤りとして生じるような簡単なものを考える. Alice と Bob は 2.5 節で導入したスタビライザー S から定まるプロトコルを以下のように実行する.

まず Alice は 2.5 節で述べた S から定まる観測量を測定する. このとき状態が $Q \subset \mathcal{H}_A^{\otimes n}$ に射影されたとする. もし通信路で誤りが全く生じていない場合は Alice と Bob の系全体の状態は

$$Q \otimes Q \subset \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$$

という部分空間に射影される. 従ってもし誤り $M \in \mathcal{B}$

が生じた場合は系全体の状態は

$$Q \otimes MQ \subset \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$$

に射影される

Alice は測定結果を古典通信路を介して Bob に通知する. Bob も 2.5 節で述べた S から定まる観測量を測定する. Bob の測定結果は状態が Q' に射影されたことを示していたとすると, Bob と Alice の測定結果の違いから生じた誤りは集合 (6) の中のどれかであることが Bob にわかる. Bob は有り得る誤りの中で通信路の特性からもっとも有りそうな誤りの逆行列を Bob が持っている $\mathcal{H}_B^{\otimes n}$ で表される n 個の二準位系に適用する.

Bob が生じた誤りを正しく推測した場合には, $\mathcal{H}^{\otimes k}$ の状態を Q に符号化する操作を逆転させることにより Alice と Bob は k 個の状態 (7) を共有することができる. 但しここで k は式 (4) と同じである.

また Bob は測定結果の違いと通信路の特性から生じた誤りの推測がどの程度の確率でうまく行くか計算できる. もしうまく行く確率が小さい場合には Alice にプロトコルのやり直しを通知することができる. Bennett ら [3] が最初に提案した recurrence プロトコルはこの節で述べたプロトコルでスタビライザーを $S = \{Z \otimes Z, I \otimes I\}$ と取り, 測定結果が一致しない場合にプロトコルのやり直しを行うものと等価である.

この節ではプロトコルを適用する状況をかなり限定した. 一般の $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ の混合状態は twirling と呼ばれる操作を行うと Werner 状態と呼ばれる状態に変換される. Werner 状態は, この節で仮定したように状態 (7) を $\mathcal{B}$ の要素だけが確率的に誤りとして生じる通信路を通して得られた出力状態と見なすことができる. 従って一般的な $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ の混合状態が最初に与えられている場合でも, twirling を前処理として行うことによりこの節で述べた特殊な状況に帰着できる. twirling や Werner 状態は [15] によくまとめられている.

文献

[1] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A, vol.54, no.5, pp.3824–3851, Nov. 1996.

[2] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett., vol.70, no.13, pp.1895–1899, March 1993.

[3] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," Phys. Rev. Lett., vol.76, no.5, pp.722–725, Jan. 1996.

[4] C.H. Bennett and S.J. Wiesner, "Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states," Phys. Rev. Lett., vol.69, no.20, pp.2881–2884, Nov. 1992.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett., vol.78, no.3, pp.405–408, Jan. 1997.

[6] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inform. Theory, vol.44, no.4, pp.1369–1387, July 1998.

[7] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," Phys. Rev. A, vol.54, no.3, pp.1862–1868, Sept. 1996.

[8] A.S. Holevo, "On the mathematical theory of quantum communication channels," Problemy Peredachi Informatsii, vol.8, no.1, pp.62–71, March 1972 (ロシア語; 英訳は Problems of Information Transmission, vol.8, no.1, pp.47–54, March 1974).

[9] R. Jozsa, "Fidelity for mixed quantum state," J. Modern Opt., vol.41, no.12, pp.2315–2323, 1994.

[10] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A, vol.55, no.2, pp.900–911, Feb. 1997.

[11] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, UK, 2000.

[12] J. Preskill, "Lecture Notes for Physics 229: Quantum Information and Computation," `http://www.theory.caltech.edu/people/preskill/ph229` , 1998.

[13] P.W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol.85, no.2, pp.441–444, July 2000.

[14] A. Uhlmann, "The 'transition probability' in the state space of a $*$-algebra," Rep. Math. Phys., vol.9, no.2, pp.273–279, April 1976.

[15] K.G. Vollbrecht and R.F. Werner, "Entanglement measures under symmetry," Phys. Rev. A, vol.64, no.6, p.062307, Dec. 2001.