2020年8月26日

量子情報数理特論
（第15回）古典・量子通信路符号化定理

電気通信大学 大学院情報理工学研究科

小川朋宏

14　古典・量子通信路符号化定理

前回補足：情報スペクトル的極限定理（その２）

Theorem 1 (情報スペクトル的極限定理１，前回証明). 任意の$a \in \mathbb{R}$について，

$$\mathrm{Tr}\,\rho_n S_n(a) = \mathrm{Tr}\,\rho^{\otimes n}\{\rho^{\otimes n} - e^{na}\sigma^{\otimes n} > 0\} \overset{n\to\infty}{\longrightarrow} \begin{cases} 1 & a < D(\rho||\sigma) \\ 0 & a > D(\rho||\sigma) \end{cases} \tag{1}$$

Theorem 2 (情報スペクトル的極限定理２). 任意の$a \in \mathbb{R}$について，

$$\mathrm{Tr}\left(\rho^{\otimes n} - e^{na}\sigma^{\otimes n}\right)_+ \overset{n\to\infty}{\longrightarrow} \begin{cases} 1 & a < D(\rho||\sigma) \\ 0 & a > D(\rho||\sigma) \end{cases} \tag{2}$$

（証明）$a < D(\rho||\sigma)$のとき，$a < b < D(\rho||\sigma)$となる実数bがとれて，

$$\begin{aligned} 0 \le 1 - \mathrm{Tr}(\rho_n - e^{na}\sigma_n)_+ &= \min_{0\le T_n \le I_n} \{\mathrm{Tr}\,\rho_n\,(I_n - T_n) + e^{na}\,\mathrm{Tr}\,\sigma_n T_n\} \\ &\le \alpha_n(S_n(b)) + e^{na}\beta_n(S_n(b)) \\ &\le \alpha_n(S_n(b)) + e^{na}e^{-nb} \longrightarrow 0 \quad (n\to\infty) \end{aligned}$$

ただし，最後の不等式では$\beta_n(S_n(b)) \le e^{-nb}$を用いた．一方，$a > D(\rho||\sigma)$のとき，

$$0 \le \mathrm{Tr}\left(\rho^{\otimes n} - e^{na}\sigma^{\otimes n}\right)_+ = \mathrm{Tr}\left[\left(\rho^{\otimes n} - e^{na}\sigma^{\otimes n}\right) S_n(a)\right] \le \mathrm{Tr}\,\rho^{\otimes n} S_n(a) \longrightarrow 0 \quad (n\to\infty)$$

14.1　古典・量子通信路

Definition 1. 量子通信路において，古典入力シグナルから出力量子状態への対応を古典・量子通信路 (classical-quantum channel, cq channel) とよぶ（途中のCPTP写像は省略して考える）.

$$W : x \in \mathcal{X} \text{ (有限集合，古典シグナルの集合)} \longmapsto W_x \in \mathcal{S}(\mathcal{H}) \text{ (密度行列の集合)}$$

14.2　i.i.d. 拡張

- 古典・量子通信路Wのi.i.d. 拡大

$$\begin{array}{ccc} x_1 & \to \boxed{W} \to & W_{x_1} \\ x_2 & \to \boxed{W} \to & W_{x_2} \\ \vdots & & \vdots \\ x_n & \to \boxed{W} \to & W_{x_n} \end{array}$$

- 記法：上を次のように書く

$$x^n := (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n \to \boxed{W^n} \to W_{x^n} := W_{x_1} \otimes W_{x_2} \otimes \cdots \otimes W_{x_n} \in \mathcal{S}(\mathcal{H}^{\otimes n})$$

- 確率$P(x)$のi.i.d. 拡張

$$P^n(x^n) = P(x_1)P(x_2)\ldots P(x_n)$$

$k \in \{1, 2, \cdots, M_n\}$　メッセージ

$\Downarrow \varphi^{(n)}$　符号器 (encoder)

$$\begin{array}{ccccccccc} \varphi^{(n)}(k) & = & x_1(k) & , & x_2(k) & , & \cdots & , & x_n(k) \\ & & \downarrow & & \downarrow & & & & \downarrow \\ & & \downarrow & & \downarrow & & & & \downarrow \\ & & \downarrow & & \downarrow & & & & \downarrow \\ W^{(n)}_{\varphi^{(n)}(k)} & = & W_{x_1(k)} & \otimes & W_{x_2(k)} & \otimes & \cdots & \otimes & W_{x_n(k)} \end{array}$$

$\Downarrow X^{(n)} = \{X_0^{(n)}, X_1^{(n)}, \ldots, X_{M_n}^{(n)}\}$（$\mathcal{H}_n = \mathcal{H}^{\otimes n}$ 上の POVM）　復号器 (decoder)

$l \in \{0, 1, 2, \cdots, M_n\}$　復号メッセージ（0 は復号失敗を表す）

Definition 2 (平均誤り確率)**.**

$$\mathrm{Pe}(\varphi^{(n)}, X^{(n)}) := \frac{1}{M_n} \sum_{k=1}^{M_n} \left(1 - \mathrm{Tr}\, W^{(n)}_{\varphi^{(n)}(k)} X_k^{(n)}\right) \tag{3}$$

Definition 3. 符号の列 $(\varphi^{(n)}, X^{(n)})$ $(n = 1, 2, \dots)$ が存在して，以下が満たされるとき，
符号化レート R は達成可能(achievable)であるという．

$$\liminf_{n\to\infty} \frac{1}{n} \log M_n \geq R \quad \text{（符号化レートが漸近的に } R \text{ 以上）} \tag{4}$$

$$\lim_{n\to\infty} \mathrm{Pe}(\varphi^{(n)}, X^{(n)}) = 0 \quad \text{（漸近的にエラーゼロ）} \tag{5}$$

Definition 4 (古典・量子通信路容量).

$$C(W) := \sup \{\, R \mid R \text{ は achievable} \,\} \tag{6}$$

Theorem 3 (古典・量子通信路符号化定理，Holevo-Schumacher-Westmoreland の定理).

$$C(W) = \max_{P \in \mathcal{P}(\mathcal{X})} I(P, W) \tag{7}$$

ここで，$I(P, W)$ はHolevo相互情報量：

$$I(P, W) = \sum_x P(x) D(W_x || W_P) \quad \text{where} \quad W_P := \sum_x P(x) W_x$$

14.5　相互情報量に関連した漸近的挙動

- Holevo相互情報量は拡大量子状態の量子相対エントロピー$I(P;W)=D(R||S)$ である

$$R=\bigoplus_x P(x)W_x=\begin{pmatrix} P(1)\,W_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & P(N)\,W_N \end{pmatrix},\quad S=\bigoplus_x P(x)W_P=\begin{pmatrix} P(1)\,W_P & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & P(N)\,W_P \end{pmatrix}$$

よって，量子仮説検定の理論により，

Lemma 1. 任意の$a\in\mathbb{R}$について，

$$\begin{aligned}\operatorname{Tr} R^{\otimes n}\{R^{\otimes n}-e^{na}S^{\otimes n}>0\}&=\sum_{x^n\in\mathcal{X}^n}P^n(x^n)\operatorname{Tr}W_{x^n}^n\{W_{x^n}^n-e^{na}W_P^{\otimes n}>0\}\\ &\overset{n\to\infty}{\longrightarrow}\begin{cases}1 & a<I(P;W)\\ 0 & a>I(P;W)\end{cases}\end{aligned}\tag{8}$$

上記等式では，以下の式と，トレースがブロックごとに計算出来ることを利用している

$$R^{\otimes n}=\left(\bigoplus_{x\in\mathcal{X}}P(x)W_x\right)^{\otimes n}=\bigoplus_{x^n\in\mathcal{X}^n}P^n(x^n)W_{x^n}^n$$

$$S^{\otimes n}=\left(\bigoplus_{x\in\mathcal{X}}P(x)W_P\right)^{\otimes n}=\bigoplus_{x^n\in\mathcal{X}^n}P^n(x^n)W_P^{\otimes n}$$

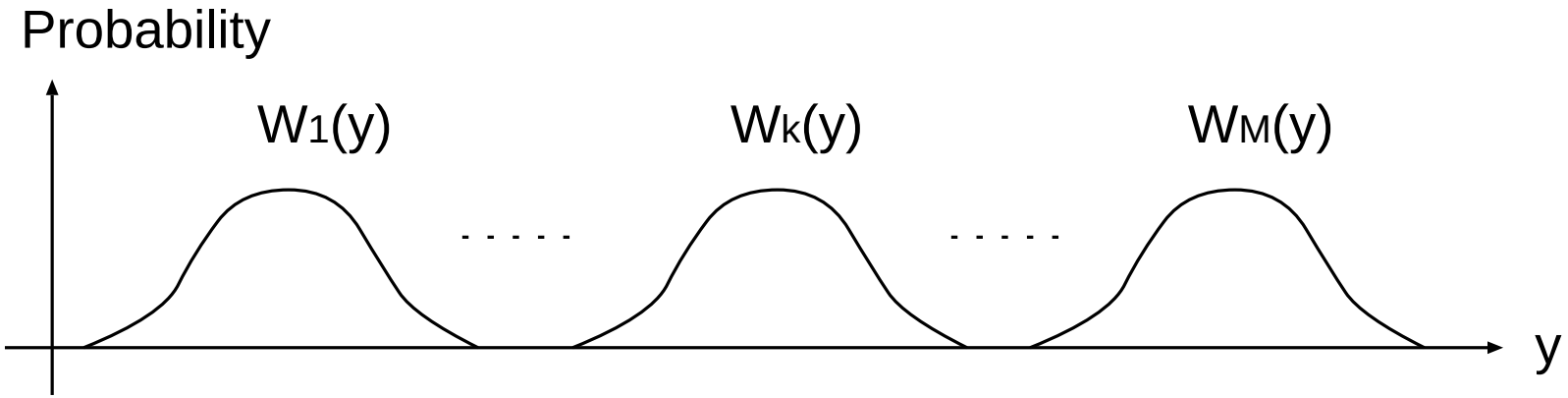
14.6　通信路符号化（メッセージ伝送）：古典系

古典通信路$W_1(y), W_2(y), \ldots, W_M(y)$の出力$y$から入力$k$を当てる問題

$$k \in \{1, 2, \ldots, M\} \longrightarrow \boxed{W(y|k) = W_k(y)} \longrightarrow y$$

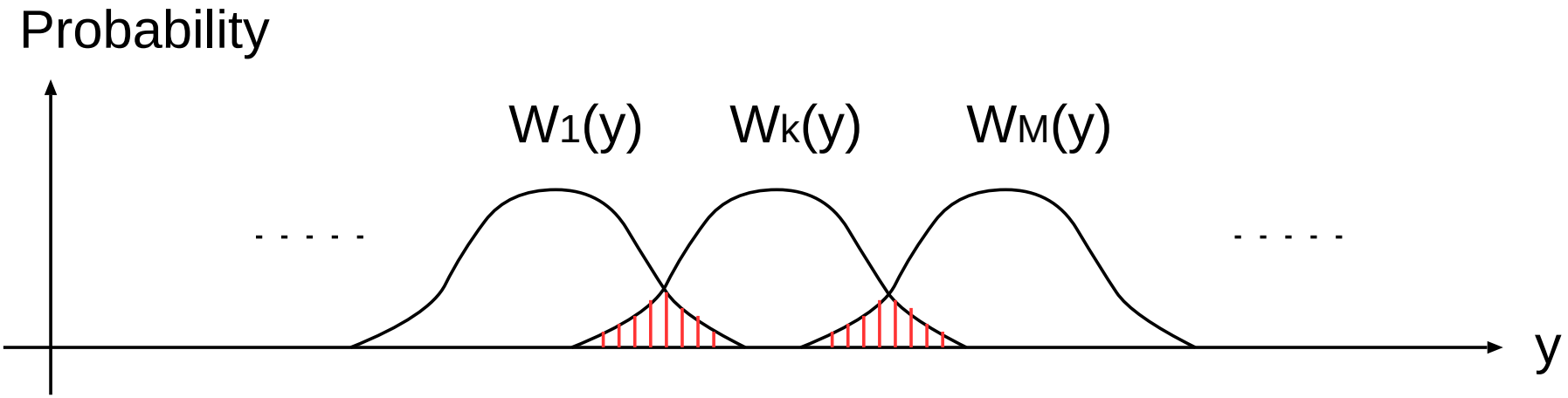
候補が3つ以上の仮説検定問題（候補が2つだけ：単純仮説検定）

- trivial zero error case



  $W_k(y)$とその他$W_l(y)$ $(l \neq k)$のオーバラップがない
- yを観測することでkをゼロエラーで識別できる

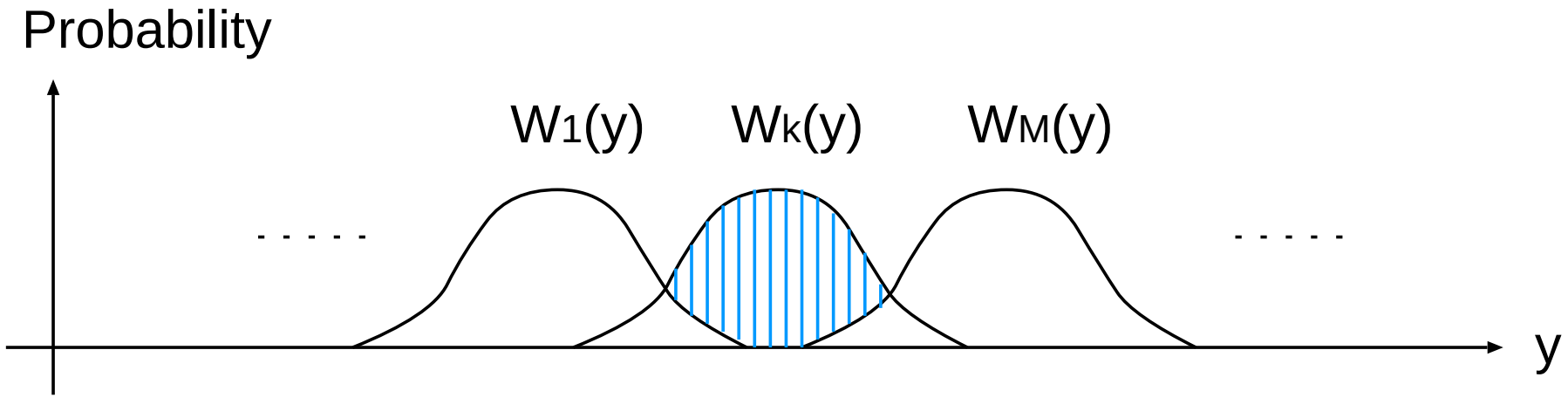
14.7 An Overlap Measure：単純仮説検定への帰着



- W_k とそれ以外 W_l $(l \neq k)$ の（ある種の）Bayes重みエラーを考える
- $T \subset \mathcal{Y}$ を k の受容域(acceptance region)とすると

$$P_e(k) := \min_{T \subset \mathcal{Y}} \left\{ \sum_{y \in T^c} W_k(y) + \sum_{l \neq k} \sum_{y \in T} W_l(y) \right\} \quad \text{1st kind + 2nd kind}$$

$$= \min_{T \subset \mathcal{Y}} \left\{ 1 - \sum_{y \in T} \left(W_k(y) - \sum_{l \neq k} W_l(y) \right) \right\}$$



- $P_s(k) := 1 - P_e(k)$： W_k とそれ以外を識別するときの成功確率（と無理やり思う）

$$P_s(k) = 1 - P_e(k) = \max_{T \subset \mathcal{Y}} \sum_{y \in T} \left(W_k(y) - \sum_{l \neq k} W_l(y) \right)$$

$$= \sum_{y} \left(W_k(y) - \sum_{l \neq k} W_l(y) \right)_+$$

ただし，$(F(x))_+ = \max\{0, F(x)\}$

14.9　単純仮説検定への帰着（量子系）

古典・量子通信路$W_1, W_2, \ldots, W_M$（密度行列）が与えられているとき，出力量子状態をPOVM測定することでkを当てる問題

$$k \in \{1, 2, \ldots, M\} \longrightarrow \boxed{W_k} \longrightarrow \boxed{\text{POVM}} \longrightarrow \widehat{k}$$

古典系と同様にoverlap measureを考える

- $P_s(k) = 1 - P_e(k)$：W_kとそれ以外を識別するBayes成功確率を考える

$$P_s(k) = \max_{0 \le T \le I} \mathrm{Tr}\left(W_k - \sum_{l \neq k} W_l\right) T = \mathrm{Tr}\left(W_k - \sum_{l \neq k} W_l\right)_+$$

14.10　漸近論：overlapの情報量スペクトル的解析

問題設定　$\{W_{x^n}^n\}_{x^n\in\mathcal{X}^n}$ に対して，$M_n = e^{nR}$ 個の入力を選んでoverlap $\max_k P_e(k) = \max_k\{1-P_s(k)\}$ がゼロになるようにする

$$\varphi_n : k \in \{1,2,\ldots,M_n\} \longmapsto x_k^n = \varphi_n(k) \longmapsto W_{\varphi_n(k)}^n$$

Theorem 4 (相互情報量はsharp limit)**.**

(1) (achievability) Choosing $\varphi_n(k)$ $(k=1,2,\ldots,M_n)$ randomly subject to $P^n(x^n)$, we have

$$\lim_{n\to\infty} E\left[\mathrm{Tr}\left(W_{\varphi_n(k)}^n - \sum_{l\neq k} W_{\varphi_n(l)}^n\right)_+\right] = 1 \quad \text{if } R < I(P,W)$$

(2) (strong converse) For any $\{\varphi_n\}_{n=1}^\infty$, we have

$$\lim_{n\to\infty} \max_{k\in[1,M_n]} \mathrm{Tr}\left(W_{\varphi_n(k)}^n - \sum_{l\neq k} W_{\varphi_n(l)}^n\right)_+ = 0 \quad \text{if } R > I(P,W),$$

14.11 proof of (1) achievability

Given a cq channel $x \in \mathcal{X} \mapsto W_x$ and a map $k \in \{1, 2, \ldots, M\} \mapsto \varphi(k) \in \mathcal{X}$, for any $P(x)$, $a \in \mathbb{R}$, and $k \in \{1, 2, \ldots, M\}$, it obviously holds that

$$\mathrm{Tr}\left(W_{\varphi(k)} - \sum_{l \neq k} W_{\varphi(l)}\right)_+ \geq \mathrm{Tr}\left(W_{\varphi(k)} - \sum_{l \neq k} W_{\varphi(l)}\right)\left\{W_{\varphi(k)} - e^{na} W_P > 0\right\}.$$

Taking expectation, we have

$$\begin{aligned}
&E\left[\mathrm{Tr}\left(W^n_{\varphi_n(k)} - \sum_{l \neq k} W^n_{\varphi_n(l)}\right)_+\right] \\
&\geq E\left[\mathrm{Tr}\, W_{\varphi_n(k)}\left\{W_{\varphi_n(k)} - e^{na} W_P > 0\right\}\right] - M_n \cdot E\left[\mathrm{Tr}\, W_P\left\{W_{\varphi_n(k)} - e^{na} W_P > 0\right\}\right] \\
&\geq (1 - e^{nR} e^{-na}) E_{P^n}\left[\mathrm{Tr}\, W^n_{x^n}\left\{W^n_{x^n} - e^a W^n_{P^n} > 0\right\}\right].
\end{aligned}$$

If $R < I(P, W)$, then there exists $R < a < I(P, W)$, and the property (8) of $I(P, W)$ assures that RHS $\to 1$ $(n \to \infty)$

14.12　通信路符号化の誤り確率との関係

cq channel $W : x \mapsto W_x$ と符号器 $\varphi : k \mapsto \varphi(k) \in \mathcal{X}$

$$k \in \{1, 2, \ldots, M\} \to \varphi(k) \to \boxed{W_{\varphi(k)}} \to \boxed{\text{POVM } Y = \{Y_l\}_{l=0}^{M}} \to \widehat{k} = l,$$

復号器 Y (POVM) が与えられると，誤り確率 $\mathrm{Pe}(k; \varphi, Y)$ が自然に定まる

Theorem 5. For any map $\varphi : \{1, 2, \ldots, M\} \to \mathcal{X}$
there exists POVM $Y = \{Y_k\}_{k=0}^{M}$ such that for any k and T $(0 \le T \le I)$

$$\mathrm{Pe}(k; \varphi, Y) \le \mathrm{Tr}\, W_{\varphi(k)}(I - T) + \mathrm{Tr}\left(\sum_{l \ne k} W_{\varphi(l)}\right) T \tag{9}$$

holds. Taking the minimum w.r.t. $0 \le T \le I$, we have

$$Pe(k; \varphi, Y) \le 1 - \mathrm{Tr}\left(W_k - \sum_{l \ne k} W_l\right)_+ \tag{10}$$

これと Theorem 4 より，$R < I(P, W)$ であれば，R が achievable であることが示される．すなわち，

$$C(W) \ge I(P, W) \tag{11}$$

が示された．

14.13 sketch proof

- POVM $Y = \{Y_k\}_{k=0}^M$ is constructed by Beigi-Gohari (2014) [*1]

$$Y_k = \begin{cases} T_\varphi^{-1/2} W_{\varphi(k)} T_\varphi^{-1/2} & (k = 1, 2, \dots, M) \\ I - \mathrm{suppot}(T_\varphi) & (k = 0) \end{cases}, \quad T_\varphi = \sum_{l=1}^M W_{\varphi(l)}$$

  T_φ^{-1} is the generalized inverse satisfying $T_\varphi^{-1/2} T_\varphi T_\varphi^{-1/2} = s(T_\varphi)$
- monotonicity of the Sandwiched Renyi divergence for $\alpha = 2$
  (Collision relative entropy)

$$D_\alpha^*(A||B) = \frac{1}{\alpha - 1} \log Q_\alpha^*(A||B) - \frac{1}{\alpha - 1} \log \mathrm{Tr}\, A$$
$$Q_\alpha^*(A||B) = \mathrm{Tr} \left(B^{\frac{1-\alpha}{2\alpha}} A B^{\frac{1-\alpha}{2\alpha}} \right)^\alpha$$
$$Q_2^*(A||B) = \mathrm{Tr} \left(B^{-1/4} A B^{-1/4} \right)^2 = \mathrm{Tr} \left(A \cdot B^{-1/2} A B^{-1/2} \right)$$

Let

$$W_k = W_{\varphi(k)}, \quad V_k = \sum_{l \neq k} W_{\varphi(l)}$$

[*1] $*$ S. Beigi and A. Gohari, "Quantum achievability proof via collision relative entropy," *IEEE Trans. Inform. Theory*, vol. 60, pp. 7980–7986, 2014.

For simplicity, we neglect the support treatment. Then we have

$$Y_k = (W_k + V_k)^{-1/2} W_k (W_k + V_k)^{-1/2}$$

and

$$\begin{aligned}
&Pe(k; \varphi, Y) = 1 - \operatorname{Tr} W_k (W_k + V_k)^{-1/2} W_k (W_k + V_k)^{-1/2} \\
&= \operatorname{Tr} W_k (W_k + V_k)^{-1/2} V_k (W_k + V_k)^{-1/2} \\
&= \operatorname{Tr} W_k - Q_2^*(W_k || W_k + V_k) \\
&\leq \frac{\operatorname{Tr} W_k T \times \operatorname{Tr} V_k T}{\operatorname{Tr} W_k T + \operatorname{Tr} V_k T} + \frac{\operatorname{Tr} W_k (I - T) \times \operatorname{Tr} V_k (I - T)}{\operatorname{Tr} W_k (I - T) + \operatorname{Tr} V_k (I - T)} \quad \text{monotonicity} \\
&\leq \operatorname{Tr} W_k T + \operatorname{Tr} V_k (I - T)
\end{aligned}$$

14.14 Hayashi-Nagaokaの不等式

Hayashi-Nagaoka (2003)　量子情報理論に飛躍的進歩をもたらした

Given c-q channel $W : x \mapsto W_x$, for any $P(x)$ there exists (φ, Y) such that

$$\mathrm{Pe}(\varphi, Y) \le 2 \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} W_x \{ W_x - e^a W_P \le 0 \} + 4(M-1) \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} W_P \{ W_x - e^a W_P > 0 \}$$

for any $a \in \mathbb{R}$, where $W_P = \sum_{x \in \mathcal{X}} P(x) W_x$.

- (9)式で$T = \{W_{\varphi(k)} - e^a W_P > 0\}$ とおいて，ランダムコーディング$\varphi(k) \overset{i.i.d.}{\sim} P(x)$を考える．
  ランダムコーディングに関する期待値は

$$\begin{aligned}
E\big[\mathrm{Pe}(k; \varphi, Y)\big] &\le E\Big[\operatorname{Tr} W_{\varphi(k)} \{W_{\varphi(k)} - e^a W_P \le 0\}\Big] + E\Big[\operatorname{Tr}\Big(\sum_{l \ne k} W_{\varphi(l)}\Big) \{W_{\varphi(k)} - e^a W_P > 0\}\Big] \\
&= E_{\varphi(k)}\Big[\operatorname{Tr} W_{\varphi(k)} \{W_{\varphi(k)} - e^a W_P \le 0\}\Big] + E_{\varphi(k)}\Big[\operatorname{Tr}\Big(\sum_{l \ne k} E_{\varphi(l)}\big[W_{\varphi(l)}\big]\Big) \{W_{\varphi(k)} - e^a W_P > 0\}\Big] \\
&= \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} W_x \{ W_x - e^a W_P \le 0 \} + (M-1) \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} W_P \{ W_x - e^a W_P > 0 \}
\end{aligned}$$

  よって，ランダムコーディングの論法により，次式を満たす符号(φ, Y)の存在が示された．

$$\mathrm{Pe}(\varphi, Y) \le \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} W_x \{ W_x - e^a W_P \le 0 \} + (M-1) \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} W_P \{ W_x - e^a W_P > 0 \}$$

  Hayashi-Nagaokaの不等式の別証明と係数の改善が得られる．