Lecture 2: Quantum Circuit

Isaac H. Kim

7/14/2022

UC Davis

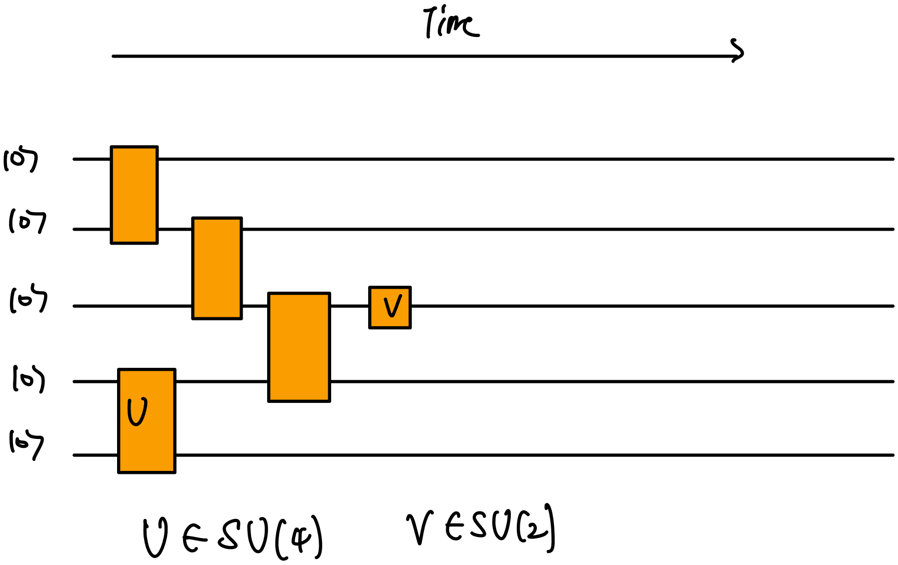
Gate-based model

The standard model of quantum computation is a gate-based model of quantum computation.

- A gate is a unitary transformation acting on $O(1)$ qubits.
- A quantum circuit is a sequence of quantum gates.

In quantum computing literature, there are standard gates and gate identities that are often used. The purpose of this lecture is to explain the motivation behind these standard gate set and the ideas behind how the identities are derived.

Circuit Diagram



Part 1. Universal Gate set

Quantum computation

Quantum computation, at the highest level, is a unitary transformation acting on n qubits.

(Nielsen and Chuang) ↓

Fact

Arbitrary unitary $U \in \mathcal{B}(\mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_2)$ can be decomposed into a sequence of one- and two-qubit gates.

Universal Gate Set

A gate set $\mathcal{G}$ is *universal* if any unitary can be approximated arbitrarily well using the set of gates in $\mathcal{G}$.

Is quantum computing analog?

The set of unitaries is not a finite set. So it appears that QC is analog. However, surprisingly, any element in this set can be approximated arbitrarily well by a *finite set* of one- and two-qubit gates. It is in this sense quantum computing is “digital.”

Is quantum computing analog?

Some of the early critiques of quantum computing said that it will be impossible to do quantum computation because coherence over exponentially many branches will be very difficult to maintain. We now know that this is a fallacious argument.

In the theory of quantum error correction, one can detect the presence/absence of error by performing a measurement. This measurement process "collapses" the state onto one of discrete set of states, after which the error can be corrected. This is another sense in which quantum computing is "digital."

Which gate set?

It is well-known that almost all discrete gate set is universal [Harrow, Recht, Chuang (2001)]. So there is a natural question: which gate set should we choose?

Experimental Constraint

- Current hardware error rate: $10^{-2} \sim 10^{-3}$
- Number of gates needed to solve commercially useful problems: $10^{10} \sim 10^{15}$.

$\rightarrow$ Error correction is absolutely necessary to do something useful.

Which gate set?

It is well-known that almost all discrete gate set is universal [Harrow, Recht, Chuang (2001)]. So there is a natural question: which gate set should we choose?

Experimental Constraint

- Current hardware error rate: $10^{-2} \sim 10^{-3}$
- Number of gates needed to solve commercially useful problems: $10^{10} \sim 10^{15}$.

→ Error correction is absolutely necessary to do something useful.

Quantum Error Correction is compatible only with a rather specific set of gates. All these gates can be cleanly organized into what is known as the Clifford Hierarchy.

Part 2. Clifford Hierarchy

High-level

1. Level-0: Paulis $P_1, P_2 \ldots$
2. Level-1: Unitaries that send Paulis to Paulis : U s.t. $UP_1U^\dagger$ is Pauli
3. Level-2: Unitaries that send Paulis to Level-1 $UP_1U^\dagger$: level 1
4. Level-3: Unitaries that send Paulis to Level-2 $UP_1U^\dagger$: Level 2
5. . . .

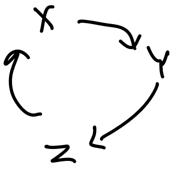
Single-Qubit Paulis

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For any Pauli $P, Q \neq I$,

- $P^2 = I$.
- $\{P, Q\} = 0$.
- $XY = iZ, YZ = iX, ZX = iY$.

$YX = -iZ$



$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad \sigma^Y \quad \sigma^Z$

$X^2 = I$

$\mathrm{Tr}(X) = 0$

$X = U \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} U^\dagger$ $\quad X^2 = U \begin{pmatrix} \lambda_1^2 & 0 \\ 0 & \lambda_2^2 \end{pmatrix} U^\dagger$

$= I$

$\begin{pmatrix} \lambda_1^2 & 0 \\ 0 & \lambda_2^2 \end{pmatrix} = I$

λ_1, λ_2

$\pm 1 \quad \pm 1$

$\mathrm{Tr}(X) = \lambda_1 + \lambda_2$

Multi-Qubit Paulis

→ Pauli String

$$\boxed{P = \pm P_1 \otimes P_2 \otimes \dots P_{n-1} \otimes P_n}$$

$P_i \in \{I, X, Y, Z\}$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For any multi-qubit Paulis P, Q

- $P^2 = I$
- $[P, Q] = 0$ or $\{P, Q\} = 0$.

$P^2 = I$

$P = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix} U^\dagger$

$\lambda_1^2 = \lambda_2^2 = \cdots \lambda_N^2 = 1$

$\mathrm{Tr}(P) = 0$

$= \mathrm{Tr}(P_1)\,\mathrm{Tr}(P_2) \cdots \mathrm{Tr}(P_n)$

$= 0 = \sum_{i=1}^{N} \lambda_i$

$(P_1 \otimes \cdots \otimes P_n)(|\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle) = P_1|\phi_1\rangle \otimes \cdots \otimes P_n|\psi_n\rangle$

$(P_1 \otimes \cdots \otimes P_n)(P_1 \otimes \cdots \otimes P_n) = P_1P_1 \otimes \cdots \otimes P_nP_n$

$= I \otimes \cdots \otimes I$

$(Z \otimes Z)(X \otimes X) = ZX \otimes ZX = (-XZ) \otimes (-XZ) = (-1)^2\, XZ \otimes XZ$

$= (X \otimes X)(Z \otimes Z)$

Clifford Unitaries

Definition

A n-qubit unitary U is *Clifford* if for all Pauli P, $UPU^\dagger$ is a Pauli.

ex) H, S, $CNOT$, ...

$\pm I, \pm X, \pm Y, \pm Z$

$UPU^\dagger \in \{\pm I, \pm X, \pm Y, \pm Z\}$

Single-qubit Clifford Unitaries

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$HXH^\dagger = HXH = Z$ $\qquad HZH^\dagger = H^2XH^2 = X$ $\qquad HYH = H(iZX)H = HiZH\ HXH = iXZ = -iZX$
$= -Y$

$H^2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow H = H^\dagger$

$SXS^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y$

$SYS^\dagger = S^2X(S^\dagger)^2 = ZXZ = -X$

$S^2 = Z$

Two-qubit Clifford Unitaries

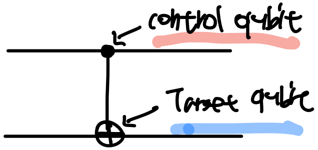
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

ex) CX (=CNOT), CZ

$CX(|0\rangle\otimes|\psi\rangle) = |0\rangle\otimes|\psi\rangle$

$CX(|1\rangle\otimes|\psi\rangle) = |1\rangle\otimes X|\psi\rangle$

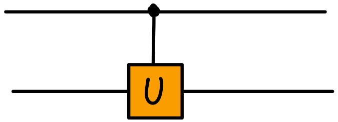
$CX = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X$



$CU(|0\rangle\otimes|\psi\rangle) = |0\rangle\otimes|\psi\rangle$

$CU(|1\rangle\otimes|\psi\rangle) = |1\rangle\otimes U|\psi\rangle$

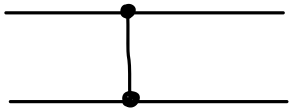
$CU = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U$



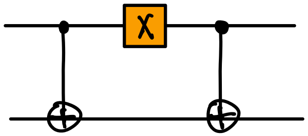
$CZ(|0\rangle\otimes|\psi\rangle) = |0\rangle\otimes|\psi\rangle$

$CZ(|1\rangle\otimes|\psi\rangle) = |1\rangle\otimes Z|\psi\rangle$

$CZ = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes Z$
$= I\otimes|0\rangle\langle 0| + Z\otimes|1\rangle\langle 1|$



$CX\, P\, CX^{\dagger} = Q \in \text{Pauli}$



$CX^2 = I$

$|0\rangle\otimes|\psi\rangle \xrightarrow{CX} |0\rangle\otimes|\psi\rangle \xrightarrow{X} |1\rangle|\psi\rangle \xrightarrow{CX} |1\rangle X|\psi\rangle = (X\otimes X)(|0\rangle\otimes|\psi\rangle)$

$|1\rangle\otimes|\psi\rangle \xrightarrow{CX} |1\rangle\otimes X|\psi\rangle \xrightarrow{X} |0\rangle\otimes X|\psi\rangle \xrightarrow{CX} |0\rangle\otimes X|\psi\rangle = (X\otimes X)(|1\rangle\otimes|\psi\rangle)$

$\underline{CX(X\otimes I)CX = X\otimes X}$

Clifford Unitaries

Clifford unitaries form a group, and this group can be generated by H, S, and CNOT.

Gottesman-Knill theorem

The exact amplitude/expectation value of any Pauli over a state created by applying a Clifford to $|0\dots0\rangle$ can be efficiently computed on a classical computer.
$\rightarrow$ Clifford unitaries are classically efficiently simulable.

T-gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}$$

This gate is in the second level of the Clifford hierarchy.

$TXT^\dagger \in$ Clifford

$TYT^\dagger \in$ ''

$TZT^\dagger \in$ ''

$$\boxed{TXT^\dagger} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i}^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \sqrt{i}^{-1} \\ \sqrt{i} & 0 \end{pmatrix}$$

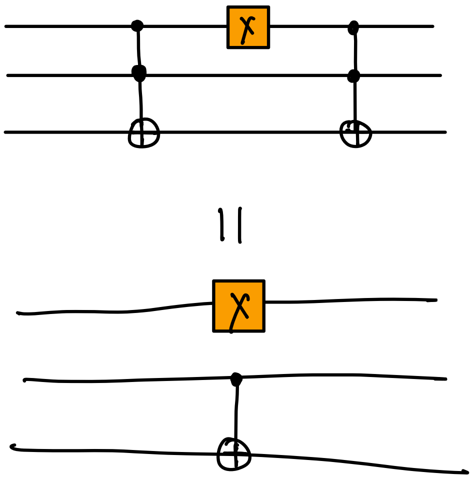
$$= \sqrt{i}^{-1} \underline{\begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}}$$

$$\underline{SX} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \underline{\begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}}$$

Toffoli gate

Toffoli gate is also in the second level of the Clifford hierarchy.



$$\text{Toffoli} = CCX\, |1\rangle|1\rangle|\psi\rangle = |1\rangle|1\rangle\, X|\psi\rangle$$

$$CCX\, |x\rangle|y\rangle|\psi\rangle = |x\rangle|y\rangle|\psi\rangle$$ Otherwise (i.e., $x \neq 1$ or $y \neq 1$)

$$CCX\,(X\otimes I\otimes I)\,CCX\quad |0\rangle\otimes|\psi\rangle\otimes|\psi'\rangle$$

$$CCX\,(X\otimes I\otimes I)\,CCX\quad |1\rangle\otimes|\psi\rangle\otimes|\psi'\rangle$$

A very important fact

The following gate sets are universal.

- Clifford + T
- Clifford + Toffoli

These are often the standard gate sets that people use in the literature.

Part 2. Side comment: Algorithm to gates

A question

Often a quantum algorithm is specified in terms of sequence of *continuous gates.* How can this be translated into a sequence of discrete gate set?

Solovay-Kitaev theorem

Theorem. Let $\mathcal{G}$ be a finite set of elements in $SU(2)$ containing their inverses such that the group they generate is dense in $SU(2)$. For any $\epsilon > 0$, there is a constant $\underset{\sim}{c}$ such that for any $U \in SU(2)$, there is a sequence of gates in $\mathcal{G}$ (denoted as S) such that

$$\|S - U\| \leq \epsilon.$$

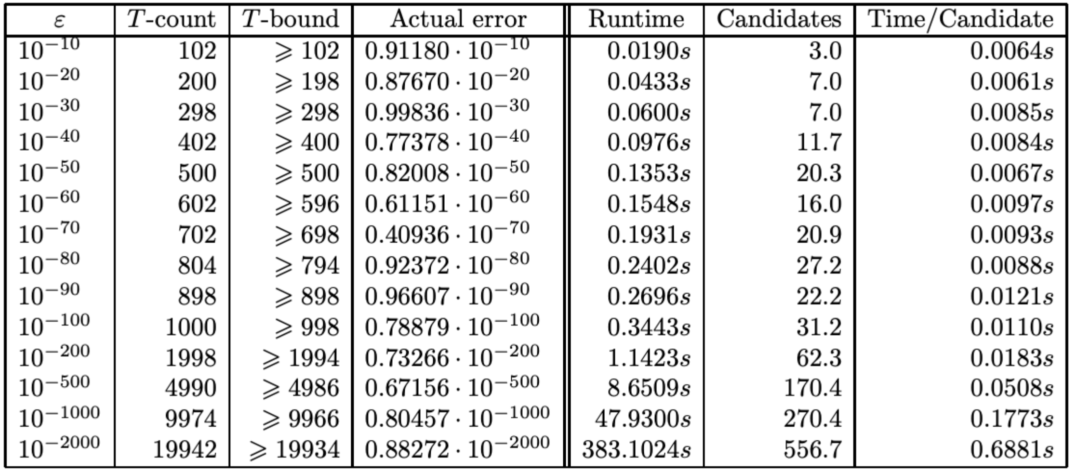
Length of the sequence

$= O\left(\log^c \frac{1}{\varepsilon}\right)$

* Remark: The proof is constructive.

Approximating rotation by Clifford + T

The Solovay-Kitaev theorem is already pretty good, but for Clifford+T, we can do much better. We can approximate any gate in $SU(2)$ up to an error ϵ using $O(\log 1/\epsilon)$ gates. [Kliuchnikov and Mosca, Ross and Selinger]



ε	T-count	T-bound	Actual error	Runtime	Candidates	Time/Candidate
10^{-10}	102	$\geqslant 102$	$0.91180 \cdot 10^{-10}$	$0.0190s$	3.0	$0.0064s$
10^{-20}	200	$\geqslant 198$	$0.87670 \cdot 10^{-20}$	$0.0433s$	7.0	$0.0061s$
10^{-30}	298	$\geqslant 298$	$0.99836 \cdot 10^{-30}$	$0.0600s$	7.0	$0.0085s$
10^{-40}	402	$\geqslant 400$	$0.77378 \cdot 10^{-40}$	$0.0976s$	11.7	$0.0084s$
10^{-50}	500	$\geqslant 500$	$0.82008 \cdot 10^{-50}$	$0.1353s$	20.3	$0.0067s$
10^{-60}	602	$\geqslant 596$	$0.61151 \cdot 10^{-60}$	$0.1548s$	16.0	$0.0097s$
10^{-70}	702	$\geqslant 698$	$0.40936 \cdot 10^{-70}$	$0.1931s$	20.9	$0.0093s$
10^{-80}	804	$\geqslant 794$	$0.92372 \cdot 10^{-80}$	$0.2402s$	27.2	$0.0088s$
10^{-90}	898	$\geqslant 898$	$0.96607 \cdot 10^{-90}$	$0.2696s$	22.2	$0.0121s$
10^{-100}	1000	$\geqslant 998$	$0.78879 \cdot 10^{-100}$	$0.3443s$	31.2	$0.0110s$
10^{-200}	1998	$\geqslant 1994$	$0.73266 \cdot 10^{-200}$	$1.1423s$	62.3	$0.0183s$
10^{-500}	4990	$\geqslant 4986$	$0.67156 \cdot 10^{-500}$	$8.6509s$	170.4	$0.0508s$
10^{-1000}	9974	$\geqslant 9966$	$0.80457 \cdot 10^{-1000}$	$47.9300s$	270.4	$0.1773s$
10^{-2000}	19942	$\geqslant 19934$	$0.88272 \cdot 10^{-2000}$	$383.1024s$	556.7	$0.6881s$

From Ross and Selinger (2014).

Compilation

continuous

Algorithm → One- and Two-Qubit Gates → Discrete Gate Sequence

Another evidence that quantum computing is digital!

Part 3. Gate/Circuit Identities

Motivation

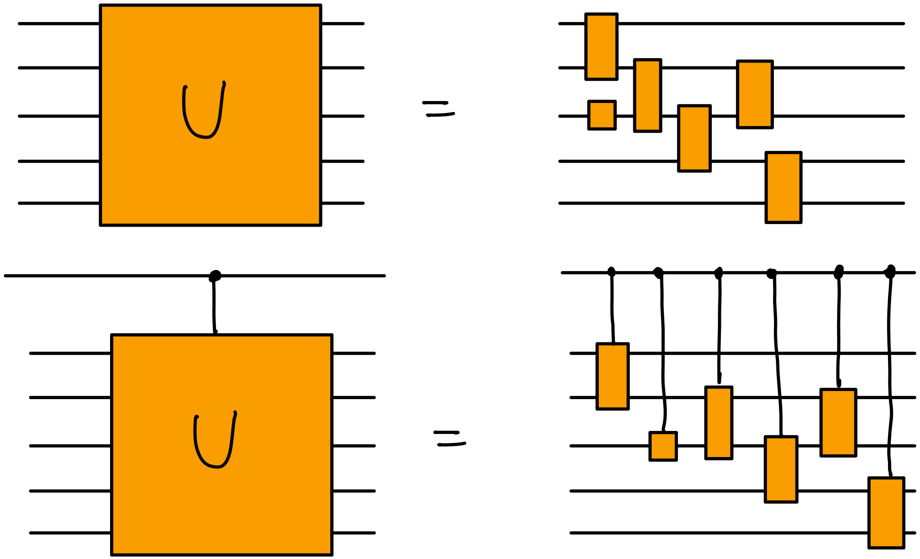
When we convert an algorithm into one- and two-qubit gates, there are many well-known identities that people use.

The gate identities involving a single qubit is often straightforward and easy to work out via brute-force calculation. However, multi-qubit identities tend to be trickier. We will discuss several tricks.

Controlled-Unitary

Suppose we are given a unitary U described in terms of a sequence of gates. How can we implement the following?

$$(\alpha|0\rangle \otimes +\beta|1\rangle)|\psi\rangle \to \alpha|0\rangle \otimes |\psi\rangle + \beta|1\rangle \otimes U|\psi\rangle$$



Multiplying controlled unitaries

We know that

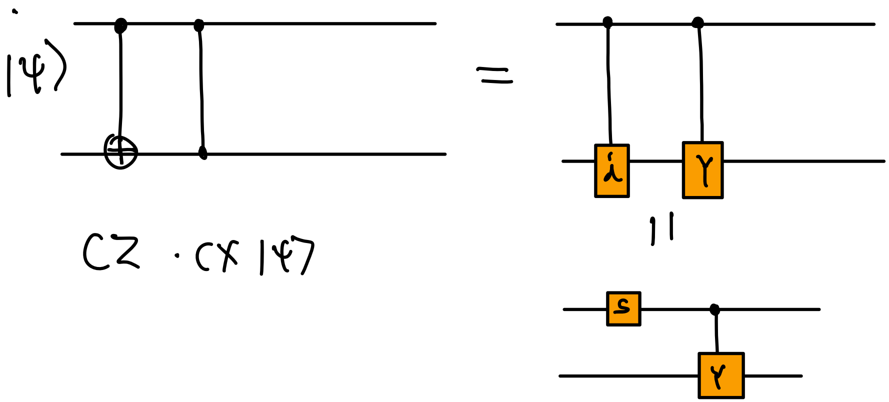
$$ZX|\psi\rangle = iY|\psi\rangle \equiv Y|\psi\rangle,$$

because the global state does not matter in quantum mechanics.

What about $CZ \cdot CX$?

$$CZ \cdot CX \neq CY$$

$$CZ \cdot CX = C(iY) = C(i) \cdot C(Y)$$



$$C(i)\,|0\rangle\,|\psi\rangle = |0\rangle\,|\psi\rangle$$

$$C(i)\,|1\rangle\,|\psi\rangle = |1\rangle\; i\,|\psi\rangle$$

$$= i\,|1\rangle\,|\psi\rangle$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$e^{iP\theta}$

It will become pretty evident in the next lecture that the gates of the form of $e^{iP\theta}$, where P is a multi-qubit Pauli, appears very frequently in quantum algorithms. How can we decompose this into one-and two-qubit gates?

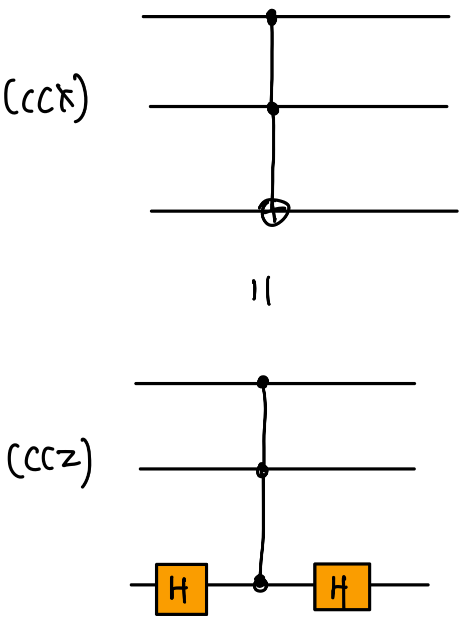
e^{-iHt}

$$P = \underset{\text{Clifford}}{\underset{\downarrow}{C}} \; Z_1 \; C^{\dagger}$$

$$e^{iP\theta} = e^{iCZ_1C^{\dagger}\theta} = C \, e^{iZ_1\theta} \, C^{\dagger}$$

Decomposing Toffoli

How do you decompose a Toffoli into one- and two-qubit gates?



$$CCX|x\rangle|y\rangle|\psi\rangle = \begin{cases} |x\rangle|y\rangle|\psi\rangle & \text{if } x\neq 1 \text{ or } y\neq 1 \\ |x\rangle|y\rangle X|\psi\rangle & \text{otherwise,} \end{cases}$$

$$CCZ|x\rangle|y\rangle|\psi\rangle = \begin{cases} |x\rangle|y\rangle|\psi\rangle & \text{if } x\neq 1 \text{ or } y\neq 1 \\ |x\rangle|y\rangle Z|\psi\rangle & \text{otherwise} \end{cases}$$

$$X = HZH$$

$$CCZ = e^{i\pi\underline{\left(\frac{I-Z_1}{2}\otimes\frac{I-Z_2}{2}\otimes\frac{I-Z_3}{2}\right)}}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\frac{I-Z}{2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= e^{i\pi(\frac{1}{8}(I - Z_1 - Z_2 - Z_3 + Z_1Z_2 + Z_1Z_3 + Z_2Z_3 - Z_1Z_2Z_3)}$$

$$\frac{I-Z}{2}|0\rangle = 0$$

$$\frac{I-Z}{2}|1\rangle = |1\rangle$$

Recap

1. Universal Gate Set: It makes a lot of sense to use Clifford + T
2. Algorithm $\rightarrow$ one-and two-qubit gates $\rightarrow$ Clifford + T
3. Various circuit identities: These will prove to be useful for tomorrow's lecture.