Quantum Circuits (pt. 2)

CSE 490Q: Quantum Computation

Quantum Universal Instruction Set

- With quantum circuits, here is one universal set:
  - any 1-qubit operation
  - CNOT
- Classical 1-bit operations are boring: identity and NOT
- Quantum 1-bit operations have much more complexity
  - there are infinitely many of them!
  - might seem unreasonable to ask of hardware, but…

Practical Quantum Instruction Sets

- Other quantum computers would restrict 1-qubit operations further
  - e.g., to just H and T (introduced later)
- Such finite sets of operations can approximate any 1-qubit operation
  - see the textbook for a proof for one such set
- This approximation has some error, but that is no problem
  - BQP allows us to fail up to 1/3 of the time
  - errors on different operations do not multiply (homework problem)
- Quantum compiler will hide the details of this from us

Theoretical Quantum Instruction Sets

- Measure "time" by the number of unitaries performed
  - want this to be polynomial, not exponential in input size
- For theory purposes, can assume we have k-qubit operations for any $k = O(1)$ that we want
  - can approximate any such U with O(1) allowed instructions
  - Increases total time by factor of O(1)
    - doesn't change what is "polynomial time"
- (Constant factors do matter, though, for current quantum computers.)

Theoretical Quantum Instruction Sets

- Measure "time" by the number of unitaries performed
  - want this to be polynomial, not exponential in input size
- For theory purposes, can assume we have k-qubit operations for any k = O(1) that we want
- We can apply U to *any* k of the qubits
  - (figuring out how is, again, the compiler's job)
  - sometimes write, e.g., by $[U]_{4,7}$ to denote a 2x2 unitary U applied to qubits 4 and 7 (identity on rest)

Z Gate

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \mathrm{diag}(1, -1)$$

$$Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -\begin{bmatrix} 0 \\ 1 \end{bmatrix} = -|1\rangle$$

$$\boxed{Z|0\rangle = |0\rangle \quad \text{and} \quad Z|1\rangle = -|1\rangle}$$

+ and -

Define $|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

and $|-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$$Z|+\rangle = Z\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}Z|0\rangle + \frac{1}{\sqrt{2}}Z|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$$

$$Z|-\rangle = \frac{1}{\sqrt{2}}Z|0\rangle - \frac{1}{\sqrt{2}}Z|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$$

[Z swaps $|+\rangle$ and $|-\rangle$]

X Gate

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$X|0\rangle = |1\rangle$ and
$X|1\rangle = |0\rangle$

$$X|+\rangle = X\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$$

$$X|-\rangle = X\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle = -\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = -|-\rangle$$

X and Z Gates

$+1 \qquad -1$

- X is swap on |0> and |1> and phase on |+> and |->
  - X|0> = |1> and X|1> $= |0\rangle$
  - X|+> = |+> and X|-> = -|->

- Z is phase on |0> and |1> and swap on |+> and |->
  - Z|0> = |0> and Z|1> = -|1>
  - Z|+> = |-> and Z|-> = |+>

$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}^T \begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{2}(1-1) = 0$

- Same operation but on basis {|0>,|1>} vs {|+>,|->)
  - note that |+> and |-> are orthogonal
  - called Z-basis and X-basis

Changing Bases

$$(A^{\dagger})^{\dagger} = I$$

$$\overset{H}{\cancel{m}} = |+\rangle\langle 0| + |-\rangle\langle 1|$$

$$\overset{H^{\dagger}}{\cancel{m^{\dagger}}} = (|+\rangle\langle 0|)^{\dagger} + (|-\rangle\langle 1|)^{\dagger}$$

$$= |0\rangle\langle +| + |1\rangle\langle -|$$

$$m|0\rangle = |+\rangle$$

$$m|1\rangle = |-\rangle$$

recall $(AB)^{\dagger} = B^{\dagger}A^{\dagger}$

$$m|+\rangle = |0\rangle$$

$$m|-\rangle = |1\rangle$$

$$m = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0 & 1\\0 & -1\end{bmatrix} = \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}} = H.$$

$$H^{\dagger} = H.$$

X, Z, and H

$$X = |1\rangle\langle 0| + |0\rangle\langle 1|$$

$$Z = |-\rangle\langle +| + |+\rangle\langle -| \;?$$

$$= \frac{1}{2}\begin{bmatrix}1\\-1\end{bmatrix}\begin{bmatrix}1 & 1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1 & -1\end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix}1 & 1\\-1 & -1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1 & -1\\1 & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & -2\end{bmatrix}$$

$$= \mathrm{diag}(1,-1).$$

$|+\rangle, |-\rangle$ $(|0\rangle, |1\rangle)$ $\{|+\rangle, |-\rangle\}$

$$\boxed{HXH^\dagger} = H|1\rangle\underbrace{\langle 0|H^\dagger}_{(H|0\rangle)^\dagger} + H|0\rangle\underbrace{\langle 1|H^\dagger}_{(H|1\rangle)^\dagger}$$

$$= |-\rangle\langle +| + |+\rangle\langle -| = \boxed{Z.}$$

X, Z and H

- {|0>, |1>} is called the Z basis
- {|+>, |->) is called the X basis

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix} = I$$

- X and Z operation but on different bases
- $\boxed{Z = H X H \text{ and } X = H Z H}$ $\quad H^{\dagger}H = I$
  - second follows since $H^2 = I$

$$HZH = H(HXH)H$$
$$= H^2 X H^2 = X$$

CNOT

- CNOT acts as
  - I on the second bit if first bit is |0>
  - X on the second bit if first bit is |1>
- CNOT also called "CX"
- CZ is the same but with Z replacing X
  - but H turns X into Z…

CX and CZ

$|0\rangle \otimes |x\rangle + |1\rangle \otimes |y\rangle$

CX → NOT I ⊗ X

- Since H X H = Z and H I H = H H = I, we have
  - CZ = (I ⊗ H) CX (I ⊗ H)
  - CX = (I ⊗ H) CZ (I ⊗ H)

- H turns Z into X and vice versa
- I ⊗ H turns CZ into CX and vice versa

SWAP

00
01
10
11

- SWAP = |00><00| + |10><01| + |01><10| + |11><11|
- Note that CZ|01> = |01> and CZ|10> = |10> CZ|11> = -|11>
  - so CZ is symmetric on the two qubits
  - i.e., SWAP CZ SWAP = CZ
- Same applies to U ⊗ U for any unitary U SWAP^2 = I
  - in particular, we have SWAP (H ⊗ H) SWAP = H ⊗ H
  - or equivalently, SWAP (H ⊗ H) = (H ⊗ H) SWAP
- Whereas we have, SWAP (U ⊗ I) = (I ⊗ U) SWAP for any U

SWAP and CNOT

- Define $CNOT_{1,2}$ = CNOT
  - first bit determines whether to apply I or X on second

$I \otimes H$ $\quad$ $I \otimes H$

- Define $CNOT_{2,1}$ = SWAP $CNOT_{1,2}$ SWAP
  - second bit determines whether to apply I or X on first

- Can see that $(I \otimes H)\ CNOT_{1,2}\ (I \otimes H) = (H \otimes I)\ CNOT_{2,1}\ (H \otimes I)$

$$(H \otimes H)\ CNOT_{1,2}\ (H \otimes H) = (H \otimes I)(I \otimes H)\ CNOT_{1,2}\ (I \otimes H)(H \otimes I)$$
$$= (H \otimes I)(H \otimes I)\ CNOT_{2,1}\ (H \otimes I)(H \otimes I)$$
$$= (H^2 \otimes I)\ CNOT_{2,1}\ (H^2 \otimes I)$$
$$= CNOT_{2,1}$$

SWAP and CNOT

- Define $CNOT_{1,2}$ = CNOT
  - first bit determines whether to apply I or X on second
- Define $CNOT_{2,1}$ = SWAP $CNOT_{1,2}$ SWAP
  - second bit determines whether to apply I or X on first
- $(H \otimes H)\ CNOT_{1,2}\ (H \otimes H) = CNOT_{2,1}$
- $\boxed{(H \otimes H)\ CNOT_{1,2} = CNOT_{2,1}\ (H \otimes H)}$

X and CNOT

$(I \otimes X)\,CNOT = CNOT\,(I \otimes X)$

- $(I \otimes X)$ CNOT $(I \otimes X)$ = CNOT
  - CNOT acts as either I or X on the second qubit
  - $X\,I\,X = X^2 = I$
  - $X\,X\,X = X^2\,X = X$

$I \otimes X$

- $(X \otimes I)$ CNOT $(X \otimes I)$ = $(I \otimes X)$ CNOT = CNOT $(I \otimes X)$
  - correctly leaves the first bit unchanged $X^2 = I$
  - but means ~~second~~ second bit gets an extra X
    - first bit is |0>, it gets X instead of I
    - first bit is |1>, it gets I = X X instead of X

Summary

- Deep *algebraic* relationships between
  X, Z, H, CX, CZ, and SWAP
- We will see useful applications of this later on…
- Full relationships are deeper than we've seen