量子コンピューティングⅠ

量子計算の基礎は初歩数理統計学

---確率現象に「不思議」はない一

(研究録　Do not　quote)

松原　　望*

＊森本栄一述

4. 量子ビット(qubits)と量子状態(quantum states)

4.4 量子状態（Quantum State）と状態空間（State Space）

量子状態「重ね合わせ」（Superposition）の一般形･･･ket ベクトルを用いる

$$|S\rangle = \beta_0 |E_0\rangle + \beta_1 |E_1\rangle \quad (4.1)$$

重ね合わせは量子 computing の中心概念で、その係数が重要な意味を持つ。

計算上の基底（Computational basis）によるなら

$$|S\rangle = a_0 |0\rangle + a_1 |1\rangle \quad (4.2)$$

列ベクトルによる表示

$$|S\rangle = a_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \quad (4.3)$$

偏光（Polarized light）による基底：h=horizontal, v=vertical

$$|S\rangle = a_0 |h\ell p\rangle + a_1 |v\ell p\rangle \quad (4.4)$$

*光子（photon）の例もあり

4.7 一般的な線形代数

$$\boldsymbol{B} = b_x\hat{x} + b_y\hat{y} \Rightarrow b_x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b_y \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b_x \\ b_y \end{pmatrix} \quad (4.5)$$

ベクトルの長さ B は「ノルム」とも云われ、次で定義、

$$\| \boldsymbol{B} \|^2 = B^2 = b_x^2 + b_y^2 \quad (4.6)$$

4.8 偏光に戻って

量子状態 $|S\rangle$ に対しても

$$\| |S\rangle \|^2 = a_h^2 + a_v^2 \quad (4.7)$$

$|S\rangle$ を測定する一般的物差しもないので、一応の共通基準として、規格化する

$$a_h^2 + a_v^2 = 1 \quad (4.8)$$

4.9 状態ベクトルの直交性･･･今後の数学上の発展課題

$$|B\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}, \quad |C\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \quad (4.9)$$

内積(B,C)を　bracket=bra〈と ket〉　と分解して、bra ベクトルを創成する(cf. P.Dirac)

$$\langle C \| B \rangle = \langle C \mid B \rangle = (c_0 \;\; c_1)\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = c_0 b_0 + c_1 b_1 \tag{4.10}$$

直交性も次の表示になる。

$$\langle C \mid B \rangle = c_0 b_0 + c_1 b_1 = 0 \tag{4.11}$$

排反的量子状態 $|0\rangle, |1\rangle$も直交性で表現される（確認）

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{4.12}$$

$A = a_0 |A_0\rangle + a_1 |A_1\rangle$に対しては

$$\langle A \mid A \rangle = (a_0 \;\; a_1)\begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = a_0^2 + a_1^2 \tag{4.13}$$

長さ 1 のベクトルが同方向なら次の様になるが一般には-1～1 の間になる

$$\langle C \mid B \rangle = c_0 b_0 + c_1 b_1 = 1 \tag{4.14}$$

5. 量子状態 $|S\rangle$の観測（Quantum Measurements）：確率

偏光の例をとる。

$$|S\rangle = a_h |h\ell p\rangle + a_v |v\ell p\rangle \tag{5.1}$$

偏光面の水平からの偏向角θとすると、強度は波形のエネルギーで振幅の 2 乗に比例し、各方向に分解し

$$I_{2h} = I_1 \cos^2\theta, \quad I_{2v} = I_1 \sin^2\theta \tag{5.2.3}$$

光子数の割合は確率

$$P_h = n_h/N, \quad P_v = n_v/N \tag{5.4.5}$$

と考えられる。当然

$$P_h + P_v = 1 \tag{5.6}$$

であり、結局 $|S\rangle$の規格化条件に合致することから

Postulate（前提）：$a_h^2 = P_h, \; a_v^2 = P_v$ (5.7)

と考えれば、重ね合わせ状態 $|S\rangle$の係数の観測上の意味（確率）がはっきりする。

6. 量子ゲートと量子回路

古典的論理ゲートと論理回路を量子的に読み替える

6.1 量子ゲート

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{6.1}$$

1 ビットの 2 状態 $(0,\ 1)$ をR^2の単位ベクトルで表現した場合、互いの反転（否定）の行列表現である。

$$NOT\,|\,0\,\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad NOT\,|\,1\,\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{6.2}$$

量子 computing では

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{6.3}$$

とも書かれる。

(6.4) skipped

もちろん

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{6.5}$$

続いて、パウリのスピン行列に似せて（本来、$i\ -i$ が入る）

$$Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{6.6}$$

と定義する。また、

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{6.7}$$

さし当り パウリ流に

$$\sigma_x = X, \quad \sigma_y = Y, \quad \sigma_z = Z \tag{6.8}$$

とおくが、詳しくは後日とする。

ちなみに

$$Z\,|\,1\,\rangle \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\,|\,1\,\rangle \tag{6.9}$$

$$Z\,|\,0\,\rangle \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \ \ |\,0\,\rangle \tag{6.10}$$

量子コンピューティングで非常に重要なのはいわゆる「アダマール・ゲート」で

$$\text{Hadamard Gate:} \quad H \Rightarrow \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{6.11}$$

$1/\sqrt{2}$は平方して確率 50-50 を生成し、$|\,0\,\rangle, |\,1\,\rangle$から 2 つの重要な重ね合わせ（アダマール基底）

$$H\,|\,0\,\rangle = \frac{1}{\sqrt{2}}\left\{|\,0\,\rangle + |\,1\,\rangle\right\} = |\,S_+\rangle = |\,+\,\rangle \tag{6.12}$$

$$H\,|\,1\,\rangle = \frac{1}{\sqrt{2}}\left\{|\,0\,\rangle - |\,1\,\rangle\right\} = |\,S_-\rangle = |\,-\,\rangle \tag{6.13}$$

が導く。さらに、重要な性質があり、一般に

$|\,\psi\,\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}$ に対し、

$$\begin{aligned} H\,|\psi\,\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha_0+\alpha_1\\ \alpha_0-\alpha_1\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}(\alpha_0+\alpha_1)\,|\,0\,\rangle + \frac{1}{\sqrt{2}}(\alpha_0-\alpha_1)\,|\,1\,\rangle\\ &= \alpha_0|\,S_+\rangle + \alpha_1|\,S_-\rangle \end{aligned} \tag{6.14}$$

という重ね合わせを生じる。詳しくは

英国版 *WIKIPEDIA* https://en.wikipedia.org/wiki/Hadamard_transform

6.3 X, H を連ねる。

$$|\,\psi_{HX}\,\rangle = XH\,|\,\psi\,\rangle,\quad |\,\psi_{XH}\,\rangle = HX\,|\,\psi\,\rangle \tag{6.15}$$

は行列表現では

$$XH = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix},\quad HX = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix} \tag{6.15.1}$$

(6.18) ～ (6.21) skipped

なお、 直交行列（ユニタリ行列）であって、

$$H'H = I \tag{6.22}$$

つまり、アダマール行列の中でも直交性

$$(\,1\;\;1\,)\begin{pmatrix}1\\ -1\end{pmatrix} = 0 \tag{6.23}$$

がある。

(6.24) skipped

以下にも注目する。 Hを 2 回重ねると、元の $|\,0\,\rangle$ が復元する：

$$\begin{aligned} H[\,H\,|\,0\,\rangle] &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\left[\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\ 0\end{pmatrix}+\begin{pmatrix}0\\ 1\end{pmatrix}\right)\right]\\ &= \frac{1}{2}\begin{pmatrix}2\\ 0\end{pmatrix}\\ &= \begin{pmatrix}1\\ 0\end{pmatrix}\\ &= |\,0\,\rangle \end{aligned} \tag{6.25}$$

関係は Hadamard 基底$|+\rangle|-\rangle$と計算基底$|\,0\,\rangle|\,1\,\rangle$の間の変換となっている。

6.6 観測は不可逆（さしあたり skipped）

$$M_0 = |\,0\,\rangle\langle\,0\,| \tag{6.26}$$

$$M_0\,|\,S\,\rangle = |\,0\,\rangle\langle\,0\,|\,S\,\rangle \tag{6.27}$$

9 （多）量子ビット：エンタングル（相関*）

* 数理統計学での表現、entanglement は「からみ」と訳されているが、語感に問題あり。

9.1 2 量子ビットと量子状態

確率論では

$$P(5\ and\ 表) = P(5)P(表) = (1/6)(1/2) = 1/12 \tag{9.1}$$

量子 computing では、2 量子ビットの状態$|S\rangle$は

$$|S\rangle = |A\rangle \otimes |B\rangle = |A\rangle\,|B\rangle \tag{9.2}$$

などと表記される（⊗ が正式）。重ね合わせの組の積なら、たとえば偏光とスピンの積では

$$|S\rangle = |A\rangle \otimes |B\rangle = \{a_0\,|h\ell p\rangle + a_1\,|v\ell p\rangle\} \otimes \{\beta_0\,|\uparrow\rangle + \beta_1\,|\downarrow\rangle\} \tag{9.3}$$

9.2 一般の 2 量子ビット状態

以上は、一般には

$$|0\rangle_A,\quad |1\rangle_A,\quad |0\rangle_B,\quad |1\rangle_B \tag{9.4}$$

の「積」の多項式だが、積の表示はさまざまで

$$|0\rangle_A \otimes |0\rangle_B = |0\rangle_A\,|0\rangle_B = |0_A\,0_B\rangle \quad \text{etc.} \tag{9.1}$$

とか、あるいは、スピン的表現では

$$|\uparrow\rangle_A\,|\uparrow\rangle_B \Leftrightarrow |\uparrow_A\,\uparrow_B\rangle \Leftrightarrow |00\rangle \Leftrightarrow (1\ 0\ 0\ 0)' \tag{9.2}$$

など一定していない。最後は 00～11 のうち‘1 番目’の意味のベクトル表示である。実は

「積」の定義：$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$ テンソル積（Kronecker 積） (9.5)

「テンソル」とは、「多数の添字がついた量」程度の意味で、それ以上の内容はない（cf. 微分幾何学）

9.3 2 量子ビット状態

一般には

$$\text{Superposition:}\quad |\psi\rangle = \sum a_x\,|x\rangle,\ \ x = 000\cdots0 \sim 2^n - 1 \tag{9.6}$$

はn量子ビット状態の重ね合わせで 2 ビットなら

$$|\psi\rangle = a_{00}\,|00\rangle + \cdots + a_{11}\,|11\rangle \tag{9.7}$$

なお、nビットの場合、{ }を用いて

$$|\psi\rangle = \text{Superposition: } |\psi\rangle = \sum a_x\,|x\rangle,\ \ x = 000\cdots0 \sim 2^{n-1} \quad = \{a_x\,|x\rangle\} \tag{9.8}$$

と略記する。

9.4 1 量子ビットとその積状態

1 量子ビットの積の例として

$|S\rangle =$ |偏光⟩|方向⟩|エネルギー⟩ (9.9)

2 量子ビットの重ね合わせの重ね合わせもあり、その例として

$|S\rangle = \frac{1}{\sqrt{2}}|v\ell p\rangle \otimes |$照射$C\rangle + \frac{1}{\sqrt{2}}|h\ell p\rangle \otimes |$照射$D\rangle$ (9.10)

9.5 量子エンタングル

2 量子ビットによる状態の一般表現は（スピン表示で）4 基底状態の重ね合わせで

$|S\rangle = c|\uparrow_A\uparrow_B\rangle + \cdots + f|\downarrow_A\downarrow_B\rangle$ (9.11)

もし、子の重ね合わせが、「因数分解」されて、

$$|S\rangle = c|\uparrow_A\uparrow_B\rangle + \cdots + f|\downarrow_A\downarrow_B\rangle$$
$$= \{g|\uparrow_A\rangle + h|\downarrow_A\rangle\}\{m|\uparrow_B\rangle + n|\downarrow_B\rangle\}\ (?) \quad (9.12)$$

と別々の積に分解されるなら、係数は

$c = gm,\ d = gn,\ e = hm,\ f = hn$ (9.13)

となっているが、c～fは制約の関係

$\therefore\ cf = de$ (9.14)

があるはずである。この場合 2 量子ビットとはいえ、別々 1 量子ビットが併記されているだけで、関係のない（エンタングルでない）状態となる。 確率論的には「独立性」に他ならない。

練習として、例えば、

$$|S_3\rangle = \frac{\sqrt{3}}{2}|\uparrow_A\downarrow_B\rangle + \frac{1}{2}|\uparrow_A\uparrow_B\rangle$$
$$= |\uparrow_A\rangle\left\{\frac{\sqrt{3}}{2}|\uparrow_B\rangle + \frac{1}{2}|\downarrow_B\rangle\right\} \quad (9.15.3)$$

はどうか（練習問題）

$c = \sqrt{3}/2,\ d = 1/2,\ e = f = 0$ だから

$cf = de = 0$

故にエンタングルではない（(9.18)～(9.21)は冗超な証明）。

一般に、重ね合わせ

$|\psi\rangle = a_{00}|\mathbf{00}\rangle + \cdots + a_{11}|\mathbf{11}\rangle$ (9.22)

で

$a_{00}a_{11} = a_{01}a_{10}$ (9.23)

のように等しいなら、エンタングルではない。ちなみに

$$|\psi\rangle = (a_0|\mathbf{0}\rangle + a_1|\mathbf{1}\rangle) \otimes (b_0|\mathbf{0}\rangle + b_1|\mathbf{1}\rangle)$$
$$= a_0 b_0|\mathbf{00}\rangle + \cdots + a_1 b_1|\mathbf{11}\rangle \quad (9.24)$$

で試してみよ。両辺とも$a_0 b_0 a_1 b_1$となる。

3 量子ビットの重ね合わせ状態

$$|\Phi\rangle = a_{000}|\mathbf{000}\rangle + a_{001}|\mathbf{001}\rangle \cdots + a_{111}|\mathbf{111}\rangle \tag{9.25}$$

が、1 量子ビットの積

$$|\Phi\rangle = (\alpha_0|\mathbf{0}\rangle + \alpha_1|\mathbf{1}\rangle) \otimes (\beta_0|\mathbf{0}\rangle + \beta_1|\mathbf{1}\rangle) \otimes (\gamma_0|\mathbf{0}\rangle + \gamma_1|\mathbf{1}\rangle) \tag{9.26}$$

になっているなら、正確に

$$a_{000}\,a_{111} = a_{001}a_{110} = a_{011}a_{100} = a_{101}a_{010} \tag{9.27}$$

がエンタングルでない条件である。

まとめ．エンタングルが多量子ビットの本来的効用のある状態で（統計学でいう多変量解析）、エンタングルでなければ 1 量子ビットが同時に扱われている trivial な場合にすぎない。

10. 量子回路（quantum circuit）と多量子ビット(multi-qubit)への応用

10.2　CNOT ゲート

2 量子ビットの次表を見てみよう。A, Bに対し、排他的論理和 XOR $A \oplus B$（2 進加法）が示されているが、これはAが$|0\rangle$のときBはそのまま、Aが$|1\rangle$のときはBは反転（NOT）するというに等しい。AがBを「制御」control する、あるいは数理統計学的には、Aの「条件付」conditional ということができる。

A	B	A	$A \oplus B$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

これを行列で

$$CNOT^* \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{10.1}$$

$* \ Controlled\ NOT\ (conditional\ NOT)$

で表す。実際、A, Bの表の行番号を 1～4 とすると 3↔4 の交換（Bの反転）が起こる：

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{10.2}$$

一般の n 量子ビットへの発展は

英国版 *WIKIPEDIA* https://en.wikipedia.org/wiki/Controlled_NOT_gate

注目すべきは、*CNOT* のエンタングル生成作用である。例えば

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

$$|B\rangle = |0_B\rangle \qquad (10.3)$$

の積はもちろんエンタングルではない。例えば、入力として

$$|S_{input}\rangle = \frac{1}{\sqrt{2}}\{|0_A\rangle + |1_A\rangle\}|0_B\rangle$$

$$= \frac{1}{\sqrt{2}}|0_A\rangle|0_B\rangle + \frac{1}{\sqrt{2}}|1_A\rangle|0_B\rangle \qquad (10.4)$$

であっても、CNOT 作用後では第 2 項でAによってBの反転が起り

$$|S_{output}\rangle = \frac{1}{\sqrt{2}}|0_A\rangle|0_B\rangle + \frac{1}{\sqrt{2}}|1_A\rangle|1_B\rangle \qquad (10.6)$$

$$(cf = 1/2,\ de = 0 \quad \therefore entangled)$$

となっている。

一般に *CNOT* は

$$CNOT\{c|00\rangle + d|01\rangle + e|10\rangle + f|11\rangle\}$$

$$= c|00\rangle + d|01\rangle + f|10\rangle + e|11\rangle \qquad (10.7)$$

のように作用し、最後の 2 項が交換される (|10⟩ ↔ |11⟩)。

まとめ このように$n = 10$の n量子ビットならa_0~a_{1023}の係数から成るエンタングル状態を作り出すことができる。$n = 20$さらに $n = 100,\ n = 1000,$…ならどうか？この量子ゲート、量子回路の機能はもし実装されれば空恐ろしいしい程度となる。**‘**量子コンピュータ**’**ができたとしても、それは「並列処理」によるものでない。

実装は途方もなく困難と言われる。電子のスピン上で実装するとしても、スピンのエネルギーは極めて小さいため、熱雑音からの SN 比を大きく確保するためには、device を絶対零度近くの超低温にに置く必要があるがそれでも保障の限りでなはい上、汎用的実装は当分無理であろう。Kurzweil も 2040 年代半ばの singularity でも幼児的段階と予想している。しかし、絶対的に不可能というわけではないので、到達不能な計算量に基づく RSA 暗号も、解読可能な計算力の前では解読される可能性がるある一方、むしろ暗号化に役立つかも知れない。RSA 暗号が解読可能となれば、今日のコンピュータ人類文明はたちどころに崩壊する。通信システムはすべて他者に明らかになってて効力を失い、、金融システムの安全性は地に落ち，経済取引は対面の物々交換の古代以前に戻り、サイバー化している世界安全保障システムは作用を完全停止し、古代文明の再現となる。はたしてどうだろうか。

以下 II へ（続）

文献 Flarend, B.Hilborn （2022） *Quantum Computing* Oxford

P.Dirac（1958） *The Principles Of Quantum Mechanics* Oxford

松原 望(2025)『入門 確率過程』（改訂版） 東京図書 （第４章)