“量子コンピューターの頭の中”

＜第1章　量子コンピューターへのいざない＞

＜第2章　量子コンピューターの入門以前＞

要点整理

第1章　量子コンピュータへのいざない

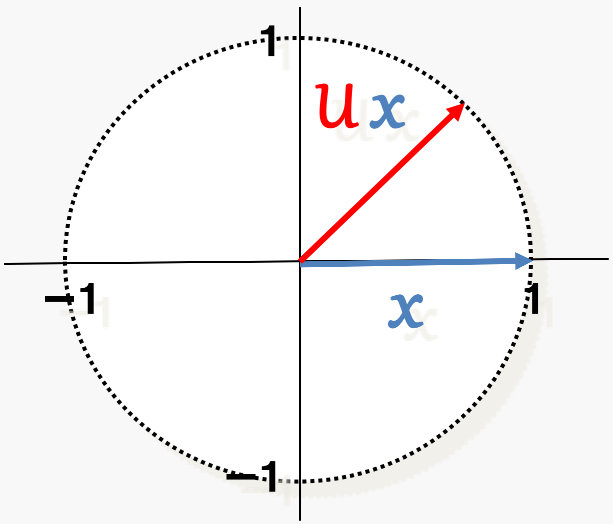
■量子ビット

ビット数	量子ビット
1量子ビット	｜0＞　｜1＞
2量子ビット	｜00＞　｜01＞　｜10＞　｜11＞

＊量子ビットのｎビットが同時にもてる値・・・２のｎ乗通り（古典ビットでは１通り）

■ユニタリ行列（unitary matrix）

・ベクトル（x)にかけても長さを変えない（x)行列（u）



第2章　量子コンピュータ入門以前

■量子コンピュータの計算で必要な数学

・行列・ベクトル
・確率
・複素数

■量子コンピュータにおける重要ワード

・ブラケット記法
・ユニタリ行列
・テンソル積

＊量子コンピュータは、どんなに複雑なアルゴリズムでも、**行列のかけ算を繰り返しているだけ**。行列の計算方法に慣れれば、怖がる必要はありません。

■行列の「行」と「列」・・・２（行）×２（列）行列（サイズ）

$$
\begin{array}{ll}
\text{第１行} & \multirow{2}{*}{$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$} \\
\text{第２行} &
\end{array}
\qquad\qquad
\begin{array}{cc}
\text{第１列} & \text{第２列} \\
\end{array}
\atop
\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}
$$

■ベクトルの定義

・成分・・・行列に並べられた数字（上記・・1,2,3,4）
・サイズ・・・ｍ（行）×ｎ（列）
・正方行列・・・行と列の大きさが同じ（ｎ×ｎ）
・行ベクトル・・・行が１つの行列
・列ベクトル・・・列が１つの行列

＊ベクトルの長さ・・・ベクトルの各成分を２乗したものの和に対して平方根をとった値

第2章　量子コンピュータ入門以前

■行列の和・差

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

“:=”「左辺(新しい概念の数式)を右辺(既知の数式)で定義する」

・(和)

$$A+B := \begin{pmatrix} 1+2 & 1+2 \\ 1+2 & 1+2 \end{pmatrix}$$

・(差)

$$A-B := \begin{pmatrix} 1-2 & 1-2 \\ 1-2 & 1-2 \end{pmatrix}$$

行列の(和)、(差)を
使うところってある？

＊サイズの合わない行列は、和・差を定義出来ない！

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 3 & 3 \end{pmatrix} \quad A+B := \begin{pmatrix} 1+2 & 1+2 \\ 1+2 & 1+2 \\ ?+3 & ?+3 \end{pmatrix}$$

第2章　量子コンピュータ入門以前

■行列とベクトルの積

$$A=\begin{pmatrix}1 & 1\\ 1 & 1\\ 1 & 1\end{pmatrix}\quad v=\begin{pmatrix}2\\ 2\end{pmatrix}$$

ベクトル：列がひとつの行列

・（積）

$$A*v:=\begin{pmatrix}1*2+1*2\\ 1*2+1*2\\ 1*2+1*2\end{pmatrix}$$

＊「行列の列数」と「ベクトルのサイズ」が異なると定義できないｂ

$$A=\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}\quad v=\begin{pmatrix}2\\ 2\end{pmatrix}\quad A+v=\begin{pmatrix}1*2+\cancel{1*2}+1*?\\ 1*2+\cancel{1*2}+1*?\end{pmatrix}$$

第2章　量子コンピュータ入門以前

■行列と行列の積

$$A=\begin{pmatrix}1 & 1\\ 1 & 1\\ 1 & 1\end{pmatrix} \quad v=\begin{pmatrix}2 & 2\\ 2 & 2\end{pmatrix}$$

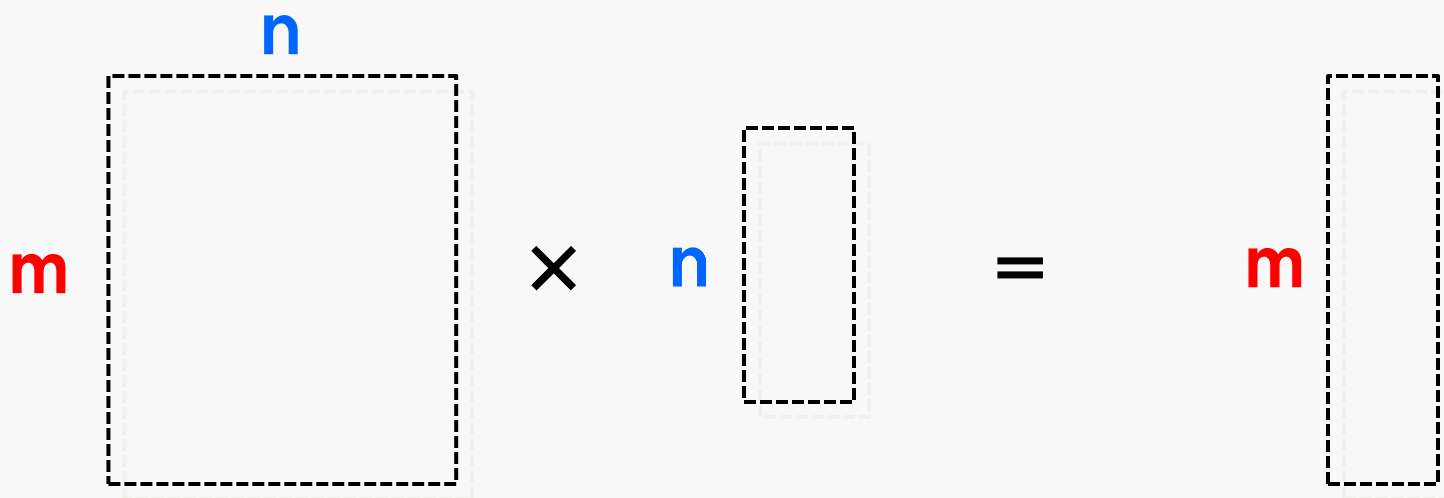
・（積）$A*v:=\begin{pmatrix}1*2+1*2 & 1*2+1*2\\ 1*2+1*2 & 1*2+1*2\\ 1*2+1*2 & 1*2+1*2\end{pmatrix}$

但し$v*A:=$ $\begin{pmatrix}2 & 2\\ 2 & 2\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 1\\ 1 & 1\end{pmatrix}$

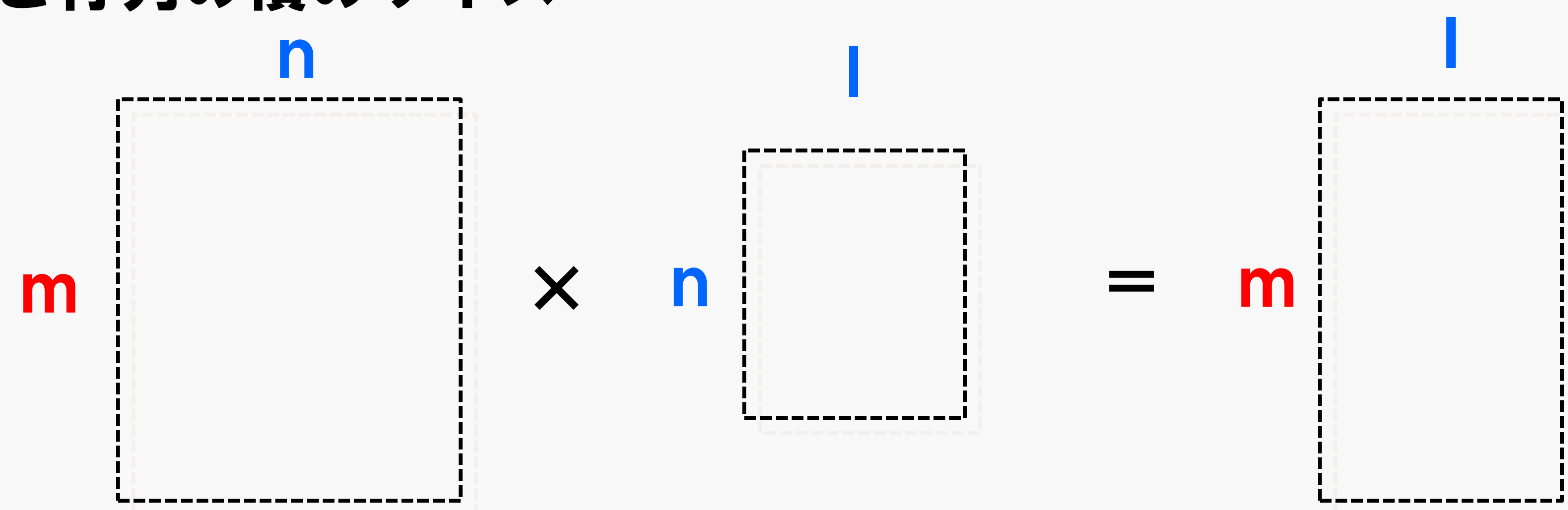
＊「行列の列数」と「行列のサイズ」が異なると定義できない

$$\begin{pmatrix}2*1+2*1+?*1 & 2*1+2*1+?*1\\ 2*1+2*1+?*1 & 2*1+2*1+?*1\end{pmatrix}$$

■行列とベクトルの積のサイズ



■行列と行列の積のサイズ



第2章　量子コンピュータ入門以前

■分配法則

（１）左分配法則

A,B,C を $A+B,AC,B+C$ が計算できるサイズの行列とすると

$A(B+C) = AB + AC$

（１）右分配法則

A,B,C を $AC,AC,A+B$ が計算できるサイズの行列とすると

$(A+B)C = AC + BC$

■行列とベクトルの積のサイズ

法則		実数	行列	定理
結合法則	（A＋B）＋C ＝ A＋（B＋C）	成り立つ	成り立つ	和の結合法則
	（AB）C ＝ A(BC)	成り立つ	成り立つ	積の結合法則
交換法則	A＋B ＝ B＋A	成り立つ	成り立つ	和の交換法則
	AB ＝ BA	成り立つ	成り立たない	
分配法則	A（B＋C） ＝ AB＋AC	成り立つ	成り立つ	左分配法則
	（A＋B）C ＝ AC＋BC	成り立つ	成り立つ	右分配法則

■単位行列

・単位行列 (identity matrix)・・・n 次正方行列で
「行と列が同じ成分が１で、行と列が異なる成分が０」

$$I_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

$n=2$　　$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$n=3$　　$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

■正規行列

・正規行列 (reguiar matrix)・・・n 次正方行列Ａに対し以下の２つの条件を満たすｎ次正方行列Ｂが存在する時の行列Ａ

$$AB = I_n \text{ , } BA = I_n$$

第2章　量子コンピュータ入門以前

■逆行列

・逆行列 (inverse matrix)・・・n 次正方行列 A に対し、
$AB=I_n$, $BA=I_n$ を満たす n 次正方行列 B が存在する時の
行列Bを Aの逆行列といい A^{-1} と書く

・ $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の場合、逆行列 $A^{-1}=\dfrac{1}{ad-bd}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

＊ $ad-bc=0$ のときは逆行列は存在しない。
$ad-bc\neq 0$ のときのみ逆行列は存在する。

$$AA^{-1}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I_n$$

$$A^{-1}A=\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I_n$$

■集合（ものの集まり）

・外延的記法・・・集合を構成しているものをすべて列挙

{１，２，３，４，５}

・内延的記法・・・集合を構成しているものの性質を記述

{ｎ｜ｎは１から５までの自然数}

「｜」の左は集合を構成している変数、「｜」の右は集合を構成しているものの性質

■要素（elemennt）・・集合を構成するひとつひとつのもの

・「１が{1,2,3,4,5}の要素である」

$1 \in \{1,2,3,4,5\}$

・「６が{1,2,3,4,5}の要素でない」

$6 \notin \{1,2,3,4,5\}$

・「集合が{1,2,3}は {1,2,3,4,5}に含まれる」

$\{1,2,3\} \subset \{1,2,3,4,5\}$

■よく使う集合の記号

$\mathbb{N}$:= 自然数(natural number)全体の集合 {1,2,3}
$\mathbb{Z}$:= 整数(integer)全体の集合 {...,−3,−2,−1,0,1,2,3..}
$\mathbb{R}$:= 実数(real number)全体の集合 {1, π ,$\sqrt{2}$}
$\mathbb{C}$:= 複素数(complex number)全体の集合 {1,i,1+$\sqrt{2}$i}

＜上記集合は包含関係がある＞

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$

■積集合・・・複数の集合の組(tuple)を表す集合

- $\mathbb{R} \times \mathbb{R}$ 又は $\mathbb{R}^2$ ・・・積集合の要素は（1,0）
- コンピュータの世界はビットを０，１で表す

１ビットの集合・・・ $\{0,1\}$
ｎビットの集合・・・ $\{0,1\}^n$
２ビットの集合の要素
$(0,0),(0,1),(1,0),(1,1) \in \{0,1\}^2$

■複素数

- 虚数単位 (imaginary unit) 「i」・・・２乗すると－１

$$i^2 = -1$$

- 複素数 (complex number)

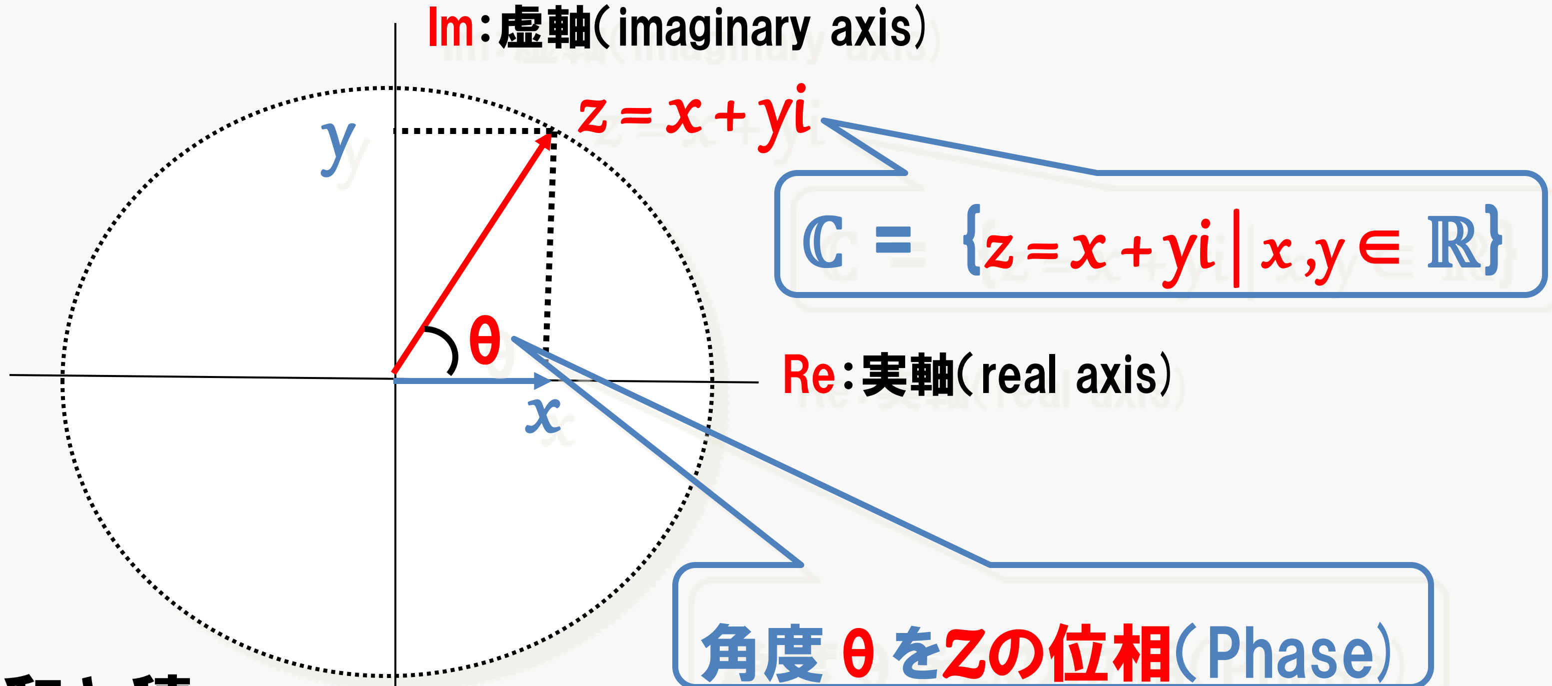
  ・・・２つの実数x、yと虚数単位 i で表せる数

$$x + yi$$

$$z = x + yi \ (x, y\text{は実数})$$

x を実部 (real part) ･･･Re(z)
y を虚部 (imaginary part) ･･･Im(z)

■複素平面 (complex plane)



■複素数の和と積

$z_1 = x_1 + y_1 i$（x_1, y_1は実数）

$z_2 = x_2 + y_2 i$（x_2, y_2は実数）

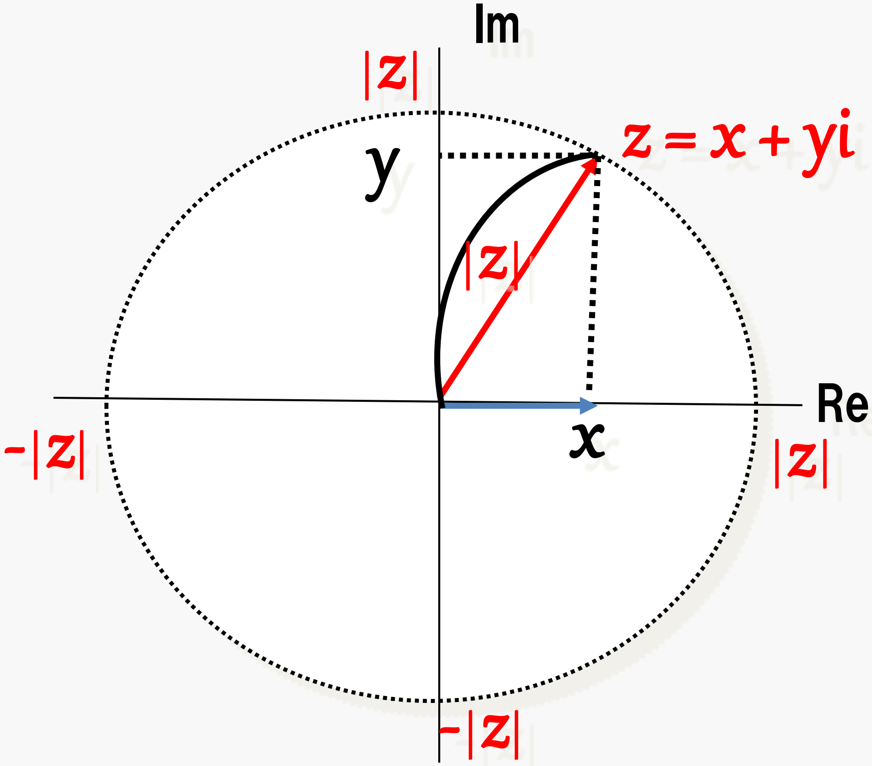
- （和）$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i$
- （積）$z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i$

■絶対値・・・複素数の大きさ（複素平面の原点からの距離）

$$|z| = \sqrt{x^2 + y^2}$$

$$|z| \geq 0$$

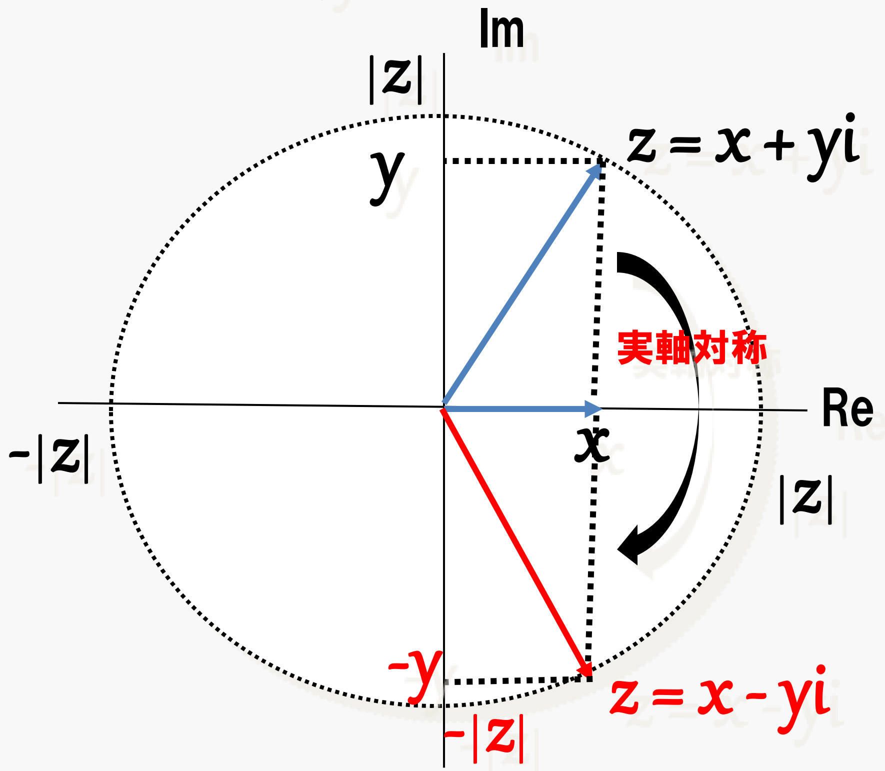
■複素数の絶対値



■複素共役 (complex conjugate)・・・y の符号を変更

$z = x + yi$ (x,yは実数)

$z^* := x - yi$



■転地行列と随伴行列

＊実行列 (real matrix)・・行列の成分が実数であるもの
＊複素行列 (complex matrix)・・行列の成分が複素数であるもの

①転置行列 (transposed matrix)

・・・行列Aの行と列を入れ替えた行列

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}^T=\begin{pmatrix}1 & 3\\ 2 & 4\end{pmatrix}\qquad \begin{pmatrix}1\\ 2\end{pmatrix}^T=\begin{pmatrix}1 & 2\end{pmatrix}$$

＊　m X n 行列の転置行列はm X n 行列

$(a_{ij})^T=(a_{ji})$ となります

②複素共役行列 (complex conjugate of a matrix)

・・・行列Aの各成分を複素共役にした行列

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}^*=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\qquad \begin{pmatrix}\sqrt{5} & 2\\ i & 3+i\end{pmatrix}^*=\begin{pmatrix}\sqrt{5} & 2\\ -i & 3-i\end{pmatrix}$$

$\boxed{(a_{ij})^*=(a^*_{ij})\text{ となります}}$

第2章　量子コンピュータ入門以前

■随伴行列

①随伴行列(adjoint matrix)=エルミート行列

・・・「複素共役して転置した行列」$(A^*)^T$と

「転置して複素共役した行列」$(A^T)^*$は同じ

$$A^\dagger := (A^*)^T = (A^T)^*$$

ダガー(dagger)

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}^\dagger = \begin{pmatrix}1&3\\2&4\end{pmatrix}$$

$$\begin{pmatrix}\sqrt{5}&2\\i&3+i\end{pmatrix}^\dagger = \begin{pmatrix}\sqrt{5}&-i\\2&3-i\end{pmatrix}$$

$(a_{ij})^\dagger = (a^*_{ji})$ となります

■ユニタリー行列

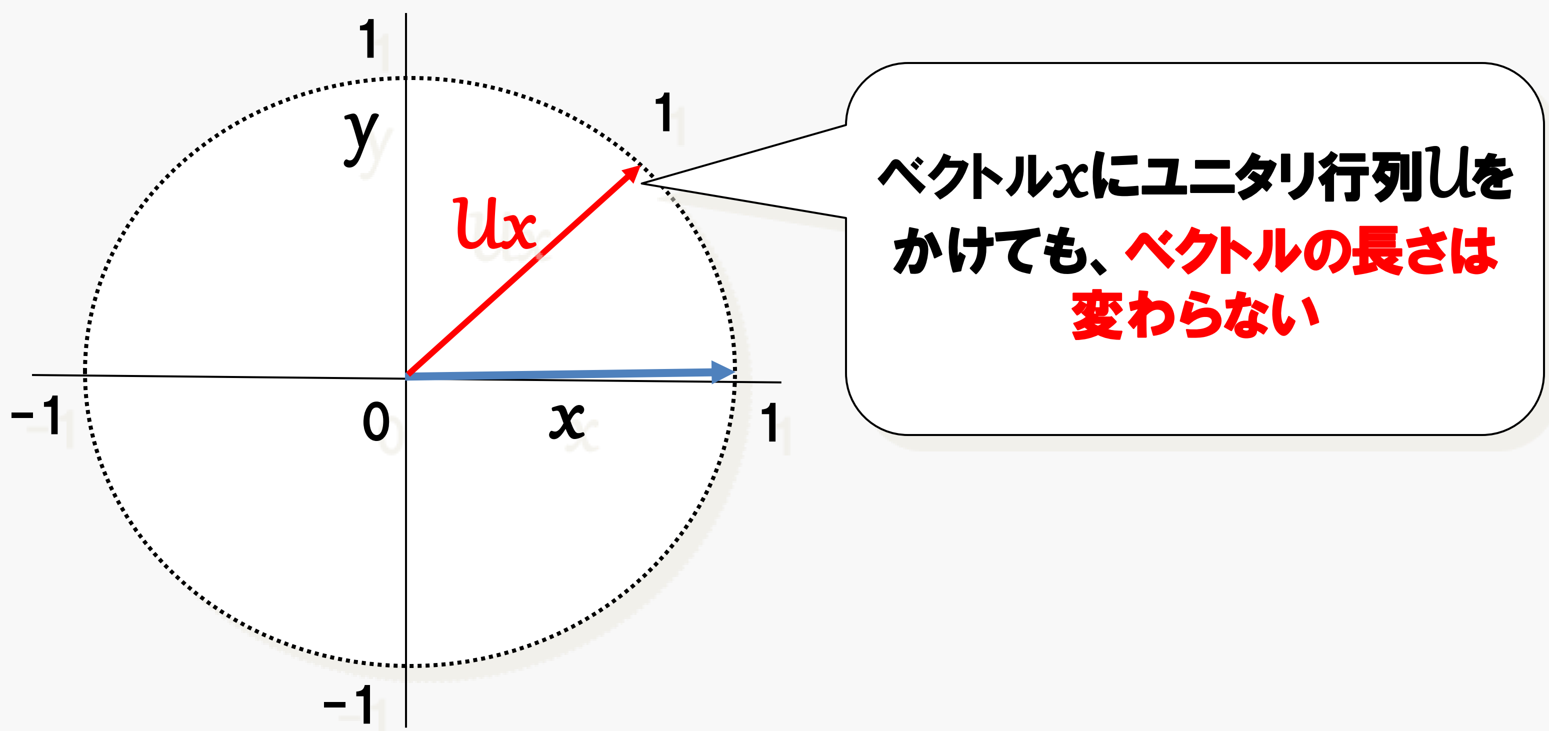
①ユニタリー行列(unitary matrix)

・・・随伴行列が逆行列となる正方行列U

単位行列

$$U^{\dagger}U = I、\ UU^{\dagger} = I、\ U^{\dagger} = U^{-1}$$

＊ 上記3個の式のどれか一個でも成り立てば他の2個も成り立つ



第2章　量子コンピュータ入門以前

■ユニタリー行列・・・随伴行列が逆行列となる正方行列

$u^\dagger u = I$ （単位行列）

ユニタリー行列	$u^\dagger$	u	$u^\dagger u$	I

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1\ast1+0\ast0 & 1\ast0+0\ast1 \\ 0\ast1+1\ast0 & 0\ast0+1\ast1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

“i”を二乗すると“−1”

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} : \quad \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0\ast0+-i\ast i & 0\ast-i+-i\ast0 \\ i\ast0+0\ast i & i\ast-i+0\ast0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1\ast1+0\ast0 & 1\ast0+0\ast-1 \\ 0\ast1+(-1\ast0) & 0\ast0+(-1\ast-1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} : \quad \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\ast\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}\ast\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\ast\frac{-1}{\sqrt{2}}+\frac{1}{\sqrt{2}}\ast\frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}}\ast\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}\ast\frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}}\ast\frac{-1}{\sqrt{2}}+\frac{1}{\sqrt{2}}\ast\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

第2章　量子コンピュータ入門以前

■ブラケット記法

- 量子力学では、列ベクトル　ϕ（ファイ）＝ $\begin{pmatrix} a1 \\ a2 \end{pmatrix}$ ➡ ｜ϕ＞
- 記号 “｜ ＞” ケット(ket)・・列ベクトル

- 記号 “＜ ｜” ブラ(bra)・・ケットの随伴行列（行ベクトル）

$$\langle \phi | := | \phi \rangle^{\dagger} = (a_1^{*} \; a_2^{*})$$

$$*|\phi\rangle = \begin{pmatrix} 1+2i \\ 3+4i \end{pmatrix} \text{の場合}$$

$$\langle \phi | = | \phi \rangle^{\dagger} = \begin{pmatrix} 1+2i \\ 3+4i \end{pmatrix}^{\dagger} = (1-2i \;\; 3-4i)$$

複素共役・・・複素数の符号を返納

転置・・・m、n行列 → n, m行列

■内積 (inner product) の定義

読み方:ファイ　読み方:ファイ　複素数

・$|\phi\rangle = \begin{pmatrix} a1 \\ a2 \end{pmatrix}$, $|\Psi\rangle = \begin{pmatrix} b1 \\ b2 \end{pmatrix} \in \mathbb{C}^2$

＊・・・複素共役

＊内積　$\langle\phi,\Psi\rangle := \begin{pmatrix} a1^* & a2^* \end{pmatrix} \begin{pmatrix} b1 \\ b2 \end{pmatrix} = a1^*\, b1 + a2\ b2^* \in \mathbb{C}$

＊　$|\phi\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}$, $|\psi\rangle = \begin{pmatrix} 1+i \\ 2 \end{pmatrix}$ の場合

$$\langle\phi\ \psi\rangle = \begin{pmatrix} 1^* & i^* \end{pmatrix} \begin{pmatrix} 1+i \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & -i \end{pmatrix} \begin{pmatrix} 1+i \\ 2 \end{pmatrix} = 1 - i$$

■内積(inner product)の定理

$\phi, \phi 1, \phi 2$と$\psi, \psi 1, \psi 2$をベクトルとし、Zを複素数とする。
このとき、次の式が成り立つ。

(1) $\langle \phi 1+\phi 2|\psi\rangle = \langle \phi 1|\psi\rangle+\langle \phi 2|\psi\rangle$
(2) $\langle \phi|\psi 1+\psi 2\rangle = \langle \phi|\psi 1\rangle+\langle \phi|\psi 2\rangle$
(3) $\langle z\phi|\psi\rangle = z^*\langle \phi|\psi\rangle$ （前に出したZが複素共役になる点に注意）
(4) $\langle \phi|z\psi\rangle = z\ \langle \phi|\psi\rangle$
(5) $\langle \phi|\psi\rangle = \langle \psi|\phi\rangle^*$ （順番を入れ替えると複素共役になる）
(6) $\langle \phi|\phi\rangle \geq 0$であり、$|\phi\rangle = 0$のときに限り$\langle \phi|\phi\rangle=0$になる

複素数zが$|z|=1$を満たすとする。
このとき、以下の式が成り立つ。

$$|\langle \phi|Z\psi\rangle|^2 = |\langle \phi|\psi\rangle|^2$$

■テンソル積 (tensor product) の定義・・・２量子ビット以上

- m x n行列A= (a_{ij}) とr x s行列Bに対してmr x rS行列$A\otimes B$

読み方:テンソル

$$A\otimes B := \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

$$C = \begin{pmatrix} 1 \\ 2 \end{pmatrix},\ D = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$ の場合

$$C\otimes D = \begin{pmatrix} 1\ D \\ 2\ D \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 3 \\ 4 \end{pmatrix} \\ 2\begin{pmatrix} 3 \\ 4 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$$

行列サイズは　2x1行列Cと2x1行列Dより2・2 X 1・1 ＝ 4 X 1行列

第2章　量子コンピュータ入門以前

■テンソル積 (tensor product) の定理

A,A1,A2 を*m x n* 行列、*B,B1,B2* を*n x n* 行列、Zを複素数とする。
このとき、次の式が成り立つ。

(1) $A \otimes (B1 + B2) = A \otimes B1 + A \quad B2$

(2) $(A+A2) \otimes B = A1 \otimes B + A2 \otimes B$

(3) $(zA) \otimes B = A \otimes (zB) = z(A \otimes B)$

(4) $(A1 \otimes B1)(A2 \otimes B2) = A1A2 \otimes B1B2$

(5) $(A \otimes B)^{\dagger} = A^{\dagger} \otimes B^{\dagger}$

(6) A^{-1}, B^{-1} が存在するとき、$(A \otimes B)^{-1} = A^{-1} \otimes B$

(7) $Im \otimes In = Imn$（サイズ*m* の単位行列とサイズ*n* のテンソル積は、サイズ*mn* の単位行列になる）

$\otimes$ はテンソル積を表し、記号を省略している積は通常の行列積を表す

■古典回路における真理値表

＊ ANDの演算

A	*B*	*A* AND *B*
0	0	0
0	1	0
1	0	0
1	1	1

かけ算と同じ演算
論理積（*A*・*B*）

＊ ORの演算

A	*B*	*A* AND *B*
0	0	0
0	1	1
1	0	1
1	1	1

足し算と同じ演算
論理和（*A*+*B*）

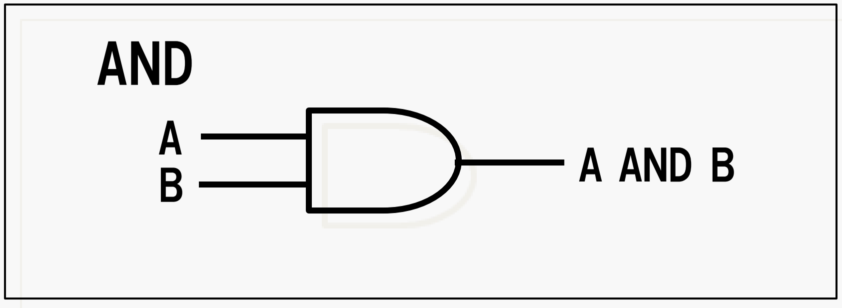
＊ NOTの演算

A	*B*
0	1
1	0

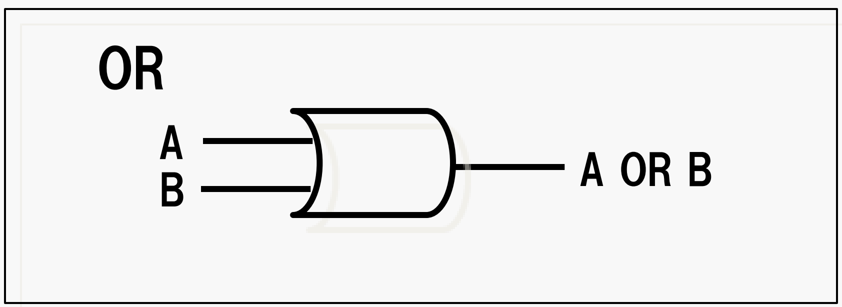
ビットを反転させる演算
（0と1を入れ替え）

■古典回路におけるゲート

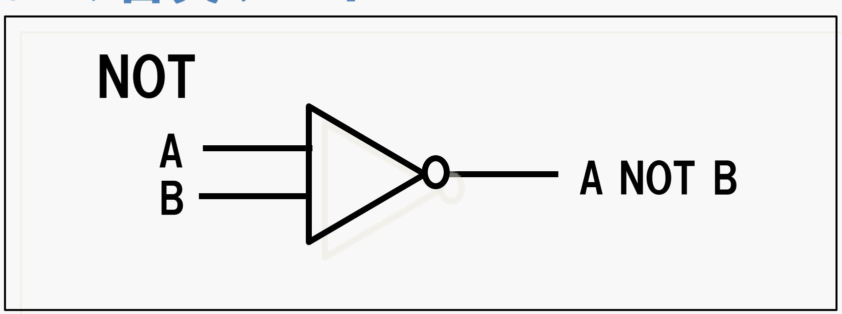
＊ ANDの古典ゲート



＊ ORの古典ゲート

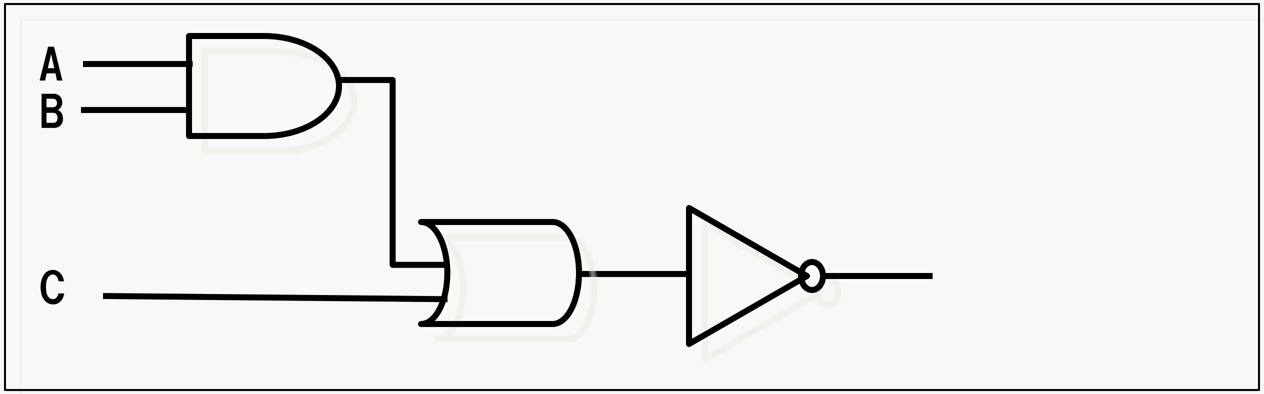


＊ NOTの古典ゲート



■半加算器・・・２個の１ビットデータの足し算

＊ NOT ((*A* AND *B*) OR *C*) を表す回路

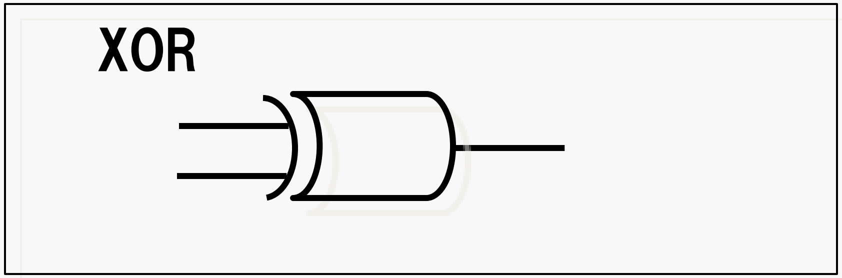


＊ 半加算器の真理値表と対応する計算

入力1	入力2	出力1	出力2	対応する計算
0	0	0	0	*0 + 0 = 00*
0	1	0	1	*0 + 1 = 01*
1	0	0	1	*1 + 0 = 01*
1	1	1	0	*1 + 1 = 10*

■半加算器・・・２個の１ビットデータの足し算

＊ XORの古典ゲート



＊ XORの演算・・・**排他的論理和** (exclusive or)

A	*B*	*A AND B*
0	0	0
0	1	1
1	0	1
1	1	0

＊ XORを利用して簡素化した半加算器の古典回路