Sec 4.10~12 Perfectly universal sets of quantum gates

	Classical	Quantum
state	$\{0,1\}^n$	$\mathbb{H}_n$, $\mathbb{C}^{2^n}$.
Need to implement	Boolean ft.	Unitary matrix
Universal set	{AND, OR, NOT}	?
	{NAND}	
	{NOR}	
		{H, T, CNOT}
		{all rotation, CNOT}

"primitive set"

Review

One qubit unitary operator $U \in \mathbb{H}_1$

$$U = e^{i\delta} A X B X C, \quad ABC = \mathbb{1}$$

(Thm 4.3.33)

Def 4.8.4.

(1) S: universal for a set T of unitary operator

if $\forall \varepsilon \in \mathbb{R}_+$, $\forall U \in T$, $\exists$ unitary operator V.

$E(U,V) < \varepsilon$.

$$E(U,V) = \sup_{\substack{|\varphi\rangle \in \mathbb{H}_n \\ \langle\varphi|\varphi\rangle = 1}} \| U|\varphi\rangle - V|\varphi\rangle \|$$

(2) S: Universal for quantum computation

if S: universal for all unitary operators.

(3) Perfectly universal for quantum computation

if all unitary operators $U \in \mathbb{H}_n$ can be

implemented by the gates in S, ancilary, erasure.

§ 4.10 Perfectly universal sets of quantum gates

Def 4.10.1. $A \in \mathbb{C}^{k \times k}$: two level gate.

if there are $i, j \in \mathbb{Z}_k$. s.t for $\forall \hat{v} \in \mathbb{C}^k$,

$$\hat{v}_k = A\hat{v}_k \quad \text{for } k \neq i, \; k \neq j$$

(2개 외하고는 다 같은걸)

Ex ;

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{bmatrix} \; ; \text{ two - level gate}$$

$U \in \mathbb{C}^{1 \times 1}$

$U \in \mathbb{C}^{2 \times 2}$; two - level gate.

Thm 4.10.4. Let $U \in \mathbb{C}^{k\times k}$ unitary.

Then U can be written as a product of $\frac{k(k-1)}{2}$

unitary two-level gates, for $k \geq 2$.

proof),

Induction

$n=2$ $U \in \mathbb{C}^{2\times 2}$: two-level gate.

Assume. $n=k$ hold. : For $U \in \mathbb{C}^{k\times k}$

$$U_k = \underbrace{V_{\frac{k(k-1)}{2}} \cdots V_1}_{\frac{k(k-1)}{2} \text{ product.}}$$ where V_j : two level gate

For $n=k+1$ consider $U_{k+1} \in \mathbb{C}^{(k+1)\times k+1}$.

sketchy, (we want to find $\frac{(k+1)k}{2}$ two level gate)

$$U_{k+1} = A_k \cdots A_1 \begin{pmatrix} 1 & 0 \\ 0 & U_k \end{pmatrix} = A_k \cdots A_1 \, \overline{V}_{\frac{k(k-1)}{2}} \cdots \overline{V}_1$$

where $\bar{V}_k := \begin{pmatrix} 1 & 0 \\ 0 & V_k \end{pmatrix} \in \mathbb{C}^{(k+1)\times(k+1)}$

Claim (two-level gate k개를 ~~곱하면~~ $\begin{pmatrix} 1 & 0 \\ 0 & \end{pmatrix}$ 된다.),

$$U_{k+1} = \underbrace{A_k \cdots A_1}_{\text{two level gate in } \mathbb{C}^{(k+1)\times(k+1)}} \begin{pmatrix} 1 & 0 \\ 0 & U_k \end{pmatrix}.$$

Construction of A_k.

$$U_{k+1} = (a_{ij})_{(k+1)\times k+1}$$

$$c = \frac{1}{\sqrt{|a_{11}|^2 + |a_{k1}|^2}}$$

$$\begin{array}{r l} & A_k = \begin{bmatrix} c\,\overline{a_{11}} & 0 \cdots 0 & c\,\overline{a_{k,1}} & 0 \cdots 0 \\ 0 & & 0 & \\ \vdots & I & \vdots & \\ 0 & & 0 & \\ c\,a_{k,1} & 0 \cdots 0 & -c\,a_{1,1} & \\ 0 & & & \\ \vdots & & & I \\ 0 & & & \end{bmatrix} \\ \text{k th row} & \end{array}$$

: Unitary two column gates.

$$(A_k U_{k+1})_{(1,1)} = c(a_{11})^2 + c(a_{k,1})^2 = \frac{1}{c}$$

$$(A_k U_{k+1})_{(1,k)} = c\,a_{k1}\,a_{11} - c\,a_{11}\,a_{k1} = 0.$$

$$\underline{A_1 \cdots A_k U_{k+1}} = \begin{bmatrix} x & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{bmatrix}.$$

Product of unitary

$\Rightarrow$ unitary,

column : orthonormal

basis $x=1$

$$= \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{bmatrix},$$

We proved

$$U_{k+1} = A_k^{-1} \cdots A_1^{-1} \begin{bmatrix} 1 & 0 \\ 0 & U_k \end{bmatrix}.$$

Cor : Set of all two level gates is perfectly universal for quantum computation

Thm 4.10.6. $S := \{$ all rotation gates, standard CNOT gate $\}$

Perfectly universal for quantum computing

Def 4.10.7. Let $\vec{s}, \vec{t} \in \{0,1\}^n$.

A Gray code connecting $\vec{s}$ and $\vec{t}$ is a sequence.

$$G = (\underset{\vec{s}}{\underset{\parallel}{\vec{g}_0}}, \cdots, \underset{\vec{t}}{\underset{\parallel}{\vec{g}_m}})$$ Pairwise distinct vectors in $\{0,1\}^n$.

and successive element G differ by exactly one bit.

Example. Gray code $\vec{s} = (0,0,0)$ $\vec{t} = (1,1,1)$

$$G = ((0,0,0), (1,0,0), (1,1,0), (1,1,1))$$

Prop. 4.10.10. Let $\vec{s}, \vec{t} \in \{0,1\}^n$, then there is a Gray code of length $\leq n+1$ that connect $\vec{s}$ and $\vec{t}$.

Thm 4.10.12.

For every two-level unitary gate U on $\mathbb{H}_n$,

$\exists$ unitary single qubit operator V.

s.t U can be implemented by quantum circuits

that uses V, $O(n^2)$ Pauli X, Hadamard, $\pi/8$,

standard CNOT, ancillary, erasure gates.

and four other single qubit gates.

Proof)

U: two level gate. on $\mathbb{H}_n$,

For $\vec{s}, \vec{t} \in \{0,1\}^n$, $\alpha, \beta, \gamma, \delta \in \mathbb{C}$

$$U|\vec{s}\rangle = \alpha|\vec{s}\rangle + \beta|\vec{t}\rangle, \quad U|\vec{t}\rangle = \gamma|\vec{s}\rangle + \delta|\vec{t}\rangle$$

U leaves all other computational basis. Ex $\begin{bmatrix} 1 & & & \\ & \alpha & & \beta \\ & & 1 & \\ & \gamma & & \delta \end{bmatrix}$

define $V \in \mathbb{H}_1$.

$$V|0\rangle = \alpha|0\rangle + \beta|1\rangle. \quad V|1\rangle = \gamma|0\rangle + \delta|1\rangle$$

Claim $\exists P$: unitary s.t

$$P|\vec{s}\rangle = |t_0 \cdots t_{i-1}\rangle|0\rangle|t_{i+1} \cdots t_{n-1}\rangle$$

$$P|\vec{t}\rangle = |t_0 \cdots t_{i-1}\rangle|1\rangle|t_{i+1} \cdots t_{n-1}\rangle$$

If the claim hold.

$$U = P^* C^{c_0, c_1, i}(V) P.$$

U is implemented by P^*, $C^{c_0, c_1, i}(V)$

Proof of the claim

Let G : gray code. $G = (\vec{q}_0, \dots, \vec{q}_m)$, $\vec{q}_0 = \vec{s}$, $\vec{q}_m = \vec{t}$.

Let T_j : transposition operator

$\vec{q}_{j-1} \overset{T_j}{\longleftrightarrow} \vec{q}_j$

s.t. $|\vec{q}_j\rangle = T_j|\vec{q}_{j-1}\rangle$, $|\vec{q}_{j-1}\rangle = T_j|\vec{q}_j\rangle$

Let $P := T_{m-1} \cdots T_1$

$\Rightarrow$ $P|\vec{s}\rangle = |\vec{q}_{m-1}\rangle$, $T_m|q_{m-1}\rangle = |\vec{q}_m\rangle = |\vec{t}\rangle$.

$P|\vec{s}\rangle$ and $|\vec{t}\rangle$ differ in exactly one qubit

If $t_i = 1$, claim is prove.

If $t_i = 0$ replace P by $\text{Trans}_{\vec{c}}\, P$, ($\vec{c} = (t_0 \cdots t_{i-1} * t_{i+1} \cdots t_{n-1})$).

P : $O(n)$ transposition : X, H, T, CNOT, ancila, erasure.
(Thm 4.9.15)

$C^{c_0, c_1, i}(V)$: X, H, T, CNOT, ancila, erasure
(Thm 4.9.14)

Goal : Finding universal set

for the quantum computing

$\{ U \in \mathbb{H}_n \}$: universal

$\Big\updownarrow$ Thm 4.10.4.

$\{ U \in H_n$: two-level gate $\}$: universal.

$\Big\updownarrow$ Thm 4.10.6

$\left\{ \begin{array}{l} U \in \mathbb{H}_1 : \text{unitary single qubit operator} \\ \underbrace{X,\ T,\ H}_{\text{rotation}},\ \text{CNOT}. \end{array} \right\}$: universal

unitary single qubit

$\{ U \in \mathbb{H}_1,\ \text{CNOT} \}$: universal

$\{ H,\ T,\ \text{CNOT} \}$: universal,

$\quad \| \quad\quad \|$ ($\pi/8$ gate)

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}.$

$\left(\{ H, T \} \text{ : universal for } U \in \mathbb{H}_1 \right)$ Thm 4.11.2.

Sketch of the proof of Thm 4.11.2

$\{H, T\}$: universal for $U \in \mathbb{H}_1$

Let $$\hat{n} = \frac{1}{\sqrt{\cos^2 \frac{\pi}{8} + 1}} \left(\cos \frac{\pi}{8}, \sin \frac{\pi}{8}, \cos \frac{\pi}{8} \right)$$

$$\hat{m} = \frac{1}{\sqrt{\cos^2 \frac{\pi}{8} + 1}} \left(\cos \frac{\pi}{8}, -\sin \frac{\pi}{8}, \cos \frac{\pi}{8} \right)$$

$\hat{n}, \hat{m}$: non parallel unit vector

By Thm 4.3.35. $\exists\ \delta, \alpha_i, \beta_i$ for $0 \le i \le k-1$ s.t.

$$U = e^{i\delta} \prod_{i=0}^{k-1} R_{\hat{n}}(\alpha_i) R_{\hat{m}}(\beta_i)$$

by $\boxed{\text{Lem 4.11.6}}$

$$= e^{i\delta} \prod_{i=0}^{k-1} \underbrace{R_{\hat{n}}(\alpha_i)}_{\text{For each rotation}} H R_{\hat{n}}(\beta_i) H. \quad ①$$

Proposition 4.11.10. ②

For all $\varepsilon > 0$. $\exists\ a_i, b_i \in \mathbb{N}$ s.t.

$$E(R_{\hat{n}}(\alpha_i), R_{\hat{n}}^{a_i}(\theta)) < \frac{\varepsilon}{2k}.$$

$$E(R_{\hat{n}}(\beta_i), R_{\hat{n}}^{b_i}(\theta)) < \frac{\varepsilon}{2k}.$$

Let $V = \prod_{i=0}^{k-1} R_{\hat{n}}^{a_i}(\theta)\, H\, R_{\hat{n}}^{b_i}(\theta)\, H.$

$$\boxed{\begin{array}{c} \text{Prop } 4.11.3 \quad 3 \\ E\left(\prod U_k, \prod V_k\right) \leq \sum E(U_k, V_k) \end{array}}$$

$$E(U,V) \leq \sum_{i=0}^{k-1} E\left(R_{\hat{n}}(\alpha_i), R_{\hat{n}}^{a_i}(\theta)\right) + \sum_{i=0}^{k-1} E\left(R_{\hat{n}}(\beta_i), R_{\hat{n}}^{b_i}(\theta)\right)$$

$$\leq k \frac{\varepsilon}{2k} + k \cdot \frac{\varepsilon}{2k} \leq \varepsilon.$$

$\Rightarrow$ we found approximation V.

Lem 4.11.5 $\quad R_{\hat{n}}(\theta) = e^{-i\frac{\pi}{4}} THTH.$ $\quad$ 4.

$$V = e^{-i\frac{\pi}{4}\left(\sum (a_i + b_i)\right)} \prod_{i=0}^{k-1} (THTH)^{a_i} H (THTH)^{b_i} H.$$

Using $\{T, H\}$ we constructed V. s.t $E(U,V) < \varepsilon$

Proof of Prop (4.11.3). $E\left(\prod_{i=1}^{k} U_k, \prod_{i=1}^{k} V_k\right) \leq \sum_{i=1}^{k} E(U_k, V_k)$

Induction

$k = 1$ Trivial

Let $k-1$ step hold.

i.e. $U = \prod_{i=1}^{k-1} U_i \qquad V = \prod_{i=1}^{k-1} V_i$. $(k-1)$ product.

$$E(U, V) \leq \sum_{i=1}^{k-1} E(U_i, V_i)$$

For k-step, $U_k U$, $V_k V$: k Product

$$E(U_k U, V_k V) = \sup_{\substack{\varphi \in \mathbb{H}_n \\ \|\varphi\|_{L^2} = 1}} \|(U_k U - V_k V)|\varphi\rangle\|_{L^2}.$$

$$\leq \sup \|U_k (U - V)|\varphi\rangle\|_{L^2} + \sup \|(U_k - V_k) V|\varphi\rangle\|_{L^2}.$$

$$\leq \sup \|(U - V)|\varphi\rangle\|_{L^2} + \sup \|(U_k - V_k) V|\varphi\rangle\|_{L^2}.$$

$\because U_k$: unitary

$$\leq E(U, V) + E(U_k, V_k) \leq \sum_{i=1}^{k} E(U_i, V_i)$$

Proof of Lem 4.11.4.) $R_{\hat{m}}(r) = H R_{\hat{n}}(r) H$

Def 4.3.4

$$R_{\hat{n}}(r) = e^{-ir\hat{n}\cdot\sigma/2} \qquad (\sigma = (X, Y, Z))$$

$$= \cos\frac{r}{2} I - i\sin\frac{r}{2}\,\hat{n}\cdot\sigma$$

$$= \cos\frac{r}{2} I - i\sin\frac{r}{2}\left(n_x X + n_y Y + n_z Z\right).$$

Note. $HH = I$, $HXH = Z$, $HYH = -Y$, $HZH = X$.

$$H R_{\hat{n}}(r) H = \cos\frac{r}{2} I - i\sin\frac{r}{2}\left(\underbrace{n_x}_{= m_z} Z \underbrace{- n_y}_{= m_y} Y + \underbrace{n_z}_{= m_x} X\right),$$

$$= R_{\hat{m}}(r)$$

$$\left(\because \begin{array}{l} n_x = n_z = m_x = m_z = \cos\frac{\pi}{8}, \\ n_y = \sin\frac{\pi}{8} = -m_y \end{array} \right)$$

Proof of Lem 4.11.5.

statement

$$\left(R_{\hat{n}}(\theta) = e^{-i\frac{\pi}{4}} THTH. \quad \underbrace{\theta = 2\arccos\left(\cos^2\frac{\pi}{8}\right)}_{\Downarrow \; \cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}} \right).$$

Recall Def 4.3.4

$$\boxed{R_{\hat{n}}(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}\,\hat{n}\cdot\sigma}$$

$$\sin^2\frac{\theta}{2} = 1 - \cos^4\frac{\pi}{8} = \frac{1-\cos^4\frac{\pi}{8}}{1+\cos^2\frac{\pi}{8}} = \frac{1}{\|\vec{n}\|^2}\sin^2\frac{\theta}{2}.$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} = e^{\frac{i\pi}{8}} \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix}$$

$$e^{-i\frac{\pi}{8}} T = \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix} = \cos\frac{\pi}{8} I - i\sin\frac{\pi}{8} Z.$$

$$e^{-i\frac{\pi}{8}} HTH = e^{-i\frac{\pi}{8}} H|0\rangle\langle 0|H + e^{i\frac{\pi}{8}} H|1\rangle\langle 1|H$$

$$= \cos\frac{\pi}{8} I - i\sin\frac{\pi}{8} X.$$

$$e^{-i\frac{\pi}{4}} THTH = \underbrace{e^{-i\frac{\pi}{8}} T}_{Z\ 3\ \frac{\pi}{4}} \; \underbrace{e^{-i\frac{\pi}{8}} THT}_{X\ 3\ \frac{\pi}{4}}.$$

rotates

$$= \left(\cos\frac{\pi}{8} I - i\sin\frac{\pi}{8} Z\right)\left(\cos\frac{\pi}{8} I - i\sin\frac{\pi}{8} X\right)$$

$$= \cos^2\frac{\pi}{8} I - i\sin\frac{\pi}{8}\cos\frac{\pi}{8}(X+Z) - \sin^2\frac{\pi}{8} \underbrace{ZX}_{\overset{-iY}{\|}}$$

$$= \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} \underbrace{\boxed{\frac{1}{\|\vec{n}\|}\left(\cos\frac{\pi}{8} X + \sin\frac{\pi}{8} Y + \cos\frac{\pi}{8} Z\right)}}_{\hat{n}\cdot\sigma.}$$

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

Proof of Proposition 4.11.10.

$$\left(\text{For } \forall \varepsilon > 0,\ \forall r \in \mathbb{R}.\ \exists k \in \mathbb{N} \text{ s.t. } E\left(R_{\hat{n}}(r), R^k_{\hat{n}}(\theta)\right) < \varepsilon. \right)$$

Choose $r \in [0, 2\pi)$.

Note $\underbrace{\theta_k := k\theta}_{\text{countably many}}$ mod 2π. for $k \in \mathbb{N}$.

By Lem 4.11.9. $\exists k \in \mathbb{N}$ s.t. $|r - \theta_k| < \varepsilon$.

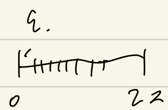
For $|\varphi\rangle \in \mathbb{H}$,

$$\left\| \left(R_{\hat{n}}(r) - R^k_{\hat{n}}(\theta)\right)|\varphi\rangle \right\|_{L^2}.$$

$$= \left\| \left(\cos\frac{r}{2} - \cos\frac{\theta_k}{2}\right) I|\varphi\rangle - i\left(\sin\frac{r}{2} - \sin\frac{\theta_k}{2}\right)\hat{n}\cdot\sigma|\varphi\rangle \right\|_{L^2}.$$

$$\left(\text{Def } R_{\hat{n}}(\theta) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}\,\hat{n}\cdot\sigma \right)$$

$$\leq 2\left|\frac{r}{2} - \frac{\theta_k}{2}\right| < \varepsilon.$$



Lem 4.11.9.

$\{k\theta \bmod 2\pi : k \in \mathbb{N}\}$ is dense in $[0, 2\pi)$

Let $I_k := [\varepsilon k, \varepsilon(k+1))$. $\displaystyle\bigcup_{k=0}^{\lfloor \frac{2\pi}{\varepsilon} \rfloor} I_k \supset [0, 2\pi)$

$\Rightarrow \exists\, k, l.$ s.t $0 < k\theta - l\theta < \varepsilon$ (pigeon hole principle)

$x \in [0, 2\pi) \Rightarrow \exists n.\ x = \varepsilon n + (x - \varepsilon n),\ (x - \varepsilon n) < \varepsilon.$

$\exists v \in \mathbb{N}.\ |v(k\theta - l\theta) - x| < \varepsilon.$