付録 B

定理，補題の証明

B.1　定理 3.1 の証明

以下では $A(x) = b$ となる $x \in L$ が存在する場合のみ考える*1)。存在しない場合は双方とも無限小になる。

はじめに $A(x) = b$ となる $x \in L$ と $A^T(y) - c \in L^T$ となる y は $0 \le \langle A^T(y) - c, x\rangle = \langle y, A(y)\rangle - \langle c, x\rangle = \langle y, b\rangle - \langle c, x\rangle$ を満たすことから、

$$\max_{x\in V_1}\{\langle c, x\rangle | x \in L, A(x) = b\} \le \min_{y\in V_2}\{\langle y, b\rangle | A^T(y) - c \in L^T\}. \quad \text{(B.1)}$$

を確認することができる。さらに、

$$\begin{aligned}&\min_{y\in V_2}\{\langle y, b\rangle | A^T(y) - c \in L^T\}\\ =&\min_{(\mu,y)\in\mathbb{R}\times V_2}\{\mu | \exists y \in V_2, \forall x \in L, \langle y, b\rangle - \langle A^T(y) - c, x\rangle \le \mu\}\end{aligned}$$

が確認できる。これには $A^T(y) - c \in L^T$ を満たす $y \in V_2$ に対しては、$\mu = \langle y, b\rangle$ ととれば、右辺の条件式が満たされるので、$\ge$ が示せる。次に、右辺の条件式を満たす (μ, y) の組を考える。そのとき、$\langle A^T(y) - c, x\rangle$ は全ての $x \in L$ に対して、0 以上であることが分かる。なぜなら、$\langle A^T(y) - c, x\rangle$ が負となる $x \in L$ が存在するとすると、$t > 0$ を十分大きくとり、$tx \in L$ を考えると、右辺の条件式を満たさなくなるからである。したがって、$\le$ を示すことができる。

さらに、$\eta_0 \overset{\text{def}}{=} \max_{x\in V_1}\{\langle c, x\rangle | x \in L, A(x) = b\}$ とすると、$(\eta_0, 0)$ は凸集合 $\{(\langle c, x\rangle, A(x) - b)\}_{x\in L} \subset \mathbb{R} \times V_2$ の境界上の点となる。したがって適当に $y_0 \in V_2$ を選び、$(1, -y_0) \in \mathbb{R} \times V_2$ に注目すると、

$$\eta_0 = \eta_0 - \langle y, 0\rangle \ge \langle c, x\rangle - \langle y_0, A(x) - b\rangle, \quad \forall x \in L$$

となる。この事実から、

$$\eta_0 \ge \min_{(\mu,y)\in\mathbb{R}\times V_2}\{\mu | \exists y \in V_2, \forall x \in L, \langle y, b\rangle - \langle A^T(y) - c, x\rangle \le \mu\}$$

となり、(B.1) と逆向きの不等式が得られ、題意を得る。

*1)　ここで紹介する証明は文献 [269] を参考にした。

B.2　定理 8.2 の証明

証明:　①⇒② ⇒③ ⇒①, ②⇒④ ⇒① の順に示す.

はじめに①⇒②を次元 d についての帰納法で示す．$d = 2$ の場合は $t \stackrel{\text{def}}{=} (y_1 - x_1)/(y_1 - y_2) = (x_2 - y_2)/(y_1 - y_2)$ とすると，$x \preceq y$ であることから，$0 \leq t \leq 1$ となることを示せる．さらに，

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1-t & t \\ t & 1-t \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \tag{B.2}$$

となるので題意を得る．以下，$d \leq n-1$ のとき，成り立つと仮定して，$d = n$ のときについて示す．置換に対応する行列の演算は，T 変換の積で与えられる．それゆえ，適当な置換を考えることで $x_1 \geq x_2 \geq \ldots \geq x_n, y_1 \geq y_2 \geq \ldots \geq y_n$ となる場合に②を示せば他の場合も②を示すことができる．$x \preceq y$ であることから，$y_n \leq x_1 \leq y_1$ となる．それゆえ，適切に k を選ぶと，$y_k \leq x_1 \leq y_{k-1}$ となる．さらに $x_1 = ty_1 + (1-t)y_k$ となるように t を選ぶと $0 \leq t \leq 1$ となる．$1, k$ 成分についての t により定義される T 変換を T_1 で表すことにする．ここで

$$x' \stackrel{\text{def}}{=} (x_2, \ldots, x_n)^T \tag{B.3}$$

$$y' \stackrel{\text{def}}{=} (y_2, \ldots, y_{k-1}, (1-t)y_1 + ty_k, y_{k+1}, \ldots, y_n)^T \tag{B.4}$$

と定義すると，$T_1 y = (x_1, y')$ となる．さらに以下に示すように $x' \preceq y'$ となるので，帰納法の仮定より，適切に T 変換 $T_f, \ldots, T_2$ を選ぶと，$T_f \ldots T_2 y' = x'$ となる．従って，$T_f \ldots T_2 T_1 y = T_f \ldots T_2(x_1, y') = (x_1, x') = x$ となり題意を得る．以下，$x' \preceq y'$ を示す．$2 \leq m \leq k-1$ となる整数 m について

$$\sum_{j=2}^{m} x_j \leq \sum_{j=2}^{m} y_j \tag{B.5}$$

となる．さらに $k \leq m \leq n$ となる場合には

$$\begin{aligned} \sum_{j=2}^{m} {y'}_j &= \left(\sum_{j=2}^{k-1} y_j \right) + (1-t)y_1 + ty_k + \left(\sum_{j=k+1}^{m} y_j \right) \\ &= \left(\sum_{j=1}^{m} y_j \right) - ty_1 + (t-1)y_k = \sum_{j=1}^{m} y_j - x_1 \geq \sum_{j=1}^{m} x_j - x_1 = \sum_{j=2}^{m} x_j \end{aligned}$$

となり，$x' \preceq y'$ を得る．

次に②⇒③を示す．2 重確率遷移行列 A_1, A_2 の積 $A_1 A_2$ も 2 重確率遷移行列になる．さらに，T 変換は 2 重確率遷移行列になるので，③が得られる．

さらに③⇒①を示す．任意の整数 k と任意の 1 から d までの k 個の整数の組 $i_1, \ldots, i_k$ について，

$$\sum_{t=1}^{k}\sum_{j=1}^{d} x^{i_t,j} a_j \le \sum_{j=1}^{k} a_j^{\downarrow}$$

となることを示せば十分である．これは $\sum_{j=1}^{d}\sum_{t=1}^{k} x^{i_t,j} = k$ かつ，各 j について $\sum_{t=1}^{k} x^{i_t,j} \le 1$ であることから示せる．

さらに②⇒④を示す．はじめに簡単のため，$d = 2$ の場合は，

$$B = \begin{pmatrix} \frac{(y_1/y_2)^2-(x_2/x_1)(y_1/y_2)}{(y_1/y_2)^2-1} & \frac{(y_1/y_2)(x_1/x_2)-1}{(y_1/y_2)^2-1} \\ \frac{(x_2/x_1)(y_1/y_2)-1}{(y_1/y_2)^2-1} & \frac{(y_1/y_2)^2-(y_1/y_2)(x_1/x_2)}{(y_1/y_2)^2-1} \end{pmatrix} \tag{B.6}$$

とおくと，条件よりこれが確率遷移行列であることが確かめられる．そして，

$$\begin{pmatrix} \frac{(y_1/y_2)^2-(x_2/x_1)(y_1/y_2)}{(y_1/y_2)^2-1} x_1 \\ \frac{(y_1/y_2)(x_1/x_2)-1}{(y_1/y_2)^2-1} x_2 \end{pmatrix} = \frac{(y_1/y_2)x_1 - x_2}{(y_1/y_2)^2-1} \begin{pmatrix} (y_1/y_2) \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} \frac{(x_2/x_1)(y_1/y_2)-1}{(y_1/y_2)^2-1} x_1 \\ \frac{(y_1/y_2)^2-(y_1/y_2)(x_1/x_2)}{(y_1/y_2)^2-1} x_2 \end{pmatrix} = \frac{(y_1/y_2)x_2 - x_1}{(y_1/y_2)^2-1} \begin{pmatrix} 1 \\ (y_1/y_2) \end{pmatrix}$$

となることから，$B^1 \circ x \approx B^2 \circ x \approx y$ となることが確認できる．

この事実から k, l 成分 $(k < l)$ についての t により定義される T 変換 T_0 について $x = T_0 y$ となるときは，

$$\begin{pmatrix} b^{1,k} & b^{1,l} \\ b^{2,k} & b^{2,l} \end{pmatrix} = \begin{pmatrix} \frac{(y_k/y_l)^2-(x_l/x_k)(y_k/y_l)}{(y_k/y_l)^2-1} & \frac{(y_k/y_l)(x_k/x_l)-1}{(y_k/y_l)^2-1} \\ \frac{(x_l/x_k)(y_k/y_l)-1}{(y_k/y_l)^2-1} & \frac{(y_k/y_l)^2-(y_k/y_l)(x_k/x_l)}{(y_k/y_l)^2-1} \end{pmatrix}$$

$$b^{1,i} = \frac{(y_k/y_l)x_k - x_l}{(y_k/y_l)-1}, \quad b^{2,i} = \frac{(y_k/y_l)x_l - x_k}{(y_k/y_l)-1} \quad \text{if } i \ne k, l$$

とおくと，$B^1 \circ x \approx B^2 \circ x \approx y$ となることが確認できる．

さらに，2 つの確率遷移行列 B, C に対して，$y \approx (B^j)^* \circ x$, $z \approx (C^i)^* \circ y$ $(i, j$ は任意$)$ となるとき，適当な置換 s_j を選ぶと，

$$y \propto s(j)((B^j)^* \circ x)$$

となる．（ここで置換 $s(j)$ とそれを表す行列を同一視した．）したがって，$s(j)^* = (s(j))^{-1}$ であるから，

$$\begin{aligned} z \approx &(C^i)^* \circ y = s(j)\left(((s(j))^{-1}(C^i)^*) \circ (s(j))^{-1} y\right) \\ \propto &s(j)\left(((s(j))^{-1}(C^i)^*) \circ (B^j)^* \circ x\right) = s(j)\left((C^i s(j))^* \circ (B^j)^* \circ x\right) \\ = &s(j)\left((C^i s(j))^* \circ (B^j)^* \circ x\right) \approx (C^i s(j))^* \circ (B^j)^* \circ x \end{aligned}$$

したがって，

$$\begin{aligned} &\sum_{i,j} (C^i s(j))^* \circ (B^j)^* = \sum_j (\sum_i C^i s(j))^* \circ (B^j)^* \\ = &\sum_j (e^* s(j))^* \circ (B^j)^* = \sum_j e \circ (B^j)^* = \sum_j (B^j)^* = e \end{aligned}$$

となるので，$(D^{i,j})^* \stackrel{\mathrm{def}}{=} (C^i s(j))^* \circ (B^j)^*$ （i,j で一つの行を指定していることに注意）で定義される行列 D は確率遷移行列となり，

$$(D^{i,j})^* \circ x = z \tag{B.7}$$

を満たす．この事実と先に示したことから，②⇒④が得られる．

最後に④⇒①を示す．これには，任意の整数 k に対して，さらに，正の実数を成分にもつ d 次元のベクトル $c = (c_i)$ で

$$c_i \leq 1, \quad \sum_{i=1}^{d} c_i = k, \quad \sum_{j=1}^{k} y_{i_j} \geq \sum_{j=1}^{k} x_j^{\downarrow} \tag{B.8}$$

となるものが存在することを示せば十分である．そのために，異なる k 個の整数 $i_1, \ldots, i_k$ で

$$\sum_{j=1}^{k} x_j^{\downarrow} = \sum_{j=1}^{k} x_{i_j}$$

を選ぶ．ここで j に応じて置換 $s(j)$ と正の実数 d_j を $(B^j)^* \circ x = d_j s(j) y$ となる．$\sum_{j=1}^{d} d_j = 1$ となることに注意．そして，

$$\sum_{j=1}^{d} b^{j,i} x_i = x_i$$

となるので，

$$\sum_{j=1}^{k} x_{i_j} = \sum_{t=1}^{d} \sum_{j=1}^{k} b^{t,i_j} x_{i_j} = \sum_{t=1}^{d} \sum_{j=1}^{k} d_t (s(t)y)_{i_j} = \sum_{t=1}^{d} \sum_{j=1}^{k} \sum_{l=1}^{d} d_t s(t)_{i_j,l} y_l$$

を得る．

$$\sum_{j=1}^{k} s(t)_{i_j,l} \leq 1, \quad \sum_{l=1}^{d} \sum_{j=1}^{k} s(t)_{i_j,l} = k$$

なので，$\sum_t d_t = 1$ であることに注意すると，

$$\sum_t \sum_{j=1}^{k} d_t s(t)_{i_j,l} \leq 1, \quad \sum_{l=1}^{d} \sum_t \sum_{j=1}^{k} s(t)_{i_j,l} = k$$

となり，(B.8) を満たすベクトル $c = (c_i)$ の存在が示せた． □

B.3 定理 8.3 の証明

ρ を $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の separable な状態とする。すると適当な $\mathcal{H}_A$ のベクトルの組 u_i と $\mathcal{H}_B$ のベクトルの組 v_i を選ぶと $\rho = \sum_i |u_i \otimes v_i\rangle\langle u_i \otimes v_i| = \sum_j \lambda_j |e_j\rangle\langle e_j|$ となる．なお，右辺は ρ の対角化である．このとき，補題 A.4

より，等長行列 $W=(w_{i,j})$ で，$u_i \otimes v_i = \sum_j w_{i,j}\sqrt{\lambda_j}e_j$ となるものが取れる．$W^*W=I$ となることから，

$$\sum_i w_{i,j}^* u_i \otimes v_i = \sqrt{\lambda_j}e_j \tag{B.9}$$

となる．同様に，$\mathrm{Tr}_B\,\rho$ の対角化を $\mathrm{Tr}_B\,\rho = \sum_k \lambda'_k |f_k\rangle\langle f_k|$ とすると，等長行列 $W'=(w'_{i,k})$ で，$u_i = \sum_k w'_{i,k}\sqrt{\lambda'_k}f_k$ となるものが取れ，(B.9) に代入すると，

$$\sqrt{\lambda_j}e_j = \sum_i \sum_k w'_{i,k} w^*_{i,j}\sqrt{\lambda'_k} f_k \otimes v_i$$

を得る．両辺のノルムを取ると，

$$\lambda_j = \sum_k D_{j,k}\lambda'_k, \quad D_{j,k} \stackrel{\mathrm{def}}{=} \left(\sum_{i,i'} w'_{i,k} w^*_{i,j} (w'_{i',k})^* w_{i',j}\langle v_{i'}|v_i\rangle\right)$$

を得る．定理 8.2 の条件③より，$D_{j,k}$ が 2 重確率遷移行列であることが示せると，$(\lambda'_k) \preceq (\lambda_j)$ を得る．

$$\left(\sum_{i,i'} w'_{i,k} w^*_{i,j} (w'_{i',k})^* w_{i',j}\langle v_{i'}|v_i\rangle\right) = \left\langle \sum_{i'} w'_{i',k} w^*_{i',j} v_{i'} \middle| \sum_i w'_{i,k} w^*_{i,j} v_i \right\rangle \geq 0$$

であり，$W'^*W'=I, W^*W=I$ であることから，

$$\begin{aligned}&\sum_k \left(\sum_{i,i'} w'_{i,k} w^*_{i,j} (w'_{i',k})^* w_{i',j}\langle v_{i'}|v_i\rangle\right) = \sum_{i,i'} \delta_{i,i'} w^*_{i,j} w_{i',j}\langle v_{i'}|v_i\rangle \\ =& \sum_i w^*_{i,j} w_{i,j} = 1\end{aligned}$$

を得る．同様に $\sum_j D_{j,k}=1$ を示すことができるので，$D_{j,k}$ が 2 重確率遷移行列であることがわかる．

B.4　混合状態の場合での定理 8.8 の証明

次に一般の状態 ρ について (8.66) の $\leq$ を示す．S-TP-CP 写像 κ の Kraus 表現を $\{E_{A,i} \otimes E_{B,i}\}_i$ とする．このとき，

$$\kappa(\|L\rangle\langle L\|) = \sum_i (E_{A,i} \otimes E_{B,i})\,\|L\rangle\langle L\|\,(E_{A,i} \otimes E_{B,i})^*$$

となる．ここで

$$\begin{aligned} p'_i &\stackrel{\mathrm{def}}{=} \mathrm{Tr}\,(E_{A,i} \otimes E_{B,i})\,\|L\rangle\langle L\|\,(E_{A,i} \otimes E_{B,i})^* \\ p'_i|y_i\rangle\langle y_i| &= (E_{A,i} \otimes E_{B,i})\,\|L\rangle\langle L\|\,(E_{A,i} \otimes E_{B,i})^* \end{aligned}$$

となるように y_i を選ぶ．系 8.1 より，適当に ρ の確率的な分解 $\{(p_i, x_i)\}$ を選ぶと，

$$F(\kappa(\|L\rangle\langle L\|), \rho) = \sum_i \sqrt{p_i p'_i} |\langle x_i | y_i \rangle|$$

となる．先ほどと同じ理由により，y_i の Schmidt ランクは 高々L であるので，

$$|\langle x_i | y_i \rangle| \le \sqrt{P(x_i, L)} \tag{B.10}$$

となる．よって，Schwarz の不等式より，

$$\begin{aligned} F(\kappa(\|L\rangle\langle L\|), \rho) &\le \sum_i \sqrt{p_i p'_i} \sqrt{P(x_i, L)} \\ &\le \sqrt{\sum_i p'_i} \sqrt{\sum_i p_i P(x_i, L)} = \sqrt{\sum_i p_i P(x_i, L)} \end{aligned} \tag{B.11}$$

となり，(8.66) の $\le$ を得る．

逆に，Schmidt ランクが高々 L となる y_i で (B.10) で等号を達成し，

$$p'_i = \frac{p_i P(x_i, L)}{\sum_j p_j P(x_j, L)}$$

のとき，(B.11) で等号が成立するので，よって定理 8.4 より，(8.64) の右辺を達成する，１方向の LOCC が存在する．

B.5 混合状態の場合での定理 8.9 の証明

B.5.1 順定理の証明

(8.63) と補題 A.1 より，(8.72) の 2 つの目の等号は成立する．したがって，以下では１つ目の等号のうち $\le$ の部分を示す．はじめに $R > E_f(\rho)$ とすると，

$$\min_{(p_i, x_i)} \left\{ \sum_i p_i (1 - P(x_i, [e^{nR}])) \middle| \sum_i p_i |x_i\rangle\langle x_i| = \rho^{\otimes n} \right\}$$

が指数的に 0 に収束することを示す．この値が 0 に収束することと (8.66) に右辺の $\sqrt{\ }$ 内の値が 1 に収束することとは同値であるので、以下ではこの値に注目する。そのために $R > \sum_i p_i E(|x_i\rangle\langle x_i|)$ となる分解 $\{(p_i, x_i)\}$ を選ぶ。そして $\rho_i \stackrel{\mathrm{def}}{=} \mathrm{Tr}_B |x_i\rangle\langle x_i|$ とすると，(8.67) より，

$$\sum_i p_i P(x_i, [e^R]) \le \sum_i p_i e^{\frac{\log \mathrm{Tr}\, \rho_i^{1-s} - sR}{1-s}}$$

となる．特に $\frac{\log \mathrm{Tr}(\rho_i \otimes \rho_j)^{1-s} - 2sR}{1-s} = \frac{\log \mathrm{Tr}\, \rho_i^{1-s} - sR}{1-s} + \frac{\log \mathrm{Tr}\, \rho_j^{1-s} - sR}{1-s}$ となることから，$i^n \stackrel{\mathrm{def}}{=} (i_1, \dots, i_n)$ に対して，$x^n_{i^n} \stackrel{\mathrm{def}}{=} x_{i_1} \otimes \cdots \otimes x_{i_n}$, $\rho^n_{i^n} \stackrel{\mathrm{def}}{=} \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}$, とおくと，

$$\sum_{i^n} p^n_{i^n} P(x^n_{i^n}, [e^{nR}]) \le \sum_{i^n} p^n_{i^n} e^{\frac{\log \mathrm{Tr}(\rho^n_{i^n})^{1-s} - snR}{1-s}}$$
$$= \left(\sum_i p_i e^{\frac{\log \mathrm{Tr}\, \rho_i^{1-s} - sR}{1-s}} \right)^n \tag{B.12}$$

を得る．なお，p^n は p の独立同一分布である．以下の式の左辺の log 内は $s=0$ のとき，1 となることに注意すると，

$$\lim_{s\to 0} \frac{1}{s} \log\left(\sum_i p_i e^{\frac{\log \mathrm{Tr}\, \rho_i^{1-s} - sR}{1-s}} \right) = \frac{d}{ds} \log\left(\sum_i p_i e^{\frac{\log \mathrm{Tr}\, \rho_i^{1-s} - sR}{1-s}} \right)\Bigg|_{s=0}$$
$$= \sum_i p_i (H(\rho_i) - R) < 0$$

を得る．したがって，適当な $1 > s_0 > 0$ を取ると，$\log\left(\sum_i p_i e^{\frac{\log \mathrm{Tr}\, \rho_i^{1-s_0} - s_0 R}{1-s_0}} \right) < 0$ となるので，(B.12) の右辺は指数的に 0 に近づく．よって，$E_c(\rho) \le E_f(\rho)$ を得る．同様にして，$E_c(\rho^{\otimes k}) \le E_f(\rho^{\otimes k})$ を得る．

次に n に対して，$(m_n - 1)k \le n \le m_n k$ となるように数列 $\{m_n\}$ を選ぶ．そして、$(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes m_n k - n}$ についての部分トレースを C_n で表すとすると，O_m, L_m に対して，

$$F(\rho^{\otimes m_n k}, O_{m_n}(\|L_{m_n}\rangle\langle L_{m_n}\|)) \ge F(\rho^{\otimes n}, C_n \circ O_{m_n}(\|L_{m_n}\rangle\langle L_{m_n}\|)) \tag{B.13}$$

が成り立つ。それゆえ，(B.13) の左辺が 0 に収束するのであれば，右辺も 0 に収束する．さらに，

$$\overline{\lim} \frac{1}{n} \log L_{m_n} = \frac{1}{k} \overline{\lim}_{m\to\infty} \frac{1}{m} \log L_m$$

となることと，C_n が局所量子操作であることと $E_c(\rho^{\otimes k}) \le E_f(\rho^{\otimes k})$ となることから，

$$E_c(\rho) \le \frac{E_c(\rho^{\otimes k})}{k} \le \frac{E_f(\rho^{\otimes k})}{k}$$

となる．したがって，$\inf_k$ を考えることにより (8.72) の $\le$ の部分を得る．

B.5.2　逆定理の証明

この定理を示すために，以下の補題を準備する．

補題 B.1　確率分布 $p = \{p_i\}_{i=1}^d$ に対して次の式が成り立つ．

$$\sum_{i=L+1}^{d} p_i^{\downarrow} \ge \frac{H(p) - \log L - \log 2}{\log(d-L) - \log L} \tag{B.14}$$

証明:　2 重確率遷移行列 $A=(a_{i,j})$:

$$a_{i,j} \stackrel{\text{def}}{=} \begin{cases} \frac{1}{L} & \text{if } i,j \le L \\ \frac{1}{d-L} & \text{if } i,j > L \\ 0 & \text{otherwise} \end{cases}$$

による像，Ap は $(Ap)_i = \begin{cases} \frac{P(p,L)}{L} & \text{if } i \le L \\ \frac{1-P(p,L)}{d-L} & \text{if } i > L \end{cases}$ となる．したがって、定理 8.2 の条件③より，$Ap \preceq p$ となるので，

$$H(p) \ge H(Ap) = -P(p,L)\log\frac{P(p,L)}{L} - (1-P(p,L))\log\frac{1-P(p,L)}{d-L}$$

を得る．そして，2 値エントロピー $h(x)$ は $\log 2$ より小さいので，

$$\begin{aligned} & P^c(p,L)(\log(d-L)-\log L)+\log 2 \\ \ge & P^c(p,L)(\log(d-L)-\log L)+h(P(p,L)) \ge H(p)-\log L \end{aligned}$$

となり，(B.14) を得る．　$\square$

以下この補題 B.1 を用いて定理 8.9 の $\ge$ の部分を示す．S-TP-CP 写像の列 $\{O_n\}$ と最大エンタングルド状態の列 $\{\|L_n\rangle\}$ で

$$F(O_n(\|L_n\rangle\langle L_n\|),\rho^{\otimes n}) \to 1 \tag{B.15}$$

を満たすものを考える．定理 8.8 の (8.65) と (8.66) 及び補題 B.1 を組み合わせることにより，

$$\begin{aligned} & 1-F^2(O_n(\|L_n\rangle\langle L_n\|),\rho^{\otimes n}) \\ \ge & \min_{(p_i,x_i)}\left\{\sum_i p_i P^c(x_i,L_n)\middle|\sum_i p_i|x_i\rangle\langle x_i| = \rho^{\otimes n}\right\} \\ \ge & \min_{(p_i,x_i)}\left\{\sum_i p_i \frac{E(|x_i\rangle\langle x_i|)-\log L_n-\log 2}{\log(d^n-L_n)-\log L_n}\middle|\sum_i p_i|x_i\rangle\langle x_i| = \rho^{\otimes n}\right\} \\ = & \frac{E_f(\rho^{\otimes n})-\log L_n-\log 2}{\log(d^n-L_n)-\log L_n} = \frac{\frac{E_f(\rho^{\otimes n})}{n}-\frac{\log L_n}{n}-\frac{\log 2}{n}}{\frac{\log(d^n-L_n)}{n}-\frac{\log L_n}{n}} \end{aligned}$$

を得る．(B.15) と補題 A.1 を用いると，

$$\begin{aligned} 0 = & \lim\left(\frac{\log(d^n-L_n)}{n}-\frac{\log L_n}{n}\right)\left(1-\left(F(O_n(\|L_n\rangle\langle L_n\|),\rho^{\otimes n})\right)^2\right) \\ & \ge \overline{\lim}\left(\frac{E_f(\rho^{\otimes n})}{n}-\frac{\log L_n}{n}-\frac{\log 2}{n}\right) = \lim\frac{E_f(\rho^{\otimes n})}{n}-\underline{\lim}\frac{\log L_n}{n} \end{aligned}$$

となり、以下の式が得られ、定理 8.9 が示された。

$$\lim\frac{E_f(\rho^{\otimes n})}{n} \le \underline{\lim}\frac{\log L_n}{n} \le \overline{\lim}\frac{\log L_n}{n} \le E_c(\rho).$$

B.6 補題 9.4 の証明

テキストに与えた補題 9.4 は若干のミスを含んでおり，以下では代わりに次の補題 B.2 を示す．なお，最終的な定理 9.7 についてはこの補題 B.2 から示すことができる．

補題 B.2 κ を $\mathcal{H}_A$ から $\mathcal{H}_B$ への TP-CP 写像とし，M, L を $\dim \mathcal{H}_A \ge ML$ となる任意の整数とする．また，$\mathcal{H}_E$ を κ の環境系とする．そして，$\mathcal{H}_A$ の正規直交基底 $\{u_x\}_{x\in\mathcal{X}}$ を選び，$\mathcal{X}$ 上の 確率分布 p に注目し，$W_{B,x} \stackrel{\mathrm{def}}{=} \kappa(u_x), W_{E,x} \stackrel{\mathrm{def}}{=} \kappa_E(u_x)$ とし，v を $W_{E,p}$ の固有値の数とする。すると、以下の条件を満たす $\mathbb{C}^M$ から $\mathcal{H}_A$ への等長写像 V と $\mathcal{H}_B$ から $\mathbb{C}^M$ への TP-CP 写像 ν が取れる。

$$
\begin{aligned}
&1 - F_e(\rho_{\mathrm{mix}}, \nu\circ\kappa\circ\kappa_V) \\
\le& 32 \sum_x p(x) \operatorname{Tr} W_{B,x}\{W_{B,x} - MLW_{B,p} < 0\} \\
&+ 16ML \operatorname{Tr} W_{B,p}\{W_{B,x} - MLW_{B,p} \ge 0\} \\
&+ 4\sqrt{\sum_x p(x) \operatorname{Tr} W_{E,x}\{\kappa_{W_{E,p}}(W_{E,x}) - CW_{E,p} \ge 0\}} + \sqrt{\frac{Cv}{L}}.
\end{aligned}
\tag{B.16}
$$

この補題を示すために，定理 9.6 の証明と同様の議論を用いる．すなわち，ML 個の $\mathcal{X}$ の要素 $\{x_{m,l}\}_{(m,l)\in\{1,\dots,M\}\times\{1,\dots,L\}}$ と POVM $\{Y_{m,l}\}$ を取ることができる．(この場合，必ずしも $x_{m,l}$ が互いに全て異なるとは限らない．)

$$
\begin{aligned}
&\frac{8}{ML}\sum_{m,l}\epsilon_{B,m,l} + \frac{1}{M}\sum_{m=1}^{M}\epsilon_{E,m} \le ((B.16) \text{ の右辺}) \\
&\epsilon_{B,m,l} \stackrel{\mathrm{def}}{=} 1 - \operatorname{Tr} W_{B,x_{m,j}} Y_{m,l}, \quad \epsilon_{E,m} \stackrel{\mathrm{def}}{=} \left\| \frac{1}{L}\sum_{l=1}^{L} W_{E,x_{m,l}} - \sum_x p_x W_{E,x} \right\|
\end{aligned}
\tag{B.17}
$$

以下この議論を次の補題 B.3 に結びつけて示すが，ここで選んだ，$x_{m,l}$ は重複している場合もあるが，補題 B.3 を適用するには，これらが異なる必要がある．このために，$x_{m,l}$ の中で重複のあったものついては，同じ $x_{m,l}$ のうち 1 つを除いて，$\mathcal{X}\setminus\{x_{m,l}\}$ の要素から，重複が無いように選ぶ．このようにして構成されたものを新たに $x'_{m,l}$ と記すことにする．さらに，POVM についても $\{Y_{m,l}\}$ を次にように変形する．

$$
Y'_{m,l} \stackrel{\mathrm{def}}{=} \begin{cases} \sum_{x_{m',l'}=x_{m,l}} Y_{m',l'} & x_{m,l} = x'_{m,l} \\ 0 & x_{m,l} \ne x'_{m,l} \end{cases}
$$

このとき，(B.17) と同様に誤り確率を $\epsilon'_{B,m,l}$ と記すと，

$$\sum_{m,l} \epsilon_{B,m,l} = \sum_{m,l} \epsilon'_{B,m,l}$$

が成り立つ．また，$\{x_{m,l} \neq x'_{m,l}\}$ の要素の数であるが，これは，$\sum_{m,l} \epsilon'_{B,m,l}$ 以下である．したがって，

$$\frac{1}{M}\sum_{m=1}^{M}\left\| \frac{1}{L}\sum_{l=1}^{L} W_{E,x_{m,l}} - \frac{1}{L}\sum_{l=1}^{L} W_{E,x'_{m,l}} \right\| \leq \frac{2}{ML}\sum_{m,l} \epsilon_{B,m,l}$$

となる．

すなわち，$\{x'_{m,l}\}$ と $Y'_{m,l}$ の組について $\epsilon'_{E,m}$ を (B.17) と同様に定義すると，以下を満たすことが確認できる．

$$\frac{6}{ML}\sum_{m,l} \epsilon'_{B,m,l} + \frac{1}{M}\sum_{m=1}^{M} \epsilon'_{E,m} \leq ((B.16) \text{ の右辺})$$

よって，$u_{x'_{m,l}}$ を以下の補題 B.3 に適用することで，補題 B.2 を得る．

補題 B.3 $\mathcal{H}_A$ の互いに直交する ML 個の長さ 1 のベクトル $\{u^A_{m,l}\}_{(m,l)\in\{1,\dots,M\}\times\{1,\dots,L\}}$ $\mathcal{H}_A$ から $\mathcal{H}_B \otimes \mathcal{H}_E$ への等長な写像 $U^{B,E}_A$ と $\mathcal{H}_B$ 上の POVM $Y = \{Y_{m,l}\}_{(m,l)\in\{1,\dots,M\}\times\{1,\dots,L\}}$ を考える．なお $U^{B,E}_A$ によって定義される $\mathcal{H}_A$ から $\mathcal{H}_B$ への TP-CP 写像を κ とする．このとき，$\mathcal{H}_E$ 上の状態 W_E に対して，

$$\epsilon^B_{m,l} \stackrel{\text{def}}{=} 1 - \operatorname{Tr} U^{B,E}_A |u^A_{m,l}\rangle\langle u^A_{m,l}| (U^{B,E}_A)^* (Y_{m,l} \otimes I_E) \tag{B.18}$$

$$\epsilon^E_m \stackrel{\text{def}}{=} \left\| \left(\frac{1}{L}\sum_{l=1}^{L} W^E_{m,l} \right) - W_E \right\|_1, \quad W^E_{m,l} \stackrel{\text{def}}{=} \operatorname{Tr}_B U^{B,E}_A |u^A_{m,l}\rangle\langle u^A_{m,l}| (U^{B,E}_A)^* \tag{B.19}$$

とおく．

このとき，M 次元空間 $\mathcal{H}_C \stackrel{\text{def}}{=} \langle u^C_1, \dots, u^C_M \rangle$, $\mathcal{H}_D \stackrel{\text{def}}{=} \langle u^D_1, \dots, u^D_M \rangle$ に対して，以下の方法で確率変数 $\alpha = (\alpha_1, \dots, \alpha_M)$ に応じて $\mathcal{H}_C$ から $\mathcal{H}_A$ への符号化 τ_α 及び $\mathcal{H}_B$ から $\mathcal{H}_D$ への復号化 ν_α を選ぶと，

$$1 - \mathrm{E}_\alpha F_e(\rho_{\mathrm{mix},C}, \nu_\alpha \circ \kappa \circ \tau_\alpha) \leq \frac{6}{ML}\sum_{m,l} \epsilon^B_{m,l} + \frac{1}{M}\sum_{M} \epsilon^E_m \tag{B.20}$$

を満たす．なお，α_m $(m = 1, \dots M)$ はそれぞれ 0 から $L-1$ までの整数に一様な確率で値を取る互いに独立な確率変数とする．また，$\mathcal{H}_C$ と $\mathcal{H}_D$ は自然な対応 $u^C_m \mapsto u^D_m$ の下で同一視することとする．

以下，τ_α 及び ν_α の構成を与える．$\mathcal{H}_C$ から CH_A への等長な写像 $U^A_{C,\alpha}$ を

$$U^A_{C,\alpha} u^C_m \stackrel{\text{def}}{=} \left(u^A_{m,\alpha} \stackrel{\text{def}}{=} \sum_{l=1}^{L} e^{(2l\alpha_m \pi i)/L} u^A_{m,l} \right) \tag{B.21}$$

で定義し，τ_α を $\tau_\alpha(\rho) \stackrel{\text{def}}{=} U^A_{C,\alpha} \rho (U^A_{C,\alpha})^*$ で与えることとする．

次に，$\mathcal{H}_B$ を含む空間 $\mathcal{H}_{B'}$ を W_E の純粋状態化 $\hat{u} \in \mathcal{H}_E \otimes \mathcal{H}_{B'}$ が取れるように十分広く取る．そして，$\mathcal{H}_B$ から $\mathcal{H}_B \otimes \mathcal{H}_D$ への等長写像 $U_B^{B,D}$，$\mathcal{H}_{B'}$ 上のユニタリ行列 $U_{m,\alpha}^{B'}$，及び $\mathcal{H}_{B'} \otimes \mathcal{H}_D$ 上のユニタリ行列 $U_\alpha^{B',D}$ を以下を満たすようにとる．

$$\langle u_m^D | U_B^{B,D} \rho (U_B^{B,D})^* | u_m^D \rangle = \operatorname{Tr} \rho Y_m \quad Y_m \stackrel{\text{def}}{=} \sum_{l=1}^{L} Y_{m,l} \tag{B.22}$$

$$U_{m,\alpha}^{B'} \stackrel{\text{def}}{=} \operatorname*{argmax}_{U} |\langle u_m^D \otimes (U^* \otimes I_E)\hat{u} | U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A \rangle| \tag{B.23}$$

$$U_\alpha^{B',D} \stackrel{\text{def}}{=} \sum_{m=1}^{M} |u_m^D\rangle\langle u_m^D| \otimes U_{m,\alpha}^{B'}. \tag{B.24}$$

なお，１つ目の条件 (B.22) は $U_B^{B,D}$ が $\{Y_m\}_{m=1}^M$ の Naǐmark 拡張を与えることに他ならない．さらに，$\langle u_m^D \otimes ((U_{m,\alpha}^{B'})^* \otimes I_E)\hat{u} | U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A \rangle$ が非負の実数になるように $U_{m,\alpha}^{B'}$ を選ぶこととする．そして，ν_α を以下で与える．

$$\nu_\alpha(\rho) \stackrel{\text{def}}{=} \operatorname{Tr}_{B'} U_\alpha^{B',D} U_B^{B,D} \rho (U_B^{B,D})^* (U_\alpha^{B',D})^*. \tag{B.25}$$

証明:　$\mathcal{H}_C$ の環境系を $\mathcal{H}_R \stackrel{\text{def}}{=} \langle u_1^R, \ldots, u_M^R \rangle$ とすると，

$$\begin{aligned}
&\mathrm{E}_\alpha F_e(\rho_{\mathrm{mix},C}, \nu_\alpha \circ \kappa \circ \tau_\alpha) \\
=&\mathrm{E}_\alpha F\left(\frac{1}{\sqrt{M}} \sum_{m=1}^{M} u_m^R \otimes u_m^C, \nu_\alpha \circ \kappa \circ \tau_\alpha \left(\frac{1}{\sqrt{M}} \sum_{m=1}^{M} u_m^R \otimes u_m^C \right) \right) \\
\le& F\left(\left(\frac{1}{\sqrt{M}} \sum_{m=1}^{M} u_m^R \otimes u_m^C \right) \otimes \hat{u}, \frac{1}{\sqrt{M}} \sum_{m=1}^{M} u_m^R \otimes U_\alpha^{B',D} U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A \right) \\
=&\left| \left\langle \frac{1}{\sqrt{M}} \sum_{m'=1}^{M} u_{m'}^R \otimes u_{m'}^C \otimes \hat{u} \right| \left. \frac{1}{\sqrt{M}} \sum_{m=1}^{M} u_m^R \otimes U_\alpha^{B',D} U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A \right\rangle \right| \\
=&\left| \frac{1}{M} \sum_{m=1}^{M} \left\langle u_m^C \otimes \hat{u} \left| U_\alpha^{B',D} U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A \right. \right\rangle \right| \\
=&\frac{1}{M} \sum_{m=1}^{M} \left\langle u_m^C \otimes \hat{u} \left| U_\alpha^{B',D} U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A \right. \right\rangle \\
=&\frac{1}{M} \sum_{m=1}^{M} F(U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A, u_m^C \otimes (U_{m,\alpha}^{B'})^* \hat{u})
\end{aligned} \tag{B.26}$$

を得る．以下 $1 - F(U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A, u_m^C \otimes (U_{m,\alpha}^{B'})^* \hat{u})$ を評価することにする．なお，以下では関係式 $b^2(\rho,\sigma) = 1 - F(\rho,\sigma)$ は頻繁に用いられるので注意．この評価のために，空間 $\mathcal{H}_{B'}$ を含む十分大きい空間 $\mathcal{H}_{B''}$ と m に応じた $\mathcal{H}_{B''}$ 上の PVM $E^m = \{E_l^m\}_{l=1}^L$ を

$$\begin{aligned}
&\operatorname{Tr} \rho Y_{m,l} (= \operatorname{Tr} \sqrt{Y_m} \rho \sqrt{Y_m} (\sqrt{Y_m})^{-1} \rho Y_{m,l} (\sqrt{Y_m})^{-1}) \\
=& \operatorname{Tr}(|u_m^D\rangle\langle u_m^D| \otimes E_l^m) U_B^{B,D} \rho (U_B^{B,D})^* \\
&\left(= \operatorname{Tr}(I_D \otimes E_l^m)(|u_m^D\rangle\langle u_m^D| \otimes I_B) U_B^{B,D} \rho (U_B^{B,D})^* (|u_m^D\rangle\langle u_m^D| \otimes I_B) \right)
\end{aligned}$$

を満たすように選ぶ，そして，$\mathcal{H}_{B'',E}$ 上の長さ 1 のベクトルを $u_{m,l}^{B'',E}$ を

$$u_m^D \otimes u_{m,l}^{B'',E} \stackrel{\text{def}}{=} \frac{1}{\sqrt{1-\epsilon_{m,l}^E}} (|u_m^D\rangle\langle u_m^D| \otimes E_l^m) U_B^{B,D} U_A^{B,E} u_{m,l}^A$$

とし，

$$U_{m,\alpha}^{B''} \stackrel{\text{def}}{=} \operatorname*{argmax}_U F\left(\frac{1}{\sqrt{L}} \sum_{l=1}^L e^{(2l\alpha_m \pi i)/L} u_m^D \otimes u_{m,l}^{B'',E}, u_m^C \otimes (U)^* \hat{u} \right)$$

とすると，

$$\begin{aligned}
& b^2(U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A, u_m^C \otimes (U_{m,\alpha}^{B'})^* \hat{u}) \le b^2(U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A, u_m^C \otimes (U_{m,\alpha}^{B''})^* \hat{u}) \\
\le & 2b^2 \left(\frac{1}{\sqrt{L}} \sum_{l=1}^L e^{(2l\alpha_m \pi i)/L} u_m^D \otimes u_{m,l}^{B'',E}, u_m^C \otimes (U_{m,\alpha}^{B''})^* \hat{u} \right) \\
& + 2b^2 \left(U_B^{B,D} U_A^{B,E} u_{m,\alpha}^A, \frac{1}{\sqrt{L}} \sum_{l=1}^L e^{(2l\alpha_m \pi i)/L} u_m^D \otimes u_{m,l}^{B'',E} \right) \qquad \text{(B.27)}
\end{aligned}$$

が成り立つ．以下 (B.27) の第 1 項を評価する．

$$\begin{aligned}
& \operatorname{Tr}_{B''} \left| \frac{1}{\sqrt{L}} \sum_{l=1}^L e^{(2l\alpha_m \pi i)/L} u_{m,l}^{B'',E} \right\rangle \left\langle \frac{1}{\sqrt{L}} \sum_{l'=1}^L e^{(2l'\alpha_m \pi i)/L} u_{m,l'}^{B'',E} \right| \\
=& \operatorname{Tr}_{B''} \sum_{l''=1}^L (E_{l''}^m \otimes I_E) \frac{1}{L} \sum_{l=1}^L \sum_{l'=1}^L e^{(2(l-l')\alpha_m \pi i)/L} \left| u_{m,l}^{B'',E} a \right\rangle \left\langle u_{m,l'}^{B'',E} \right| (E_{l''}^m \otimes I_E) \\
=& \operatorname{Tr}_{B''} \sum_{l=1}^L \frac{1}{L} \left| u_{m,l}^{B'',E} \right\rangle \left\langle u_{m,l}^{B'',E} \right|
\end{aligned}$$

と $U_{m,\alpha}^{B''}$ の定義に注意して，補題 8.2 を用いると，

$$\begin{aligned}
& b^2 \left(\frac{1}{\sqrt{L}} \sum_{l=1}^L e^{(2l\alpha_m \pi i)/L} u_m^D \otimes u_{m,l}^{B'',E}, u_m^C \otimes (U_{m,\alpha}^{B''})^* \hat{u} \right) \\
=& b^2 \left(\frac{1}{\sqrt{L}} \sum_{l=1}^L e^{(2l\alpha_m \pi i)/L} u_{m,l}^{B'',E}, (U_{m,\alpha}^{B''})^* \hat{u} \right) \\
=& b^2 \left(\operatorname{Tr}_{B''} \sum_{l=1}^L \frac{1}{L} \left| u_{m,l}^{B'',E} \right\rangle \left\langle u_{m,l}^{B'',E} \right|, W_E \right) \\
\le & 2b^2 \left(\operatorname{Tr}_{B''} \sum_{l=1}^L \frac{1}{L} \left| u_{m,l}^{B'',E} \right\rangle \left\langle u_{m,l}^{B'',E} \right|, \sum_{l=1}^L \frac{1}{L} \operatorname{Tr}_{B,D} \left| U_B^{B,D} U_A^{B,E} u_{m,l}^A \right\rangle \left\langle U_B^{B,D} U_A^{B,E} u_{m,l}^A \right| \right) \\
& + 2b^2 \left(\sum_{l=1}^L \frac{1}{L} W_{m,l}^E, W_E \right) \qquad \text{(B.28)}
\end{aligned}$$

を得る．なお，ここで $\mathrm{Tr}_{B,D}\left|U_B^{B,D}U_A^{B,E}u_{m,l}^A\right\rangle\left\langle U_B^{B,D}U_A^{B,E}u_{m,l}^A\right| = W_{m,l}^E$ となることを用いた．(B.28) の第 2 項については，(5.22) より，

$$b^2\left(\sum_{l=1}^L \frac{1}{L}W_{m,l}^E, W_E\right) \le \frac{1}{2}\left\|\sum_{l=1}^L \frac{1}{L}W_{m,l}^E - W_E\right\|_1 \le \frac{1}{2}\epsilon_m^E \tag{B.29}$$

を得る．さらに，(B.28) の第 1 項については，

$$\begin{aligned}
&b^2\left(\mathrm{Tr}_{B''}\sum_{l=1}^L \frac{1}{L}\left|u_{m,l}^{B'',E}\right\rangle\left\langle u_{m,l}^{B'',E}\right|, \sum_{l=1}^L \frac{1}{L}\mathrm{Tr}_{B,D}\left|U_B^{B,D}U_A^{B,E}u_{m,l}^A\right\rangle\left\langle U_B^{B,D}U_A^{B,E}u_{m,l}^A\right|\right)\\
\le&\sum_{l=1}^L \frac{1}{L}b^2\left(\mathrm{Tr}_{B''}\left|u_{m,l}^{B'',E}\right\rangle\left\langle u_{m,l}^{B'',E}\right|, \mathrm{Tr}_{B'',D}\left|U_B^{B,D}U_A^{B,E}u_{m,l}^A\right\rangle\left\langle U_B^{B,D}U_A^{B,E}u_{m,l}^A\right|\right)\\
\le&\sum_{l=1}^L \frac{1}{L}b^2\left(u_m^D\otimes u_{m,l}^{B'',E}, U_B^{B,D}U_A^{B,E}u_{m,l}^A\right) = \sum_{l=1}^L \frac{1}{L}\left(1-\sqrt{1-\epsilon_{m,l}^B}\right) \le \sum_{l=1}^L \frac{1}{L}\epsilon_{m,l}^B
\end{aligned} \tag{B.30}$$

となる．ここで $\mathrm{Tr}_{B''}\left|u_{m,l}^{B'',E}\right\rangle\left\langle u_{m,l}^{B'',E}\right| = \mathrm{Tr}_{B'',D}\left|u_m^D\otimes u_{m,l}^{B'',E}\right\rangle\left\langle u_m^D\otimes u_{m,l}^{B'',E}\right|$ を用いた．次に (B.27) の第 2 項を評価する．

$$\begin{aligned}
&\mathrm{E}_\alpha F\left(U_B^{B,D}U_A^{B,E}u_{m,\alpha}^A, \frac{1}{\sqrt{L}}\sum_{l=1}^L e^{(2l\alpha_m\pi i)/L}u_m^D\otimes u_{m,l}^{B'',E}\right)\\
=&\mathrm{E}_\alpha\left\langle \frac{1}{\sqrt{L}}\sum_{l=1}^L e^{(2l\alpha_m\pi i)/L}U_B^{B,D}U_A^{B,E}u_{m,l}^A, \frac{1}{\sqrt{L}}\sum_{l=1}^L e^{(2l\alpha_m\pi i)/L}u_m^D\otimes u_{m,l}^{B'',E}\right\rangle\\
=&\frac{1}{L}\sum_{l=1}^L\sum_{l'=1}^L(\mathrm{E}_\alpha e^{(2(l-l')\alpha_m\pi i)/L})\left\langle U_B^{B,D}U_A^{B,E}u_{m,l'}^A, u_m^D\otimes u_{m,l}^{B'',E}\right\rangle\\
=&\frac{1}{L}\sum_{l=1}^L\langle U_B^{B,D}U_A^{B,E}u_{m,l}^A, u_m^D\otimes u_{m,l}^{B'',E}\rangle\\
=&\frac{1}{L}\sum_{l=1}^L\left\langle U_B^{B,D}U_A^{B,E}u_{m,l}^A, \frac{1}{\sqrt{1-\epsilon_{m,l}^E}}(|u_m^D\rangle\langle u_m^D|\otimes E_l^m)U_B^{B,D}U_A^{B,E}u_{m,\alpha}^A\right\rangle\\
=&\frac{1}{L}\sum_{l=1}^L\sqrt{1-\epsilon_{m,l}^E} \ge \frac{1}{L}\sum_{l=1}^L(1-\epsilon_{m,l}^E)
\end{aligned} \tag{B.31}$$

したがって，(B.26) に (B.27),(B.28),(B.29), (B.30),(B.31) を組み合わせることで，(B.20) を得る． □

B.7　補題 10.3 の証明

次に補題 10.3 の証明のために以下の補題を示す．

補題 B.4　$\mathcal{X}$ から $\mathcal{S}(\mathcal{K})$ への写像として visible な符号器は表されるが，T, T' について凸結合

$$(\lambda T+(1-\lambda)T')(x) \stackrel{\mathrm{def}}{=} \lambda T(x)+(1-\lambda)T'(x), \quad 0<\forall\lambda<1$$

を考えると，visible な符号器のなす集合は凸集合になり，その端点（定義については A.4 節を見よ.）の集合は

$$\{T\,|T(x) \text{ は純粋状態 } \forall x\in\mathcal{X}\}. \tag{B.32}$$

と一致する.

証明:　各 x に対して，$T(x)$ が純粋状態になるとき，符号器 T を異なる符号器の凸結合で表すことは不可能なので，T は端点である．したがって，任意の visible な符号器 $T(x)=\sum_{j_x} s_{j_x}|\phi_{j_x}\rangle\langle\phi_{j_x}|$ が上の条件を満たす符号器の凸結合で表されることを示せば十分である．そのために，visible な符号器 $T(j_1,j_2,\ldots,j_n)$ を

$$T(j_1,j_2,\ldots,j_n|i)=|\phi_{j_x}\rangle\langle\phi_{j_x}|$$

で定義すると，これは (B.32) に属する．従って，$T=\sum_{j_1,j_2,\ldots,j_n} s_{j_1}s_{j_2}\cdots s_{j_n}$ $T(j_1,j_2,\cdots,j_n)$ となることから，補題を得る.　□

さらに補題 10.3 の証明には以下の補題が必要となる。この補題は 8.4 節でエンタングルメントの観点から証明される定理 8.3 と同値な内容である。

補題 B.5　$\rho\in\mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B)$ が separable であるとき，任意の整数 k について不等式

$$\begin{aligned}&\max\{\mathrm{Tr}\,P\rho_A|P:\mathcal{H}_A\text{上の射影，}\mathrm{rank}\,P=k\}\\ \geq&\max\{\mathrm{Tr}\,P\rho|P:\mathcal{H}_A\otimes\mathcal{H}_B\text{上の射影，}\mathrm{rank}\,P=k\}\end{aligned}$$

が成立する.

補題 10.3 の証明:　補題 B.4 より，(B.32) に属す visible な符号 T に対して，(10.13) を示せば十分である．定理 5.1 の条件⑥より，$\mathcal{H}$ と同じ次元の空間 $\mathcal{H}'$ と $\mathcal{H}'\otimes\mathcal{H}$ 上の純粋状態 ρ_0 と $\mathcal{K}\otimes\mathcal{H}'\otimes\mathcal{H}$ 上のユニタリ行列 U を適切に選ぶと，$\nu(\rho)=\mathrm{Tr}_{\mathcal{K},\mathcal{H}'}U(\rho\otimes\rho_0)U^*$ となり，

$$\rho_x \stackrel{\mathrm{def}}{=} \frac{(W_x\otimes I)\,U\,(T(x)\otimes\rho_0)\,U^*\,(W_x\otimes I)}{\mathrm{Tr}\,U\,(T(x)\otimes\rho_0)\,U^*\,(W_x\otimes I)}\in\mathcal{S}(\mathcal{K}\otimes\mathcal{H}\otimes\mathcal{H}')$$

は純粋状態となる。さらに、$UT(x)\otimes\rho_0U^*$ が純粋状態であり，$(W_x\otimes I)$ が射影であることに注意すると，

$$\mathrm{Tr}\,\nu(T(x))W_x=\mathrm{Tr}UT(x)\otimes\rho_0U^*\,(W_x\otimes I)=\mathrm{Tr}U(T(x)\otimes\rho_0)\,U^*\rho_x \tag{B.33}$$

が成り立つ．$\mathrm{Tr}_{\mathcal{K},\mathcal{H}'}\rho_x=W_x$ であるから，ρ_x は適切に純粋状態 $\sigma_x\in\mathcal{S}(\mathcal{K}\otimes\mathcal{H}')$ を選ぶことにより，$\rho_x=W_x\otimes\sigma_x$ と書ける．したがって，状態 $\rho_p \stackrel{\mathrm{def}}{=} \sum_{i\in\mathcal{X}}p(x)\rho_x=\sum_{x\in\mathcal{X}}p(x)W_x\otimes\sigma_x$ は separable となり，$W_p=\mathrm{Tr}_{\mathcal{H},\mathcal{K}'}\rho_p$

を満たす．$I_{\mathcal{K}} \geq T(x)$ であるから，$U\left(I_{\mathcal{K}} \otimes \rho_0\right) U^* \geq U\left(T(x) \otimes \rho_0\right) U^*$ が成り立つ．それゆえ，(B.33) より，

$$
\begin{aligned}
&\sum_{x \in \mathcal{X}} p(x) \operatorname{Tr} \nu(T(x)) W_x = \sum_{x \in \mathcal{X}} p(x) \operatorname{Tr}_{\mathcal{H}} \operatorname{Tr}_{\mathcal{K} \otimes \mathcal{H}'} U\left(T(x) \otimes \rho_0\right) U^* \rho_x \\
&\leq \sum_{x \in \mathcal{X}} p(x) \operatorname{Tr} U\left(I_{\mathcal{K}} \otimes \rho_0\right) U^* \rho_x = \operatorname{Tr} U\left(I_{\mathcal{K}} \otimes \rho_0\right) U^* \rho_p \qquad \text{(B.34)}
\end{aligned}
$$

が成り立つ．さらに，関係式 $I \geq U\left(I_{\mathcal{K}} \otimes \rho_0\right) U^* \geq 0$ と $\operatorname{Tr} U\left(I_{\mathcal{K}} \otimes \rho_0\right) U^* = \operatorname{Tr} I_{\mathcal{K}} = \dim \mathcal{K}$ から，

$$
\begin{aligned}
&\operatorname{Tr} U\left(I_{\mathcal{K}} \otimes \rho_0\right) U^* \rho_p \leq \max \left\{ \operatorname{Tr} P \rho_p \,\middle|\, \begin{array}{l} P : \mathcal{K} \otimes \mathcal{H} \otimes \mathcal{H}' \text{上の射影}, \\ \operatorname{rank} P = \dim \mathcal{K} \end{array} \right\} \\
&\leq \max\{\operatorname{Tr} P W_p | P : \mathcal{H} \text{ 上の射影}, \operatorname{rank} P = \dim \mathcal{K}\} \qquad \text{(B.35)}
\end{aligned}
$$

が得られる．なお，(B.35) は ρ_p が separable であることと，補題 B.5 より得られる．特に $\mathcal{H}$ 上の射影 P は

$$
\operatorname{Tr}(W_p - a) P \leq \operatorname{Tr}(W_p - a)\{W_p - a \geq 0\}
$$

を満たし，P の rank が $\dim \mathcal{K}$ であれば ($\operatorname{Tr} P = \dim \mathcal{K}$ であれば)，

$$
\operatorname{Tr} W_p P \leq a \dim \mathcal{K} + \operatorname{Tr} W_p \{W_p - a \geq 0\}. \qquad \text{(B.36)}
$$

となる．(B.34), (B.35), (B.36) から

$$
\begin{aligned}
&1 - \varepsilon(\Psi) = \sum_{x \in \mathcal{X}} p(x) \operatorname{Tr} \nu(T(x)) W_x \\
&\leq \max\{\operatorname{Tr} P W_p | P : \mathcal{H} \text{ 上の射影 }, \operatorname{rank} P = \dim \mathcal{K}\} \\
&\leq a \dim \mathcal{K} + \operatorname{Tr} W_p \{W_p - a \geq 0\}
\end{aligned}
$$

となり (10.13) を得る． □