

タイトル 量子計算理論

著者 森前智行

訳者

出版日 2017/11/14

出版社 森北出版

ISBN10 4627854013

ISBN13 9784627854017

ページ数 183

言語 ja

内容 従来のコンピュータのしくみと何がどう違うのか?なぜ速いのか?気鋭の若手研究者が基礎から最先端の話題までを幅広く解説.

版 1

刷 2

## 1 Tensor product

本書の p14 で与えられるテンソル積のルール以外に、次の式を仮定する。

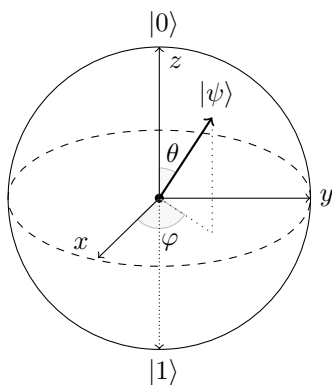
$$(|a\rangle\langle b|) \otimes (|c\rangle\langle d|) = |ac\rangle\langle bd|$$

さらに一般に (積が上手く定義できる時)

$$AB \otimes CD = (A \otimes B) \cdot (C \otimes D)$$

が言える。ここで  $\cdot$  は行列としての積を意味する。

## 2 Bloch Sphere



1bit の状態を考える。

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

とした時、 $\alpha$  と  $\beta$  は  $|\alpha|^2 + |\beta|^2 = 1$  を満たす任意の複素数なので、 $\alpha = ae^{i\kappa}$ ,  $\beta = be^{i\mu}$  ( $a \geq 0, b \geq 0$ ) とすると、 $a^2 + b^2 = 1$  より、 $a = \cos \frac{\theta}{2}$ ,  $b = \sin \frac{\theta}{2}$  ( $0 \leq \theta \leq \pi$ ) と書ける。

$$|\psi\rangle = e^{i\kappa} \cos \frac{\theta}{2} |0\rangle + e^{i\mu} \sin \frac{\theta}{2} |1\rangle$$

ここでフェーズだけが違う状態ベクトルは同一状態と見做すことを用いれば、 $e^{-i\kappa}$  を全体に掛けることができ、 $e^{i(\mu-\kappa)}$  を  $e^{i\varphi}$  とおけば、以下のようなものを考えても一般性を失わない。

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad (0 \leq \theta \leq \pi, 0 \leq \varphi \leq 2\pi)$$

以上より、 $|\psi\rangle$  と図に示した Bloch 球面上の点

$$(\cos \varphi \sin \frac{\theta}{2}, \sin \varphi \sin \frac{\theta}{2}, \cos \frac{\theta}{2})$$

が対応する。

例

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  を考えよう。

$$\begin{cases} \cos \frac{\theta}{2} &= \frac{1}{\sqrt{2}} \\ e^{i\varphi} \sin \frac{\theta}{2} &= \frac{1}{\sqrt{2}} \end{cases}$$

であるから、 $\theta = \frac{\pi}{2}, \varphi = 0$  を得る。したがって  $|+\rangle$  は  $x$  軸正の方向に位置することが分かる。

### 3 Questions

p6, 古典計算機の場合はベクトルの L1 ノルムが保存される—

- L1 ノルム  $x_1 + x_2$
- L2 ノルム  $x_1^2 + x_2^2$

p12, 演習問題, チューリングマシンで実際に足し算と—

motomu

p13, 演習問題, チューリングマシンのテープのビット列が—

motomu

p14, 古典計算機の状態は  $2^n$  次元線形空間の—ということもできる。

ここはテンソル積を知らなければ理解できない。基底の数を次元と言い、 $n$  次元線型空間と  $m$  次元線型空間のテンソル積  $V \otimes V$  は  $n \times m$  次元線型空間となる。

例

2 次元線型空間  $V$  の基底を  $e_1, e_2$  とするとき  $e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2$  は  $V \otimes V$  の基底となる。ここではこれら基底を  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  と書いている。2 ビットの古典計算機の状態は  $2^2$  次元線型空間の正規直交基底である！

p15, 演習問題, チューリングマシンが  $1+1$  を計算する様子を—

motomu

p15, 演習問題,  $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$  となることを—

成分を用いて計算すると

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

あるいは以下の表式から明らかである。

$$X = |1\rangle\langle 0| + |0\rangle\langle 1|$$

p16, 演習問題, 任意の  $a, b, c \in \{0, 1\}$  に対し、—

$$T|a, b, c\rangle = |a, b, c \oplus ab\rangle$$

$$T := (I \otimes I - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes X$$

$$\begin{aligned} T|a, b, c\rangle &= (I|a\rangle \otimes I|b\rangle - |11\rangle\langle 11|a, b\rangle) \otimes I|c\rangle + |11\rangle\langle 11|a, b\rangle \otimes X|c\rangle \\ &= |a, b, c\rangle + |11\rangle\langle 11|a, b\rangle \otimes (-|c\rangle + X|c\rangle) \end{aligned}$$

ここで  $a, b$  が 11 以外であれば後ろの項は落ちる。11 であれば

$$|11, c\rangle - |11, c\rangle + |11, \neg c\rangle = |11, \neg c\rangle$$

より言える。

p19, 演習問題, 上記の演算子を  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  に作用させて—

motomu

p19, 演習問題,—を表す  $3 \times 3$  の確率行列を書け.

motomu

p19, 演習問題,—も, この条件を必ず満たすことを示せ.

$\psi$  を  $w$  を用いて  $\sum_w c_w |w\rangle$  と書いておき、 $S|\psi\rangle$  を計算する。

$$S(\{p_{z',z}\}) := \sum_{z \in \{0,1\}^n} \sum_{z' \in \{0,1\}^n} p_{z',z} |z'\rangle \langle z|$$

であるから

$$\begin{aligned} S|\psi\rangle &= \sum_{z \in \{0,1\}^n} \sum_{z' \in \{0,1\}^n} \sum_{w \in \{0,1\}^n} p_{z',z} c_w |z'\rangle \langle z|w\rangle \\ &= \sum_{z, z', w} p_{z',z} c_w \delta_{zw} |z'\rangle \\ &= \sum_{z, z'} p_{z',z} c_z |z'\rangle \end{aligned}$$

ここで係数に注目すると、

$$\sum_z \left( \sum_{z'} p_{z',z} c_z \right) = \sum_z c_z \left( \sum_{z'} p_{z',z} \right) = \sum_z c_z = 1$$

より言えた。

p25, 演習問題,  $\{p_{z',z}\}_{z, z' \in \{0,1\}^n}$  が式 (3,1) を満たすなら—

p19 の演習問題と同様にして

$$U|\psi\rangle = \sum_{z'} \sum_z \underline{p_{z',z} c_z} |z'\rangle$$

を得る。下線部を新たに  $c_{z'}$  と看做して、 $\sum_{z'} |c_{z'}|^2 = 1$  を示せば良い。

$$\begin{aligned} \sum_{z'} |c_{z'}|^2 &= \sum_{z'} \sum_{\alpha} \sum_{\beta} p_{z',\alpha}^* c_{\alpha}^* p_{z',\beta} c_{\beta} \\ &= \sum_{\alpha, \beta} \delta_{\alpha\beta} c_{\alpha}^* c_{\beta} \\ &= \sum_{\alpha} |c_{\alpha}|^2 = 1 \end{aligned}$$

p25, よりシンプルな式と等価であることが分かる。

ユニタリー行列とは  $U^\dagger U = I$  を満たすような行列である。ここで  $\dagger$  はエルミート転置を表す<sup>\*1</sup>。行列  $A$  を  $(i, j)$  成分  $a_{ij}$  を用いて  $(a_{ij})$  と書くことがある。この記号を用いれば、 $A^\dagger = (a_{ji}^*)$  である<sup>\*2</sup>。したがって、

$$U^\dagger U = \left( \sum_k u_{ki}^* u_{kj} \right) = (\delta_{ij}) = I$$

である。演算子  $U$  の定義を用いて  $U^\dagger U$  を計算する。

$$\begin{aligned} U^\dagger U &= \sum_{\alpha \in \{0,1\}^n} \sum_{\beta \in \{0,1\}^n} p_{\alpha,\beta}^* |\beta\rangle \langle \alpha| \sum_{\alpha' \in \{0,1\}^n} \sum_{\beta' \in \{0,1\}^n} p_{\alpha',\beta'} |\alpha'\rangle \langle \beta'| \\ &= \sum_{\alpha,\beta,\alpha',\beta'} p_{\alpha,\beta}^* p_{\alpha',\beta'} \delta_{\alpha,\alpha'} |\beta\rangle \langle \beta'| \\ &= \sum_{\alpha,\beta,\beta'} p_{\alpha,\beta}^* p_{\alpha,\beta'} |\beta\rangle \langle \beta'| \end{aligned}$$

ここで式 (3.1) を用いると、

$$\begin{aligned} &= \sum_{\beta,\beta'} \delta_{\beta,\beta'} |\beta\rangle \langle \beta'| \\ &= \sum_{\beta} |\beta\rangle \langle \beta| = I \end{aligned}$$

逆に  $U^\dagger U = I$  を仮定すると

$$\sum_{\beta,\mu,\nu} p_{\beta,\mu}^* p_{\beta,\nu} |\mu\rangle \langle \nu| = I$$

を得るから、左から  $\langle \alpha|$  を右から  $|\gamma\rangle$  を掛けることで、式 (3.1) を導出することができる。

ちなみに  $\sum_{\beta} |\beta\rangle \langle \beta| = I$  であるが、1 ビットの具体例を計算して見るとよく分かる。

$$\sum_{\beta \in \{0,1\}} |\beta\rangle \langle \beta| \psi = (|0\rangle \langle 0| + |1\rangle \langle 1|)(c_0 |0\rangle + c_1 |1\rangle) = c_0 |0\rangle + c_1 |1\rangle = |\psi\rangle$$

p27, 演習問題, 以下が成り立つことを確認せよ。

$$|\psi\rangle = \sum_{y \in \{0,1\}^{n-1}} c_{1y} |1y\rangle + \sum_{y \in \{0,1\}^{n-1}} c_{0y} |0y\rangle$$

<sup>\*1</sup> 物理ではエルミート転置に  $\dagger$  を用いるが、数学では  $*$  を用いることが多い。エルミート共軛、エルミート随伴、エルミート共役、あるいは随伴行列とも呼ばれる。

<sup>\*2</sup> 物理では複素共役に  $*$  を用いるが、数学では  $\bar{\phantom{x}}$  のように上線で表すことが多い。

p35, 演習問題, パウリ演算子は以下の性質を満たすことを—

$$XX = (|1\rangle\langle 0| + |0\rangle\langle 1|)(|1\rangle\langle 0| + |0\rangle\langle 1|) = |0\rangle\langle 0| + |1\rangle\langle 1| = I$$

$$YY = (i|1\rangle\langle 0| - i|0\rangle\langle 1|)(i|1\rangle\langle 0| - i|0\rangle\langle 1|) = |0\rangle\langle 0| + |1\rangle\langle 1| = I$$

$$ZZ = (|0\rangle\langle 0| - |1\rangle\langle 1|)(|0\rangle\langle 0| - |1\rangle\langle 1|) = |0\rangle\langle 0| + |1\rangle\langle 1| = I$$

p35, 演習問題, またパウリ演算子の固有値、固有ベクトルを求めよ.

motomu

p35, 演習問題, さらに,  $n$  量子ビットパウリ演算子は掛け算について —

motomu

p35, 量子ゲートには, パウリゲートのほかに, アダマール (Hadamard) ゲートや—

p28 で導入された記号

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

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

を用いれば

$$H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$$

と書くことができる。

p36,  $R_{2/\pi} = Z^{1/2}$

$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$  を 2 乗すると  $Z$  になる。

p36, 一般に — コントロール U ゲート (controlled-U gate) と呼ばれる.

容易に示せるように

$$\Lambda(A)\Lambda(B) = \Lambda(AB)$$

である。

p36, CCZ ゲート — がよく使われる.

$I^{\otimes 2}$  を明示的に書くと、

$$\begin{aligned} I^{\otimes 2} &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01| + |11\rangle\langle 11| \end{aligned}$$

である。これを CCZ の定義に代入すると、

$$\begin{aligned} CCZ &:= (I^{\otimes 2} - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes Z \\ &= (|00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01|) \otimes I + |11\rangle\langle 11| \otimes Z \end{aligned}$$

を得る。この式を眺めると、CCZ の意味がはっきりと分かる。

また、 $\Lambda(U)$  に関しても同様の形に書き換えておこう。

$$\begin{aligned} \Lambda(U) &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U \\ &= (I - |1\rangle\langle 1|) \otimes I + |1\rangle\langle 1| \otimes U \end{aligned}$$

以上の議論からより高次の一般形についても容易に導出できる。

$$CCZ = |0\rangle\langle 0| \otimes I^{\otimes 2} + |1\rangle\langle 1| \otimes CZ$$

なお  $CCZ$  はこのようにかけることも注意しておく。

p37, 演習問題, CZ ゲートは、コントロールとターゲットを入れ替えても —

それぞれ計算する。

$$\begin{aligned} |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \end{aligned}$$

$$\begin{aligned} I \otimes |0\rangle\langle 0| + Z \otimes |1\rangle\langle 1| &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes |0\rangle\langle 0| + (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes |1\rangle\langle 1| \\ &= |00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01| - |11\rangle\langle 11| \end{aligned}$$

p37, 演習問題, また図 4,1(f) のように CX ゲートをコントロールと —

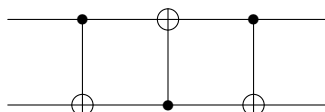


図 1 SWAP Gate

p16 で導入した記号  $\oplus$ (exclusive or) を用いると

$$\begin{aligned} CX |\psi\phi\rangle &= (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X) |a, b\rangle \\ &= \delta_{0a} |0b\rangle + \delta_{1a} |1\neg b\rangle \\ &= |a, a \oplus b\rangle \end{aligned}$$

が分かる。同様にコントロールとターゲットを入れ替えたものを  $CX'$  とすると、

$$CX' |a, b\rangle = |a \oplus b, b\rangle$$

が言える。これから、

$$CX'CX |a, b\rangle = |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle$$

ここで  $\oplus$  を 2 回取ると元に戻ることを使った。同様にすれば

$$CXCX'CX |a, b\rangle = |b, a\rangle$$

後は線型結合  $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$  などを考えれば言える。

p37, 演習問題, CCZ ゲートは、図 4.2 の回路と等価であることを確認せよ。

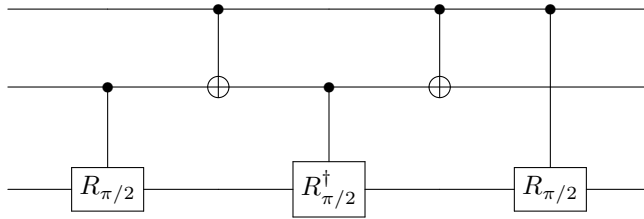


図 2 CCZ equivalent

最後のゲートを除いて先に計算する。

巻末に示した公式集において  $A = R_{\pi/2}, B = X, C = R_{\pi/2}^\dagger, D = X$  とすると、

$$\begin{aligned} &|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| D \otimes R_{2/\pi}^\dagger \\ &+ |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes I + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes R_{2/\pi} \end{aligned}$$

を得る。これに最後のゲート

$$|0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes I \otimes R_{2/\pi}$$

を掛ければ言える。

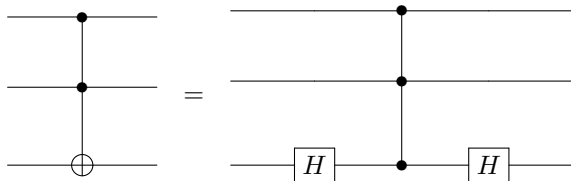


p38, 演習問題, 図 4.3 の回路において, 一番上の量子ビットを—

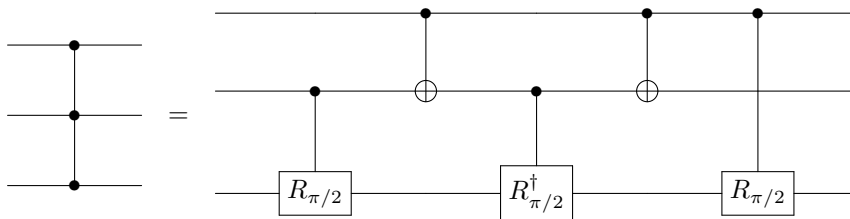
$$\frac{2 + \langle \phi | U \phi \rangle + \langle \phi | U^\dagger | \phi \rangle}{4}$$

## 4 Equivalent circuit

### 4.1 Toffoli



### 4.2 CCZ



## 5 Formula

$$5.1 \quad (I \otimes \Lambda(A))(\Lambda(B) \otimes I)$$

$$\begin{aligned} &|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| B \otimes I \\ &+ |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes A + |1\rangle\langle 1| \otimes |1\rangle\langle 1| B \otimes A \end{aligned}$$

$$5.2 \quad (I \otimes \Lambda(A))(\Lambda(B) \otimes I)(I \otimes \Lambda(C))(\Lambda(D) \otimes I)$$

$$\begin{aligned} &|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |0\rangle\langle 0| B|0\rangle\langle 0| D \otimes I \\ &+ |1\rangle\langle 1| \otimes |0\rangle\langle 0| B|1\rangle\langle 1| D \otimes C + |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes AC \\ &+ |1\rangle\langle 1| \otimes |1\rangle\langle 1| B|0\rangle\langle 0| D \otimes A + |1\rangle\langle 1| \otimes |1\rangle\langle 1| B|1\rangle\langle 1| D \otimes AC \end{aligned}$$