A single qubit

Ryuhei Mori

Tokyo Institute of Technology

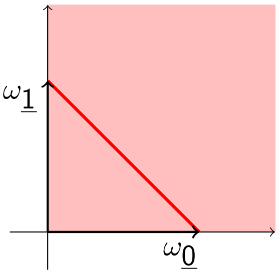
5, Oct., 2020

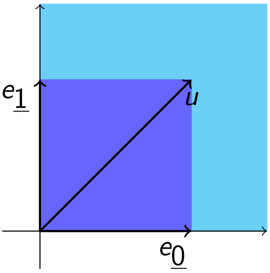
A single bit

Let $u := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

- Set of states $= \left\{\omega \in \mathbb{R}^2 \mid \omega \in C_{\geq 0}, \langle u, \omega \rangle = 1\right\}$.

- Set of binary measurements $=$ $\left\{e \in \mathbb{R}^2 \mid e \in C_{\geq 0}, u - e \in C_{\geq 0}\right\}$.



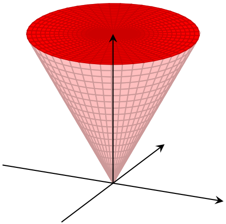


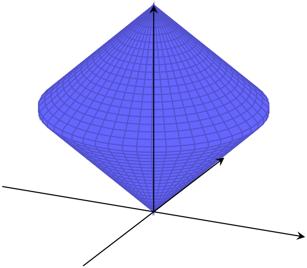
A single qubit

Let $u := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\langle e, \omega \rangle := \mathrm{Tr}(e\omega)$.

- Set of states $= \{\omega \in V \mid \omega \in C_{\succeq 0}, \langle u, \omega \rangle = 1\}$.

- Set of binary measurements $=$ $\{e \in V \mid e \in C_{\succeq 0}, u - e \in C_{\succeq 0}\}$.





A single qubit

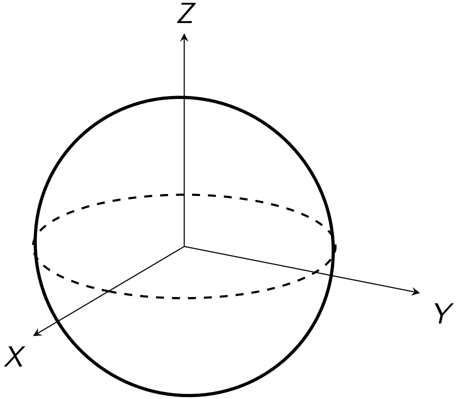
- A qubit can be represented by

$$\rho = \frac{1}{2}\left(I + r_X X + r_Y Y + r_Z Z\right)$$

for $[r_X\ r_Y\ r_Z] \in \mathbb{R}^3$ satisfying $r_X^2 + r_Y^2 + r_Z^2 \leq 1$.

- A qubit can be represented by a point $[r_X\ r_Y\ r_Z]$ in a three-dimensional sphere of radius 1.

The Bloch sphere



Complex space and Hermitian operator

- $\mathcal{X}$: A finite-dimensional inner product space on $\mathbb{C}$.
- $\mathcal{L}(\mathcal{X})$: A set of linear operators on $\mathcal{X}$.

For $A \in \mathcal{L}(\mathcal{X})$, an adjoint map $A^\dagger$ of A is a unique operator satisfying

$$\langle v, Aw \rangle = \langle A^\dagger v, w \rangle$$

for any $v, w \in \mathcal{X}$. $H \in \mathcal{L}(\mathcal{X})$ is Hermitian if and only if $H^\dagger = H$.

- $\mathcal{H}(\mathcal{X})$: A set of Hermitian operators on $\mathcal{X}$.

$\mathcal{L}(\mathcal{X})$ and $\mathcal{H}(\mathcal{X})$ are often regarded as inner product space on $\mathbb{C}$ and $\mathbb{R}$, respectively for the Hilbert–Schmidt inner product $\langle A, B \rangle = \mathrm{Tr}(A^\dagger B)$.

Spectral decomposition theorem

Definition (Normal operator)

$A \in \mathcal{L}(\mathcal{X})$ is said to be normal if $AA^\dagger = A^\dagger A$.

Hermitian matrix ($H^\dagger = H$) and unitary matrix ($UU^\dagger = I$) are normal.

Theorem (Spectral decomposition theorem)

$A \in \mathcal{L}(\mathbb{C}^n)$ is normal if and only if there exist orthonormal basis $\{|\psi_j\rangle\}$ of $\mathbb{C}^n$ and complex numbers $\{\lambda_j\}$ such that

$$A = \sum_j \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right|.$$

Pauli matrices

- $$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix}$$

- $$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \end{bmatrix} - \frac{1}{2} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \begin{bmatrix} 1 & -1 \end{bmatrix}$$

- $$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \end{bmatrix} \begin{bmatrix} 1 & -i \end{bmatrix} - \frac{1}{2} \begin{bmatrix} 1 \\ -i \end{bmatrix} \begin{bmatrix} 1 & i \end{bmatrix}$$

Braket notation

$$|0\rangle := \begin{bmatrix}1\\0\end{bmatrix}, \qquad |1\rangle := \begin{bmatrix}0\\1\end{bmatrix}$$

$$\begin{aligned} |+\rangle &:= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, & |-\rangle &:= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

for $|\alpha|^2 + |\beta|^2 = 1$.

$$\langle\psi| = |\psi\rangle^\dagger = \alpha^*\,\langle 0| + \beta^*\,\langle 1| = \begin{bmatrix}\alpha^* & \beta^*\end{bmatrix}$$

Pauli matrices in braket notation

- $$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle \langle 0| - |1\rangle \langle 1|$$

- $$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |+\rangle \langle +| - |-\rangle \langle -|$$

- $$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \end{bmatrix} \begin{bmatrix} 1 & -i \end{bmatrix} - \frac{1}{2} \begin{bmatrix} 1 \\ -i \end{bmatrix} \begin{bmatrix} 1 & i \end{bmatrix}$$

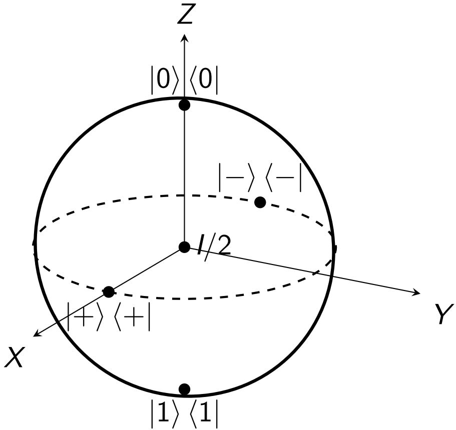
Special states

$$\rho = \frac{1}{2}\left(I + r_X X + r_Y Y + r_Z Z\right)$$

$$r_X^2 + r_Y^2 + r_Z^2 \leq 1.$$

Coordinate	State
$[0\ 0\ 0]$	$\frac{1}{2}I$
$[1\ 0\ 0]$	$\frac{1}{2}(I+X) = \|+\rangle\langle+\|$
$[-1\ 0\ 0]$	$\frac{1}{2}(I-X) = \|-\rangle\langle-\|$
$[0\ 0\ 1]$	$\frac{1}{2}(I+Z) = \|0\rangle\langle0\|$
$[0\ 0\ -1]$	$\frac{1}{2}(I-Z) = \|1\rangle\langle1\|$

Special states in the Bloch sphere



Pure states are rank-1 density operators

ρ is a pure state

$\overset{\text{def}}{\Longleftrightarrow}$ $\rho \neq p\rho_1 + (1-p)\rho_2 \quad \forall p \in (0,1)$ and states $\rho_1 \neq \rho_2$.

Lemma

A quantum state ρ is a pure state if and only if ρ is rank-1.

Proof.

Let the spectral decomposition of ρ be

$$\rho = \sum_j \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right|$$

where $\lambda_j \geq 0$ and $\sum_j \lambda_j = 1$. If ρ is not rank-1, ρ is a convex combination of quantum states $(\left|\psi_j\right\rangle\left\langle\psi_j\right|)_j$.
Assume $\rho = \left|\varphi\right\rangle\left\langle\varphi\right|$ and $\rho = p_1\rho_1 + p_2\rho_2$. $\mathrm{Tr}(\sigma\left|\varphi\right\rangle\left\langle\varphi\right|) = 1$ if and only if $\sigma = \left|\varphi\right\rangle\left\langle\varphi\right|$ since $\mathrm{Tr}(\sigma\left|\varphi\right\rangle\left\langle\varphi\right|) = \left\langle\varphi\right|\sigma\left|\varphi\right\rangle = \sum_j \lambda_j \left|\left\langle\psi_j|\varphi\right\rangle\right|^2$. Then, $\mathrm{Tr}((p_1\rho_1 + p_2\rho_2)\left|\varphi\right\rangle\left\langle\varphi\right|) = 1$ implies that $\mathrm{Tr}(\rho_1\left|\varphi\right\rangle\left\langle\varphi\right|) = \mathrm{Tr}(\rho_2\left|\varphi\right\rangle\left\langle\varphi\right|) = 1$, and hence $\rho_1 = \rho_2 = \rho$. $\square$

Pure states and state vector

Pure state $|\psi\rangle\langle\psi|$ can be represented by a state vector $|\psi\rangle \in \mathbb{C}^2$ with $\langle\psi|\psi\rangle = 1$.

$|\psi\rangle$ and $|\varphi\rangle := e^{i\theta}|\psi\rangle$ represent the same state since $|\psi\rangle\langle\psi| = |\varphi\rangle\langle\varphi|$.

Inner product of pure states

- ρ is a qubit pure state with a coordinate $[r_X\ r_Y\ r_Z]$.
- σ is a qubit pure state with a coordinate $[-r_X\ -r_Y\ -r_Z]$.

$$\mathrm{Tr}(\rho\sigma) = \mathrm{Tr}(\rho(I-\rho)) = \mathrm{Tr}(\rho) - \mathrm{Tr}(\rho^2) = 1 - 1 = 0$$

- $\rho = |\psi\rangle\langle\psi|$.
- $\sigma = |\varphi\rangle\langle\varphi|$.

$$\begin{aligned}\mathrm{Tr}(\rho\sigma) &= \mathrm{Tr}(|\psi\rangle\langle\psi|\,|\varphi\rangle\langle\varphi|) = \langle\psi|\varphi\rangle\,\mathrm{Tr}(|\psi\rangle\langle\varphi|)\\ &= \langle\psi|\varphi\rangle\langle\varphi|\psi\rangle = |\langle\psi|\varphi\rangle|^2\end{aligned}$$

Single qubit measurement

$$\text{Set of measurements} = \{(e_1, \ldots, e_k) \mid e_1 + \cdots + e_k = I, e_j \in C_{\succeq 0} \\ i = 1, 2, \ldots, k,\ k = 1, 2, \ldots\}$$

If $e_i e_j = \delta_{i,j} e_i$, the measurement is called an orthogonal measurement.

If $|0\rangle\langle 0|$ is measured by $(|0\rangle\langle 0|, |1\rangle\langle 1|)$, the output is 0 with probability $\mathrm{Tr}(|0\rangle\langle 0|\,|0\rangle\langle 0|) = |\langle 0|0\rangle|^2 = 1$.

If $|+\rangle\langle +|$ is measured by $(|0\rangle\langle 0|, |1\rangle\langle 1|)$, the output is 0 with probability $\mathrm{Tr}(|0\rangle\langle 0|\,|+\rangle\langle +|) = |\langle 0|+\rangle|^2 = 1/2$.

If $|\psi\rangle\langle \psi|$ is measured by $(|\varphi_0\rangle\langle \varphi_0|, |\varphi_1\rangle\langle \varphi_1|)$, the output is 0 with probability $\mathrm{Tr}(|\varphi_0\rangle\langle \varphi_0|\,|\psi\rangle\langle \psi|) = |\langle \varphi_0|\psi\rangle|^2$.

Unitary operation

For unitary operation U, let us consider

$$\rho \mapsto U\rho U^\dagger.$$

It is easy to see that

- $\mathrm{Tr}(U\rho U^\dagger) = 1$
- $U\rho U^\dagger \succeq 0$

A pure state $|\psi\rangle$ is mapped to a pure state $U|\psi\rangle$.

U and $e^{i\theta}U$ are physically equivalent.

Examples of unitary operations

- The identity matrix I.
- Pauli matrices X, Y and Z.
- Hadamard matrix $H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- Product UV of unitary operators U and V.

Multiplications of Pauli matrices

For any unitary matrices U and V, UV is also unitary matrix.

- $XY = iZ$
- $YZ = iX$
- $ZX = iY$

Pauli matrices X on the Bloch sphere

$$\rho = \frac{1}{2}\left(I + r_X X + r_Y Y + r_Z Z\right)$$

$$\begin{aligned} X\rho X^\dagger = X\rho X &= \frac{1}{2}\left(X^2 + r_X X^3 + r_Y XYX + r_Z XZX\right) \\ &= \frac{1}{2}\left(I + r_X X - r_Y Y - r_Z Z\right) \end{aligned}$$

$$[r_X \; r_Y \; r_Z] \xmapsto{X} [r_X \; -r_Y \; -r_Z]$$

π-rotation with respect to X axis.

Similarly, Y and Z corresponds to π-rotation with respect to Y and Z axes, respectively.

Hadamard matrix H is unitary and Hermitian.

$$\begin{aligned} H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} &= |+\rangle \langle 0| + |-\rangle \langle 1| \\ &= |0\rangle \langle +| + |1\rangle \langle -| \end{aligned}$$

$$|0\rangle , |1\rangle \overset{H}{\longleftrightarrow} |+\rangle , |-\rangle$$

$$\begin{aligned} HXH &= H(|+\rangle \langle +| - |-\rangle \langle -|)H \\ &= |0\rangle \langle 0| - |1\rangle \langle 1| = Z \end{aligned}$$

Similarly, $HZH = X$.
$HYH = H(iXZ)H = iHXHHZH = iZX = -Y$

Hadamard matrix on the Bloch sphere

$$\rho = \frac{1}{2}\left(I + r_X X + r_Y Y + r_Z Z\right)$$

$$\begin{aligned} H\rho H^{\dagger} = H\rho H &= \frac{1}{2}\left(H^2 + r_X HXH + r_Y HYH + r_Z HZH\right) \\ &= \frac{1}{2}\left(I + r_X Z - r_Y Y + r_Z X\right) \end{aligned}$$

$$[r_X \ r_Y \ r_Z] \xmapsto{H} [r_Z \ -r_Y \ r_X]$$

Hadamard operation can be decomposed to $\pi/2$-rotation with respect to Y axis

$$[r_X \ r_Y \ r_Z] \overset{R_Y(\pi/2)}{\longmapsto} [r_Z \ r_Y \ -r_X]$$

and X.

Rotation matrices

$$R_X(\theta) := \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X$$
$$R_X(\theta)^\dagger = R_X(-\theta)$$

$$\begin{aligned} R_X(\theta)R_X(\theta)^\dagger &= (\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X)(\cos\frac{\theta}{2} I + i \sin\frac{\theta}{2} X) \\ &= \cos^2\frac{\theta}{2} I + \sin^2\frac{\theta}{2} X^2 = I \end{aligned}$$

$$R_X(\theta)X = XR_X(\theta), \qquad R_X(\theta)Y = YR_X(-\theta), \qquad R_X(\theta)Z = ZR_X(-\theta)$$

$$R_X(\theta)R_X(\tau) = R_X(\theta + \tau)$$

$$[1\ 0\ 0] \xmapsto{R_X(\theta)} [1\ 0\ 0]$$

$$[0\ 1\ 0] \xmapsto{R_X(\theta)} [0\ \ \cos\theta\ \ \sin\theta]$$

$$[0\ 0\ 1] \xmapsto{R_X(\theta)} [0\ \ -\sin\theta\ \ \cos\theta]$$

θ-rotation with respect to X axis.

Matrix function

Definition

For f: $\mathbb{C} \to \mathbb{C}$ and orthonormal basis $(|\psi_j\rangle)_j$ of $\mathcal{X}$,

$$f\left(\sum_j \lambda_j |\psi_j\rangle \langle\psi_j|\right) := \sum_j f(\lambda_j) |\psi_j\rangle \langle\psi_j| .$$

For $H \in \mathcal{H}(\mathcal{X})$, $\exp(iH)$ is unitary.

Since the radius of convergense of exp at 0 is infinity,

$$\exp(A) = \sum_{j=0}^{\infty} \frac{1}{j!} A^j.$$

In general, $\exp(A + B) \neq \exp(A)\exp(B)$.

General unitary matrix

A normal matrix U is unitary iff all eigenvalues of U have absolute value 1 since for

$$U = \sum_j \lambda_j \left|\psi_j\right\rangle \left\langle\psi_j\right| .$$

it holds

$$UU^\dagger = \sum_j |\lambda_j|^2 \left|\psi_j\right\rangle \left\langle\psi_j\right| .$$

Let $\lambda_j = e^{i\theta_j}$. Then, for Hermitian matrix

$$H = \sum_j \theta_j \left|\psi_j\right\rangle \left\langle\psi_j\right| .$$

$U = \exp(iH)$.

Assignments

1. For $a, b, c, d \in \mathbb{R}$, show $r_I,\ r_X,\ r_Y,\ r_Z \in \mathbb{R}$ satisfying
$$\begin{bmatrix} a & b+ci \\ b-ci & d \end{bmatrix} = r_I I + r_X X + r_Y Y + r_Z Z.$$

2. Express $\exp\left(-i\frac{\theta}{2}X\right)$ for $\theta \in \mathbb{R}$ as a complex linear combination of $I,\ X,\ Y$ and Z. A summation with infinite number of terms is not allowed.

3. [Advanced] For $a_I,\ a_X,\ a_Y,\ a_Z \in \mathbb{R}$, represents
$$\exp\left(i(a_I I + a_X X + a_Y Y + a_Z Z)\right)$$
by a linear combination of I, X, Y and Z. A summation with infinite number of terms is not allowed.