

# Session 1: An overview of quantum computing

## Organizers



Aritra Bose, PhD  
IBM Research



Filippo Utro, PhD  
IBM Research



Laxmi Parida, PhD  
IBM Research

# Learning outcomes of Session 1

---

- Learning about the history of quantum computing
- Understanding different technologies for building quantum computers
- The difference between classical computing and quantum computing
- A clear understanding of the fundamental concepts in quantum computing such as qubits, quantum gates and circuits, and measurement
- Distinguishing different complexity classes and where quantum can make a difference
- Exploration of different application of quantum computing
- Learning about the near-term and fault-tolerant quantum hardware developments
- Setting up a local environment to use Qiskit 1.0
- Learning the implementation of quantum gates, observables and primitives in Qiskit
- Understanding the transpilation of a circuit on a real quantum backend

# A brief history of quantum computing

---

- Quantum computing is the field of computation where we investigate the computational power and other properties of computation based on quantum mechanics
- These fundamental principles of quantum mechanics such as superposition, entanglement and interference are the main building blocks for the quantum computational theory
- The main ideas that built a foundation for quantum computing can be traced back to early 20<sup>th</sup> century (Planck, Bohr, Heisenberg, Schrodinger etc.)
- Starting in 1960s, there were some theoretical results, as well as earlier quantum algorithms (Simon's, Deutsch-Jozsa, Bernstein-Vazirani)

# A brief history of quantum computing

2/24/70/11 Quantum Information Theory False  
Conversation w/ Steve Wiesner, who told me that:  
A variation on the Einstein-Rosen-Podolsky Gedankenexperiment can be used to send, through a channel with a nominal capacity of one bit, two bits of information; subject however to the constraint that ~~the receiver may choose at his choice to read either~~ whichever bit the receiver chooses to read, ~~the~~ the other bit is destroyed.

First usage of the word Quantum Information Theory in Bennett's notebook

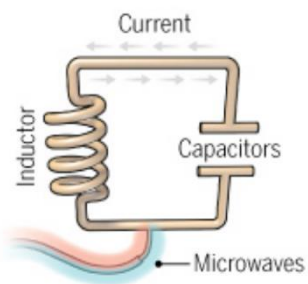


IBM – MIT Conference on the Physics of Computation, 1981

- One big breakthrough was Shor's algorithm in 1994 about prime decomposition for RSA cryptography
- Since then, quantum computing has become a very impactful area at the intersection of physics, computer science, mathematics, chemistry and many other disciplines!

# What does a quantum computer look like?

## Superconducting loops



A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into super-position states.

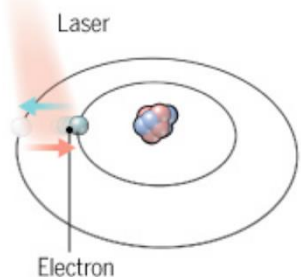
**Longevity (seconds)** 0.00005  
**Logic success rate** 99.4%  
**Number entangled** 9

### Company support

Google, IBM, Quantum Circuits

- + Pros**  
Fast working. Build on existing semiconductor industry.
- Cons**  
Collapse easily and must be kept cold.

## Trapped ions



Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in super-position states.

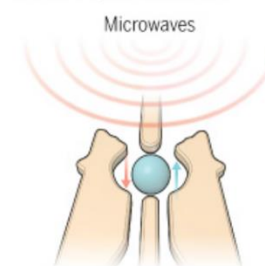
**Longevity (seconds)** >1000  
**Logic success rate** 99.9%  
**Number entangled** 14

### Company support

ionQ

- + Pros**  
Very stable. Highest achieved gate fidelities.
- Cons**  
Slow operation. Many lasers are needed.

## Silicon quantum dots



These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.

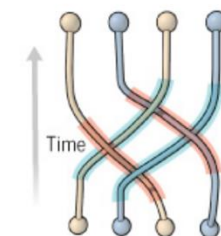
**Longevity (seconds)** 0.03  
**Logic success rate** ~99%  
**Number entangled** 2

### Company support

Intel

- + Pros**  
Stable. Build on existing semiconductor industry.
- Cons**  
Only a few entangled. Must be kept cold.

## Topological qubits



Quasiparticles can be seen in the behavior of electrons channeled through semiconductor structures. Their braided paths can encode quantum information.

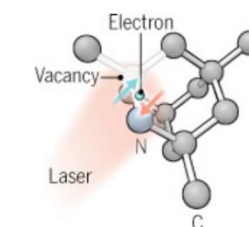
**Longevity (seconds)** N/A  
**Logic success rate** N/A  
**Number entangled** N/A

### Company support

Microsoft, Bell Labs

- + Pros**  
Greatly reduce errors.
- Cons**  
Existence not yet confirmed.

## Diamond vacancies



A nitrogen atom and a vacancy add an electron to a diamond lattice. Its quantum spin state, along with those of nearby carbon nuclei, can be controlled with light.

**Longevity (seconds)** 10  
**Logic success rate** 99.2%  
**Number entangled** 6

### Company support

Quantum Diamond Technologies

- + Pros**  
Can operate at room temperature.
- Cons**  
Difficult to entangle.

Image source: <https://www.science.org/content/article/scientists-are-close-building-quantum-computer-can-beat-conventional-one>, Dec 2016

# Superconducting qubits



IBM Quantum chip, 2021 (IBM Official)



IBM Quantum Computer, golden chandelier design

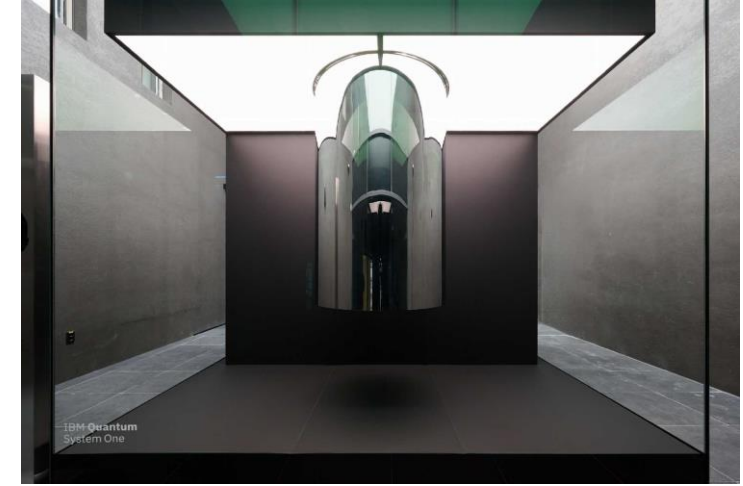
# One of the largest quantum computers in the world



Cleveland Clinic, Cleveland, OH



RPI, Troy, NY



Yonsei University, Seoul, South Korea



RIKEN, Wako, Japan

# Classical computing

CLASSICAL  
COMPUTING

## INPUT

- Numerical values
- Vectors/matrices
- Graphs
- Images
- Text
- ...

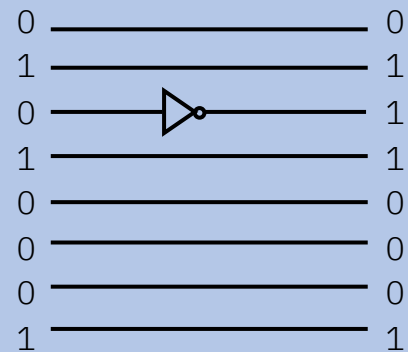
“Quantum”



01010001  
01110101  
01100001  
01101110  
01110100  
01110101  
01101101

## COMPUTATION

- Basic arithmetic
- Linear/matrix algebra
- Regression
- Statistical analysis
- Machine learning
- ...



## OUTPUT

Solution to the computational task

01110001  
01010101  
01000001  
01001110  
01010100  
01010101  
01001101



“Quantum”

# From bits to quantum bits (qubits)

- Qubits and in general quantum computations take place in a Hilbert space, that is a complete inner product space (a complex vector space)
- Qubits can be in the superposition of 0 and 1 states.

For basis states  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  and  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ , we can have

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle \text{ where } |\alpha_0|^2 + |\alpha_1|^2 = 1$$

- Polarized sunglasses is a good analogy for a quantum system where qubits are polarized photons. Say horizontal polarization is the qubit  $|0\rangle$  and vertical polarization  $|1\rangle$ .

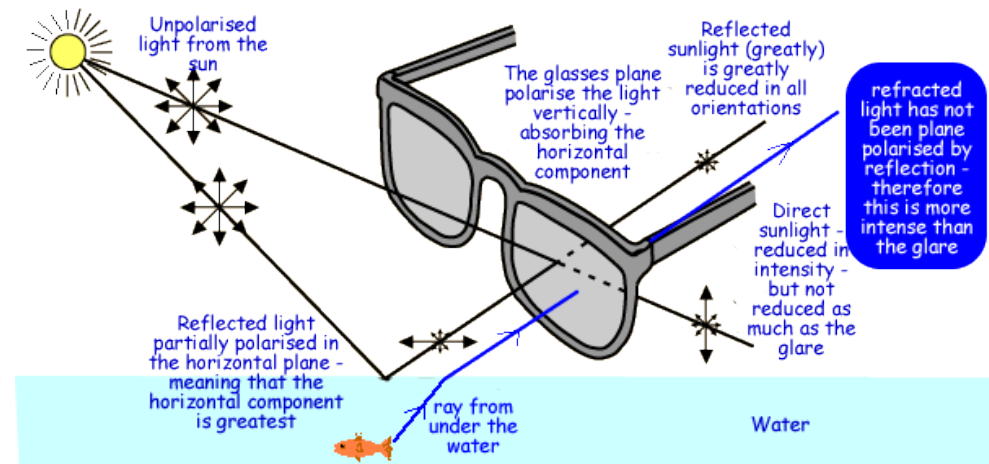


Image source: [https://www.cyberphysics.co.uk/topics/light/polarised\\_spex.htm](https://www.cyberphysics.co.uk/topics/light/polarised_spex.htm)

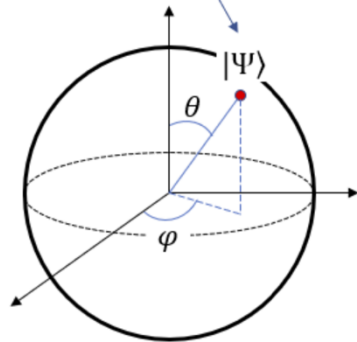
# Visual representation of qubits

- A convenient way to picture these quantum states (single qubits) is Bloch sphere.

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

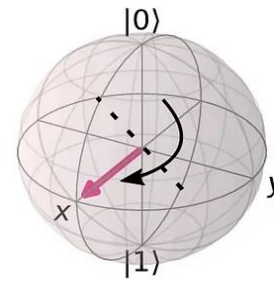
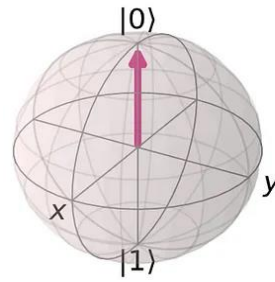
The absolute value (magnitude) of this term is always 1 regardless of the value  $\varphi$ .  
(i.e., the magnitude of  $\alpha$  and  $\beta$  is determined by  $\theta$  only)

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

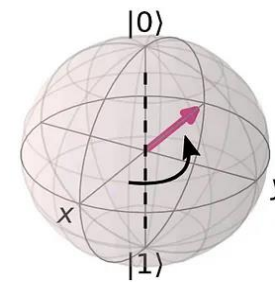


$$0 \leq \theta \leq \pi$$

$$0 \leq \varphi \leq 2\pi$$



$|+\rangle$



$|-\rangle$

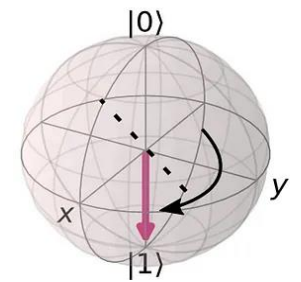


Image source: [https://www.sharetechnote.com/html/QC/QuantumComputing\\_BlochSphere.html](https://www.sharetechnote.com/html/QC/QuantumComputing_BlochSphere.html)

# Classical Bits

A single set of  $N$  bits can be in any one of  $2^N$  possible states.

$N = 4$  possible states

(0000), (0001), (0010), (0011)...

...(1100), (1101), (1110), (1111)

# Quantum Qubits

A single set of  $N$  qubits can be in a superposition of ALL  $2^N$  possible states, simultaneously.

$$|\psi\rangle = c_0 |0001\rangle + c_1 |0001\rangle + \dots$$

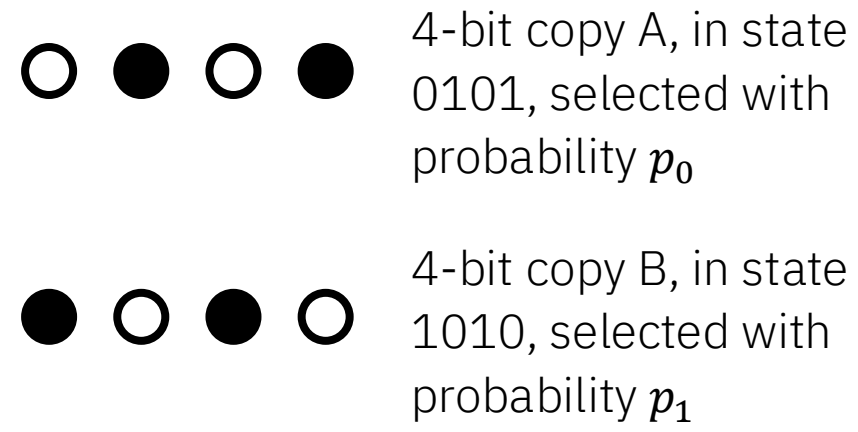
$$+ c_{14} |1110\rangle + c_{15} |1111\rangle \quad c_i \in \mathbb{C}$$

# Classical Entanglement

Correlations exist in classical systems. You can prepare a state like this classically, but

$$s = p_0(0101) + p_1(1010)$$

- (a) Using a copy of resources
- (b) Measurement of bit 0 doesn't affect bit 2, it reveals which copy you have



# Quantum Entanglement

Qubits can be entangled, with different entanglements in different superpositions on a single set of qubits:

If you measure  $q_0$  to be in  $|0\rangle$ , you know  $q_2$  is also in  $|0\rangle$ .

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0101\rangle + |1010\rangle)$$

Here, we use “littleendian” ordering:

$$|q_3q_2q_1q_0\rangle$$

# Operating on qubits

---

- Since we model qubits as complex vectors in Hilbert space, we operate on a quantum state with linear transformations, hence matrices!
- In this case, the matrices must be *unitary matrices*, that is  $U^\dagger U = I$ . So, potentially all the elements of  $SU(n)$ .
- For single qubits, we have very commonly used matrices called Pauli matrices.

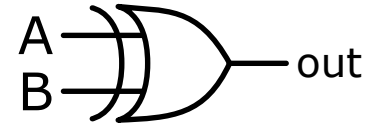
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- We have larger unitary matrices for multi-qubit operations (4x4 for 2-qubits etc.)
- Now, we can think about these as quantum gates and build quantum circuits

# Classical Gates

Classical gates may or may not be unitary

XOR<sup>1</sup>



A	B	A XOR B
0	0	0
1	0	1
0	1	1
1	1	0

<sup>1</sup>Source: Wikipedia Commons

# Quantum Unitary Gates

Quantum gates are unitary.

CNOT



$$|x\rangle|y\rangle \rightarrow |x, x \oplus y\rangle$$

Reversible!

x	y	output
$ 0\rangle$	$ 0\rangle$	$ 00\rangle$
$ 1\rangle$	$ 0\rangle$	$ 11\rangle$
$ 0\rangle$	$ 1\rangle$	$ 01\rangle$
$ 1\rangle$	$ 1\rangle$	$ 10\rangle$

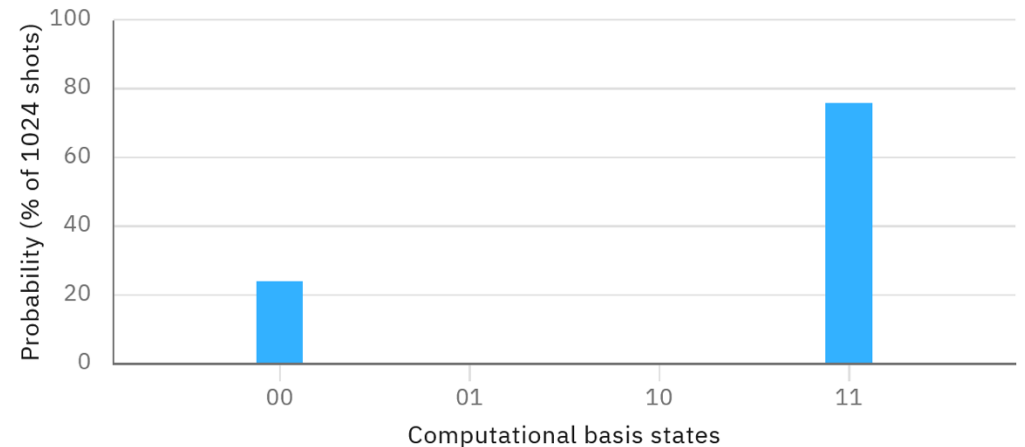
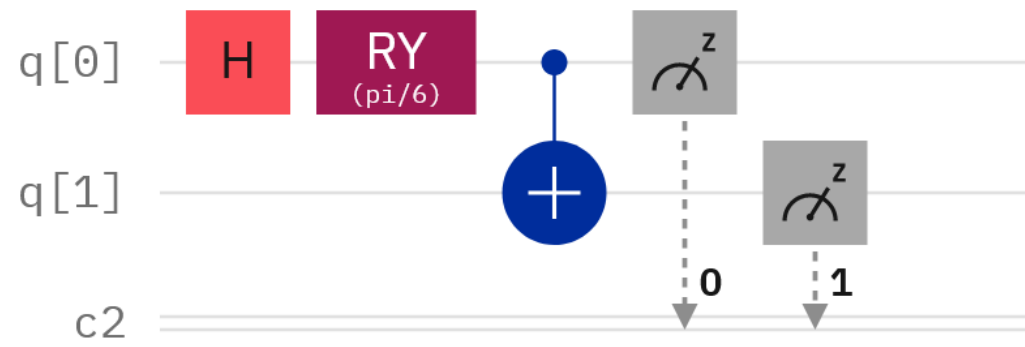
# Measurement

Measuring the state of a qubit, even one in superposition, yields a  $|0\rangle$  or a  $|1\rangle$ .

The probability of measuring these states is related to the coefficients in the state vector.

The probabilities to the right are measured in the absence of noise.

$$CNOT_{0,1}R_{y,0}\left(\frac{\pi}{6}\right)H_0|\psi\rangle \approx 0.50|0\rangle|0\rangle + 0.866|1\rangle|1\rangle$$



H, above and in the diagram, is the Hadamard gate, not to be confused with the Hamiltonian.

# Unitaries

---

Time evolution in quantum is described by the Schrödinger equation.

This means unitary matrices, which leads to unitary gates.

It also gives us complex coefficients.

Schrödinger equation:

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H|\psi(t)\rangle$$
$$\rightarrow |\psi(t)\rangle = \underbrace{e^{-iHt}} |\psi(t=0)\rangle$$

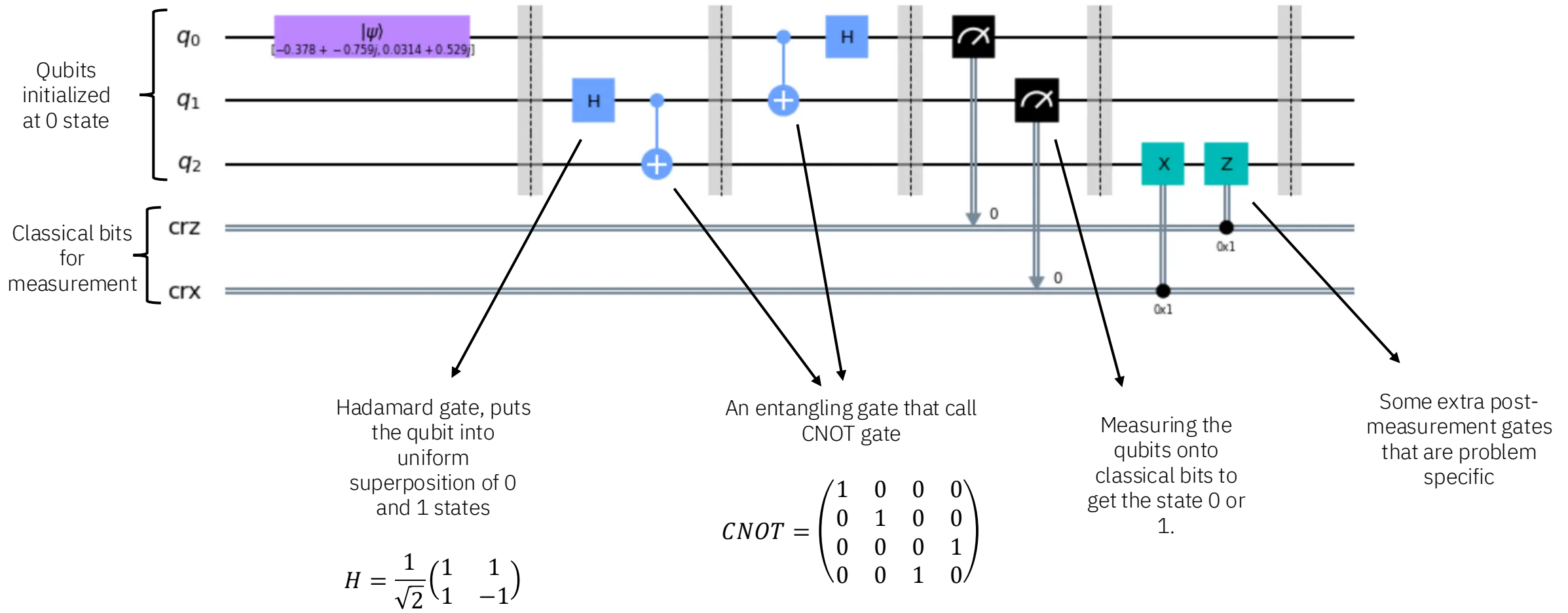
$U = e^{-iHt}$  is unitary!

Unitary operators:

$$U^\dagger U = e^{iH^\dagger t} e^{-iHt} = \mathbf{1} \rightarrow \text{reversibility}$$

H is the Hamiltonian, the operator describing the energy of the system, different from case to case, not to be confused with the Hadamard gate.

# An example of quantum circuit



# Foundations - differences

## Quantum

Superposition

Entanglement

Interference

Measure a single state

Unitary gates

Complex coefficients

## Classical

On or off – probabilistic  
“superposition” has cost

Independent system states –  
“entanglement” possible

No interference

Measure a single state

Unitary & non-unitary gates

Real coefficients

Are these attributes of quantum *better* in all cases?

No. They're different. So where can they bring value?

# Understanding complexities

**P (polynomial):** problems that can be solved in polynomial time.

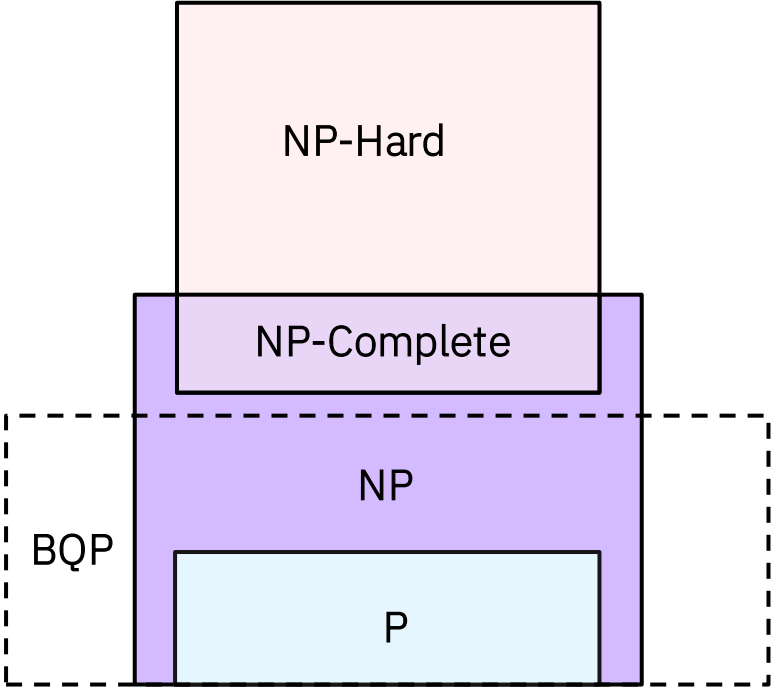
**NP – (non-deterministic polynomial):** Can check a solution in polynomial time, but can't find one in polynomial time.

**NP Complete:** NP-Hard problems also in NP, solutions of which map to solve all NP.

**NP Hard:** Problems as hard as the hardest problems in NP.

**BQP (Bounded-error quantum polynomial):** solvable by a quantum computer in polynomial time, with an error probability of at most 1/3

$$t(n) = c_0 + c_1n + c_2n^2 + \dots c_m n^m$$



Some complexity classes, under the assumption that P is not equal to NP. Note all class assignments are subject to the uncertainty of complexity class structure.

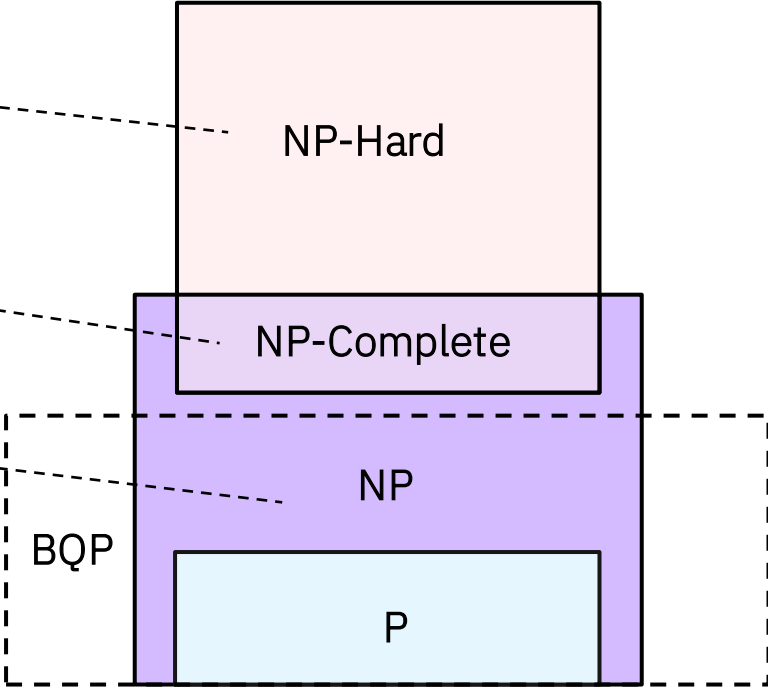
# Understanding complexities

$$t(n) = c_0 + c_1n + c_2n^2 + \dots + c_m n^m$$

Max-cut problem & Travelling salesperson problem

Protein folding (hydrophobic/hydrophilic, self-avoiding model)

Prime factoring



Some complexity classes, under the assumption that P is not equal to NP. Note all class assignments are subject to the uncertainty of complexity class structure.

# What can we do with quantum computers?

Optimization problems

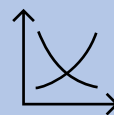
Finance/portfolio optimization



Better financial modeling

More accurate risk management methods

Improved flight/traffic scheduling



Supply chain optimization

...

Chemistry simulations

More energy efficient batteries



Better fertilizer for lower CO2 emission



More effective therapeutics for diseases



More durable materials resisting corrosion

...

Machine learning/  
Cryptography

Classification/  
Regression tasks



High dimensional data analysis



RSA cryptography/prime factorization

Feature selection/identification



Natural language processing

...

Faster and more accurate solutions!

# What's next in quantum?



# Questions

---

## Conclusions:

- Quantum computing is different from classical computing
- The differences are what make it valuable:
  - Superposition, entanglement
  - Unitary operations
- Groundbreaking research is already emerging at the utility scale

