量子情報基礎

竹内勇貴

NTT コミュニケーション科学基礎研究所

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

「量子情報基礎」→「量子計算基礎」

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

「量子情報基礎」→「量子計算基礎」→「量子計算の古典検証」

「格子暗号」

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

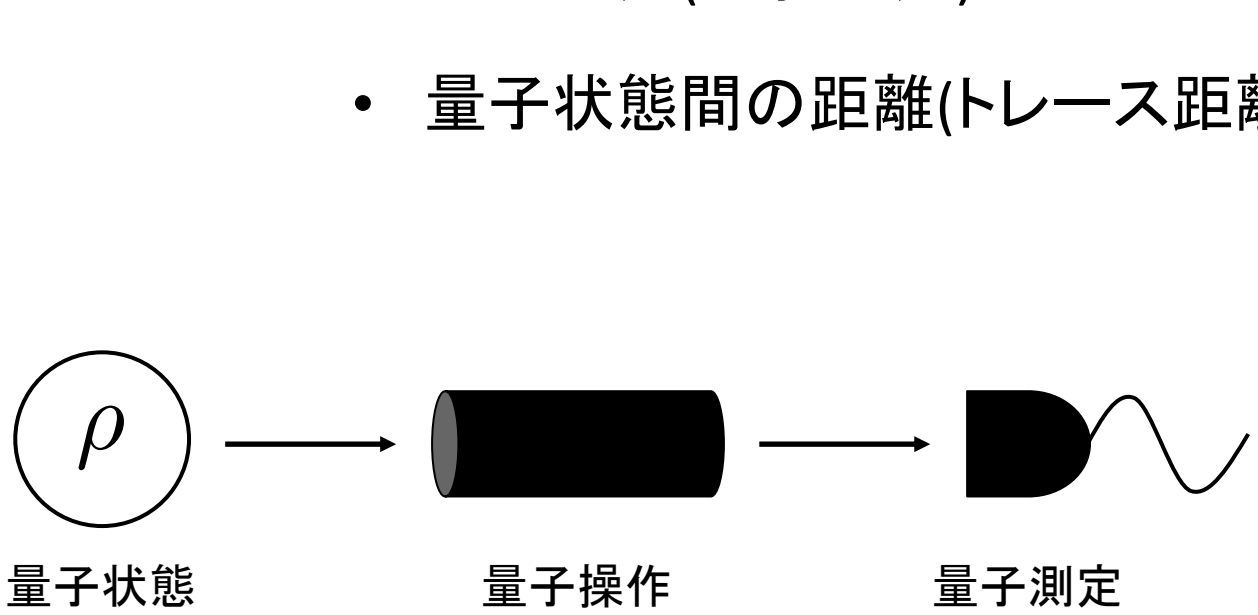
「量子情報基礎」→「量子計算基礎」→「量子計算の古典検証」→山川さんのトーク

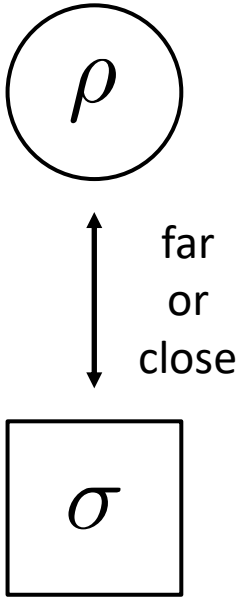
「格子暗号」

本講演の目的

量子情報処理の前提知識を理解すること!!

- 量子状態(純粋状態、混合状態)
- 量子操作(ユニタリ操作、Kraus表現)
- 量子測定(射影測定)
- 量子状態間の距離(トレース距離)





量子情報処理の目的

量子力学の原理(重ね合わせ、エンタングルメントなど)を用いて、(従来の)古典情報処理を超える情報処理を達成すること

量子情報処理の目的

量子力学の原理(重ね合わせ、エンタングルメントなど)を用いて、(従来の)古典情報処理を超える情報処理を達成すること

例えば、

量子計算

- 古典計算機では既知の最良のアルゴリズムでも超多項式時間かかる問題(の一部)を、多項式時間で解く
- クエリ計算量、通信計算量における指数関数的な差の証明

量子情報処理の目的

量子力学の原理(重ね合わせ、エンタングルメントなど)を用いて、(従来の)古典情報処理を超える情報処理を達成すること

例えば、

量子計算

- 古典計算機では既知の最良のアルゴリズムでも超多項式時間かかる問題(の一部)を、多項式時間で解く
- クエリ計算量、通信計算量における指数関数的な差の証明

量子暗号

- ワンタイムパッド用の秘密鍵を情報理論的安全に共有する方法(量子鍵配送)
- 現代暗号では不可能な新しい暗号機能の付加

量子情報処理の目的

量子力学の原理(重ね合わせ、エンタングルメントなど)を用いて、(従来の)古典情報処理を超える情報処理を達成すること

例えば、

量子計算

- 古典計算機では既知の最良のアルゴリズムでも超多項式時間かかる問題(の一部)を、多項式時間で解く
- クエリ計算量、通信計算量における指数関数的な差の証明

量子暗号

- ワンタイムパッド用の秘密鍵を情報理論的安全に共有する方法(量子鍵配送)
- 現代暗号では不可能な新しい暗号機能の付加

量子計測

- 古典計測の精度(標準量子限界)を超える精度(ハイゼンベルグ限界)の達成

量子情報処理の目的

量子力学の原理(重ね合わせ、エンタングルメントなど)を用いて、(従来の)古典情報処理を超える情報処理を達成すること

例えば、

量子計算
- 古典計算機では既知の最良のアルゴリズムでも超多項式時間かかる問題(の一部)を、多項式時間で解く
- クエリ計算量、通信計算量における指数関数的な差の証明

量子暗号
- ワンタイムパッド用の秘密鍵を情報理論的安全に共有する方法(量子鍵配送)
- 現代暗号では不可能な新しい暗号機能の付加

量子計測
- 古典計測の精度(標準量子限界)を超える精度(ハイゼンベルグ限界)の達成

量子ゲーム理論
- ジレンマ(e.g., 囚人のジレンマ)の解消

量子状態

(従来の)古典情報処理

情報の最小単位はビット

0　　1

量子状態

(従来の)古典情報処理

情報の最小単位はビット

0 1

一般化

量子情報処理

情報の最小単位は量子ビット

重ね合わせ状態

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\alpha, \beta \in \mathbb{C} \quad \text{s.t.} \quad |\alpha|^2 + |\beta|^2 = 1$$

量子状態

(従来の)古典情報処理

情報の最小単位はビット

一般化

量子情報処理

情報の最小単位は量子ビット

0 1

$(\alpha, \beta) = (0, 1)$の特別ケース

$(\alpha, \beta) = (1, 0)$の特別ケース

重ね合わせ状態

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\alpha, \beta \in \mathbb{C} \quad \text{s.t.} \quad |\alpha|^2 + |\beta|^2 = 1$$

量子状態

量子ビットが2つある時

$$C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle = \begin{pmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{pmatrix}$$

$$\forall i, j \in \{0, 1\},\ |ij\rangle \equiv |i\rangle \otimes |j\rangle$$

$$\forall i, j \in \{0, 1\},\ C_{ij} \in \mathbb{C} \quad \text{s.t.} \quad \sum_{i,j \in \{0,1\}} |C_{ij}|^2 = 1$$

量子状態

(古典)ビットの場合

00

01

10

11

量子ビットが2つある時

$$C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle = \begin{pmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{pmatrix}$$

$$\forall i, j \in \{0, 1\},\ |ij\rangle \equiv |i\rangle \otimes |j\rangle$$

$$\forall i, j \in \{0, 1\},\ C_{ij} \in \mathbb{C} \quad \text{s.t.} \quad \sum_{i,j \in \{0,1\}} |C_{ij}|^2 = 1$$

量子状態

(古典)ビットの場合

00

01

10

11

量子ビットが2つある時

$$C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle = \begin{pmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{pmatrix}$$

古典と同じ？

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$$

$$\forall i, j \in \{0, 1\},\ |ij\rangle \equiv |i\rangle \otimes |j\rangle$$

$$\forall i, j \in \{0, 1\},\ C_{ij} \in \mathbb{C} \quad \text{s.t.} \quad \sum_{i,j \in \{0,1\}} |C_{ij}|^2 = 1$$

量子状態

(古典)ビットの場合

00

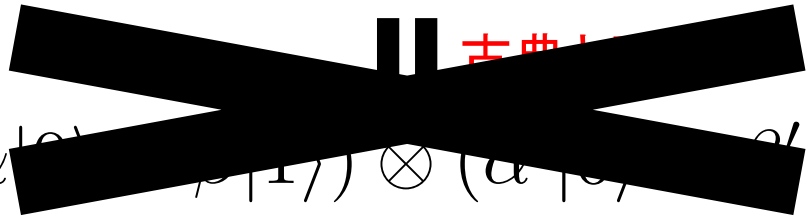
01

10

11

量子ビットが2つある時

$$C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle = \begin{pmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{pmatrix}$$



$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$$

$$\forall i, j \in \{0, 1\},\ |ij\rangle \equiv |i\rangle \otimes |j\rangle$$

$$\forall i, j \in \{0, 1\},\ C_{ij} \in \mathbb{C} \quad \text{s.t.} \quad \sum_{i,j \in \{0,1\}} |C_{ij}|^2 = 1$$

量子状態

エンタングル状態(Bell状態): 量子的に相関した状態

$C_{00} = C_{11} = \dfrac{1}{\sqrt{2}},\ C_{01} = C_{10} = 0$ の時、

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

量子状態

エンタングル状態(Bell状態): 量子的に相関した状態

$C_{00} = C_{11} = \dfrac{1}{\sqrt{2}},\ C_{01} = C_{10} = 0$ の時、

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$ の形に書くためには

$$\alpha\beta' = \beta\alpha' = 0 \quad \text{かつ} \quad \alpha\alpha' = \beta\beta' = \frac{1}{\sqrt{2}}$$

が要求されるが、この条件を満たす$(\alpha, \beta, \alpha', \beta')$は存在しない。

$\mathcal{H}$: ヒルベルト空間

量子状態

$n(\in \mathbb{N})$量子ビットの量子状態

$$|\psi\rangle = \sum_{z\in\{0,1\}^n} C_z|z\rangle \quad (\in \mathcal{H})$$

$$\forall z \in \{0,1\}^n,\ C_z \in \mathbb{C} \quad \text{s.t.} \quad \sum_{z\in\{0,1\}^n} |C_z|^2 = 1$$

◆ ポイント

n個の量子ビットで2^n次元の正規ベクトルを表現出来る。

量子状態

純粋状態と混合状態

ここまでは、確率*1*である状態

$$|\psi\rangle$$

になっている場合だけを考えていた。このような、状態を**純粋状態**と呼ぶ。

$\langle\psi| \equiv (|\psi\rangle)^\dagger$

量子状態

純粋状態と混合状態

ここまでは、確率*1*である状態

$$|\psi\rangle$$

になっている場合だけを考えていた。このような、状態を**純粋状態**と呼ぶ。

一般化

混合状態: どの状態になるかが確率的な場合の量子状態 $\sum_i p_i |\psi_i\rangle\langle\psi_i|$

p_i: 確率

$\langle\psi| \equiv (|\psi\rangle)^\dagger$

量子状態

純粋状態と混合状態

ここまでは、確率*1*である状態

$$|\psi\rangle$$

になっている場合だけを考えていた。このような、状態を**純粋状態**と呼ぶ。

一般化

混合状態: どの状態になるかが確率的な場合の量子状態

$$\sum_i p_i |\psi_i\rangle\langle\psi_i|$$

(p_i: 確率)

例1) 確率*1/2*で$|\psi\rangle$、確率*1/2*で$|\psi'\rangle$になっている場合

$$\frac{|\psi\rangle\langle\psi| + |\psi'\rangle\langle\psi'|}{2}$$

例2) コインフリップ

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

量子状態

密度行列(密度演算子)

一般の量子状態は**密度行列**ρとして書くことが出来、この行列は

- トレースの値が*1*
- 半正定値

を満たす。

量子状態

密度行列(密度演算子)

一般の量子状態は**密度行列**ρとして書くことが出来、この行列は

- トレースの値が*1*
- 半正定値

を満たす。

- 密度行列 = 混合状態の証明

量子状態

密度行列(密度演算子)

一般の量子状態は**密度行列**ρとして書くことが出来、この行列は

- トレースの値が*1*
- 半正定値

を満たす。

- 密度行列 = 混合状態の証明

1. 混合状態 ⇒ 密度行列

$$\mathrm{Tr}\left[\sum_i p_i|\psi_i\rangle\langle\psi_i|\right] = \sum_i p_i\langle\psi_i|\psi_i\rangle = 1$$

$$\forall|\phi\rangle,\ \langle\phi|\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)|\phi\rangle = \sum_i p_i\left|\langle\phi|\psi_i\rangle\right|^2 \geq 0$$

量子状態

密度行列(密度演算子)

一般の量子状態は**密度行列**ρとして書くことが出来、この行列は

- トレースの値が*1*
- 半正定値

を満たす。

- 密度行列 = 混合状態の証明

2. 密度行列 ⇒ 混合状態

半正定値という性質から、密度行列は正規行列であるため、対角化が可能

$$\rho \xrightarrow{\text{スペクトル分解}} \sum_i c_i |\psi_i\rangle\langle\psi_i| \quad (\forall i,\ c_i \geq 0)$$

さらに、トレースの値が1という性質より、$\{c_i\}_i$は確率になる。 $\sum_i c_i = 1$

量子状態

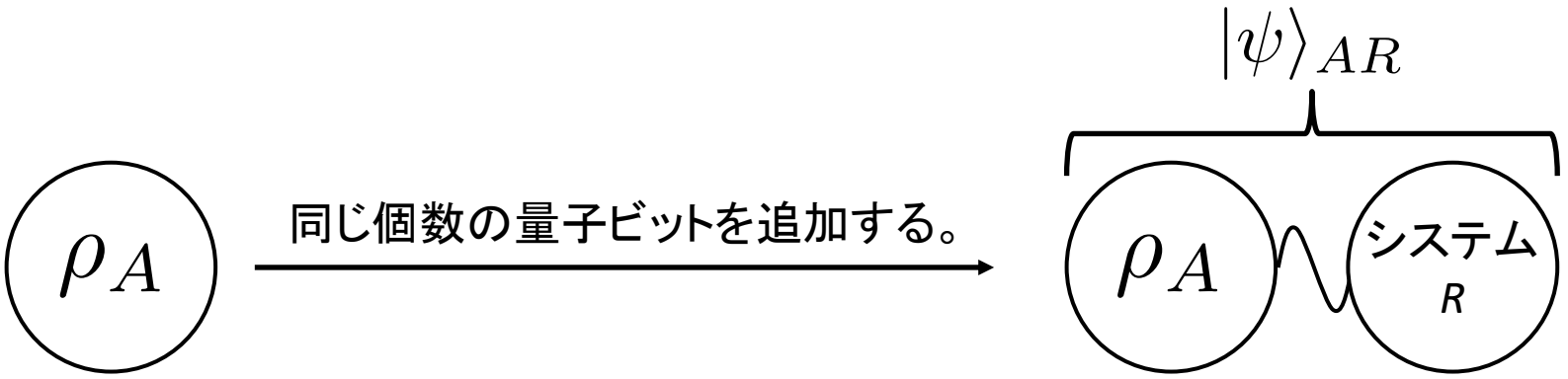
純粋化(purification): 混合状態を純粋状態に“変換”する手法

任意の密度行列$\rho_A (\in \mathcal{H}_A)$に対して、

$$\mathrm{Tr}_R \left[|\psi\rangle_{AR} \langle\psi|_{AR} \right] = \rho_A$$

を満たす純粋状態$|\psi\rangle_{AR} (\in \mathcal{H}_A \otimes \mathcal{H}_R)$が存在する。

※ $|\mathcal{H}_A| = |\mathcal{H}_R|$



量子状態

純粋化(purification): 混合状態を純粋状態に“変換”する手法

任意の密度行列$\rho_A (\in \mathcal{H}_A)$に対して、

$$\mathrm{Tr}_R \left[|\psi\rangle_{AR} \langle\psi|_{AR} \right] = \rho_A$$

を満たす純粋状態$|\psi\rangle_{AR} (\in \mathcal{H}_A \otimes \mathcal{H}_R)$が存在する。

- 証明

$\rho_A = \sum_i p_i |\psi_i\rangle_A \langle\psi_i|_A$(対角化)に対して、

$$|\psi_{AR}\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle_A |\psi_i\rangle_R$$

量子状態

純粋化(purification): 混合状態を純粋状態に“変換”する手法

任意の密度行列$\rho_A (\in \mathcal{H}_A)$に対して、

$$\mathrm{Tr}_R \left[|\psi\rangle_{AR} \langle\psi|_{AR} \right] = \rho_A$$

を満たす純粋状態$|\psi\rangle_{AR} (\in \mathcal{H}_A \otimes \mathcal{H}_R)$が存在する。

- 証明

$\rho_A = \sum_i p_i |\psi_i\rangle_A \langle\psi_i|_A$(対角化)に対して、

$$|\psi_{AR}\rangle \equiv \sum_i \sqrt{p_i} |\psi_i\rangle_A |\psi_i\rangle_R$$

◆ポイント

純粋状態に限定して議論しても、一般性を失わない。

量子操作

シュレディンガー方程式

量子情報処理は、量子力学の原理に基づいた情報処理
→可能な操作は量子力学のルールによって決まる。

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \quad \Rightarrow \quad |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

ハミルトニアン
(エルミート行列)

量子操作

シュレディンガー方程式

量子情報処理は、量子力学の原理に基づいた情報処理
→可能な操作は量子力学のルールによって決まる。

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \quad \Rightarrow \quad |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

ハミルトニアン
(エルミート行列)

量子操作は**ユニタリ行列**で書ける

量子操作

シュレディンガー方程式

量子情報処理は、量子力学の原理に基づいた情報処理
→可能な操作は量子力学のルールによって決まる。

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \quad \Rightarrow \quad |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

ハミルトニアン
(エルミート行列)

量子操作は**ユニタリ行列**で書ける

◆ポイント

※量子状態 = 純粋状態 = 正規ベクトル

量子状態にユニタリをかけても、量子状態の条件を満たす。

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

量子操作

よく使われる量子操作(量子ゲート)

- 単一量子ビットに対する操作

パウリ-*X*ゲート

$$X \equiv |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

パウリ-*Z*ゲート

$$Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

パウリ-*Y*ゲート

$$Y \equiv i|1\rangle\langle 0| - i|0\rangle\langle 1| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

アダマールゲート

$$H \equiv |+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

*S*ゲート

$$S \equiv \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

*T*ゲート

$$T \equiv \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

恒等(Identity)ゲート

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

量子操作

よく使われる量子操作(量子ゲート)

- 単一量子ビットに対する操作

パウリ-*X*ゲート

$$X \equiv |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

パウリ-*Z*ゲート

$$Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$H(\cdot)H^\dagger$

パウリ-*Y*ゲート

$$Y \equiv i|1\rangle\langle 0| - i|0\rangle\langle 1| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

アダマールゲート

$$H \equiv |+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

*S*ゲート

$$S \equiv \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

*T*ゲート

$$T \equiv \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

恒等(Identity)ゲート

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

量子操作

よく使われる量子操作(量子ゲート)

- 2量子ビットに対する操作

制御Z(CZ)ゲート

$$CZ \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

制御NOT(CNOT)ゲート

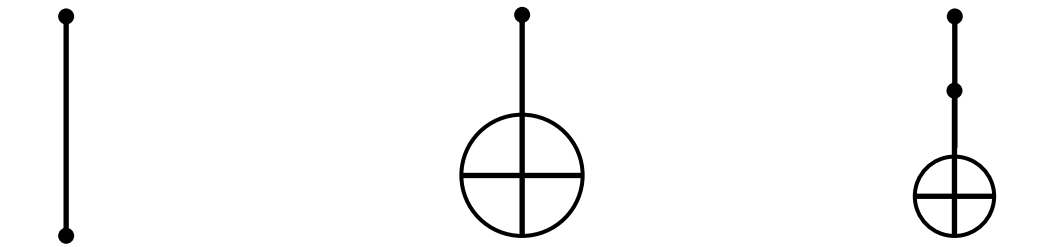
$$CX \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

- 3量子ビットに対する操作

Toffoliゲート

$$CCX \equiv |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes CX$$

CZ CX CCX



量子操作

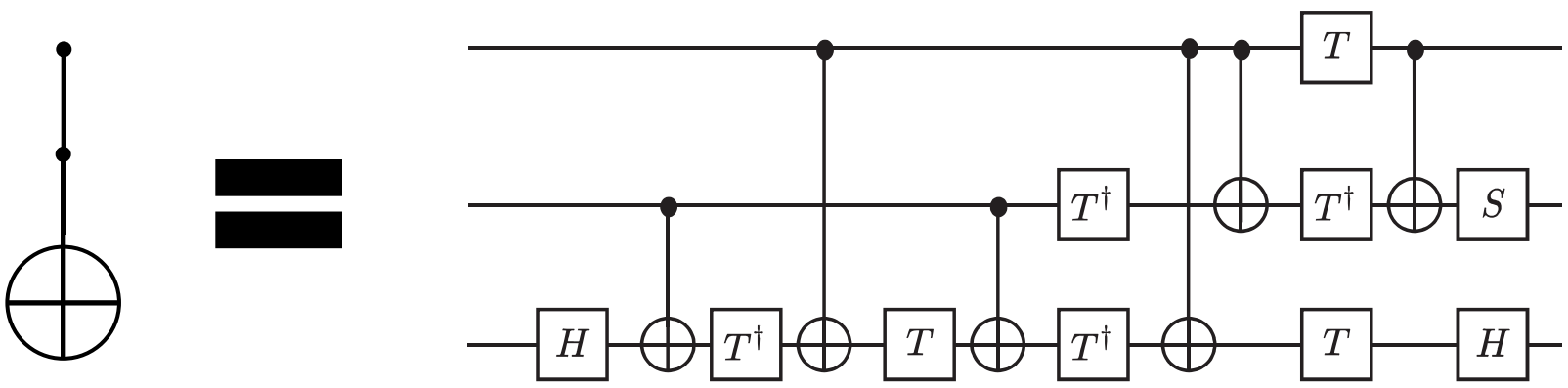
ユニバーサルゲートセット

Solovay-Kitaevの定理 [C. M. Dawson and M. A. Nielsen, QIC **6**, 81 (2006)]

H, *T*, *CX*の組み合わせ(掛け算やテンソル積)で、*n*量子ビットに対する任意のユニタリ行列を*1/exp(n)*精度で効率良く構成出来る。

例) Toffoliゲートの分解

※ $T^\dagger = T^7$



[M. Rahman and G. Paul, IEEE Trans. on Quant. Engineering **3**, 3100809 (2022)]

量子操作

ユニバーサルゲートセット

Solovay-Kitaevの定理 [C. M. Dawson and M. A. Nielsen, QIC **6**, 81 (2006)]

H, *T*, *CX*の組み合わせ(掛け算やテンソル積)で、*n*量子ビットに対する任意のユニタリ行列を*1/exp(n)*精度で効率良く構成出来る。

アダマールゲートの役割: 重ね合わせ状態の生成

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

*T*ゲートの役割: 重ね合わせ具合の調整

$$T\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

CNOTゲートの役割: エンタングル状態の生成

$$CX\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

量子操作

重ね合わせ状態と混合状態の違い

重ね合わせの場合

$$|0\rangle$$

$$\downarrow H$$

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

古典混合の場合

$$|0\rangle$$

$$\downarrow$$

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

どちらの場合でも、
50%の確率で1が出る

量子操作

重ね合わせ状態と混合状態の違い

重ね合わせの場合	古典混合の場合
$\|0\rangle$	$\|0\rangle$
$\downarrow H$	$\downarrow$
$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle\langle 0\| + \|1\rangle\langle 1\|}{2}$
$\downarrow H$	$\downarrow H$
$\|0\rangle$	$\frac{\|0\rangle\langle 0\| + \|1\rangle\langle 1\|}{2}$

重ね合わせの場合、
0に戻る

量子操作

ユニタリ操作 + 量子ビットの追加・削除

ここまで考えていた量子情報処理を図示すると

最初の
量子状態

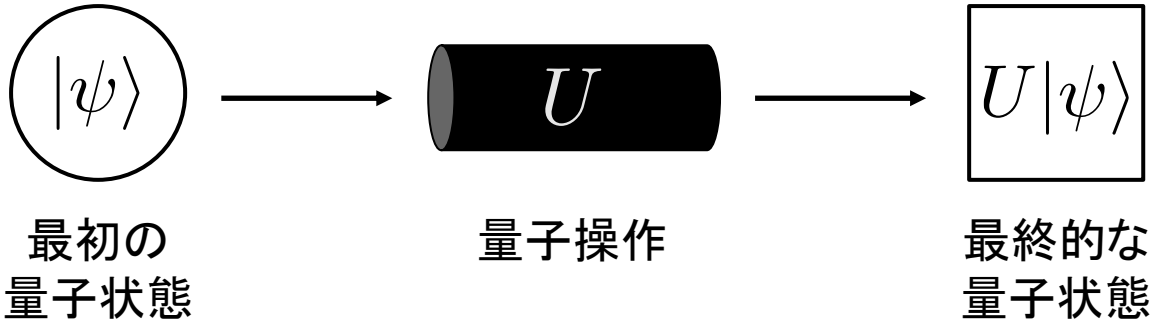
量子操作

最終的な
量子状態

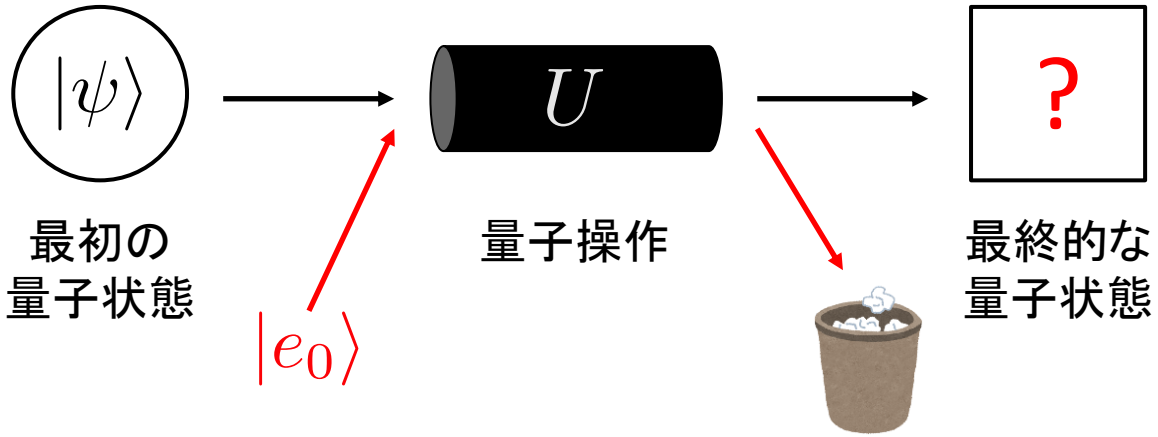
量子操作

ユニタリ操作 + 量子ビットの追加・削除

ここまで考えていた量子情報処理を図示すると

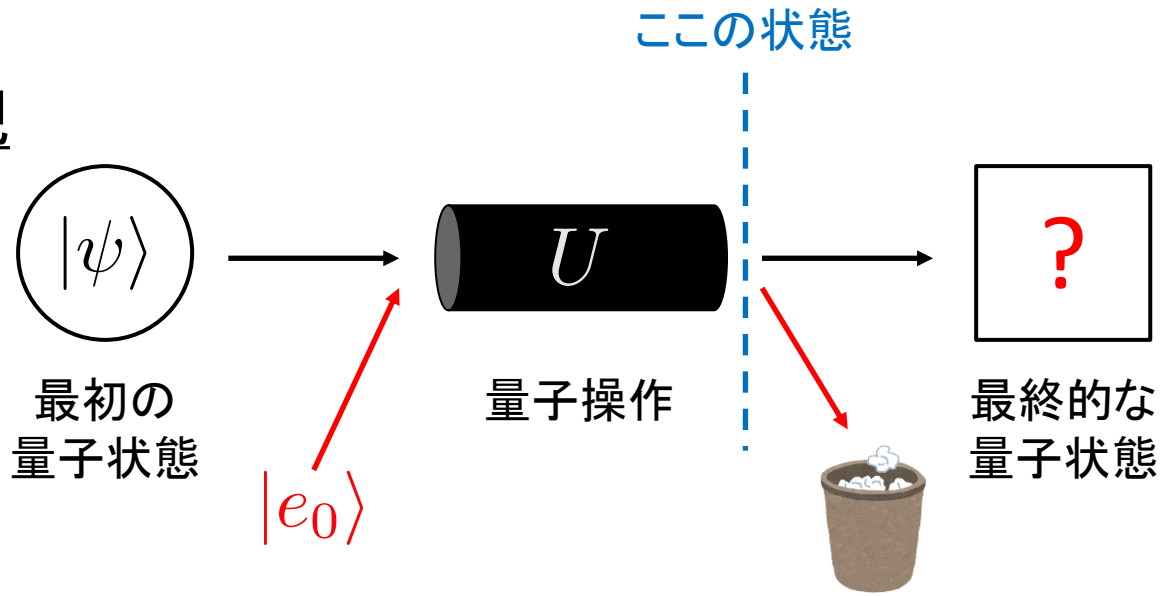


一般的には、量子操作の前後で補助量子状態の追加・削除が可能:



量子操作

Kraus表現



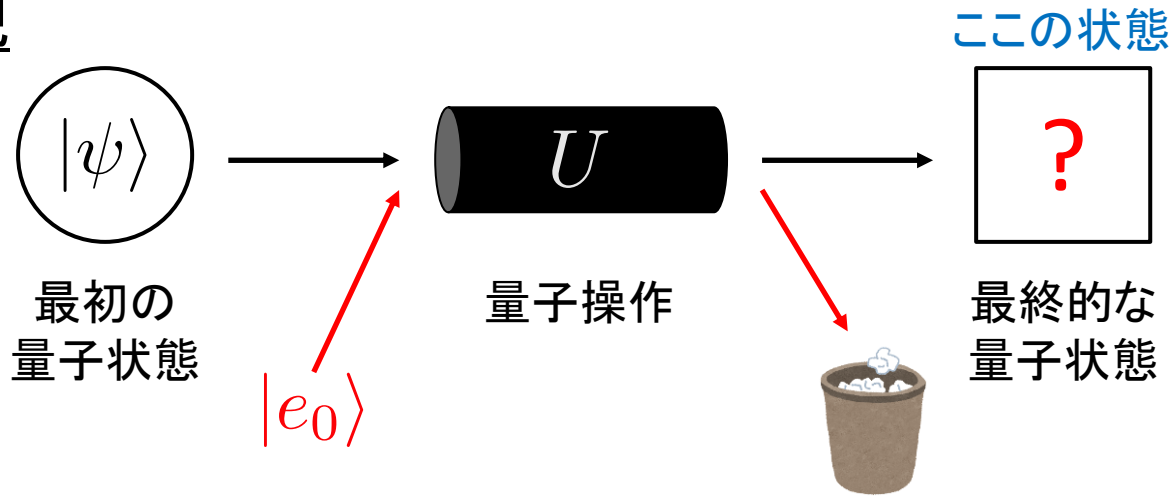
捨てる直前の状態は、

$$U(|\psi\rangle|e_0\rangle\langle\psi|\langle e_0|)U^\dagger$$

$\{|e_k\rangle\}_k$ は基底

量子操作

Kraus表現



捨てる直前の状態は、

$$U(|\psi\rangle|e_0\rangle\langle\psi|\langle e_0|)U^\dagger$$

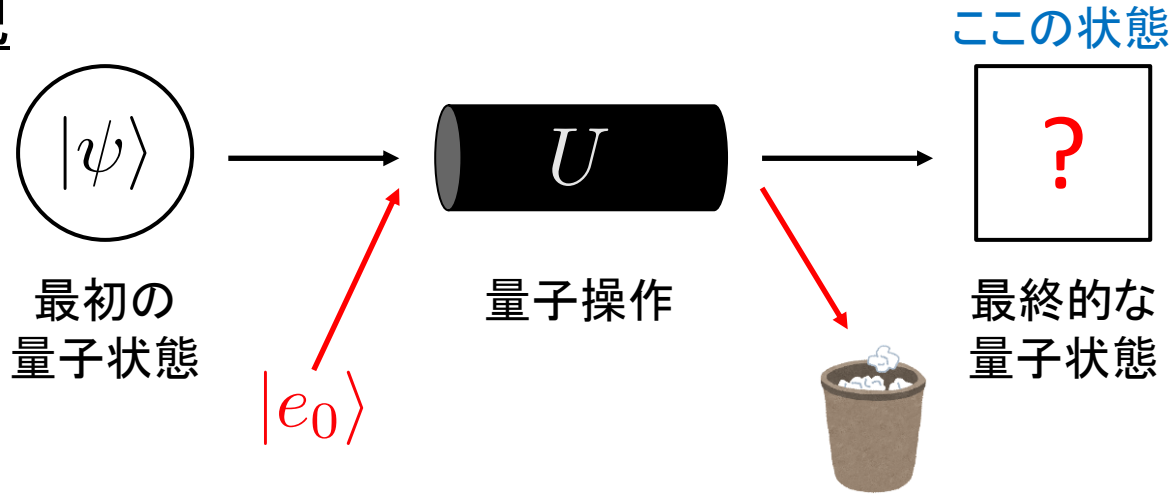
よって、捨てた(部分トレースを取った)後の状態は、

$$\mathrm{Tr}_{e_0}\left[U(|\psi\rangle|e_0\rangle\langle\psi|\langle e_0|)U^\dagger\right] = \sum_k \langle e_k|U|e_0\rangle(|\psi\rangle\langle\psi|)\langle e_0|U^\dagger|e_k\rangle$$

$\{|e_k\rangle\}_k$ は基底

量子操作

Kraus表現



捨てる直前の状態は、

$$U(|\psi\rangle|e_0\rangle\langle\psi|\langle e_0|)U^\dagger$$

よって、捨てた(部分トレースを取った)後の状態は、

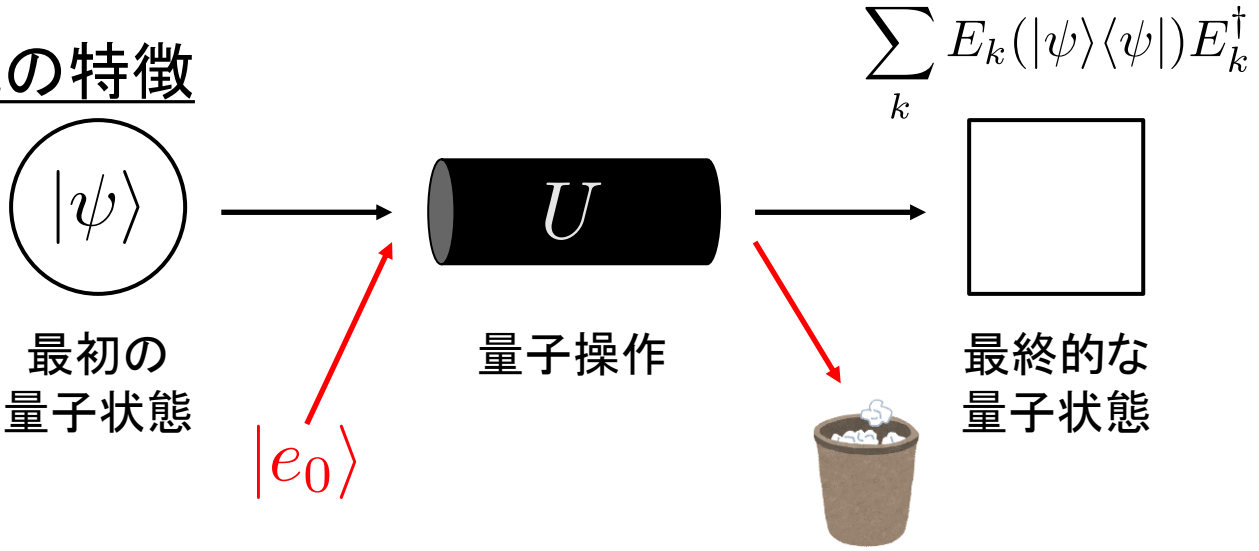
$$\mathrm{Tr}_{e_0}\left[U(|\psi\rangle|e_0\rangle\langle\psi|\langle e_0|)U^\dagger\right] = \sum_k \underbrace{\langle e_k|U|e_0\rangle}_{E_k}(|\psi\rangle\langle\psi|)\underbrace{\langle e_0|U^\dagger|e_k\rangle}_{E_k^\dagger}$$

Kraus行列

CPTP = Completely Positive and Trace Preserving

量子操作

Kraus表現の特徴



1. Kraus行列は

$$\sum_k E_k^\dagger E_k = \sum_k \langle e_0|U^\dagger|e_k\rangle\langle e_k|U|e_0\rangle = \langle e_0|U^\dagger U|e_0\rangle = 1$$

恒等行列

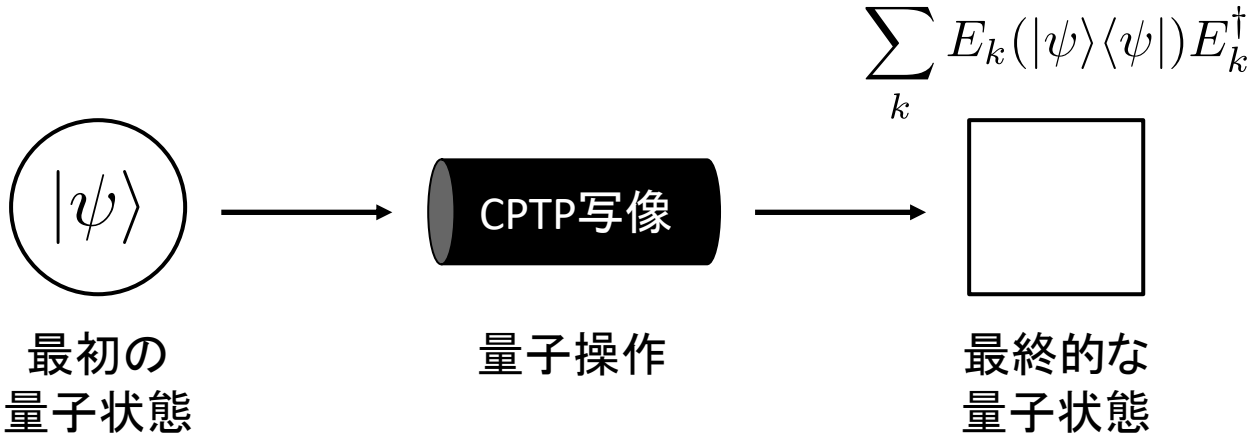
2. 任意のCPTP写像に対して、対応するKraus表現が存在する。(Krausの定理)

CPTP = Completely Positive and Trace Preserving

量子操作

一般的な量子操作

一般的な量子操作はCPTP写像で記述される。



◆ ポイント

量子操作は常にKraus行列を用いて記述することが出来る。

量子測定

(射影)測定: 量子状態(ベクトル)をビットに変換する確率的操作

ここでは、特に**射影測定**について考える。
射影測定は、射影行列の集合

$$\{P_z\}_z \qquad \text{s.t.} \qquad \sum_z P_z = I^{\otimes n}$$

で特徴付けられ、以下のルールで変換が行われる。

1. 測定結果zが出る確率は、n量子ビットの被測定状態が$|\psi\rangle$の時、

$$p_z = \mathrm{Tr}\left[P_z|\psi\rangle\langle\psi|\right]$$

2. 測定結果zが出た後の量子状態は

$$\frac{P_z|\psi\rangle}{\sqrt{\mathrm{Tr}\left[P_z|\psi\rangle\langle\psi|\right]}}$$

量子測定

(射影)測定: 量子状態(ベクトル)をビットに変換する確率的操作

ここでは、特に**射影測定**について考える。
射影測定は、射影行列の集合

$$\{P_z\}_z \qquad \text{s.t.} \qquad \sum_z P_z = I^{\otimes n}$$

で特徴付けられ、以下のルールで変換が行われる。

1. 測定結果*z*が出る確率は、*n*量子ビットの被測定状態が$|\psi\rangle$の時、

$$p_z = \mathrm{Tr}\left[P_z|\psi\rangle\langle\psi|\right]$$

量子状態が規格化されているのは、確率の和を*1*にするため!

2. 測定結果*z*が出た後の量子状態は

$$\frac{P_z|\psi\rangle}{\sqrt{\mathrm{Tr}\left[P_z|\psi\rangle\langle\psi|\right]}}$$

量子測定

射影測定の具体例

1. 1量子ビットの状態$\alpha|0\rangle + \beta|1\rangle$を**計算基底**$\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$で測定した場合

- *0*が出る確率とその時の量子状態

$$p_0 = |\alpha|^2, \quad |0\rangle$$

- 1が出る確率とその時の量子状態

$$p_1 = |\beta|^2, \quad |1\rangle$$

量子測定

*n*量子ビットの時は

$\{|z\rangle\langle z|\}_{z\in\{0,1\}^n}$

射影測定の具体例

1. 1量子ビットの状態$\alpha|0\rangle+\beta|1\rangle$を**計算基底**$\{|0\rangle\langle 0|,|1\rangle\langle 1|\}$で測定した場合

- *0*が出る確率とその時の量子状態

$$p_0=|\alpha|^2,\quad |0\rangle$$

- 1が出る確率とその時の量子状態

$$p_1=|\beta|^2,\quad |1\rangle$$

量子測定

射影測定の具体例

1. 1量子ビットの状態$\alpha|0\rangle + \beta|1\rangle$を**計算基底**$\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$で測定した場合

- *0*が出る確率とその時の量子状態

$$p_0 = |\alpha|^2, \quad |0\rangle$$

- 1が出る確率とその時の量子状態

$$p_1 = |\beta|^2, \quad |1\rangle$$

2. Bell状態の1量子ビット目を計算基底で測定して*0*が出る場合

$$p_0 = \mathrm{Tr}\left[(|0\rangle\langle 0| \otimes I)\frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right] = \mathrm{Tr}\left[\frac{|00\rangle\langle 00| + |00\rangle\langle 11|}{2}\right] = \frac{1}{2}$$

量子測定

射影測定の具体例

1. 1量子ビットの状態$\alpha|0\rangle + \beta|1\rangle$を**計算基底**$\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$で測定した場合

- *0*が出る確率とその時の量子状態

$$p_0 = |\alpha|^2, \quad |0\rangle$$

- 1が出る確率とその時の量子状態

$$p_1 = |\beta|^2, \quad |1\rangle$$

2. Bell状態の1量子ビット目を計算基底で測定して*0*が出る場合

$$\frac{(|0\rangle\langle 0| \otimes I)\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}}{\dfrac{1}{\sqrt{2}}} = |00\rangle$$

量子測定

射影測定の具体例

1. 1量子ビットの状態$\alpha|0\rangle + \beta|1\rangle$を**計算基底**$\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$で測定した場合

- *0*が出る確率とその時の量子状態

$$p_0 = |\alpha|^2, \quad |0\rangle$$

- 1が出る確率とその時の量子状態

$$p_1 = |\beta|^2, \quad |1\rangle$$

2. Bell状態の1量子ビット目を計算基底で測定して*0*が出る場合

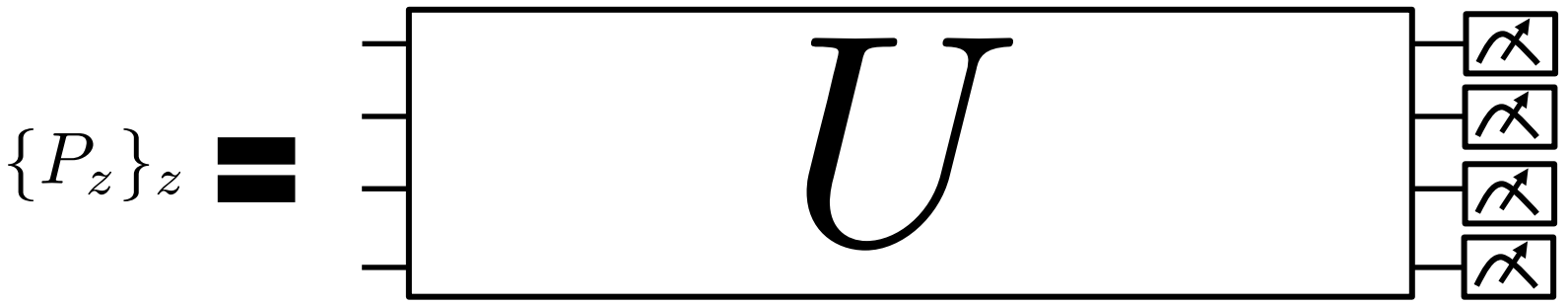
$$\frac{(|0\rangle\langle 0| \otimes I)\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}}{\dfrac{1}{\sqrt{2}}} = |00\rangle$$

量子状態の収縮

量子測定

射影測定 = ユニタリ操作 + 計算基底測定

任意の射影測定は、適切なユニタリ操作をした後に計算基底測定を行うことでシミュレート出来る。



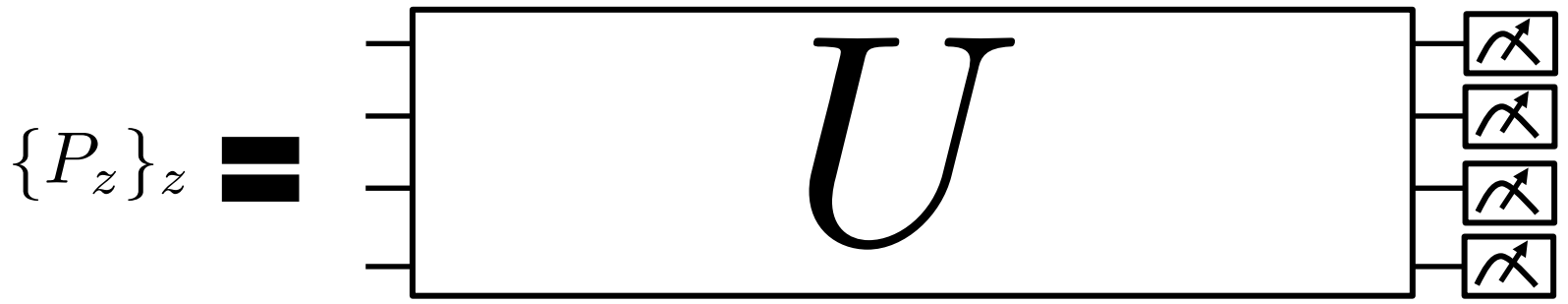
$$X \equiv |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

量子測定

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

射影測定 = ユニタリ操作 + 計算基底測定

任意の射影測定は、適切なユニタリ操作をした後に計算基底測定を行うことでシミュレート出来る。



例) パウリ*X*ゲートの固有状態の基底(アダマール基底)で測定したい場合

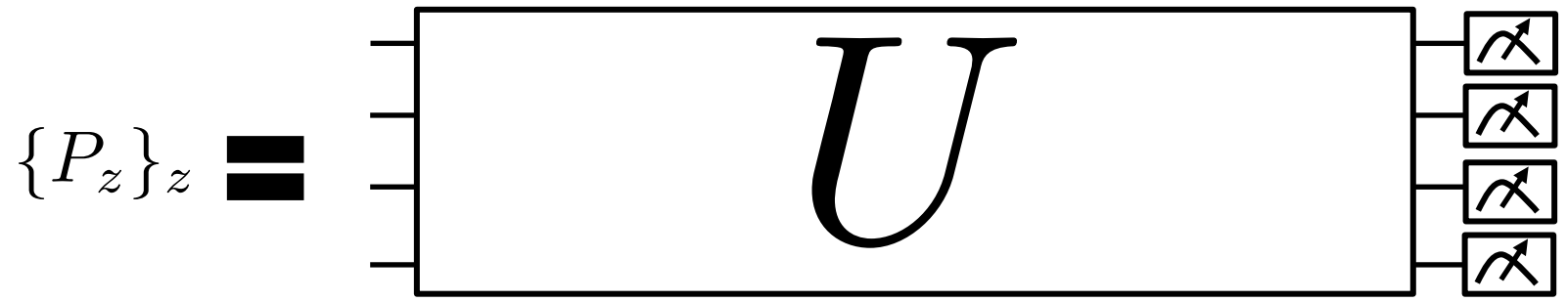
$$X \equiv |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

量子測定

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

射影測定 = ユニタリ操作 + 計算基底測定

任意の射影測定は、適切なユニタリ操作をした後に計算基底測定を行うことでシミュレート出来る。



例) パウリ*X*ゲートの固有状態の基底(アダマール基底)で測定したい場合

$$\{|+\rangle\langle +|, |-\rangle\langle -|\} \quad = \quad \{H|0\rangle\langle 0|H^\dagger, H|1\rangle\langle 1|H^\dagger\}$$

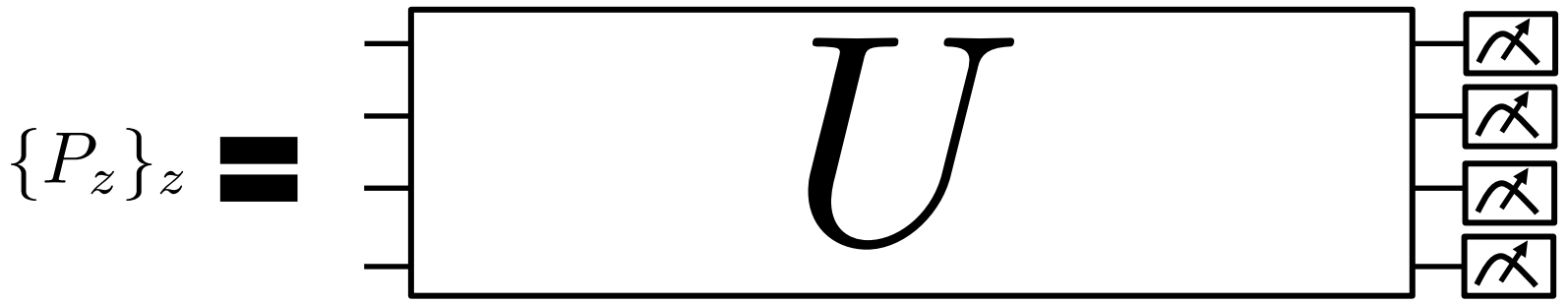
$$X \equiv |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

量子測定

射影測定 = ユニタリ操作 + 計算基底測定

任意の射影測定は、適切なユニタリ操作をした後に計算基底測定を行うことでシミュレート出来る。



◆ ポイント

ユニタリ操作が可能な時は、計算基底測定だけ考えれば良い。

量子測定

観測量の期待値の推定

射影測定を用いて行える操作に、観測量(=エルミート行列)*A*の期待値

$$\langle\psi|A|\psi\rangle$$

の推定がある。(明日の「量子計算基礎」でも使う。)

*A*は対角化可能なので、

$$A = \sum_z a_z|\phi_z\rangle\langle\phi_z| = \sum_z a_z U|z\rangle\langle z|U^\dagger$$

固有値　固有ベクトル

量子測定

観測量の期待値の推定

射影測定を用いて行える操作に、観測量(=エルミート行列)*A*の期待値

$$\langle\psi|A|\psi\rangle$$

の推定がある。(明日の「量子計算基礎」でも使う。)

*A*は対角化可能なので、

$$A = \sum_z a_z |\phi_z\rangle\langle\phi_z| = \sum_z a_z U|z\rangle\langle z|U^\dagger$$

固有値　固有ベクトル

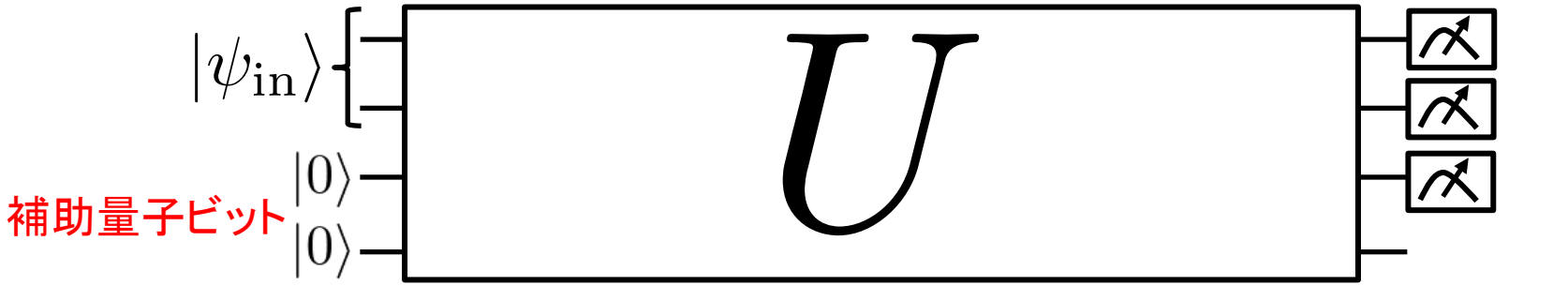
$$\langle\psi|A|\psi\rangle = \sum_z a_z \mathrm{Tr}\left[(|z\rangle\langle z|)U^\dagger|\psi\rangle\langle\psi|U\right]$$

$|\psi\rangle$に$U^\dagger$をかけて計算基底測定した時に、*z*が出る確率

量子計算

量子回路

量子計算は以下の図で表現出来る。



入力量子ビット
(2次元正規ベクトル)

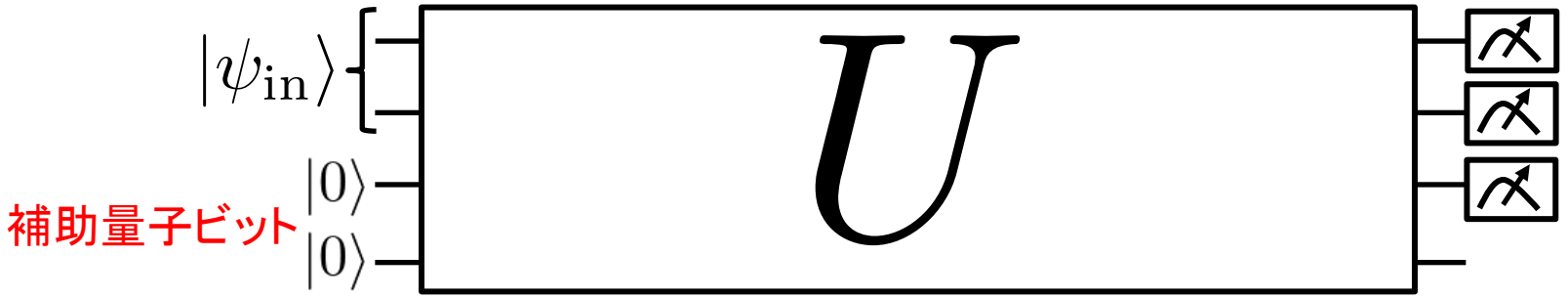
量子ゲート
(ユニタリ行列)

出力ビット

量子計算

量子回路

量子計算は以下の図で表現出来る。



入力量子ビット
(2次元正規ベクトル)

量子ゲート
(ユニタリ行列)

出力ビット

Remark 1(純粋化)
純粋状態に限定してOK

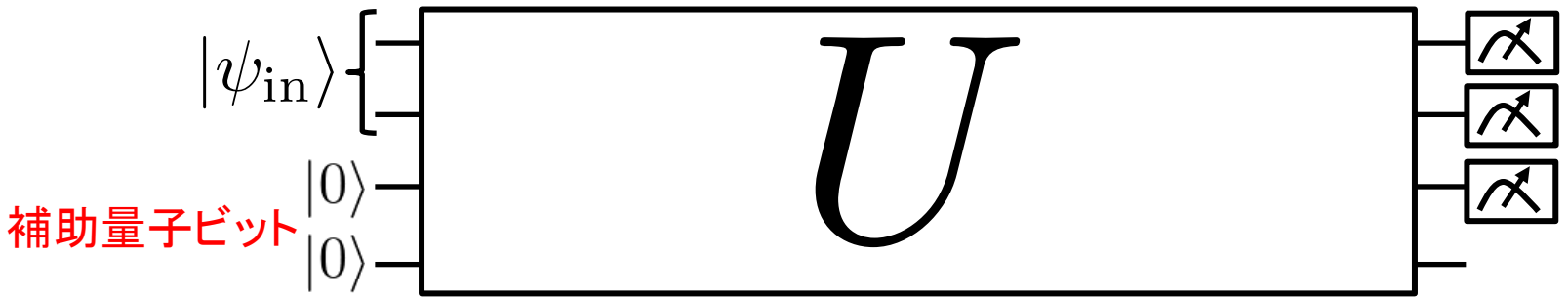
Remark 2(Kraus表現)
ユニタリ行列に限定してOK

Remark 3(基底変換)
計算基底測定に限定してOK

量子計算

量子回路

量子計算は以下の図で表現出来る。



入力量子ビット
(2次元正規ベクトル)

量子ゲート
(ユニタリ行列)

出力ビット

Remark 4(Solovay-Kitaevの定理)
*H, T, CX*の組み合わせだけ考えればOK

→ 計算の効率(計算時間)は、*H, T, CX*をいくつ必要とするかで議論出来る (詳細は明日)

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

余談

量子暗号でも利用されている

複製不可能定理 [W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982)]

任意の量子状態を複製する量子操作は存在しない。

(証明)
これまでの議論より、一般の量子操作は
補助量子状態$|e_0\rangle$を付けて、全体にユニタリ行列Uをかける
という操作として表現出来る。
よって、もし任意の量子状態を複製する量子操作が存在するならば、

$$U(|0\rangle|e_0\rangle) = |0\rangle|0\rangle|g(0)\rangle$$

$$U(|+\rangle|e_0\rangle) = |+\rangle|+\rangle|g(+)\rangle$$

という2つの式が成り立つ事になる。

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

余談

量子暗号でも利用されている

複製不可能定理 [W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982)]

任意の量子状態を複製する量子操作は存在しない。

(証明の続き)

$$U(|0\rangle|e_0\rangle) = |0\rangle|0\rangle|g(0)\rangle$$

$$U(|+\rangle|e_0\rangle) = |+\rangle|+\rangle|g(+)\rangle$$

しかし、左辺の内積の絶対値は

$$|(\langle e_0|\langle 0|)U^\dagger U(|+\rangle|e_0\rangle)| = \frac{1}{\sqrt{2}}$$

右辺の内積の絶対値は

$$|(\langle 0|\langle 0|\langle g(0)|)(|+\rangle|+\rangle|g(+)\rangle)| = \frac{|\langle g(0)|g(+)\rangle|}{2} < \frac{1}{2}$$

絶対に一致しない

$$\forall A,\ |A| \equiv \sqrt{A^\dagger A}$$

量子状態間の距離

トレース距離

2つの量子状態(密度行列)ρとσ間の距離を表す量

$$D(\rho,\sigma) \equiv \frac{\mathrm{Tr}\left[|\rho-\sigma|\right]}{2}$$

- 性質

1. 距離の条件1(非退化性)

$$D(\rho,\sigma)=0 \iff \rho=\sigma$$

2. 距離の条件2(対称性)

$$D(\rho,\sigma)=D(\sigma,\rho)$$

3. 距離の条件3(三角不等式)

$$\forall\tau,\ D(\rho,\sigma)\leq D(\rho,\tau)+D(\tau,\sigma)$$

4. 量子操作(CPTP写像ε)に対して収縮的(contractive)

$$\forall\mathcal{E},\ D(\mathcal{E}(\rho),\mathcal{E}(\sigma))\leq D(\rho,\sigma)$$

$$\forall A,\ |A| \equiv \sqrt{A^\dagger A}$$

量子状態間の距離

トレース距離

2つの量子状態(密度行列)ρとσ間の距離を表す量

$$D(\rho,\sigma) \equiv \frac{\mathrm{Tr}\left[|\rho-\sigma|\right]}{2}$$

- 性質

1. 距離の条件1(非退化性)

$$D(\rho,\sigma)=0 \iff \rho=\sigma$$

2. 距離の条件2(対称性)

$$D(\rho,\sigma)=D(\sigma,\rho)$$

3. 距離の条件3(三角不等式)

$$\forall\tau,\ D(\rho,\sigma)\le D(\rho,\tau)+D(\tau,\sigma)$$

4. 量子操作(CPTP写像ε)に対して収縮的(contractive)

$$\forall\mathcal{E},\ D(\mathcal{E}(\rho),\mathcal{E}(\sigma))\le D(\rho,\sigma)$$

量子状態同士を近付けることは出来ても、遠ざけることは出来ない!

量子状態間の距離

トレース距離とL$_1$距離(Kolmogorov距離)の関係

トレース距離は、量子状態から得られる測定結果の確率分布間の距離の最大値を与える。

$P \equiv \{P_z\}_z$という射影測定を行うことを考える。
この時、ρとσから得られる測定結果の確率分布は

$$\{p_z = \mathrm{Tr}\left[P_z \rho\right]\}_z$$

$$\{q_z = \mathrm{Tr}\left[P_z \sigma\right]\}_z$$

である。これらのL$_1$距離に対して、

$$\mathrm{max}_P \left\{ \frac{1}{2} \sum_z |p_z - q_z| \right\} \leq D(\rho, \sigma)$$

量子状態間の距離

トレース距離とL$_1$距離(Kolmogorov距離)の関係

トレース距離は、量子状態から得られる測定結果の確率分布間の距離の最大値を与える。

$P \equiv \{P_z\}_z$という射影測定を行うことを考える。
この時、ρとσから得られる測定結果の確率分布は

$$\{p_z = \mathrm{Tr}\left[P_z \rho\right]\}_z$$

$$\{q_z = \mathrm{Tr}\left[P_z \sigma\right]\}_z$$

である。これらのL$_1$距離に対して、

$$\max_P \left\{ \frac{1}{2} \sum_z |p_z - q_z| \right\} \leq D(\rho, \sigma)$$

一般の量子測定(POVM測定)も含めると、等号が成立する。

量子状態間の距離

※1 https://www.pref.fukuoka.lg.jp/contents/ecoton-hp.html
※2 https://www.city.atsugi.kanagawa.jp/soshiki/kankoshinkoka/3/3/3142.html

トレース距離の物理的解釈

以下のようなゲームを考える。

あゆコロちゃん [※2]

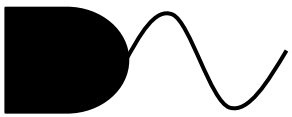
ρ

or

σ

確率*1/2*で選ぶ。

$$\{P_0, P_1 = I^{\otimes n} - P_0\}$$



エコトン [※1]

0 → ρ
1 → σ と判断する。

量子状態間の距離

※1 https://www.pref.fukuoka.lg.jp/contents/ecoton-hp.html
※2 https://www.city.atsugi.kanagawa.jp/soshiki/kankoshinkoka/3/3/3142.html

トレース距離の物理的解釈

以下のようなゲームを考える。

あゆコロちゃん [※2]

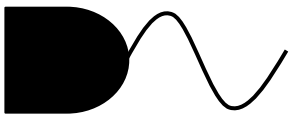
ρ

or

σ

確率*1/2*で選ぶ。

$\{P_0, P_1 = I^{\otimes n} - P_0\}$



エコトン [※1]

0 → ρ
1 → σ と判断する。

エコトンが正しく当てられる確率は

$$\frac{\mathrm{Tr}\left[P_0\rho\right] + \mathrm{Tr}\left[P_1\sigma\right]}{2} = \frac{1 + \mathrm{Tr}\left[P_0(\rho - \sigma)\right]}{2} \leq \frac{1 + 2D(\rho, \sigma)}{2}$$

量子状態間の距離

※1 https://www.pref.fukuoka.lg.jp/contents/ecoton-hp.html
※2 https://www.city.atsugi.kanagawa.jp/soshiki/kankoshinkoka/3/3/3142.html

トレース距離の物理的解釈

以下のようなゲームを考える。

あゆコロちゃん [※2]

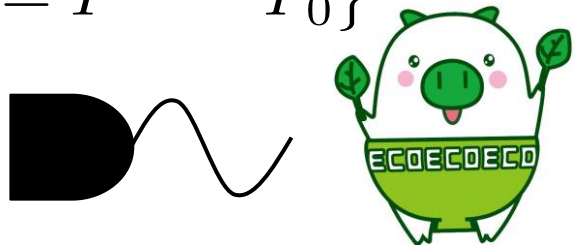
ρ

or

σ

確率*1/2*で選ぶ。

$\{P_0, P_1 = I^{\otimes n} - P_0\}$



エコトン [※1]

0 → ρ
1 → σ と判断する。

エコトンが正しく当てられる確率は

よりタイトな不等式を使えば消せる。

$$\frac{\mathrm{Tr}\left[P_0\rho\right] + \mathrm{Tr}\left[P_1\sigma\right]}{2} = \frac{1 + \mathrm{Tr}\left[P_0(\rho - \sigma)\right]}{2} \leq \frac{1 + 2D(\rho, \sigma)}{2}$$