

Universality of single qubit gates & CNOT (Nielsen - Chuang § 4.5.2)

Suppose we have N qubits. state space $(\mathbb{C}^2)^{\otimes N} \simeq \mathbb{C}^d$
 $d = 2^N$

Last time: any unitary gate $U \in U(d)$ can be factorized as $U = V_0 \dots V_{k-1}$, V_i concentrated on two rows & columns.

Today's goal:

Thm U : unitary gate on $(\mathbb{C}^2)^{\otimes N}$ can be factorized as $U = \tilde{V}_0 \dots \tilde{V}_{k-1}$, $\tilde{V}_i$: either

1) single qubit gate $I_{2^a} \otimes W \otimes I_{2^{N-a-1}}$

$W \in U(2)$ acting on a -th qubit.

2) CNOT on two qubits.

It's enough to deal with the case when U is concentrated on two rows and columns.

i.e. only affects $|s_0 \dots s_{N-1}\rangle$ and $|t_0 \dots t_{N-1}\rangle$

among $\{|x_0 \dots x_{N-1}\rangle : x_i = 0, 1\}$

Machinery: Gray code

array of bits $g^0, \dots, g^m$ $g^i = g^i_0 \dots g^i_{N-1}$, $g^i_j \in \{0, 1\}$

- $g^0 = s$, $g^m = t$

- g^i and g^{i+1} differ at one position.

Prop 1 factorization of U in terms of

a) controlled- W gate for some $W \in U(2)$

($W \leftrightarrow U$ up to $|0\rangle \leftrightarrow |s\rangle$, $|1\rangle \leftrightarrow |t\rangle$).

b) controlled flip of bits.

Algorithm: given input $|\psi\rangle \in (\mathbb{C}^2)^{\otimes N}$.

Step 1 i : the position where g^0 and g^1 differ.

Consider $S_1: |x\rangle \mapsto |x'\rangle$ $x \in \{0, 1\}^N$

cont. if $x_j = g^0_j$ for $j \neq i$ then
 $x'_j = x_j$ ($j \neq i$), $x'_i = \text{NOT}(x_i)$
 otherwise $x' = x$, $|\psi^1\rangle = S_1 |\psi\rangle$

Step 2: do the same with $|g^1\rangle$ and $|g^2\rangle$
 $|\psi^2\rangle = S_2 |\psi^1\rangle$

Step $m-1$: $|\psi^{m-1}\rangle = S_{m-1} |\psi^{m-2}\rangle$

Step m : i : index where $t = g^m$ and S_{m-1} differ.

consider $T(|x_0 \dots x_{i-1}\rangle \otimes |\psi\rangle \otimes |x_{i+1} \dots x_{N-1}\rangle)$
 $= \begin{cases} |x_0 \dots x_{i-1}\rangle \otimes W |\psi\rangle \otimes |x_{i+1} \dots x_{N-1}\rangle \\ |x_0 \dots x_{i-1}\rangle \otimes |\psi\rangle \otimes |x_{i+1} \dots x_{N-1}\rangle \end{cases}$
 $x_j = g^m_j$ for $j \neq i$

$$|\psi^m\rangle = T |\psi^{m-1}\rangle$$

Step $m+1$: $|\psi^{m+1}\rangle = S_{m-1}^\dagger |\psi^m\rangle = S_{m-1} |\psi^m\rangle$

:

Step $2m-1$: $|\psi^{2m-1}\rangle = S_1^\dagger |\psi^{2m-2}\rangle$

If $|\psi\rangle = |g^0\rangle = |s\rangle$ then $|\psi^1\rangle = |g^1\rangle, \dots, |\psi^{m-1}\rangle = |g^{m-1}\rangle$

If $|\psi\rangle = |g^m\rangle = |t\rangle$ then $|\psi^1\rangle = |g^m\rangle, \dots, |\psi^{m-1}\rangle = |g^m\rangle$

T on $|g^{m-1}\rangle, |g^m\rangle$ is like W on $\mathbb{C}^2$

$\Rightarrow$ after "rewinding" (Steps $m+1 \sim 2m-1$) we get the action of U .

If $|\psi\rangle = |g^k\rangle$ $0 \leq k < m$. then $|\psi^1\rangle = |\psi\rangle, \dots, |\psi^k\rangle = |\psi\rangle$
 $|\psi^{k+1}\rangle = |g^{k-1}\rangle$, rewinding brings it back to $|g^k\rangle$

If $|\psi\rangle = |x\rangle$ $x \in \{0, 1\}^N$ $x \neq g^i$ then no effect.

Prop 2. control by single bit.

Suppose $W = e^{i\alpha} A \otimes B \otimes C$ $A, B, C \in U(2)$

$$ABC = I_2, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Then



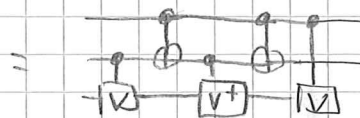
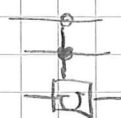
$$|0\rangle \otimes |\varphi\rangle \mapsto |0\rangle \otimes ABC|\varphi\rangle = |0\rangle \otimes |\varphi\rangle$$

$$|1\rangle \otimes |\varphi\rangle \mapsto e^{i\alpha} |1\rangle \otimes AXBX C|\varphi\rangle = |1\rangle \otimes W|\varphi\rangle$$

Fact : any W is of this form. (N-C Cor 4.2)

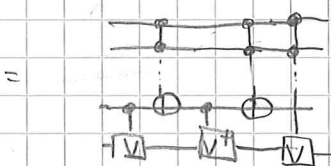
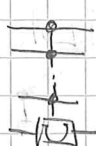
Prop 3. control by multiple bits.

two-bit control :



$$U = V^2$$

multiple bits control :



Prop 4 control by opposite condition.

$$\begin{aligned} |x\rangle &\text{---} \text{---} |x\rangle \\ |\varphi\rangle &\text{---} \boxed{U} \begin{cases} U|\varphi\rangle & \text{if } x=0 \\ |\varphi\rangle & \text{if } x=1 \end{cases} \end{aligned}$$



Universality with finite sets

we want a finite set of gates for universality
(March 9).

scalar part $e^{i\alpha} I_2$

if $\alpha = 2\pi\theta$, θ irrational, $(e^{i\alpha} I_2)^k = e^{2\pi i k \theta} I_2$

can approximate any $e^{i\beta} I_2$

$$SU(2) = \{U \in U(2), \det U = 1\}$$

simple compact Lie group

$$S = \{U_0, \dots, U_{k-1}\} \subset SU(2) \text{ generic choice, } k \geq 1$$

$\Rightarrow$ any $U \in SU(2)$ can be approximated by
products of U_i : $U \sim V_0 \dots V_{m-1}$, $V_i \in S$.

Generally, given $S \subset SU(2)$ put

$$G = \{U \in SU(2) : \forall \epsilon > 0 \exists V_0, \dots, V_{m-1} \in S$$

$$U \sim_{\epsilon} V_0 \dots V_{m-1}\}$$

then

• G is a subgroup : $U, U' \in G \Rightarrow UU' \in G$

$$U \sim_{\mathbb{Z}} V_0 \cdots V_{m-1}, U' \sim_{\mathbb{Z}} V'_0 \cdots V'_{l-1} \Rightarrow UU' \sim_{\mathbb{Z}} V_0 \cdots V_{m-1} V'_0 \cdots V'_{l-1}$$

• G is closed : $U \in \text{SU}(2), V_0, V_1, \dots \in G, V_i \rightarrow U \Rightarrow U \in G$.

Closed subgroups of $\text{SU}(2)$ are classified

• $\text{SU}(2)$

$$\bullet \left\{ \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix}, \begin{bmatrix} 0 & e^{i\alpha} \\ -e^{-i\alpha} & 0 \end{bmatrix} : \alpha \in \mathbb{R} \right\}$$

$$\bullet \left\{ \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix} : \alpha \in \mathbb{R} \right\}$$

• finite subgroups. (symmetry of regular polyhedra, regular polygons)

up to conjugation (UGU^+ is as above)