4. Basics of Quantum Computer

Vaughan Sohn

October 10, 2024

Contents

Quantum Circuit model

Quantum Gates

Universial Quantum gate set: {CNOT, single qubit gates}

Universial Quantum Discrete gate set: {CNOT, H, S, T}

Measurement

Quantum Circuit model

Component of quantum circuit model

- Classical computer를 표현하기 위해서 circuit model을 사용한 것 처럼, quantum computer를 표현하기 위한 circuit model을 설계할 수 있다.
- Quantum circuit은 정보의 단위로 *qubit*를 사용하며, logic gate와 같이 간단한 연산을 수행하는 quantum gate를 이용한다.
- Qubit와 quantum gate는 다음과 같은 특징을 가진다.
  - Qubit는 superposition, entanglement와 같은 특징을 가진다.
  - Quantum gate는 input과 output qubit의 개수가 동일한 *unitary operator*여야 한다.
- Quantum circuit은 다음과 같이 나타낸다. Operation 순서는 left to right, qubit의 나열순서는 top to bottom이다. ⇒ Matrix-vector 표기법과의 순서를 혼동하지 않도록 주의하자.

$$|\psi\rangle = C(X)C(X)U\,|q_0q_1q_2q_3\rangle$$

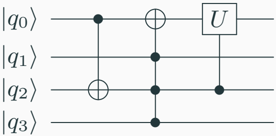


Table 1: Quantum Circuit

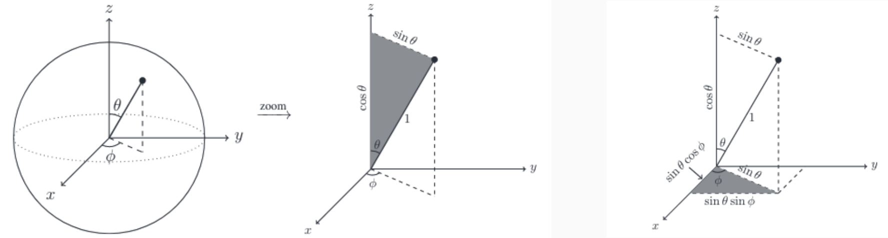
Qubit

- Computational basis $\{ket0, |1\rangle\}$에 대하여 single qubit은 다음과 같이 표현한다.

$$
\begin{aligned}
|\psi\rangle &= a\,|0\rangle + b\,|1\rangle \\
&= e^{i\alpha}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\right) \\
&= \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle
\end{aligned}
$$

- Bloch sphere를 이용하여 2개의 parameter (θ, ϕ)에 대해 qubit을 나타낼 수 있다.

$$|\psi\rangle = (\sin\theta\cos\varphi,\ \sin\theta\sin\varphi,\ \cos\theta)$$



Quantum Gates

Single-qubit gate

- Pauli operator:

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Hadamard, Phase, $\pi/8$ gate [$*$]:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}.$$

$\Rightarrow$

$$T =$$

Single-qubit gate

- Rotation operator:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

- *Generalized* rotation operator:
  $\hat{n} = (n_x, n_y, n_z)$를 기준으로 θ만큼 회전을 수행하는 rotation gate.

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\hat{n}\cdot\vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_xX + n_yY + n_zZ)$$

Rotation operator

Rotation operator가 중요한 이유는 서로 다른 두 axis에 대한 rotation operator가 존재한다면, single qubit unitary gate를 decomposition할 수 있기 때문이다!

Single-qubit gate decomposition

Theorem 1 (ZY decomposition)

Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that,

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

Theorem 2

Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and

$$U = e^{i\alpha} AXBXC$$

where α is some overall phase factor and X is a Pauli-X operator.

✓meaning: 어떤 single-qubit unitary gate이던지 rotation operator decomposition을 활용하면 arbitrary single qubit gate 3개와 Pauli-X gate로 나타낼 수 있다.

Single-qubit gate decomposition

∗ Proof:
Theorem 6를 이용하면, single qubit gate A, B, C를 rotation gate로 decomposition 할 수 있다. 각 gate가 다음과 같이 decomposition 된다고 하자.

- $A \triangleq R_z(\beta)R_y\left(\frac{\gamma}{2}\right)$
- $B \triangleq R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)$
- $C \triangleq R_Z\left(\frac{\delta-\beta}{2}\right)$

$$ABC =$$

$$XBX =$$

$$AXBXC =$$

Controlled gate

- Controlled gate는 기본적으로 2-qubit gate이다.
- Control qubit의 값에 따라서, target qubit에 대한 operator U의 적용 유무가 결정된다. (일반적으로 $|1\rangle$이면 적용한다는 의미)

$$C(U)\,|ct\rangle = \begin{cases} U\,|ct\rangle & \text{if } |c\rangle = |1\rangle \\ |ct\rangle & \text{if } |c\rangle = |0\rangle \end{cases}$$

- Control qubit의 spectral decomposition은 다음과 같다.

$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

- Gate symbol:
  - 점이 있는 곳이 control qubit이고 gate symbol이 있는 곳이 target qubit이다.
  - Target qubit이 검은색이면 $|1\rangle$일 때 동작함을 의미하고, 만약 속이 채워지지 않은 점이라면 $|0\rangle$일 때 동작함을 의미한다.

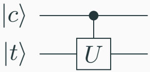


Table 2: Controlled-U gate

Controlled NOT gate

- 어떤 unitary gate이든지 controlled gate로 사용될 수 있지만, Pauli X gate에 대한 controlled gate인 CNOT gate가 특히나 더 중요하다.
- CNOT gate는 control qubit가 $|1\rangle$일 때, target qubit의 값을 반전시킨다. 마치 XOR gate처럼 동작하기 때문에, CNOT gate를 다음과 같이 표현한다.

$$C(X)|00\rangle = |00\rangle$$
$$C(X)|01\rangle = |01\rangle$$
$$C(X)|10\rangle = |11\rangle$$
$$C(X)|11\rangle = |10\rangle$$

$$C(X)|ct\rangle = |c\rangle|t \oplus c\rangle$$

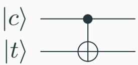
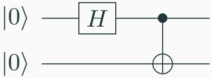


Table 3: Controlled NOT gate

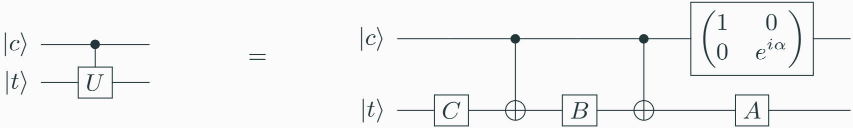
- CNOT gate를 사용하면 entangled state를 만들 수 있다.
  1. initial state: $|00\rangle$
  2. after H gate: $(H \otimes I)|00\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle$
  3. after $C(X)$ gate: $C(X)\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \rightarrow$ *Bell state!*



Controlled gate decomposition

Theorem 6를 이용하면, CNOT gate를 다음과 같이 3개의 single-qubit unitary operation A, B, C와 Controlled-X gate 2개를 사용하여 decomposition할 수 있다.

$$C(U) = e^{i\alpha} A C(X) B C(X) C$$



$$C(U)|00\rangle = |00\rangle$$
$$C(U)|01\rangle = |01\rangle$$
$$C(U)|10\rangle = |1\rangle U|0\rangle$$
$$C(U)|11\rangle = |1\rangle U|1\rangle$$

=

- If $|c\rangle = |0\rangle$:

$$\xrightarrow{I\otimes C} |0\rangle C|t\rangle \xrightarrow{C(X)} |0\rangle C|t\rangle \xrightarrow{I\otimes B} |0\rangle BC|t\rangle$$
$$\xrightarrow{C(X)} |0\rangle BC|t\rangle \xrightarrow{I\otimes A} |0\rangle ABC|t\rangle$$

- If $|c\rangle = |1\rangle$:

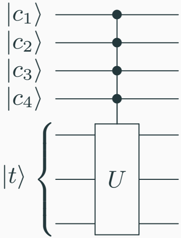
$$\xrightarrow{I\otimes C} |1\rangle C|t\rangle \xrightarrow{C(X)} |1\rangle XC|t\rangle \xrightarrow{I\otimes B} |1\rangle BXC|t\rangle$$
$$\xrightarrow{C(X)} |1\rangle XBXC|t\rangle \xrightarrow{I\otimes A} |1\rangle AXBXC|t\rangle$$

(generalize) $n+k$개의 qubit에 대해, n개가 control qubit이고 k개가 target qubit; 즉 U가 k-qubit에 대한 operator인 controlled gate는 다음과 같이 정의한다.

$$C^n(U)\,|c_1c_2\cdots c_n\rangle\,|t\rangle = |c_1c_2\cdots c_n\rangle\,U^{\prod_i c_i}\,|t\rangle$$

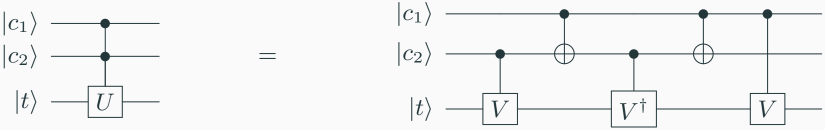
⇒ control qubit들이 모두 1이면 U operator가 적용되고, 그렇지 않으면 아무것도 수행하지 않는다.

Example $n=4, t=3$ controlled gate



Controlled gate on multiple-qubit decomposition

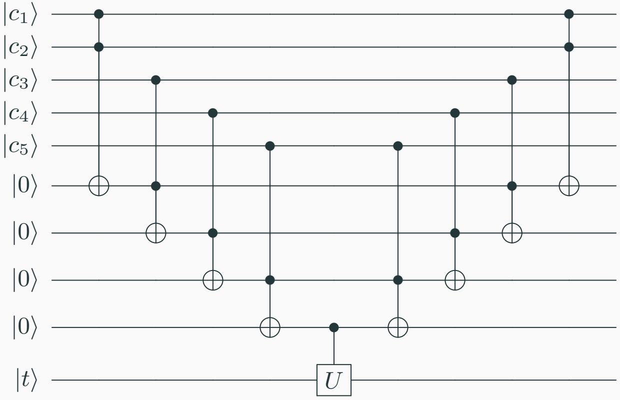
Decomposition of $C^2(U)$
Control qubit이 2개인 unitary gate는 $V^2 = U$를 만족하는 unitary gate V에 대해서 다음과 같이 decomposition 할 수 있다.



$*$ Proof: 위와 같이 decomposition한 gate가 실제로 $C^2(U)$와 동일하게 동작하는지 확인해보자.
$\Rightarrow$

Controlled gate on multiple-qubit decomposition

(generalize) Control qubit이 n개인 unitary gate는 Toffoli gate ($C^2(X)$)를 이용하여 다음과 같이 구현한다. 구현을 위해서 $n-1$개의 ancilla qubit을 필요로한다.



Controlled gate on multiple-qubit decomposition

Complexity:
$C^n(U)$ gate를 구현하기 위해서는 다음과 같은 complexity를 가진다.

- $n-1$개의 ancilla qubit
- $2(n-1)$개의 Toffoli gate
  - $4(n-1)$개의 CNOT gate
  - $6(n-1)$개의 single unitary gate

$$O(n)$$

∗ Proof:$2(n-1)$개의 Toffoli gate, 그리고 $C(U)$ gate를 사용하여 decomposition한 회로가 왜 $C^n(U)$와 동일하게 동작하는지 분석해보자.
$\Rightarrow$

Summary

Summary

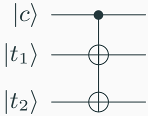
- Quantum circuit을 구성하는 다양한 gate들을 소개한다.
- Single qubit gate는 다음과 equivalent하다.
  - 두 가지 axis에 대한 rotation gates
  - single qubit gates와 Pauli-X gates
- Single qubit controlled gate = single qubit gates and CNOT gates
- Multiple-qubit controlled gate = *single qubit controlled gates* and CNOT gates
  → *single qubit gates and CNOT gates*

Some remarks

- control qubit이 $|0\rangle$일 때 동작하는 controlled gate의 구현은 다음과 같다.

$$XC(U)X = C'(U)$$

- (symbol) single-qubit gate가 여러개의 target qubit에 적용되는 경우:



Universial Quantum gate set: $\{$CNOT, single qubit gates$\}$

Decomposition from n-qubit unitary gate to two-level unitary gates

Theorem 3

Unitary operator U which acts on a d-dimensional Hilbert space ($d = 2^n$) may be decomposed into a product of two-level unitary matrices;

Two-level unitary:

- d차원 Hilbert space의 벡터에 대해서 2개의 벡터요소에만 작용
- $d \times d$ matrix에서 대부분은 identity matrix이고 자신이 작용하는 state에 대응되는 부분에만 항등행렬이 아닌 2×2 행렬이 위치한다.

$$\begin{pmatrix} u_{11} & u_{12} & 0 \\ u_{22} & u_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} u_{11} & 0 & u_{12} \\ 0 & 1 & 0 \\ u_{21} & 0 & u_{22} \end{pmatrix}$$

$*$ Proof: from 3×3 example, $(d = 3)$ 3×3 unitary U에 대하여, 다음을 만족하는 two-level matrices가 존재함을 보이자.

$$U_3 U_2 U_1 U = I \qquad \Leftrightarrow \qquad U_1^\dagger U_2^\dagger U_3^\dagger$$

where

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

Decomposition from n-qubit unitary gate to two-level unitary gates

* <u>Proof</u>: (contd.)
  - b의 값에 따라서 다음과 같이 U_1를 가정하자.

$$U_1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} (b=0), \qquad U_1 \equiv \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix} (b \neq 0)$$

  - 이렇게 가정한 U_1를 U에 곱하면, $b=0$이 된다.

$$U_1 U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}$$

  - c'의 값에 따라서 다음과 같이 U_2를 가정하자.

$$U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} (c'=0), \quad U_2 \equiv \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix} (c' \neq 0)$$

Decomposition from n-qubit unitary gate to two-level unitary gates

* Proof: (contd.)
  - 이렇게 가정한 U_2를 U_1U에 곱하면, $c' = 0$이 되고, $a' = 1$이 된다. 이때, unitary matrix의 조건에 의해서 첫번째 row vector의 norm이 반드시 1이 되어야하므로 $d'' = 0, g'' = 0$이어야한다. [*]

$$U_2U_1U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

  - 마지막으로 $U_3 = (U_2U_1U)^\dagger$로 가정하자.그럼 자명하게 다음을 만족하므로, 3×3 unitary matrix를 3개의 two-level matrix의 multiplication으로 decomposition 할 수 있다.

$$U_3U_2U_1U = (U_2U_1U)^\dagger(U_2U_1U) = I$$

  - (generalize) $d \times d$ matrix에 대해서도 $u_{11} = 1$이고 나머지 행과 열은 0인 행렬을 two-level matrix들을 곱하여; $U_1U_2 \cdots U_{d-1}U$ 얻을 수 있다. 그러고 나서, 나머지 $d-1 \times d-1$ 부분 행렬이 2×2 부분 행렬이 될 때까지 이 절차를 반복하면, 임의의 $d \times d$ 유니타리 행렬을 다음과 같이 표현할 수 있다.□

$$U = V_1 \cdots V_k, \qquad k \leq (d-1) + (d-2) + \cdots + 1 = \frac{d(d-1)}{2}$$

Two-level unitary gate is controlled-U gate

- 2-level unitary matrix는 n system 전체에 작용하는 gate이지만 특정 벡터요소에만 작용하며, 이는 특정 basis state에 대해서만 작용한다고 생각할 수 있다.
- 예를 들어, 다음과 같은 2-level unitary matrix는 $|10\rangle, |11\rangle$ basis state에만 비자명하게 작용한다. $|c\rangle = |1\rangle$일 때 동작하는 controlled-U gate로 생각할 수 있다.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix} = u_{00} |10\rangle \langle 10| + u_{01} |10\rangle \langle 11| + u_{10} |11\rangle \langle 10| + u_{11} |11\rangle \langle 11| + I_{\perp}$$

- 그러나 문제점은 다음과 같은 two-level unitary matrix도 존재한다는 것이다.

$$\begin{pmatrix} u_{00} & 0 & 0 & u_{01} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ u_{10} & 0 & 0 & u_{11} \end{pmatrix} = u_{00} |00\rangle \langle 00| + u_{01} |00\rangle \langle 11| + u_{10} |11\rangle \langle 00| + u_{11} |11\rangle \langle 11| + I_{\perp}$$

- Two-level unitary matrix가 작용하는 basis가 1bit의 값이 다르다면, 그 1bit를 target qubit으로 생각해서 controlled-U gate로 표현할 수 있다.
- 그러나, 1bit이상이 달라지게 되면 더이상 controlled-U gate로 생각할 수 없다.

Decomposition from n-qubit controlled-U gate to $\{$CNOT gates, single-qubit$\}$ $\Rightarrow$ Single qubit and CNOT gates are universal!

Idea

Basis $|s\rangle, |t\rangle, D_H(s,t) > 1$에 대한 작용을 basis $D_H(g_i, g_j) = 1$에 대한 작용들의 연속으로 생각하는 것이다.

$$|s\rangle = |g_1\rangle \to |g_2\rangle \to |g_3\rangle \cdots \to |g_{m-1}\rangle, \ D_H(|g_{m-1}\rangle, |t\rangle) = 1$$

예를 들어, $|s\rangle = |101001\rangle$이고 $|t\rangle = |110011\rangle$이면 다음과 같은 변환을 수행할 수 있다.

$$\begin{aligned} s &= \quad 101001 \\ g_2 &= \quad 101011 \\ g_3 &= \quad 100011 \\ t &= \quad 110011 \end{aligned}$$

Theorem 4

n-qubit controlled-U gate can be decomposed into a single qubit gate and CNOT gates;

Decomposition from n-qubit controlled-U gate to {CNOT gates, single-qubit}
⇒ Single qubit and CNOT gates are universal!

$*$ Proof:

- $|s\rangle = |g_1\rangle, |t\rangle = |g_m\rangle$에 대해서 작용하는 two-level unitary matrix는 다음과 같다.

$$U = u_{00} |g_1\rangle \langle g_1| + u_{01} |g_1\rangle \langle g_m| + u_{10} |g_m\rangle \langle g_1| + u_{11} |g_m\rangle \langle g_m| + \sum_{s' \neq g_1, g_m} |s'\rangle \langle s'|$$

- $|g_1\rangle$을 $|g_2\rangle$로 변환하는 operator는 다음과 같다. (특정 qubit의 값을 반전)

$$V_{12} = |g_2\rangle \langle g_1| + |g_1\rangle \langle g_2| + \sum_{s' \neq g_1, g_2} |s'\rangle \langle s'|$$

- 따라서 변환하면 다음과 같이 $|g_2\rangle, |g_m\rangle$에 대해서 작용하는 operator가 된다.

$$V_{12}^\dagger U V_{12} = u_{00} |g_2\rangle \langle g_2| + u_{01} |g_2\rangle \langle g_m| + u_{10} |g_m\rangle \langle g_2| + u_{11} |g_m\rangle \langle g_m| + I_\perp$$

- 이를 반복하면, $|g_{m-1}\rangle, |g_m\rangle$에 대한 변환을 수행하는 controlled-U gate가 된다.

$$C^{n-1}(U) \triangleq V_{m-2,m-1} \cdots V_{2,3} V_{1,2} U V_{1,2}^\dagger V_{2,3}^\dagger \cdots V_{m-2,m-1}^\dagger$$

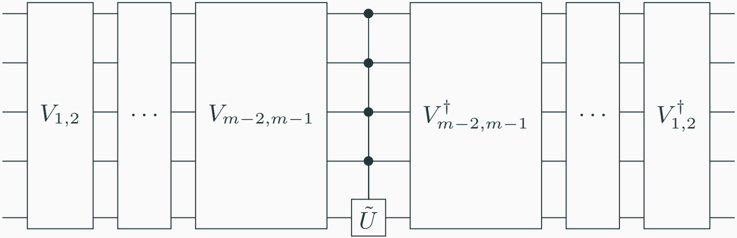
Decomposition from n-qubit controlled-U gate to $\{$CNOT gates, single-qubit$\}$
$\Rightarrow$ Single qubit and CNOT gates are universal!

∗ Proof: (contd.)

- $C^{n-1}(U)$ gate에 다시 basis를 변환하는 operator를 가하면, 원래의 matrix와 동등하다는 것을 알 수 있다.

  $$(V_{m-2,m-1} \cdots V_{2,3} V_{1,2})^\dagger C^{n-1}(U) (V_{1,2}^\dagger V_{2,3}^\dagger \cdots V_{m-2,m-1}^\dagger)^\dagger$$
  $$= (V_{m-2,m-1} \cdots V_{1,2})^\dagger (V_{m-2,m-1} \cdots V_{1,2}) U (V_{1,2}^\dagger \cdots V_{m-2,m-1}^\dagger)^\dagger (V_{1,2}^\dagger \cdots V_{m-2,m-1}^\dagger$$

- 따라서, 다음의 과정을 거쳐서 two-level matrix를 구현할 수 있다.
  1. basis 변환: $|s\rangle \rightarrow |g_{m-1}\rangle$
  2. Controlled-U gate: $C^{n-1}(U)$
  3. 원본 basis로 다시 변환: $|g_{m-1}\rangle \rightarrow |s\rangle$



Decomposition from n-qubit controlled-U gate to {CNOT gates, single-qubit}
$\Rightarrow$ Single qubit and CNOT gates are universal!

Example 다음의 8×8 two-level unitary operator를 구현하는 회로를 설계하라.

$$U = \begin{bmatrix} a & 0^{\otimes 6} & c \\ 0^{\otimes 6} & I^{6\times 6} & 0^{\otimes 6} \\ b & 0^{\otimes 6} & d \end{bmatrix}, \quad \tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

$\Rightarrow$

Corollary 5

single qubit and CNOT gates together can be used to implement an arbitrary n-qubit unitary operation.

$*$ Proof: Combine theorem 3 and 4, we can easily proof this corollary.□

Circuit complexity

그렇다면, n-qubit arbitrary unitary operator를 구현하기 위해서 필요한 총 gate의 개수는 몇 개일까?

- $d \times d$ gate $\equiv$ 최대 $d(d-2)/2$개의 two-level gate

$$O(d^2) = O(4^n)$$

- (each) two-level gate $\equiv$ 최대 $2(n-1)+1$개의 controlled gate (*basis change*)

$$O(n)$$

- (each) controlled gate $\equiv$ 최대 $2(n-1)$개의 Toffoli gate

$$O(n)$$

$\Rightarrow$ 따라서 다음과 같은 circuit complexity를 가지고 CNOT gates, single-qubit gates를 이용하여 어떤 unitary gate도 구현할 수 있다!

$$O(4^n) \times O(n) \times O(n) = O(n^2 4^n)$$

Summary

Summary

- n-qubit unitary $= O(4^n)$개의 two-level unitary gates.
- n-qubit two-level unitary gate $= O(n)$개의 controlled gates.
(basis를 변환한 뒤, controlled-U gate를 취하고 다시 원래 basis로 변환한다.)
- n-qubit controlled gate $= O(n)$개의 CNOT / single-qubit gates.
- 따라서 총 $O(n^2 4^n)$의 복잡도로 universal gate set $\{CNOT,$ single-qubit gate$\}$를 이용하여 어떤 quantum gate이든지 구현할 수 있다.

Universial Quantum Discrete gate set: $\{$CNOT, H, S, T$\}$

Approximating quantum circuits via discrete gate set

Problem: Universal gate set $\{CNOT, \text{single-qubit gate}\}$을 사용하면 어떠한 quantum gate이든지 오류없이 구현할 수 있다. 하지만, single-qubit gates는 θ에 따라서 continuos 한 gate이기 때문에 이로인하여 noise에 큰 영향을 받게된다.

⇒ **Idea**: Discrete gate set $\{CNOT, H, S, T\}$을 사용하여 gate를 approximation하여 구현하고자 한다.

Definition 6 (approximation error)

We define the **error** when V is implemented instead of U by

$$E(U, V) \triangleq \max_{|\psi\rangle} \| (U - V) |\psi\rangle \|$$

where the maximum is over all normalized quantum states $|\psi\rangle$ in the state space.

✓meaning: U를 V로 근사했을 때 발생하는 error중에서 가장 큰 값으로 정의한다.

Approximating quantum circuits via discrete gate set

Definition 7 (variational distance)

We detine the **variational distance** as

$$VD(P_U(m), P_V(m)) = \frac{1}{2}|P_U(m) - P_V(m)|,$$

and total variational distance

$$TVD(P_U, P_V) = \frac{1}{2}\sum_m |P_U(m) - P_V(m)|,$$

where

$$P_U(m) = \mathrm{tr}[E_m U |\psi\rangle\langle\psi| U^\dagger], \quad P_V(m) = \mathrm{tr}[E_m V |\psi\rangle\langle\psi| V^\dagger].$$

✓meaning: 각 gate U, V를 $|\psi\rangle$에 가한 뒤 관측했을 때, 그 outcome이 m일 확률이 $P_U(m), P_V(m)$이다. 두 probability distribution의 차이로 variational distance를 정의한다. 만약 두 분포가 거의 유사하다면, 두 unitary U, V를 구분하기 어려울 것이다.

Corollary 8

If $E(U, V) < \epsilon$ *then,* $TVD(P_U, P_V) < \epsilon$

Theorem 9 (quantum gate error bound)

$$|P_U(m) - P_V(m)| \leq 2E(U,V)$$

✓ meaning: If $E(U,V)$ is small, then measurement outcomes occur with similar probabilities.

$*$ Proof: (hint. 코시-슈바르츠 부등식)
$\Rightarrow$

$$\begin{aligned} |P_U(m) - P_V(m)| &= |\mathrm{tr}[MU|\psi\rangle\langle\psi|U^\dagger] - \mathrm{tr}[MV|\psi\rangle\langle\psi|V^\dagger]| \\ &= \\ &\leq \\ &\leq 2E(U,V) \end{aligned}$$

Approximating quantum circuits via discrete gate set

Theorem 10 (quantum circuit error bound)

$$E\left(U_m U_{m-1} \ldots U_1, V_m V_{m-1} \ldots V_1\right) \leq \sum_{j=1}^{m} E\left(U_j, V_j\right)$$

∗ <u>Proof</u>: (hint. triangle inequality) $m = 2$일 때,
$\Rightarrow$

$$\begin{aligned} E\left(U_2 U_1, V_2 V_1\right) &= \left\| \left(U_2 U_1 - V_2 V_1\right) |\psi\rangle \right\| \\ &= \\ &\leq \\ &\leq E(U_2, V_2) + E(U_1, V_1) \end{aligned}$$

Generate two type of rotational gate $R_{\hat{n}}(\hat{\theta}), R_{\hat{m}}(\hat{\theta})$

- Discrete gate set $\{H, S, T, CNOT\}$에 대하여, 다음의 연산을 생각해보자. 즉, H gate를 양옆에 가하면 rotation 축을 변경시킬 수 있다.

$$HTH = e^{-i\frac{\pi}{8}X}$$

- 그럼 다음 연산을 생각해보자.

$$\begin{aligned} THTH &= \exp\left(-i\frac{\pi}{8}Z\right)\exp\left(-i\frac{\pi}{8}X\right) = \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right] \\ &= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8} \end{aligned}$$

- 위 연산은 다음과 같은 형태의 rotation gate $R_{\hat{n}}(\theta)$로 생각해볼 수 있다.

$$R_{\hat{n}}(\theta) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z)$$

where $\hat{n} = (\cos(\pi/8), \sin(\pi/8), \cos(\pi/8)),\ \cos(\theta/2) = \cos^2(\pi/8)$

- 또한, H gate를 사용하여 또다른 임의의 축 $\hat{m}$에 대한 rotation gate를 만들 수 있다.

$$H(R_{\hat{n}}(\theta))H = R_{\hat{m}}(\theta)$$

where $\hat{m} = (\cos(\pi/8), -\sin(\pi/8), \cos(\pi/8)),\ \cos(\theta/2)$

우리가 만든 2개의 rotation gate $R_{\hat{n}}(\theta) \triangleq THTH$, $R_{\hat{m}}(\theta) \triangleq HTHTHH$를 이용하면, 어떤 unitary gate도 특정 error rate이하로 근사할 수 있다!

Theorem 11

We can implement arbitrary single-qubit gate V via $\{H, T, S\}$ that satisfy following bound

$$E(U, V) \leq \epsilon,$$

where ϵ is target error rate.

$*$ Proof: (hint) using kronecker theorem

$\Rightarrow$

$$\begin{aligned}
|U - V| &= |R_{\hat{n}}(\alpha)R_{\hat{m}}(\beta)R_{\hat{n}}(\gamma) - (R_{\hat{n}}(\theta))^{n_1}(R_{\hat{m}}(\theta))^{n_2}(R_{\hat{n}}(\theta))^{n_3}| \\
&\leq |R_{\hat{n}}(\alpha) - (R_{\hat{n}}(\theta))^{n_1}| + |R_{\hat{m}}(\beta) - (R_{\hat{m}}(\beta))^{n_2}| + |R_{\hat{n}}(\gamma) - (R_{\hat{n}}(\gamma))^{n_3}| \\
&\leq \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon
\end{aligned}$$

Circuit complexity: for # of single qubit gates

그렇다면, n-qubit gate를 discrete gate set만을 사용하여 구현할 때, single qubit gate의 개수에 대한 circuit complexity는 무엇일까? $(\max(n_1, n_2, n_3) = ?)$

- (아이디어) $\theta_{i-j} < \epsilon_1$에 대하여, $k\theta i - j, \forall k$는 $[0, 2\pi)$범위를 uniform하게 채우기 때문에, 최악의 경우라 하더라도 $n_1 \approx 2\pi/\epsilon_1$일 것이다.
- 따라서 각 gate에 대한 error가 ϵ_1일 때, n-qubit gate를 근사하기 위해 필요한 single-qubit gate가 m개라면, error rate는 $\epsilon = \epsilon_1/m$으로 표현할 수 있다.

$$\Omega\left(m\frac{2\pi}{\epsilon_1}\right) = \Omega\left(m\frac{2\pi m}{\epsilon}\right) = \Omega(m^2)$$

- 그러나 다음 정리를 이용하면, 이보다 훨씬 적은 gate만을 사용하여 구현할 수 있다.

Theorem 12 (Solovay Kitaev theorem)

$$m \times O\left(\log^c\left(\frac{m}{\epsilon}\right)\right) = O(m \log^c m)$$

where

$$n_1 = O\left(\log^c\left(\frac{1}{\epsilon_1}\right)\right) = O\left(\log^c\left(\frac{m}{\epsilon}\right)\right)$$

그렇다면, n-qubit gate를 discrete gate set만을 사용하여 구현할 때, qubit 개수에 대한 circuit complexity는 무엇일까?

Theorem 13

For implement arbitrary n-qubit unitary gate U needs $\Omega(2^n)$ number of gates.

* Proof: U가 만들어낼 수 있는 $|\psi\rangle$의 경우의 수를 이용한다.

method 1 initial state $|0\rangle^{\otimes n}$에 대하여,
g개의 서로다른 유형의 gate가 있고 각 gate들은 최대 f개의 qubit에 적용되는 discrete set을 가정하자. n-qubit gate를 표현하기 위해 필요한 gate가 m개일 때,
$\Rightarrow$

$$O(n^{mfg})$$

method 2

- 반면, quantum state를 2^n개의 coefficient로 생각하면, n qubit system의 state space를 $2^{n+1}-1$차원에서 unit sphere의 surface로 생각해볼 수 있다. [*]
- 마찬가지로 quantum state에 대해 error bound ϵ 내부에 있는 state들은$2^{n+1}-2$ 차원에서 반지름이 ϵ인 sphere들의 volume와 유사하다.
- 따라서 quantum state space를 epsilon ball로 덮기위해 필요한 ball의 개수는 다음과 같다.

$$\frac{S_{2^{n+1}-1}(1)}{V_{2^{n+1}-2}(\epsilon)} = \Omega\left(\frac{1}{\epsilon^{2^{n+1}}-1}\right)$$

$\Rightarrow$

$$\boxed{m \geq \Omega\left(\frac{2^n \log\left(\frac{1}{\epsilon}\right)}{\log n}\right)}$$

Summary

Summary

- If arbitrary n-qubit needs m number of single qubit gates, then needs $\Omega(m \log^c m)$ number of gates which in discrete gate set.
- Arbitrary n-qubit needs $\Omega(2^n)$ number of gates.

Some remarks

- 실제 HW에서는 멀리 떨어진 qubit간 연산을 위해 추가적인 SWAP gate가 필요하다. 따라서 이론보다 더 많은 gate가 필요할 수 있다.
- 우리가 사용한 discrete set은 universal이지만, unique하지는 않다.

Measurement

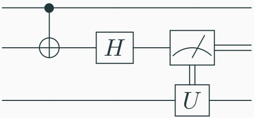
Principle of deferred measurement

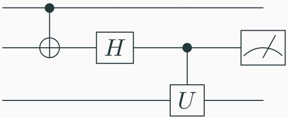
Computational basis: $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

Principle of deferred measurement

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

✓meaning: 회로 중간에 intermediate measurement를 수행하고 그 결과로부터 다른 gate를 control하는 회로는, measurement를 가장 마지막에 수행하도록 한 circuit과 equivalent하다.



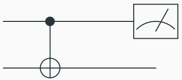


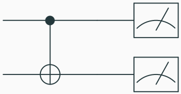
Principle of implicit measurement

Principle of implicit measurement

Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

✓meaning: 특정 qubit만 관측하는 partial measurement 회로는, 모든 qubit을 measurement하는 circuit과 equivalent하다.





References

- M. A. Nielson and I. L. Chuang, Quantum Computation and Quantum Information
- Lecture notes for QU511: Quantum Computing (Fall 2024)