量子誤り訂正符号と量子秘密分散

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** 11 **月** 6 **日**
第 13 **回情報論的学習理論ワークショップ** (IBIS 2010)

目次

タイプミス修正＋補足をしました

(1) 量子力学系の枠組み

量子力学系の公理について

量子力学系の特徴

- **確率法則**
  測定結果は**系の状態**と**測定**に依存して確率的にのみ定まる
- **系の状態変化**
  測定結果に依存して状態が変化 → 測定順序によって結果が異なる

⇓ スカラーでは記述しきれない

Hilbert 空間上の作用素 (行列) により記述される

- Hilbert 空間：内積を持つ (複素) ベクトル空間
- 有限次元の場合：$\mathcal{H} \simeq \mathbb{C}^d$
- 内積 $\langle \varphi \,|\, \psi \rangle \quad (\varphi, \psi \in \mathcal{H})$ を持つ

Dirac のブラケット記法　（$\mathcal{H} = \mathbb{C}^d$ 数ベクトル空間，標準内積）

- **角括弧 $\langle \quad \rangle$ は英語で** bracket**．慣れると便利な記法．**
- **$\mathcal{H}$ の元をケットで表す (縦ベクトル) →ブラ (共役転置：横ベクトル)**

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} \quad \xrightarrow{\text{双対ベクトル空間}} \quad \langle\psi| = \begin{pmatrix} \psi_1^* & \cdots & \psi_d^* \end{pmatrix}$$

- **内積：**

$$\langle\varphi\,|\,\psi\rangle = \begin{pmatrix} \varphi_1^* & \cdots & \varphi_d^* \end{pmatrix} \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} = \sum_{i=1}^{d} \varphi_i^* \psi_i$$

- **ケット×ブラは行列：**

$$|\psi\rangle\langle\varphi| = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} \begin{pmatrix} \varphi_1^* & \cdots & \varphi_d^* \end{pmatrix} = \begin{pmatrix} \psi_1\varphi_1^* & \cdots & \psi_1\varphi_d^* \\ \vdots & & \vdots \\ \psi_d\varphi_1^* & \cdots & \psi_d\varphi_d^* \end{pmatrix}$$

量子状態と測定

- **量子状態＝長さ (ノルム) が 1 のベクトルで表現 (ベクトル状態)**

$$\textbf{量子状態：}|\psi\rangle \in \mathcal{H} \quad (\textbf{規格化条件：}\|\psi\| = \sqrt{\langle\psi\,|\,\psi\rangle} = 1)$$

- m **個の測定結果を持つ測定の表現** (m-valued measurement)

$$\textbf{測定：}E = \{E_1, \ldots, E_m\}$$

$E_i\,(i = 1, \ldots, m)$ **は** $\mathcal{H}$ **上の正方行列で以下を満たすもの**

$$E_i^* = E_i, \quad E_i E_j = \delta_{i,j} E_i, \quad \sum_{i=1}^{m} E_i = I$$

- **互いに直交する部分空間への射影子の集合，単位の分解**
- **射影測定** (Projection Valued Measure, PVM) **という**
- **後で一般化測定を導入**

測定と状態の重ね合わせ

- **測定 $\Rightarrow$ 直交する単位ベクトルの “量子力学的重ね合わせ” を指定**

$$|\psi\rangle = \sum_{i=1}^{m} E_i |\psi\rangle = \sum_{i=1}^{m} \alpha_i |e_i\rangle$$

ただし

- $$|e_i\rangle := \frac{E_i |\psi\rangle}{\| E_i |\psi\rangle \|} = \frac{E_i |\psi\rangle}{\sqrt{\langle\psi| E_i |\psi\rangle}}$$ **(互いに直交，ノルム 1)**

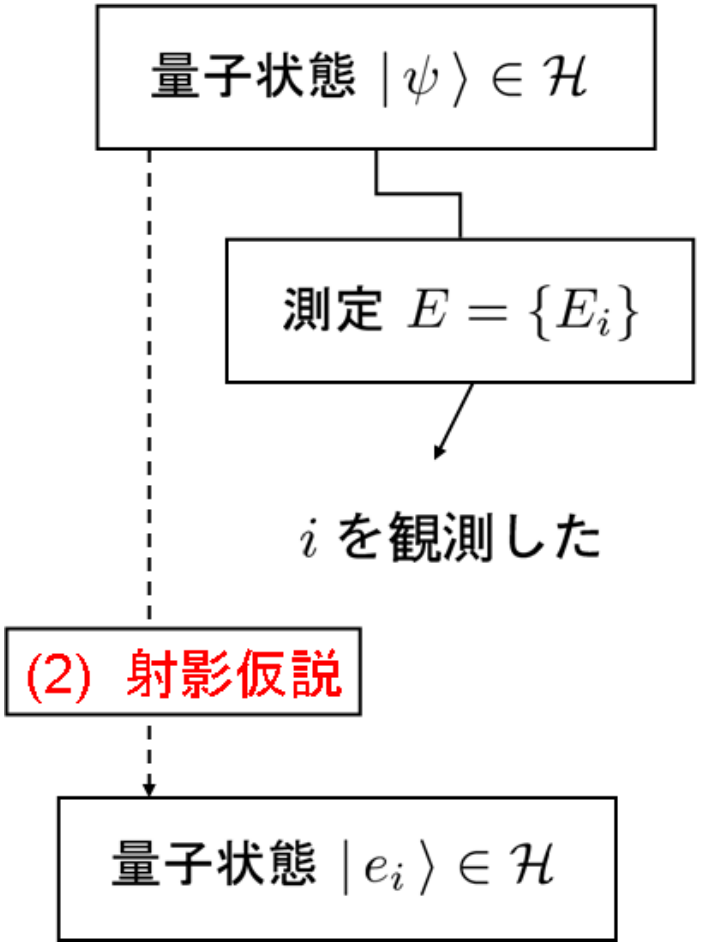
$$\because \quad \| E_i |\psi\rangle \|^2 = \langle\psi| E_i^* E_i |\psi\rangle = \langle\psi| E_i |\psi\rangle$$

- $$\alpha_i := \langle e_i | \psi\rangle = \frac{\langle\psi| E_i |\psi\rangle}{\sqrt{\langle\psi| E_i |\psi\rangle}} = \sqrt{\langle\psi| E_i |\psi\rangle}$$ **(振幅)**

- **振幅の二乗 $|\alpha_i|^2$ は確率分布**

$$|\alpha_i|^2 = \langle\psi| E_i |\psi\rangle, \quad \sum_{i=1}^{m} |\alpha_i|^2 = \langle\psi| \sum_{i=1}^{m} E_i |\psi\rangle = 1$$

量子力学の公理



$$|\psi\rangle = \sum_{i=1}^{m} E_i|\psi\rangle = \sum_{i=1}^{m} \alpha_i|e_i\rangle$$

(1) 確率法則

測定値 i を観測する確率

$$|\alpha_i|^2 = \langle\psi|E_i|\psi\rangle$$

(3) 孤立系の量子状態の変化はユニタリ変換 $|\psi\rangle \to U|\psi\rangle$ で与えられる

密度行列 (密度作用素, density operator)

- **密度行列：古典的確率も含んだ量子状態を記述**
- **記法：** $\mathcal{L}(\mathcal{H}) := \{X \mid X : \mathcal{H} \to \mathcal{H}$ **(線形作用素)** $\}$
- $\mathcal{H} = \mathbb{C}^n$ **のとき，** $\mathcal{L}(\mathcal{H})$ **は** $n \times n$ **正方行列全体とみなせる**
- $\rho \in \mathcal{L}(\mathcal{H})$ **で以下を満たすものを密度行列という**

$$\rho = \rho^*, \quad \rho \geq 0, \quad \operatorname{Tr} \rho = 1 \quad \text{(エルミート，半正定値，トレース 1)}$$

- **純粋状態 (=ベクトル状態)**

$$\operatorname{rank} \rho = 1 \Longleftrightarrow \rho = |\psi\rangle\langle\psi| \text{ の形に書ける}$$

- **記法：** $\mathcal{S}(\mathcal{H})$ **を密度行列全体とする**

密度行列の記述例

- 確率 q_j で量子状態 $|\psi_j\rangle$ の粒子が発生する装置を考える
- 粒子に対して測定 $E = \{E_i\}$ を行う

$$\boxed{\{q_j, |\psi_j\rangle\}} \Rightarrow \quad \longrightarrow \quad |\psi_j\rangle \curvearrowright \boxed{\text{測定 } E = \{E_i\}} \rightarrow \text{測定値 } i$$

- 状態 $|\psi_j\rangle$ の場合，測定値 i を得る確率は

$$p(i|j) = \langle\psi_j| E_i |\psi_j\rangle = \mathrm{Tr}\, |\psi_j\rangle\langle\psi_j| E_i$$

- よって測定値 i を得る確率は

$$p(i) = \sum_j q_j p(i|j) = \mathrm{Tr} \left(\sum_j q_j |\psi_j\rangle\langle\psi_j| \right) E_i = \mathrm{Tr}\, \rho E_i$$

ただし，$\rho := \sum_j q_j |\psi_j\rangle\langle\psi_j|$ とおいた (“古典確率的重ね合わせ”)

- 密度行列 ρ はあらゆる測定について，系の確率を規定している

密度行列とベクトル状態についての注意

- **一般に異なるアンサンブル $\{p_j, |\varphi_j\rangle\}$, $\{q_j, |\psi_j\rangle\}$ が同じ密度行列 ρ を与えることがある**

$$\rho = \sum_j p_j \, |\varphi_j\rangle\langle\varphi_j| = \sum_j q_j \, |\psi_j\rangle\langle\psi_j|$$

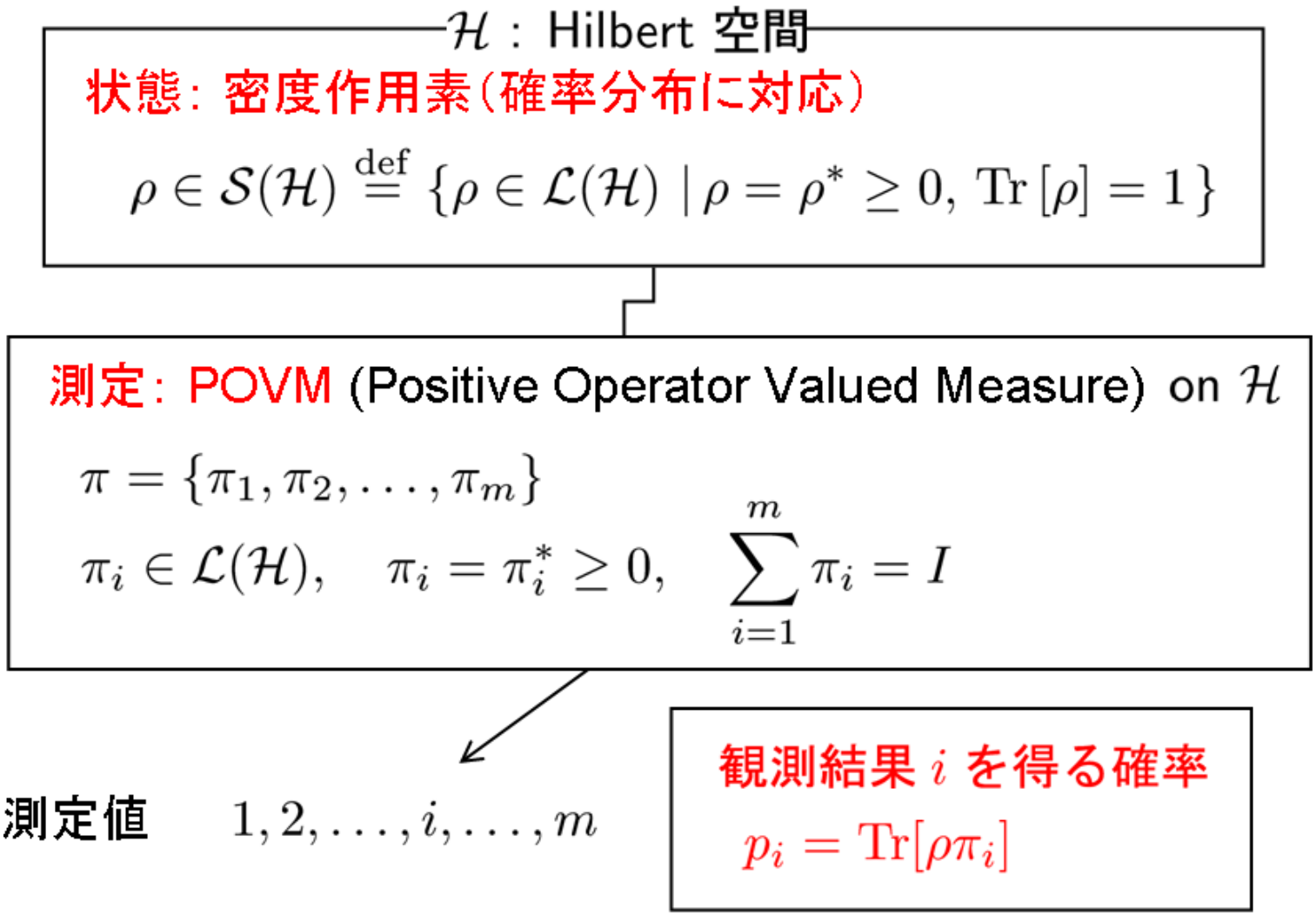
- **例：$\mathcal{H} = \mathbb{C}^2$, 以下の二つは同じ密度行列 $\rho = \frac{1}{2} I$ を与える**

$$(p_1, p_2) = (1/2, 1/2), \quad |\varphi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |\varphi_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$(q_1, q_2) = (1/2, 1/2), \quad |\psi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |\psi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

- **この粒子の測定だけから，どちらのアンサンブルかを区別することはできない→アンサンブル $\{p_j, |\varphi_j\rangle\}$ と書く物理的根拠はない**
- **一方，密度行列は粒子の測定結果についての確率を一意に指定する**

密度行列を用いた量子力学系の公理



- **一般化測定** (POVM)**：補助系を利用することで射影測定** (PVM) **から構成できる** (Naimark **拡張**)

合成系の状態と測定 (後でまた出します)

n 個の系 $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ の合成系

$\bigotimes_{k=1}^{n} \mathcal{H}_k$: テンソル積空間

状態: $\rho_n \in \mathcal{S}\left(\bigotimes_{k=1}^{n} \mathcal{H}_k\right)$

測定: POVM on $\bigotimes_{k=1}^{n} \mathcal{H}_k$

$\pi = \{\pi_1, \pi_2, \ldots, \pi_m\}$

$\pi_i \in \mathcal{L}(\bigotimes_{k=1}^{n} \mathcal{H}_k), \quad \pi_i = \pi_i^* \geq 0, \quad \sum_{i=1}^{m} \pi_i = I$

合成系：ベクトルのテンソル積

- **物理系 $\mathcal{H}_A, \mathcal{H}_B$ の合成系は**テンソル積空間 $\mathcal{H}_A \otimes \mathcal{H}_B$ **で表される**
- **ベクトルのテンソル積演算 (= クロネッカー積)**

$$|\psi_A\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}, \quad |\psi_B\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ に対して}$$

$$|\psi_A\rangle \otimes |\psi_B\rangle := \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ \vdots \\ a_m \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{pmatrix} \quad (m \times n \text{ 次元ベクトル})$$

合成系：テンソル積空間

- **テンソル積演算の性質：双線形性**

$$(\alpha |\psi_A\rangle + \beta |\varphi_A\rangle) \otimes |\psi_B\rangle = \alpha |\psi_A\rangle \otimes |\psi_B\rangle + \beta |\varphi_A\rangle \otimes |\psi_B\rangle$$
$$|\psi_A\rangle \otimes (\alpha |\psi_B\rangle + \beta |\varphi_B\rangle) = \alpha |\psi_A\rangle \otimes |\psi_B\rangle + \beta |\psi_A\rangle \otimes |\varphi_B\rangle$$

- **内積**

$$\langle \psi_A \otimes \psi_B | \varphi_A \otimes \varphi_B \rangle = \langle \psi_A | \varphi_A \rangle \langle \psi_B | \varphi_B \rangle$$

- **テンソル積空間の定義：基底のテンソル積で張られるベクトル空間**

$$\mathcal{H}_A \otimes \mathcal{H}_B := \left\{ \sum_{i,j} c_{ij} |e_i\rangle \otimes |f_j\rangle \;\middle|\; c_{ij} \in \mathbb{C},\ |e_i\rangle : \mathcal{H}_A\text{の基底},\ |f_j\rangle : \mathcal{H}_B\text{の基底} \right\}$$

行列 (作用素) のテンソル積

- $X \in \mathcal{L}(\mathcal{H}_A)$, $Y \in \mathcal{L}(\mathcal{H}_B)$ **に対して**

$$(X \otimes Y)(|\psi_A\rangle \otimes |\psi_B\rangle) = (X|\psi_A\rangle) \otimes (Y|\psi_B\rangle)$$

を線形に拡大して $X \otimes Y \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ **を定義**
(基底 $|e_i\rangle \otimes |f_j\rangle$ **の行き先を定めたので行列が定義された)**

- **成分では：行列のテンソル積 = クロネッカー積**

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mm} \end{pmatrix}, \quad Y = \begin{pmatrix} y_{11} & \cdots & y_{1n} \\ \vdots & & \vdots \\ y_{n1} & \cdots & y_{nn} \end{pmatrix}$$

$$X \otimes Y = \begin{pmatrix} x_{11}Y & \cdots & x_{1m}Y \\ \vdots & & \vdots \\ x_{m1}Y & \cdots & x_{mm}Y \end{pmatrix}$$

合成系の状態と測定 (再掲)

n 個の系 $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ の合成系

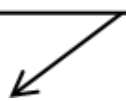
$\bigotimes_{k=1}^{n} \mathcal{H}_k$: テンソル積空間

状態: $\rho_n \in \mathcal{S}\left(\bigotimes_{k=1}^{n} \mathcal{H}_k\right)$

測定: POVM on $\bigotimes_{k=1}^{n} \mathcal{H}_k$

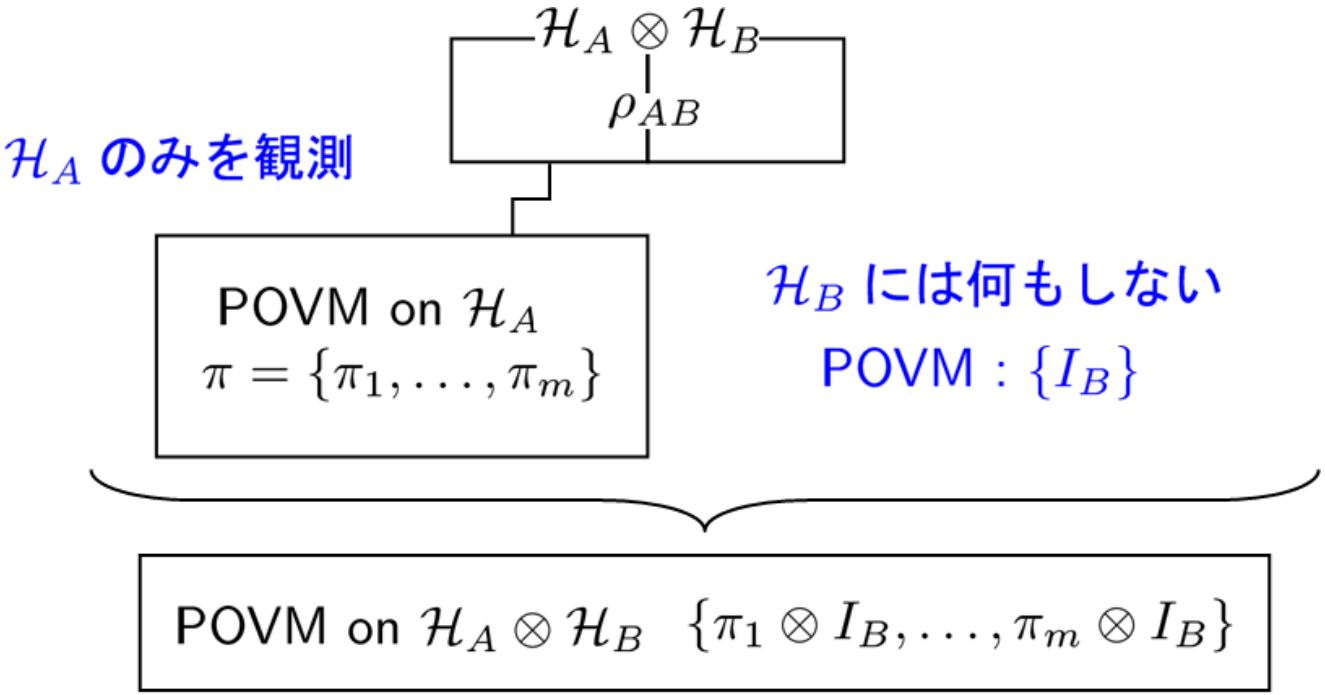
$\pi = \{\pi_1, \pi_2, \ldots, \pi_m\}$

$\pi_i \in \mathcal{L}(\bigotimes_{k=1}^{n} \mathcal{H}_k), \quad \pi_i = \pi_i^* \geq 0, \quad \sum_{i=1}^{m} \pi_i = I$



部分トレース (partial trace)：周辺分布を求める操作に対応

- **合成系上の密度行列 $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ に対して**



測定値の従う確率 $\mathrm{Tr}[\rho_{AB}(\pi_i \otimes I_B)] = \mathrm{Tr}[\rho_A \pi_i]$

系 $\mathcal{H}_A$ のみの観測結果を記述 $\Longleftarrow$ $\rho_A := \mathrm{Tr}_B[\rho_{AB}]$ 部分トレース

- $\mathrm{Tr}[\rho_{AB}(X_A \otimes I_B)] = \mathrm{Tr}[\rho_A X_A]\ (\forall X_A \in \mathcal{L}(\mathcal{H}_A))$ **を満たす** $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ **が一意に存在 (部分トレース)**

部分トレースの計算方法 (追加しました)

- **部分トレースの定義 (再掲)**

$$\exists! \rho_A \in \mathcal{S}(\mathcal{H}_A),\ \forall X_A \in \mathcal{L}(\mathcal{H}_A),\ \mathrm{Tr}[\rho_{AB}(X_A \otimes I_B)] = \mathrm{Tr}[\rho_A X_A]$$

- **計算方法：$I_B = \sum_i |e_i\rangle\langle e_i|$ を用いると**

$$\begin{aligned}
\mathrm{Tr}\,\rho_{AB}(X_A \otimes I_B) &= \sum_i \mathrm{Tr}\,\rho_{AB}(X_A \otimes |e_i\rangle\langle e_i|) \\
&= \sum_i \mathrm{Tr}\,\rho_{AB}(I_A \otimes |e_i\rangle)(X_A \otimes 1)(I_A \otimes \langle e_i|) \\
&= \sum_i \mathrm{Tr}(I_A \otimes \langle e_i|)\rho_{AB}(I_A \otimes |e_i\rangle)(X_A \otimes 1) \\
&= \mathrm{Tr}\left\{\sum_i (I_A \otimes \langle e_i|)\rho_{AB}(I_A \otimes |e_i\rangle)\right\} X_A \\
&\quad [\because\ X_A \otimes 1 = X_A]
\end{aligned}$$

すなわち $\rho_A = \mathrm{Tr}_B\,\rho_{AB} = \sum_i (I_A \otimes \langle e_i|)\rho_{AB}(I_A \otimes |e_i\rangle)$

(2) 量子通信路

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 (1) **線形写像**

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

で，次の条件を満たすものとして定義される．

(2) **完全正値性** (complete positivity)
任意の系 $\mathcal{H}_R$ と任意の $X_{RA} \in \mathcal{L}(\mathcal{H}_R \otimes \mathcal{H}_A)$ について

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

ただし，$\mathcal{I}_R$ は恒等写像である．

(3) **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 $\mathrm{Tr}[\mathcal{E}(X)] = \mathrm{Tr}[X]$

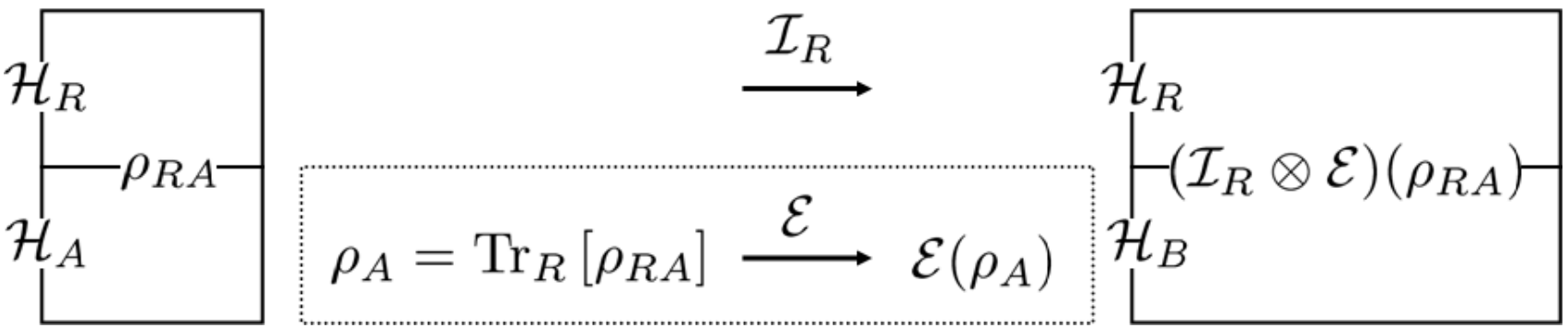
量子通信路の完全正値性について

- **再掲**

$$\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \longrightarrow \mathcal{S}(\mathcal{H}_B) \quad \text{が量子通信路}$$

$$\overset{\text{def}}{\Longleftrightarrow} \begin{cases} (1)\ \text{線形性}：\mathcal{E}(t\rho + (1-t)\sigma) = t\mathcal{E}(\rho) + (1-t)\mathcal{E}(\sigma) \\ (2)\ \text{完全正}：(\mathcal{I}_R \otimes \mathcal{E})(\rho_{RA}) \geq 0 \\ (3)\ \text{トレース保存}：\mathrm{Tr}\,[\mathcal{E}(\rho)] = \mathrm{Tr}\,[\rho] = 1 \end{cases}$$

(2) の意味：一部の系を操作しても，密度行列の条件を満足



- **最低限** (1), (2), (3) **が成立していないと “どうしようもない” 要請**

量子通信路の表現

Theorem (量子通信路の表現)

写像 $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ 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 $E_i : \mathcal{H}_A \to \mathcal{H}_B$ 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) **$V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ が存在して**

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

シュタインスプリング表現と物理的実現

- $V : \mathcal{K} \to \mathcal{H}$ **が等距離作用素** (isometory) $\overset{\text{def}}{\iff} V^*V = I_{\mathcal{K}}$
- $\mathcal{K}$ **の** $\mathcal{H}$ **への "埋め込み方法"**
- **このとき，** VV^* **は** $\mathcal{H}$ **の部分空間** $\operatorname{Im} V$ **への射影子**
- **全写であればユニタリ作用素**

- **シュタインスプリング表現**
  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) $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ **が存在して**

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

- V **は** $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ **上の**U **に拡張できて，**
  環境系の初期状態 $\rho_{0,E} \in \mathcal{S}(\mathcal{H}_E)$**，出力系の初期状態** $\rho_{0,B} \in \mathcal{S}(\mathcal{H}_B)$
  (どちらも純粋状態) を用いて，以下のように表される

$$\mathcal{E}(\rho) = \operatorname{Tr}_{AE}[U(\rho \otimes \rho_{0,E} \otimes \rho_{0,B})U^*]$$

- **量子通信路は量子力学の許す範囲で物理的実現が可能**

Stinespring 表現と Kraus 表現の関係 (追加しました)

- isometry $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ は次式で書ける．
  - $\sum_k E_k^* E_k = I_A$ を満たす作用素の組 $E_k : \mathcal{H}_A \to \mathcal{H}_B$
  - $\mathcal{H}_E$ の正規直交基底 $\{|f_k\rangle\}_k$

$$V : |\psi\rangle \in \mathcal{H}_A \mapsto \sum_k |\psi_k\rangle \otimes |f_k\rangle = \sum_k E_k |\psi\rangle \otimes |f_k\rangle \in \mathcal{H}_B \otimes \mathcal{H}_E$$

- すなわち，$V = \sum_k E_k \otimes |f_k\rangle$ だから

$$V\rho V^* = \sum_{k,l} E_k \rho E_l^* \otimes |f_k\rangle\langle f_l|$$

- この部分トレースをとることで Kraus 表現が得られる

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

- どちらも Stinespring-Kraus 表現と呼ばれることがある

量子通信路の例：二準位系 $\mathbb{C}^2$ 上のユニタリ変換

- **標準基底：** $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Pauli **行列**

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

- X, Y, Z **はエルミートかつユニタリ**
- $X^2 = I, \ Y^2 = I, \ Z^2 = I$
- Pauli **行列の交換関係**

$$XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -ZX = -iY \quad (Y = iXZ)$$

- bit flip：$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$
- phaze flip：$Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle$

量子通信路の例：Pauli 通信路

- Pauli **通信路**

  $$\mathcal{E} : \rho \in \mathcal{S}(\mathbb{C}^2) \mapsto \mathcal{E}(\rho) = p_0\rho + p_1 X\rho X^* + p_2 Y\rho Y^* + p_3 Z\rho Z^* \in \mathcal{S}(\mathbb{C}^2)$$

  (p_0, p_1, p_2, p_3) **は確率ベクトル**
- I (**エラーなし**), X (bit flip), Y, Z (phaze flip) **の確率的な凸結合**
- $Y\rho Y^* = XZ\rho Z^* X^*$ **に注意**
- Y **に対応するエラー** $=$ phaze flip $+$ bit flip
- $XZ = -ZX$ **なので上記の順番は関係ない**

(3) 量子誤り訂正

量子誤り訂正符号の例

- $\mathbb{C}^2$ 上の任意の量子状態：$\psi = \alpha|0\rangle + \beta|1\rangle$ $(\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1)$
- $|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle \in (\mathbb{C}^2)^{\otimes 3}$ に符号化
- この符号化は次の等距離作用素 $V : \mathbb{C}^2 \to (\mathbb{C}^2)^{\otimes 3}$ を考えている

$$V : \mathbb{C}^2 \overset{\text{isometry}}{\longrightarrow} \mathcal{C} := \mathrm{span}\{|000\rangle, |111\rangle\} \subset (\mathbb{C}^2)^{\otimes 3}$$

  $(\mathbb{C}^2)^{\otimes 3}$ の部分空間 $\mathcal{C}$ を符号という
- エラー：二番目に bit flip が起きたとする

$$|\Psi\rangle = \alpha|010\rangle + \beta|101\rangle \in (\mathbb{C}^2)^{\otimes 3}$$

- 復号：以下の測定 $P = \{P_0, P_1, P_2, P_3\}$ を行う

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad (\mathrm{span}\{|000\rangle, |111\rangle\} \text{ への射影子})$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad (\mathrm{span}\{|100\rangle, |011\rangle\} \text{ への射影子})$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad (\mathrm{span}\{|010\rangle, |101\rangle\} \text{ への射影子})$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad (\mathrm{span}\{|001\rangle, |110\rangle\} \text{ への射影子})$$

- 測定値 2 が得られるので，2 番目を bit flip することで訂正可能

量子誤り訂正符号の枠組み (追加しました)

- 量子通信路 $\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ が与えられたとき，$\mathcal{H}_A$ の線形部分空間 $\mathcal{C}$ (符号とよぶ) に限って純粋状態を訂正可能なようにする

$$\mathcal{H} \overset{V:\text{符号化}}{\longrightarrow} \mathcal{C} \subset \mathcal{H}_A \overset{\mathcal{E}:\text{エラー}}{\longrightarrow} \mathcal{H}_B \overset{\mathcal{R}:\text{復号}}{\longrightarrow} \mathcal{H}$$

- 正確には，$\mathcal{S}(\mathcal{H}) \overset{\text{符号化}}{\longrightarrow} \mathcal{S}(\mathcal{C}) \subset \mathcal{S}(\mathcal{H}_A) \overset{\mathcal{E}:\text{エラー}}{\longrightarrow} \mathcal{S}(\mathcal{H}_B) \overset{\mathcal{R}:\text{復号}}{\longrightarrow} \mathcal{S}(\mathcal{H})$
- 符号化は等距離作用素 $V : \mathcal{H} \to \mathcal{C} \subset \mathcal{H}_A$ により以下で行う

$$\rho = |\psi\rangle\langle\psi| \in \mathcal{S}(\mathcal{H}) \overset{\text{符号化}}{\longmapsto} V|\psi\rangle\langle\psi|V^* \in \mathcal{S}(\mathcal{C}) \subset \mathcal{S}(\mathcal{H}_A)$$

- 等距離作用素 = “埋め込み” ($\mathcal{H}$ と $\mathcal{C}$ を同一視)
- 復号操作 $\mathcal{R}$ も量子通信路 (量子操作)

Remark

- $\mathcal{S}(\mathcal{H})$ は凸集合で端点は純粋状態全体である
- $\mathcal{H}$ の純粋状態がすべて復号可能 $\Longleftrightarrow \mathcal{S}(\mathcal{H})$ の元すべてが復号可能

量子誤り訂正可能な必要十分条件 (追加しました)

Knill-Laflamme の定理

- 以下では $\mathcal{H}$ と $\mathcal{C}$ を同一視する

Kraus 表現 $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^*$ で与えられる **量子通信路**
$\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ と $\mathcal{H}_A$ の **部分空間** $\mathcal{C} \subset \mathcal{H}_A$ について以下は同値

(1) (復号可能) 逆向きの量子操作 $\mathcal{R} : \mathcal{S}(\mathcal{H}_B) \to \mathcal{S}(\mathcal{H}_A)$ が存在して

$$\forall \rho \in \mathcal{S}(\mathcal{C}),\ \mathcal{R} \circ \mathcal{E}(\rho) = \rho \quad (\text{部分空間 } \mathcal{C} \text{ 上の量子状態は元にもどる})$$

(2) エルミート行列 $\alpha = [\alpha_k]$ が存在して

$$P E_l^* E_k P = \alpha_{lk} P \quad (P \text{ は } \mathcal{C} \text{ への射影子})$$

Knill-Laflamme の定理 (2) の意味 (追加しました)

- Stinespring 表現 $\mathcal{E}(\rho) = \mathrm{Tr}_E\, V\rho V^*$ より

$$\mathcal{F}(\rho) := \mathrm{Tr}_B\, V\rho V^*, \quad \mathcal{F} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_E)$$

  を定義する (**補通信路**, complementary channel)
- Stinespring 表現と Kraus 表現の関係により

$$V\rho V^* = \sum_{k,l} E_k \rho E_l^* \otimes |e_k\rangle\langle e_l|$$

$$\therefore \quad \mathcal{F}(\rho) = \mathrm{Tr}_B\, V\rho V^* = \sum_{k,l} \mathrm{Tr}[\rho E_l^* E_k] \cdot |e_k\rangle\langle e_l|$$

- $\rho \in \mathcal{S}(\mathcal{C}) \Leftrightarrow \rho = P\rho P$ (P は $\mathcal{C}$ への射影子, $\mathcal{C}$ では単位行列) なので

$$\mathcal{F}(\rho) = \sum_{k,l} \mathrm{Tr}[\rho E_l^* E_k] \cdot |e_k\rangle\langle e_l| = \sum_{k,l} \mathrm{Tr}[P\rho P E_l^* E_k] \cdot |e_k\rangle\langle e_l|$$

$$= \sum_{k,l} \mathrm{Tr}[\rho P E_l^* E_k P] \cdot |e_k\rangle\langle e_l| = \sum_{k,l} \alpha_{lk} \cdot |e_k\rangle\langle e_l|$$

- (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ "$\mathcal{F}(\rho)$ が $\rho \in \mathcal{S}(\mathcal{C})$ によらない" (環境系で invisible)

誤り訂正の離散化について (追加しました)

Theorem

Kraus 表現 $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^*$ で与えられる量子通信路
$\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ が部分空間 $\mathcal{C}$ について復号可能であるとき，
$E'_m = \sum_k c_{km} E_k$ を満たす $\{E'_m\}$ によって与えられる Kuraus 表現

$$\mathcal{E}'(\rho) = \sum_{m,n} E'_m \rho E'^*_n$$

を持つ量子通信路も復号可能

$$\because \quad P E'^*_n E'_m P = \sum_{k,l} c^*_{ln} c_{km} P E^*_l E_k P = \sum_{k,l} c^*_{ln} c_{km} \alpha_{lk} P = \alpha'_{nm} P$$

- 実は $\mathcal{E}$ と同じ復号方法で $\mathcal{E}'$ が復号できる
- 有限次元系でも量子通信路は連続的に無数存在
- 復号操作を有限個に限ることができる

(4) CSS (Calderbank-Shor-Steane) **符号**

古典的な線形符号：$GF(2)^n = \mathbb{Z}_2^n$ における線形符号

- 符号 C とは $\mathbb{Z}_2^n$ の線形部分空間：$C \subset \mathbb{Z}_2^n$
- C の基底を並べることで**生成行列** G $(n \times k)$ が作られる：

$$C = \left\{ Gu \,\middle|\, u \in \mathbb{Z}_2^k \right\}$$

- $[n, k]$ 線形符号：k ビットの情報ビットを n ビットの符号に変換
- C の**パリティ検査行列** H $((n-k) \times n)$

$$C = \ker H = \{ x \in \mathbb{Z}_2^n \mid Hx = 0 \}$$

- 符号語間の最小距離と誤り訂正能力

$$d = \min_{x,y \in C} \mathsf{weight}(x - y)$$

  $2d + 1 \geq t$ ならば t ビットの誤りを訂正可能
- 双対符号 (dual code)

$$C^{\perp} := \{ x \in \mathbb{Z}_2^n \mid \forall y \in C,\, x \cdot y = 0 \}$$

CSS (Calderbank-Shor-Steane) 符号の構成

- **元になる古典的な $GF(2)^n = \mathbb{Z}_2^n$ 上の線形符号**
  - $C_1 : [n, k_1]$ **線形符号，** $C_2 : [n, k_2]$ **線形符号**
  - $C_2 \subset C_1$ **(加法について部分群)，** C_1 **と** $C_2^{\perp}$ **は** t**-誤り訂正符号**
- **加法の部分群 $C_2 \subset C_1$ による同値類**
  - $x, y \in C_1$ **について** $x \sim y \overset{\text{def}}{\iff} x - y \in C_2$
  - **同値類による類別**

$$C_1 = \bigcup_{x\text{: 同値類の代表元}} x + C_2$$

  - **同値類の数：** $\frac{|C_1|}{|C_2|} = 2^{k_1 - k_2}$
- CSS **符号：** $[n, k_1 - k_2]$ **量子符号，** t**-誤り訂正符号**

$$|x + C_2\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \in (\mathbb{C}^2)^{\otimes n}$$

代表元の取り方に依存しない

CSS 符号の性質

- **CSS 符号は代表元の取り方に依存しない：$x' \sim x$ $(x' - x \in C_2)$ のとき**

$$|x' + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x' + y\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + (x' - x) + y\rangle$$

$$= \frac{1}{\sqrt{|C_2|}} \sum_{y' \in C_2} |x + y'\rangle = |x + C_2\rangle$$

[$\because \quad y' = (x' - x) + y$ **とおくと，** y' **は** C_2 **のすべての元をわたるので**]

- **異なる同値類については直交する：$x' \nsim x$ $(x' - x \notin C_2)$ のとき**

$$x + C_2 \cap x' + C_2 = \emptyset$$

だから，任意の $y, y' \in C_2$ **について** $|x + y\rangle$ **と** $|x' + y'\rangle$ **は直交**
よって，以下の二つのベクトルは直交

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle, \quad |x' + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y' \in C_2} |x' + y'\rangle$$

CSS 符号における量子誤り訂正

誤りに対する仮定

- **エラーベクトル** $e_1 \in \mathbb{Z}_2^n$ **に相当する箇所で** bit flip
- **エラーベクトル** $e_2 \in \mathbb{Z}_2^n$ **に相当する箇所で** phaze flip
- $XZ = -ZX$ **より，**bit flip **と** phaze flip **の順番は無視できる**

$$|x + C_2\rangle \xrightarrow{e_2:\text{phase flip}} \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle$$

$$\xrightarrow{e_1:\text{bit flip}} \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$$

CSS 符号：bit flip の訂正

(1) **作業用の量子状態を付加**

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle \otimes |0\rangle$$

(2) C_1 **のパリティ検査行列** H_1 **によりユニタリ変換**

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle \otimes |H_1 e_1\rangle$$

(3) **シンドロームの測定：作業用の量子状態を測定して** $H_1 e_1$ **が分かる**

(4) $H_1 e_1$ **から** C_1 **の古典的誤り訂正能力により，** e_1 **が分かる**

(5) **作業用の量子状態を捨てて，エラーベクトル** e_1 **の箇所を** bit flip

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle$$

(phaze flip 訂正の前に) アダマール変換について

- $\mathbb{C}^2$ **上のアダマール変換：** $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $(H^{-1} = H$ **に注意)**
- H **の作用**

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

- **まとめて書くと**

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z \in \mathbb{Z}_2} (-1)^{xz} |z\rangle \quad (x \in \mathbb{Z}_2)$$

- $(\mathbb{C}^2)^{\otimes n}$ **上の拡大アダマール変換**

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \mathbb{Z}_2^n} (-1)^{x \cdot z} |z\rangle \quad (x \in \mathbb{Z}_2^n)$$

CSS 符号：phase flip の訂正

bit flip **訂正後の状態ベクトル**

$$(*) \quad \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} \, |x+y\rangle \;\rightarrow\; e_2 = \text{“0 ベクトル” としたい}$$

(1) 拡大アダマール変換を行う

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} \frac{1}{\sqrt{2^n}} \sum_{z \in \mathbb{Z}_2^n} (-1)^{(x+y)\cdot z} \, |z\rangle$$

$$= \frac{1}{\sqrt{2^n |C_2|}} \sum_{y \in C_2} \sum_{z \in \mathbb{Z}_2^n} (-1)^{(x+y)\cdot (e_2+z)} \, |z\rangle$$

$$= \frac{1}{\sqrt{2^n |C_2|}} \sum_{z' \in \mathbb{Z}_2^n} \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} \, |z' + e_2\rangle$$

[**和を交換**, $z' := z + e_2 \rightarrow z = z' - e_2 = z' + e_2$]

C_2 に関する補題

$$\sum_{y \in C_2} (-1)^{y \cdot z'} = \begin{cases} |C_2| & (z' \in C_2^{\perp}) \\ 0 & (z' \notin C_2^{\perp}) \end{cases}$$

- $z' \in C_2^{\perp}$ **のとき：**$y \cdot z' = 0 \ (\forall y \in C_2)$ **より明らか**
- $z' \notin C_2^{\perp}$ **のとき：**

$$f : y \in C_2 \subset \mathbb{Z}_2^n \longmapsto y \cdot z' \in \mathbb{Z}_2 = \{0, 1\}$$

の核 $\ker f = \{y \in C_2 \,|\, y \cdot z' = 0\}$ **を考える．**$\ker f$ **は加法群** C_2 **の部分群であるから，同値類による類別を考えると**

$$\#\left\{y \in C_2 \,\middle|\, y \cdot z' = 0\right\} = \#\left\{y \in C_2 \,\middle|\, y \cdot z' = 1\right\}$$

上記の和で 1 **と** -1 **は同じ数だけ現れる**

CSS 符号：phase flip の訂正 (つづき)

$$\frac{1}{\sqrt{2^n|C_2|}} \sum_{z' \in \mathbb{Z}_2^n} \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} \left| z' + e_2 \right\rangle$$

$$= \frac{1}{\sqrt{2^n|C_2|}} \sum_{z' \in \mathbb{Z}_2^n} (-1)^{x \cdot z'} \left\{ \sum_{y \in C_2} (-1)^{y \cdot z'} \right\} \left| z' + e_2 \right\rangle$$

$$= \frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} \left| z' + e_2 \right\rangle \quad [\because \textbf{補題}]$$

(2) bit flip **訂正と同様の手続きで，$C_2^\perp$ の誤り訂正能力により以下を得る**

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} \left| z' \right\rangle$$

(3) **拡大アダマール変換を再び行う：**
$H^{-1} = H$ **に注意すると** $(*)$ **で** $e_2 = 0$ **としたものに戻る**

参考文献

- M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge, 2000.
- **林正人**, **量子情報理論入門**, **サイエンス社**, 2004.
- M. Hayashi, Quantum Information: An Introduction, Springer, 2006. (**上記の英訳＋内容大幅増**)

(5) 量子秘密分散法

量子通信路の可逆性，消失性

○ 量子誤り訂正，量子暗号などで重要

○ $\mathcal{E}$ が $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H}_A)$ について可逆　(逆向き通信路で復元できる)

$$\overset{\text{def}}{\iff} \exists \mathcal{R}, \forall \rho_A \in \mathcal{S}, \mathcal{R}\mathcal{E}(\rho_A) = \rho_A$$

$$\forall \rho_A \in \mathcal{S} = \boxed{\mathcal{E}} \Rightarrow \mathcal{E}(\rho_A) = \boxed{\mathcal{R}} \Rightarrow \mathcal{R}\mathcal{E}(\rho_A) = \rho_A$$

○ $\mathcal{E}$ が $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H}_A)$ について消失的　(完全秘匿条件)

$$\overset{\text{def}}{\iff} \exists \rho_0 \in \mathcal{S}(\mathcal{H}_B), \forall \rho_A \in \mathcal{S}, \mathcal{E}(\rho_A) = \rho_0$$

$$\forall \rho_A \in \mathcal{S} = \boxed{\mathcal{E}} \Rightarrow \mathcal{E}(\rho_A) = \rho_0$$

(入力を変化 ==> 出力が同じ)

Holevo 量子相互情報量

Holevo, 1973

- $\mathcal{E} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$　量子通信路
- $\mathcal{P}_+(\mathcal{S})$: $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H}_A)$ 上至るところ正の確率測度全体
- $\mu \in \mathcal{P}_+(\mathcal{S})$ についての平均　$E_\mu[\,\cdot\,] := \int_{\mathcal{S}} \cdot\, \mu(\mathrm{d}\rho)$
- Holevo 情報量

$$I(\mu;\mathcal{E}) := E_\mu[D(\mathcal{E}(\rho)||\mathcal{E}(\sigma_\mu))]$$

$\rho \sim \mu$

$\sigma_\mu := E_\mu[\rho]$

小さくなる
(単調性)

特に，$I(\mu;\mathcal{I}_A) = E_\mu[D(\rho||\sigma_\mu)]$

Holevo 情報量と可逆性，消失性

Ogawa, Sasaki, Iwamoto, Yamamoto, 2004

定理：それぞれ (a), (b), (c) は同値

(1) [Holevo 情報量が不変 <==> 可逆]

(a) $\mathcal{E}$ は $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H}_A)$ について可逆

(b) $\forall \mu \in \mathcal{P}_+(\mathcal{S}),\ I(\mu;\mathcal{E}) = I(\mu, \mathcal{I}_A)$

(c) $\exists \mu \in \mathcal{P}_+(\mathcal{S}),\ I(\mu;\mathcal{E}) = I(\mu, \mathcal{I}_A)$

(2) [Holevo 情報量がゼロ <==> 消失的]

(a) $\mathcal{E}$ は $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H}_A)$ について消失的

(b) $\forall \mu \in \mathcal{P}_+(\mathcal{S}),\ I(\mu;\mathcal{E}) = 0$

(c) $\exists \mu \in \mathcal{P}_+(\mathcal{S}),\ I(\mu;\mathcal{E}) = 0$

応用例：量子秘密分散法

$\rho_A \in \mathcal{S}(\mathcal{H}_A)$

$\Downarrow$ W_N：分散符号化 (量子通信路)

$\mathcal{H}_N = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$

$W_N(\rho_A)$

全体

$N := \{1, \ldots, n\}$

$\mathcal{H}_X = \bigotimes_{i \in X} \mathcal{H}_i$

$W_X(\rho_A) := \mathrm{Tr}_{N \setminus X} W_N(\rho_A)$

一部を取り出す

$X \subseteq N$

○ X で ρ_A が復元可能 $\Longleftrightarrow$ W_X が $\mathcal{S}(\mathcal{H}_A)$ について可逆

Xは有資格集合と呼ぶ

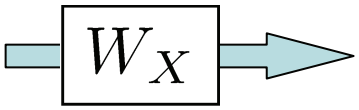
○ X で ρ_A が全く分からない $\Longleftrightarrow$ W_X が $\mathcal{S}(\mathcal{H}_A)$ について消失的

Xは禁止集合と呼ぶ

有資格条件と禁止条件

$\mathcal{S}_1(\mathcal{H})$：純粋状態全体

$$\rho \sim \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$$
$$\sigma_\mu = \mathrm{E}_\mu[\rho]$$



$$W_X(\rho)$$
$$W_X(\sigma_\mu)$$

Holevo 情報量

$$I(\mu;\mathcal{I}) = H(\sigma_\mu) - \mathrm{E}_\mu[H(\rho)] \qquad I(\mu;W_X)$$

0 for pure state

定理

以下の条件はそれぞれ同値

1. X は有資格集合 (resp. 禁止集合)
2. $\forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, $I(\mu;W_X) = H(\sigma_\mu)$ (resp. $= 0$)
3. $\exists \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, $I(\mu;W_X) = H(\sigma_\mu)$ (resp. $= 0$)

量子秘密分散法の符号化効率限界　Ogawa et al., 2004

○ von Neumann エントロピー　$H(\sigma) := -\operatorname{Tr}[\rho \log \rho]$

定理： 任意の (意味のある) 部分集合 $X \subseteq N$ について

Holevo情報量不変性の帰結　　pure state 全体

$$\forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}_A)), \quad H(\sigma_\mu) \leq H(W_X(\sigma_\mu))$$

μ： pure state 全体 $\mathcal{S}_1(\mathcal{H}_A)$ 上の一様分布とする

系 (Gottesman，2000)

任意の (意味のある) 物理系 $i \in N$ について

$\dim \mathcal{H}_A \leq \dim \mathcal{H}_i$　　オリジナルの系より小さくできない