Solovay–Kitaev theorem

Ryuhei Mori

Tokyo Institute of Technology

January 14, 2020

Solovay–Kitaev theorem

Theorem

Assume that $\{U_1, \ldots, U_k\}$ *generates a dense subset of* $\mathrm{SU}(2)$*. Then, any* $U \in \mathrm{SU}(2)$ *can be approxmiated with error* ϵ *by* $[\log(1/\epsilon)]^c$ *multiplications of* $\{U_1, \ldots, U_k\}$ *for* $c = \log 5/\log(3/2) \approx 3.97$*.*

Special unitary group

- $\mathrm{U}(n) :=$ the set of $n \times n$ unitary matrices.

- $\mathrm{SU}(n) :=$
  the set of $n \times n$ unitary matrices U with $\det(U) = 1$.

- $\mathrm{U}(n)$ and $\mathrm{SU}(n)$ are groups.

- For $U \in \mathrm{SU}(n)$ and $V \in \mathrm{U}(n)$, $VUV^\dagger \in \mathrm{SU}(n)$.

- For $V \in \mathrm{U}(n)$ and $W \in \mathrm{U}(n)$, $VWV^\dagger W^\dagger \in \mathrm{SU}(n)$.

Special unitary group and rotation

For a real unit vector $\hat{n} = [n_X \ n_Y \ n_Z]$, let

$$R_{\hat{n}}(\theta) := \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}(n_X X + n_Y Y + n_Z Z).$$

For any $U \in \mathrm{U}(2)$, there exist α, $\theta \in \mathbb{R}$ and a real unit three-dimensional vector $\hat{n}$ such that $U = \mathrm{e}^{i\alpha} R_{\hat{n}}(\theta)$.

$U \in \mathrm{U}(2)$ is in $\mathrm{SU}(2)$ iff $\mathrm{Tr}(U) \in \mathbb{R}$ since two eigenvalues of $U \in \mathrm{SU}(2)$ are in the form $\{\mathrm{e}^{i\theta}, \mathrm{e}^{-i\theta}\}$.

$U \in \mathrm{U}(2)$ is in $\mathrm{SU}(2)$ iff $U = R_{\hat{n}}(\theta)$ for some $\theta \in \mathbb{R}$ and rear unit vector $\widehat{n} \in \mathbb{R}^3$.

Special unitary group and commutator

Theorem

For any $U \in \mathrm{SU}(2)$, *there exist* V, $W \in \mathrm{U}(2)$ *such that* $U = VWV^\dagger W^\dagger$.

Proof.

$R_Z(\theta)R_X(\theta)R_Z(\theta)^\dagger R_X(\theta)^\dagger = R_Z(\theta)R_X(\theta)R_Z(-\theta)R_X(-\theta)$

$$= R_Z(\theta)R_X(\theta)R_Z(-\theta)R_X(-\theta)$$

$$= \left[\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z\right]\left[\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X\right]\left[\cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}Z\right]\left[\cos\frac{\theta}{2}I + i\sin\frac{\theta}{2}\right.$$

$$= \left[\cos^4\frac{\theta}{2} + 2\cos^2\frac{\theta}{2}\sin^2\frac{\theta}{2} - \sin^4\frac{\theta}{2}\right]I + \cdots$$

$$= \left[1 - 2\sin^4\frac{\theta}{2}\right]I + \cdots = R_{\widehat{n}_\theta}(\varphi)$$

$\cos\frac{\varphi}{2} = 1 - 2\sin^4\frac{\theta}{2}$. For some $S \in \mathrm{U}(2)$ and $\varphi \in \mathbb{R}$, $U = SR_{\widehat{n}_\theta}(\varphi)S^\dagger$.
For $V := SR_Z(\theta)S^\dagger$ and $W := SR_X(\theta)S^\dagger$, $U = VWV^\dagger W^\dagger$. $\square$

Rotation matrix and distance

$$\|I - R_{\hat{n}}(\theta)\| = \left\| \begin{bmatrix} 1 - e^{i\theta/2} & 0 \\ 0 & 1 - e^{-i\theta/2} \end{bmatrix} \right\|$$
$$= \left| 1 - e^{i\theta/2} \right|$$
$$= 2 \left| \sin \frac{\theta}{4} \right|$$

For $U \in \mathrm{SU}(2)$, $V, W \in \mathrm{SU}(2)$ satisfying $U = VWV^\dagger W^\dagger$ in the construction

$$\|I - U\| = 2 \left| \sin \frac{\varphi}{4} \right| = 2\sqrt{\frac{1 - \cos\frac{\varphi}{2}}{2}} = 2\sin^2\frac{\theta}{2} \approx 8\sin^2\frac{\theta}{4} = 2\|I - V\|^2$$

With some constant $c_{\mathrm{GC}} > 1/\sqrt{2}$, $\|I - V\| \leq c_{\mathrm{GC}}\sqrt{\|I - U\|}$.

Solovay–Kitaev algorithm

function $\textsc{Solovay–Kitaev}(U, n)$
  if $n = 0$ **then**
    return Basic approximation to U
  end if
  $U_{n-1} \leftarrow \textsc{Solovay–Kitaev}(U, n-1)$
  $V, W \leftarrow \textsc{GC–Decompose}(UU_{n-1}^{\dagger})$
  $V_{n-1} \leftarrow \textsc{Solovay–Kitaev}(V, n-1)$
  $W_{n-1} \leftarrow \textsc{Solovay–Kitaev}(W, n-1)$
  return $V_{n-1}W_{n-1}V_{n-1}^{\dagger}W_{n-1}^{\dagger}U_{n-1}$.
end function

function $\textsc{GC–Decompose}(\Delta)$
  return (V, W) satisfying $VWV^{\dagger}W^{\dagger} = \Delta$ with
$\|I - V\|, \|I - W\| \leq c_{\mathsf{GC}}\sqrt{\|I - \Delta\|}$.
end function

Analysis

Theorem

If $\|I - V\|, \|I - W\| \leq \delta$, $\|V - \widetilde{V}\|, \|W - \widetilde{W}\| \leq \Delta$

$$\|VWV^\dagger W^\dagger - \widetilde{V}\widetilde{W}\widetilde{V}^\dagger \widetilde{W}^\dagger\| \leq c_{\mathrm{B}}\Delta(\delta + \Delta)$$

From this (surprising) theorem for $\Delta = \epsilon_{n-1}$, $\delta = c_{\mathrm{GC}}\sqrt{\epsilon_{n-1}}$, for $c_{\mathrm{approx}} \approx c_B c_{\mathrm{GC}}$.

$$\ell_n \leq 5\ell_{n-1}$$
$$\epsilon_n \leq c_{\mathrm{approx}}\epsilon_{n-1}^{3/2}$$

Then,

$$\ell_n \leq 5^n \ell_0$$
$$c_{\mathrm{approx}}^2 \epsilon_n \leq c_{\mathrm{approx}}^3 \epsilon_{n-1}^{3/2} = (c_{\mathrm{approx}}^2 \epsilon_{n-1})^{3/2}$$
$$\leq (c_{\mathrm{approx}}^2 \epsilon_0)^{(3/2)^n}$$

If $\epsilon_0 < 1/c_{\mathrm{approx}}^2$, $\ell_n = O\left((\log(1/\epsilon))^{\frac{\log 5}{\log(3/2)}}\right)$.

Proof 1/2

Theorem

If $\|I - V\|, \|I - W\| \le \delta$, $\|V - \widetilde{V}\|, \|W - \widetilde{W}\| \le \Delta$

$$\|VWV^\dagger W^\dagger - \widetilde{V}\widetilde{W}\widetilde{V}^\dagger\widetilde{W}^\dagger\| \le 8\Delta^2 + 8\Delta\delta + 4\Delta\delta^2 + 4\Delta^3 + \Delta^4.$$

Proof.

Let $\Delta_V := \widetilde{V} - V$ and $\Delta_W := \widetilde{W} - W$.

$$\begin{aligned}\widetilde{V}\widetilde{W}\widetilde{V}^\dagger\widetilde{W}^\dagger = {} & VWV^\dagger W^\dagger + \Delta_V WV^\dagger W^\dagger + V\Delta_W V^\dagger W^\dagger \\ & + VW\Delta_V^\dagger W^\dagger + VWV^\dagger\Delta_W^\dagger + O(\Delta^2).\end{aligned}$$

$$\begin{aligned}\|VWV^\dagger W^\dagger - \widetilde{V}\widetilde{W}\widetilde{V}^\dagger\widetilde{W}^\dagger\| \le {} & \|\Delta_V WV^\dagger W^\dagger + VW\Delta_V^\dagger W^\dagger\| \\ & + \|V\Delta_W V^\dagger W^\dagger + VWV^\dagger\Delta_W^\dagger\| + \binom{4}{2}\Delta^2 + \binom{4}{3}\Delta^3 + \Delta^4.\end{aligned}$$

$\square$

Proof 2/2

Proof.
Let $\delta_W := W - I$.

$$\begin{aligned}\|\Delta_V W V^\dagger W^\dagger + V W \Delta_V^\dagger W^\dagger\| &= \|\Delta_V V^\dagger + V \Delta_V^\dagger + \Delta_V \delta_W V^\dagger + V \Delta_V^\dagger \delta_W^\dagger + \cdots\| \\ &\le \|\Delta_V V^\dagger + V \Delta_V^\dagger\| + 4\Delta\delta + 2\Delta\delta^2\end{aligned}$$

Since V and $V + \Delta_V$ are unitary,

$$\begin{aligned}&(V + \Delta_V)(V + \Delta_V)^\dagger = I \\ \iff &VV^\dagger + V\Delta_V^\dagger + \Delta_V V^\dagger + \Delta_V \Delta_V^\dagger = I \\ \iff &V\Delta_V^\dagger + \Delta_V V^\dagger + \Delta_V \Delta_V^\dagger = 0\end{aligned}$$

$$\|\Delta_V W V^\dagger W^\dagger + V W \Delta_V^\dagger W^\dagger\| \le \Delta^2 + 4\Delta\delta + 2\Delta\delta^2.$$

□

$c_{\mathrm{B}} \approx 8.$

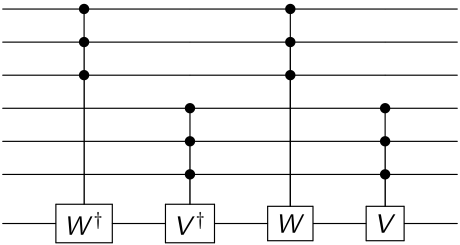
Commutator and controlled-unitary

Theorem

For any $U \in \mathrm{SU}(2)$, controlled-U gate with n controlled qubits can be realized by $O(n^2)$ CNOT and arbitrary single-qubit gates without ancillas (working qubits).

Proof.

Induction on n. For the group commutator decomposition $U = VWV^\dagger W^\dagger$ using V, $W \in \mathrm{SU}(2)$,



$S_n = 4S_{n/2} = 4^{\log n} S_1 = O(n^2)$. □

Any normal matrix has a spectral decomposition

Induction on the dimension n. Spectral decomposition theorem obviously holds for $n = 1$. M has complex eigenvalue λ. Let P be a projection to the eigenspace for λ. Let $Q = I - P$.

$$M = (P + Q)M(P + Q) = PMP + PMQ + QMP + QMQ$$

$$PMP = \lambda P$$
$$QMP = Q\lambda P = 0$$

Since $MM^\dagger |\psi\rangle = M^\dagger M |\psi\rangle = \lambda M^\dagger |\psi\rangle$, $QM^\dagger P = 0$.

$QMQ(QMQ)^\dagger = QMQM^\dagger Q = QM(I - P)M^\dagger Q = QMM^\dagger Q = QM^\dagger MQ = QM^\dagger(P + Q)MQ = QM^\dagger QMQ = (QMQ)^\dagger QMQ$.
QMQ is a linear map on linear subspace of dimension at most $n - 1$.
From the induction hypothesis, QMQ has a spectral decomposition.

Assignments (Deadline is Jan. 24)

1. Show a group commutator decomposition in SU(2) of

$$U = \begin{bmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{bmatrix}$$

   i.e., show V and W in SU(2) satisfying $VWV^\dagger W^\dagger = U$.

2. [Very advanced] By modifying levels of Solovay–Kitaev algorithm in the recursion, can we improve the exponent $c = \log 5 / \log(3/2)$?