量子情報 ー物理と情報ー

0. 量子力学の復習 ← スライド

残りは板書

1. 量子情報の基礎

2. 量子の"情報"とは? ー Schumacherの圧縮プロトコル ー

3. Hayden-Preskill模型 ー"多体系"での誤り訂正 ー

4. 量子通信容量 ー 誤り訂正の原理限界 ー

成績 : レポート (+出席) 〆切 :

参考書 : Nielsen & Chuang. やや古,

"Q. info. theory" by Mark Wilde

"The theory of Q. info." by John Watrous.

「量子情報科学入門」 by 石坂さん他.

「量子情報理論」 中田芳史 (朝倉書店)

↪ 今年中に出版.

0. 量子力学 (Quantum Mechanics) の復習

0-1. Q.M. の五公理

> 1. 物理系に付随するヒルベルト空間 $\mathcal{H}$ が存在し、
> その系の状態は $\mathcal{H}$ の単位ベクトル $|\psi\rangle \in \mathcal{H}$ で与えられる。

e.g.)

✓ spin-1/2 $\Longleftrightarrow$ 2次元ヒルベルト空間 $\mathbb{C}^2 = \mathrm{span}\{|0\rangle, |1\rangle\}$

↳ 基底 $\{|0\rangle, |1\rangle\}$

量子状態 : $\alpha|0\rangle + \beta|1\rangle \quad (|\alpha|^2 + |\beta|^2 = 1)$

↳ 任意の二準位系を qubit と呼ぶ。

✓ 波動関数 $\psi(x,t) \in L^2$: ∞次元ヒルベルト空間

↳ 本講義では取り扱わない。

2. 時間発展はユニタリUで与えられる。

Eg.1)

時刻 t $\qquad\qquad\qquad\qquad$ $t+dt$

$$|\psi(t)\rangle \xrightarrow{\text{ユニタリ}} |\psi(t+dt)\rangle = U(t,t+dt)\,|\psi(t)\rangle \quad ㊍$$

任意のユニタリUは、エルミート演算子Hを用いて $U = e^{-iH}$
$\approx I - iH + O(H^2)$
とかける。

$$\Rightarrow U(t,t+dt) = I - iH(t)\,dt$$

よって、㊍の両辺をdtの1次まで展開すれば、

$$|\psi(t)\rangle + d|\psi(t)\rangle = (I - iH(t)\,dt)\,|\psi(t)\rangle$$

$$\Leftrightarrow \frac{d}{dt}|\psi(t)\rangle = -i\underbrace{H(t)}_{\text{ハミルトニアン}}|\psi(t)\rangle\ ,\quad : \text{シュレーディンガー eq.}$$

E.g.2) 1 qubit：2×2 のユニタリ行列.

基底 $\{|0\rangle, |1\rangle\}$

ユニタリの例

✓ Pauli ops

$$
\begin{cases}
Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}
\end{cases}
$$

✓ Hadamard op.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$|0\rangle \stackrel{H}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =: |+\rangle$$

$$|1\rangle \stackrel{H}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |-\rangle$$

X の固有状態

よって、 $H = |+\rangle\langle 0| + |-\rangle\langle 1|$ ：Z と X に変換する.

E.g. 3) 1 qudit = d次元の系. Basis = $\{|0\rangle, \cdots, |d-1\rangle\}$.

ユニタリの例

$$X_d = \sum_{j=0}^{d-1} |j+1\rangle\langle j| \quad , \quad Z_d = \sum_{j=0}^{d-1} \omega^j |j\rangle\langle j| .$$

mod d

where $\omega = e^{2\pi i/d}$

$$= \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix} \qquad = \begin{pmatrix} 1 & & & 0 \\ & \omega & & \\ & & \omega^2 & \\ & & & \ddots & \\ 0 & & & & \omega^{d-1} \end{pmatrix}$$

$\{X_d^m Z_d^n\}_{m,n=0,\cdots,d-1}$: Heisenberg-Weyl ops.

Pauli ops の一般化.

3. 測定は基底 $\{|e_j\rangle\}_{j=0}^{d-1}$ で与えられて、

状態 $|\psi\rangle$ ⟶ 確率 $|\langle e_j|\psi\rangle|^2$ で結果 j を出力し、状態を $|e_j\rangle$ に変化させる。

e.g.) $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

✓ $\{|0\rangle, |1\rangle\}$ で測定
- → 0 prob. $|\langle 0|\psi\rangle|^2 = |\alpha|^2$
- → 1 prob. $|\langle 1|\psi\rangle|^2 = |\beta|^2$

✓ $\{|+\rangle, |-\rangle\}$ で測定
- → + prob. $|\langle +|\psi\rangle|^2 = \dfrac{|\alpha+\beta|^2}{2}$
- → − prob. $|\langle -|\psi\rangle|^2 = \dfrac{|\alpha-\beta|^2}{2}$

※ 測定基底で異なる確率分布

1つの状態からは実験では確率分布はわからない。

※ 1つの量子状態を測定すると、結果が1つ出力されて状態は破壊

後々のため、書き換えておく。

$$|\langle e_j|\psi\rangle|^2 = \langle e_j|\psi\rangle\langle\psi|e_j\rangle$$
$$= \mathrm{Tr}\left[\,|e_j\rangle\langle e_j|\ \ |\psi\rangle\langle\psi|\,\right]$$

ここで、 $\underbrace{\langle\psi|}_{\shortparallel} = \underbrace{(|\psi\rangle)}_{\shortparallel}^{\dagger}$, $|\psi\rangle\langle\psi| = |\psi\rangle\otimes\langle\psi|$ etc.

$(\bar{\psi}_1, \cdots, \bar{\psi}_d)$ 行ベクトル

$\begin{pmatrix}\psi_1\\ \vdots\\ \psi_d\end{pmatrix}$ 列ベクトル

$$:= \begin{pmatrix}\psi_1\langle\psi|\\ \vdots\\ \psi_d\langle\psi|\end{pmatrix}$$

$$= \begin{pmatrix}|\psi_1|^2 & \psi_1\bar{\psi}_2 & \cdots & \psi_1\bar{\psi}_d\\ \vdots & & \ddots & \vdots\\ \psi_d\bar{\psi}_1 & & \cdots & |\psi_d|^2\end{pmatrix}$$

4. 複合量子系 ⇒ テンソル積.

e.g.1)

系A　　　　系B

$\mathcal{H}^A$　　　　$\mathcal{H}^B$

基底 $\{|e_j\rangle\}_{j=1}^{d_A}$　　　　$\{|f_\alpha\rangle\}_{\alpha=1}^{d_B}$

⟹ 1つの系とみなす = 系AB

$$\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$$

$$:= \mathrm{span}\{|e_j\rangle^A \otimes |f_\alpha\rangle^B\}_{j=1,\alpha=1}^{d_A,\ d_B}$$

※ $\mathcal{H}^{AB} = \mathrm{span}\{|e_j\rangle^A \otimes |f_\alpha\rangle^B\}_{j,\alpha}$ なので、$|\varphi\rangle^{AB} \in \mathcal{H}^{AB}$ は一般に

$$|\varphi\rangle^{AB} = \sum_{j=1}^{d_A} \sum_{\alpha=1}^{d_B} C_{j\alpha} |e_j\rangle^A \otimes |f_\alpha\rangle^B$$

という形をしている。必ずしも $|\varphi\rangle^{AB} = \underbrace{|\xi\rangle^A \otimes |\zeta\rangle^B}_{\text{積状態 (プロダクト状態)}}$ とは書けない

"非プロダクト状態" = エンタングル状態

e.g.2) 2 qubits $= \mathrm{span}\{\underbrace{|00\rangle}_{=|0\rangle\otimes|0\rangle}, |01\rangle, |10\rangle, |11\rangle\}$

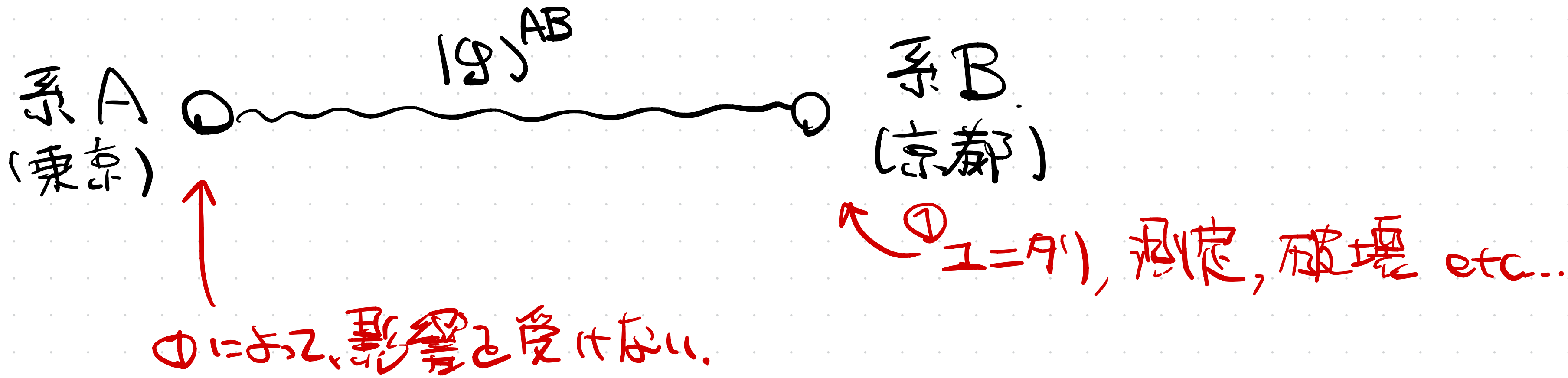
プロダクト状態の例 : $|00\rangle, \cdots, |11\rangle, |++\rangle, |0+\rangle, |-\varphi\rangle, \cdots$

エンタングル状態の例 : $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)$, etc.

$$\frac{1}{2}(|+0\rangle + \sqrt{2}|-1\rangle + |1-\rangle)$$

5. 因果律

> 複合系AB ： Bでどのような操作を行っても、その操作の結果がAに伝えられない限り、Aの状態は変化しない。



ただし、Bから Aに測定結果が伝えられた場合はこの限りではない。

↳ 量子特有ではないことに注意。

Bでサイコロを振って、1を得る。

- 伝えない → A：prob. 1/6 です!!
  ↓ 変化
- 伝える → A：prob. 1 で 1 !!

0-2. Q.M. から Quantum Information へ

Q.M. の五公理の拡張

0-2-1. 量子状態

アンサンブル

「確率 p_j で状態 $|\varphi_j\rangle$ を準備する」 $= \{p_j, |\varphi_j\rangle\}_{j=1}^{J}$

⟺ ベクトルでは表現できない。

密度行列 : $\rho = \sum_{j=1}^{J} p_j \underbrace{|\varphi_j\rangle\langle\varphi_j|}_{\text{行列}}$

全ての固有値 ≥ 0

⟺

✓ 性質1. $\rho \geq 0$ $\quad (\Leftrightarrow \forall |\psi\rangle, \ \langle\psi|\rho|\psi\rangle \geq 0)$

[∵) $\langle\psi|\rho|\psi\rangle = \sum_j p_j \langle\psi|\varphi_j\rangle\langle\varphi_j|\psi\rangle = \sum_j p_j |\langle\psi|\varphi_j\rangle|^2 \geq 0$

✓ 性質2. $\mathrm{Tr}[\rho] = 1$ $\quad$ ∵) $\mathrm{Tr}[\rho] = \sum_j p_j \mathrm{Tr}[|\varphi_j\rangle\langle\varphi_j|]$

$= \sum_j p_j \langle\varphi_j|\varphi_j\rangle = \sum_j p_j = 1$

拡張公理1

量子状態 $\overset{\text{def}}{\Longleftrightarrow}$ 密度行列 ρ ($\rho \geq 0$, $\mathrm{Tr}[\rho]=1$)

※ ベクトルで表せる状態 $|\varphi\rangle$: pure state (純粋状態)

$\Updownarrow$

⇔ 密度行列は $|\varphi\rangle\langle\varphi|$ 　　ランクが1の密度行列

(対角化可能な行列) non-zeroの固有値の数

$$\mathrm{rank}\,\rho \begin{cases} =1 & : \text{pure state} \\ \geq 2 & : \text{mixed state (混合状態)} \end{cases}$$

重要なこと!!

アンサンブル $\underset{\text{多対1}}{\rightleftarrows}$ 密度行列

e.g.) 1 qubit

完全混合状態

$$\pi = \frac{I}{2} = \begin{cases} \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right), \quad \frac{1}{2}\left(|+\rangle\langle +| + |-\rangle\langle -|\right) \\ \frac{1}{3}\left(|\varphi_1\rangle\langle\varphi_1| + |\varphi_2\rangle\langle\varphi_2| + |\varphi_3\rangle\langle\varphi_3|\right) \quad \text{etc....} \end{cases}$$

> 定理：同じ密度行列を持つ2つのアンサンブルを見分ける物理操作は存在しない。

因果律の帰結

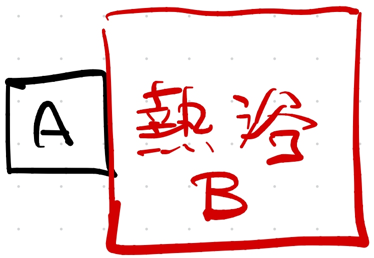
$$\sum_j p_j |\varphi_j\rangle\langle\varphi_j| = \sum_\alpha q_\alpha |\psi_\alpha\rangle\langle\psi_\alpha|$$

$\Rightarrow \{p_j, |\varphi_j\rangle\}$ と $\{q_\alpha, |\psi_\alpha\rangle\}$ は物理として同一.

$\Leftrightarrow$ アンサンブル表記は物理として"冗長"な表現.

0-2-2 時間発展

e.g.) 熱平衡化.



Aの状態

$t=0$ $\qquad$ $t\gg1$

$$|\varphi\rangle\langle\varphi| \longrightarrow \rho_{th} \propto e^{-\beta H}$$

非ユニタリ

ランクが増化 $\left(|\varphi\rangle\langle\varphi| \xrightarrow{U} U|\varphi\rangle\langle\varphi|U^\dagger \right)$

↳ 全系(AB)がユニタリでも、部分系はユニタリとは限らない。

部分系を"捨てる" = 部分トレース.

$\mathcal{H}^{AB}$ 上の密度行列: ρ^{AB}.

$\{|f_\alpha\rangle^B\}_\alpha$: 系Bの基底

$$\rho^A := \mathrm{Tr}_B[\rho^{AB}] = \sum_{\alpha=1}^{d_B} \left(I^A \otimes \langle f_\alpha|^B \right) \rho^{AB} \left(I^A \otimes |f_\alpha\rangle^B \right)$$

系Aの縮約密度行列 (reduced density matrix, marginal state)

拡張公理2.

Stinespring拡張

時間発展 $\overset{\mathrm{def}}{\Longleftrightarrow}$ 全系のユニタリ + 部分トレース

$\Longleftrightarrow$ 量子チャンネル (CPTP写像)

$\Longleftrightarrow$ Kraus表現.

CPTP map   Completely-Positive Trace-Preserving

$\mathcal{J}^{A\to C}$: $\mathfrak{A}^A$上のop. $\longrightarrow$ $\mathfrak{A}^C$上のop で以下をみたすもの

CP性

任意の系R $\rho^{AR} \geq 0$

$$\Rightarrow (\mathcal{J}^{A\to C} \otimes \mathrm{id}^R)(\rho^{AR}) \geq 0$$

TP性

$$\mathrm{Tr}[\mathcal{J}^{A\to C}(\rho^A)] = \mathrm{Tr}[\rho^A].$$

Kraus 表現

$\{K_j^{A\to C}\}_j$ で $\sum_j (K_j^{A\to C})^\dagger K_j^{A\to C} = I^A$ をみたし、

$d_A \times d_C$の行列.

$$\mathcal{J}^{A\to C}(\rho^A) = \sum_j K_j^{A\to C} \rho^A (K_j^{A\to C})^\dagger$$

とかける。

e.g.) ユニタリ時間発展 : $U^A \rho^A U^{A\dagger}$ から $U^{A\dagger} U^A = I^A$

Stinespring 拡張

$AB = CD$

ユニタリ

$$\mathcal{J}^{A\to C}(\rho^A) = \mathrm{Tr}_D\left[U^{AB}(\rho^A \otimes |0\rangle\langle 0|^B)(U^{AB})^\dagger\right]$$

0-2-3. 量子測定.

拡張公理 3.

量子測定 $\overset{\text{def}}{\Longleftrightarrow}$ Positive-Operator-Valued Measure

✓ POVM : $\{M_j\}_j$ で $\begin{cases} M_j \geq 0 \\ \sum_j M_j = I \end{cases}$ をみたすもの.

ρ を測定 $\Longrightarrow$ 結果 j を prob. $\mathrm{Tr}[M_j \rho]$ で得る.

[測定後の状態も気にする場合は、Instrument]

✓ $\{|e_j\rangle\}_j$ を基底として、 $M_j = |e_j\rangle\langle e_j|$ とすれば、元の公理.

Naimark拡張 : POVM = 部分系を $\{|e_j\rangle\}_j$ で測定.

0-2-4. コメント.

Q.M. 公理1〜5 $\overset{\text{等価}}{\Longleftrightarrow}$ Q.info. 拡張1〜3, 公理4,5

全系を見るイメージ

部分系も重要.

(広義の)Q.info.の目標.

この5公理から何を示せるか?

→ 化学

→ 生物.

→ 量子動.

量子計算

暗号

通信

多体系 (量子カオス, トポロジカル秩序, 熱平衡化 etc..)

基礎論 (非局所性 etc..)

今回のターゲット.

NOTE　混合状態 $\Leftrightarrow$ 純粋状態 + 部分トレース

$\rho^A = \sum_j p_j |e_j\rangle\langle e_j|^A \Rightarrow$ 新しい系 A' を導入して、

対角化

$$|\rho\rangle^{AA'} := \sum_j \sqrt{p_j}\, |e_j\rangle^A |e_j\rangle^{A'}$$

ρ^A の純粋化

を考えると、

$$\mathrm{Tr}_{A'}\left[|\rho\rangle\langle\rho|^{AA'}\right] = \rho^A.$$

※純粋化は一意ではないことに注意。

例1)

$$\pi^A = I^A/2 \xleftarrow{\mathrm{Tr}_{A'}} \frac{1}{\sqrt{2}}\left(|00\rangle^{AA'} \pm |11\rangle^{AA'}\right),$$

$$\frac{1}{\sqrt{2}}\left(|++\rangle^{AA'} \pm |--\rangle^{AA'}\right),$$

$$\frac{1}{2}\left(|0\rangle^A|e_1\rangle^{A'} + |1\rangle^A|e_2\rangle^{A'} + |+\rangle^A|e_3\rangle^{A'} + |-\rangle|e_4\rangle^{A'}\right)$$

etc...

1 qubitの完全混合状態。

0-3. いくつかの数学的準備

✓ よく用いる恒等式：

$$I^A = \sum_{j=1}^{d_A} |e_j\rangle\langle e_j|^A \quad : \{|e_j\rangle\}_{j=1}^{d_A} \text{ は } \mathcal{H}^A \text{ の基底}$$

✓ アイソメトリ（等長写像，埋め込み）

ユニタリの一般化みたいなもの.

$V^{A\to B}$: $d_B \times d_A$ の行列で，$(V^{A\to B})^\dagger V^{A\to B} = I^A$ をみたす.

アイソメトリ

Remark

- $d_A = d_B$ の場合は単にユニタリ.
- $d_A > d_B$ の場合は存在しない. $\Longrightarrow$ $d_A \leq d_B$ は暗黙の了解.

・$\{|e_j\rangle^A\}_{j=1}^{d_A}$: Aの基底 , $\{|f_j\rangle\}_{j=1}^{d_B}$: Bの基底.

アイソメトリ $V^{A\to B} = \sum_{j=1}^{d_A} |f_j\rangle^B \otimes \langle e_j|^A = {}_{d_B}\begin{pmatrix} \text{た} \\ \text{て} \\ \text{な} \\ \text{が} \\ \text{い} \end{pmatrix}$

d_A

check : $V^\dagger V = \left(\sum_{i=1}^{d_A} |f_i\rangle\langle e_i|\right)^\dagger \sum_{j=1}^{d_A} |f_j\rangle\langle e_j|$

$= \sum_{j=1}^{d_A} |e_j\rangle\langle e_j|^A = I^A$

$V^{A\to B}(V^{A\to B})^\dagger = \left(\sum_{i=1}^{d_A} |f_i\rangle\langle e_i|\right)\left(\sum_{j=1}^{d_A} |f_j\rangle\langle e_j|\right)^\dagger$

$= \sum_{j=1}^{d_A} |f_j\rangle\langle f_j|^B$ ← I^Bではなく projection.

$|\varphi\rangle^A = \sum_{j=1}^{d_A} c_j |e_j\rangle^A$ とすると、$V^{A\to B}|\varphi\rangle^A = \underbrace{\sum_{j=1}^{d_A} c_j |f_j\rangle^B}_{\leftarrow \text{Bの部分空間}}$: 埋め込み

e.g.) アイソメトリの例.

- pure state $|\varphi\rangle^A$: $d_A \times 1$ の(縦長)行列で

$$(|\varphi\rangle)^\dagger |\varphi\rangle = \langle\varphi|\varphi\rangle = 1.$$

↪「状態$|\varphi\rangle^A$を準備する」という物理操作,

- $\underset{\text{ユニタリ}}{U^A} \otimes |\psi\rangle^B$

$$U^A \otimes |\psi\rangle^B = \begin{pmatrix} u_{11} & \cdots & u_{1d_A} \\ \vdots & \ddots & \vdots \\ u_{d_A1} & \cdots & u_{d_Ad_A} \end{pmatrix} \otimes \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_{d_B} \end{pmatrix}$$

$$= \left.\underbrace{\begin{pmatrix} u_{11}\begin{pmatrix} \psi_1 \\ \vdots \\ \psi_{d_B} \end{pmatrix} & \cdots & u_{1d_A}\begin{pmatrix} \\ \\ \\ \end{pmatrix} \\ \vdots & \ddots & \vdots \\ u_{d_A1}\begin{pmatrix} \\ \vdots \\ \\ \end{pmatrix} & \cdots & u_{d_Ad_A}\begin{pmatrix} \\ \\ \\ \end{pmatrix} \end{pmatrix}}_{d_A}\right\} d_Ad_B$$

系AにユニタリU^Aをかけて、系Bに$|\psi\rangle^B$を準備する.

$\boxed{d_Ad_B \times d_A \text{ の行列}}$

✓ 純粋化の自由度

定理：$|\rho\rangle^{AR_1}$, $|\rho\rangle^{AR_2}$ が ρ^A の純粋化で $d_{R_1} \le d_{R_2}$ とすると、

アイソメトリ $V^{R_1\to R_2}$ が存在し、

$$|\rho\rangle^{AR_2} = V^{R_1\to R_2} |\rho\rangle^{AR_1}$$

<u>check</u>

$$\mathrm{Tr}_{R_2}\left[|\rho\rangle\langle\rho|^{AR_2} \right]$$

$$= \mathrm{Tr}_{R_2}\left[V^{R_1\to R_2} |\rho\rangle\langle\rho|^{AR_1} (V^{R_1\to R_2})^\dagger \right]$$

↓ cyclic.

$$= \mathrm{Tr}_{R_1}\left[|\rho\rangle\langle\rho|^{AR_1} \underbrace{(V^{R_1\to R_2})^\dagger V^{R_1\to R_2}}_{= I^{R_1}} \right]$$

$= I^{R_1}$ ∵ アイソメトリ

$$= \mathrm{Tr}_{R_1}\left[|\rho\rangle\langle\rho|^{AR_1} \right] = \rho^A.$$