

量子情報科学春の勉強会

量子情報科学春の勉強会実行委員

2009 年 2 月 25 日-3 月 1 日

概 要

本講義ノートは、量子情報科学春の勉強会（2009 年 2 月 25 日-3 月 1 日）@川渡共同センターの 4 人の講師（石坂智（NEC）、小川朋宏（電気通信大学 / JST）、木村元（AIST）、林正人（東北大学））による講義に関する講義ノートです。作成者は鹿野豊（東京工業大学 / MIT）、秋本大樹（東北大学（当時、東京大学））によるものです。講義中に作成しているノートをもとに作成しているため、完全なノートとは違いますので、ご了承ください。また、このノートをもとに勉強し、量子情報科学の魅力を発見、再発見していただければ幸いです。

目 次

1	木村 元 (AIST) 2/26 講義	1
1.1	数学の準備	1
1.2	量子力学とは?	2
1.3	量子力学の”公理”	2
1.4	量子力学の再定式化	4
1.4.1	隠れた変数があるか?	4
1.4.2	量子力学の再定式化	4
2	石坂 智 (NEC) 2/26 講義	6
2.1	エンタングルメントとは?	6
2.2	エンタングルメントの判定	7
3	小川 朋宏 (電通大) 2/26 講義	7
3.1	イントロ	7
3.2	例	7
3.3	量子通信路	8
3.4	Kraus 表現	9
3.5	パラメータ表現	10
4	林 正人 (東北大) 2/27 講義	10
5	林 正人 (東北大) 2/28 講義	13
6	石坂 智 (NEC) 2/28 講演	15
6.1	局所操作と古典通信 (LOCC)	15
6.2	エンタングルメントの定量化	15
6.3	エンタングルメントの濃縮	16
6.4	量子データ圧縮	17
6.5	エンタングルメントの希釈	17
6.6	混合状態のエンタングルメント	17
6.7	混合状態のエンタングルメント判定	18
6.7.1	ペレス判定法	18
6.7.2	縮約判定法	18
6.8	混合状態と LOCC	18
7	小川 朋宏 (電通大) 2/28 講演	19
7.1	Kraus Steinespring	21
7.2	量子暗号	22
7.3	量子暗号の安全性	22

1 木村 元 (AIST) 2/26 講義

量子情報科学入門

量子力学系（量子効果・現象）を利用した様々な情報処理の原理や応用を研究する学問。

量子力学 情報科学 量子情報

（今回の講義の概要） 量子力学基礎論（測定 etc.） ← 量子計算理論 量子通信理論 量子推
定理論 エンタングルメント

（応用） 量子コンピューター 量子テレポーテーション 量子暗号

（Outline） 1. 量子力学の一般的枠組み

2. 量子力学の再定式化 - 操作論に自然な定式化

3. 量子情報理論入門 - 量子テレポーテーション、Dense Coding(高密度符号化)

（Motivation） 自然の解明 存在論 自然の可能性 認識論

1.1 数学の準備

$\mathbb{C}^d$ Hilbert space

ケットベクトル

$$|x\rangle := \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix} \in \mathbb{C}^d \quad (1)$$

ブラベクトル

$$\langle x| := (\bar{x}_1, \bar{x}_2, \bar{x}_d) \quad (2)$$

内積

$$\langle x|y\rangle = (\bar{x}_1, \bar{x}_2, \bar{x}_d) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_d \end{pmatrix} = \sum_{i=1}^d \bar{x}_i y_i \quad (3)$$

$$|x\rangle\langle y| = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{pmatrix} (\bar{y}_1, \bar{y}_2, \bar{y}_d) = \begin{pmatrix} x_1 \bar{y}_1 & \cdots & x_1 \bar{y}_d \\ \vdots & \ddots & \vdots \\ x_d \bar{y}_1 & \cdots & x_d \bar{y}_d \end{pmatrix} \quad (4)$$

A:エルミート

固有値分解

$$\begin{aligned} A &= \sum_i a_i |a_i\rangle\langle a_i| \\ &= \sum_j a_j \left(\sum_i |a_j\rangle\langle a_i| \right) \\ &= \sum_j a_j P_j \end{aligned} \quad (5)$$

ただし、 $\{|a_i\rangle\}$: CONS

$$A|a_i\rangle = a_i|a_i\rangle \quad (6)$$

$$\forall |\psi\rangle \in \mathbb{C}^d$$

$$\sum \langle a_i | \psi \rangle \langle a_i | = |\psi\rangle \quad (7)$$

$$P_j P_k = \delta_{j,k} P_j \quad (8)$$

$$\sum P_j = 1 \quad (9)$$

1.2 量子力学とは？

”原子や素粒子などの微視的な世界の現象を説明する物理の基礎理論”

$\hbar$: Plank 定数 $\simeq 6.626 \times 10^{-34} J \cdot s$ 大きさ 原子の大きさ $1\text{\AA} (= 10^{-10}m)$ テニスボールと原子 地球の大きさと $2cm$

1.3 量子力学の”公理”

公理 1 全ての量子系には、一つの複素 Hilbert space ($\mathcal{H}$) が伴う。量子系の状態は $\mathcal{H}$ の単位ベクトルであらわされる。

今日は $\dim \mathcal{H} < \infty$ $\mathcal{H} \simeq \mathbb{C}^d$

$= d$ d 準位量子系

$= 2$ qubit(量子ビット) 系

例: qubit

$$|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (10)$$

(注意) 全体の位相因子 ($e^{j\theta}$) の相違は同一視する。 $|\psi\rangle \simeq |\psi'\rangle = e^{i\theta} |\psi\rangle$

(注意) 状態を足すことができる。(重ね合わせの原理)

(注意) 全ての単位ベクトル(「状態ベクトル」と呼ぶ。)は状態とみなす。

公理 2 物理量(位置、運動量 etc.) A はエルミート演算子で表される、測定値は、 A の固有値の一つが確率的に得られる。固有値 a_j を得られる確率は

$$\Pr[a_j | A, |\psi\rangle] = \langle \psi | P_j | \psi \rangle \quad (11)$$

(Born の確率規則)

(注意) $\langle \psi | P_j | \psi \rangle$ は確率分布か? $\langle \psi | P_j | \psi \rangle \geq 0, \sum_j \langle \psi | P_j | \psi \rangle = 1$

(注意) A : 縮退がない (A の固有値に重複度がない) 場合

$$P_j = |a_j\rangle \langle a_j| \quad \Pr[a_j | A, |\psi\rangle] = \langle \psi | (|a_j\rangle \langle a_j|) | \psi \rangle = |\langle a_j | \psi \rangle|^2 \quad |\psi\rangle = \sum \langle a_j | \psi \rangle |a_j\rangle$$

(例) $d = 2$ qubit

Pauli 行列

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (12)$$

- エルミート
- 固有値 ± 1

- $\sigma_j^2 = 1$ σ_j はユニタリー

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (13)$$

交換子

$$[A, B] = AB - BA \quad (14)$$

$$[\sigma_x, \sigma_y] = 2i\sigma_z \quad (15)$$

$|\psi\rangle = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ のとき、 σ_z を測定すると

$$|\psi\rangle = \frac{1}{\sqrt{5}}|\uparrow\rangle + \frac{2}{\sqrt{5}}|\downarrow\rangle \quad (16)$$

確率 $1/5$ で $+1$, $1/5$ で -1

(注意) 期待値

$$\langle A \rangle_\psi = \sum a_i \text{Pr}[a_i|A, \psi] = \langle \psi | (\sum a_i P_i) | \psi \rangle = \langle \psi | A | \psi \rangle \quad (17)$$

(例) $|\psi\rangle = |\uparrow\rangle$ のとき σ_x を測定

$$\langle \sigma_x \rangle_\psi = \langle \psi | \sigma_x | \psi \rangle = 0 \quad (18)$$

→ 確率 $1/2$ で $+1$, 確率 $1/2$ で -1

(注意) 全てのエルミート演算子は測定可能

(注意) A, B, C を同時に測定できるとは限らない! → 不確定性関係ただし、 A と B が可換な場合 ($[A, B] = 0$)、同時測定可能 a_i, b_j を得る結合確率分布は

$$\text{Pr}[a_i, b_j|A, B, |\psi\rangle] = \langle \psi | P_i^A P_j^B | \psi \rangle \quad (19)$$

(注意) $C = A + B$ 測定値の間に関数関係が定まるだろうか? ← $[A, B] = 0$ の場合、 A の測定値 $a + B$ の測定値 $b = C$ の測定値 c 一般には成り立たない。

(注意) A の規格化された固有ベクトル ← 固有状態

固有状態 A の確定的状態

(注意) 測定後、状態は一般に変化する。

反復仮説: A を測定して、 a が得られたとするならば、その直後に A を測定すると、必ず a が得られる。

A : 非縮退

$$A|u_i\rangle = a_i|u_i\rangle \quad (20)$$

$|\psi\rangle$ で A を測定 $a_u \rightarrow$ (波束の収縮) $\rightarrow |u_i\rangle$

(注意) σ_x, σ_z は互いに相補的 σ_z の確定状態は、 σ_x の最も不確定な状態 (vice versa)

(注意)

$$\langle \psi' | P_j | \psi' \rangle = e^{-i\theta} \langle \psi | P_j e^{i\theta} | \psi \rangle = \langle \psi | P_j | \psi \rangle \quad (21)$$

公理 3 孤立系の状態の時間発展はユニタリー演算子 U で記述される。

$$\begin{array}{ccc} |\psi\rangle & \longrightarrow & U|\psi\rangle \\ t = t_0 & & t = t_1 \end{array} \quad (22)$$

(背後に Schrödinger eq. がある。)

公理 4 二つの量子系 $\mathcal{H}_1, \mathcal{H}_2$ の豪勢系には、テンソル積 Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ で記述される。 $\mathcal{H}_1$ 上で物理量 A は、 $\mathcal{H}_1 \otimes \mathcal{H}_2$ 上では、 $A \otimes 1$ に対応する。

(注意) $|\phi\rangle, |\xi\rangle$ を $\mathcal{H}_1, \mathcal{H}_2$ の状態ベクトル $|\psi\rangle = |\phi\rangle \otimes |\xi\rangle$: $\mathcal{H}_1 \otimes \mathcal{H}_2$ の状態ベクトル: 積状態 (セパラブル状態)

$|\psi\rangle \neq \quad \quad \quad$: エンタングル状態

(注意) $\mathcal{H}_1$ での物理量 A 、 $\mathcal{H}_2$ での物理量 B は同時測定可能

(例) 2 つの qubit 系の場合 $\simeq \mathbb{C}^4$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle) \quad (23)$$

$$n \cdot \sigma = n_x \sigma_x + n_y \sigma_y + n_z \sigma_z < n \cdot \sigma_1, m \cdot \sigma_2 > = \sum a_i b_j P_j(a_i, b_j) = -n \cdot m \quad (24)$$

$n = m$ のとき、 $\langle n \cdot \sigma_1, m \cdot \sigma_2 \rangle = -1$ $n \cdot \sigma \otimes 1$ と $1 \otimes m \cdot \sigma$ 完全反相関

1.4 量子力学の再定式化

1.4.1 隠れた変数があるか？

量子力学には隠れた変数？ $\rightarrow$ Bohm 流、Nelson 流 etc.

しかし、”もっともらしい”仮定を課すと、量子力学には隠れた変数はなさそう。

Kochen-Specker の定理 (1967) 量子力学 ($\dim \mathcal{H} \geq 3$) では、整合性条件を満たす (文脈非依存型) 隠れた変数は存在しない。全ての物理量には、観測には無関係に実在の値を持つ。

整合性条件 $A \longrightarrow (\nu) \longrightarrow \nu(A) \in \{A \text{ の固有値} \}$

If $[A, B]=0$ then

$$\nu(A+B) = \nu(A) + \nu(B), \nu(AB) = \nu(A)\nu(B) \quad (25)$$

EPR パラドックス (1935) 実在とは?(十分条件)

もし、系を乱さずに確実に値が预言できる時、その物理量に対応する実在の要素が存在する。

Bell の不等式 (1960) 量子力学には、局所隠れた変数は存在しない!!

1.4.2 量子力学の再定式化

今まで $|\psi\rangle$: 状態ベクトル

今後 $\{p_i, |\psi_i\rangle\}$ 確率 p_i で状態 $|\psi_i\rangle$ に準備 $\rightarrow$ 密度行列

今まで $\rho_\psi = |\psi\rangle\langle\psi|$

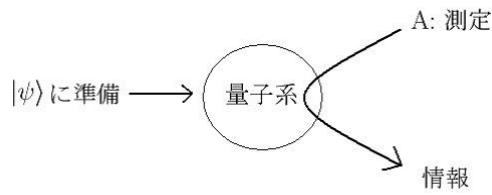
今後 $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$

EPR パラドックス

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)$$



測定のイメージ



Born の確率規則

$$\Pr[a_k|A, P] = \text{Tr}(\rho P_k) \quad (26)$$

(i) ρ_ψ のとき

$$\text{Tr}(\rho_\psi P_k) = \text{Tr}(|\psi\rangle\langle\psi| P_k) = \langle\psi| P_k |\psi\rangle \quad (27)$$

(ii) ρ のとき

$$\text{Tr}(\rho P_k) = \text{Tr}[(\sum p_i |\psi_i\rangle\langle\psi_i|) P_k] = \sum p_i \text{Tr}[|\psi_i\rangle\langle\psi_i| P_k] = \sum p_i \langle\psi_i| P_k |\psi_i\rangle \quad (28)$$

一般に、行列 ρ が $\rho \geq 0$, $\text{Tr} \rho = 1$ のとき、 ρ は密度行列と呼ぶ。

1. $\rho_\psi = |\psi\rangle\langle\psi|$, $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$ は密度行列

2. $\forall \rho$: 密度行列は

$$\rho = \sum p_i |P_i\rangle\langle P_i| \quad (29)$$

以後、量子系の状態は密度行列で表される。 $\rho = |\psi\rangle\langle\psi|$ と書ける時、純粋状態。それ以外は混合状態

$$S(H) = \{\rho \in M(\mathbb{C}^d) | \rho \geq 0, \text{Tr} \rho = 1\} : \text{凸集合}$$

$$\forall \lambda \in [0, 1], \rho_1, \rho_2 \in S(H)$$

$$\lambda \rho_1 + (1 - \lambda) \rho_2 \in S(H) \quad (30)$$

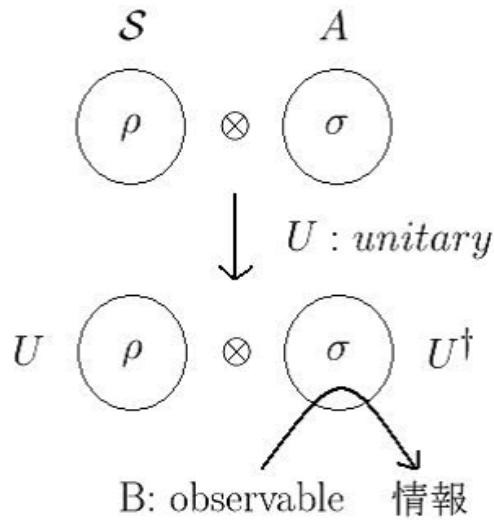
Positive Operator Valued Measure (POVM) 測定 一般的考察測定 M とは、状態 ρ に依存して、測定値 $\{m_i\}$ が得られる確率が決まる。 $\Pr[m|M, \rho]$ は以下の性質を満たす。

1. 確率分布

2. ρ に関して affine $\forall \lambda \in [0, 1] \rho_1, \rho_2 \in S(H),$

$$\Pr(m_i|M, \lambda \rho_1 + (1 - \lambda) \rho_2) = \lambda \Pr(m_i|M, \rho_1) + (1 - \lambda) \Pr(m_i|M, \rho_2) \quad (31)$$

測定とは？



Theorem 1. 一般に上記の (1)(2) を満たす測定は *POVM* で記述される。

Definition 1. *POVM* $M \in \{M_j\}$ s.t. $M_j \geq 0, \sum M_i = 1$

$$\Pr[n_j|M, \rho] = \text{Tr}[\rho M_j] \quad (32)$$

$A = \sum \alpha_j P_j$ は observable $\text{Tr} \rho P_j$: $\{P_j\}$:*POVM* を *PVM* と呼ぶ。

$$\text{Tr}[U(\rho \otimes \sigma)U^\dagger(1 \otimes P_j)] = \Pr[b_j] \quad (33)$$

Theorem 2. $\forall$ *POVM* $\exists(H_d, \sigma, U, B)$

$$\text{Tr}(\rho M_j) = \text{Tr}[U(\rho \otimes \sigma)U^\dagger(1 \otimes P_j)] \quad (34)$$

以後 (2) 測定は *POVM* $\{M_i\}$ で記述され、 $\Pr(n_j) = \text{Tr}(\rho M_j)$

2 石坂 智 (NEC) 2/26 講義

2.1 エンタングルメントとは？

(スライド)

測定のプロセス

PVM $\{P_i\}$

$$p_i = \text{Tr} \rho P_i \quad (35)$$

$$\rho \longrightarrow \rho' = \frac{1}{p_i} P_i \rho P_i \quad (36)$$

$$|\psi\rangle \longrightarrow P_i |\psi\rangle \quad (37)$$

2.2 エンタングルメントの判定

還元密度行列 σ_{AB}

$$\sigma_A := \text{Tr}_B \sigma = \sum_k \langle b_k | \sigma_{AB} | b_k \rangle \quad (38)$$

$$\sigma_B := \text{Tr}_A \sigma = \sum_k \langle a_k | \sigma_{AB} | a_k \rangle \quad (39)$$

(例 1)

$$|\psi\rangle = |00\rangle \quad (40)$$

$$\sigma_{AB} = |\psi\rangle\langle\psi| = |00\rangle\langle 00| = |0\rangle\langle 0| \otimes |0\rangle\langle 0| \quad (41)$$

$$\sigma_A = \text{Tr}_B |0\rangle\langle 0| \otimes |0\rangle\langle 0| = |0\rangle\langle 0| \quad (42)$$

(例 2)

$$\sigma_{AB} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11| \quad (43)$$

$$\sigma_A = \frac{1}{2} \quad (44)$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (45)$$

$$\rho_{AB} = |\psi\rangle\langle\psi| \quad (46)$$

$$\rho_A = \frac{1}{2} \quad (47)$$

$\sigma_A = \rho_A$ となり、違う状態なのにもかかわらず、区別がつかない。

シュミットの分解定理 (スライド)

3 小川 朋宏 (電通大) 2/26 講義

3.1 イントロ

量子操作 quantum operation

通信路 channel

3.2 例

$\mathbb{C}^2$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (48)$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (49)$$

1. bit flip

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (50)$$

$$X|0\rangle = |1\rangle \quad (51)$$

$$X|1\rangle = |0\rangle \quad (52)$$

2. phase flip

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (53)$$

$$Z|0\rangle = |0\rangle \quad (54)$$

$$Z|1\rangle = -|1\rangle \quad (55)$$

3. Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (56)$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (57)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (58)$$

4. prob. 1/2 X operation: $X|\psi\rangle$, prob. 1/2 Z operation: $Z|\psi\rangle$

密度行列 (Density operator) $|\psi\rangle\langle\psi|$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (59)$$

純粋状態 (pure state)

出力は (notation: $X^\dagger \quad X^*$)

$$\frac{1}{2}X|\psi\rangle\langle\psi|X^* + \frac{1}{2}Z|\psi\rangle\langle\psi|Z^* \quad (60)$$

一方で

$$A = \frac{1}{\sqrt{2}}(X + Z) = H, B = \frac{1}{\sqrt{2}}(X - Z) \quad (61)$$

prob. 1/2 A operation, prob. 1/2 B operation をしたとすると、

$$\frac{1}{2}A|\psi\rangle\langle\psi|A^* + \frac{1}{2}B|\psi\rangle\langle\psi|B^* = \frac{1}{2}X|\psi\rangle\langle\psi|X^* + \frac{1}{2}Z|\psi\rangle\langle\psi|Z^* \quad (62)$$

3.3 量子通信路

記号の整理

$H_1, H_A, H_B, H_2,$

$H \simeq \mathbb{C}^d$

$L(H)$: $\dim H$ 正方行列全体

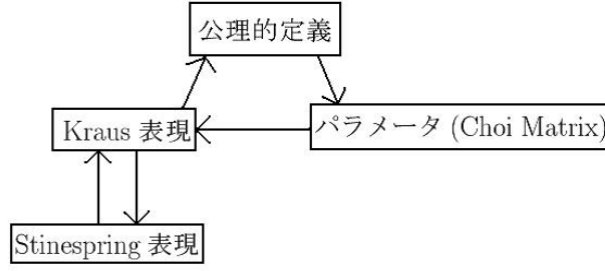
$S(H)$: 密度行列全体

量子通信路の公理的定義

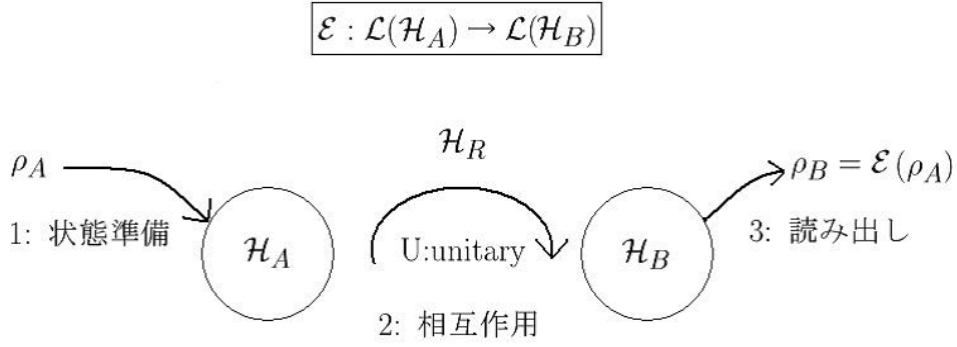
Definition 2 (quantum operation). $\mathcal{E}: L(H_A) \longrightarrow L(H_B)$ is called a quantum operation if

1. 線形性

ロードマップ



Stinespring 表現のイメージ



2. 完全正値性 (Completely Positive)

$$\begin{array}{ccc} \mathcal{H}_A & \xrightarrow{\mathcal{E}} & \mathcal{H}_B \\ \rho_A & \mapsto & \mathcal{E}(\rho_A) \end{array} \quad (63)$$

$\mathcal{H}_R \otimes \mathcal{H}_A$ を写す map も quantum operation であって欲しい。

$$\begin{aligned} \forall \mathcal{H}_R, \forall X_{RA} \in L(\mathcal{H}_R \otimes \mathcal{H}_A) \quad X_{RA} \geq 0 \quad (I \otimes \mathcal{E})(X_{RA}) \\ (\mathcal{E}_1 \otimes \mathcal{E}_2)(X_R \otimes X_A) := \mathcal{E}_1(X_R) \otimes \mathcal{E}_2(X_A) \end{aligned} \quad (64)$$

の線形結合から与えられる。

3. Trace Preserving

3.4 Kraus 表現

Definition 3. $\mathcal{E} : L(\mathcal{H}_A) \longrightarrow L(\mathcal{H}_B)$ は

$$(\mathcal{E})(\mathcal{X}) = \sum_k E_k \mathcal{X} E_k^* \quad (65)$$

$$E_k : \mathcal{H}_A \rightarrow \mathcal{H}_B \quad \sum_k E_k^* E_k = I$$

Lemma 1. Kraus 表現 Quantum Operation

Proof. 1. 線形性 OK

3.

$$\mathrm{Tr} \mathcal{E}(X) = \mathrm{Tr} \left(\sum_k E_k X E_k^* \right) = \sum_k \mathrm{Tr} E_k^* E_k X = \mathrm{Tr} X \quad (66)$$

2. $(I \otimes \mathcal{E})(X_{RA}) = \sum_k (I \otimes E_k) X_{RA} (I \otimes E_k)^*$ を示せばよい。これは $X_{RA} = X_R \otimes X_A$ のときを示せば、線形性より十分である。

$$(I \otimes \mathcal{E})(X_R \otimes X_A) = X_R \otimes \mathcal{E}(X_A) \quad (67)$$

□

3.5 パラメータ表現

Definition 4. $QO = \{ \mathcal{E} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B) \text{ is a quantum operation} \}$
 $d = \dim \mathcal{H}_A, \mathcal{H}_R \simeq \mathcal{H}_A$

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum |i\rangle_R \otimes |i\rangle_A \text{ where } \{|i\rangle\} : \text{CONS} \quad (68)$$

$$M(\mathcal{E}) := (I \otimes \mathcal{E})(|\Phi\rangle\langle\Phi|) : \text{Choi matrix} \in S(\mathcal{H}_R \otimes \mathcal{H}_A) \quad (69)$$

Definition 5 (Choi map).

$$\begin{aligned} \mathcal{E} &\rightarrow M(\mathcal{E}) \\ \in QO &\quad \in \mathcal{M} \end{aligned} \quad (70)$$

$$\mathcal{M} = \{ \rho_{RB} \in S(\mathcal{H}_R \otimes \mathcal{H}_B) \mid \mathrm{Tr}_B \rho_{RB} = \frac{I_R}{d} \} \quad (71)$$

Theorem 3. Choi map $QO \rightarrow \mathcal{M}$ is one-to-one and affine (linear).

for $0 \leq t \leq 1, \mathcal{E}, \mathcal{F} \in QO$

$$M(t\mathcal{E} + (1-t)\mathcal{F}) = tM(\mathcal{E}) + (1-t)M(\mathcal{F}) \quad (72)$$

$$(t\mathcal{E} + (1-t)\mathcal{F})(X) = t\mathcal{E}(X) + (1-t)\mathcal{F}(X) \quad (73)$$

4 林 正人 (東北大) 2/27 講義

測定に伴う状態変化 POVM $M = \{M_\omega\}_{\omega \in \Omega}$ ω が測定値、 Ω が測定値の集合
 状態 ρ に対して、

$$\mathrm{Pr}(\omega) = \mathrm{Tr}[M_\omega \rho] \quad (74)$$

という確率分布が定まる。

しかし、典型的な場合、

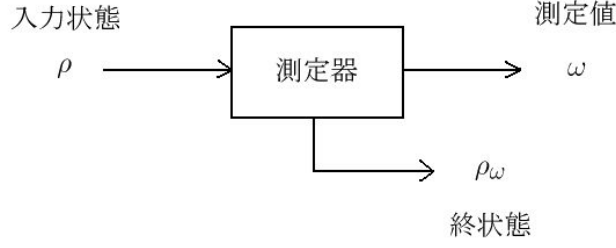
$$\rho_\omega = \frac{1}{\mathrm{Tr} M_\omega \rho} \sqrt{M_\omega} \rho \sqrt{M_\omega} \quad (75)$$

$\forall \omega \in \Omega$ が射影 (PVM) のとき、

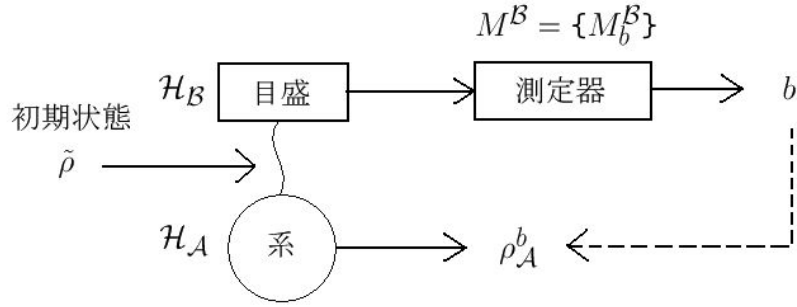
$$\rho_\omega = \frac{1}{\mathrm{Tr} M_\omega \rho} M_\omega \rho M_\omega \quad (76)$$

(射影仮説)

入力状態と終状態



測定器の中身



条件付き確率

$$\Pr^{\{A|B\}}(a|b) = \frac{\Pr^{A,B}(a,b)}{\Pr^B(b)} \quad (77)$$

$$\rho_b^A = \frac{1}{\text{Tr} \tilde{\rho}(I_A \otimes M_b^B)} \text{Tr}_B \tilde{\rho}(I_A \otimes M_b^B) = \rho_b'^A \quad (78)$$

と結論づけられる。なぜならば、 A で POVM $\{M_a^A\}$ で測るとする。

$$\begin{aligned} \Pr^{A,B}(a,b) &= \text{Tr} \tilde{\rho}(M_a^A \otimes M_b^B) = \text{Tr} \tilde{\rho}(I_A \otimes M_b^B)(M_a^A \otimes I_B) \\ &= \text{Tr}_A[\text{Tr}_B(\tilde{\rho}(I_A \otimes M_b^B))M_a^A] = (\text{Tr} \tilde{\rho}(I_A \otimes M_b^B))(\text{Tr} \rho_b'^A M_a^A) \end{aligned} \quad (79)$$

$$\text{Tr} \rho_b'^A M_a^A = \frac{\Pr^{A,B}(a,b)}{\Pr^B(b)} \quad (80)$$

となるので、

$$\rho_b^A = \rho_b'^A \quad (81)$$

測定器のモデルを一般的に拡張してみる。

Theorem 4 (Naimark-Ozawa の拡張定理の修正版). $\forall$ POVM $\{M_\omega\}_{\omega \in \Omega}$ on $\mathcal{H}$

$\exists$ CONS $\{u_\omega\}_{\omega \in \Omega}$ $H_0 = \langle u_\omega \rangle$

$\exists \rho_0$: pure state on $\mathcal{H}_0$

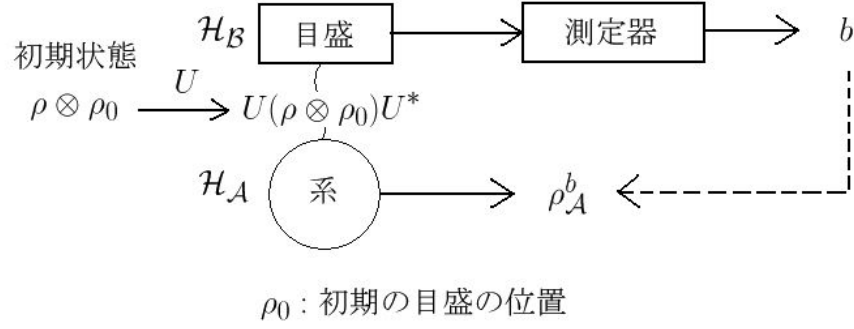
$\exists U$ on $\mathcal{H}_0 \otimes \mathcal{H}$

$\exists$ PVM $\{E_\omega\}_{\omega \in \Omega}$ on $\mathcal{H}_0$ s.t.

1.

$$\text{Tr} \rho M_\omega = \text{Tr}(I \otimes E_\omega)U(\rho \otimes \rho_0)U^* \quad (82)$$

間接測定モデル



2.

$$\sqrt{M_\omega} \rho \sqrt{M_\omega} = \text{Tr}_{\mathcal{H}_0}(I \otimes E_\omega) U(\rho \otimes \rho_0) U^* \quad (83)$$

平均化演算子

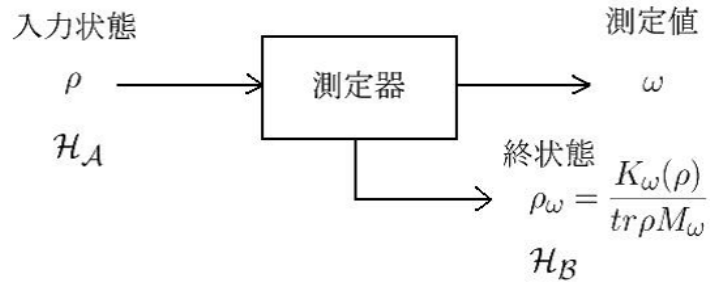
$$O(M) = \sum_{\omega} x_{\omega} M_{\omega} \quad (84)$$

$$\longrightarrow \text{Tr}_{H_0}[O(E \otimes I) U(I \otimes \rho_0) U^*] = O(M) \quad (85)$$

このとき、 $0 \leq \forall \lambda \leq 1$,

一般の測定器

測定値の出現確率は $\{M_\omega\}$ に従う



(ただし、 $K_\omega(\rho) \stackrel{\text{def}}{=} (\text{tr} \rho M_\omega) \rho_\omega$)

$$K_\omega(\lambda \rho_1 + (1 - \lambda) \rho_2) = \lambda K_\omega(\rho_1) + (1 - \lambda) K_\omega(\rho_2) \quad (86)$$

$$\begin{aligned} \Pr(\omega, b) &= \Pr(\omega) \Pr(b|\omega) = \text{Tr}_A \rho M_\omega \text{Tr}_B \frac{K_\omega(\rho)}{\text{Tr}_A \rho M_\omega} M_b^B \\ &= \text{Tr}_B K_\omega(\rho) M_b^B \Pr(\omega, b) = \text{Tr} K_\omega(\lambda \rho_1 + (1 - \lambda) \rho_2) M_b^B \end{aligned} \quad (87)$$

$K_\omega : L_H(\mathcal{H}_A) \longrightarrow L_H(\mathcal{H}_B)$: Hermite 演算子の全体

1. $\forall \xi \geq 0 \quad K_\omega(\xi) \geq 0$ (K_ω の正値性)

2. $\forall \tilde{\xi} \geq 0$ on $\mathcal{H} \otimes \mathbb{C}^n (\forall n)$ $(K_\omega \otimes I)(\tilde{\xi}) \geq 0$ (K_ω の完全正値性)

ゆえに K_ω は完全正値写像となる。

(a) K_ω は完全正値写像

(b) $\forall \rho, \text{Tr} \sum_\omega K_\omega(\rho) = 1$ (なぜなら、 $\sum_\omega \text{Tr} K_\omega(\rho) = \sum_\omega \text{Tr} \rho M_\omega = 1$)

Theorem 5. $\forall \{K_\omega\}_{\omega \in \Omega}$ ($POVM \{M_\omega\}$ に対応) $\exists TP\text{-}CP \text{ map } K'_\omega \text{ s.t. } K_\omega(\rho) = K'_\omega(\sqrt{M_\omega} \rho \sqrt{M_\omega})$

Theorem 6. $\{K_\omega\}$ について以下は同値

1. $\{K_\omega\}$ は (a)(b) を満たす。

2. $\exists$ 間接測定モデル (U, H_0, ρ_0, E) s.t.

$$K_\omega(\rho) = \text{Tr}_{H_0}(I \otimes E_\omega)U(\rho \otimes \rho_0)U^* \quad (88)$$

不確定性

1. 物理量 X についての不確定性

$$\Delta_1^2(X, \rho) := \text{Tr}(\rho X^2) - (\text{Tr} \rho X)^2 = \text{Tr} \rho (X - (\text{Tr} \rho X)I)^2 \quad (89)$$

2. 測定 M を行ったときのデータの不確定性

$$\Delta_2^2(M, \rho) := \sum (x_i - E_\rho(M))^2 \text{Tr} \rho M_i \text{ where } M = (M_i, x_i)_i, E_\rho(M) = \sum x_i \text{Tr} \rho M_i \quad (90)$$

3. 物理量 X と測定 M とのズレを表す。

$$\Delta_3^2(M, X, \rho) := \sum_i \text{Tr}(x_i I - X)M_i(x_i I - X)\rho \quad (91)$$

$$\Delta_2^2(M, \rho) = \Delta_3^2(M, O(M), \rho) + \Delta_1^2(O(M), \rho) \quad (92)$$

M の間接測定モデル

$$\Delta_3^2(M, X, \rho) = \Delta_1^2(U^*(I \otimes O(E))U - X \otimes I, \rho \otimes \rho_0)(H_0, U, \rho_0, E), \quad (93)$$

$$\Delta_3^2(M, X, \rho) = \Delta_3^2(M, O(M), \rho) + \Delta_1^2(O(M) - X, \rho) \quad (94)$$

4. 状態変化 $\mathcal{E}$ の後に測定 M を行ったとき、 X をどれだけ測定できるか？

$$\Delta_4((\mathcal{E}), X, \rho) = \min_M \Delta_3(\mathcal{E}^*(M), X, \rho) \text{ where } \mathcal{E}^*(M) = \mathcal{E}^*(M_i, x_i) \quad (95)$$

5 林 正人(東北大) 2/28 講義

不確定性

1. 物理量 X についての不確定性

$$\Delta_1^2(X, \rho) := \text{Tr}(\rho X^2) - (\text{Tr} \rho X)^2 = \text{Tr} \rho (X - (\text{Tr} \rho X)I)^2 \quad (96)$$

2. 測定 M を行ったときのデータの不確定性

$$\Delta_2^2(M, \rho) := \sum (x_i - E_\rho(M))^2 \text{Tr } \rho M_i \text{ where } M = (M_i, x_i)_i, E_\rho(M) = \sum x_i \text{Tr } \rho M_i \quad (97)$$

3.

$$\begin{aligned} \Delta_3^2(M, X, \rho) &:= \sum_i \text{Tr } M_i (x_i I - X) \rho (x_i I - X) \\ &= \sum_i \text{Tr} (I \otimes E_i) U (x_i I - X \otimes I) (\rho \otimes \rho_0) (x_i I - X \otimes I) U^* \\ &= \Delta_1^2(U^*(I \otimes O(E))U - X \otimes I, \rho \otimes \rho_0) \end{aligned} \quad (98)$$

M の間接測定モデル

$$\Delta_3^2(M, X, \rho) = \Delta_1^2(U^*(I \otimes O(E))U - X \otimes I, \rho \otimes \rho_0)(H_0, U, \rho_0, E), \quad (99)$$

$$\Delta_3^2(M, X, \rho) = \Delta_3^2(M, O(M), \rho) + \Delta_1^2(O(M) - X, \rho) \quad (100)$$

4.

$$\text{Tr } \mathcal{E}(X)Y = \text{Tr } X\mathcal{E}^*(Y) \text{ で } \mathcal{E}^* \quad (101)$$

(双対写像) を定義する。

状態変化 $\mathcal{E}$ の後に測定 M を行ったとき、X をどれだけ測定できるか？

$$\Delta_4((\mathcal{E}), X, \rho) = \min_M \Delta_3(\mathcal{E}^*(M), X, \rho) \text{ where } \mathcal{E}^*(M) = \{\mathcal{E}^*(M_i), x_i\} \quad (102)$$

$$\Delta_4^2(\{K_\omega\}, X, \rho) = \Delta_4^2(\bar{K}, X, \rho) \text{ where } \bar{K} := (K_\omega(X) \otimes |u_\omega\rangle\langle u_\omega|) \quad (103)$$

$\{u_\omega\}$: 正規直交基底

不確定性関係

1.

$$\Delta_1(X, \rho)\Delta_1(Y, \rho) \geq \frac{\text{Tr } |\sqrt{\rho}[X, Y]\sqrt{\rho}|}{2} \text{ where } A = \sum_i a_i P_i \quad (104)$$

のとき $|A| = \sum_i |a_i| P_i$ となる。

$\text{Tr } \rho X = \text{Tr } \rho Y = 0$ の場合を議論する。

$$0 \leq (X \pm iY)(X \pm iY)^* = (X \pm iY)(X \mp iY) = X^2 + Y^2 \mp i[X, Y] \quad (105)$$

なので、 $X^2 + Y^2 \geq \pm i[X, Y]$

$$\sqrt{\rho}(X^2 + Y^2)\sqrt{\rho} \geq \pm i\sqrt{\rho}[X, Y]\sqrt{\rho} \quad (106)$$

$$\sqrt{\rho}[X, Y]\sqrt{\rho} = \sum_j a_j |j\rangle\langle j| \quad (107)$$

$$\langle j|\sqrt{\rho}(X^2 + Y^2)\sqrt{\rho}|j\rangle \geq |\langle j|\sqrt{j}[X, Y]\sqrt{\rho}|j\rangle| \quad (108)$$

$$\sum_j \langle j|\sqrt{\rho}(X^2 + Y^2)\sqrt{\rho}|j\rangle \geq |\sum_j \langle j|\sqrt{j}[X, Y]\sqrt{\rho}|j\rangle| \quad (109)$$

$$\text{Tr } \rho(X^2 + Y^2) \geq \text{Tr } |\sqrt{\rho}[X, Y]\sqrt{\rho}| \quad (110)$$

$$\Delta_1^2(X, \rho) + \Delta_1^2(Y, \rho) \geq \text{Tr } |\sqrt{\rho}[X, Y]\sqrt{\rho}| \quad (111)$$

X に tX を代入して任意の t で以下の式が成り立たなければならない。

$$\Delta_1^2(X, \rho)t^2 - t \operatorname{Tr} |\sqrt{\rho}[X, Y]\sqrt{\rho}| + \Delta_1^2(Y, \rho) \geq 0 \quad (112)$$

(判別式) ≤ 0

$$\Delta_1(X, \rho) \cdot \Delta_1(Y, \rho) \geq \frac{\operatorname{Tr} |\sqrt{\rho}[X, Y]\sqrt{\rho}|}{2} \quad (113)$$

2.

$$\Delta_3(M, O(M), \rho) \cdot \Delta_4(K_\omega, Y, \rho) \geq \frac{\operatorname{Tr} |\sqrt{\rho}[O(M), Y]\sqrt{\rho}|}{2} \text{ where } \{K_\omega\} \quad (114)$$

は $M = \{M_\omega\}$ に対応している。

3. POVM

$$\{(M_i, x'_i, x_2^2)\}_i O'(M) = \sum M_i x'_i, O^2(M) = \sum M_i x_i^2 \quad (115)$$

$$\Delta_3(M, O'(M), \rho) \cdot \Delta_3(M, O^2(M), \rho) \geq \frac{\operatorname{Tr} |\sqrt{\rho}[O'(M), O^2(M)]\sqrt{\rho}|}{2} \quad (116)$$

6 石坂 智 (NEC) 2/28 講演

$$|\psi\rangle_{AB} = \sqrt{p_0}|00\rangle + \sqrt{p_1}|11\rangle + \dots \quad (117)$$

6.1 局所操作と古典通信 (LOCC)

(スライド)

LOCC はエンタングルメントを生成できない。

6.2 エンタングルメントの定量化

$$|\phi^+\rangle = \frac{|0\rangle_A|0\rangle_B + |0\rangle_A|0\rangle_B}{2} \quad (118)$$

基本単位 (ebit) entangled bit (EPR 状態、Bell 状態)

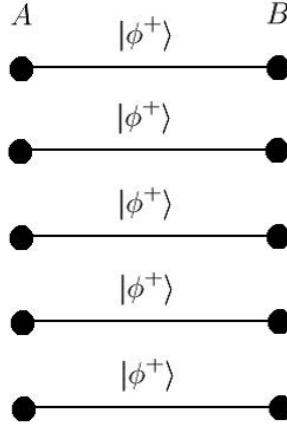
$$n \text{ ebit} = |\phi^+\rangle \otimes |\phi^+\rangle \otimes \dots \otimes |\phi^+\rangle := |\phi^+\rangle^{\otimes n} = \left(\frac{|0\rangle_A|0\rangle_B + |0\rangle_A|0\rangle_B}{2} \right)^{\otimes n} \quad (119)$$

$$= \frac{1}{\sqrt{2^n}} (|00 \dots 0\rangle_A |00 \dots 0\rangle_B + |11 \dots 1\rangle_A |11 \dots 1\rangle_B) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle_A |i\rangle_B \quad (120)$$

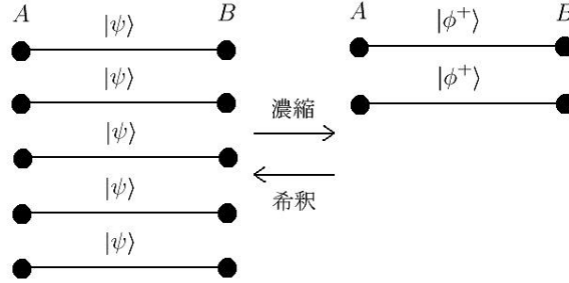
$$= \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle |i\rangle \quad (121)$$

$\log d$: d 項の直交状態の重ね合わせ $= \log d$ ebit

n ebit



エンタングルメントの濃縮



6.3 エンタングルメントの濃縮

$$|\psi\rangle = \sqrt{p}|00\rangle + \sqrt{1-p}|11\rangle \quad (122)$$

$$\begin{aligned} |\psi\rangle^{\otimes 2} &= (\sqrt{p}|00\rangle + \sqrt{1-p}|11\rangle) \otimes (\sqrt{p}|00\rangle + \sqrt{1-p}|11\rangle) \\ &= \sqrt{p^2}|00\rangle_A|00\rangle_B + \sqrt{(1-p)^2}|11\rangle_A|11\rangle_B + \sqrt{2p(1-p)} \left(\frac{|01\rangle_A|01\rangle_B + |10\rangle_A|10\rangle_B}{\sqrt{2}} \right) \end{aligned} \quad (123)$$

Alice は 2 つの量子ビットに対して、”I” の数 (k) を決める。

$$P_{k=0} := |00\rangle\langle 00|, P_{k=1} := |01\rangle\langle 01| + |10\rangle\langle 10|, P_{k=2} := |11\rangle\langle 11| \quad (124)$$

の projective measurement をすればよい。

$k = 1$ (確率 $2p(1-p)$) $\rightarrow$ 1 ebit (k を教えるのを LOCC で行う。)

$$|\psi\rangle^{\otimes n} = \sum_k \sqrt{{}_nC_k p^k (1-p)^{n-k}} \left(\frac{|0 \cdots 1 \cdots\rangle |0 \cdots 1 \cdots\rangle + \cdots}{\sqrt{{}_nC_k}} \right) \quad (125)$$

k が出たときには、 $\log({}_nC_k)$ ebit

$$\begin{aligned} n \text{ ebit} &= \sum_k {}_nC_k p^k (1-p)^{n-k} \log {}_nC_k \quad (n \gg 1) \\ &\simeq \log {}_nC_{n(1-p)} \simeq n(p \log p - (1-p) \log(1-p)) = nS(p) \end{aligned} \quad (126)$$

where $S(p)$ は binary entropy

6.4 量子データ圧縮

$$|\xi\rangle^{\otimes n} = (\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle)^{\otimes n} \quad (127)$$

n bit string $\longrightarrow m$ bit string にデータ圧縮 ($nS(p)$)

典型系列	"1" の数が $n(1-p)$ の状態	$ 00 \cdots 11 \cdots\rangle$	$\rightarrow 0000000000\rangle$
	$nC_{n(1-p)}$ 項	$\cdots$	$\rightarrow 0000001111\rangle \rightarrow 2^m = {}_n C_{n(1-p)} \rightarrow m = nS(p)$
それ以外	出現しないと近似		

6.5 エンタングルメントの希釈

(スライド)

$$|\phi^+\rangle^{\otimes nS(p)} \xrightarrow[\text{希釈}]{\text{LOCC}} |\psi\rangle^{\otimes n} \xrightarrow[\text{濃縮}]{\text{LOCC}} |\phi^+\rangle^{\otimes nS(p)} \quad (128)$$

つまり、LOCC は可逆 = エンタングルメント損失ゼロ

$$|\psi\rangle = \sqrt{p}|00\rangle + \sqrt{1-p}|11\rangle \quad (129)$$

つまり、 $|\psi\rangle^{\otimes n}$ — $S(p)$ ebit 持っている。

$$S(p) \text{ ebit} = -p \log p - (1-p) \log(1-p) \quad (130)$$

6.6 混合状態のエンタングルメント

$$\sigma = \frac{1}{2}|\phi^+\rangle\langle\phi^+| + \frac{1}{2}|\phi^-\rangle\langle\phi^-| \text{ where } |\phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \quad (131)$$

$$\sigma = \frac{1}{2} \left[\frac{|00\rangle + |11\rangle}{\sqrt{2}} \frac{\langle 00| + \langle 11|}{\sqrt{2}} + \frac{|00\rangle - |11\rangle}{\sqrt{2}} \frac{\langle 00| - \langle 11|}{\sqrt{2}} \right] = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|00\rangle\langle 00| \quad (132)$$

Definition 6. σ が積状態の混合で書けない σ はエンタングルしている

1. $\sigma = \sigma'_A \otimes \sigma''_B$: 無相関状態 (uncorrelated state) (含 純粋状態)
2. $\sigma = \sum_i p_i \sigma_A^{(i)} \otimes \sigma_B^{(2)}$
3. エンタングル状態

正写像

$$\Lambda : \sigma_A \longrightarrow \sigma'_A \geq 0 \quad (133)$$

完全正写像 (物理的な操作)

$$(I_A \otimes \Lambda_B) \sigma_{AB} \geq \sigma_{AB} \geq 0 \quad (134)$$

σ がエンタングルしていない。 $\sigma = \sum_i p_i \sigma_A^{(i)} \otimes \sigma_B^{(ii)}$

$$(I \otimes \Lambda_B)(\sigma_{AB}) = \sum_i p_i \sigma_A^{(i)} \otimes \Lambda(\sigma_B^{(ii)}) \geq 0 \quad (135)$$

この対偶を考える。 Λ は正写像があって、 $(I \otimes \Lambda_B)(\sigma_{AB}) \not\geq 0$ σ_{AB} はエンタングルしている。

6.7 混合状態のエンタングルメント判定

6.7.1 ペレス判定法

Λ を転置: 正写像 ($\Lambda(\sigma_A) \geq \sigma_A^T \geq 0$)

$$(I \otimes \Lambda)\sigma_{AB} = \sigma_{AB}^{T_B} = \sum a_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l| \not\geq 0 \quad (136)$$

σ はエンタングルしている。

$$\sigma_{AB} = \sum a_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l| \quad (137)$$

(例)

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (138)$$

$$\sigma_{AB} = |\phi^+\rangle\langle\phi^+| = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2} \quad (139)$$

$$\sigma_{AB}^{T_B} = \frac{|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|}{2} = \text{固有値 } \left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right\} \quad (140)$$

6.7.2 縮約判定法

$$\Lambda(X) = (\text{Tr } X)I - X \quad (141)$$

$$\Lambda(\sigma_A) = I - \sigma_A \geq 0 \quad (142)$$

$$(I \otimes \sigma_A)\sigma_{AB} = \text{Tr}_B \sigma_{AB} \otimes I_B - \sigma_{AB} = \sigma_A \otimes I_B - \sigma_{AB} \not\geq 0 \quad (143)$$

σ_{AB} はエンタングル

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (144)$$

$$\sigma_{AB} = |\phi^+\rangle\langle\phi^+| \quad (145)$$

$$\sigma_A = \frac{I}{2} \quad (146)$$

$$\frac{I_A \otimes I_B}{2} - |\phi^+\rangle\langle\phi^+| = \text{固有値 } \left\{-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right\} \not\geq 0 \quad (147)$$

2つの量子ビット ($\mathbb{C}^2 \otimes \mathbb{C}^2$) と $\mathbb{C}^2 \otimes \mathbb{C}^N$ をペレス判定法が縮約 $\mathbb{C}^2 \otimes \mathbb{C}^2$ と $\mathbb{C}^2 \otimes \mathbb{C}^3$ と $\mathbb{C}^2 \otimes \mathbb{C}^4$ の時は逆も成立 ($\sigma_{AB}^{T_B} \geq 0$ σ_{AB} はエンタングルメントしていない。)

6.8 混合状態と LOCC

(スライド)

ペレス判定法と蒸留 [Horodecki] の証明の outline

LOCC

$$\sigma_{AB} = (a_i \otimes I) \sigma_{AB} (a_i^\dagger \otimes I) \rightarrow \sigma''_{AB} = (I \otimes b_j(i)) \sigma'_{AB} (I \otimes b_j^*(i)) = (a_i \otimes b_j(i)) \sigma_{AB} (a_i^* \otimes b_j^*(i)) \quad (148)$$

$$\sigma'_{AB} = \sum_i (a_i \otimes b_i) \sigma_{AB} (a_i^* \otimes b_i^*) \quad (149)$$

$$\sigma_{AB}^{T_B} \geq 0 \quad (150)$$

$$\text{LOCC } \sigma_{AB} = \sum_i (a_i \otimes b_i) \sigma_{AB} (a_i^* \otimes b_i^*) = \sigma'_{AB} \quad (151)$$

$$\sigma_{AB}'^{T_B} = \sum_i (a_i \otimes \bar{b}_i) \sigma_{AB}^{T_B} (a_i^* \otimes b_i^T) \geq 0 \quad (152)$$

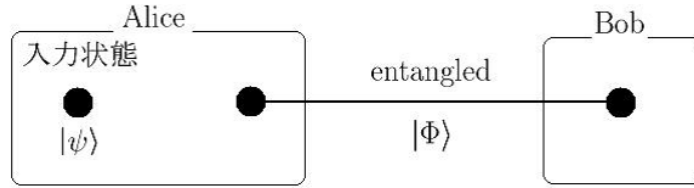
$$|\psi\rangle^{T_B} \geq 0 \quad (153)$$

$|\psi\rangle$ はエンタングルメントしていない。

7 小川 朋宏 (電通大) 2/28 講演

量子テレポーテーション ベル基底

量子テレポーテーション



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (|\alpha|^2 + |\beta|^2 = 1)$$

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad (154)$$

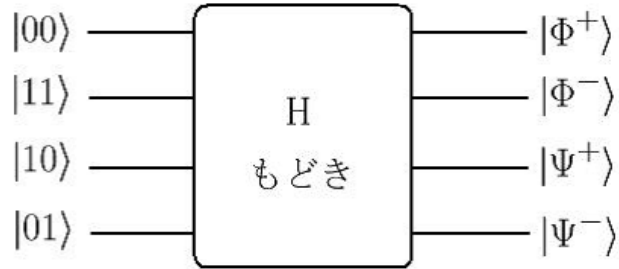
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad (155)$$

$$\begin{aligned} |\psi\rangle \otimes |\Phi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{2} |\Phi^+\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |\Phi^-\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |\Psi^+\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + |\Psi^-\rangle \otimes (\alpha|1\rangle - \beta|0\rangle) \end{aligned} \quad (156)$$

手順

1. Alice は入力系と自分の系の合成系に対して、Bell 基底で測定
2. 測定結果を Bob へ

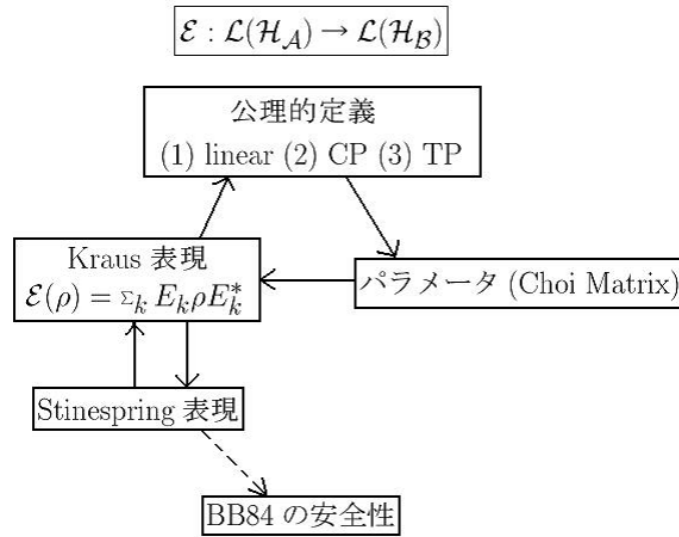
ベル基底の構成



3. Bob

- (a) $|\Phi^+\rangle \rightarrow \text{そのまま}$
- (b) $|\Phi^-\rangle \rightarrow Z$
- (c) $|\Psi^+\rangle \rightarrow X$
- (d) $|\Psi^-\rangle \rightarrow ZX$

Review



パラメータ表現 $\mathcal{H}_R \simeq \mathcal{H}_A, \dim \mathcal{H}_A = d, |\Phi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle$ Choi map (Choi isomorphism):

$$\begin{aligned} \mathcal{E} &\longrightarrow M(\mathcal{E}) = (I \otimes \mathcal{E})(\Phi) \\ &\in \text{量子通信路全体} \in \mathcal{M} = \left\{ \rho_{RB} \in S(H_R \otimes H_B), \text{Tr}_B \rho_{RB} = \frac{I_R}{d} \right\} \end{aligned} \quad (157)$$

Theorem 7. Choi map は one to one、 affine

Lemma 2. Choi map は単射、 affine

Proof.

$$M(\mathcal{E})(I \otimes \mathcal{E})(|\Phi\rangle\langle\Phi|) = \sum |i\rangle\langle j| \otimes |i\rangle\langle j| = \frac{1}{d} \sum |i\rangle\langle j| \otimes \mathcal{E}(|i\rangle\langle j|) = (\mathcal{E}(|i\rangle\langle j|)) \quad (158)$$

affine 性も明らか。 $\square$

Lemma 3. *Choi map は全射*

Proof. $M \in \mathcal{M} \quad \exists \mathcal{E}: \text{linear, CPTP } M(\mathcal{E}) = M$ を示す。

$$M = \sum |i\rangle\langle j| \otimes M_{ij} \quad (159)$$

$$\mathcal{E}_M(|i\rangle\langle j|) = M_{ij} \quad (160)$$

作り方により、 $M(\mathcal{E}) = M$ は自明。以下で、CP 性を示す。← Kraus 表現を持つことを示す。

Claim 1. $(\mathcal{E} : \mathcal{H}_A \rightarrow \mathcal{H}_B) \longrightarrow (I_R \otimes \mathcal{E})|\Phi\rangle$ は *one to one, linear*

$M = \sum_k |\Phi_k\rangle\langle\Phi_k|$ と分解。すると、 $\exists E_k (k = 1, 2, 3, \dots)$ s.t. $|\Phi_k\rangle = (I_R \otimes E_k)|\Phi\rangle \longrightarrow$

$$M = \sum_k (I_R \otimes E_k)|\Phi\rangle\langle\Phi|(I_R \otimes E_k^*) = \sum |i\rangle\langle j| \otimes (\sum E_k |i\rangle\langle j| E_k^*) \quad (161)$$

$\text{Tr}_B M = \frac{I_R}{d}$ より TP を示せる。

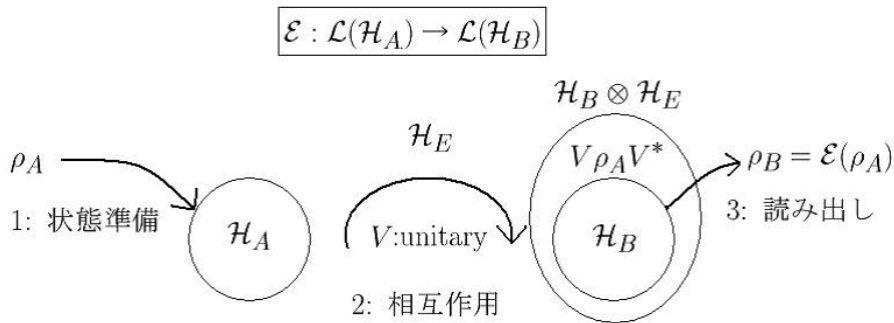
7.1 Kraus Steinspring

Steinspring 表現

Definition 7. $V : \mathcal{H}_A \rightarrow \mathcal{H}_B$ isometry (等長) $\forall |x\rangle\forall |y\rangle \langle x||y\rangle = \langle Vx|Vy\rangle = \langle x|V^*Vy\rangle$
 $\langle x|(V^*V - I)y\rangle = 0$

Definition 8. $\mathcal{E} = \text{Tr}_E V X V^*$ with some $\mathcal{H}_E$, $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$ isometry を Steinspring 表現と呼ぶ。

Steinspring 表現のイメージ



Remark 1. V は $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ 上のユニタリ行列に拡張できる。

Lemma 4. *Kraus Steinspring*

Proof. given $(\mathcal{X}) = \sum_k E_k X E_k^*$, $E_k : \mathcal{H}_A \rightarrow \mathcal{H}_B$ with $\sum_k E_k^* E_k = I_A$ $\mathcal{H}_E = \mathbb{C}^n$

$V: |\psi\rangle \in \mathcal{H}_A \rightarrow \sum E_k |psi\rangle \otimes |k\rangle$ where $|k\rangle \mathcal{H}_E$ 上での CONS

このとき、 $|\psi\rangle, |\phi\rangle \in \mathcal{H}_A$ に対して

$$\begin{aligned} \langle V\psi | V\phi \rangle &= \sum (\langle E_k \psi | \otimes \langle k |) (E_l |\phi\rangle \otimes |l\rangle) = \sum \langle E_k \psi | E_l \phi \rangle \langle k | l \rangle \\ &= \sum \langle E_k \psi | E_k \phi \rangle = \langle \psi | \sum_k E_k^* E_k \phi \rangle = \langle \psi | \phi \rangle \end{aligned} \quad (162)$$

$$\text{Tr}_E V |i\rangle \langle j| V^* = \text{Tr}_E \sum_k \sum_l (E_k |i\rangle \otimes |k\rangle) (\langle j| E_l^* \otimes \langle l|) \quad (163)$$

$$\text{Tr}_E \sum E_k |i\rangle \langle j| E_l \otimes |k\rangle \langle k| j\rangle = \sum E_k |j\rangle \langle j| E_k^* \quad (164)$$

□

Lemma 5. *Steinsprings Kraus*

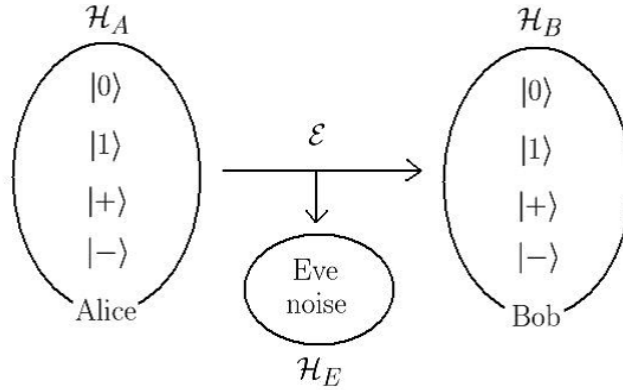
(証明はプリント参照)

7.2 量子暗号

(スライド)

7.3 量子暗号の安全性

量子暗号のモデル



仮定：

1. 送信状態と受信状態が一致 (厳密に)

2. Eve の盗聴は毎回同じ

(1) より

$$\mathcal{E}(|0\rangle\langle 0|) = |0\rangle\langle 0| \quad (165)$$

$$\mathcal{E}(|1\rangle\langle 0|) = |1\rangle\langle 0| \quad (166)$$

$$\mathcal{E}(|0\rangle\langle 1|) = |0\rangle\langle 1| \quad (167)$$

$$\mathcal{E}(|1\rangle\langle 1|) = |1\rangle\langle 1| \quad (168)$$

となる。

noise と Eve を環境系とみる。

Steinespring 表現

$$\mathcal{E}(\rho_A) = \text{Tr}_E V \rho_A V^* \quad (169)$$

$$V: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$$

$$\mathcal{H}_A \simeq \mathcal{H}_B \simeq \mathbb{C}^2$$

Lemma 6 (No cloning). $|\psi\rangle, |\phi\rangle \in \mathcal{H}_A$ $\langle\psi|\phi\rangle \neq 0$ とする。このとき、

$$\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \quad (170)$$

$$\mathcal{E}(|\phi\rangle\langle\phi|) = |\phi\rangle\langle\phi| \quad (171)$$

とすると、

$$V|\psi\rangle = |\psi\rangle \otimes |\xi\rangle \quad (172)$$

$$V|\phi\rangle = |\phi\rangle \otimes |\xi\rangle \quad (173)$$

Proof. 仮定より

$$V|\psi\rangle = |\psi\rangle \otimes |\xi_\psi\rangle \quad (174)$$

$$V|\phi\rangle = |\phi\rangle \otimes |\xi_\phi\rangle \quad (175)$$

と書ける。(なぜなら、Schmidt 分解)

上記の二式の内積をとると

$$\langle\psi|\psi\rangle = \langle V\psi|V\phi\rangle = \langle\psi|\psi\rangle\langle\xi_\psi|\xi_\phi\rangle \quad (176)$$

つまり、 $\langle\xi_\psi|\xi_\phi\rangle = 1$ でなくてはならない。

□

よって、BB84 では、 $\exists|\xi\rangle$

$$V|0\rangle = |0\rangle \otimes |\xi\rangle \quad (177)$$

$$V|1\rangle = |1\rangle \otimes |\xi\rangle \quad (178)$$

$$V|+\rangle = |+\rangle \otimes |\xi\rangle \quad (179)$$

$$V|-\rangle = |-\rangle \otimes |\xi\rangle \quad (180)$$