Week 1 : Introduction to Quantum Computing Theory

Category	
Created	@August 5, 2022 4:37 PM
Status	Archived
Updated	@August 5, 2022 8:48 PM

Quantum Computation

> Topics covered : Density Operator, Quantum Operations, Quantum Algorithms, Quantum Entanglement, Quantum Circuits etc. Will also cover Quantum Error Correction in part 2 of this course.

Quantum Information Science = Quantum Theory + Computer Science + Information Theory

There are many brnaches of Quantum Information Science, like:

1. Quantum Sensing - Improving sensitivity and spatial resolution
2. Quantum Cryptography - Privacy founded on fundamental laws of quantum physics
3. Quantum Networking - Distributing quantumness around the world.
4. Quantum Simulation - Probes of exotic quantum many body phenomena
5. Quantum Computinng - Speeding up solutions to hard problems
6. Quantum Information Concepts - Entanglement, error correction, complexity

There are two fundamental ideas that outline quantum computing:

- Quantum Complexity

  Why we think quantum computing is powerful

- Quantum Error Correction

  Why we think quantum computing is scalable.

Quantum Entanglement

Classical Book and Quantum Book example

> The information does not reside in the pages. It is in the correlation between the pages. You can't access the information if you read the book one page at a time.

A complete description of a typical quantum state of just 300 qubits require more bits than the number of atoms in the visible universe.

Why we think quantum computing is powerful?

1. Problems believed to be hard classically , which are easy for quantum computers. Factoring is the best known example.
2. Complexity theory argument indicating that quantum computers are hard to simulate classically.

3. We don’t know how to simulate a quantum computer efficiently using a digital computer. The cost of the best known simulation algorithm rises exponentially with the number of qubits.

> The Power of quantum computing is limited. For example, we don’t believe that quantum computers can efficiently solve worst-case instances of NP-hard optimization problems.

The Theory of Everything?

The theory of everything is not even remotely a theory of every thing..

We know this equation is correct. .. However , it cannot be solved accurately when the number of particles exceed about 10. No computer exisiting or that will ever exist, can break this barrier because it is a catastrophe of dimension.

We have succeeded in reducing all of ordinary physical behavior to simple , correct Theory of Everything only to discover that it has revealed exactly nothing about many things of great importance.

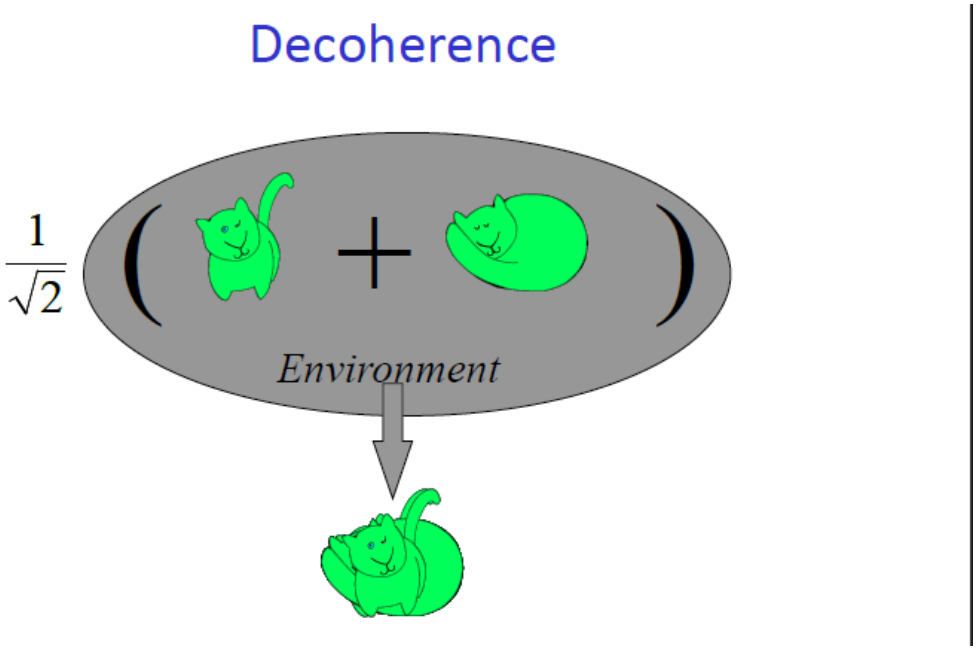
~ R.B Laughlin and D.Pines, PNAS 2000.

> Nature isn’t classical , dammit, and if you want to make simulation of Nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem because it doesn’t look so easy. ~ Richard P. Feynman (1981)

Why quantum computing is hard?

- We want qubits to interact strongly with one another.
- We don’t want qubits to interact with the environment
- Except when we control or measure them.

Decoherence



Decoherence explains why quantum phenomena, though observable in the microscopic systems studied in the physics lab, are not manifest in the macroscopic physical systems that we encounter in our ordinary experience.

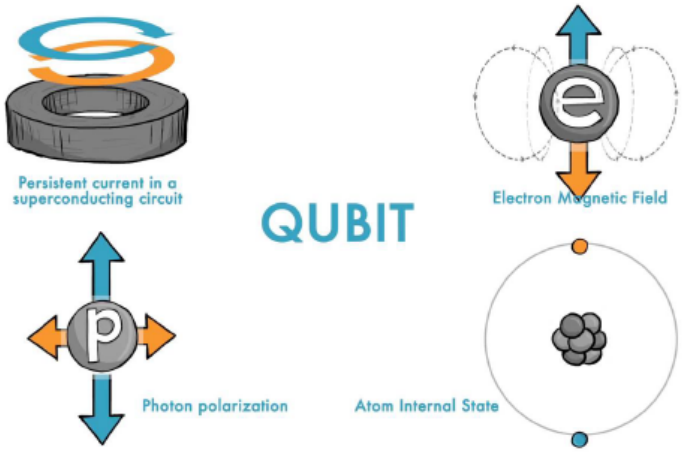
How can we protect a quantum computer from decoherence and other sources of error?

To resist decoherence we must prevent the environment from “learning” about the state of quantum computer during the computation.

Quantum Error Correction

The protected “logical” quantum information is encoded in a highly entangled state of many physical qubits.

The environment can’t access this information if it interacts locally with the protected system.



New materials are being explored to make quantum hardware, that have intrinsic resistance to decoherence.

Classical systems cannot simulate quantum systems efficiently (a widely believed but unproven conjecture)

About Sycamore

Quantum David vs. Classical Goliath

A fully programmable circuit-based quantum computer, $n = 53$ working qubits in a two-dimensional array with coupling of nearest neighbors.

A circuit with 20 layers of 2-qubits gates can be *executed a million of times in a few minutes* , yielding verifiable results.

Simulating this quantum circuit using a classical supercomputer is hard. It would take at least days ,possibly much longer.

Furthermore, the cost of the classical simulation grows exponentially with the number of qubits.

Conclusion: the hardware is working well enough to produce meaningful results in a regime where classical simulation is very difficult.

What quantum computational supermacy means?

- It's a programmable circuit-based quantum computer.
- An impressive achievement in experimental physics and a testament to ongoing progress in building quantum computing hardware.

- We have arguably entered the regime where the extravagant exponential resources of the quantum world can be validated.
- This confirmation does not surprise (most) physicists, but it's a milestone for technology on planet earth.
- Building a quantum computer is merely really, really hard, not ridiculously hard. The hardware is working; we can begin a serious search for usefull applications.
- But the specific task performed by Sycamore to demonstrate quantum computational supermacy is not particularly useful.

Quantum computing in the NISQ era

The noisy $50 - 100$ qubit quantum computer has arrived.

(NISQ = noisy intermediate-scale quantum)

NISQ devices cannot be simulated by brute force using the most powerful currently existing supercomputers.

Noise limits the computational power of NISQ-era technology

NISQ will be an interesting tool for explorinng physics. It might also have other useful applications.

NISQ will not change the world by itself, rather it is a step toward more powerful quantum technologies of the future.

Potentially transformative scalable quantum computers may still be decades away. We're not sure how long it will take.

Hybrid quantum/classical optimizers

We don’t expect a quantum computer to solve worst case instances of NP-hard problems, but it might find better approximate solutions, or find them faster.

Classical optimization algorithms are sophisticated and well-honed after decades of hard work.

We don’t know whether NISQ devices can do better, but we can try it and see how well it works.

The era of quantum heuristics

> Peter Shor: “You don’t need them [testbeds] to be big enough to solve useful problems, just big enough to tell whether you can solve useful problems”

Sometimes algorithms are effective in practice even though theorists are not able to validate their performance in advance.

Example: Deep learning. Mostly tinkering so far, without much theory input

Possible quantum examples:

Quantum annealers, approximate optimizers, variational eigensolvers, quantum machine learning…playing around may give us new ideas.

What can we do with , say < 100 qubits, depth < 100? We need a dialog between quantum algorithm experts and application users.

The steep climb to scalability

NISQ-era quantum devices will not be protected by quantum error correction. Noise will limit the scale of computations that can be executed accurately.

Quantum error correction (QEC) will be essential for solving some hard problems. But QEC carries a high overhead cost in number of qubits & gates.

This cost depends on both the hardware quality and algorithm complexity. With today's hardware, solving (say) useful chemistry problems may require hundreds to thousands of physical qubits for each protected logical qubit.

Recent estimate: 20 million physical qubits to break RSA 2048 (Gidney, Ekerå2019), for gate error rate 10^{-3}.

To reach scalability, we must cross the daunting "quantum chasm" from hundreds to millions of physical qubits. This may take a while.

Advances in quantum gate fidelity, systems engineering, algorithm design, and error correction protocols can hasten the arrival of the fully fault-tolerant quantum computer.

"Quantum computing is a marathon not a sprint"

Chris Monroe (UMD/IonQ)

Quantum speedups in the NISQ era and beyond

Quantum computational supremacy demonstrations confirm the extravagant computation resources provided by the quantum world.

In the NISQ era we can explore heuristic quantum algorithms. Near-term quantum advantage for useful applications is possible, but not guaranteed.

For truly scalable quantum computing, quantum error correction will be required. But QEC has a dauntingly high overhead cost, and will not be feasible in the near term.

Lower quantum gate error rates will lower the overhead cost of quantum error

correction, and also extend the reach of quantum algorithms which do not use error correction.

NISQ will not change the world by itself. Realistically, the goal for near-term quantum platforms should be to pave the way for bigger payoffs using future devices. Progress toward fault-tolerant QC must continue to be a high priority for quantum technologists.

Quantum Information vs. Classical Information

1. Randomness - Clicks in a Geiger counter are intrinsically random, not pseudorandom. Can't predict outcome even with the most complete possible knowledge of the state.
2. Uncertainty - Operators A and B do not commute means that measuring A influences the outcome of a subsequent measurement of B.
3. Entanglement - The whole is more definite than the parts.Even if we have the complete possible knowledge of the (pure) state of joint system AB, the (mixed) state of A may be highly uncertain.

Qubit

A vector (actually a "ray" because the normalization is 1 by convention, and the overall phase does not matter) in a two dimensional complex Hilbert space.

$$|\psi\rangle = a|0\rangle + b|1\rangle, \;\; a, b \in C, \; |a|^2 + |b|^2 = 1, \; |\psi\rangle \approx e^{\iota\alpha}|\psi\rangle$$

"Classical" in the special case where $|0\rangle$ or $|1\rangle$ is "promised".

The two orthogonal states $|0\rangle$ and $|1\rangle$ are perfectly distinguishable. If Alice sends one or the other to Bob, he can measure in the $\{|0\rangle, |1\rangle\}$ basis and identify the state.

The orthogonal states

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

are also perfectly distinguishable.

Suppose Alice sends either $|1\rangle$ or $|+\rangle$ to Bob.

Now Bob cannot distinguish the states perfectly. His best measurement, which succeeds with probability $\cos^2(\pi/8) \approx 0.853$ if the two states are equally likely, projects onto the orthogonal basis shown. (Prove it! Generalize it!) Alternative: a measurement which is sometimes inconclusive, but identifies the state correctly when conclusive.

Information vs Disturbance

Suppose Alice prepares either |ϕ⟩ or |ψ⟩. To distinguish the two possible states, Eve performs a unitary transformation that rotates her probe while leaving Alice's state intact.

$$\begin{aligned} U : |\varphi\rangle_A \otimes |0\rangle_E &\to |\varphi\rangle_A \otimes |e\rangle_E \\ |\psi\rangle_A \otimes |0\rangle_E &\to |\psi\rangle_A \otimes |f\rangle_E \end{aligned}$$

where $|e\rangle$ and $|f\rangle$ are normalized states. Since U preseves inner products.

$$\langle\psi|\varphi\rangle \cdot \langle f|e\rangle = \langle\psi|\varphi\rangle$$

and if $|\varphi\rangle$ and $|\psi\rangle$ are nonorthogonal, then $\langle f|e\rangle = 1$; the states of the probe are the same. Eve's measurement of the probe cannot reveal any information about whether the state is |ϕ⟩ or |ψ⟩ . On the other handif |ϕ⟩ and |ψ⟩ are orthogonal, the probe states can also be orthogonal. Eve can copy the info.

Tensor Product

System divided into two subsystems

$\{|i\rangle_A,\ i = 1, 2, ..., d_A\}$ and $\{|a\rangle_B,\ i = 1, 2, ..., d_B\}$

Basis states of the composite system are distinguishable if they can be distinquishedon either Alice's or Bob's side:

$$(\langle j| \otimes \langle b|)(|i\rangle \otimes a\rangle) = \delta_{ij}\delta_{ab}$$

If Alcie and Bob both have qubits, the basis states

$$\{|00\rangle, |01\rangle.|10\rangle.|11\rangle\}$$

are all distinguishable.

Many Qubits

$$\mathbb{C}^{2n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes .....\mathbb{C}^2$$

spanned by …

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes |x_{n-3}\rangle \otimes .....|x_1\rangle \otimes |x_0\rangle\otimes,\ \ x \in \{0, 1\}^n$$

where $\langle x|y\rangle = \delta_{x,y}$

For 300 qubits, vector in a space with dimension $2^{300} \approx 10^{90}$, more than the the number of atoms in the visible universe. No succinct classical description of the quantum state, in general.

Quantum Computer : the circuit model

1. Hilbert space of n qubits :

   Spanned by:

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes |x_{n-3}\rangle \otimes .....|x_1\rangle \otimes |x_0\rangle \otimes, \quad x \in \{0,1\}^n$$

> 💡 Important: The Hilbert space is equipped with a natural tensor-product decomposition into subsystems.

$$\mathbb{C}^{2n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes .....\mathbb{C}^2$$

Physically, this decomposition arises from spatial locality. Elementary operations (“quantum gates”) that act on a small number of qubits(independent of n)are “easy;” operations that act on many qubits(increasing with n) are “hard.”

2. Initial State:

$$|000....0000\rangle = |0\rangle^{\otimes n}$$

3. A finite set of fundamental quantum gates:

$$\{U_1, U_2, U_3, ..., U_{n_G}\}$$

Each gate is a unitary transformation acting on a bounded number of qubits. The gates form a universal set: arbitrary unitary transformations can be constructed, to any specified accuracy, as a quantum circuit constructed from the gates:

> 💡 Important: One universal set of gates can simulate another efficiently, so there is a notion of complexity that is independent of the details of the quantum hardware.

4. Classical Control:

The construction of a quantum circuit is directed by a classical computer, i.e.,a Turing machine. (We're not interested in what a quantum circuit can do unless the circuit can be designed efficiently by a classical machine.)

5. Readout:

At the end of the quantum computation, we read out the result by measuring σ_z i.e., projecting onto the basis $\{|0\rangle, |1\rangle\}$
(We don't want to hide computational power in the ability to perform difficult measurements.)

Clearly, the model can be simulated by a classical computer with access to a random number generator.

But there is an exponential slowdown, since the simulation involves matrices of exponential size $2^n \times 2^n$

The quantum computer might solve efficiently some problems that can't be solved efficiently by a classical computer.

("Efficiently" means that the number of quantum gates = polynomial of the number of bits of input to the problem.)

Is this "circuit model" sufficiently powerful to simulate efficientlyany physical process that occurs in Nature (the "strong quantum Church-Turing thesis")? Some challenges are:

--Local quantum field theory (standard model of particle physics). Field modes of arbitrarily small wavelength, hence an infinite number of degrees of freedom per unit volume. Need to include energy as well as time and space in resource accounting.

--Quantum gravity. May be described by local quantum field theory or (large) matrix quantum mechanics. But subtle resource accounting because short distance in the bulk spacetimecorresponds to long distance in the dual boundary field theory.

Three Crucial Lessons

1. Quantum Computers can solve hard problems
2. Quantum Errors can be controlled

3. Quantum hardware can be constructed

Lots of questions

What problems can be solved efficiently with quantum computers?
What problems cannot be?

Can we build a “quantum Internet” and how would be use it?

Can we construct much more reliable quantum hardware than we have now?

How can quantum information concepts illuminate issues of fundamental interest in the physical science?