Universality of quantum circuit

Ryuhei Mori

Tokyo Institute of Technology

5, Nov., 2021

Universality of a quantum circuit

Theorem (Universality of finite gate set)

For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ and $\epsilon > 0$, there is a quantum circuit with X, Y, Z, H, S, T, CNOT gates computing $\widetilde{U}$ satisfying $\|U - \widetilde{U}\| < \epsilon$.

Proof.

1. Any unitary matrix can be decomposed to a product of two-level unitary matrices. Done

2. Any two-level unitary matrix can be decomposed to a product of controlled-unitary gates. Done

3. Any controlled-untary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

4. Any single-qubit gate can be approximated by X, Y, Z, H, S and T.

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

- For $U \in \mathrm{U}(n)$, there exists $V \in \mathrm{SU}(n)$ and $\theta \in \mathbb{R}$ such that $U = \mathrm{e}^{i\theta} V$.

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

1. Controlled-U(2) with single controlled qubit.
2. Controlled-SU(2) with n controlled qubits.
3. Controlled-U(2) with n controlled qubits.

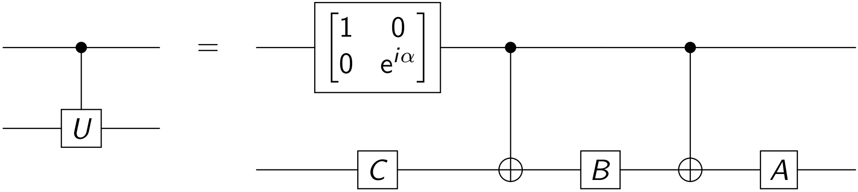
□

Decomposition of single qubit unitary

Lemma

Any single qubit unitary $U \in \mathrm{U}(2)$, there is single qubit unitary matrices A, B, C such that $ABC = I$ and $\mathrm{e}^{i\alpha} AXBXC = U$.

From this lemma,



Decomposition of single qubit unitary

Lemma

Any single qubit unitary $U \in \mathrm{U}(2)$, there is single qubit unitary matrices A, B, C and $\alpha \in \mathbb{R}$ such that $ABC = I$ and $\mathrm{e}^{i\alpha} AXBXC = U$.

Proof.

For any $U \in \mathrm{U}(2)$, there exists $\alpha \in [0, 2\pi)$ and $V \in \mathrm{SU}(2)$ such that $U = e^{i\alpha} V$.

For $R_Z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$, $XR_Z(\theta)XR_Z(-\theta) = R_Z(-2\theta)$.

For any $V \in \mathrm{SU}(2)$, there exists $\theta \in [0, 2\pi)$ and $P \in \mathrm{SU}(2)$ such that

$$V = PR_Z(-2\theta)P^\dagger = PXR_Z(\theta)XR_Z(-\theta)P^\dagger.$$

$A = P$, $B = R_Z(\theta)$, $C = R_Z(-\theta)P^\dagger$ satisfy the conditions. □

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

1. Controlled-U(2) with single controlled qubit. Done
2. Controlled-SU(2) with n controlled qubits.
3. Controlled-U(2) with n controlled qubits.

□

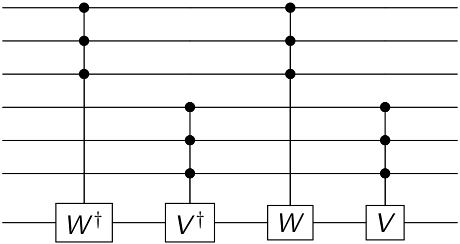
Group commutator and controlled-unitary

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 $V = PiXP^\dagger$, $W = PR_Z(\theta)P^\dagger \in \mathrm{SU}(2)$ for some $\theta \in [0, 2\pi)$ and $P \in \mathrm{SU}(2)$.



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

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

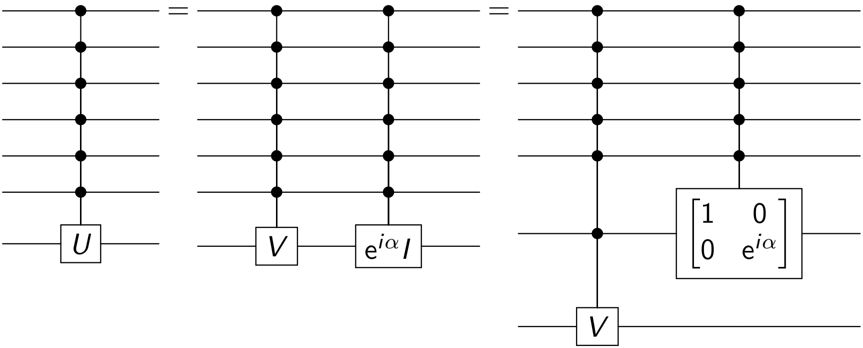
Proof.

1. Controlled-U(2) with single controlled qubit. Done
2. Controlled-SU(2) with n controlled qubits. Done
3. Controlled-U(2) with n controlled qubits.

□

Controlled-$U(2)$ with n controlled qubits

For any $U \in \mathrm{U}(2)$, there exists $V \in \mathrm{SU}(2)$ and $\alpha \in \mathbb{R}$ such that $U = \mathrm{e}^{i\alpha} V$.



$$A_n = S_n + A_{n-1} = O(n^3)$$

Controlled-unitary

Theorem

Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

1. Controlled-U(2) with single controlled qubit. Done
2. Controlled-SU(2) with n controlled qubits. Done
3. Controlled-U(2) with n controlled qubits. Done

□

Universality of a quantum circuit

Theorem (Universality of finite gate set)

For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ *and* $\epsilon > 0$*, there is a quantum circuit with* X, Y, Z, H, S, T, CNOT *gates computing* $\widetilde{U}$ *satisfying* $\|U - \widetilde{U}\| < \epsilon$*.*

Proof.

1. Any unitary matrix can be decomposed to a product of two-level unitary matrices. Done
2. Any two-level unitary matrix can be decomposed to a product of controlled-unitary gates. Done
3. Any controlled-untary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates. Done
4. Any single-qubit gate can be approximated by X, Y, Z, H, S and T.

Approximation of a single-qubit gate is sufficient

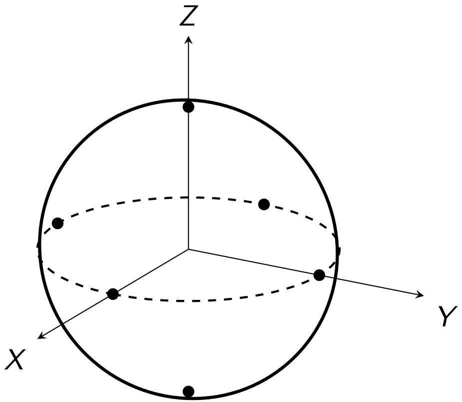
Theorem

Any single-qubit gate can be approximated by X, Y, Z, H, S and T.

Assume that this theorem holds. For $A \in L(\mathbb{C}^d)$, Let $\|A\|$ be the spectral norm, which satisfies $\|UAV\| = \|A\|$ for any unitary matrices U and V. Assume $\|U_i - V_i\| \leq \epsilon$ for $i = 1, \ldots, m$.

$$
\begin{aligned}
&\|U_m U_{m-1} \cdots U_1 - V_m V_{m-1} \cdots V_1\| \\
&= \left\| \sum_{i=1}^{m} (U_m \cdots U_i V_{i-1} \cdots V_1 - U_m \cdots U_{i+1} V_i \cdots V_1) \right\| \\
&\leq \sum_{i=1}^{m} \|U_m \cdots U_i V_{i-1} \cdots V_1 - U_m \cdots U_{i+1} V_i \cdots V_1\| \\
&= \sum_{i=1}^{m} \|U_m \cdots U_{i+1} (U_i - V_i) V_{i-1} \cdots V_1\| = \sum_{i=1}^{m} \|U_i - V_i\| \leq m\epsilon.
\end{aligned}
$$

Universality of X, Y, Z, H, S, T



Special unitary group and rotation

$$
\begin{aligned}
\mathrm{SU}(2) \ni U &= \exp\{i(\alpha_X X + \alpha_Y Y + \alpha_Z Z)\} \\
&= \sum_{j=0}^{\infty} \frac{i^j}{j!}(\alpha_X X + \alpha_Y Y + \alpha_Z Z)^j \\
&= \sum_{j=0}^{\infty} \frac{(-1)^j}{(2j)!}(\alpha_X X + \alpha_Y Y + \alpha_Z Z)^{2j} \\
&\quad + i \sum_{j=0}^{\infty} \frac{(-1)^j}{(2j+1)!}(\alpha_X X + \alpha_Y Y + \alpha_Z Z)^{2j+1} \\
&= \cos\left(\sqrt{\alpha_X^2 + \alpha_Y^2 + \alpha_Z^2}\right) I \\
&\quad + i \sin\left(\sqrt{\alpha_X^2 + \alpha_Y^2 + \alpha_Z^2}\right) \frac{\alpha_X X + \alpha_Y Y + \alpha_Z Z}{\sqrt{\alpha_X^2 + \alpha_Y^2 + \alpha_Z^2}}.
\end{aligned}
$$

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 $U \in \mathrm{SU}(2)$, there exist $\theta \in [0, 2\pi)$ and a real unit three-dimensional vector $\hat{n}$ such that $U = R_{\hat{n}}(\theta)$.

Universality of X, Y, Z, H, S, T

$T \cong R_Z(\pi/4)$. $HTH \cong R_X(\pi/4)$.

$$\begin{aligned}
R_Z(\pi/4)R_X(\pi/4) &= \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right] \\
&= \cos^2\frac{\pi}{8}I - i\sin\frac{\pi}{8}\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right] \\
&=: \cos\frac{\eta}{2}I - i\sin\frac{\eta}{2}\left(n_x X + n_Y Y + n_Z Z\right) \\
&= R_{\widehat{n}}(\eta)
\end{aligned}$$

where η satisfying $\cos(\eta/2) = \cos^2(\pi/8)$ and $\widehat{n}$ is a unit vector along with $(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$. Here, η is an irrational multiple of π. $HR_{\widehat{n}}(\eta)H = R_{\widehat{m}}(\eta)$ where $\widehat{m}$ is a unit vector along with $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.

For any $U \in \mathrm{SU}(2)$, there exists $\beta, \gamma, \delta \in [0, 2\pi)$ such that $U = R_{\widehat{n}}(\beta)R_{\widehat{m}}(\gamma)R_{\widehat{n}}(\delta)$.

Universality of a quantum circuit

Theorem (Universality of finite gate set)

For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ *and* $\epsilon > 0$, *there is a quantum circuit with* X, Y, Z, H, S, T, CNOT *gates computing* $\widetilde{U}$ *satisfying* $\|U - \widetilde{U}\| < \epsilon$.

Proof.

1. Any unitary matrix can be decomposed to a product of two-level unitary matrices. Done
2. Any two-level unitary matrix can be decomposed to a product of controlled-unitary gates. Done
3. Any controlled-untary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates. Done
4. Any single-qubit gate can be approximated by X, Y, Z, H, S and T. Done

Solovay–Kitaev theorem

Theorem

Assume $\{U_1, \dots, U_k\}$ *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* $\{U_1, \dots, U_k\}$*.*

Assignments

1. Prove that for any $U \in \mathrm{SU}(2)$, there exists $\beta, \gamma, \delta \in [0, 2\pi)$ such that $U = R_Z(\beta)R_Y(\gamma)R_Z(\delta)$ or $U = -R_Z(\beta)R_Y(\gamma)R_Z(\delta)$.