Lecture 8 CPSC 447/547 - Intro to QC.

Quantum Compiling

In the next two lectures, we will derive what we now know as (efficient) universality in the context of quantum computation. Today, we focus on small examples, then next time, we will prove the universality theorem.

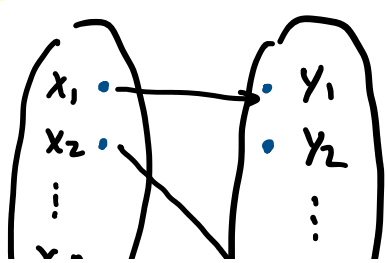
Circuit Synthesis.

Classical case: Boolean circuits on n bits

- How many different functions (i.e., truth tables) can we define for the transformations on n bits?

X : 2^n possible inputs , Y : 2^n possible outputs.

 # functions on n bits $= Y^X = (2^n)^{2^n} = 2^{2^n \cdot n}$



- All Boolean functions on n bits can be labeled (parametrized) by $2^n \cdot n$ bits
- (Previously) we also used the fact that all Boolean functions can be implemented by AND, OR, NOT gates (and FANOUT, SWAP)

Can we say something similar in the quantum case?

Quantum case : quantum circuits on <u>n qubits</u>

$$|x\rangle : \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle \quad \text{possible input state}$$

$$|y\rangle : \sum_{j \in \{0,1\}^n} \beta_j |j\rangle \quad \text{possible output state}$$

Possible transformations : unitary $U \in \mathbb{C}^{2^n \times 2^n}$

<u>E.g.</u> $n=1$

$$U = \begin{bmatrix} e^{i\alpha}\cos(\theta) & e^{i\beta}\sin(\theta) \\ -e^{-i\beta}\sin(\theta) & -e^{-i\alpha}\cos(\theta) \end{bmatrix}$$

- All unitary transformation on n qubits can be parametrized $O(2^{2n})$ indep real numbers.

- Can all unitary transformation be implemented by a finite set of elementary gates?

(*) **Theorem** Single-qubit and two-qubit gates are computationally universal.

① Two-qubit gates are necessary : entanglement

② Two-qubit gates are sufficient : (prove later) ☆

Example universal instruction set:

$\{H, CNOT, T\}$

E.g. How to get Z gate from this?

$$Z = T^4$$

- How about Y?

$$Y = (i)ZX = (i)T^4HT^4H$$

- How about $\sqrt{T} \equiv R_z(\frac{\pi}{8})$?

(Efficient) compling algorithms / synthesis algorithms

- Exact synthesis

→ Some algorithms well-known for single- and two-qubit unitaries.

single ...

- **Approximate synthesis**

  → Solovay-Kitaev algorithm, optimization-based, etc.

* Efficient Compiling:

For some instruction set, a **polynomial # of gates** is sufficient to synthesize arbitrary unitary.

Sequential and Parallel Execution of gates

- Order of gates:

$$|\psi\rangle \;-\boxed{A}-\boxed{B}- \quad : |\psi'\rangle = B\cdot A\cdot|\psi\rangle$$

$$\xrightarrow{\text{time}}$$

- Reordering

① Commutation relations

Def. The commutator of two gates A, B is $[A, B] = AB - BA$.

If $[A, B] = 0$, "A and B commute"

$AB = BA$ $\quad -\boxed{B}-\boxed{A}- \;=\; -\boxed{A}-\boxed{B}-$

Free to reorder.

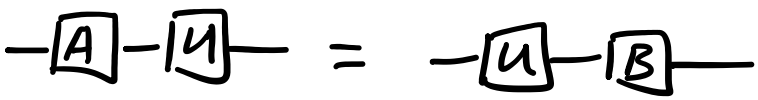
Q: Is $[X, H] = 0$?

② Conjugation relations.

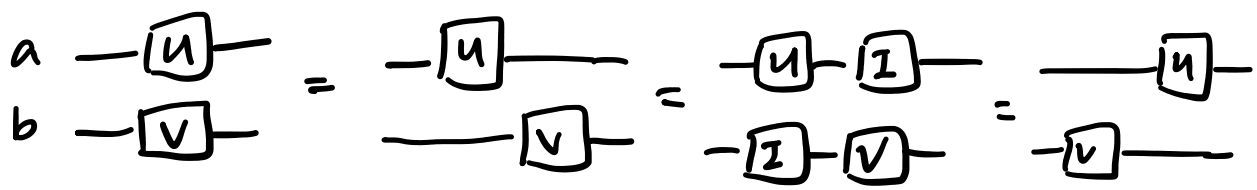
<u>Def</u> Two gates, A and B, are conjugate (by U), if there exists a gate U, s.t.

$$UAU^{\dagger} = B$$

$$\Rightarrow UAU^{\dagger}U = BU \Rightarrow UA = BU.$$



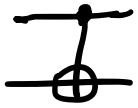
· <u>Parallelism</u>



$$(U \otimes V) = (U \otimes I)(I \otimes V) = (I \otimes V)\cdot(U \otimes I)$$

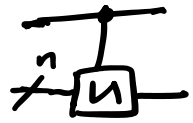
Controlled Quantum Gates

<u>Eg.</u> <u>CNOT gate</u>: C-X gate



$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \left[\begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array}\right]$$

Controlled-U gate:



control qubit is the first qubit

$$C\text{-}U = \begin{array}{c} 00\cdots0 \\ 0\cdots1 \\ \vdots \\ 011\cdots1 \\ 100\cdots0 \\ 100\cdots1 \\ \vdots \\ 111\cdots1 \end{array} \left[\begin{array}{c|c} I & 0 \\ \hline 0 & U \end{array}\right]$$

Note $C\text{-}U \neq I \otimes U$.

E.g. $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$. $C\text{-}U = \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & u_1 & u_2 \\ & & u_3 & u_4 \end{bmatrix}$

What is $C\text{-}U \cdot \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} = ?$

$$= \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ u_1\alpha_{10} + u_2\alpha_{11} \\ u_3\alpha_{10} + u_4\alpha_{11} \end{bmatrix}.$$

Block-Diagonal Gates

$$T_i(V) = \begin{bmatrix} I_{i-1} & & & \\ & V & & \\ & & I_{d-i-1} & \\ & & & \end{bmatrix}, \text{ where } d = 2^n$$

$I_k = (k \times k)$ Identity matrix

$V = (2 \times 2)$ unitary matrix.

$1 \leq i \leq d-1$

- Unitary?
- What is $T_i(V) \cdot \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_i \end{bmatrix} = ?$ $\left(V = \begin{bmatrix} v_1 & v_2 \\ v_3 & v_4 \end{bmatrix} \right)$

$$\begin{bmatrix} \vdots \\ \alpha_{d-1} \end{bmatrix}$$

Let $|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, $|i\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i\text{th}$

$$T_i(U)|0\rangle = |0\rangle$$

$$T_i(U)|1\rangle = |1\rangle.$$

$$\vdots$$

$$T_i(U)|i-1\rangle = v_1|i-1\rangle + v_2|i\rangle.$$

$$T_i(U)|i\rangle = v_3|i-1\rangle + v_4|i\rangle.$$

$$\vdots$$

$$T_i(U)|d-1\rangle = |d-1\rangle.$$

Proof for Theorem (*)

Outline

① Represent unitary for n-qubits as a product of $O(2^{2n})$ matrices of Block-Diagonal form:

$$T_i(U) = \begin{bmatrix} I & & \\ & U & \\ & & I \end{bmatrix}$$

② Decompose each $T_i(U)$ into two-qubit gates.

(Prove in next lecture!)