Universality of quantum circuit

Ryuhei Mori

Tokyo Institute of Technology

January 10, 2020

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.

Controlled-unitary

Theorem

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

Proof.

1. Controlled-unitary with single controlled qubit.
2. Controlled-unitary with two controlled qubit.
3. Controlled-unitary with n controlled qubit.

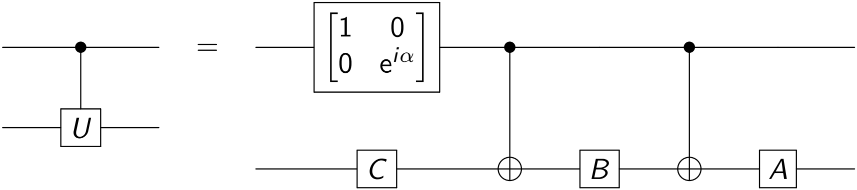
□

Decomposition of single qubit unitary

Lemma

Any single qubit unitary U, 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, 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 2×2 unitary matrix, there exist α, β, γ, $\delta \in \mathbb{R}$ such that

$$U = e^{i\alpha} R_Z(\beta) R_Y(\gamma) R_Z(\delta)$$

Let $A := R_Z(\beta) R_Y(\gamma/2)$, $B := R_Y(-\gamma/2) R_Z(-(\beta+\delta)/2)$, $C := R_Z((\delta-\beta)/2)$. Then, $ABC = I$. Since $R_Y(\theta)X = XR_Y(-\theta)$ and $R_Z(\theta)X = XR_Z(-\theta)$,.

$$\begin{aligned} AXBXC &= R_Z(\beta)R_Y(\gamma/2)XR_Y(-\gamma/2)R_Z(-(\beta+\delta)/2)XR_Z((\delta-\beta)/2) \\ &= R_Z(\beta)R_Y(\gamma/2)R_Y(\gamma/2)R_Z((\beta+\delta)/2)R_Z((\delta-\beta)/2) \\ &= R_Z(\beta)R_Y(\gamma)R_Z(\delta) = e^{-i\alpha}U. \end{aligned}$$

Theorem

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

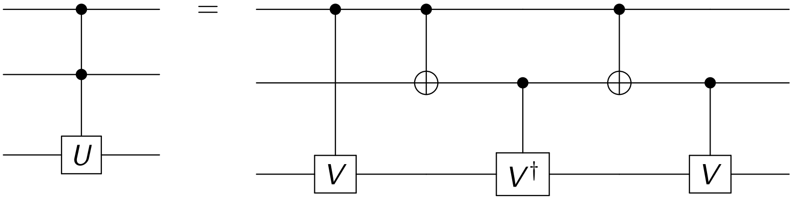
Proof.

1. Controlled-unitary with single controlled qubit. Done
2. Controlled-unitary with two controlled qubit.
3. Controlled-unitary with n controlled qubit.

$\square$

Decomposition of two qubit unitary

For V satisfying $V^2 = U$,



Controlled-unitary

Theorem

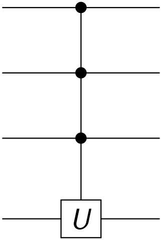
Any controlled-unitary gate can be decomposed to a product of CNOT and arbitrary single-qubit gates.

Proof.

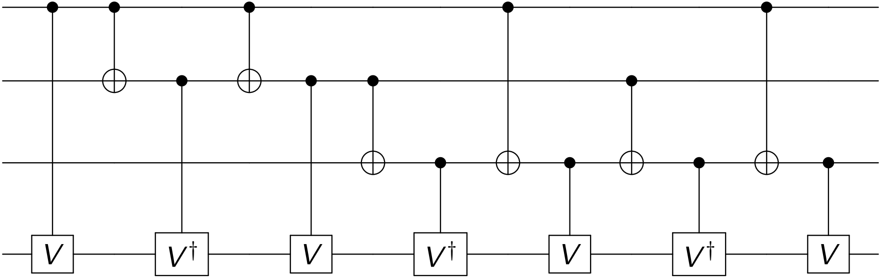
1. Controlled-unitary with single controlled qubit. Done
2. Controlled-unitary with two controlled qubit. Done
3. Controlled-unitary with n controlled qubit.

□

For V satisfying $V^4 = U$,



$=$



Grey code

$$000 \mapsto 001 \mapsto 011 \mapsto 010 \mapsto 110 \mapsto 111 \mapsto 101 \mapsto 100$$

$$1 \mapsto 2 \mapsto 1 \mapsto 3 \mapsto 1 \mapsto 2 \mapsto 1$$

$$x_1+x_2+x_3-(x_1\oplus x_2)-(x_2\oplus x_3)-(x_3\oplus x_1)+(x_1\oplus x_2\oplus x_3) = 4(x_1\wedge x_2\wedge x_3)$$

n controlled qubits

Theorem

For any single-qubit unitary U,

$$\sum_{S\subseteq\{1,2,\ldots,n\}} (-1)^{|S|+1} \left(\bigoplus_{i\in S} x_i\right) = 2^{n-1} \bigwedge_{i=1}^{n} x_i$$

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

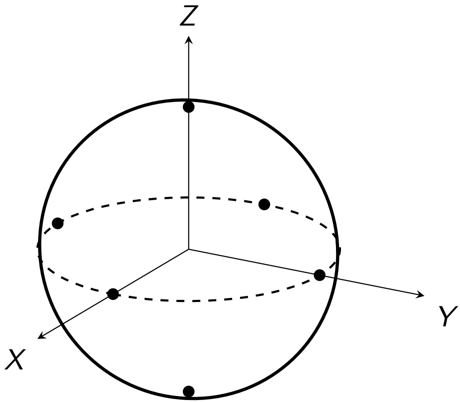
Theorem

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 $\|U_i - V_i\| \le \epsilon$ for $i = 1, \ldots, m$.

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

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



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

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

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

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 $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.

$U = e^{i\alpha}R_{\widehat{n}}(\beta)R_{\widehat{m}}(\gamma)R_{\widehat{n}}(\delta)$.

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

Let $\{U_1, \dots, U_k\}$ be a dense subset of $\mathsf{SU}(2)$. Then, any $U \in \mathsf{SU}(2)$ can be approxmiated with error ϵ by $[\log(1/\epsilon)]^c$ multiplications of $\{U_1, \dots, U_k\}$.