

Universality of quantum circuit

Ryuhei Mori

Tokyo Institute of Technology

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 $X, Y, Z, H, S, T, \text{CNOT}$ gates computing \tilde{U} satisfying $D(U, \tilde{U}) < \epsilon$.

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-unitary 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

- $U(n) :=$ the set of $n \times n$ unitary matrices.
- $SU(n) :=$
the set of $n \times n$ unitary matrices U with $\det(U) = 1$.
- $U(n)$ and $SU(n)$ are groups.
- For $U \in SU(n)$ and $V \in U(n)$, $VUV^\dagger \in SU(n)$.
- For $V \in U(n)$ and $W \in U(n)$, $VWV^\dagger W^\dagger \in SU(n)$.
- For $U \in U(n)$, there exists $V \in SU(n)$ and $\theta \in \mathbb{R}$ such that $U = e^{i\theta} V$.

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.

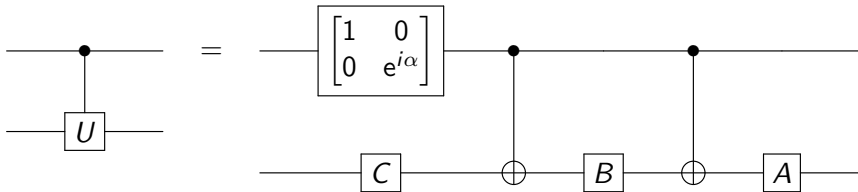


Decomposition of single qubit unitary

Lemma

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

From this lemma,



Decomposition of single qubit unitary

Lemma

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

Proof.

For any $U \in \text{U}(2)$, there exists $\alpha \in [0, 2\pi)$ and $V \in \text{SU}(2)$ 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 $V \in \text{SU}(2)$, there exists $\theta \in [0, 2\pi)$ and $P \in \text{SU}(2)$ 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

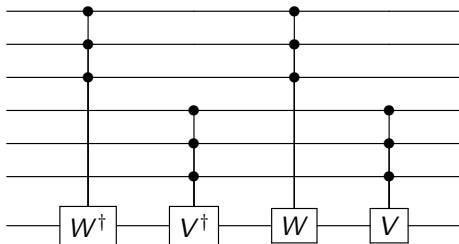
Theorem

For any $U \in \text{SU}(2)$, 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 $V = P i X P^\dagger$, $W = P R_Z(\theta) P^\dagger \in \text{SU}(2)$ for some $\theta \in [0, 2\pi)$ and $P \in \text{SU}(2)$.



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



Controlled-unitary

Theorem

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

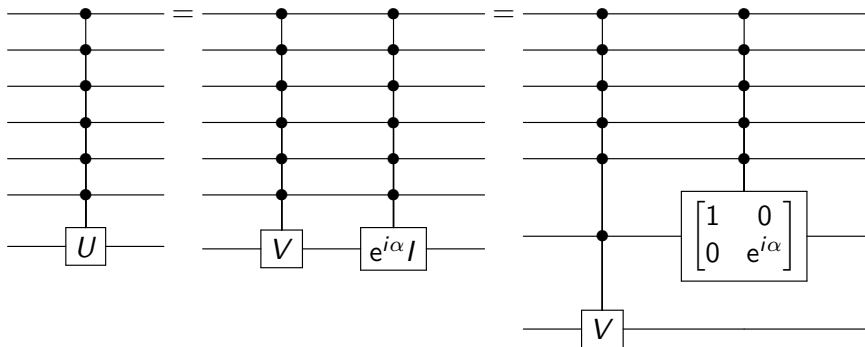
Proof.

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



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

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 $X, Y, Z, H, S, T, \text{CNOT}$ gates computing \tilde{U} satisfying $D(U, \tilde{U}) < \epsilon$.

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-unitary 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

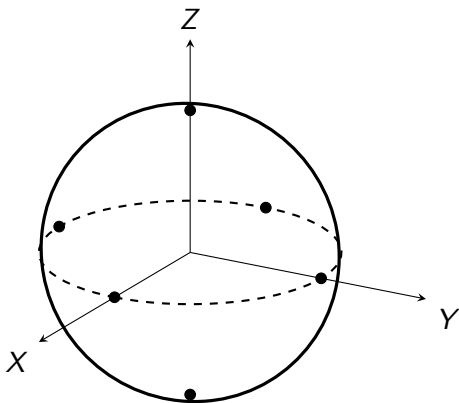
Theorem

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

This theorem shows the universality of the gate set with CNOT. Assume $D(U_i, V_i) \leq \epsilon$ for $i = 1, \dots, m$.

$$\begin{aligned} & D(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \\ & \leq \sum_{i=1}^m D(U_m \cdots U_i V_{i-1} \cdots V_1, U_m \cdots U_{i+1} V_i \cdots V_1) \quad (\text{triangle inequality}) \\ & = \sum_{i=1}^m D(U_i, V_i) \quad (\text{unitary invariance}) \\ & \leq m\epsilon. \end{aligned}$$

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



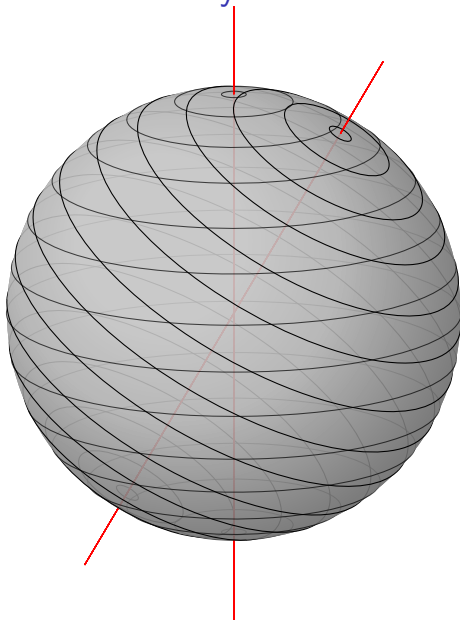
Universality of X, Y, Z, H, S, T

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

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

where η satisfying $\cos(\eta/2) = \cos^2(\pi/8)$ and \hat{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** . $HR_{\hat{n}}(\eta)H = R_{\hat{m}}(\eta)$ where \hat{m} is a unit vector along with $(\cos \frac{\pi}{8}, -\sin \frac{\pi}{8}, \cos \frac{\pi}{8})$.

Universality of two rotations $1/2$



Universality of two rotations 2/2

Theorem

For any $U \in \text{SU}(2)$, there exists $n \in \mathbb{Z}_{\geq 0}$ and $\alpha_1, \dots, \alpha_n \in (0, 2\pi)$ such that $R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\alpha_2)R_{\hat{n}}(\alpha_3) \cdots R_{\hat{n}}(\alpha_n)$ is equal to U or $-U$.

Proof.

Let $|\psi\rangle$ and $|\psi^\perp\rangle$ be the eigenvectors of $R_{\hat{n}}(\theta)$.

Let $|\varphi\rangle := U|\psi\rangle$, $|\varphi^\perp\rangle := U|\psi^\perp\rangle$.

There exists $n \in \mathbb{Z}_{\geq 0}$ and $\theta_0, \theta_1, \alpha_1, \dots, \alpha_n \in (0, 2\pi)$ such that

$$\begin{aligned} |\varphi\rangle &= e^{i\theta_0} R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\alpha_2)R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) |\psi\rangle \\ &= e^{i(\theta_0 + \frac{\alpha_n}{2})} R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\alpha_2)R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) R_{\hat{n}}(\alpha_n) |\psi\rangle \\ |\varphi^\perp\rangle &= e^{i\theta_1} R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\alpha_2)R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) |\psi^\perp\rangle \\ &= e^{i(\theta_1 - \frac{\alpha_n}{2})} R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\alpha_2)R_{\hat{n}}(\alpha_3) \cdots R_{\hat{m}}(\alpha_{n-1}) R_{\hat{n}}(\alpha_n) |\psi^\perp\rangle. \end{aligned}$$

By choosing $\alpha_n = \theta_1 - \theta_0$, then $\theta_0 + \frac{\alpha_n}{2} = \theta_1 - \frac{\alpha_n}{2}$. Hence, $R_{\hat{n}}(\alpha_1) \cdots R_{\hat{n}}(\alpha_n)$ maps $|\psi\rangle \mapsto e^{i\theta} |\varphi\rangle$, $|\psi^\perp\rangle \mapsto e^{i\theta} |\varphi^\perp\rangle$, implying $R_{\hat{n}}(\alpha_1) \cdots R_{\hat{n}}(\alpha_n) = e^{i\theta} U$. Since $U \in \text{SU}(2)$, θ must be 0 or π .

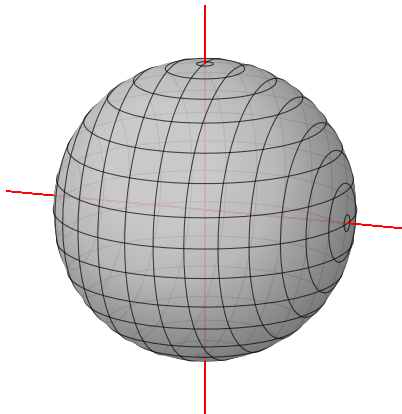


Matrix decomposition

Corollary

For any $U \in \text{U}(2)$, there exists $\alpha, \beta, \gamma, \delta \in (0, 2\pi)$ such that $U = e^{i\alpha} R_Z(\beta) R_Y(\gamma) R_Z(\delta)$.

Proof.



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 $X, Y, Z, H, S, T, \text{CNOT}$ gates computing \tilde{U} satisfying $D(U, \tilde{U}) < \epsilon$.

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-unitary 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 $SU(2)$. Then, any $U \in SU(2)$ can be approximated with error ϵ by $[\log(1/\epsilon)]^c$ multiplications of $\{U_1, \dots, U_k\}$ for some constant c .

Assignments

- 1 Show a quantum circuit for controlled- $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ gate with **two** controlled qubits using the CNOT gates and arbitrary single-qubit gates.
- 2 [Advanced] Show a quantum circuit for controlled- $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ gate with **two** controlled qubits using **six** CNOT gates and **seven** T and T^\dagger gates.