Chapter 4 The theory of Quantum Algorithms.

① single qubit operator $\simeq$ Rotation in $\mathbb{R}^3$ / Block sphere

② Controlled operators for multi-qubit
- every Boolean function can be implemented by a quantum circuit.

③ Universal set of operators. cf) In classical case, "NAND" or "NOR".

④ Quantum algorithm : probabilistic algorithm. Complexity?

4.1 Simple single-qubit operators

(Bloch sphere)

I, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$X = |x_+\rangle\langle x_+| - |x_-\rangle\langle x_-|$

$(|x_+\rangle, |x_-\rangle)$

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

likewise

⋮

properties

X, Y, Z, H are Hermitian, involution, unitary

$$\begin{cases} XY = iZ = -YX, \quad ZX = iY = -XZ, \quad YZ = iX = -ZY \\ -iXYZ = I \end{cases}$$

$HXH = Z$, $HYH = -Y$, $HZH = X$

proposition

(I, X, Y, Z) is a $\underbrace{\text{orthogonal}}$ $\mathbb{C}$-basis of $\mathrm{End}(\mathbb{H}_1)$ (w.r.t Hilbert-Schmidt inner product)

$tr(A^* B) = \sum \overline{a_{ij}} b_{ji}$

4.2 Geometry in $\mathbb{R}^3$

focus on $\mathbb{R}^3$

① Rotations of $\mathbb{R}^3$ is $SO(3)$

② Decomposition of rotation into simpler form

* $(\vec{a}, \vec{b}, \vec{c}) \simeq (\vec{a}|\vec{b}|\vec{c})$

$\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ $\hat{u}$ means unit vector on $\mathbb{R}^3$

Def

$\angle(\vec{a}, \vec{b}) = \cos^{-1}\left(\frac{\langle \vec{a} | \vec{b} \rangle}{\|\vec{a}\| \|\vec{b}\|}\right)$ (by Cauchy-Schwarz inequality)

$\cos^{-1} : [-1, 1] \to [0, \pi]$

$\vec{a} \times \vec{b}$ usually.

Lots of properties : $\|\vec{a} \times \vec{b}\| = \|\vec{a}\| \|\vec{b}\| \sin \angle(\vec{a}, \vec{b})$, $\det(\vec{a}, \vec{b}, \vec{c}) = \langle \vec{a} \times \vec{b} | \vec{c} \rangle$ ...

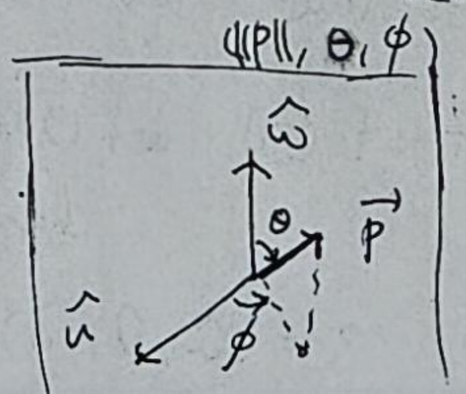
Thm If $\vec{a} \perp \vec{b}$, $\|\vec{a}\| = \|\vec{b}\| = 1$, $(\vec{a} \times \vec{b}, \vec{a}, \vec{b})$, $(\vec{a}, \vec{b} \times \vec{a}, \vec{b})$, $(\vec{a}, \vec{b}, \vec{a} \times \vec{b})$ are orthonormal bases with det 1. (such vectors are unique) ($\hat{a}, \hat{b}$ for unit vec)

(Note that acutally they produce $SO(3)$)

Def General spherical coordinate

$\hat{u} \perp \hat{w}$. By last thm, take $B = (\hat{u}, \hat{v}, \hat{w})$ ONB with det 1.

"Spherical coordinate w.r.t. $(\hat{u}, \hat{w})$: $B\vec{p}$'s spherical version.



(Ex) $\vec{p} = (\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{\sqrt{2}})$, $\hat{u} = (1,0,0)$, $\hat{\omega} = (0,0,-1)$.
↑ typo

$B = \begin{pmatrix} 1 & & 0 \\ & -1 & \\ 0 & & -1 \end{pmatrix}$ $\quad B^{-1}\vec{p} = Bp = (\frac{1}{2}, -\frac{1}{2}, -\frac{1}{\sqrt{2}}) = (1, \frac{4}{3}\pi, \frac{5}{4}\pi)_{r,\theta,\phi}$

Recall $= r(\cos\phi \sin\theta, \sin\phi\sin\theta, \cos\theta)$ $\quad (x,y,z)$

proposition change of coordinate in spherical coordinate. (Just $\hat{u}$) $[\hat{u}, \hat{u}' \perp \hat{\omega}]$

① Sph. coor. rep. of $\hat{u}'$ w.r.t. $(\hat{u}, \hat{\omega})$: $(1, \frac{\pi}{2}, \delta)$ where $\begin{cases} \cos\delta = \langle \hat{u} | \hat{u}' \rangle \\ \sin\delta = \langle \hat{\omega} \times \hat{u} | \hat{u}' \rangle \end{cases}$ need both to determine δ.

② $(r,\theta,\phi)_{(\hat{u},\hat{\omega})} = (r',\theta',\phi')_{(\hat{u}',\hat{\omega}')} = \vec{p}$

$\Rightarrow r = r'$, $\theta = \theta'$, $\phi' = \begin{cases} 0 & \theta \in \{0,\pi\} \\ \phi - \delta \mod 2\pi & \end{cases}$ ← typo (pf) Graphically obvious.

Def Orthogonal matrix : $O^T = O^{-1}$, $O(n)$: orthogonal group, $SO(n)$

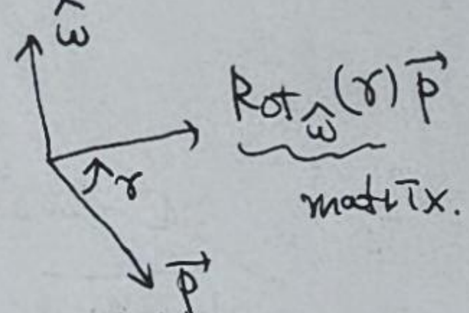
properties TFAE : $O \in O(3)$, columns are ONB, rows are ONB, preserves inner product, preserves norm

Def Rotation in $\mathbb{R}^3$

$\gamma \in \mathbb{R}$, $\hat{u} \perp \hat{\omega}$ be given. Rotation is a mapping s.t. $\vec{p} = (r,\theta,\phi)_{(\hat{u},\hat{\omega})} \mapsto (r',\theta',\phi')_{(\hat{u},\hat{\omega})}$ s.t.

$r' = r$, $\theta' = \theta$, $\phi' = \begin{cases} \phi & \text{if } \theta \in \{0,\pi\} \\ \phi + \gamma \pmod{2\pi} & \text{else} \end{cases}$. This is independent of $\hat{u}$; so call it

$\mathrm{Rot}_{\hat{\omega}}(\gamma)$. Rotation about $\hat{\omega}$ through the angle γ.



Now prepare to prove rot $= SO(3)$

proposition

① $\mathrm{Rot}_{\hat{x}}(\gamma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma & -\sin\gamma \\ 0 & \sin\gamma & \cos\gamma \end{pmatrix}$ and so forth. (Note that these are $SO(3)$)

② Let $B = (\hat{u}, \hat{v}, \hat{\omega})$. Then $\mathrm{Rot}_{\hat{\omega}}(\gamma) = B\,\mathrm{Rot}_{\hat{x}}(\gamma)\,B^{-1}$ and so forth. ⟨Important technique⟩
$\in \underline{SO(3)}$

for consistency with coordinate (e_1, e_2, e_3).

③ Thus, all rotations are $SO(3)$.

④ $O \in SO(3)$. Then $O = I_3 \Leftrightarrow O = \mathrm{Rot}_{\hat{\omega}}(\gamma)$ for $\gamma \equiv 0 \pmod{2\pi}$

⑤ If $O \neq I_3$, then $\exists\, \hat{\omega}$ s.t. $O\hat{\omega} = \hat{\omega}$ (unique up to scale), and $\exists\, \gamma \in \mathbb{R}$ (unique up to mod 2π) s.t $O = \mathrm{Rot}_{\hat{\omega}}(\gamma)$ $(= \mathrm{Rot}_{\hat{\omega}}(-\gamma))$

⑥ Thus, all $SO(3)$ are rotations.

(pf of ⑤) $\det O = 1$, $|\lambda_i| = 1$ (isometry) $\Rightarrow$ exactly one 1 as an eigenvalue.
characteristic poly, $\Pi \lambda_i = 1$, $\hat{\omega}$ be (unit) corresponding eigenvector.

$B = (\hat{u}, \hat{v}, \hat{\omega}) \in SO(3)$, $R = B^{-1}OB \Rightarrow BR = OB \Rightarrow R = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{pmatrix}$.

Since $R \in SO(3)$, $R = \begin{pmatrix} a & b & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $a^2+b^2=1 \Rightarrow R = Rot_{\hat{z}}(\gamma)$ $\begin{pmatrix} \cos\gamma = a \\ \sin\gamma = -b \end{pmatrix}$ ∎

Next, there are two decomposition thm of Rotation in $\mathbb{R}^3$.

<u>Lemma</u> $\hat{u}, \hat{u}' \perp \hat{\omega}$. Then $\exists!\, \delta \in \mathbb{R}/2\pi$ s.t. $Rot_{\hat{\omega}}(\delta)\hat{u} = \hat{u}'$. (pf) Graphically obvious.

<u>Thm</u> $\forall O \in SO(3)$, $\exists \alpha, \beta, \gamma \in \mathbb{R}$ s.t. $O = Rot_{\hat{z}}(\alpha) Rot_{\hat{y}}(\beta) Rot_{\hat{z}}(\gamma)$

α, β, γ are called Euler angles of O.

pf) Let $O = (\hat{x}', \hat{y}', \hat{z}')$. If $\hat{z}' = \pm\hat{z}$ (i.e. $(0,0,\pm1)$) then $O = Rot_{\hat{z}}(\gamma)$ so the end.

Else, since $\hat{z}' \perp span(\hat{x}', \hat{y}')$, $span(\hat{x}', \hat{y}') \cap span(\hat{x}, \hat{y}) = span(\hat{v})$

since $\hat{v} \in span(\hat{x}, \hat{y})$, $\hat{v} \perp \hat{z}$. By lemma, $\hat{v} = \exists Rot_{\hat{z}}(\alpha)\hat{y}$.

$B_1 = Rot_{\hat{z}}(\alpha) I_3 = (\hat{x}_1, \hat{v}, \hat{z})$. Now, $\hat{v} \perp \hat{z}, \hat{z}' \Rightarrow \exists Rot_{\hat{v}}(\beta)(\hat{z}) = \hat{z}'$
$\in SO(3)$

By proposition, $Rot_{\hat{v}}(\beta) = B_1 Rot_{\hat{y}}(\beta) B_1^{-1}$. Apply this to ONB B_1 to get

$B_2 = Rot_{\hat{v}}(\beta) B_1 = Rot_{\hat{z}}(\alpha) Rot_{\hat{y}}(\beta) = (\hat{x}_2, \hat{v}, \hat{z}') \in SO(3)$.

Finally, $\hat{y}', \hat{v} \perp \hat{z}'$ so $\exists Rot_{\hat{z}'}(\gamma)\hat{v} = \hat{y}'$. By proposition,

$Rot_{\hat{z}'}(\gamma) = B_2 Rot_{\hat{z}}(\gamma) B_2^{-1}$. Apply this to ONB B_2 to get

$B_3 = Rot_{\hat{z}}(\alpha) Rot_{\hat{y}}(\beta) Rot_{\hat{z}}(\gamma) \in SO(3)$ But such $\hat{x}_3$ making $SO(3)$
$= (\hat{x}_3, \hat{y}', \hat{z}')$ is unique $\Rightarrow \hat{x}_3 = \hat{x}$. ∎

<u>Cor</u> For $\hat{v} \perp \hat{\omega}$, similar thm holds:

$\forall O \in SO(3)$ $\exists \alpha, \beta, \gamma \in \mathbb{R}$ s.t. $O = Rot_{\hat{\omega}}(\alpha) Rot_{\hat{v}}(\beta) Rot_{\hat{\omega}}(\gamma)$.

what if $\hat{v} \not\perp \hat{\omega}$?

<u>Lemma</u> $\hat{\omega}, \hat{\omega}', \gamma \in \mathbb{R}$, $O \in SO(3)$ with $O\hat{\omega} = \hat{\omega}'$. Then $Rot_{\hat{\omega}'}(\gamma) = O Rot_{\hat{\omega}}(\gamma) O^{-1}$.

pf) $B = (\hat{u}, \hat{v}, \hat{\omega})$. $OB = (\hat{u}', \hat{v}', \hat{\omega}') \Rightarrow Rot_{\hat{\omega}'}(\gamma) = OB Rot_{\hat{z}}(\gamma) B^{-1} O^{-1} = O Rot_{\hat{\omega}}(\gamma) O^{-1}$.

<u>Thm</u>

$\hat{a} \not\parallel \hat{b}$ (not parallel). $\varphi = \angle(\hat{a}, \hat{b})$. $\forall O \in SO(3)$, $\exists k \in \mathbb{N}$, $\alpha_i, \beta_i \in \mathbb{R}$ for $i = 1 \sim k$ s.t. $k = O(\frac{1}{\varphi})$ (↖ Big-O), and

$$O = \prod_{i=1}^{k} Rot_{\hat{a}}(\alpha_i) Rot_{\hat{b}}(\beta_i)$$

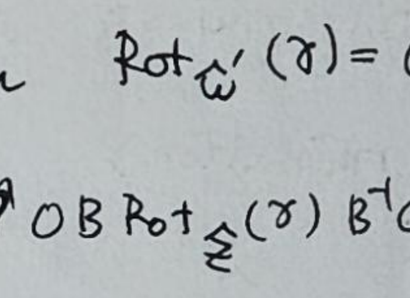
pf) By thm, $O = Rot_{\hat{\omega}}(\gamma)$. <u>W.T.D</u> Find $O' = \prod_{i=1}^{l} Rot_{\hat{a}}(\alpha_i) Rot_{\hat{b}}(\beta_i)$ s.t. $O'\hat{\omega} = \hat{b}$.

Then by the lemma, $O = (O')^{-1} Rot_{\hat{b}}(\gamma) O'$.

① Reduce the case.

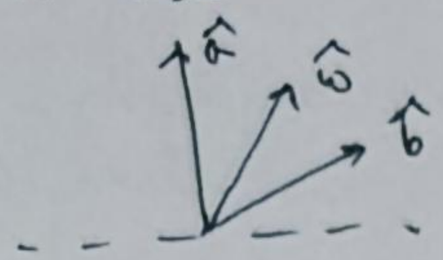
1. Rotate $\hat{\omega}$ by $\hat{a}$ to bring it in $span(\hat{a}, \hat{b})$.

2. Use $Rot_{\hat{\omega}}(\gamma) = Rot_{-\hat{\omega}}(-\gamma)$ to bring $\hat{\omega}$ in upper half.

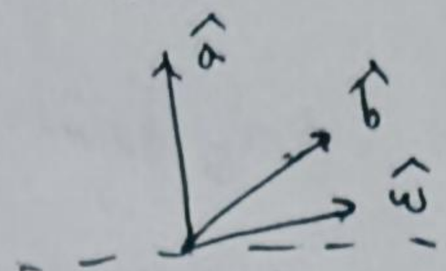


3. Bring $\hat{\omega}$ to 1st quadrant by rotation w.r.t. $\hat{a}$

$\therefore$ Case 1



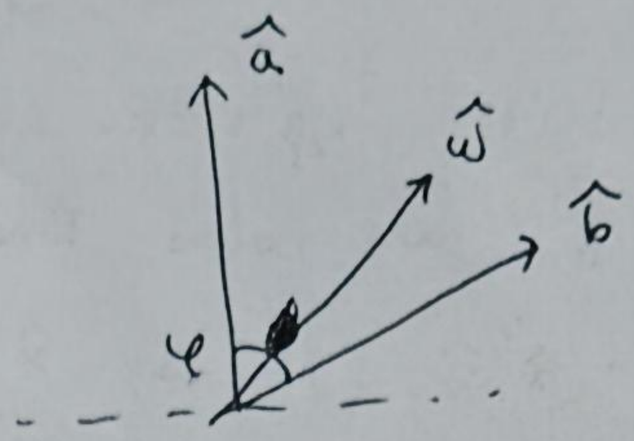
Case 2



② Case 1.

Rotate $\hat{\omega}$ by $\hat{b}$ until $\angle(\hat{a}, \hat{\omega}) = \varphi$

Now rotate by $\hat{a}$ to arrive at $\hat{b}$.

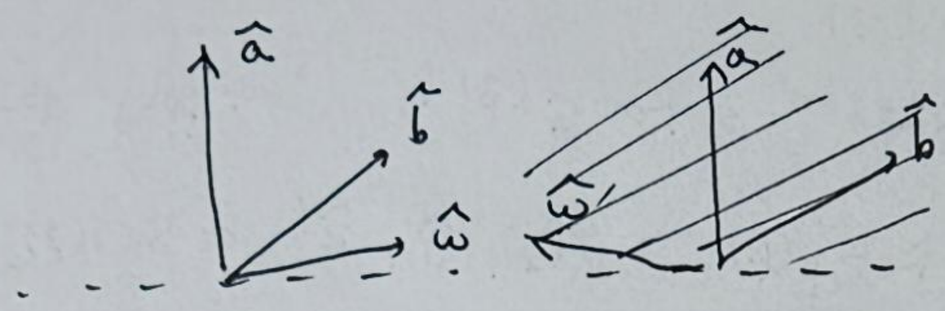


③ Case 2.

w.T.S. One can reduce to case 1 (in $O(\frac{1}{\varphi})$ times) ← big-O

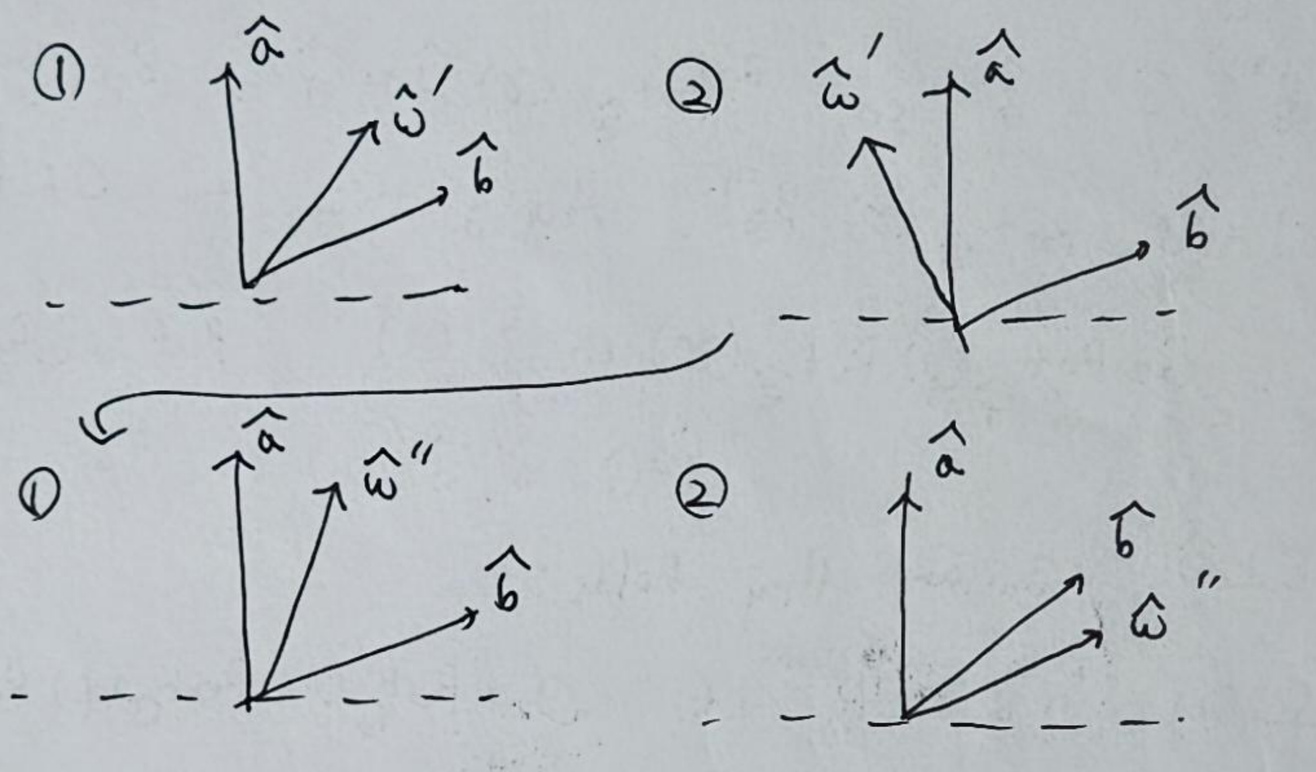
~~(One step)~~

~~$Rot_{\hat{a}}(\pi)\, Rot_{\hat{b}}(-\pi)$~~



(Step 1)

$Rot_{\hat{b}}(-\pi)$



~~(Two step)~~

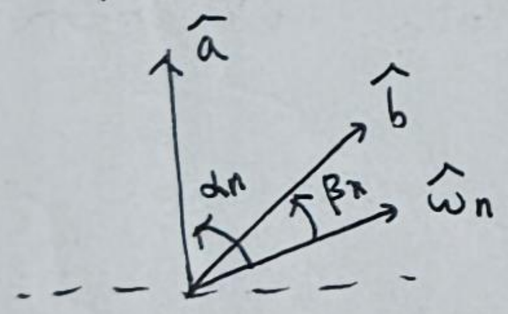
(Step 2)

$Rot_{\hat{a}}(\pi)$

Repeat until $\hat{\omega}$ is inside $\hat{a}, \hat{b}$.

(proof of termination)

Let



n step of 1 and 2.

By calculation,

$$\begin{cases} \alpha_{n+\frac{1}{2}} = \alpha_n - 2\beta_n \\ \beta_{n+\frac{1}{2}} = -\beta_n \end{cases} \qquad \begin{cases} \alpha_{n+1} = 2\beta_n - \alpha_n \\ \beta_{n+1} = 3\beta_n - 2\alpha_n \end{cases}$$

$\downarrow$ fails if $\alpha_{n+\frac{1}{2}} < 0$ $\Leftrightarrow \frac{\alpha_n}{\beta_n} < 2$

$\downarrow$ fails if $\beta_{n+1} > 0$ $\Leftrightarrow \frac{\alpha_n}{\beta_n} < \frac{3}{2}$

Note $\alpha_0 = \beta_0 + \varphi$

$$\begin{bmatrix} \alpha_n \\ \beta_n \end{bmatrix} = \begin{bmatrix} -1 & 2 \\ -2 & 3 \end{bmatrix}^n \begin{bmatrix} \alpha_0 \\ \beta_0 \end{bmatrix} = \left(n \begin{bmatrix} -1 & 2 \\ -2 & 3 \end{bmatrix} + (1-n) I \right) \begin{bmatrix} \alpha_0 \\ \beta_0 \end{bmatrix} = \begin{bmatrix} (1-2n)\alpha_0 + 2n\beta_0 \\ -2n\alpha_0 + (1+2n)\beta_0 \end{bmatrix}$$

Using Jordan form

$$\frac{\alpha_n}{\beta_n} = \frac{\beta_0 - \alpha_0 + \frac{\alpha_0}{2n}}{\beta_0 - \alpha_0 + \frac{\beta_0}{2n}} = \frac{\varphi - \frac{\alpha_0}{2n}}{\varphi - \frac{\beta_0}{2n}} \to 1 \quad \text{as } n \to \infty \qquad ④$$

4.3 Rotation operators

W.T.D: ① Define rotation operators, show that it acts on $\mathbb{H}_1$ as if rotation is applied to Bloch sphere.

② Rotation operators $\simeq SU(2)$, $SU(2)/\{\pm 1\} \simeq SO(3)$

→ can use decomposition theorems

Recall Pauli operators

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Def $\sigma = (X, Y, Z) \in U(2)^3$. Define $\vec{p} \cdot \sigma = p_1 X + p_2 Y + p_3 Z$ for $\vec{p} \in \mathbb{R}^3$ (Not a matrix product)

prop $\hat{p} \in \mathbb{R}^3$ (unit vector). Then $\hat{p} \cdot \sigma$ is Hermitian, unitary, involution with trace 0, eigenvalues $\{\pm 1\}$ (not subset, both).

Def Rotation gate (operator): $R_{\hat{\omega}}(\gamma) = e^{-i\gamma \hat{\omega} \cdot \sigma/2} = \cos\frac{\gamma}{2} I - i \sin\frac{\gamma}{2} \hat{\omega} \cdot \sigma$ ↑ 2.4.14

where $\hat{\omega} \in \mathbb{R}^3$, $\gamma \in \mathbb{R}$. Then, $R_{\hat{\omega}}(\gamma) \in SU(2)$.

prop $R_{\hat{\omega}}(\beta) R_{\hat{\omega}}(\gamma) = R_{\hat{\omega}}(\beta+\gamma)$

Def Special rotations

$$R_{\hat{x}}(\gamma) = \begin{pmatrix} \cos\frac{\gamma}{2} & -i\sin\frac{\gamma}{2} \\ -i\sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix}, \quad R_{\hat{y}}(\gamma) = \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix}, \quad R_{\hat{z}}(\gamma) = \begin{pmatrix} e^{-i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{pmatrix}$$

(lower case)

Def $su(2) := \{A : \text{Hermitian operator on } \mathbb{H}_1 \text{ with } \operatorname{tr} A = 0\} = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix} : a \in \mathbb{R}, b \in \mathbb{C} \right\}$

$\Rightarrow SU(2) = \{e^{iA} : A \in su(2)\}$ by 2.4.13.

prop X, Y, Z are ONB of $su(2)$.

Thm If $U \in SU(2)$, the following holds:

① $U = I \Leftrightarrow U = R_{\hat{\omega}}(\gamma)$ with $\gamma/2 \equiv 0 \pmod{2\pi}$

② $U = -I \Leftrightarrow U = R_{\hat{\omega}}(\gamma)$ with $\gamma/2 \equiv \pi \pmod{2\pi}$

③ Let $U \neq \pm I$. Then $\exists \hat{\omega}, \gamma$ s.t. $U = R_{\hat{\omega}}(\gamma)$. It is unique up to:

$\hat{\omega} = \hat{\omega}'$, $\gamma/2 \equiv \gamma'/2 \pmod{2\pi}$ or $\hat{\omega} = -\hat{\omega}'$, $\gamma/2 \equiv \gamma'/2 \pmod{2\pi}$

Sketch of the proof) Take $A \in su(2)$ s.t. $U = e^{iA}$. Then $\exists \vec{p}$ s.t. $A = \vec{p} \cdot \sigma$.

Now take $\gamma = 2\|\vec{p}\|$, $\hat{\omega} = -\vec{p}/\|\vec{p}\|$.

Cor $U \in U(2) \Rightarrow \exists \delta \in \mathbb{R}$ s.t. $e^{-i\delta} U$ is a rotation operator on $\mathbb{H}_1$ (used in decomposition thm)

Cor Let $U \in SU(2)$. For any $\hat{\omega}, \gamma$ s.t. $U = R_{\hat{\omega}}(\gamma)$, $\mathrm{Rot}_{\hat{\omega}}(\gamma)$ is constant.

- prop 4.2.27, thm 4.3.15

⇒ **Def** $U \in SU(2)$. For $\hat{\omega}, \gamma$ s.t. $U = R_{\hat{\omega}}(\gamma)$, define $\mathrm{Rot}(U) = \mathrm{Rot}_{\hat{\omega}}(\gamma)$

Thm Map $\mathrm{Rot}: SU(2) \to SO(3)$ is a surjective group homomorphism with kernel $\{\pm I\}$. Also for Bloch sphere repr. $\vec{p}$, $\vec{p}(U|\psi\rangle) = \mathrm{Rot}(U)\,\vec{p}(|\psi\rangle)$

- surjection is obvious by $\left(O = \mathrm{Rot}_{\hat{\omega}}(\gamma) \to \text{take } U = R_{\hat{\omega}}(\gamma)\right)$.

To show homomorphism, we need some results (quite technical).

Def $\tau = (\tau_u, \tau_v, \tau_w) \in su(2)^3$.

① $\vec{p} = (p_u, p_v, p_w) \in \mathbb{R}^3 \Rightarrow \vec{p}\cdot\vec{\tau} = p_u\tau_u + p_v\tau_v + p_w\tau_w \in M_{2\times 2}(\mathbb{C})$

② $B = (\hat{u}, \hat{v}, \hat{w}) \in \mathbb{R}^{3\times 3} \Rightarrow B\cdot\tau = (\hat{u}\cdot\tau,\ \hat{v}\cdot\tau,\ \hat{w}\cdot\tau) \in M_{2\times 2}(\mathbb{C})^3$

Lemma $(B\vec{p})\cdot\tau = \vec{p}\cdot(B\cdot\tau)$ for $\vec{p}\in\mathbb{R}^3$, $B\in\mathbb{R}^{3\times 3}$, $\tau\in su(2)$

Lemma $(\vec{p}\cdot\sigma)(\vec{q}\cdot\sigma) = \langle\vec{p}|\vec{q}\rangle I + i(\vec{p}\times\vec{q})\cdot\sigma$

prop $B\in SO(3)$, let $\tau = (\tau_u, \tau_v, \tau_w) = B\cdot\sigma$. Then τ_u, τ_v, τ_w acts similarly with X, Y, Z, i.e.

$$\tau_u^2 = \tau_v^2 = \tau_w^2 = I, \quad \tau_u\tau_v = i\tau_w = -\tau_v\tau_u \quad -i\tau_u\tau_v\tau_w = I$$
$$\tau_v\tau_w = i\tau_u = -\tau_w\tau_v$$
$$\tau_w\tau_u = i\tau_v = -\tau_u\tau_w$$

↑ $\vec{p}\cdot\sigma$ involution

Lemma $U\in SU(2)$, $\vec{p}\in\mathbb{R}^3$. Then $(\mathrm{Rot}(U)\vec{p})\cdot\sigma = U(\vec{p}\cdot\sigma)U^{-1}$.

pf $U = R_{\hat{\omega}}(\gamma)$. Take $B = (\hat{u}, \hat{v}, \hat{\omega}) \in SO(3)$, $\tau = B\cdot\sigma$, $\vec{q} = B^{-1}\vec{p}$.

$$(\mathrm{Rot}(U)\vec{p})\cdot\sigma = (\mathrm{Rot}_{\hat{\omega}}(\gamma)\vec{p})\cdot\sigma = (B\,\mathrm{Rot}_{\hat{z}}(\gamma)B^{-1}\vec{p})\cdot\sigma = (B\,\mathrm{Rot}_{\hat{z}}(\gamma)\vec{q})\cdot\sigma = (\mathrm{Rot}_{\hat{z}}(\gamma)\vec{q})\cdot\tau$$
$$U(\vec{p}\cdot\sigma)U^{-1} = U(B\vec{q}\cdot\sigma)U^{-1} = U(\vec{q}\cdot\tau)U^{-1}$$

Next check that two expressions match for $\vec{q} = \hat{x}, \hat{y}, \hat{z}$ ∎.

Now homomorphism is shown:

$$(\mathrm{Rot}(U_1U_2)\vec{p})\cdot\sigma = U_1U_2(\vec{p}\cdot\sigma)U_2^{-1}U_1^{-1} = (\mathrm{Rot}(U_1)\,\mathrm{Rot}(U_2)\vec{p})\cdot\sigma$$ linearly independent

kernel Rot: $U = R_{\hat{\omega}}(\gamma) \Rightarrow \mathrm{Rot}_{\hat{\omega}}(\gamma) = I$ iff $\gamma \equiv 0 \pmod{2\pi} \Leftrightarrow \gamma/2 \equiv 0 \pmod{\pi}$

$\Leftrightarrow U = \pm I$ by 4.3.15

To show second assertion (rotation on Bloch sphere) we need two equalities.

Lemma $\vec{p}\in\mathbb{R}^3$ be a spherical coord. repr. $(1,\theta,\phi) \Rightarrow \vec{p}\cdot\sigma = \begin{pmatrix}\cos\theta & e^{-i\phi}\sin\theta\\ e^{i\phi}\sin\theta & -\cos\theta\end{pmatrix}$

prop $|\psi\rangle$ be a quantum state in $\mathbb{H}_1$. Then

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + \vec{p}(\psi)\cdot\sigma).$$

$|U|\psi\rangle\langle U|\psi\rangle| = \frac{1}{2}(I + \vec{q}\cdot\sigma)$ $\quad (\vec{p} = \vec{p}(\psi),\ \vec{q} = \vec{p}(U|\psi\rangle))$

$U|\psi\rangle\langle\psi|U^{-1} = \frac{1}{2}(I + U\vec{p}\cdot\sigma U^{-1})$

$U\vec{p}\cdot\sigma U^{-1} = (Rot(U)\vec{p})\cdot\sigma$

$\Rightarrow \quad \vec{q} = \vec{p}(U|\psi\rangle) = Rot(U)\vec{p}$ //

Now the decomposition theorems.

<u>Thm</u>

For $\forall U \in U(2)$ $\exists \alpha, \beta, \gamma, \delta \in \mathbb{R}$ s.t. $U = e^{i\delta} R_{\hat{z}}(\alpha) R_{\hat{y}}(\beta) R_{\hat{z}}(\gamma)$.

Let $A = R_{\hat{z}}(\alpha) R_{\hat{y}}(\frac{\beta}{2})$, $B = R_{\hat{y}}(-\frac{\beta}{2}) R_{\hat{z}}(-\frac{\alpha+\gamma}{2})$, $C = R_{\hat{z}}(-\frac{\alpha-\gamma}{2})$. Then

$ABC = I$, $\quad U = e^{i\delta} A \times B \times C$.

← Used in 4.4.

<u>Thm</u>

$\hat{a}, \hat{b} \in \mathbb{R}^3$ be nonparallel. $\varphi = \angle(\hat{a}, \hat{b})$. $\forall U \in U(2)$, $\exists k \in \mathbb{N}$, $\alpha_i, \beta_i, \delta \in \mathbb{R}$ s.t.

$k = O(1/\varphi)$, $\quad U = e^{i\delta} \prod_{i}^{k} R_{\hat{a}}(\alpha_i) R_{\hat{b}}(\beta_i)$.

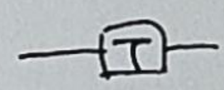
Lastly, one introduces special class of rotation operators.

$P(\gamma) := \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\gamma} \end{pmatrix} \in U$ of $\mathbb{H}_1$. $\quad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix} = P\left(\frac{-2\pi}{2^k}\right)$

$= e^{i\frac{\gamma}{2}} R_{\hat{z}}(\gamma)$

phase shift gate

$S = R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ 

$T = R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix}$ 

appears later in 4.9