

Solovay-Kitaev theorem

T : linear transform on $\mathbb{C}^d$ ($d \times d$ matrix)

Def. the operator norm (with respect to the Hilbert space structure of $\mathbb{C}^d$) is $\|T\| = \max_{|\psi\rangle \in \mathbb{C}^d, \text{state}} \|T|\psi\rangle\|$

Rem. given unitary gates U, V on $\mathbb{C}^d$,

we often write $E(U, V) = \|U - V\|$

Facts: T normal ($TT^\dagger = T^\dagger T$), $\exists$ orthonormal basis of eigenvectors $T|\psi_i\rangle = \lambda_i |\psi_i\rangle$, $\langle \psi_i | \psi_j \rangle = \delta_{ij}$

$$\Rightarrow \|T\| = \max |\lambda_i|$$

$$U \text{ unitary} \Rightarrow \|UT\| = \|T\|,$$

$$\|T^\dagger\| = \|T\|, \quad \|T\| = \sqrt{\|T^\dagger T\|}.$$

Other examples of norms: $\|T\|_p = (\text{Tr}((T^\dagger T)^{p/2}))^{1/p}$

Solovay-Kitaev theorem) For a fixed $C_2 > 3$

$\exists c_1 > 0 \quad \forall d = 2, 3, \dots \quad \exists \varepsilon > 0$

if $S \subseteq SU(d)$ is a subset s.t.

$$1) \quad \forall U \in S \Rightarrow U^\dagger \in S$$

$$2) \quad \forall U \in SU(d) \quad \exists V \in S \quad \|U - V\| < \varepsilon$$

then $\forall \delta > 0, U \in SU(d) \quad \exists V_0, \dots, V_{\ell-1} \in S$ s.t.

$$\|U - V_0 \dots V_{\ell-1}\| < \delta, \quad \ell \leq C_1 \left(\log \frac{1}{\delta}\right)^{C_2}$$

Key lemma) $1 > \delta > \Delta > 0, U, V, \tilde{U}, \tilde{V} \in U(d)$

suppose $\|U - \tilde{U}\|, \|V - \tilde{V}\| < \Delta, \|I_d - U\|, \|I_d - V\| < \delta$

$$\text{then } \|UVU^\dagger V^\dagger - \tilde{U}\tilde{V}\tilde{U}^\dagger \tilde{V}^\dagger\| < 42\delta\Delta$$

cf. Baker-Campbell-Hausdorff formula $\Rightarrow$

$$\exp(x) \exp(y) \exp(-x) \exp(-y) \sim \exp([x, y])$$

$\begin{matrix} U & V & U^\dagger & V^\dagger \end{matrix}$

Proof of lemma

Write $UVU^+V^+ - \tilde{U}\tilde{V}\tilde{U}^+\tilde{V}^+ = \underbrace{(UVU^+V^+ - \tilde{U}V\tilde{U}^+V^+)}_{\text{will estimate this}} + \tilde{U}V\tilde{U}^+V - \tilde{U}\tilde{V}\tilde{U}^+\tilde{V}^+$

Step 1 $X = U^+\tilde{U} - I_d \Rightarrow \|X\| < \Delta$

$\|X\| = \|U^+(\tilde{U} - U)\| = \|\tilde{U} - U\|$

Step 2 $UVU^+V^+ - \tilde{U}V\tilde{U}^+V^+ = -UXVU^+V^+ - \tilde{U}VX^+U^+V^+ - UXVX^+U^+V^+$

Step 3 $\|UXVU^+V^+ - X\| < 7\delta\Delta$

$UXVU^+V^+ = (I_d + A)X(I_d + B)(I_d + A^+)(I_d + B^+)$

with $A = U - I_d, B = V - I_d$ has norm $< \delta$

Step 4 $\|UVU^+V^+ - \tilde{U}V\tilde{U}^+V^+\| \leq 21\delta\Delta$

Step 3 and analogues give

(right hand side of Step 2) $\sim \frac{-(X + X^+ + XX^+)}{21\delta\Delta}$

$X + X^+ + XX^+ = U^+\tilde{U} - I_d + \tilde{U}^+U - I_d + (U^+\tilde{U} - I_d)(\tilde{U}^+U - I_d) = 0$

Lemma 2 $H = d \times d$ skew Hermitian $H^+ = -H$ such that $\text{Tr } H = 0$

Then $\exists X, Y$ $d \times d$ skew Hermitian, $\text{Tr } X = 0 = \text{Tr } Y$

$H = [X, Y] (= XY - YX)$, $\|X\|, \|Y\| \leq 2\sqrt{\|H\|}$

Example $d=2$ $H = \begin{bmatrix} i & \\ & -i \end{bmatrix} \therefore X = \frac{i}{\sqrt{2}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

Proof of Lem 2 rescale $\|H\|=1$, so we want $\|X\|, \|Y\| \leq 2$

Step 1 diagonalize $H = \begin{bmatrix} i\lambda_0 & & \\ & \ddots & \\ & & i\lambda_{d-1} \end{bmatrix}$ $\lambda_j \in \mathbb{R}, \sum \lambda_j = 0$

$0 \leq \lambda_0, \lambda_0 + \lambda_1, \dots, \lambda_0 + \dots + \lambda_{d-1} \leq 2$

Step 2

$X = i \begin{bmatrix} 0 & v_0 & & \\ v_0 & 0 & v_1 & 0 \\ & v_1 & 0 & \ddots \\ 0 & & & v_{d-2} \\ & & & v_{d-2} & 0 \end{bmatrix}$ $Y = \begin{bmatrix} 0 & -v_0 & & \\ v_0 & 0 & -v_1 & \\ & v_1 & 0 & \ddots \\ & & & -v_{d-2} \\ & & & v_{d-2} & 0 \end{bmatrix}$ $v_j = \sqrt{\frac{\lambda_0 + \dots + \lambda_j}{2}}$
Satisfy $H = [X, Y]$

(cont.) Step 3 $\|X\| \leq 2$ $X' = X$ without " z ", $\lambda \neq 0$ eigenval of X' with max absolute value. $\|X\| = |\lambda|$ $| \psi \rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_{d-1} \end{bmatrix}$ eigenvector. a_k component with max abs val

$$X | \psi \rangle = \lambda | \psi \rangle \Rightarrow \lambda a_k = v_{k-1} a_{k-1} + v_{k+1} a_{k+1}$$

$$|\lambda a_k| = |v_{k-1} a_{k-1} + v_{k+1} a_{k+1}| \leq |a_{k-1}| + |a_{k+1}| \leq 2|a_k|$$

$$\Rightarrow \|X\| = |\lambda| \leq 2$$

Step 4 $\|Y\| \leq 2$ similar as Step 3 $\square$ Lemma 3 $\exists \delta_0 > 0$ if $U \in SU(d)$, $\|I_d - U\| < \delta < \delta_0$
(dep. on d)then $\exists V, W \in SU(d)$ s.t. $\|U - VWV^\dagger W^\dagger\| < 150 \delta^{3/2}$

$$\|I_d - V\|, \|I_d - W\| < 3\sqrt{\delta}$$

$$\text{Example } d=2 \quad U = \begin{bmatrix} \frac{z}{2} & 0 \\ 0 & \frac{\bar{z}}{2} \end{bmatrix} = \exp\left(\underbrace{\begin{bmatrix} i x & 0 \\ 0 & -i x \end{bmatrix}}_H\right)$$

$$H = [X, Y], \quad X = i\sqrt{\frac{x}{2}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \sqrt{\frac{x}{2}} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad (\text{Lem 2})$$

$$V = \exp(X), \quad W = \exp(Y) \Rightarrow VWV^\dagger W^\dagger \sim U \quad \text{by Baker-Campbell-Hausdorff.}$$

$$\|I_2 - V\| \leq \|X\| = \sqrt{\frac{x}{2}} \quad \text{from } |e^{it} - 1| \leq t$$

General case. similarly $U = \exp(H)$ $H^\dagger = -H$

$$\|H\| \sim \|I_d - U\| < \delta, \quad H = [X, Y] \quad (\text{Lem 2}), \quad \|X\|, \|Y\| \leq 2\sqrt{\|H\|} < 3\sqrt{\delta}$$

$$V = \exp(X), \quad W = \exp(Y)$$

$$\|U - VWV^\dagger W^\dagger\| < 156 \delta^{3/2} \quad \text{from precise estim. of}$$

BCH formula. (here δ_0 will pick up d)Proof of Solovay-Kitaev thm $\left(\frac{C_2 \geq \log 5 / \log(3/2)}{\varepsilon} < \delta_0, 27/6 \sqrt{\varepsilon} < \frac{1}{e}\right)$ Fix $U \in SU(d)$, take $V \in S$, $\|U - V\| < \varepsilon$

$$\text{Step 1-1} \quad \exists V_1, W_1 \in SU(d) \quad \|I_d - V_1\|, \|I_d - W_1\| < 3\sqrt{\varepsilon}$$

$$\|U - V_1 V_1^\dagger W_1 W_1^\dagger\| < 150 \varepsilon^{3/2} \quad (\text{Lem 3}) \text{ for } V_1^\dagger U$$

$$\text{Step 1-2} \quad \exists \tilde{V}_1, \tilde{W}_1 \in S \quad \|U - V \tilde{V}_1 \tilde{W}_1 \tilde{V}_1^\dagger \tilde{W}_1^\dagger\| < 276 \varepsilon^{3/2} (< \varepsilon)$$

$$\text{take } \|V_1 - \tilde{V}_1\|, \|W_1 - \tilde{W}_1\| < \varepsilon$$

$$\rightarrow \|V_1 W_1 V_1^\dagger W_1^\dagger - \tilde{V}_1 \tilde{W}_1 \tilde{V}_1^\dagger \tilde{W}_1^\dagger\| < 42 \cdot 3\sqrt{\varepsilon} \cdot \varepsilon = 126 \varepsilon^{3/2}$$

↑ Key Lem.

Combine with Step 1-1.

$$\text{Step 2-0} \quad \text{put } \varepsilon_2 = 276 \varepsilon^{3/2}, \quad S_2 = \{V_0 V_1 V_2 V_3 V_4 : V_i \in S\}$$

$$\text{we know } \forall U \exists V^{(2)} \in S_2 \quad \|U - V\| < \varepsilon_2 \quad \text{by Step 1-2.}$$

$$\text{Step 2-1} \quad \exists V_2, W_2 \in SU(d) \quad \|U - V^{(2)} V_2 W_2 V_2^\dagger W_2^\dagger\| < 3\sqrt{\varepsilon_2}$$

$$\text{Step 2-2} \quad \exists \tilde{V}_2, \tilde{W}_2 \in S_2 \quad \|U - V^{(2)} \tilde{V}_2 \tilde{W}_2 \tilde{V}_2^\dagger \tilde{W}_2^\dagger\| < 276 \varepsilon_2^{3/2}$$

$$= 276^{1+3/2} \varepsilon^{(3/2)^2}$$

$$\text{Step } n-2 : \exists V^{(n)}, \tilde{V}_n, \tilde{W}_n \in S_n = \{V_0 \dots V_{L_{n-1}} : V_i \in S, L_n = 5^{n+1}\}$$

$$\|U - V^{(n)} \tilde{V}_n \tilde{W}_n \tilde{V}_n^\dagger \tilde{W}_n^\dagger\| < \delta_n' = 276^{1+3/2+\dots+(3/2)^{n-1}} \varepsilon^{(3/2)^n}$$

$$= (276^2 \cdot \varepsilon)^{(3/2)^n} < e^{-(3/2)^n}$$

This shows. U has approx. by prod. of $L_n = 5^n$ factors of elems of S , with error $e^{-(3/2)^n} = \delta_n$

$$\log \log \frac{1}{\delta_n} \geq \log \log e^{(3/2)^n} = n \cdot \log \frac{3}{2} = \frac{\log 3/2}{\log 5} \log \frac{5 L_n}{L_n}$$

$$\text{i.e. } L_n \leq \left(\log \frac{1}{\delta}\right)^{C_2} \quad C_2 = \frac{\log 5}{\log 3/2}$$