量子情報科学
ウィンタースクール2010

2010.2.25-27

1日目: 量子力学の基礎

2日目: 量子情報理論の基礎I

3日目: 量子情報理論の基礎IIと応用

木村元(産業技術総合研究所 情報セキュリティ研究センター)

Outline

- 量子力学復習 + 数学補講
- はじめに
- 量子情報科学の基礎

  -- 一般の状態 単位ベクトルから密度行列へ

  -- 合成系の部分状態 縮約密度行列と部分トレース

  -- 一般の測定 エルミート行列からPOVM測定

  -- POVMの表現(実現)定理

量子力学(復習)

① 量子系の状態はHilbert空間 $\mathcal{H} = \mathbb{C}^d$ の単位ベクトル

② 物理量はエルミート行列

③ Bornの確率規則

$$|\psi\rangle \in \mathcal{H}$$

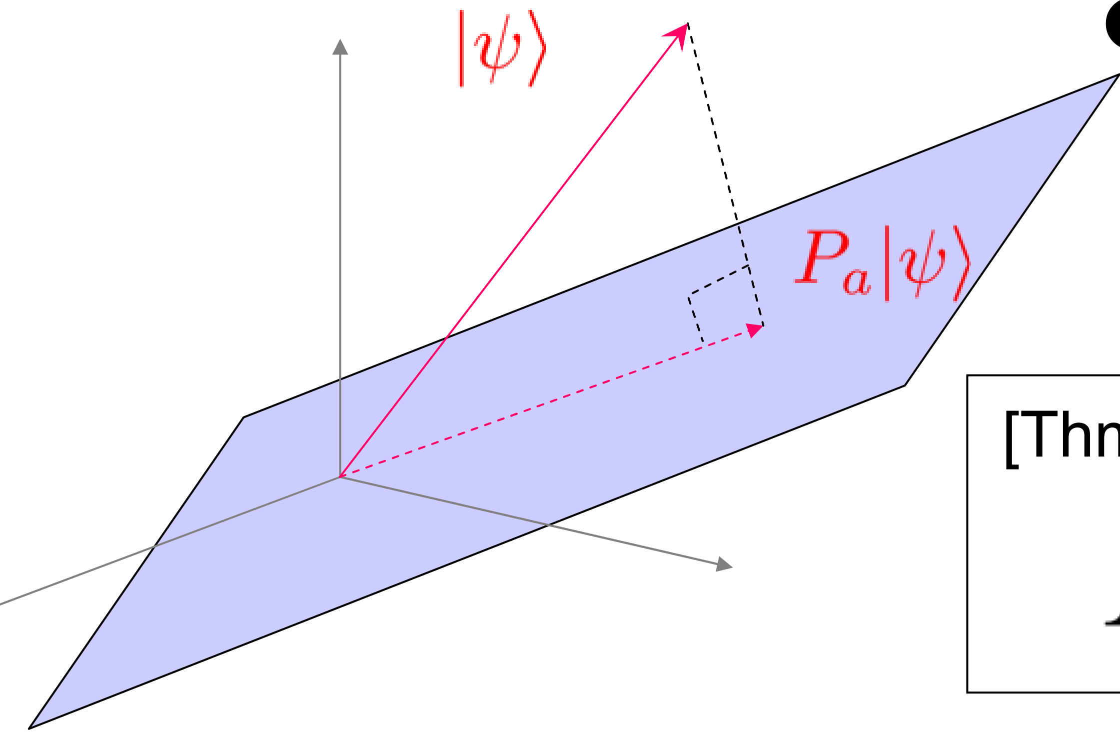
$$A = \sum_i a_i P_i$$

測定値aiを得る確率

$$\langle \psi | P_i | \psi \rangle$$

● エルミート行列Aの固有値aの固有空間:

$$E_a := \{|\psi\rangle \in \mathbb{C}^d \mid A|\psi\rangle = a|\psi\rangle\}$$



● (対応する)固有射影行列

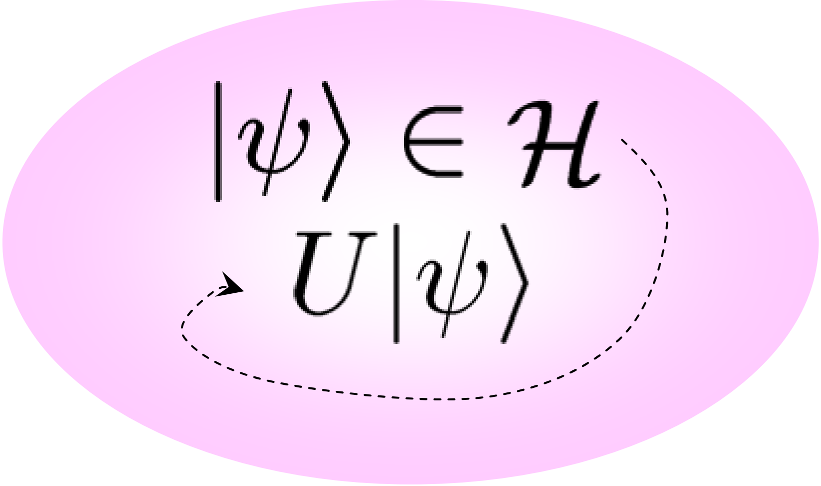
$$P_a \in M_d(\mathbb{C})$$

[Thm] 任意のエルミート行列は

$$A = \sum_a aP_a$$

量子力学（復習2）

① 孤立量子系の時間発展はユニタリー発展 U= exp(-iHt)

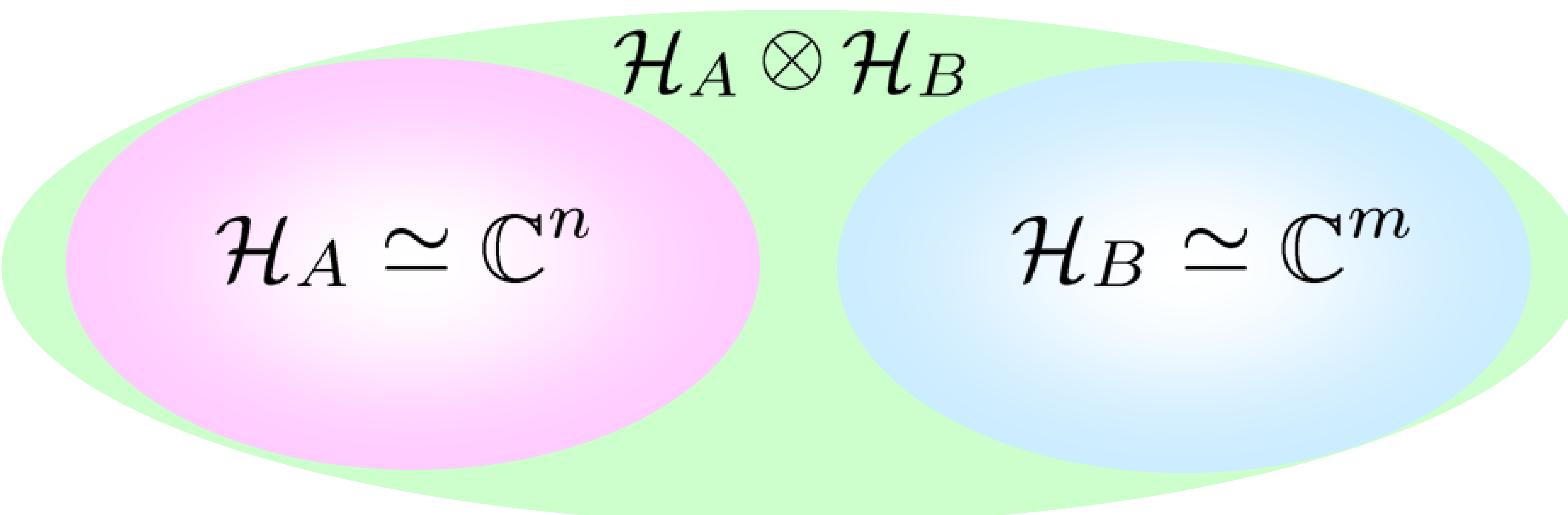


量子力学(復習2)

① 孤立量子系の時間発展はユニタリー発展 U= exp(-iHt)

$$|\psi\rangle \mapsto U|\psi\rangle$$

② 合成量子系はテンソル積Hilbert空間



Hilbert空間のテンソル積1

$$\mathcal{H}_A = \mathbb{C}^n, \mathcal{H}_B = \mathbb{C}^m \Rightarrow \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^{nm}$$

(例) $n = m = 2$:　２量子ビット

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \\ a_2 \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \cdots$$

● Hilbert空間のテンソル積2

☆最重要性質1 (双線形性)

$$|\psi\rangle \otimes (x|\phi\rangle + y|\xi\rangle) = x(|\psi\rangle \otimes |\phi\rangle) + y(|\psi\rangle \otimes |\xi\rangle)$$

$$(x|\psi\rangle + y|\chi\rangle) \otimes |\phi\rangle = x(|\psi\rangle \otimes |\phi\rangle) + y(|\chi\rangle) \otimes |\phi\rangle.$$

● Hilbert空間のテンソル積2

☆最重要性質2 (テンソル基底)

$$\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}\colon\ \mathcal{H}_A \text{ の CONS},$$
$$\{|\phi_1\rangle, \ldots, |\phi_m\rangle\}\colon\ \mathcal{H}_B \text{ の CONS}$$

$$\Rightarrow \{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j}\colon\ \mathcal{H}_A \otimes \mathcal{H}_B \text{ の CONS}$$

$$\{|\psi_1\rangle \otimes |\phi_1\rangle, |\psi_1\rangle \otimes |\phi_2\rangle, \cdots, |\psi_i\rangle \otimes |\phi_j\rangle, \cdots, |\psi_n\rangle \otimes |\phi_m\rangle\}$$

$$\Rightarrow \dim \mathcal{H}_A \otimes \mathcal{H}_B = nm.$$

● Hilbert空間のテンソル積2

☆最重要性質3 (エンタングルド状態)

$$|\phi\rangle \otimes |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$$

セパラブル状態

$$|\phi\rangle \otimes |\psi\rangle + |\chi\rangle \otimes |\xi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$$

$$\neq |\eta\rangle \otimes |\nu\rangle$$

エンタングルド状態

● 演算子のテンソル積1

X: 系 A の（エルミート）行列,
Y: 系 B の（エルミート）行列

$$\Rightarrow \ X \otimes Y\text{: 合成系 } \mathcal{H}_A \otimes \mathcal{H}_B \text{ 上の行列}$$

(例) $n = m = 2$: 2 量子ビット

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \otimes \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} x_{11} \boxed{\begin{matrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{matrix}} & x_{12} \boxed{\begin{matrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{matrix}} \\ x_{21} \boxed{\begin{matrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{matrix}} & x_{22} \boxed{\begin{matrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{matrix}} \end{pmatrix}$$

$$\sigma_z \otimes \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

● 演算子のテンソル積2

☆最重要性質1 (テンソル積演算)

$$X \otimes Y(|\psi\rangle \otimes |\phi\rangle) = (X|\psi\rangle) \otimes (Y|\phi\rangle)$$

☆最重要性質2

$$\forall Z\text{: } \mathcal{H}_A \otimes \mathcal{H}_B \text{ 上の行列} \Rightarrow Z = \sum_i X_i \otimes Y_i$$

はじめに

自然の解明，存在論 ⇒ 自然の可能性，認識論

量子力学の公理

＊Hilbert空間の単位ベクトルは実現可能な状態
＊Hilbert空間のエルミート行列は実現可能な測定

実現可能な状態

単位ベクトル

$|\psi\rangle$

実現可能な測定

エルミート行列の測定

A

はじめに

存在論

$$|\psi\rangle \in \mathcal{H}$$

$$A = \sum_i a_i P_i$$

⇒

測定値aiを得る確率

$$\langle\psi|P_i|\psi\rangle$$

操作的に
何が可能か？

① ある状態に準備

単位ベクトル
⇒ 密度行列

②系の測定をする

エルミート行列
⇒ POVM測定

③確率的に測定値
（情報）を得る

一般的な状態(密度行列)

- 量子状態の準備方法

  - 状態 $|\psi\rangle$ を準備する

$|\psi\rangle$

一般的な状態(密度行列)

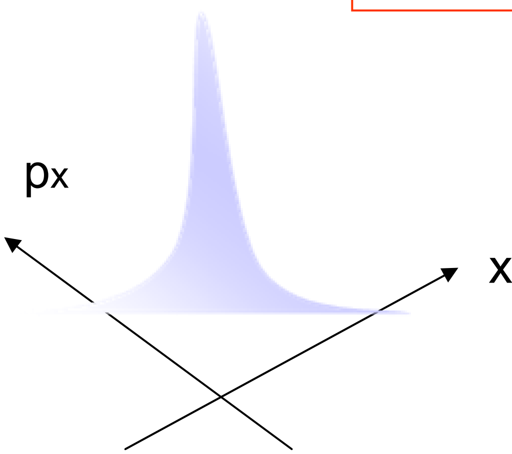
量子状態の準備方法

このような状況も
量子状態とみなしてよい!

- 状態 $|\psi\rangle$ を準備する

- 確率 p_i で状態 $|\psi_i\rangle$ を準備する $\{p_i; |\psi_i\rangle\}$

$\simeq$ 状態が確率 p_i で $|\psi_i\rangle$ にあることしか知らない



$$p_1 \quad p_2 \quad \cdots \quad p_n$$

$$|\psi_1\rangle? \quad |\psi_2\rangle? \quad \cdots \quad |\psi_n\rangle?$$

一般的な状態(密度行列)

- 密度行列による状態表現とBornの確率規則

状態 $|\psi\rangle$ の下で，物理量 $A = \sum_i a_i P_i$ を測定:

$$\boxed{\Pr\{a_i | A, |\psi\rangle\} = \langle\psi|P_i|\psi\rangle}$$

一般的な状態(密度行列)

- 密度行列による状態表現とBornの確率規則

状態 $\{p_k; |\psi_k\rangle\}$ の下で，物理量 $A = \sum_i a_i P_i$ を測定する

$$\Pr\{a_i | A, |\psi\rangle\} = \qquad \langle\psi_k | P_i | \psi_k\rangle$$

密度行列

	従来の表記	密度行列の表記
状態	$\{p_k; \lvert\psi_k\rangle\}$	$\rho = \sum_k p_k \lvert\psi_k\rangle\langle\psi_k\rvert$
確率	$\sum_k p_k \langle\psi_k\lvert P_i \rvert\psi_j\rangle$	$\mathrm{tr}(\rho P_i)$
期待値	$\sum_k p_k \langle\psi_k\lvert A \rvert\psi_j\rangle$	$\mathrm{tr}(\rho A)$

[定理]

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$$

$$\Leftrightarrow \mathrm{tr}\,\rho = 1, \rho \geq 0$$

[定義] Hilbert空間上の単位トレースを持ち，正値である行列を**密度行列**と呼ぶ.

量子力学で準備可能な一般的な状態は密度行列 ρ で与えられる. **Bornの確率規則**は

$$\rho,\ A = \sum_i a_i P_i \ \Rightarrow\ \text{確率}\ \mathrm{tr}(\rho P_i)$$

純粋状態と混合状態

$$\rho = |\psi\rangle\langle\psi|:\ \text{純粋状態}$$

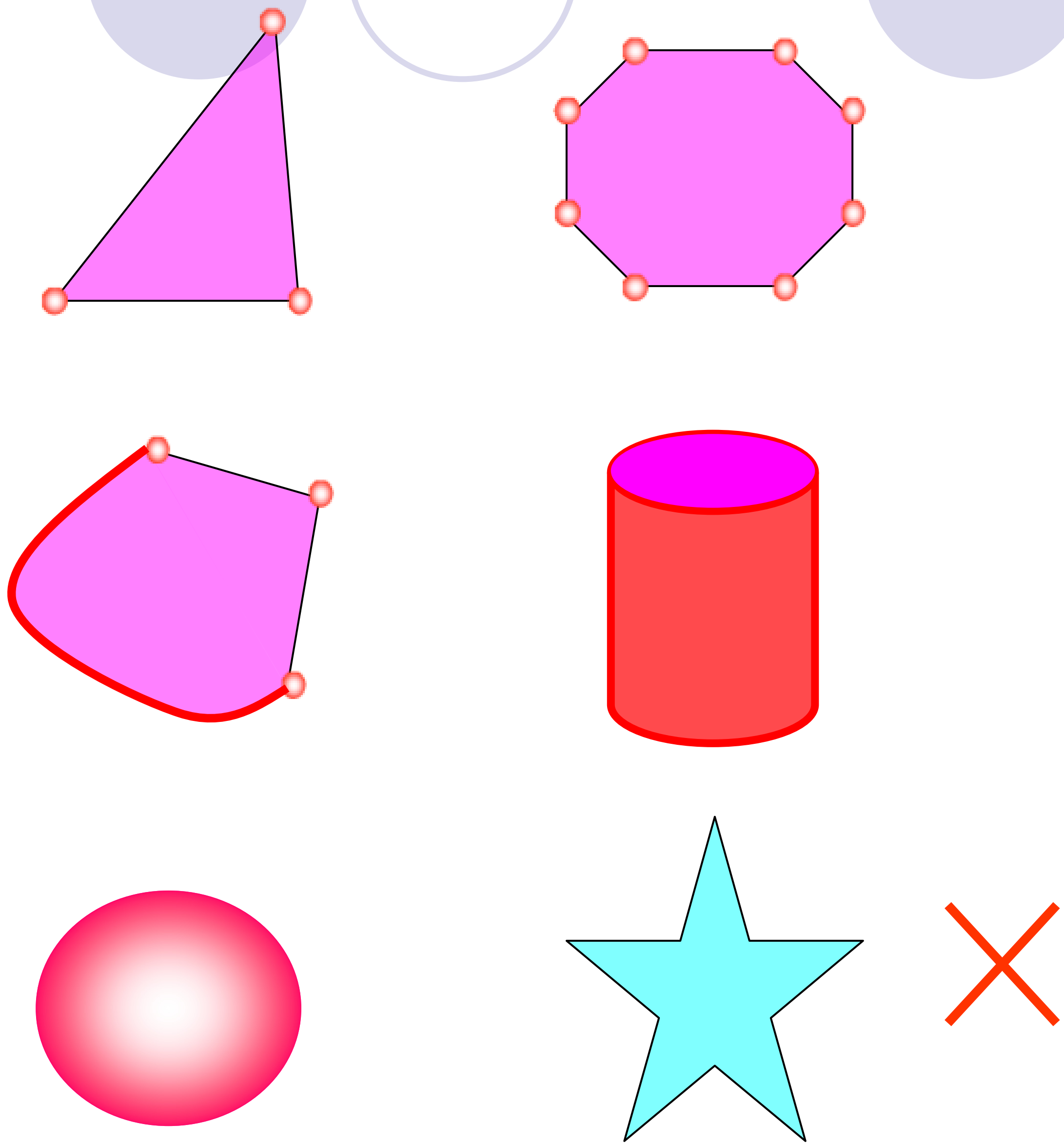
$$\rho \neq |\psi\rangle\langle\psi|:\ \text{混合状態}$$

$$\boxed{S := \{\rho \mid \operatorname{tr}\rho = 1, \rho \geq 0\} \quad \text{状態空間}}$$

（エルミート行列空間内の）凸集合

$$\rho_1, \rho_2 \in \mathcal{S}, p \in [0,1]$$

$$\Rightarrow p\rho_1 + (1-p)\rho_2 \in \mathcal{S} \quad \simeq \{p, 1-p; \rho_1, \rho_2\}$$



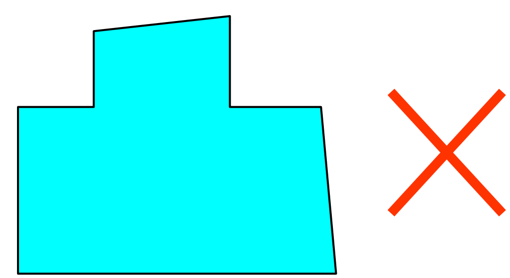
凸集合w

$$w_1, w_2 \in W, \lambda \in [0,1]$$
$$\Rightarrow w = \lambda w_1 + (1-\lambda) w_2 \in W$$

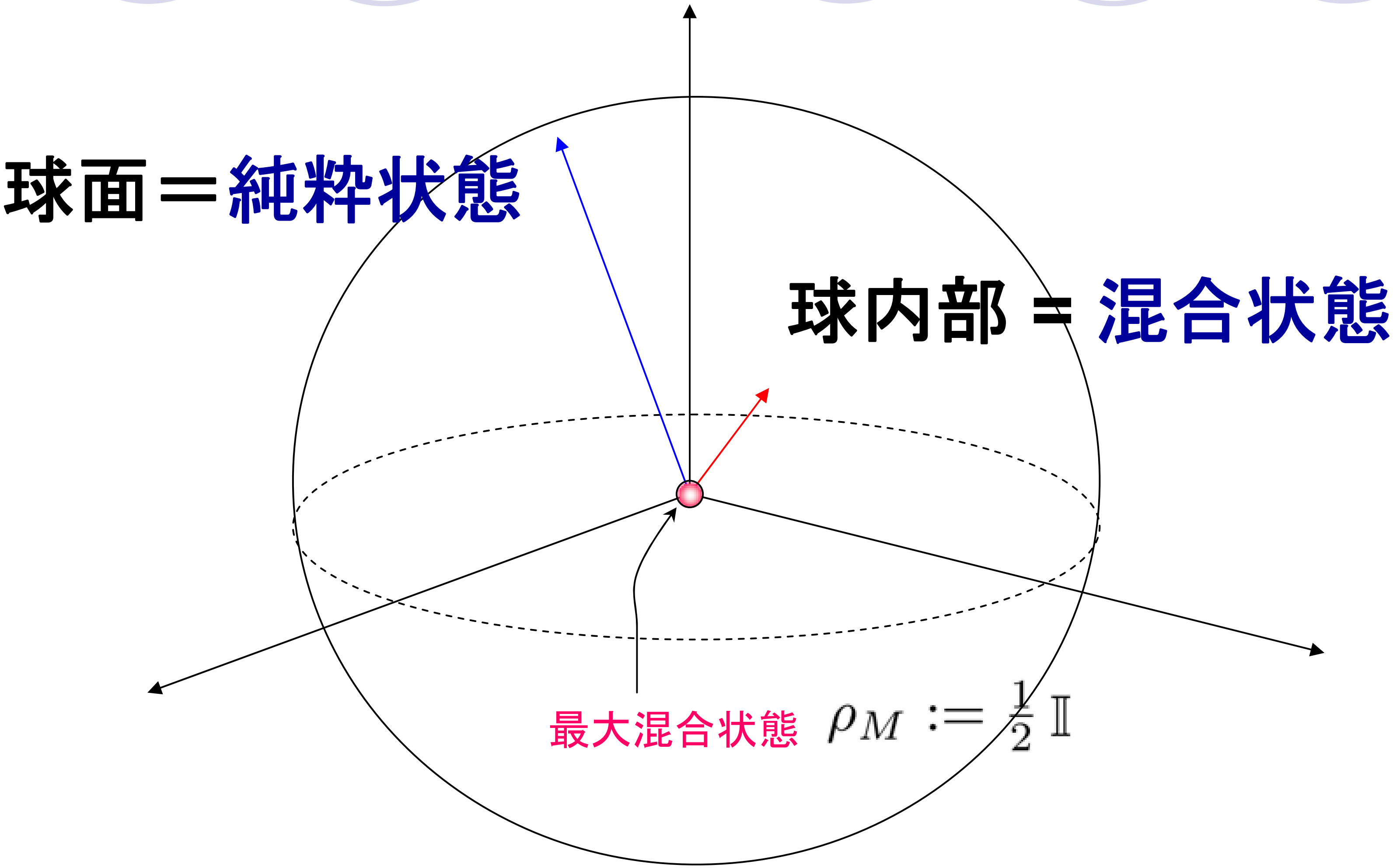
端点: w

$$\lambda \in (0,1), w_1, w_2 \in \mathcal{S}$$
$$\text{s.t. } w = \lambda w_1 + (1-\lambda) w_2$$
$$\Rightarrow w = w_1 = w_2$$

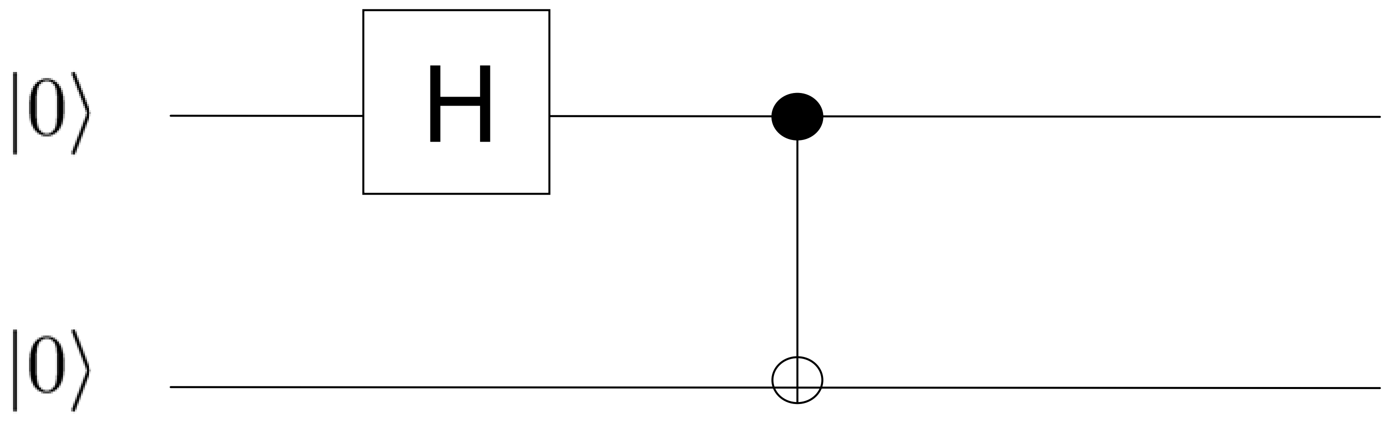
⇔ 純粋状態



量子ビットの状態空間 ≒ Bloch球

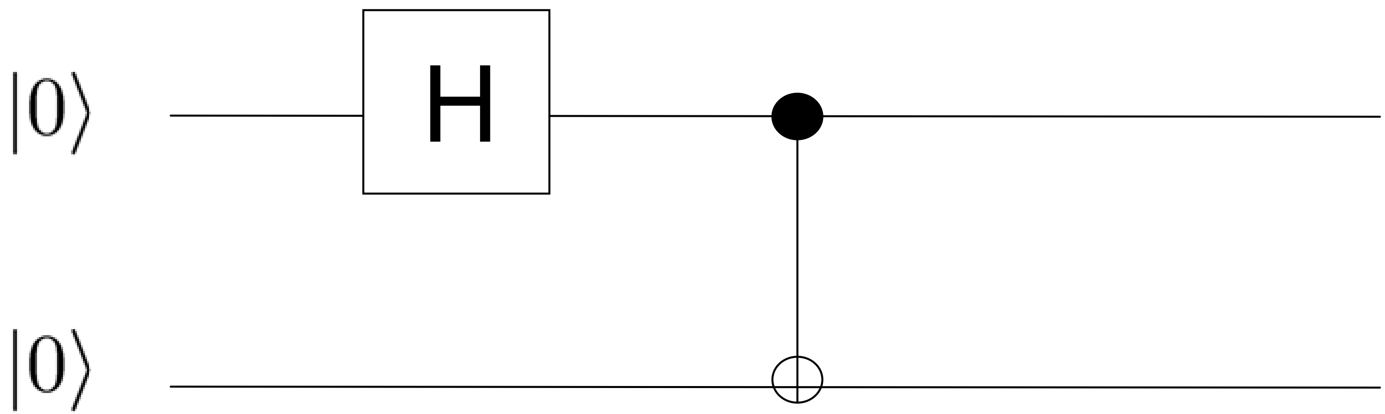


部分量子系の状態(縮約密度行列)

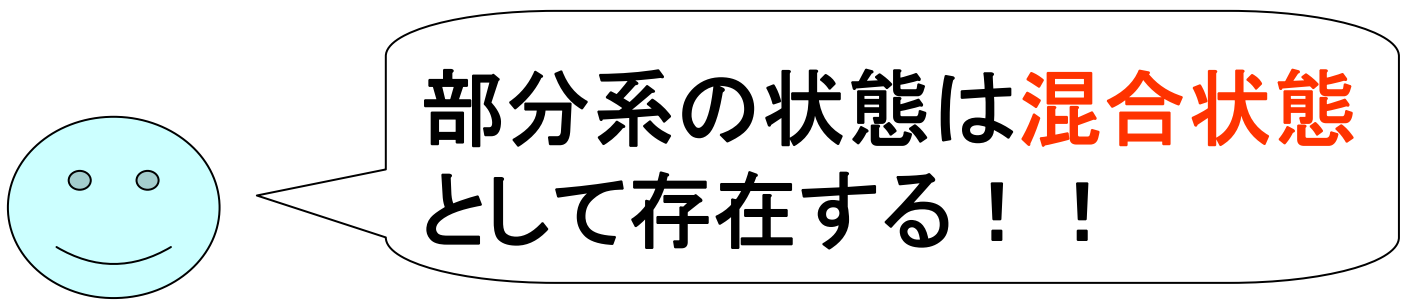


$$\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}$$

部分量子系の状態(縮約密度行列)



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



部分量子系の状態(縮約密度行列)

[定理] 合成系 $A+B$ の状態が密度行列 ρ_{AB}

$\Rightarrow$ A 系の状態は縮約密度行列 ρ_A で与えられる！

$$\rho_A := \mathrm{tr}_B\, \rho_{AB}$$

[部分トレース]

$$\mathrm{tr}_B\, Z = \mathrm{tr}_B\left(\sum_i X_i \otimes Y_i\right) := \sum_i (\mathrm{tr}_B\, Y_i) X_i$$

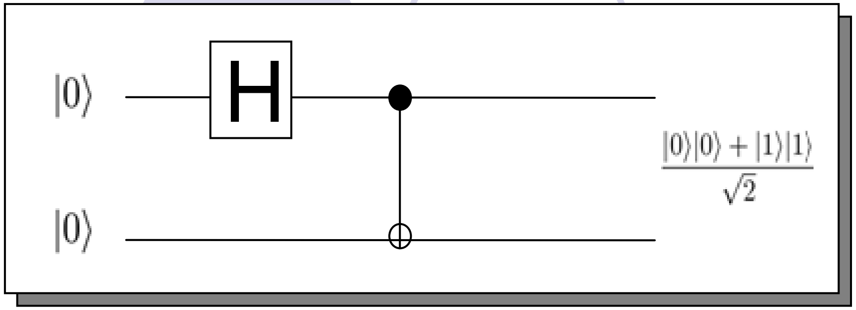
$\forall Z$: $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の行列 $\Rightarrow Z = \sum_i X_i \otimes Y_i$

A 系の状態 ρ_A, 任意の物理量 O_A の期待値：$\mathrm{tr}(\rho_A O_A)$

A 系の物理量 O_A の期待値：

$$
\begin{aligned}
E[O_A]_{\rho_{AB}} &= \mathrm{tr}_{AB}(\rho_{AB} O_A \otimes \mathbb{I}_B) \\
&= \mathrm{tr}_A\,\mathrm{tr}_B(\rho_{AB} O_A \otimes \mathbb{I}_B) \\
&= \mathrm{tr}_A(\boxed{\mathrm{tr}_B(\rho_{AB})} O_A)
\end{aligned}
$$

A系の密度行列!



[Prop] $\mathrm{tr}\,|\psi\rangle\langle\phi| = \langle\phi|\psi\rangle$

$$\rho_{AB} = |\psi\rangle\langle\psi| \;\; = \left(\tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)\left(\tfrac{1}{\sqrt{2}}(\langle 00| + \langle 11|)\right)$$

$$= \tfrac{1}{2}\,(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1|$$

$$+ |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |0\rangle\langle 1| \otimes |0\rangle\langle 1|)$$

$$\rho_A = \mathrm{tr}_B\, \rho_{AB}$$

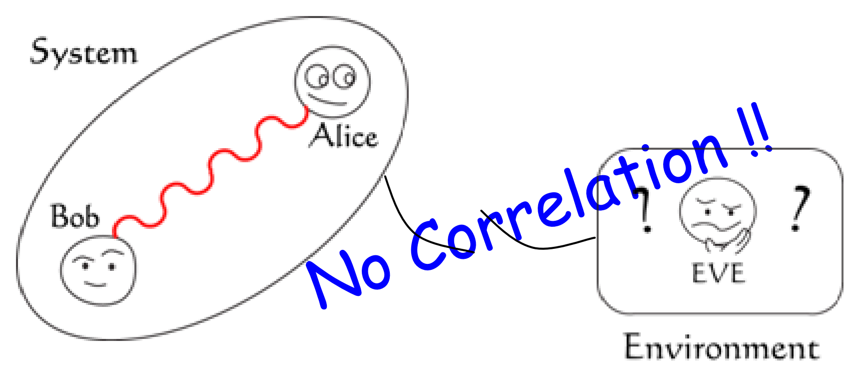
$$= \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \tfrac{1}{2}\,\mathbb{I}$$ **（最大）混合状態!**

全体系が純粋状態 $\cancel{\Rightarrow}$ 部分も純粋

[定理] 全体系の状態に相関があるとき,
部分系は必ず混合状態にある

[定理] 部分系が純粋状態ならば, その系は他の系と相関を持ち得ない！

Quantum
Key
Distribution



一般の測定（POVM測定）

測定とは？

①測定をすると，測定値xを確率的に得るもの．

$M = \{M_x\}$

確率 $\Pr\{x \mid M, \rho\}$

x

[確率混合の条件]　If $\rho = p\rho_1 + (1-p)\rho_2$,

$$\Pr\{x \mid M, \rho\} = p\Pr\{x \mid M, \rho_1\} + (1-p)\Pr\{x \mid M, \rho_2\}$$

一般の測定（POVM測定）

[定義] (離散)POVM* とは，行列の組み
$M = (M_x)_x$ で，$M_x \geq 0, \sum_x M_x = \mathbb{I}$ を満たすもの.

[定理] 確率混合の条件を満たす任意の測定は，
ある POVM により以下のように記述される：

$$\Pr\{x|\rho, M\} = \mathrm{tr}\,\rho M_x$$

* Positive operator valued measure：正作用素値測度

一般の測定（POVM測定）

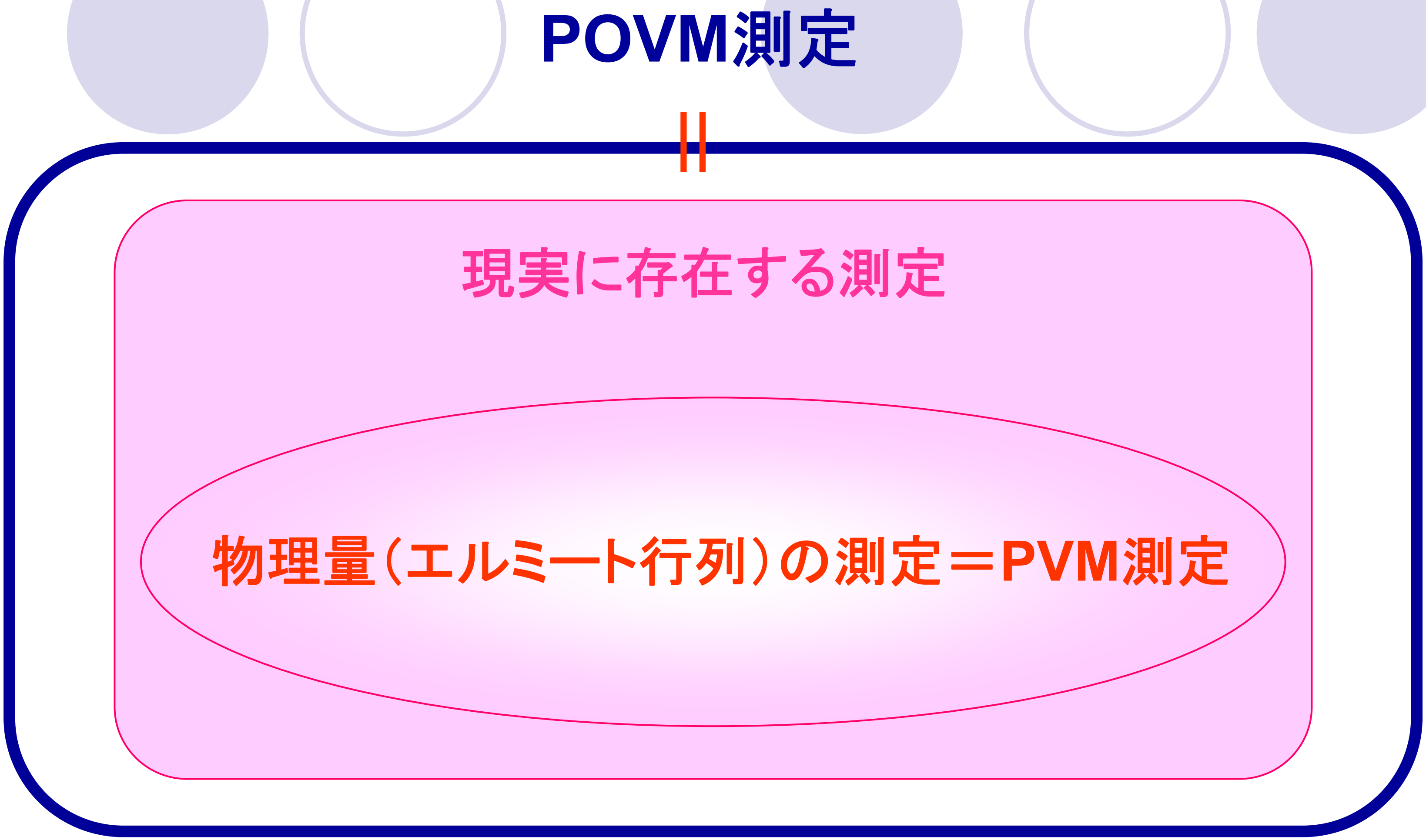
[定義] (離散)PVM**とは，POVM $M = (P_x)$ で，P_x が射影行列のものをいう．

[命題] PVM$\{P_i\}$ はエルミート演算子の固有射影 $\{P_i\}$.

[定理] 物理量の測定と PVM 測定は等価.

** projection valued measure： 射影作用素値測度

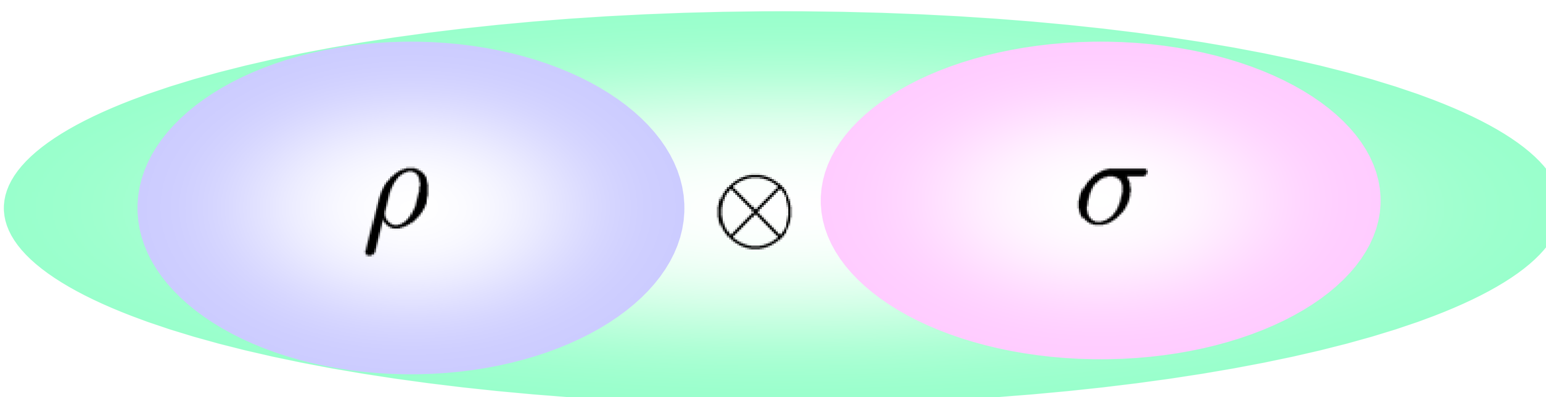
確率混合条件を満たす測定＝POVM測定



[定理] 任意のPOVM測定は物理的に実現可能！

間接測定モデル

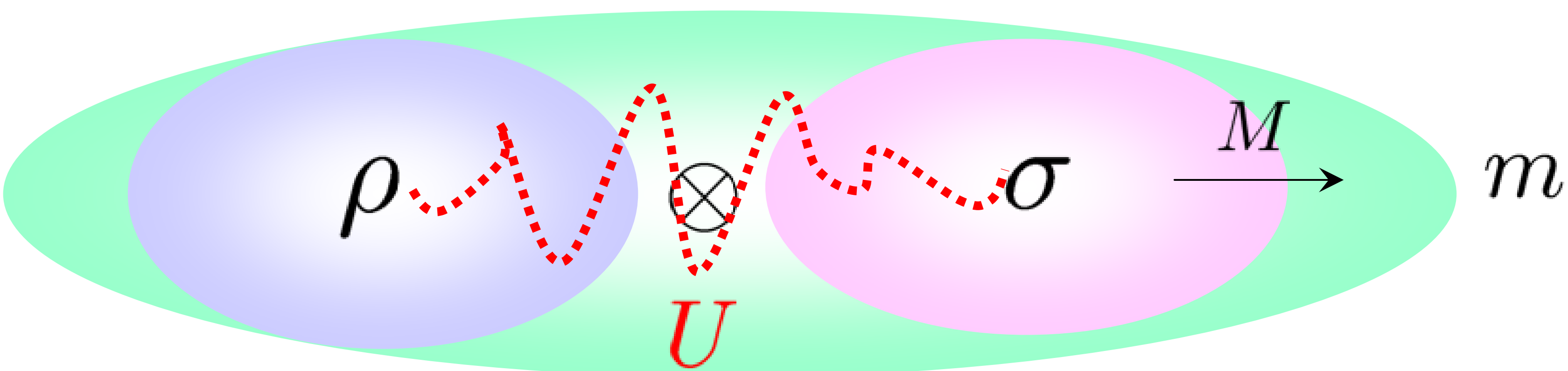
測定の役割:
系の情報を引き出す！



①状態をρに準備　②他の系（測定装置）をσに準備

間接測定モデル

測定の役割:
系の情報を引き出す！

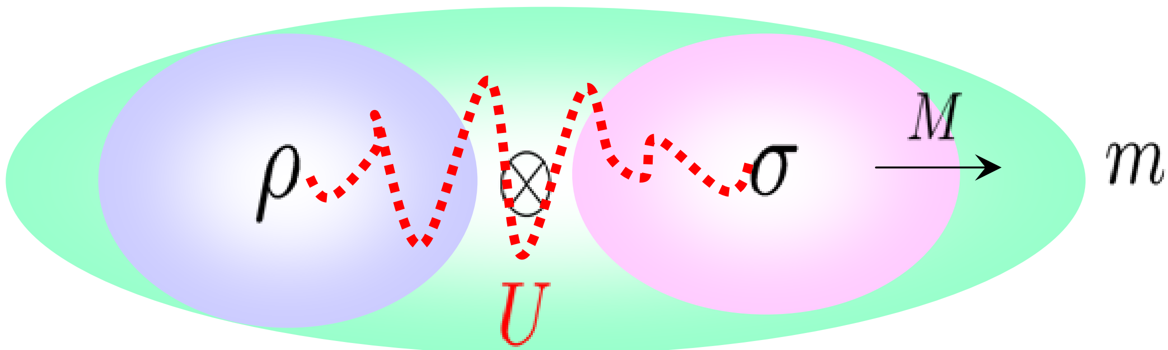


①状態をρに準備　　②他の系（測定装置）をσに準備

③ 全体系でユニタリー発展させる（相互作用）

④ 測定装置の物理量を測定する！

間接測定モデル



1 $\rho \otimes \sigma$

2 $\rho' := U\rho \otimes \sigma U^\dagger$

3 $\Pr\{m|M,\rho'\} = \mathrm{tr}[(U\rho \otimes \sigma U^\dagger)\mathbb{I} \otimes P_m]$

[定理] 任意の POVM 測定 $E = (E_m)_m$ を実現する間接測定モデル $(\mathcal{H}_M, \sigma, U, M)$ が存在する：

$$\mathrm{tr}(\rho E_m) = \mathrm{tr}[(U\rho \otimes \sigma U^\dagger)\mathbb{I} \otimes P_m]$$