Lecture 1: Basics of Quantum Computing

Isaac H. Kim

7/14/2022

UC Davis

Background

Quantum computing technologies have been rapidly developing recently.

- Various experimental platforms: Superconducting qubits, Ion traps, Photon, Atoms, Quantum Dot, Topological Qubit, NV Center, ...
- Decent-sized systems: $30 \sim 100$ qubits
  - Beyond 40 qubits, exact classical simulation becomes very difficult.
- There are plans to build $O(100)$ qubit quantum computers and more.

General Motivation

Quantum Computers seem to provide exponential advantage for certain problems.

Examples

- Factoring [Shor (1994)]
- Simulation of physical systems [Feynman (1982)]

Physics Motivation

- Quantum many-body problem becomes classically intractable as we scale the system size.
- Physics deals with simple models, which often makes implementation of quantum simulation algorithms easier (compared to realistic quantum chemical models).
- Physical property of the phase is often robust to small perturbations, so perhaps even a noisy quantum computer can make a useful prediction.
- There is an interest in using quantum computer in a certain subset of researchers in computational condensed matter/lattice QCD researchers.

Physics Application

Rigorous Approaches

- Hamiltonian Simulation $|\psi\rangle \to e^{-iHt}|\psi\rangle$
- Quantum Phase Estimation/Eigenstate Filtering

Pro: Rigorous guarantee

Con: Need a large fault-tolerant quantum computer

Heuristic Approaches

- Variational Quantum Eigensolver
- Quantum Machine Learning

Pro: ~~Near-term friendly~~

Con: Hard to guarantee anything

Prerequisites

- Undergraduate-level quantum mechanics
  - Bra-Ket notation
- Linear algebra

Part 1. Basics of Quantum Information

Hilbert Space and Born Rule

Notation

- $\mathcal{H}_d$: Hilbert space of dimension d.
- $\mathcal{B}(\mathcal{H})$: Space of (bounded) operators acting on Hilbert space $\mathcal{H}$.

Born Rule

For a state $|\psi\rangle$,

$$\Pr[\text{Measure } |x\rangle] = |\langle\psi|x\rangle|^2$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \rightarrow A \otimes B = \begin{pmatrix} \boxed{1 \cdot A} & \boxed{2 \cdot A} \\ \boxed{3 \cdot A} & \boxed{4\, A} \end{pmatrix}$$

$$= \begin{pmatrix} a & b & 2a & 2b \\ c & d & 2c & 2d \\ 3a & 3b & 4a & 4b \\ 3c & 3d & 4c & 4d \end{pmatrix}$$

Composite quantum systems

If we have two spin-$\frac{1}{2}$ particles, what is the Hilbert space that describes their joint state?

$|0\rangle, |1\rangle$

$\mathcal{H}_2 \otimes \mathcal{H}_2 : \mathrm{Span}(\{|\phi\rangle \otimes |\psi\rangle : |\phi\rangle, |\psi\rangle \in \mathcal{H}_2\})$

Product state: $|\phi\rangle \otimes |\psi\rangle$

Entangled state: ex) $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \underline{\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)} = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$

$\alpha\delta = 0 \quad \beta\gamma = 0$

$\alpha = 0 \Rightarrow$

Tensor Product: Operators

$(O\otimes I + I\otimes O')(|\phi\rangle\otimes|\psi\rangle)$

$= |0\rangle\otimes|1\rangle + |0\rangle\otimes|0\rangle$

O, $O\otimes O'$

$O\otimes I + I\otimes O'$

O $\otimes$

L_1 L_2

$L = L_1\otimes I + I\otimes L_2$ vs. $L_1\otimes L_2$

$\neq$

$L_1\otimes L_2$

Composite quantum systems

If we have two spin-$\frac{1}{2}$ particles, how do we express the operators acting on this Hilbert space?

$O\otimes O' \in \mathcal{B}(\mathcal{H}_2\otimes\mathcal{H}_2)$

$O, O' \in \mathcal{B}(\mathcal{H}_2)$

$(O\otimes O')(|\phi\rangle\otimes|\psi\rangle) = O|\phi\rangle\otimes O'|\psi\rangle$

$O = \begin{pmatrix}1&0\\0&2\end{pmatrix}$ $O' = \begin{pmatrix}0&1\\1&0\end{pmatrix}$ $|\phi\rangle = |0\rangle$ $|\psi\rangle = |1\rangle$

$O|\phi\rangle = |0\rangle$ $O'|\psi\rangle = |0\rangle$

$(O\otimes O')(|\phi\rangle\otimes|\psi\rangle) = |0\rangle\otimes|0\rangle = |0\rangle|0\rangle$

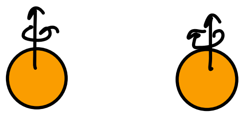
$|\phi\rangle|\psi\rangle|e\rangle = |\phi\rangle\otimes|\psi\rangle\otimes|e\rangle$

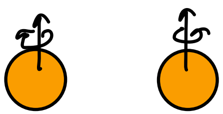
Tensor Product: Basic properties

- Associative: $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- Not commutative in general: $|\phi\rangle \otimes |\psi\rangle \neq |\psi\rangle \otimes |\phi\rangle$
  - If we exchange one spin with another spin, obviously sometimes we will get a different state.

$|0\rangle \otimes |1\rangle$

$|1\rangle \otimes |0\rangle$





Density matrix

A state $|\psi\rangle \in \mathcal{H}$ in the density matrix version:

$$|\psi\rangle\langle\psi|.$$

More generally, a density matrix is a positive semi-definite matrix with unit trace.

Born Rule (Generalization)

$$\Pr[\text{Measure } |x\rangle] = \langle x|\rho|x\rangle$$

$$\rho = |\psi\rangle\langle\psi|$$

$$\rightarrow \Pr[\,|x\rangle\,] = \langle x|\psi\rangle\langle\psi|x\rangle$$

$$= |\langle x|\psi\rangle|^2$$

Density matrix in a tensor product Hilbert space

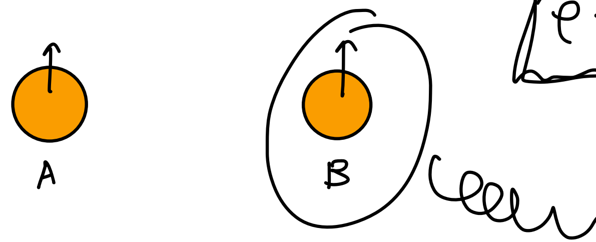
Let the Hilbert space be $\mathcal{H}_A \otimes \mathcal{H}_B$.

- ρ is separable if

$$\rho = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i}.$$

  for some $\{\rho_{A,i}\}$, $\{\rho_{B,i}\}$ and a probability ditsribution $\{p_i\}$.
- ρ is entangled otherwise.

Partial trace



$\rho = |\psi\rangle\langle\psi|$

Let ρ be a density matrix acting on $\mathcal{H}_A \otimes \mathcal{H}_B$.

$$\mathrm{Tr}_B(\rho) = \sum_i (I_A \otimes \langle i|)\rho(I_A \otimes |i\rangle),$$

where $\{|i\rangle\}$ is an orthonormal basis set for $\mathcal{H}_B$.

$|i'\rangle$ $\quad \sum_{i'} (I_A \otimes \langle i'|)\, \rho\, (I_A \otimes |i'\rangle)$

$= \mathrm{Tr}_B\left(\sum_{i'} (I_A \otimes |i'\rangle\langle i'|)\, \rho \right)$

$= \mathrm{Tr}_B(\rho)$

$\sum_{i'} |i'\rangle\langle i'| = I_B$

Measurement

Let $\{|i\rangle\}$ be an orthonormal basis set for $\mathcal{H}$. When we measure a state $|\psi\rangle \in \mathcal{H}$, what happens?

Obtain $|i\rangle$ with Probability $|\langle\psi|i\rangle|^2$ (Born Rule)

Partial Measurement

Let $\{|i\rangle\}$ be an orthonormal basis set for $\mathcal{H}_A$ and let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. When we measure a state $|\psi\rangle$, what happens?

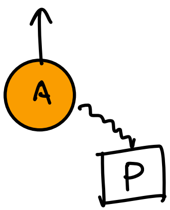
We can model the measurement as a unitary process involving a "probe." Let $|\psi\rangle = \sum_i \alpha_i |i\rangle$

$$\left(\sum_i \alpha_i |i\rangle_A\right) \otimes |0\rangle_P \to \sum_i \alpha_i |i\rangle_A \otimes |i\rangle_P$$

$\text{Prob}[\text{Probe} = i] = |\alpha_i|^2 = \| \alpha_i |i\rangle \|^2$

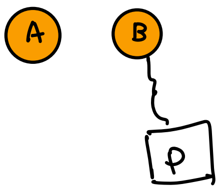
post-measurement state $= |i\rangle$

$\| |\phi\rangle \| = \sqrt{\langle\phi|\phi\rangle}$



Partial Measurement Process

We can model the measurement as a unitary process involving a "probe." Now let's think about the partial measurement process.



$$\left(\sum_{i,j} \alpha_{ij} |i\rangle_A \otimes |j\rangle_B\right) \otimes |0\rangle_P \longrightarrow \sum_{i,j} \alpha_{ij} |i\rangle_A \otimes |j\rangle_B \otimes |j\rangle_P$$

$$\text{Prob}[\text{Probe} = |j\rangle] = \left\| \sum_i \alpha_{ij} |i\rangle_A |j\rangle_B \right\|^2$$

$$\text{post-measurement state} = \left(\sum_i \alpha_{ij} |i\rangle_A\right) \otimes |j\rangle_B$$

$$(I \otimes \langle j|)\left(\sum_{i,j'} \alpha_{ij'} |i\rangle_A |j'\rangle_B\right)$$

$$\text{Prob}[B = |j\rangle] = \left\| (I_A \otimes \langle j|_B) |\psi\rangle_{AB} \right\|^2$$

post-measurement state
- A: $(I_A \otimes \langle j|_B) |\psi\rangle_{AB}$,
- B: $|j\rangle_B$

Partial Measurement

Let $\{|i\rangle\}$ be an orthonormal basis set for $\mathcal{H}_A$ and let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. When we measure a state $|\psi\rangle$, what happens?

- Probability of measuring $|i\rangle$: $\mathrm{Tr}_A((I_A \otimes \langle i|)\rho(I_A \otimes |i\rangle))$.
- Post-measurement state: Normalized version of $(I_A \otimes \langle i|)\rho(I_A \otimes |i\rangle)$.

Part 2. Basic Concepts in Quantum Computing

Qubit and Qubits

- Qubit: $\mathcal{H}_2$
- Qubits: $\underbrace{\mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_2}_{n}$

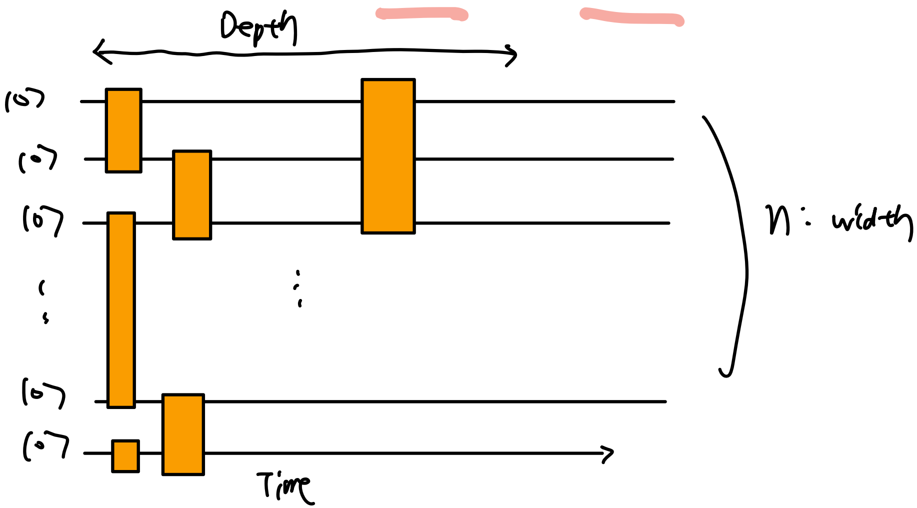
$\dim(\mathcal{H}) = 2^n$

Gates

- A gate often means a unitary acting on a few ($\approx 1, 2, 3$) qubits.
- Some people call measurement as gates. In this lecture, we will simply refer to those as measurements. Gates will be assumed to be unitary.

Circuits

- A circuit is a sequence of unitary gates.
- Useful concepts: Depth and Width



What is Quantum Computation?

- Gate-based model
- Quantum Turing Machine [Duetsch (1974)]
- Adiabatic model [Farhi, Goldstone, Guttman, Sipser (2000)]

Part 3. Some computer science concepts

Efficient and Inefficient

Computer scientists are interested in algorithms. When it comes down to assessing whether an algorithm is "efficient" or not, the absolute time does not matter. What matters is the **scaling**.

ex)

- An algorithm that takes $2^{10^{-\mathbf{100}}n}$ seconds would not be "efficient."
- An algorithm that takes $10^{10^{\mathbf{100}}}n$ seconds would ~~not~~ be efficient.

Complexity

- Gate complexity: Number of few-qubit (or few-bit) gates needed to solve a problem.
- Query complexity: Number of invocations to some "black box."

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

Guiding Example

Complexity of $e^{i \sum_{n=1}^{N} Z_n Z_{n+1}}$? $= \prod_{n=1}^{N} \boxed{e^{i Z_n Z_{n+1}}}$

$\boxed{e^{i Z_n Z_{n+1}}}$ Gate complexity $\sim N$

x, y

$x, y \to \mathrm{ADD}(x, y)$

$x \cdot y$

n-bit

```
    11101
  x 11001
  -------
    11101
   00000
  00000
 11101
11101
-------
```

n

$n-1$ additions $\to$ # of queries to the addition is $n-1$

- $\mathcal{O}(f(n))$: "Upper bounded"
- $\Omega(f(n))$: "Lower bounded"
- $\Theta(f(n))$: "On the order of"
- $o(f(n))$: "Subleading"

$O(n)$ for physicists $\approx cn$

$$2.5n^3 + o(n^3)$$

$$g(n) = 2.5n^3 + 5n^2 + 3n + 1$$

$$g(n) = O(n^3)$$

$$g(n) = \Omega(n^3)$$

$$g(n) = \Theta(n^3)$$

O for physicists

Classical vs. Quantum Computation

- Classical computation can be decomposed into a sequence of classical gates, e.g., NOT, AND, XOR, NAND, ...
- Quantum computation can be decomposed into a sequence of quantum gates.

Remarkably, there are problems which are "easy" for quantum computers that seem to be "hard" for classical computers.

Part 4. Classical vs. Quantum Computation

Unitarity Constraint

One of the basic units of classical computation is AND gate. Let's think about whether this gate is unitary.

$$\mathrm{AND}(\underbrace{x, y}_{2\times 2 = 4}) = 0, 1$$

Reversible Computation

How can we implement AND gate unitarily?

Classical vs. Quantum Computation

The class of problems that can be solved efficiently classically is a subset of the problems that can be solved efficiently quantumly.

Exponential Speedups

There appears to be a problem that can be solved efficiently on a quantum computer which cannot be solved efficiently on a classical computer.

[Shor (1994), Feynman (1982)]

Some comments

While this is beyond the scope of this lecture series, I should note that quantum computers probably cannot efficiently solve NP-hard problems, e.g., finding ground states of a spin glass. One generally shouldn't expect to be able to get an exponential speedup to search problems unless there is a special structure to the problem one can exploit.

Without much structure, one often only get a quadratic speedup.

- Database search [Grover (1996)]
- Amplitude amplification/estimation [Brassard (2002)]
- Speedup for Monte Carlo

Recap

1. Basics of Quantum Information
2. Basics in Quantum Computation
3. Computer Science Concepts
4. Classical vs. Quantum Computation

Next lecture: Basic facts about quantum circuits

Questions?