Introduction to QIS II

James Amundson

2018/2019 Fermilab Academic Lectures

November 15, 2018

Resources

Quantum Computing Resources

- There are many lectures, and even textbooks, freely available on the web
- Scott Aaronson (SA)
  - Computer Scientist at UT Austin, formerly MIT
  - https://www.scottaaronson.com/blog/?p=3943
- John Preskill (JP)
  - Physicist at Caltech, well known in HEP
  - http://www.theory.caltech.edu/people/preskill/ph229/
- Michael A. Nielsen & Isaac L. Chuang (MNIC)
  - Textbook: Quantum Computation and Quantum Information
  - http://csis.pace.edu/ctappert/cs837-18spring/QC-textbook.pdf
- Quantum Simulators
  - Tremendously useful and interesting
  - Many available
  - Adam Lyon will walk you through one of them in the next series of lectures

Calculations with Qubits

Overview

- Representation of a single qubit
- Operations on single qubits
- Operations on two qubits
- Universal gate set
- Classical computation on quantum computers
- Quantum Fourier transform
- No-cloning theorem

Bloch Sphere (MNIC)

- The difference between a classical bit and a qubit is that a qubit can be in a superposition of states

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

- Normalization condition

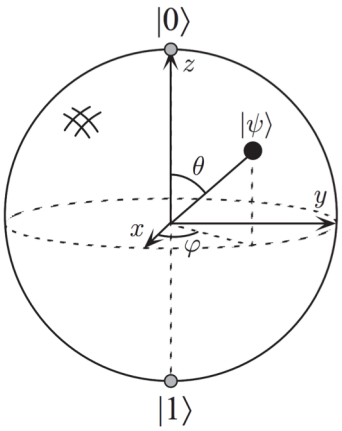
$$|\alpha|^2 + |\beta|^2 = 1.$$

- Without loss of generality

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

- Drop the unobservable phase

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle.$$



A Gate Operation (MNIC)

- Represent our state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ by $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- Define an operator $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- Now we have $X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$
- X is the quantum NOT gate
- Like so many things in life, it all boils down to linear algebra

Fermilab

More Single-Qubit Gate Operations (MNIC)

- Z gate
  - which leaves |0> unchanged, and flips the sign of |1> to give –|1>

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hadamard gate

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

This gate is sometimes described as being like a 'square-root of NOT' gate, in that it turns a $|0\rangle$ into $(|0\rangle + |1\rangle)/\sqrt{2}$ (first column of H), 'halfway' between $|0\rangle$ and $|1\rangle$, and turns $|1\rangle$ into $(|0\rangle - |1\rangle)/\sqrt{2}$ (second column of H), which is also 'halfway' between $|0\rangle$ and $|1\rangle$. Note, however, that H^2 is not a NOT gate, as simple algebra shows that $H^2 = I$, and thus applying H twice to a state does nothing to it.

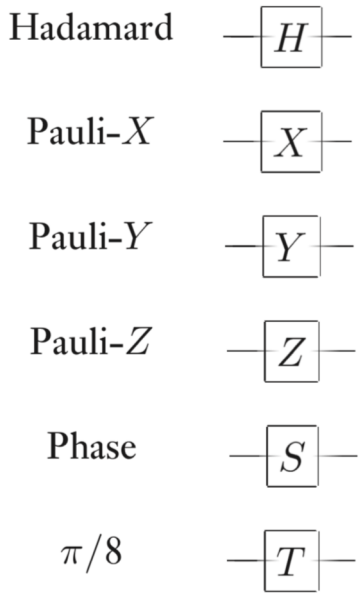
Useful Set of Single-Qubit Gates (MNIC)

- The Pauli matrices

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hadamard, phase and T (pi/8)

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$



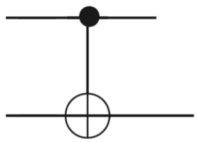
Multi-Qubit Gates (MNIC)

- CNOT
  - A quantum gate with two input qubits, known as the control qubit and target qubit, respectively

$$|c\rangle|t\rangle \longrightarrow |c\rangle|t \oplus c\rangle$$

  - If the control is |1>, the target is flipped. Otherwise, nothing happens.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$



Universal Gate Sets (SA)

- Classical computing
  - {AND, OR, NOT} can calculate an arbitrary classical function
- Quantum computing
  - Any multiple qubit logic gate may be composed from CNOT and single qubit gates
    - {CNOT, H, S}?
      - No! Not universal
      - Any circuit made of these gates can be simulated in polynomial time on a classical computer
    - {CNOT, T, S}?
      - Yes! Universal
      - Many other possibilities

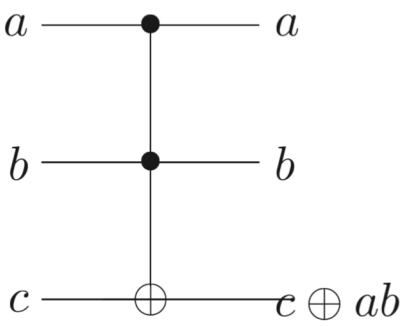
Fermilab

Classical Computing on Quantum Computers

- Classical Boolean gates such as NAND are irreversible
- Single-qubit gates are reversible
- The three-qubit *Toffoli* gate is reversible
  - Two control bits
  - One target bit can be used to simulate NAND

n.b.: basis vector

$$[|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle]$$



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

- Quantum computers can do anything classical computers can do

Quantum Fourier Transform (MNIC)

- Start with the discrete Fourier transform $$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N}$$
- quantum Fourier transform $$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$
- … which is equivalent to $$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$
  - where the amplitudes y_k are the discrete Fourier transform of the x_ks
- The quantum Fourier transform can be rewritten as

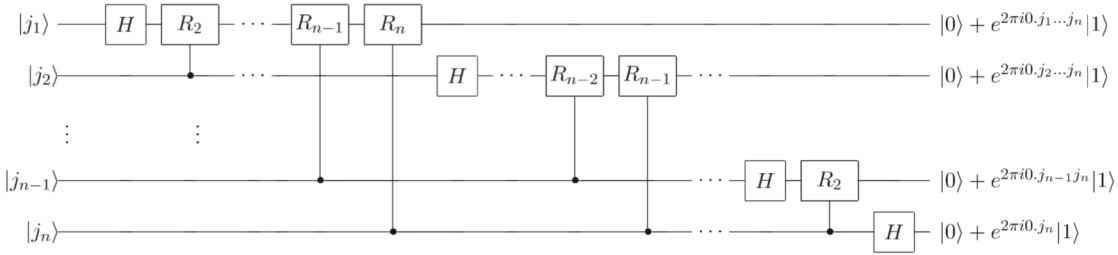
$$|j_1, \ldots, j_n\rangle \rightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

A Quantum Fourier Transform Circuit (MNIC)

- Define a unitary transformation R_k:

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

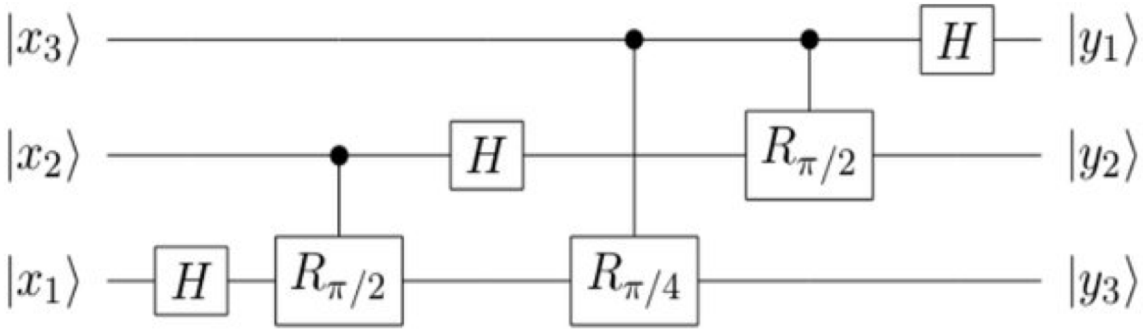
- The following circuit performs the transform

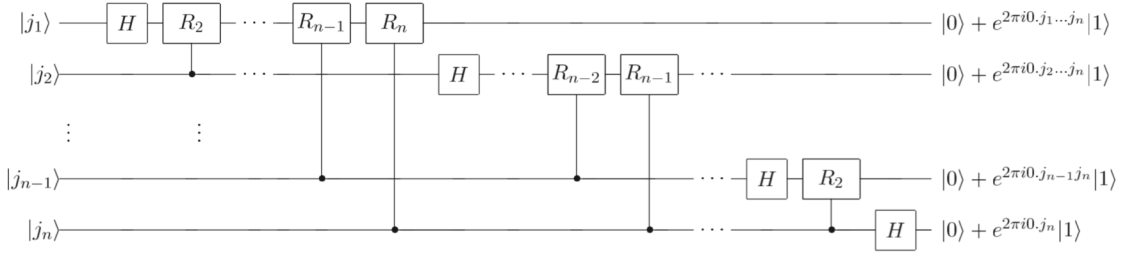


- additional swap operations are required to restore the order of the qubits

Concrete example for three qubits

- Conveniently qubits are upside-down compared to the general figure





What Did We Gain? (MNIC)

- (Discrete) Fourier transform of $N = 2^n$ numbers
  - Classical number of steps

$$N \log(N) = n2^n$$

  - Quantum number of steps

$$\log^2(N) = n^2$$

- Exponential savings

No-cloning Theorem (MNIC)

- Want to copy from $|\psi\rangle$ to $|s\rangle$
- Initial system

$$|\psi\rangle \otimes |s\rangle$$

- Unitary cloning operator U

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

- Now consider a second pure state. $|\varphi\rangle$ and apply U to both

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$
$$U\left(|\varphi\rangle \otimes |s\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle.$$

- Take inner product of two equations

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$$

- States must be either orthogonal or zero. No universal cloning operator can exist.