Quantum Circuits (pt. 2)

CSE 490Q: Quantum Computation
• 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)
$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \text{diag}(1, -1)$

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

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

$Z |0\rangle = |0\rangle$ and $Z |1\rangle = -|1\rangle$
Define \( 1+ \rangle := \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \)

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

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

[2 \text{ swaps } 1+ \rangle \text{ and } 1- \rangle]
X Gate

\[ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \]

\[ X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle \]

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

\[ X|-\rangle = X \left( \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) \]
\[ = \frac{1}{\sqrt{2}} (|1\rangle - |1\rangle) = - \left( \frac{1}{\sqrt{2}} |1\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = |-\rangle \]
X and Z Gates

• **X** is swap on \( |0\rangle \) and \( |1\rangle \) and phase on \( |+\rangle \) and \( |-\rangle \)
  - \( X|0\rangle = |1\rangle \) and \( X|1\rangle = |-\rangle \)
  - \( X|+\rangle = |+\rangle \) and \( X|-\rangle = -|-\rangle \)

• **Z** is phase on \( |0\rangle \) and \( |1\rangle \) and swap on \( |+\rangle \) and \( |-\rangle \)
  - \( Z|0\rangle = |0\rangle \) and \( Z|1\rangle = -|1\rangle \)
  - \( Z|+\rangle = -|-\rangle \) and \( Z|-\rangle = |+\rangle \)

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

\[ \frac{1}{\sqrt{2}} (|0\rangle - i|1\rangle) = 0 \]
Changing Bases

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

\[ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H^+ = H \]

\[ (A^+)^+ = I \]

\[ m\left|0\right> = \left|+\right> \]

\[ m\left|1\right> = \left|-\right> \]

Recall \((AB)^+ = B^+A^+\)

\[ m\left|1+\right> = \left|0\right> \]

\[ m\left|1-\right> = \left|1\right> \]
$X = \begin{vmatrix} 1 \end{vmatrix} + \begin{vmatrix} 0 \end{vmatrix} + \begin{vmatrix} 1 \end{vmatrix} + \begin{vmatrix} 1 \end{vmatrix}$

$Z = \begin{vmatrix} 1 \end{vmatrix} + \begin{vmatrix} 1 \end{vmatrix} + \begin{vmatrix} 1 \end{vmatrix} - \begin{vmatrix} 1 \end{vmatrix}$

$\begin{align*}
Z &= \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \\
&= \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 \\ 0 \\ -2 \end{bmatrix} \\
H &= \begin{bmatrix} H_{11}^{+} \end{bmatrix}^{+} + \begin{bmatrix} H_{10} \end{bmatrix}^{+} \\
&= \begin{bmatrix} \text{diag}(1, \text{diag}(1, -1)) \end{bmatrix} \\
H &= \begin{bmatrix} 1 \end{bmatrix}^{+} + \begin{bmatrix} 1 \end{bmatrix}^{+} - \begin{bmatrix} 1 \end{bmatrix}^{+} = \frac{1}{2}.
• \{|0\>, |1\>\} is called the Z basis
• \{|+, -\rangle\} is called the X basis
• X and Z operation but on different bases
  \[ Z = H X H \quad \text{and} \quad X = H Z H \]
  • second follows since \( H^2 = I \)
CNOT

• CNOT acts as
  • \(I\) on the second bit if first bit is \(|0\rangle\)
  • \(X\) on the second bit if first bit is \(|1\rangle\)

• CNOT also called “CX”

• CZ is the same but with \(Z\) replacing \(X\)
  • but \(H\) turns \(X\) into \(Z\)...
CX and CZ

- Since $H \times H = Z$ and $H \cdot H = H \cdot H = I$, we have
  - $CZ = (I \otimes H) \cdot CX \cdot (I \otimes H)$
  - $CX = (I \otimes H) \cdot CZ \cdot (I \otimes H)$

- $H$ turns $Z$ into $X$ and vice versa
- $I \otimes H$ turns $CZ$ into $CX$ and vice versa
SWAP

- SWAP = |00><00| + |10><01| + |01><10| + |11><11|

- Note that CZ|01> = |01> and CZ|10> = |10>
  - so CZ is symmetric on the two qubits
  - i.e., SWAP CZ SWAP = CZ

- Same applies to U \otimes U for any unitary U
  - in particular, we have SWAP (H \otimes H) SWAP = H \otimes H
  - or equivalently, SWAP (H \otimes H) = (H \otimes H) SWAP

- Whereas we have SWAP (U \otimes I) = (I \otimes U) SWAP for any U
SWAP and CNOT

• Define $\text{CNOT}_{1,2} = \text{CNOT}$
  • first bit determines whether to apply $I$ or $X$ on second

• Define $\text{CNOT}_{2,1} = \text{SWAP} \ CNOT_{1,2} \ \text{SWAP}$
  • second bit determines whether to apply $I$ or $X$ on first

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

\[ (H \otimes H) \ CNOT_{1,2} (H \otimes H) = (H \otimes I)(I \otimes H) \ CNOT_{1,2} (I \otimes H)(H \otimes I) = (H \otimes I)(H \otimes I) \ CNOT_{2,1} (H \otimes I)(H \otimes I) = (H \otimes I) \ CNOT_{2,1} (H \otimes I) = \text{CNOT}_{2,1} \]
SWAP and CNOT

• Define $\text{CNOT}_{1,2} = \text{CNOT}$
  • first bit determines whether to apply $I$ or $X$ on second

• Define $\text{CNOT}_{2,1} = \text{SWAP} \ \text{CNOT}_{1,2} \ \text{SWAP}$
  • second bit determines whether to apply $I$ or $X$ on first

• $(H \otimes H) \ \text{CNOT}_{1,2} \ (H \otimes H) = \text{CNOT}_{2,1}$

• $(H \otimes H) \ \text{CNOT}_{1,2} = \text{CNOT}_{2,1} \ (H \otimes H)$
X and CNOT

• \((I \otimes X) \text{CNOT} (I \otimes X) = \text{CNOT}\)
  • CNOT acts as either I or X on the second qubit
  • \(X \cdot I \cdot X = X^2 = I\)
  • \(X \cdot X \cdot X = X^2 \cdot X = X\)

• \((X \otimes I) \text{CNOT} (X \otimes I) = (I \otimes X) \text{CNOT} = \text{CNOT} (I \otimes X)\)
  • correctly leaves the first bit unchanged
  • but means second bit gets an extra X
    • first bit is \(|0\rangle\), it gets X instead of I
    • first bit is \(|1\rangle\), 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