

量子情報科学ウィンタースクール 量子系の情報量

小川朋宏

電気通信大学 大学院情報システム学研究科

2010 年 2 月 27 日

von Neumann エントロピー

定義 : $\rho \in \mathcal{S}(\mathcal{H})$ の von Neumann エントロピー

$$H(\rho) = -\operatorname{Tr} \rho \log \rho$$

性質 :

(1) 正值性 (positivity)

$$H(\rho) \geq 0 \quad (\text{等号成立} \Leftrightarrow \rho \text{ が純粋状態})$$

(2) 最大値

$$H(\rho) \leq \log \dim \mathcal{H} \quad (\text{等号成立} \Leftrightarrow \rho = I / \dim \mathcal{H})$$

(3) 凹性 (concavity)

任意の密度作用素 ρ_1, ρ_2 と $0 \leq p \leq 1$ に対して

$$H(p\rho_1 + (1-p)\rho_2) \geq pH(\rho_1) + (1-p)H(\rho_2)$$

(4) 劣加法性 (subadditivity)

合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ (二体系) 上の密度作用素 ρ_{AB} に対して

$$H(\rho_A) + H(\rho_B) \geq H(\rho_{AB})$$

(5) 強劣加法性 (strong subadditivity)

合成系 $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ (三体系) 上の密度作用素 ρ_{ABC} に対して

$$H(\rho_{AB}) + H(\rho_{AC}) \geq H(\rho_A) + H(\rho_{ABC})$$

(6) 二体系の密度作用素 ρ_{AB} が純粋状態ならば

$$H(\rho_A) = H(\rho_B)$$

このとき, これを entropy of entanglement という.

他にユニタリ不変性, 加法性を満たす.

量子通信路 (量子操作, quantum operation)

記法: $\mathcal{L}(\mathcal{H})$ はヒルベルト空間 $\mathcal{H}$ 上の線形作用素全体

定義: 量通信路は線形写像

$$\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$$

で, 次の条件を満たすものとして定義される.

(1) 完全正值性 (complete positivity)

任意の系 $\mathcal{H}_R$ と任意の $X_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_R)$ について

$$X_{AB} \geq 0 \Rightarrow (\mathcal{E} \otimes \mathcal{I}_R)(X_{AB}) \geq 0$$

ただし, $\mathcal{I}_R$ は恒等写像である.

(2) トレース保存条件 (trace preserving condition)

任意の $X \in \mathcal{L}(\mathcal{H}_A)$ に対して $\text{Tr}[\mathcal{E}(X)] = \text{Tr}[X]$

量子通信路の表現

Theorem (量子通信路の表現)

写像 $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ について以下は同値 .

(1) $\mathcal{E}$ は量子通信路である .

(2) クラウス表現 (Kraus representation)

線形作用素 $E_i : \mathcal{H}_A \rightarrow \mathcal{H}_B$ の組 $\{E_i\}$ で $\sum_i E_i^* E_i = I_A$ を満たすものが存在して

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*$$

(3) シュタインスプリング表現 (Stinespring representation)

あるヒルベルト空間 $\mathcal{H}_E$ (環境系, environment system) と等距離作用素 (isometry) $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$ が存在して

$$\mathcal{E}(\rho) = \text{Tr}_E[V \rho V^*]$$

量子相対エントロピーとその性質

定義：密度作用素 ρ, σ に対して

$$D(\rho||\sigma) = \text{Tr}[\rho(\log \rho - \log \sigma)]$$

Theorem (単調性, monotonicity)

任意の量子通信路 $\mathcal{E}$ に対して

$$D(\rho||\sigma) \geq D(\mathcal{E}(\rho)||\mathcal{E}(\sigma))$$

Theorem (単調性等号成立条件)

$D(\rho||\sigma) < \infty$ のとき以下は同値 .

- (1) $D(\rho||\sigma) = D(\mathcal{E}(\rho)||\mathcal{E}(\sigma))$
- (2) 量子通信路 $\mathcal{R}$ が存在して $\mathcal{R}\mathcal{E}(\rho) = \rho, \mathcal{R}\mathcal{E}(\sigma) = \sigma$

量子相対エントロピーの性質続き

(1) 正值性 (positivity)

$$D(\rho||\sigma) \geq 0 \quad (\text{等号成立} \Leftrightarrow \rho = \sigma)$$

(2) 結合凸性 (joint convexity)

任意の密度作用素 $\rho_1, \rho_2, \sigma_1, \sigma_2$ と $0 \leq p \leq 1$ に対して

$$\begin{aligned} D(p\rho_1 + (1-p)\rho_2 || p\sigma_1 + (1-p)\sigma_2) \\ \leq pD(\rho_1||\sigma_1) + (1-p)D(\rho_2||\sigma_2) \end{aligned}$$

(3) ユニタリ作用素 U に対して

$$D(U\rho U^* || U\sigma U^*) = D(\rho||\sigma)$$

(4) 加法性 (additivity)

$$D(\rho_A \otimes \rho_B || \sigma_A \otimes \sigma_B) = D(\rho_A || \sigma_A) + D(\rho_B || \sigma_B)$$

(5)

$$D(\rho||\sigma) < \infty \Leftrightarrow \text{ran } \rho \subseteq \text{ran } \sigma$$

ただし, ran は作用素の値域である.

量子相対エントロピー：測定に関する単調性

- 単調性の特別な場合として，測定に関する単調性が得られる．
- 密度作用素 ρ, σ と POVM $E = \{E_x\}$ に対して，測定値が従う確率分布

$$p_x = \text{Tr}[\rho E_x], \quad q_x = \text{Tr}[\sigma E_x]$$

- これらの古典的ダイバージェンス

$$D_E(\rho||\sigma) = \sum_x p_x (\log p_x - \log q_x)$$

- 測定に関する単調性

$$D(\rho||\sigma) \geq D_E(\rho||\sigma)$$

等号成立する POVM が存在するのは ρ と σ が可換であるときのみ．

量子相対エントロピーの計算例

- $\mathcal{H} = \mathbb{C}^2$, $\mathcal{S}(\mathcal{H})$ の Stokes パラメータ

$$\rho = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \quad (x^2 + y^2 + z^2 \leq 1)$$

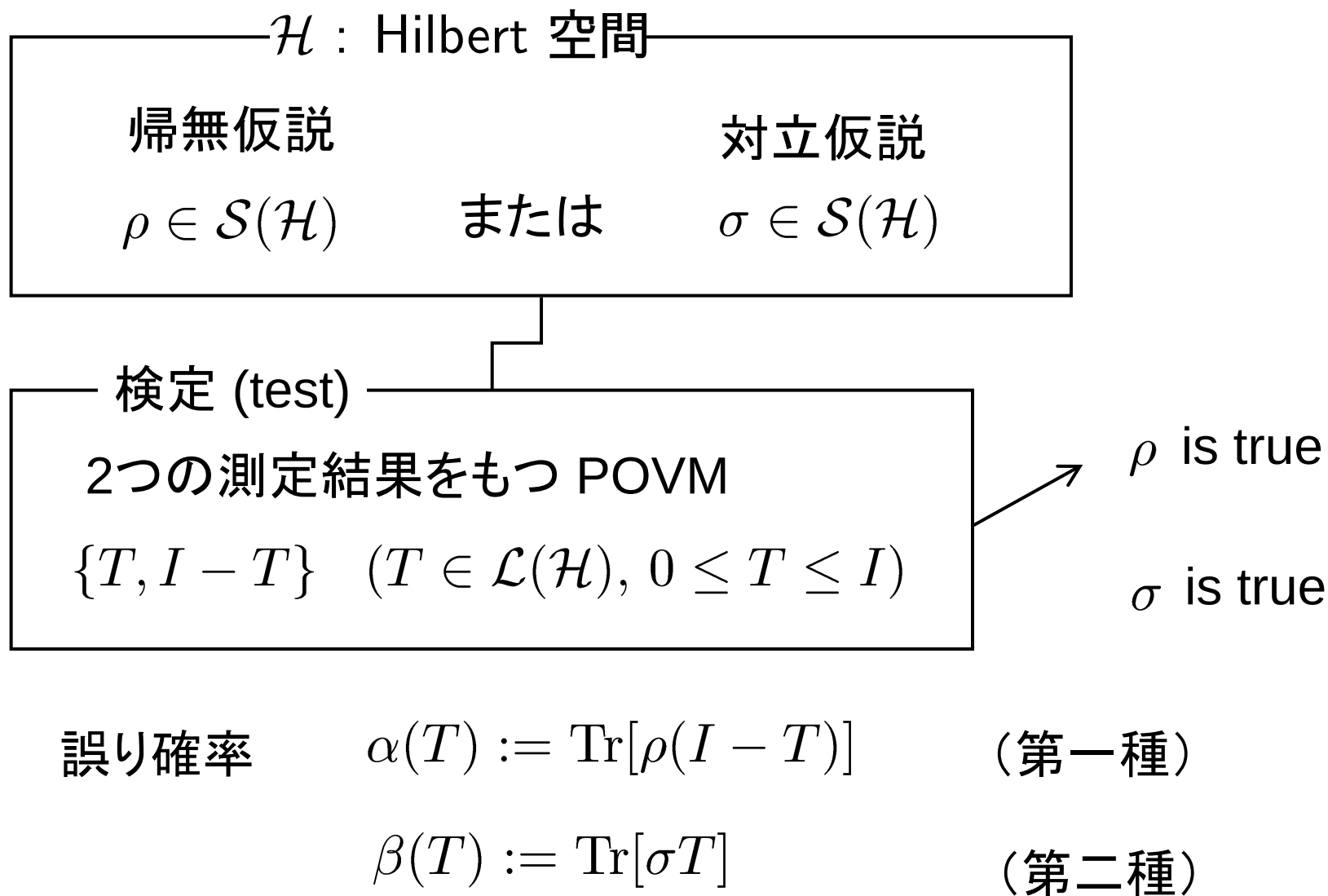
$$(\rho \geq 0 \Leftrightarrow \text{固有値がすべて } 0 \text{ 以上} \Leftrightarrow x^2 + y^2 + z^2 \leq 1)$$

- 計算例

$$\rho_x = \frac{1}{2} \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix}, \quad \sigma_z = \frac{1}{2} \begin{pmatrix} 1+z & 0 \\ 0 & 1-z \end{pmatrix}$$

$$\begin{aligned} D(\rho_x || \sigma_z) &= \text{Tr}[\rho_x (\log \rho_x - \log \sigma_z)] \\ &= -H(\rho_x) - \text{Tr} \rho_x \log \sigma_z \\ &= \frac{1+x}{2} \log \frac{1+x}{2} + \frac{1-x}{2} \log \frac{1-x}{2} - \frac{1}{2} \left(\log \frac{1+z}{2} + \log \frac{1-z}{2} \right) \end{aligned}$$

量子仮説検定問題



漸近論

例: i.i.d. 条件

$$\rho_n = \rho^{\otimes n}$$

$$\sigma_n = \sigma^{\otimes n}$$

$$\rho_n \text{ または } \sigma_n \in \mathcal{S}(\mathcal{H}^{\otimes n})$$

検定 (test)

$$\{T_n, I_n - T_n\}$$

$$(T_n \in \mathcal{L}(\mathcal{H}^{\otimes n}), 0 \leq T_n \leq I_n)$$

ρ_n is true

σ_n is true

誤り確率 $\alpha_n(T_n) := \text{Tr}[\rho_n(I_n - T_n)]$

$$\beta_n(T_n) := \text{Tr}[\sigma_n T_n]$$

誤り確率のトレードオフ

$$\alpha_n(T_n) \quad \longleftarrow \text{トレードオフ} \quad \longrightarrow \quad \beta_n(T_n)$$

定数制約問題

(Stein type)

$$\alpha_n(T_n) \leq \varepsilon, \quad \beta_n(T_n) \sim e^{-nB(\varepsilon)}$$

指数制約問題

(Hoeffding type)

$$\alpha_n(T_n) \leq e^{-nr}, \quad \beta_n(T_n) \sim e^{-nB(r)}$$

最大化
最適値は？

ベイズ誤り確率

(Chernoff type)

ρ_n : 確率 π , σ_n : 確率 $1 - \pi$

$$\pi \alpha_n(T_n) + (1 - \pi) \beta_n(T_n) \sim e^{-nB(\pi)}$$

量子 Stein の補題 (定数制約問題)

$$\beta_n^*(\varepsilon) := \min \{ \beta_n(T_n) \mid T_n : \text{test}, \alpha_n(T_n) \leq \varepsilon \}$$

量子相対エントロピー

$$D(\rho \parallel \sigma) = \text{Tr} [\rho(\log \rho - \log \sigma)]$$

定理 : 量子 Stein の補題 (i.i.d. 条件)

For $0 < \forall \varepsilon < 1$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n^*(\varepsilon) = -D(\rho \parallel \sigma)$$

$\leq$: 順定理, Hiai-Petz 1991 [5]

$\geq$: 逆定理, Ogawa-Nagaoka 2000 [6]

Holevo 相互情報量 (Holevo information, Holevo quantity)

Definition (Holevo 相互情報量)

量子通信路 $\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \rightarrow \mathcal{S}(\mathcal{H}_B)$ と $\mathcal{S}(\mathcal{H}_A)$ 上の確率測度 p に対して

$$I(p; \mathcal{E}) = E_p[D(\mathcal{E}(\rho) || \mathcal{E}(\sigma_p))] \quad \text{where} \quad \sigma_p = E_p[\rho]$$

ここで $E_p[\cdot]$ は密度作用素 ρ に関する平均

$$E_p[\cdot] = \int_{\mathcal{S}(\mathcal{H}_A)} \cdot \, p(d\rho)$$

- 確率測度 p が密度作用素の集合 $\{\rho_1, \rho_2, \dots\}$ にのみ正の確率を持つ離散的な確率分布 $p = \{p_1, p_2, \dots\}$ のとき,

$$I(p; \mathcal{E}) = \sum_i p_i D(\mathcal{E}(\rho_i) || \mathcal{E}(\sigma_p)) \quad \text{where} \quad \sigma_p = \sum_i p_i \rho_i$$

Holevo 相互情報量の性質

- 簡単な計算により $I(p; \mathcal{E}) = H(\mathcal{E}(\sigma_p)) - E_p[H(\mathcal{E}(\rho))]$

Theorem (単調性, monotonicity)

任意の量子通信路 $\mathcal{E}, \mathcal{F}$ に対して

$$I(p; \mathcal{I}) \geq I(p; \mathcal{E}) \geq I(p; \mathcal{F} \circ \mathcal{E})$$

Theorem (単調性等号成立条件)

状態族 $\mathcal{S} \subset \mathcal{S}(\mathcal{H})$ と量子通信路 $\mathcal{E}$ に対して以下は同値

- (1) 量子通信路 $\mathcal{R}$ が存在して $\forall \rho \in \mathcal{S}, \mathcal{R} \circ \mathcal{E}(\rho) = \rho$
- (2) $\mathcal{S}$ 上の忠実 (faithfull) な確率測度 p が存在して

$$I(p; \mathcal{I}) = I(p; \mathcal{E})$$

- (3) $\mathcal{S}$ 上の任意の確率測度 p に対して

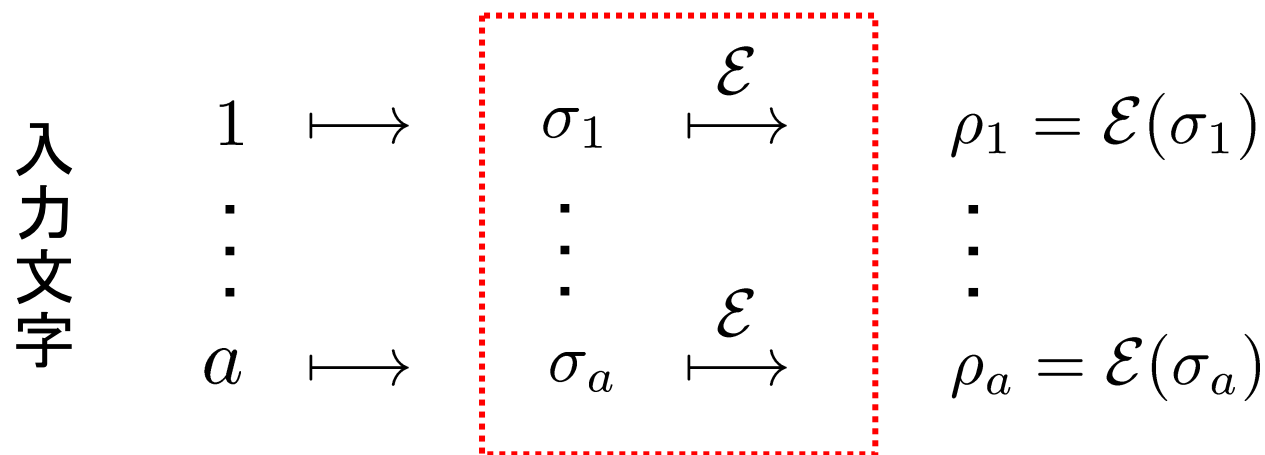
$$I(p; \mathcal{I}) = I(p; \mathcal{E})$$

量子通信路とメッセージ伝送

Shannon限界を超える

量子通信路 $\mathcal{E} : \mathcal{S}(\mathcal{K}) \longrightarrow \mathcal{S}(\mathcal{H})$

{
アファイン
トレース保存
完全正



$\Downarrow$ 省略

$$\begin{array}{ccc}
 \mathcal{X} = \{1, 2, \dots, a\} & \longrightarrow & \mathcal{E}(\mathcal{S}(\mathcal{K})) \subseteq \mathcal{S}(\mathcal{H}) \\
 \Downarrow & & \Downarrow \\
 x & \longmapsto & \rho_x
 \end{array}$$

n 次拡大量子通信路によるメッセージ伝送

$k \in \{1, \dots, M_n\}$ **メッセージ** **符号化**

$$\Downarrow \quad \boxed{\{1, \dots, M_n\} \longrightarrow \mathcal{C}^{(n)} = \{x^n(1), \dots, x^n(M_n)\} \subseteq \mathcal{X}^n}$$

$$\begin{array}{ccccccc} x^n(k) & = & (x_1(k) & , & x_2(k) & , & \dots & , & x_n(k)) \in \mathcal{C}^{(n)} \\ \Downarrow & & \downarrow & & \downarrow & & & & \downarrow \\ \rho_{x^n(k)} & = & \rho_{x_1(k)} & \otimes & \rho_{x_2(k)} & \otimes & \dots & \otimes & \rho_{x_n(k)} \in \mathcal{S}(\mathcal{H}^{\otimes n}) \end{array}$$

$$\Downarrow \quad \boxed{X^{(n)} = \{X_1, \dots, X_{M_n}\} \text{ POVM on } \mathcal{H}^{\otimes n}}$$

復号 = 測定

$l \in \{1, \dots, M_n\}$ $\text{Tr}[\rho_{x^n(k)} X_l]$ の確率で復号

通信路容量の操作的定義

符号 $(\mathcal{C}^{(n)}, X^{(n)})$

平均誤り確率 $\text{Pe}(\mathcal{C}^{(n)}, X^{(n)}) \stackrel{\text{def}}{=} \frac{1}{M_n} \sum_{k=1}^{M_n} (1 - \text{Tr}[\rho_{x^n(k)} X_k])$

目的 $\left\{ \begin{array}{l} \text{Pe}(\mathcal{C}^{(n)}, X^{(n)}) \longrightarrow 0 \quad (n \longrightarrow \infty) \\ R_n = \log M_n / n \text{ (通信速度)} \longrightarrow \text{大きく} \end{array} \right.$

定義：通信路容量

$$C(\mathcal{E}) \stackrel{\text{def}}{=} \sup \left\{ R \mid \lim_{n \rightarrow \infty} \text{Pe}(\mathcal{C}^{(n)}, X^{(n)}) = 0, \right.$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log M_n \geq R$$

となる符号の系列 $\{(\mathcal{C}^{(n)}, X^{(n)})\}_{n=1}^{\infty}$ が存在 $\}$

量子通信路符号化定理

— Holevo (1996), Schumacher-Westmoreland (1997) —

$$C(\mathcal{E}) = \max_p I(p; \mathcal{E})$$

○ Holevo相互情報量

$$I(p; \mathcal{E}) \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} p(x) D(\rho_x || \sigma_p), \quad \sigma_p = \sum_{x \in \mathcal{X}} p(x) \rho_x$$

○ 量子相対エントロピー

$$D(\rho || \sigma) \stackrel{\text{def}}{=} \text{Tr}[\rho(\log \rho - \log \sigma)]$$