# Basics of quantum information

単一システム

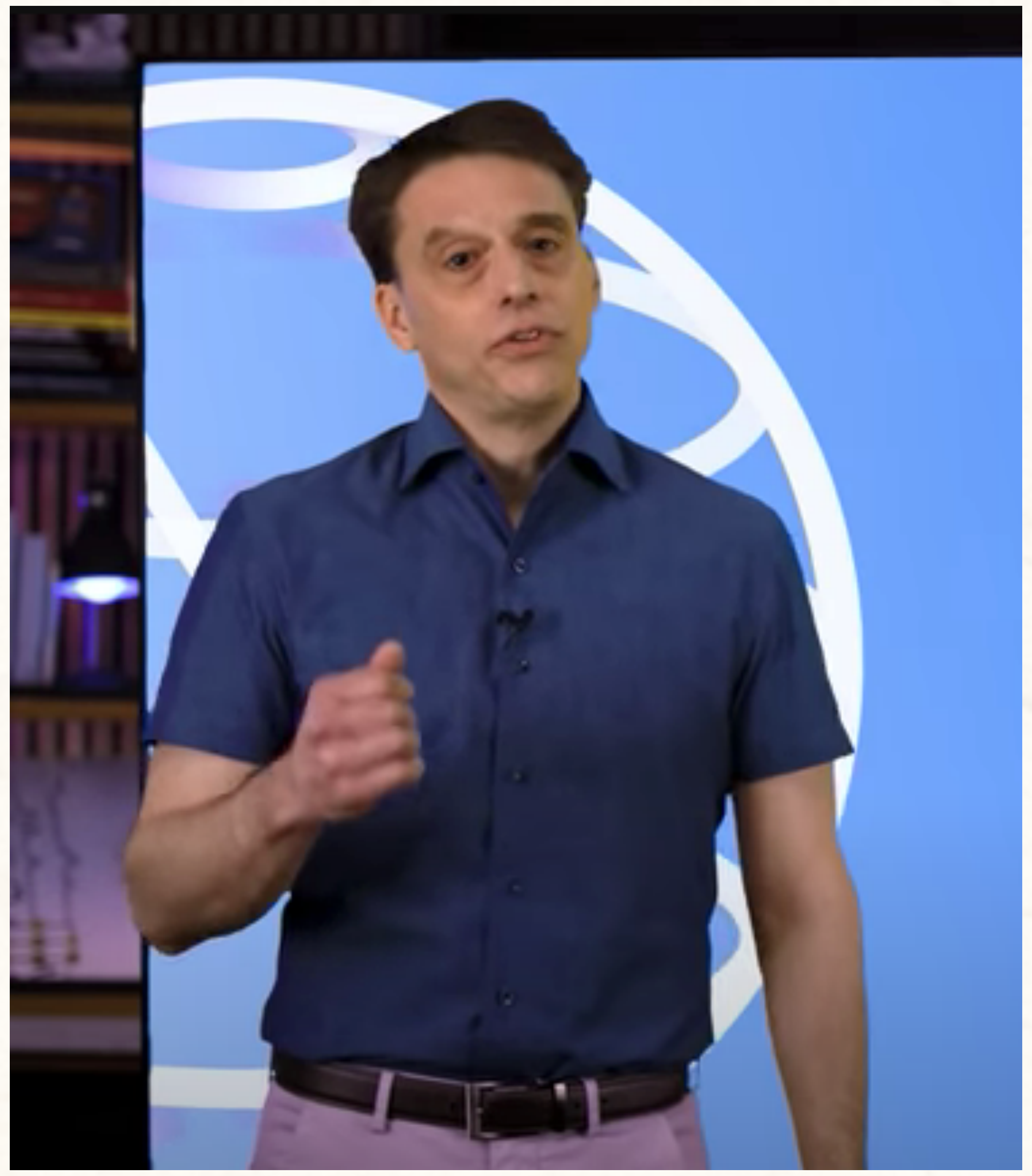
〜古典情報

Quantum Tokyo

# 全体の概要

## Understanding Quantum Information and Computation by John Watrous

- このコースはYouTubeの動画コースがベースになっています。
  https://www.youtube.com/watch?v=42OiBzfdE2o



## テーマ

- 量子情報・量子計算について数学を用いて詳しく説明します。
- 基礎をカッチリ固めたい人向けの作りになっています。
- レベル感としては大学生以上向けらしいですが、高校生でも大丈夫かと。

# あると良い知識・なくても問題ない知識

基本的には説明があるのであまり気にしなくていいと思います

## あると良い知識

1. 線形代数の基礎
2. 複素数の知識
3. 集合と関数

## なくても問題ない知識

1. 量子コンピューティングの知識
2. 物理（量子力学 etc.）の知識

# コースの内容

## 量子情報の基礎

コースの中で徐々に以下のような内容が数学的記述も交えつつ解説されていきます。

1. 測定
2. 操作
3. 量子回路
4. 量子テレポーテーション
5. etc.

# 今日の内容

## 量子情報の基礎としての古典情報

- “古典情報” を扱います。
- 古典情報とは言いつつも、コース全体が量子情報を扱いますので、そのために役立つ導入としての位置付けになります。
- 普通の古典情報の教科書では見慣れない記号も導入されます・・・。
- なので・・・

~~エントロピー~~

~~シャノンのサンプリング定理~~

~~カルバック・ライブラー情報量~~

この辺のお話は出てこない
と思います・・・

# 古典情報 — 単一システム

一番簡単なところから

# 1.1 古典的な状態と確率ベクトル

- ここからが本編です。https://learn.qiskit.org/course/basics/single-systems に対応します。
- ここで「古典的」というのは古臭いとかそういう意味ではなく、コースのメインである「量子的」な情報や計算に対しての対比で用いられています。
- よって、量子的な振る舞いが発生しない、活用しない情報理論と思ってもらえれば良いと思います。ご存知の方も多いかもしれませんが、量子的な振る舞いとは “重ね合わせ” や “量子もつれ” などを指しています・・・。

# 1.1 古典的な状態と確率ベクトル

## 「システム」の「状態」の例

- (典型的な例) “0” と “1” で表現できる状態。(例: コインの「表」と「裏」)
- “1”, “2”, “3”, “4”, “5”, “6” で表現できる状態。(例: サイコロの目の数)
- “A”, “C”, “G”, “T” (アデニン、シトシン、グアニン、チミン; DNAの塩基)
- “強”, “中”, “弱”, “切” (扇風機のスイッチ)

一般化して、$X$ (例: サイコロ) というシステムの状態 $\Sigma$ (例: 1, 2, 3, 4, 5, 6) を考えてみます。

$X$ がビットの場合には、$\Sigma = \{0, 1\}$ になります。

# 1.1 古典的な状態と確率ベクトル

量子の話に入るとビットのお話が多いので、ここではそれに似たシステム $X$ としてコインの場合で、状態 $\Sigma = \{0, 1\}$ のケースを考えてみます。

- コインを考えて、0 が表、1 が裏とします。ところでこのコインは均一ではなく偏っていて、トスすると100回中75回は表が、25回は裏が出るとします。
- これを数式で書くと以下のようになります。

$$\Pr(X = 0) = \frac{3}{4} \text{ と } \Pr(X = 1) = \frac{1}{4}$$

# 1.1 古典的な状態と確率ベクトル

$$\Pr(X=0)=\frac{3}{4} \text{ と } \Pr(X=1)=\frac{1}{4}$$

この式をまとめて書く方法として以下のような方法があります。突然ベクトル表記になりますが、後の話とのつながりの関係なのでそんなものということで。

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} \longleftarrow \text{確率ベクトル}$$

# 1.2 確率的状態の測定

- 前ページでコインというシステムを例にとり、確率的に表と裏が出るような状況を考えました。

- これを「確認」する（あるいは「測定」する）ことを考えます。つまりコイントスして表が出るか裏が出るかを確認します。

- 状態を数学的に記述するための道具を徐々に用意します。まず、ベクトルを使って、「表」と「裏」を数式にします。

$$表=\begin{pmatrix}1\\0\end{pmatrix} と 裏=\begin{pmatrix}0\\1\end{pmatrix}$$

# 1.2 確率的状態の測定

$$表 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ と } 裏 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- すると、先ほど表が100回中75回出るコインの確率ベクトルとして記載したものは以下のように書き直せて、記号の辻褄が合いました！

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}表 + \frac{1}{4}裏$$

# 1.2 確率的状態の測定

- 考えるシステム $X$ と状態 $\Sigma$ はコインの表と裏だけではありませんので、もう少し一般的な記号にします。

- 完全に後のセクションとの都合だけで “Diracのブラケット記号” というものを用いて記号を置き換えます。

- ただの記号なので「なんで 0 と 1 なんだろう・・・」ということに意味はなくて、なんとなく数字にしておくと拡張性があるからくらいでお願いします。

$$\text{表} \rightarrow |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ と 裏} \rightarrow |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

# 1.2 確率的状態の測定

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}\text{表} + \frac{1}{4}\text{裏}$$

- 新しい記号を用いると、上記の数式は以下のように一般化されます。

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$$

# 1.2 確率的状態の測定

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$$

- この式は、コインの例えでは表という状態が確率 3/4 で、裏という状態が確率 1/4 で出るような状態を数式であらわしたものでした。
- 一般化した後も状況は同じで、状態 $|0\rangle$ が確率 3/4 で、状態 $|1\rangle$ が確率 1/4 で "出る" ような状態をあらわしています。
- 何かを試行して "出た" ことを確認することを「測定する」と言います。

# 1.3 古典的な演算 —決定論的演算

- 今日の最後のサブセクション（わりと長い）です。
- 解説している側からこういうのも何ですが、後のセクションとの都合でかなり分かりにくい書き方をしているので、よく分からなくても全然問題ないと思います。
- 個人的な好みの問題で、以下も引き続きコインの表裏を例にとります。
- つまり、$X$ (コイン) とシステムの状態 $\Sigma$ (0 (表), 1 (裏)) です。 ここからは表と裏が 50% ずつの確率で出る公正なコインとしたいと思います。

# 1.3 古典的な演算 —決定論的演算

- コイン システムの状態 $a \in \Sigma$ に演算 $f$ を適用して新しい状態 $f(a) \in \Sigma$ に変換することを考えます。
- といってもイメージがわかないので、コインを手でひっくり返すというシチュエーションを考えます。
- 演算 $f$ は、コインを表裏ひっくり返すといった操作を指します。目玉焼きではやらないでくださいね・・・
- 演算としては「何もしない」も含まれます。

# 1.3 古典的な演算 —決定論的演算

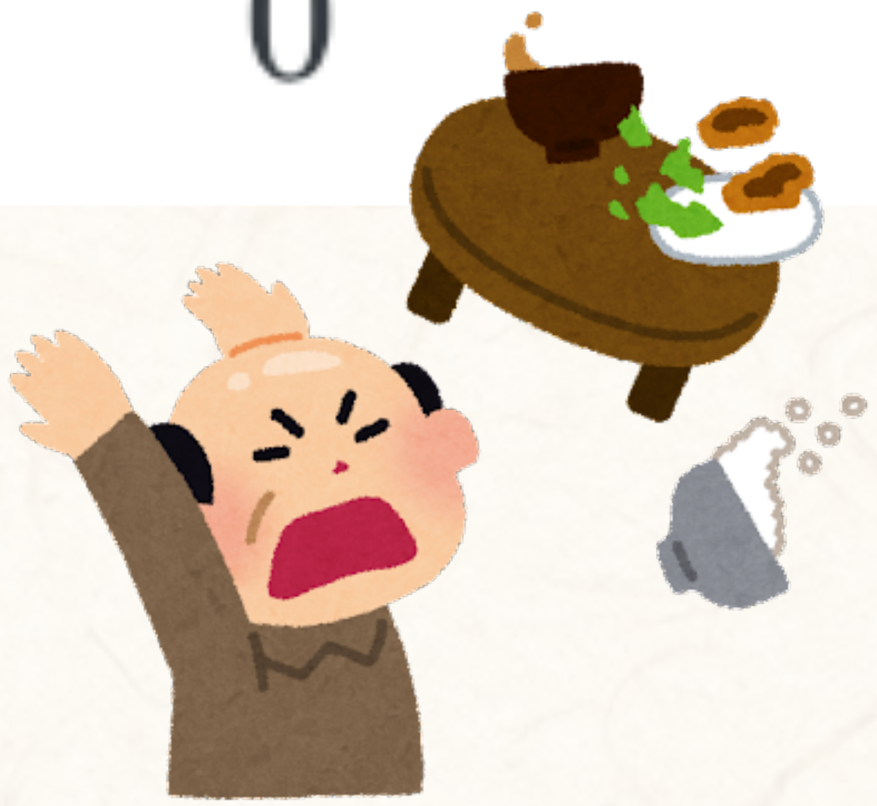
- 演算を表にすると以下のようになります。4 パターンあります。

| $a$ | $f_1(a)$ |
|---|---|
| 0 | 0 |
| 1 | 0 |

| $a$ | $f_2(a)$ |
|---|---|
| 0 | 0 |
| 1 | 1 |

| $a$ | $f_3(a)$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

| $a$ | $f_4(a)$ |
|---|---|
| 0 | 1 |
| 1 | 1 |



- $f_2$ は「何もしない」で、$f_3$ は「無条件にコインをひっくり返す」です。
- $f_1$ は「コインが裏ならひっくり返す」といったところでしょうか？

# 1.3 古典的な演算 —決定論的演算

- 当面はルールを明確にした演算のみ考えます。つまりトスしてコインをひっくり返すとかでなく、ルールに従った決定論的な演算のみ考えます。(最後のほうで確率的な演算も触れて終わります)

- $f_1, f_2, f_3, f_4$ は行列を用いて表現できます。それぞれ以下の行列に対応します:

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},\ M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ M_4 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

# 1.3 古典的な演算 —決定論的演算

- 例題をやってみましょう:「$f_3$ を確認してみよう」
- $f_3$ は行列 $M_3$ をかけることに相当します。よって、 表$=|0\rangle$ と 裏$=|1\rangle$ を思い出すと:

$$M_3|0\rangle = M_3\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$$

$$M_3|1\rangle = M_3\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle$$

- 確かに反転しました。この演算は特に NOT 演算 と呼ばれます。

# 1.3 古典的な演算 —決定論的演算

- $M_3|0\rangle = M_3\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$ を一般化します。
- すると、これは演算 $f$ と対応する行列 $M$、そして状態 $|a\rangle$ を用いて、以下のように書くことができます。

$$M|a\rangle = |f(a)\rangle$$

# 1.3 古典的な演算 —決定論的演算

- さらに計算のための道具を追加します。
- ここまで $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ と $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ という記法を用いてきました。これらは通常ケットベクトルと呼ばれます。
- これらに対応するものにブラベクトルというものがあって、次のように定義されます。

$$\langle 0| = (1 \quad 0) \text{ と } \langle 1| = (0 \quad 1)$$

- 2つ併せてブラ・ケット（カギ括弧）という P. A. M. Dirac が導入した記号です。

# 1.3 古典的な演算 —決定論的演算

- ケットベクトルもブラベクトルも数学的にはただの列ベクトルと行ベクトルですが、同時に、2行1列の行列、1行2列の行列という見方もできます。この考え方を通して、行列しての積を考えることができます。例えば以下のようなものです:

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0 \quad 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

# 1.3 古典的な演算 —決定論的演算

- すると、演算 $f:\Sigma \to \Sigma$ はかなり気色悪い書き方ですが、対応する行列 $M$ を用いて次のように書くことができます。

$$M = \sum_{a\in\Sigma} |f(a)\rangle\langle a|$$

- 大分つらいので、“無条件のひっくり返し” (NOT 演算) の場合に書き下してみましょう:

$$M_3 = |f(0)\rangle\langle 0| + |f(1)\rangle\langle 1| = |1\rangle\langle 0| + |0\rangle\langle 1|$$

# 1.3 古典的な演算 —決定論的演算

- $M_3 = |1\rangle\langle 0| + |0\rangle\langle 1|$ をネタに 2 つ目の例題を考えみましょう。
- 例題:「右辺の表示が状態 $|0\rangle$ と状態 $|1\rangle$ を反転させることを確認しよう」

$$(|1\rangle\langle 0| + |0\rangle\langle 1|)|0\rangle = |1\rangle\langle 0|0\rangle + |0\rangle\langle 1|0\rangle = |1\rangle \cdot 1 + |0\rangle \cdot 0 = |1\rangle$$

$$(|1\rangle\langle 0| + |0\rangle\langle 1|)|1\rangle = |1\rangle\langle 0|1\rangle + |0\rangle\langle 1|1\rangle = |1\rangle \cdot 0 + |0\rangle \cdot 1 = |0\rangle$$

- 目がチカチカしますが、一応確認できました。ここで、次の行列計算を使いました。

$$\langle 0|0\rangle = (1 \quad 0)\begin{pmatrix}1\\0\end{pmatrix} = 1,\ \langle 0|1\rangle = (1 \quad 0)\begin{pmatrix}0\\1\end{pmatrix} = 0,\quad \text{etc.}$$

# 1.3 古典的な演算 — 確率演算と確率行列

- ここから次回以降の量子情報に向けての伏線を敷きます。

- 今まで決定論的な演算のみ考えましたが、ここから確率的な演算を扱います。対応する行列は例えば次のようになります:

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

- 表現が難しいですが「コインが表なら何もしないが、裏なら“コインをトスする”」という演算に対応します。実は解釈を変えて「50% の確率で何もしないが、50% の確率で、“コインが裏ならひっくり返す”」という決定論的演算の確率和と見ることもできます。

# 1.3 古典的な演算 — 確率演算と確率行列

- ここから次回以降の量子情報に向けての伏線を敷きます。
- 前のほうで $\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix}$ を確率ベクトルと呼んだのですが、今回 $\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$ を確率行列と呼びます。
- 確率行列の特徴は列ベクトルが確率ベクトルになっているということです。
- この行列は「50% の確率で何もしないが、50% の確率で、“コインが裏ならひっくり返す”」という、決定論的操作の確率和としての解釈ができると書きましたので一応見ておきましょう:

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}M_2 + \frac{1}{2}M_1$$

※ 一般論をAppendixに書きます

# 1.3 古典的な演算 — 確率演算の合成

- 直感的に捉えてもらうのが良いと思いますが、確率行列は次の性質を持ちます。
  - 確率ベクトルにかけこむと、新しい確率ベクトルを返す
  - 別の確率行列にかけこむと、新しい確率行列を返す
- また、数学的にはただの行列なので行列の積の結合法則が成立します。つまり、$u$ を確率ベクトルや、確率行列あるいは何かしらの状態とすると、確率行列 $M_1$ と $M_2$ に対して以下が成立します。

$$M_2(M_1 u) = (M_2 M_1)u$$

# 1.3 古典的な演算 — 確率演算の合成

- そして、確率行列は行列であるので、一般には積の順番を入れ換えることはできません。例えば、$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ と $M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ を考えると、以下のようになります。

$$M_2 M_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = M_1 M_2$$

- つまり、確率行列の適用の順番を無造作に入れ換えてしまうと、まるっきり違うこと（演算・操作）をやっていることに対応してしまいます。

おわり

# Appendix

確率行列 $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad (\alpha + \gamma = 1, \beta + \delta = 1), \alpha, \beta, \gamma, \delta \geq 0$ の確率和への分解:

- $\alpha \geq \beta$ の時:

$$M = (\alpha - \beta)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

- $\alpha < \beta$ の時:

$$M = \alpha \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \delta \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + (\beta - \alpha)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$