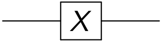
Universality of quantum circuit

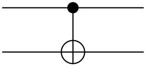
Ryuhei Mori

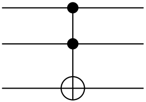
Tokyo Institute of Technology

January 7, 2020

- Quantum circuit is a model of computation of Boolean functions which consists of quantum gates.

- Single qubit gate: X gate, Y gate, Z gate, H gate, $S := \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ gate $T := \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix}$ gate 

- Two qubit gate: CNOT gate 

- Three qubit gate: Toffoli gate 

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

Two-level unitary matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_{11} & 0 & 0 & 0 & 0 & u_{12} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & u_{21} & 0 & 0 & 0 & 0 & u_{22} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

There exist $x \neq y \in \{0,1\}^n$ such that

$$|x\rangle \longmapsto u_{1,1}\,|x\rangle + u_{1,2}\,|y\rangle$$
$$|y\rangle \longmapsto u_{2,1}\,|x\rangle + u_{2,2}\,|y\rangle$$

and for any $z \in \{0,1\}^n \setminus \{x,y\}$, $|z\rangle \longmapsto |z\rangle$.

Two-level unitary matrix

Theorem (Decomposition to two-level unitary matrices)

For any unitary matrix $U \in L(\mathbb{C}^d)$, there is a sequence $U_1, U_2, \dots, U_m$ of two-level unitary matrices such that $U = U_1 U_2 \cdots U_m$.

Proof.

We will show that there is a sequence $V_1, V_2, \dots, V_m$ of two-level unitary matrices such that

$$V_m V_{m-1} \cdots V_1 U = I.$$

Since $U_i := V_i^{-1}$ is two-level unitary, this completes a proof. $\square$

Decomposition to two-level unitary matrix 1/3

$$U = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} \\ u_{4,1} & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix}$$

If $u_{2,1} = 0$, we skip this step.
If $u_{2,1} \neq 0$, apply the two-level unitary matrix

$$V_1 = \frac{1}{z} \begin{bmatrix} u_{1,1}^* & u_{2,1}^* & 0 & 0 \\ u_{2,1} & -u_{1,1} & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & z \end{bmatrix}$$

for $z := \sqrt{|u_{1,1}|^2 + |u_{2,1}|^2}$.

Decomposition to two-level unitary matrix 2/3

$$V_1 U = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} \\ 0 & u_{2,2} & u_{2,3} & u_{2,4} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} \\ u_{4,1} & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix}$$

$u_{i,j}$s are not equal to those in the previous slide for $i \in \{1, 2\}$.

If $u_{3,1} = 0$, we skip this step.
If $u_{3,1} \neq 0$, apply the two-level unitary matrix

$$V_2 = \frac{1}{z} \begin{bmatrix} u_{1,1}^* & 0 & u_{3,1}^* & 0 \\ 0 & z & 0 & 0 \\ u_{3,1} & 0 & -u_{1,1} & 0 \\ 0 & 0 & 0 & z \end{bmatrix}$$

for $z := \sqrt{|u_{1,1}|^2 + |u_{3,1}|^2}$.

Decomposition to two-level unitary matrix 3/3

$$V_3 V_2 V_1 U = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} \\ 0 & u_{2,2} & u_{2,3} & u_{2,4} \\ 0 & u_{3,2} & u_{3,3} & u_{3,4} \\ 0 & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix} = \begin{bmatrix} u_{1,1} & 0 & 0 & 0 \\ 0 & u_{2,2} & u_{2,3} & u_{2,4} \\ 0 & u_{3,2} & u_{3,3} & u_{3,4} \\ 0 & u_{4,2} & u_{4,3} & u_{4,4} \end{bmatrix}$$

$u_{1,1} = 1$ unless $u_{2,1}$, $u_{3,1}$, $u_{4,1}$ are originally 0. In this case, apply one-level unitary for making $u_{1,1} = 1$.

Arbitrary $d \times d$ unitary matrix can be decomposed to a product of at most $d(d-1)/2$ two-level unitary matrices for $d \geq 2$.

Universality of a quantum circuit

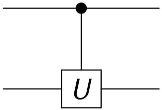
Theorem (Universality of finite gate set)

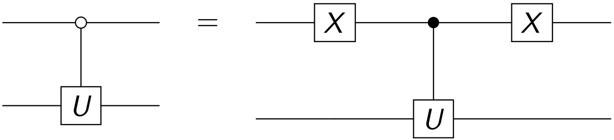
For any unitary matrix $U \in L(\mathbb{C}^{2^n})$ and $\epsilon > 0$, there is a quantum circuit with X, Y, Z, H, S, T, CNOT gates computing $\widetilde{U}$ satisfying $\|U - \widetilde{U}\| < \epsilon$.

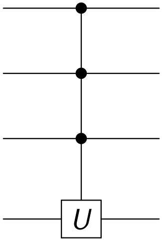
Proof.

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.
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

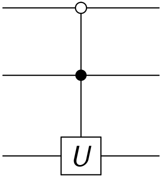






Special cases

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_{1,1} & 0 & 0 & 0 & u_{1,2} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & u_{2,1} & 0 & 0 & 0 & u_{2,2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$



Universality of a quantum circuit

Lemma

Any $2^n \times 2^n$ two-level unitary matrix can be decomposed to a product of controlled-unitary gates.

Proof.

Assume that the two-level unitary matrix acts on a 2-dimentional subspace span($\{|x\rangle, |y\rangle\}$) for $x \neq y \in \{0,1\}^n$.

Assume that for $i \in \{1, 2, \ldots, n\}$, $x_i = 1$ and $y_i = 0$. Apply at most

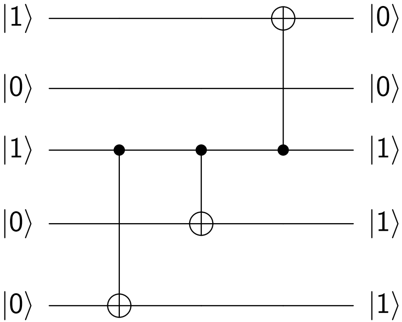
$n - 1$ CNOT gates such that

$$
\begin{aligned}
&& |x\rangle &\longmapsto |y \oplus e_i\rangle \\
&& |y\rangle &\longmapsto |y\rangle \\
\forall z \neq x, y \qquad \exists \tilde{z} \neq x, y \qquad && |z\rangle &\longmapsto |\tilde{z}\rangle ,
\end{aligned}
$$

Then, apply "controlled unitary" and reverse the permutation of the basis. □

The first part

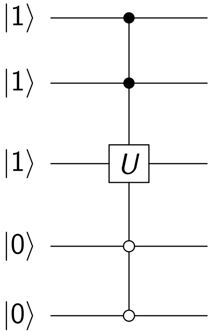
Let $x = 00\textcolor{red}{1}01$, $y = 11\textcolor{red}{0}00$.



$$|00101\rangle \longmapsto |11\textcolor{red}{1}00\rangle$$
$$|11000\rangle \longmapsto |11\textcolor{red}{0}00\rangle$$

Controlled-unitary

$$|x\rangle = |00101\rangle \longmapsto |11\textcolor{red}{1}00\rangle$$
$$|y\rangle = |11000\rangle \longmapsto |11\textcolor{red}{0}00\rangle$$

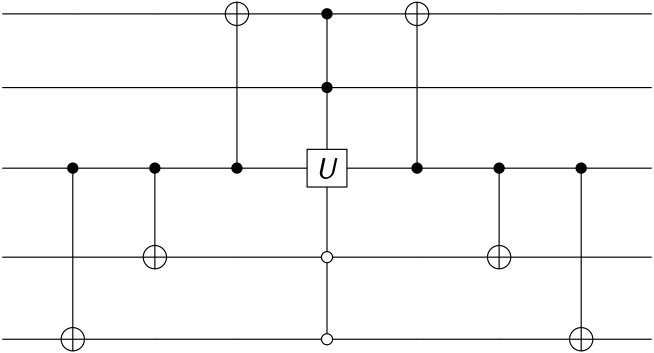


Finally, reverse the basis

$$|11\textcolor{red}{1}00\rangle \longmapsto |00101\rangle = |x\rangle$$
$$|11\textcolor{red}{0}00\rangle \longmapsto |11000\rangle = |y\rangle$$

Whole quantum circuit

Let $x = 00101$, $y = 11000$.



$$|00101\rangle \longmapsto |11100\rangle \longmapsto |00101\rangle$$

$$|11000\rangle \longmapsto |11000\rangle \longmapsto |11000\rangle$$

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.

Assignments (Deadline is Jan. 17)

1. Show a decomposition of

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

into a product of two-level unitary matrices.

2. Show a decomposition of two-level unitary

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

into a product of controlled-unitary gates.