QDA©第２回　　「量子 computing」の学び方十か条　　2024.4.5v1

Quantum Dara Analysis

　なじみのない未知分野デである。学び方の戦略が重要であり、そこを誤ると中途で挫折しかねない。最初は詳しいことは省略し以下の基本の「幹」を述べ、具体的な計算例に達したのち、枝葉の細部に戻って理解を深める手順とする。計算例にはなるべく興味を喚起する実例を考えたい。

量子力学の理論的枠組の５要素

MIT *Barton　Zwiebach* 教授

Ⅰ　線形性
Ⅱ　複素数が必要
Ⅲ　決定論が成り立たない
Ⅳ　異例の「重ね合わせ原理」
Ⅴ　エンタングル状態

①　「量子 computer」と「量子 computing」は基本的には別モノで、工学的に実装された量子 computer は近接未来には実現が望めないフィクションで区別して考えること。他方、量子 computing は論理数学、線形代数、確率論の総合体系で原理的に Python 上で実践できる。

　＊量子 programming を基礎にした理論的計算システムを「量子コンピュータ」と称することが　おおいが、実装された「量子コンピュータ」実物からみれば、virtual(仮想的)である。

②　「量子 computing」の基本理解には量子力学の最小の基本枠組みさえ知っていれば十分で、個別各論は必要ない。特に、不用意に踏み込むと混乱し、かえって行く先を見失う恐れがある。

③　＜I、II＞　線形代数の固有値問題（ことにエルミート行列）は必須で、並行して、量子力学の演算子の固有値、固有ベクトル（固有状態）が対応する。最後に題材だけ挙げておいた。解説は次回とする。

④　＜III＞　おおまかには、確率論の基礎数理（数理統計学程度で十分）の読み替えになっていて、

基礎があれば理解は飛躍的に進む。なじみのない読者には必要以上に難しく疎遠に感じられている。解説者自身が確率論に未熟なケースも一部見受けられる。

＊本当に「確率的」であるかどうかは別議論で、いわゆる Bohr-Heisenberg の「コペンハーゲン解釈」にしたがい（あまくだりに）解説されているだけである。「あたかも(as if)確率と考えてみるとわかりやすい」くらいの気持ちである。あまり考えすぎないこと。そもそも、1920 年代には、信頼に足る確率論は　まだ存在していない。

⑤　<IV> 「重ね合わせの原理」のスタートが重要だが、さいころやコイン投げをイメージすればさしあたりは十分である。たとえば、コインの表、裏の 2 状態の出方は、線形式で

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

とあらわされる。コインには表（１）,裏（(０)の状態があるが、表が出たり裏が出たりする、もちろん同時に出るわけではない。なお、これら係数は二乗して確率になることに注意する。これは深遠なことではなく、量子力学の数学的出発点の都合にすぎないから、ただ認めるだけでよい。

＊　<　|　は bra、|　> は ket と呼ばれ、量子力学の創立者の一人であるディラック P.Dirac が角かっこ <　>（ブラケット braket）を割って量子力学用に考案した、「状態」を区別するための数学的に便利な記法で、その便利さから量子 computing では多用する。使わないで済ますこともできるが煩雑になる。なお、ここで量子力学における「状態」とは何かの解説は重要なので③から徐々に解説する。

⑥　<V> 「エンタングル状態」は量子 computing の中間到達点、その基礎である。これは「（複数の）状態が相関している」ことでさしあたり説明は十分である。統計学では「多変量解析」に対応する。量子 computing が速い理由もここにあり、決して並列処理ではない。

それ以上は実践には必要ない横道でありさしあたり飛ばしてよい。まず、アダマール行列と CNOT の定義と意味から入るのがよいが、次回とする。

＊　「もつれ」はある種の「団子状態」と言った方がイメージしやすいが、イメージに合わない場合もある。

⑦　「量子 programming」の入門解説本は多いが、本解説はまず実際の計算課題を目指し、後日、一例として RSA 公開鍵暗号の解読原理を解説する。

⑧　量子 computing はデータ計算の実践（量子データ解析、Quantum Data Analysis、QDA）を目的とする。IBM の Qiskit ソフトウェアが有益である。

⑨　読者が最小限の量子力学固有の現象理解を望むなら、電子スピンの例がよい。いくつかの好適な解説書があるが、それなりの心がけが必要である。

＊小出昭一郎『量子力学（I）』裳華房、**8.1** など

⑩　明確な目標を持ったストレートで地道な努力が必要であり、「物知り」やロマンティシズムでは達成はムリである。

QDA の基礎計算例（③、⑤関連）

[1] （古屋, p95）

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

固有値 $i, \ -i$

固有ベクトル $c\begin{pmatrix} 1 \\ i \end{pmatrix}, \ c\begin{pmatrix} i \\ 1 \end{pmatrix}$

[2] （同）

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

固有値 1 （二重根）

固有ベクトル $c\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

[3] Pauli の Spin 行列

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

固有値 1, -1

固有ベクトル $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

固有値 1, -1

固有ベクトル $\begin{pmatrix} 1 \\ i \end{pmatrix}, \begin{pmatrix} 1 \\ -i \end{pmatrix}$

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

固有値 1, -1

固有ベクトル $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

なお、交換関係 $[\sigma_x, \sigma_y] = \sigma_x \sigma_y - \sigma_y \sigma_x = i\sigma_z$ が成立（知らなくてもよい）

[4] アダマール行列（量子コンピューティング）

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

固有値 $\pm\sqrt{2}$

固有ベクトル

［５］　CNOT ゲート（量子コンピューティング）

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

解説は次回とします。 次回：「重ね合わせの原理」と「エンタングル状態」

なお RSA 公開鍵暗号の解読原理はフーリエ変換のあとになるので、２，３回後を予定しています。

、