量子純粋状態の情報源符号化の指数評価

林 正人

理化学研究所 脳科学総合研究センター 脳数理研究チーム
〒 351-0198 埼玉県和光市広沢 2-1
Tel: 048-467-9664 Fax:048-467-9693
e-mail masahito@brain.riken.go.jp

あらまし: 量子純粋状態からなる無記憶情報源に対して,visible 及び blind の双方の場合について固定長符号化を施した場合の復号化の際の誤り確率が 0 に近づく指数の最適値を求めた. さらに, エントロピーレートを超えた際の正しく復号化される確率が 0 に近づく指数についても評価した.

キーワード: 量子純粋状態の情報源符号化, Rény エントロピー, Visible coding, Blind coding

Exponents of quantum pure state source coding

Masahito Hayashi

Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN
2-1 Hirosawa, Wako, Saitama, 351-0198, Japan
Tel: +81-48-467-9664 Fax: +81-48-467-9693
e-mail masahito@brain.riken.go.jp

Abstract: We calculate the optimal exponent of the error probability of the fixed lenghth quantum pure state source coding in the cases of the blind oding and the visible coding. We evaluate the optimal exponent of the correct probability in the both cases.

Key Words: quantum pure state source coding, Rény entropy, Visible coding, Blind coding

1 はじめに

量子状態からなる情報源圧縮は, 量子コンピューターのメモリの節約には必要となると思われる. 本稿では,Schumacher により始められた, 情報源が量子純粋状態からなる場合の情報源圧縮を扱う. 各 $i \in \Xi$ で指定された表現空間 $\mathcal{H}$ 上の個々の情報源 ρ_i が確率 p_i で生成されるとする. 以下では各状態 ρ_i が純粋状態である場合のみ扱うことにする. $\mathcal{S}(\mathcal{H}), \mathcal{S}_p(\mathcal{H})$ でそれぞれ, 純粋状態を含めた密度作用素の集合, 純粋状態の集合を表すとする. 情報源を $\{\rho_i, p_i\}_{i\in\Xi}$ で表すことにする. このとき, 情報源圧縮は Hilbert 空間 $\mathcal{K}$ と $\mathcal{S}(\mathcal{H})$ から $\mathcal{S}(\mathcal{K})$ への CP map E と $\mathcal{S}(\mathcal{K})$ から $\mathcal{S}(\mathcal{H})$ への CP map D の組 $(\mathcal{K}, E, D)$ で記述され, その復号化の精度は $\mathcal{E}(E,D) := \sum_{i\in\Xi} p_i(\mathrm{I} - \mathrm{Tr}\, D \circ E(\rho_i))\rho_i$ で与えられる. この問題は以下の問題と区別するため, Blind coding とよばれる. Blind coding は $\dim\mathcal{K}$ と $\mathcal{E}(E,D)$ をともに減少させる trade-off として特徴付けられる.

Blind coding に対して, Visible coding という問題も考えることができる. この問題は,Blind coding を解析する上で有用でなおかつ, Blind coding よりも理論的な扱いが容易なので重要である. Visible coding は Hilbert 空間 $\mathcal{K}$ と Ξ から $\mathcal{S}(\mathcal{K})$ への写像 F と $\mathcal{S}(\mathcal{K})$ から $\mathcal{S}(\mathcal{H})$ への CP map D の組 $(\mathcal{K}, F, D)$ で記述され, その復号化の精度は $\mathcal{F}(F,D) := \sum_{i\in\Xi} p_i\,\mathrm{Tr}(\mathrm{I} - D\circ F(i))\rho_i$ で与えられる. Visible coding は $\dim\mathcal{K}$ と $\mathcal{F}(F,D)$ をともに減少させる trade-off として特徴付けられる. Visible coding の場合 情報源 $\{\rho_i, p_i\}_{i\in\Xi}$ は情報源を与えているというよりも問題の規範を与えているという感じの方が強い. Blind coding $(\mathcal{K}, E, D)$ は $F(i) := E(\rho_i)$ とすることにより, Visible coding と見ることができる. 逆は不可能で,Visible coding の方がより広い選択肢を考えていることになる. 以下 E を Blind encoder F を Visible eoncoder D を decoder とよぶことにする. 量子暗号に関しては Blind encoder よりも Visible encoder の方が関連が深いとの指摘もある.[14]

情報源 $\{\rho_i, p_i\}_{i\in\Xi}$ が n 個独立に現れている状況を考える. この場合表現空間はテンソル積空間 $\mathcal{H}^{\otimes n}$ になり, 状態 $\rho_{n,\vec{i}_n} := \rho_{i_1}\otimes\rho_{i_2}\otimes\cdots\otimes\rho_{i_n}$, $\vec{i}_n = (i_1, i_2, \ldots, i_n)$ が確率 $p_{n,\vec{i}_n} := p_{i_1}p_{i_2}\cdots p_{i_n}$ で生成するとする. すなわち $\{\rho_{n,\vec{i}_n}, p_{n,\vec{i}_n}\}_{\vec{i}_n\in\Xi^n}$ で表される情報源を考える. $\{\rho_i, p_i\}_{i\in\Xi}$ の 離散無記憶情報源 (DMS) とよぶことにする.

$\{\rho_i, p_i\}_{i\in\Xi}$ の DMS の Blind coding 及び Visible coding についての最小許容固定長符号化レート $R_B(\{\rho_i,p_i\}_{i\in\Xi})$, $R_V(\{\rho_i,p_i\}_{i\in\Xi})$ 及び強逆最小許容固定長符号化レート $R_B^-(\{\rho_i,p_i\}_{i\in\Xi}), R_V^-(\{\rho_i,p_i\}_{i\in\Xi})$ はそれぞれ,

$$R_B(\{\rho_i,p_i\}_{i\in\Xi}) := \inf\left\{\overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n \mid \exists\{(\mathcal{K}_n, E_n, D_n)\}, \mathcal{E}(E_n,D_n)\to 0\right\}$$

$$R_V(\{\rho_i,p_i\}_{i\in\Xi}) := \inf\left\{\overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n \,\middle|\, \exists\{(\mathcal{K}_n, F_n, D_n)\}, \mathcal{F}(F_n,D_n)\to 0\right\}$$

$$R_B^-(\{\rho_i,p_i\}_{i\in\Xi}) := \inf\left\{\overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n \,\middle|\, \exists\{(\mathcal{K}_n, E_n, D_n)\}, \overline{\lim}\,\mathcal{E}(E_n,D_n) < 1\right\}$$

$$R_V^-(\{\rho_i,p_i\}_{i\in\Xi}) := \inf\left\{\overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n \,\middle|\, \exists\{(\mathcal{K}_n, F_n, D_n)\}, \overline{\lim}\,\mathcal{F}(F_n,D_n) < 1\right\}$$

で定義される. そしてこれらについては以下の定理が成り立つ.

定理 1 $\rho := \sum_{i\in\Xi} p_i\rho_i$ とし, エントロピー $H(\rho)$ を $-\mathrm{Tr}\,\rho\log\rho$ とすると, 以下の式が成り立つ.

$$\begin{aligned} &R_B(\{\rho_i,p_i\}_{i\in\Xi}) = R_V(\{\rho_i,p_i\}_{i\in\Xi}) = R_B^-(\{\rho_i,p_i\}_{i\in\Xi}) \\ &= R_V^-(\{\rho_i,p_i\}_{i\in\Xi}) = H(\rho) \end{aligned} \tag{1}$$

自明な関係式として

$$\begin{aligned} R_B(\{\rho_i,p_i\}_{i\in\Xi}) &\geq R_V(\{\rho_i,p_i\}_{i\in\Xi}), \\ R_B^-(\{\rho_i,p_i\}_{i\in\Xi}) &\geq R_V^-(\{\rho_i,p_i\}_{i\in\Xi}), \\ R_B(\{\rho_i,p_i\}_{i\in\Xi}) &\geq R_B^-(\{\rho_i,p_i\}_{i\in\Xi}), \\ R_V(\{\rho_i,p_i\}_{i\in\Xi}) &\geq R_V^-(\{\rho_i,p_i\}_{i\in\Xi}) \end{aligned}$$

が成り立つので,(1) を示すには

$$R_B(\{\rho_i,p_i\}_{i\in\Xi}) \leq H(\rho), \quad R_V^-(\{\rho_i,p_i\}_{i\in\Xi}) \geq H(\rho)$$

が示されれば十分である. 歴史的には Schumacher[1] により Direct part である $R_B(\{\rho_i,p_i\}_{i\in\Xi}) \leq H(\rho)$ が示され,Jozsa-Schumacher[2] によりその証明の簡略化がなされた. Barnum et al [3] により Converse part である $R_B(\{\rho_i,p_i\}_{i\in\Xi}) \geq H(\rho)$ が示され, M. Horodecki[4] によりその証明が簡略化された. M. Horodecki[4] の簡略化された証明は $R_V(\{\rho_i,p_i\}_{i\in\Xi}) \geq H(\rho)$ にも適用できる. さらに Winter[5] により, $R_V^-(\{\rho_i,p_i\}_{i\in\Xi}) \geq H(\rho)$ が示され, 上記の定理 1 が示された.

以下のように信頼性関数 $R_{e,B}(R|\{\rho_i,p_i\}_{i\in\Xi})$, $R_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi})$ 及びを逆信頼性関数 $R_{e,B}^*(R|\{\rho_i,p_i\}_{i\in\Xi})$, $R_{e,V}^*(R|\{\rho_i,p_i\}_{i\in\Xi})$ を

$$R_{e,B}(R|\{\rho_i,p_i\}_{i\in\Xi}) :=$$
$$\sup\left\{\underline{\lim}\,\frac{-1}{n}\log\mathcal{E}(E_n,D_n)\;\middle|\;\begin{array}{l}\exists\{(\mathcal{K}_n,E_n,D_n)\},\\ \overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n\le R\end{array}\right\}$$
$$R_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi}) :=$$
$$\sup\left\{\underline{\lim}\,\frac{-1}{n}\log\mathcal{F}(F_n,D_n)\;\middle|\;\begin{array}{l}\exists\{(\mathcal{K}_n,F_n,D_n)\},\\ \overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n\le R\end{array}\right\}$$
$$R^*_{e,B}(R|\{\rho_i,p_i\}_{i\in\Xi}) :=$$
$$\inf\left\{\overline{\lim}\,\frac{-1}{n}\log(1-\mathcal{E}(E_n,D_n))\;\middle|\;\begin{array}{l}\exists\{(\mathcal{K}_n,E_n,D_n)\},\\ \overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n\le R\end{array}\right\}$$
$$R^*_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi}) :=$$
$$\inf\left\{\overline{\lim}\,\frac{-1}{n}\log(1-\mathcal{F}(F_n,D_n))\;\middle|\;\begin{array}{l}\exists\{(\mathcal{K}_n,F_n,D_n)\},\\ \overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n\le R\end{array}\right\}$$

で定義する. これらについては以下の定理が成立する.

定理 2 $\rho:=\sum_{i\in\Xi}p_i\rho_i$ とし, *Rény* エントロピー $\psi(s)$ を $\log\mathrm{Tr}\,\rho^s$ で定義すると,

$$R_{e,B}(R|\{\rho_i,p_i\}_{i\in\Xi}) = R_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi}) \tag{2}$$
$$= \max_{0\le s\le 1}\frac{(1-s)R-\psi(s)}{s} \tag{3}$$
$$= \min\{D(\sigma\|\rho)|H(\sigma)\ge R\} \tag{4}$$
$$R^*_{e,B}(R|\{\rho_i,p_i\}_{i\in\Xi}) \ge R^*_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi}) \tag{5}$$
$$= \max_{s\ge 1}\frac{(1-s)R-\psi(s)}{s} \tag{6}$$
$$= \min\{D(\sigma\|\rho)|H(\sigma)\le R\} \tag{7}$$

となる. また, 不等式 *(5)* は自明. $D(\sigma\|\rho)$ は相対エントロピー $\mathrm{Tr}\,\sigma(\log\sigma-\log\rho)$ を表す.

不等式 $R_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi})\ge\min\{D(\sigma\|\rho)|H(\sigma)\le R\}$ は Winter [5] により既に示されている.

2 基本的な不等式

エルミート行列 X のスペクトル分解を $\sum_j s_jE_j$ としたとき,(s_j は固有値 E_j は射影.) 射影 $\{X\ge 0\},\{X<0\}$ をそれぞれ

$$\{X\ge 0\}=\sum_{s_j\ge 0}E_j,\quad \{X<0\}=\sum_{s_j<0}E_j \tag{8}$$

で定義する. 情報源 $\{\rho_i,p_i\}_{i\in\Xi}$ の Visible coding $(\mathcal{K},E,D)$ ついて以下の補題が成立する.

補題 3 $\forall\lambda\in\mathbb{R}$ に対して,

$$\mathcal{F}(F,D)+e^{\lambda}\dim\mathcal{K}\ge\mathrm{Tr}\,\rho\{\rho-e^{\lambda}<0\} \tag{9}$$
$$1-\mathcal{F}(F,D)\le e^{\lambda}\dim\mathcal{K}+\mathrm{Tr}\,\rho\{\rho-e^{\lambda}\ge 0\} \tag{10}$$

が成立する. さらに $\forall\lambda\in\mathbb{R},\forall s\ge 1$ に対して,

$$1-\mathcal{F}(F,D)\le e^{\lambda}\dim\mathcal{K}+e^{(1-s)\lambda+\psi(s)} \tag{11}$$

が成立する.

証明のために, 2 つの定義及び 2 つの補題を準備する. visible encoder F が任意の $i\in\Xi$ に対して $F(i)$ が純粋状態であるとき F は純粋状態 encoder と呼ぶ. 復号化 D に対して以下の条件を満たす適当な Hilbert 空間 $\mathcal{H}'$ が存在するとき, 準埋め込み復号化とよぶ: $\mathcal{S}(\mathcal{K})$ から $\mathcal{S}(\mathcal{H})$ への CP 写像 D が $\mathcal{S}(\mathcal{K})$ から $\mathcal{S}(\mathcal{H}\otimes\mathcal{H}')$ への等長埋め込みと $\mathcal{S}(\mathcal{H}\otimes\mathcal{H}')$ から $\mathcal{S}(\mathcal{H})$ への partial trace の合成写像として書ける. このとき以下の補題が成立する.

補題 4 任意の *visible encoder* F は有限個の純粋状態 *encoder* の確率的重ねあわせで書ける.

証明 $F(i)=\sum_{j_i}s_{j_i}|\phi_{j_i}\rangle\langle\phi_{j_i}|$ としたとき, 純粋状態 encoder $F(j_1,j_2,\dots,j_n)$ を $F(j_1,j_2,\dots,j_n|i)=|\phi_{j_i}\rangle\langle\phi_{j_i}|$ で定義すると $F=\sum_{j_1,j_2,\dots,j_n}s_{j_1}s_{j_2}\cdots s_{j_n}F(j_1,j_2,\cdots,j_n)$ となり題意が示せる. ■

補題 5 任意の D は有限個の準埋め込み復号化の確率的重ねあわせで書ける.

証明 Steinspring 表現より適当な有限次元 Hilbert 空間 $\mathcal{K}'$ と $\mathcal{K}\otimes\mathcal{K}'\otimes\mathcal{H}$ 上のユニタリ行列 U と $\rho_0\in\mathcal{S}(\mathcal{K}'\otimes\mathcal{H})$ が取れて, 以下の条件が満たされる.

$$D(\rho)=\mathrm{Tr}_{\mathcal{K}\otimes\mathcal{K}'}U\rho\otimes\rho_0U^*,\quad\forall\rho\in\mathcal{S}(\mathcal{K}) \tag{12}$$

$\rho_0=\sum_j s_j|\phi_j\rangle\langle\phi_j|$ とすると D_j を

$$D_j(\rho)=\mathrm{Tr}_{\mathcal{K}\otimes\mathcal{K}'}U\rho\otimes|\phi_j\rangle\langle\phi_j|U^*,\quad\forall\rho\in\mathcal{S}(\mathcal{K}) \tag{13}$$

と定義すると D_j は準埋め込み復号化となり, $D=\sum_j s_jD_j$ となる. ■

2.1 補題 3 の証明

補題 4,5 より, 純粋状態 encoder F と準埋め込み復号化 D の組について補題を示せば十分である. Hilbert 空間 $\mathcal{H}'$ を $D(\rho)=\mathrm{Tr}_{\mathcal{H}'}T(\rho)$ となるようにとる. ただし, T は $\mathcal{S}(\mathcal{K})$ から $\mathcal{S}(\mathcal{H}\otimes\mathcal{H}')$ への等長埋め込みとする. このとき $\rho'_i:=\frac{\rho_i\otimes\mathrm{I}\,T(F(i))\rho_i\otimes\mathrm{I}}{\mathrm{Tr}\,T(F(i))\rho_i\otimes\mathrm{I}}\in\mathcal{S}(\mathcal{H}\otimes\mathcal{H}')$ とすると, ρ'_i は純粋状態で, $\mathrm{Tr}\,D(F(i))\rho_i=\mathrm{Tr}\,T(F(i))\rho_i\otimes\mathrm{I}=\mathrm{Tr}\,T(F(i))\rho'_i$ となる. ここで純粋状態 $\sigma_i\in\mathcal{S}(\mathcal{H}')$ を取ると,$\rho'_i=\rho_i\otimes\sigma_i$ となり, $\rho':=\sum_{i\in\Xi}p_i\rho'_i=\sum_{i\in\Xi}p_i\rho_i\otimes\sigma_i$ は Separable である. $\rho=\mathrm{Tr}_{\mathcal{H}'}\rho'$ であるから, Nielsen-Kempe の補題 [6] より,

$$\mathrm{Tr}\,\rho\{\rho-e^{\lambda}\ge 0\}\ge\mathrm{Tr}\,\rho'\{\rho'-e^{\lambda}\ge 0\} \tag{14}$$

となる．さらに $\mathrm{I} \geq F(i)$ より $T(\mathrm{I}) \geq T(F(i))$ となることから，

$$\sum_{i\in\Xi} p_i \operatorname{Tr} D(F(i))\rho_i = \sum_{i\in\Xi} p_i \operatorname{Tr} T(F(i))\rho'_i$$
$$\leq \sum_{i\in\Xi} p_i \operatorname{Tr} T(\mathrm{I})\rho'_i = \operatorname{Tr} T(\mathrm{I})\rho' \tag{15}$$

が成り立つ．さらに $\mathrm{I} \geq T(\mathrm{I}) \geq 0$ より

$$\operatorname{Tr}(\rho' - e^{\lambda})T(\mathrm{I}) \leq \operatorname{Tr}(\rho' - e^{\lambda})\{\rho' - e^{\lambda} \geq 0\}$$
$$\operatorname{Tr}\rho' T(\mathrm{I}) + e^{\lambda}\operatorname{Tr}\{\rho' - e^{\lambda} \geq 0\}$$
$$\leq e^{\lambda}\operatorname{Tr} T(\mathrm{I}) + \operatorname{Tr}\rho'\{\rho' - e^{\lambda} \geq 0\}$$

となる．$\operatorname{Tr} T(\mathrm{I}) = \operatorname{Tr}\mathrm{I}_{\mathcal{K}} = \dim\mathcal{K}$ であるから，(14),(15) より，

$$1 - \mathcal{F}(F, D) = \sum_{i\in\Xi} p_i \operatorname{Tr} D(F(i))\rho_i$$
$$\leq e^{\lambda}\dim\mathcal{K} + \operatorname{Tr}\rho\{\rho - e^{\lambda} \geq 0\}$$

となり (10) を得る．$\operatorname{Tr}\rho\{\rho - e^{\lambda} \leq 0\} = 1 - \operatorname{Tr}\rho\{\rho - e^{\lambda} \geq 0\}$ より (9) を得る．また，Markov の不等式より $(t \geq 0)$

$$\operatorname{Tr}\rho\{\rho - e^{\lambda} \geq 0\} \leq e^{-t\lambda}\operatorname{Tr}\rho^{1+t}$$

を得る．$s = 1 + t$ とすると (11) を得る．

3　定理 2 の証明

始めに，$\rho = \sum_k P_k|\phi_k\rangle\langle\phi_k|$ と対角化し，確率分布 $P := \{P_k\}$ を考える．このとき，古典論の固定長情報源符号化の結果より [8, 9, 10, 12, 11],

$$\min\{D(Q\|P)|H(Q) \geq R\} = \max_{0\leq s\leq 1}\frac{(1-s)R - \psi(s)}{s}$$
$$\min\{D(Q\|P)|H(Q) \leq R\} = \max_{s\geq 1}\frac{(1-s)R - \psi(s)}{s}$$

となる．Ogawa-Nagaoka[15] により，仮説検定の場合に 2 つ目の式に対応する式が示されている．情報源符号化の場合に適用するには片方を一様分布に置けば 2 つ目の式が得られる．そこで用いられている方法を用いれば 1 つ目の式も示せる．さらに，文献 [7] の Thereom 3 及び Theorem 6 を組み合わせることにより

$$\min\{D(Q\|P)|H(Q) \leq R\} \leq \min\{D(\sigma\|\rho)|H(\sigma) \leq R\} \tag{16}$$

を得る．定義より逆の不等式が成り立つので

$$\min\{D(\sigma\|\rho)|H(\sigma) \leq R\} = \max_{s\geq 1}\frac{(1-s)R - \psi(s)}{s}$$

を得る．(16) と同じ論法で

$$\min\{D(Q\|P)|H(Q) \geq R\} \leq \min\{D(\sigma\|\rho)|H(\sigma) \geq R\}$$

が示せ，

$$\min\{D(\sigma\|\rho)|H(\sigma) \geq R\} = \max_{0\leq s\leq 1}\frac{(1-s)R - \psi(s)}{s}$$

を得る．次に

$$R_{e,B}(R|\{\rho_i, p_i\}_{i\in\Xi}) \geq r_0 := \max_{0\leq s\leq 1}\frac{(1-s)R - \psi(s)}{s} \tag{17}$$

を示す．これは Winter [5] により既に示されているがここで簡単に古典論の結果を用いて改めて示す．$\rho = \sum_{j\in J} q_j|\phi_j\rangle\langle\phi_j|$ とし，確率分布 q_j で表される情報源圧縮を考える．J^n の要素数 e^{nR} の適当な部分集合 J_n を取ると，$1 - \sum_{\vec{j}\in J_n} q_{n,\vec{j}} \cong e^{-nr_0}$ となる．ただし，$q_{n,\vec{j}} := q_{j_1}q_{j_2}\cdots q_{j_n}$ となる．したがって $P_n := \sum_{\vec{j}\in J_n}|\phi_{\vec{j}}\rangle\langle\phi_{\vec{j}}|$ $(\phi_{\vec{J}} := \phi_{j_1}\otimes\phi_{j_2}\otimes\cdots\otimes\phi_{j_n})$ とすると，$1 - \operatorname{Tr}\rho^{\otimes n}P_n \cong e^{-nr_0}$ となる．以下，P_n を用いて，Blind coding $\{(\mathcal{K}_n, E_n, D_n)\}$ を構成するまず $\mathcal{K}_n = \operatorname{Range}(P_n)$ とする．そして $E_n(\rho) := P_n\rho P_n + \rho_0(1 - \operatorname{Tr}\rho P_n)$ とし，$D_n(\rho) := \rho$ とする．ここで ρ_0 は $\mathcal{K}_n$ 上の状態であるが，特にどの状態を選んでも問題ない．このとき，

$$\mathcal{E}(E_n, D_n)$$
$$= 1 - \sum_{\vec{i}} p_{n,\vec{i}}\operatorname{Tr}\left(P_n\rho_{n,\vec{i}}P_n + \rho_0(1 - \operatorname{Tr}\rho_{n,\vec{i}}P_n)\right)\rho_{n,\vec{i}}$$
$$\leq 1 - \sum_{\vec{i}} p_{n,\vec{i}}\operatorname{Tr} P_n\rho_{n,\vec{i}}P_n\rho_{n,\vec{i}}$$
$$= 1 - \sum_{\vec{i}} p_{n,\vec{i}}(\operatorname{Tr} P_n\rho_{n,\vec{i}})^2 \leq 1 - (\sum_{\vec{i}} p_{n,\vec{i}}\operatorname{Tr} P_n\rho_{n,\vec{i}})^2$$
$$= 1 - (\operatorname{Tr}\rho^{\otimes n}P_n)^2 \cong 1 - (1 - e^{-nr_0})^2 = 2e^{-nr_0} - e^{-2nr_0}$$

よって (17) が示せた．

次に，

$$R^*_{e,V}(R|\{\rho_i, p_i\}_{i\in\Xi}) \leq r_1 := \max_{s\geq 1}\frac{(1-s)R - \psi(s)}{s} \tag{18}$$

を示す．先ほどと同じように確率分布 q_j で表される情報源圧縮を考える．J^n の要素数 e^{nR} の適当な部分集合 J_n を取ると，$\sum_{\vec{j}\in J_n} q_{n,\vec{j}} \cong e^{-nr_1}$ となる．同様に $\mathcal{H}^{\otimes n}$ 上の射影 P_n を定義し，Visible coding $\{(\mathcal{K}_n, F_n, D_n)\}$ を構成するまず $\mathcal{K}_n = \operatorname{Range}(P_n)$ とする．そして $F_n(\vec{i}) := \frac{1}{\operatorname{Tr} P_n\rho_{n,\vec{i}}}P_n\rho_{n,\vec{i}}P_n$ とし，$D_n(\rho) := \rho$ とする．このとき

$$1 - \mathcal{F}(F_n, D_n) = \sum_{\vec{i}} p_{n,\vec{i}}\operatorname{Tr}\frac{1}{\operatorname{Tr} P_n\rho_{n,\vec{i}}}P_n\rho_{n,\vec{i}}P_n\rho_{n,\vec{i}}$$
$$= \sum_{\vec{i}} p_{n,\vec{i}}\operatorname{Tr} P_n\rho_{n,\vec{i}} = \operatorname{Tr} P_n\rho^{\otimes n} = \sum_{\vec{j}\in J_n} q_{n,\vec{j}} \cong e^{-nr_1}$$

となり，(18) が示せる．

次に

$$R_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi}) \le \max_{0\le s\le 1}\frac{(1-s)R-\psi(s)}{s} \tag{19}$$

を補題 3 を用いて示す. 任意の Visible coding の無限列 $\{(\mathcal{K}_n,F_n,D_n)\}$ で

$$\overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n \le R \tag{20}$$

となるものを考える. $\eta(S) := \lim -\frac{1}{n}\log \mathrm{Tr}\,\rho^{\otimes n}\{\rho^{\otimes n} - e^{-nS}\le 0\}$ は Cramér の定理より

$$\eta(S) = \sup_{0\le s\le 1}(1-s)S-\psi(s) \tag{21}$$

と計算できる. 補題 3 の (9) より,

$$\mathcal{F}(F_n,D_n) \ge \mathrm{Tr}\,\rho^{\otimes n}\{\rho^{\otimes n}-e^{-nS}\le 0\} - e^{-nS}\dim\mathcal{K}_n \tag{22}$$

が成り立つ. $S-R\ge\eta(S)$ ならば,

$$\overline{\lim}\,-\frac{1}{n}\log\mathcal{F}(F_n,D_n) \le \eta(S) \tag{23}$$

となる. したがって

$$\overline{\lim}\,-\frac{1}{n}\log\mathcal{F}(F_n,D_n) \le \inf\{\eta(S)|S-R\ge\eta(S)\} \tag{24}$$

を得る. ここで

$$S = \psi'(s(S)) \tag{25}$$

$$S_R = R + (1-s(S_R))S_R - \psi(s(S_R)) \tag{26}$$

を満たすように $S_R, s(S)$ を定義すると,

$$\inf\{\eta(S)|S-R\ge\eta(S)\} = \eta(S_R) = S_R - R$$
$$= S_R(1-s(S_R)) - \psi(s(S_R)) = \frac{(1-s(S_R))R+\psi(s(S_R))}{s(S_R)}$$

となる. ここで $f(s) := \frac{(1-s)R-\psi(s)}{s}$ とすると, f の 2 階微分は正となり,

$$\frac{(1-s(S_R))R+\psi(s(S_R))}{s(S_R)} = \max_{0\le s\le 1}\frac{(1-s)R-\psi(s)}{s} \tag{27}$$

を得る. よって (19) を得た.

最後に

$$R^*_{e,V}(R|\{\rho_i,p_i\}_{i\in\Xi}) \ge \max_{s\ge 1}\frac{(1-s)R-\psi(s)}{s} \tag{28}$$

を示す. 任意の Visible coding の無限列 $\{(\mathcal{K}_n,F_n,D_n)\}$ で

$$\overline{\lim}\,\frac{1}{n}\log\dim\mathcal{K}_n \le R \tag{29}$$

となるものを考える. $\log\mathrm{Tr}(\rho^{\otimes n})^s = n\psi(s)$ となることから, (10) に $\lambda := -nS_R$, $s := s(S_R)$ を代入すると,

$$1-\mathcal{F}(F_n,D_n) \le e^{-n(S_R-R)} + e^{-n(S_R(1-s(S_R))-\psi(s(S_R)))} \tag{30}$$

となる. ただし $S_R, s(S)$ の定義は (25)(26) で与えられる. このとき

$$\underline{\lim}\,-\frac{1}{n}\log(1-\mathcal{F}(F_n,D_n)) \ge S_R - R$$
$$= S_R(1-s(S_R)) - \psi(s(S_R)) = \frac{(1-s(S_R))R+\psi(s(S_R))}{s(S_R)} \tag{31}$$

となる. したがって先ほどと同様に $f(s)$ の性質を調べることにより,

$$\frac{(1-s(S_R))R+\psi(s(S_R))}{s(S_R)} = \max_{s\ge 1}\frac{(1-s)R-\psi(s)}{s} \tag{32}$$

を得る. (30)(31)(32) を組み合わせることで, (28) が成り立つ.

4 Concentration との関連

定理 2 で現れる指数は文献 [7] で扱った最適な可変長 universal entanglement concentration を考えた場合にもその失敗確率や成功確率の指数にも現れる. ただ, 情報源圧縮の場合と異なるのは, 情報源圧縮ではサイズを小さくするのが目的であるのに対して, entanglement concentration ではサイズを大きくするのが目的である. そのため, (3)(4) で与えられる値が, 成功確率の減少指数になり, (6)(7) で与えられる値が失敗確率の減少指数になる. 詳しくは文献 [7] を参照して頂きたい.

5 今後の課題

本稿では情報源が純粋状態からなる場合のみ取り扱った. 情報源が混合状態からなる場合の情報源符号化については Barnum et al [14] により問題が提案され, Koashi-Imoto[13] により R_B が $H(\rho)$ で与えられることが示された. しかしながら, 他の量については Barnum et al [14] により $R_V \ge H(\rho)-\sum_i p_i H(\rho_i)$ となることが示されているのみで, 他のことについては全く分かっていない. 今後このテーマにも注目する必要がある.

謝辞

補題 3 の証明において重要な役割を果たした Nielsen-Kempe の補題 [6] を Dr. A. Winter からご教示頂いた. この場を借りて謝意をあらわしたい.

参考文献

[1] B. Schumacher, "Quantum coding," Phys. Rev. A, 51(4), 2738-2747, (1995).

[2] R. Jozsa and B. Schumacher, "A new proof of the quantum noiseless coding theorem," J. Mod. Optics, 41(12), 2343-2349, (1994).

[3] H. Barnum, C. A. Fuchs, R. Jozsa and B. Schumacher, "General Fidelity Limit for Quantum Channels," Phys. Rev. A, 54, 4707-4711 (1996).

[4] M. Horodecki, "Limits of compression of quantum information carried by ensembles of mixed state," Phys. Rev. A, 57, 3364-3369 (1998).

[5] A. Winter, "Coding Theorems of Quantum Information Theory," Ph.D. dissertation, Uni Bielefeld, LANL eprint qunat-ph/9907077, (2000).

[6] M. A. Nielsen and J. Kempe, "Separable States Are More Disordered Globally than Locally," Phys. Rev. Lett., 86, 5184-5187 (2001). LANL eprint qunat-ph/0011117, (2000).

[7] M. Hayashi and K. Matsumoto, "Variable length universal entanglement concentration by local operations and its application to teleportation and dense coding," LANL eprint qunat-ph/0109028.

[8] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, (Academic Press, New York, 1981).

[9] R. E. Blahut, Principles and Practice of Information Theory, (Addison-Wesley, 1987).

[10] I. Csiszár and G. Longo, "On the error exponent for the noiseless encoding for testing simple statistical hypothesis," Studia Sci. Math. Hunger., vol 6, 181-191, (1971).

[11] 韓 太舜, 小林欣吾「情報と符号化の数理」培風館, (1999).

[12] H. Nagaoka and M. Hayashi, "An Information-Spectrum Approach to Classical and Quantum Hypothesis Testing," in preparation.

[13] M. Koashi and N. Imoto "Compressibility of Mixed-State Signals," Phys. Rev. Lett. 87, 017902 (2001). LANL eprint qunat-ph/0103128, (2001).

[14] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. W. Schumacher "On quantum coding for ensembles of mixed states," LANL eprint quant-ph/0008024, (2000).

[15] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Trans. Inform. Theory*, vol.46, 2428-2433, (2000). LANL e-print quant-ph/9906090, (1999).