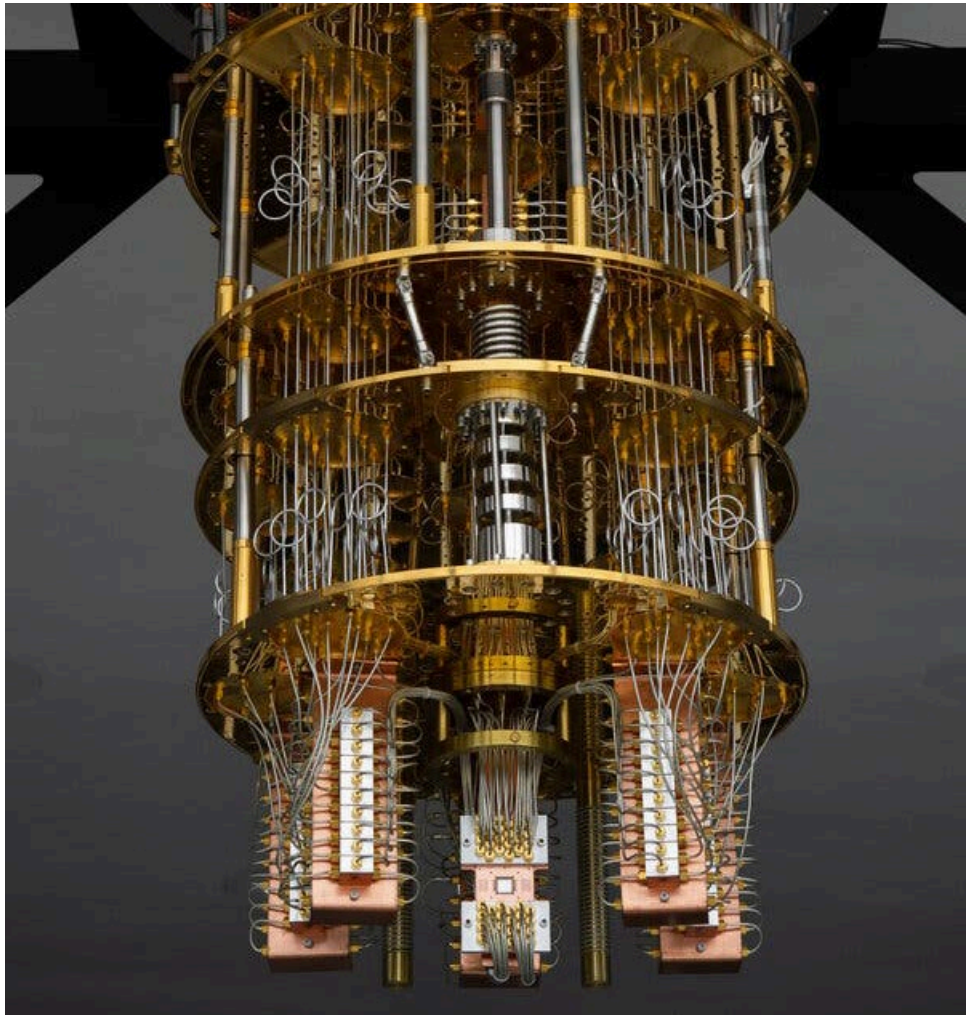
THE CATHOLIC UNIVERSITY OF AMERICA

Quantum Convergence The Future of Cybersecurity and AI

Daniel Sierra-Sosa, Ph.D.
Assistant Professor
Department of Computer Science
The Catholic University of America

What is quantum computing?

- **Quantum mechanics:** the science of matter and energy on the atomic and subatomic levels.
- **Quantum computers:**
  - harness the laws of quantum mechanics to solve complex mathematical problems
  - store information in qubits (quantum bits) as 0, 1, or a superposition of 0 and 1, and
  - typically provide ranges of possible answers due to their nondeterministic (probabilistic) nature.
- **Classical computers**:
  - store information in bits with a discrete number of possible states, 0 or 1,
  - process data logically and sequentially, and
  - provide singular answers.



“It is no longer a physicist’s dream—it is an engineer’s nightmare.”

Isaac Chuang

Why are we interested in quantum computers?

Interested in quantum computing for:

- Nature simulation
- Search and optimization
- Processing data with structure
- Secure information

Quantum computers work *with* classical computers, not replace them.

Quantum Technologies

Superconducting Architecture

IBM rigetti

Alibaba Group 阿里巴巴集团

Trapped Ions

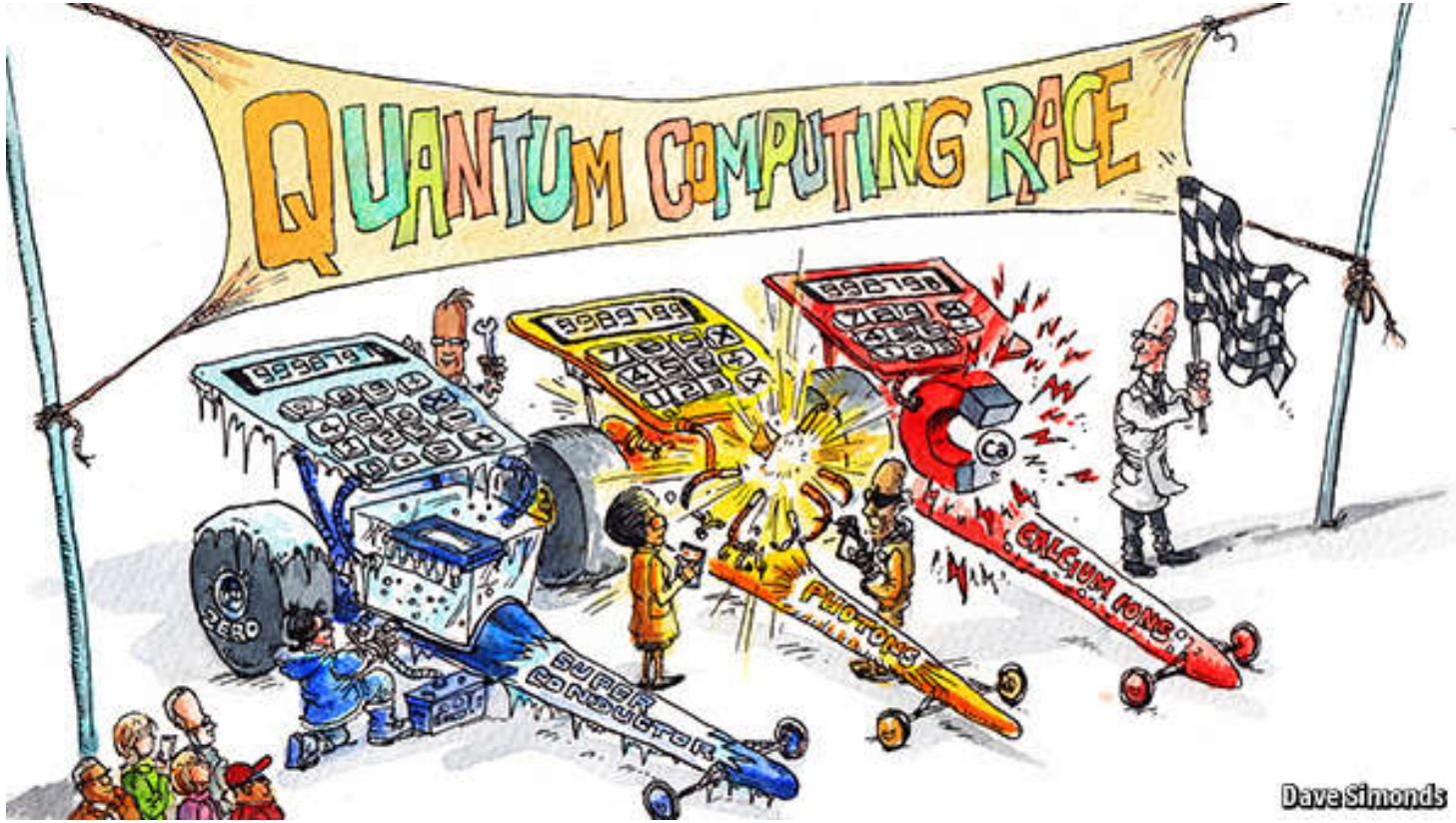
IONQ

Topological

Microsoft

Photonic

XANADU



Use Cases: Defense and Security

- **Enhanced Surveillance and Detection**

Quantum sensing allows for detection of stealth aircraft or submarines by measuring slight variations in gravitational or magnetic fields.

- **Real-Life Examples**

In April 2025, Chinese scientists tested a drone-mounted quantum sensor system capable of detecting submarines with high sensitivity. This technology aims to overcome blind spots in traditional detection methods, potentially revolutionising undersea surveillance.

https://www.qureca.com/use-cases

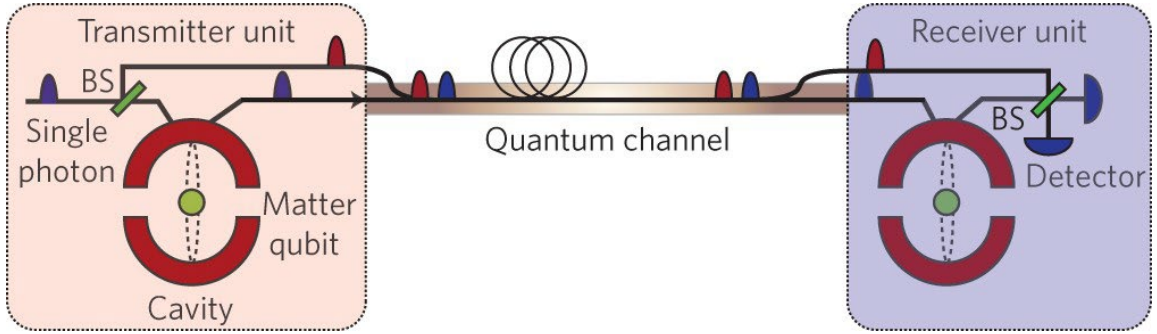
Use Cases: Defense and Security

- **Secure Military Communications**

Quantum communication ensures ultra-secure transmission of classified data, immune to interception. Nations could implement quantum key distribution (QKD) for diplomatic cables and battlefield commands.

- **Real-Life Examples**

The U.S. Navy is exploring quantum communication technologies to enable secure communications for missile submarines. Quantum communication provides a highly secure method of transmitting and receiving data, making use of quantum theory to store information in delicate quantum states that collapse if unauthorised access is attempted.



Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A., & Nemoto, K. (2012). Quantum communication without the necessity of quantum memories. *Nature Photonics*, *6*(11), 777-781.

https://www.qureca.com/use-cases

Use Cases: Financial Services

- **Advanced Risk Assessment**

Quantum algorithms can analyse complex market variables much more efficiently than classical methods, giving financial institutions deeper insights into risk and uncertainty.

- **Real-Life Examples**

Goldman Sachs is testing quantum approaches for complex financial modeling problems.

https://www.qureca.com/use-cases

Use Cases: Energy Sector

- **Optimizing Energy Grids**

A smart grid company could use quantum computing to balance load distribution across renewables, ensuring stability during peak times.

- **Real-Life Examples**

Siemens and Energy Web Foundation are looking into quantum-enhanced optimization for smart grid systems.

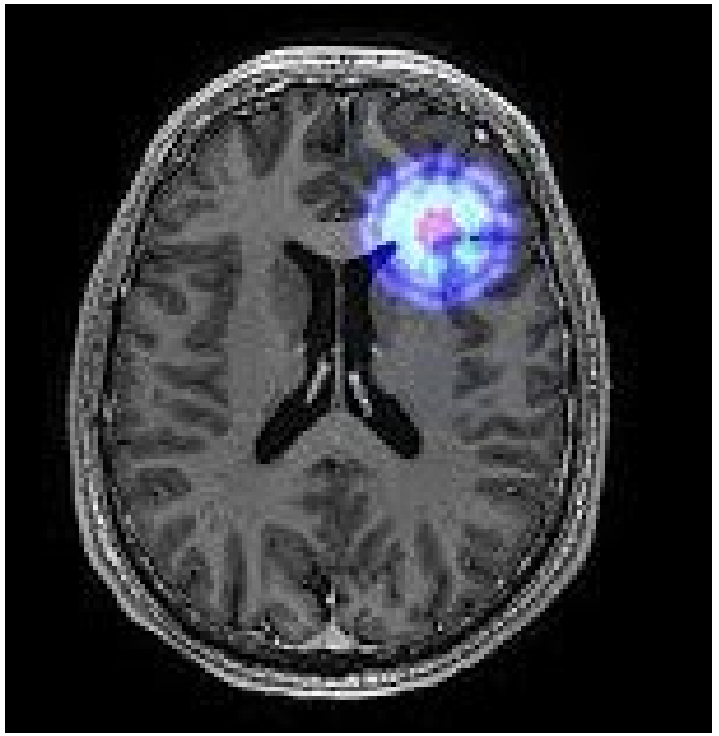
https://www.qureca.com/use-cases

Use Cases: Healthcare

- **Enhancing Medical Imaging**

Quantum sensing technologies bring a new level of precision to imaging biomolecules, making it easier to detect and diagnose diseases early. This leap forward helps doctors create more targeted and effective treatment plans, ultimately leading to better outcomes for patients.

- **Real-Life Examples**
- Startups like Qnami are already using quantum sensors for ultra-sensitive diagnostics in neurology.



https://www.qureca.com/use-cases

Use Cases: Logistics

- **Optimizing Logistics Networks**

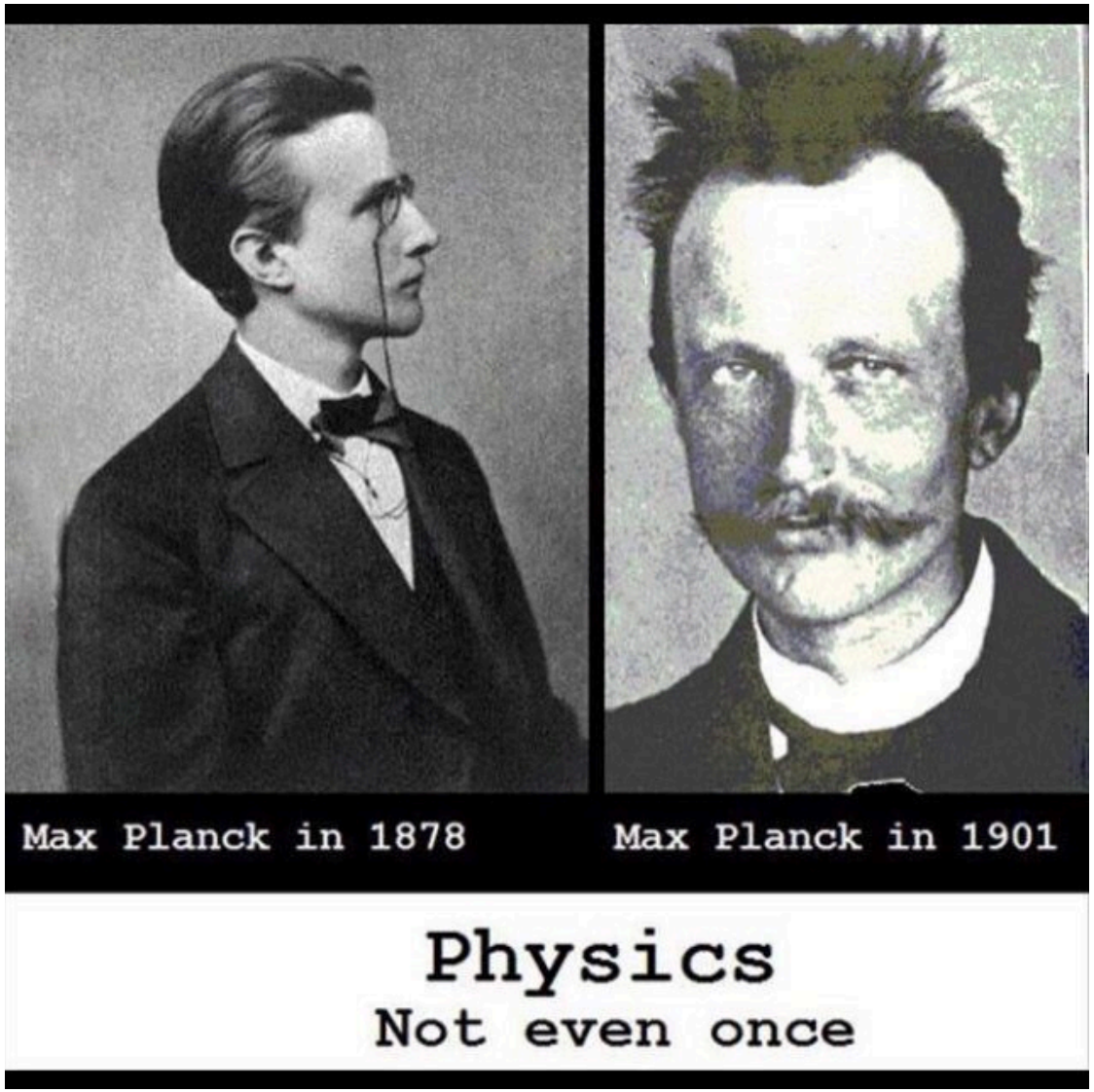
Quantum computing optimizes complex logistics networks by solving routing, scheduling, and inventory problems exponentially faster than classical computers. By analyzing vast datasets and running advanced algorithms, it enables real-time adjustments to supply chains, reducing delays, cutting costs, and minimizing waste.

- **Real-Life Examples**

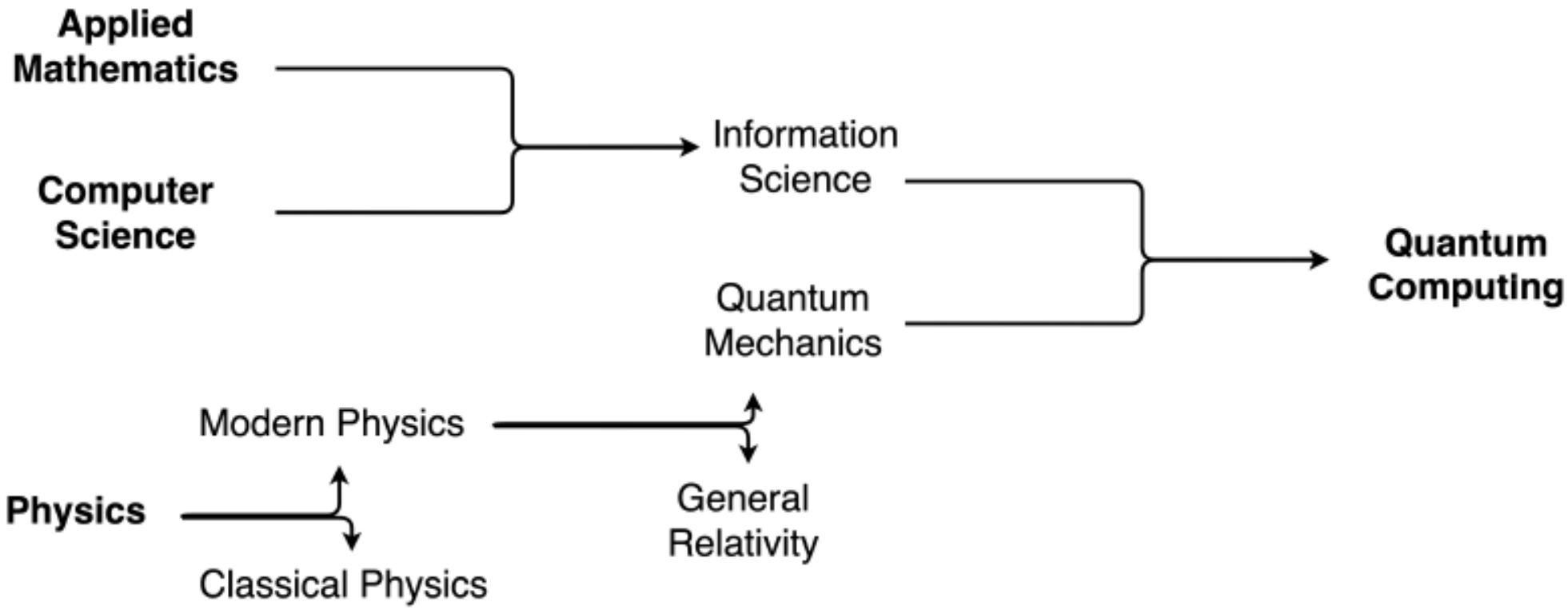
ExxonMobil is collaborating with IBM Research to apply hybrid quantum-classical algorithms for optimizing liquefied natural gas (LNG) shipping routes. By modeling vessel scheduling, inventory management, and port congestion on quantum devices, they aim to reduce fuel costs and delivery times while balancing supply chain risks.

https://www.qureca.com/use-cases

Let’s start!



Skills



Taken from: Ayoade, O., Rivas, P., & Orduz, J. (2022). Artificial Intelligence Computing at the Quantum Level. Data, 7(3), 28.

Postulates of Quantum Mechanics

- **State Space:** Describes the state of a closed system.
- **Evolution:** describes the evolution of a closed system.
- **Measurement:** describes how information is extracted from a closed system via interactions with an external system.
- **Composite systems:** describes the state of a composite system in terms of its component parts

Classical vs quantum bits

Classical bit (bit)

Only two possible states

0 and 1

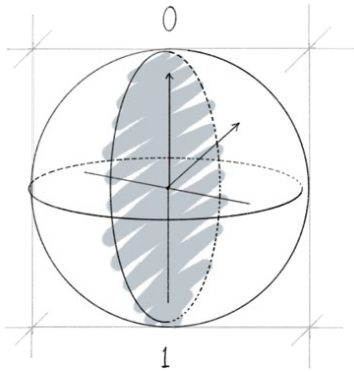
- Like the two faces of a coin
  - Heads or tails

Quantum bit (qubit)

$|0\rangle$ or $|1\rangle$

AND any linear combination of the two

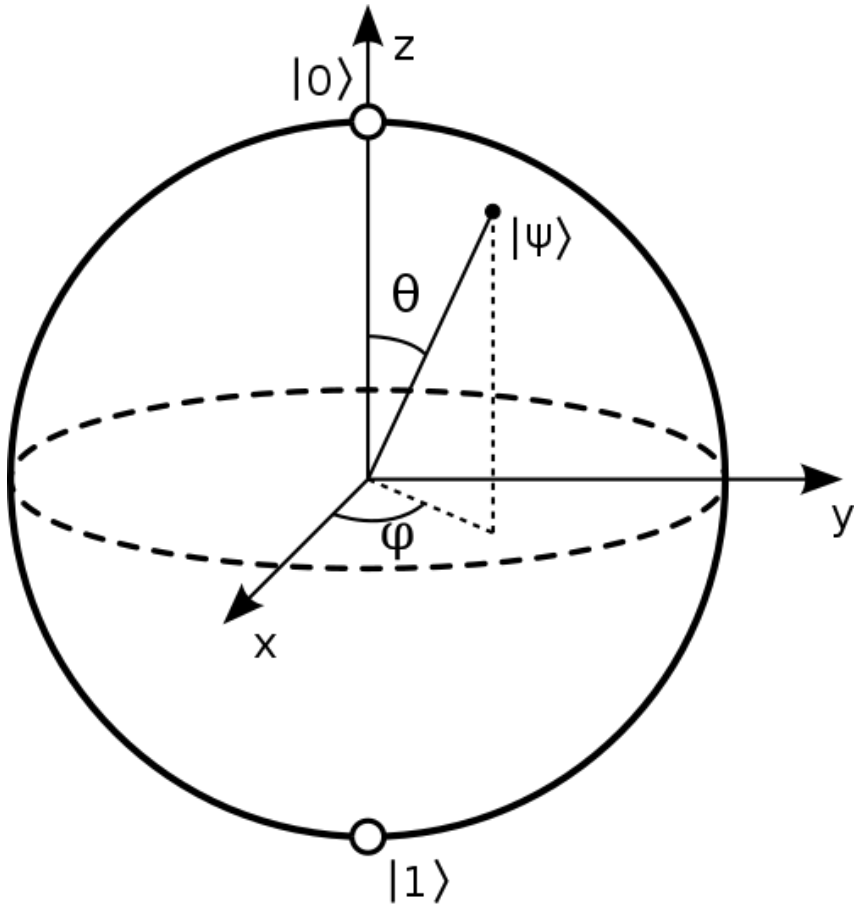
e.g. 50% $|0\rangle$ & 50% $|1\rangle$



Quantum State (qubit)

Mathematically represented as a vector, or a point on the surface of the Bloch sphere:

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



Measurement = projection of state to a basis vector
(changes the state – superposition is destroyed)

Quantum gate is a transformation from one qubit state to another.
Single-qubit gate = rotation around Bloch sphere. Reversible.
Represented by a matrix (unitary, …) acting on the vector.

NOTE: There are many possible basis vector sets – any antipodal points on the Bloch sphere are orthogonal. "Standard" basis is $\{|0\rangle,|1\rangle\}$.

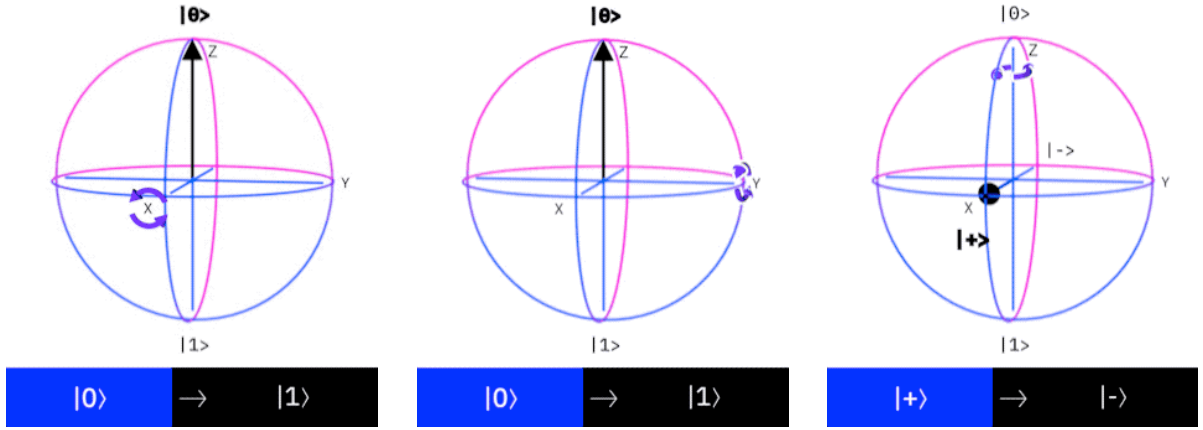
Qubit Gates

- A qubit gate is a black box transforming an input qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ into an output qubit $|\varphi\rangle = \alpha'_0|0\rangle + \alpha'_1|1\rangle$
- A gate G is represented by a $2x2$ transfer matrix with complex elements $a_{i,j}$ where $(i,j) \in \{1,2\}$:

$$G = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Recall $|a_0|^2 + |a_1|^2 = 1$ and $|a'_0|^2 + |a'_1|^2 = 1$

1. Matrix G is a unitary $G^\dagger G = \mathbb{I}$
2. The inverse of a unitary matrix G^{-1} is also unitary



X Y Z

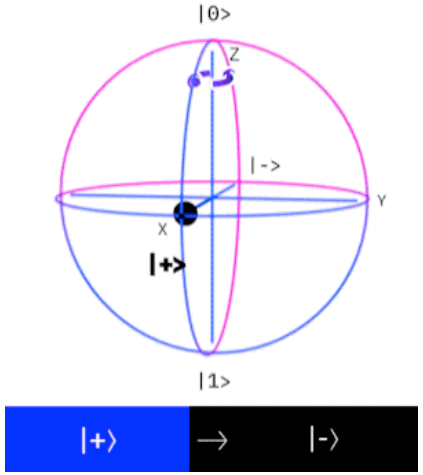
$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \longrightarrow |\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle.$$

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_0 \end{pmatrix} \longrightarrow |\phi\rangle = \alpha_1|0\rangle + \alpha_0|1\rangle.$$

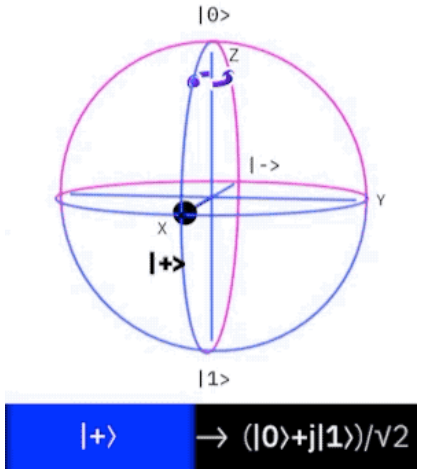
$$\sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = i\begin{pmatrix} -\alpha_1 \\ \alpha_0 \end{pmatrix} \longrightarrow |\phi\rangle = -i\alpha_1|0\rangle + i\alpha_0|1\rangle.$$

$$\sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ -\alpha_1 \end{pmatrix} \longrightarrow |\phi\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle.$$

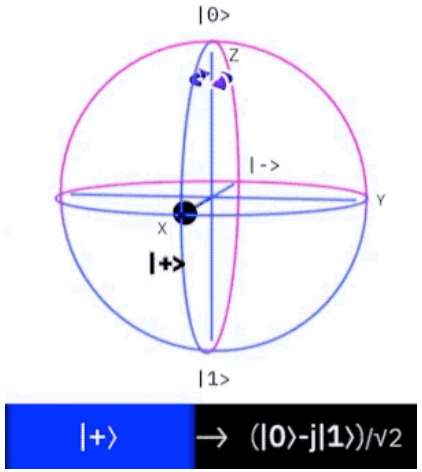
Qubit Gates Phase: Z, S, T



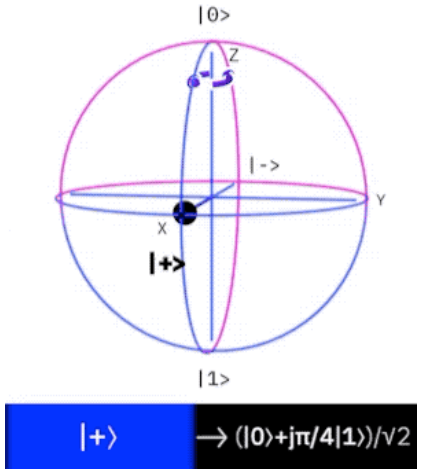
Z



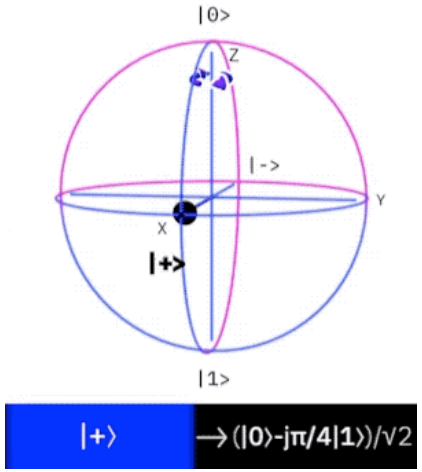
S



$S^\dagger$

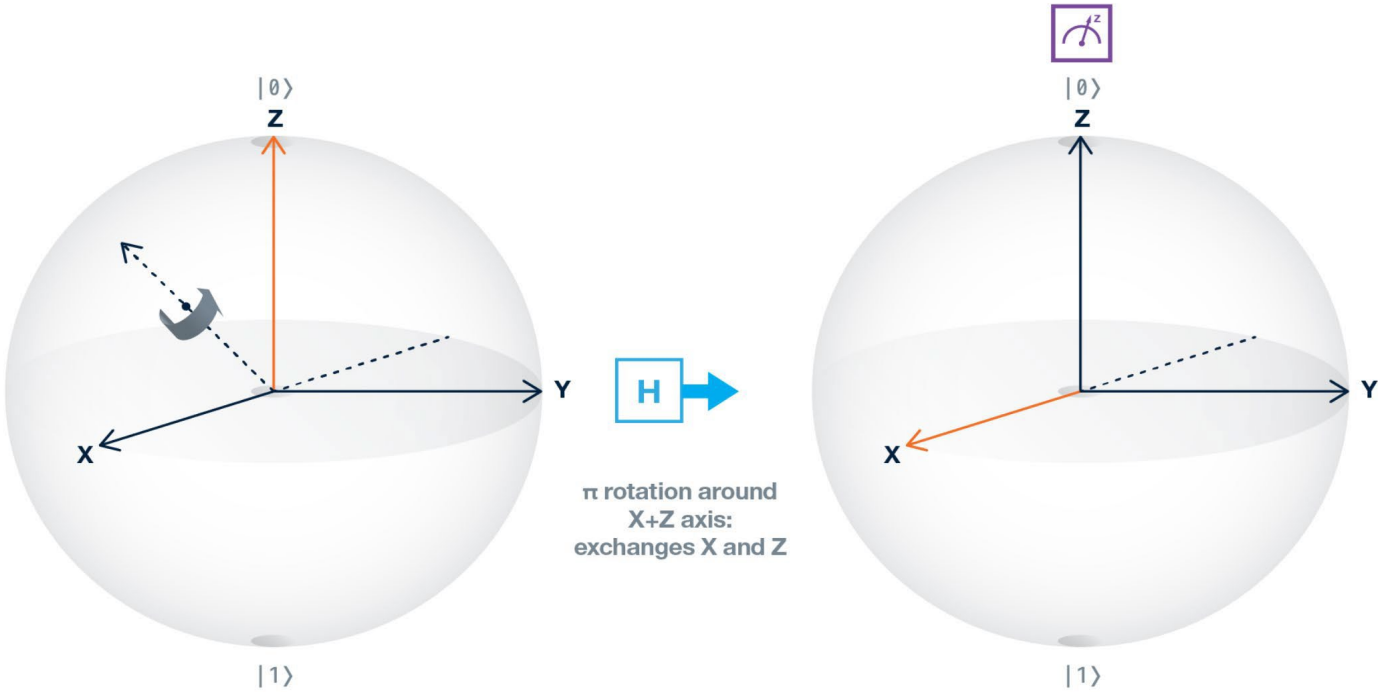


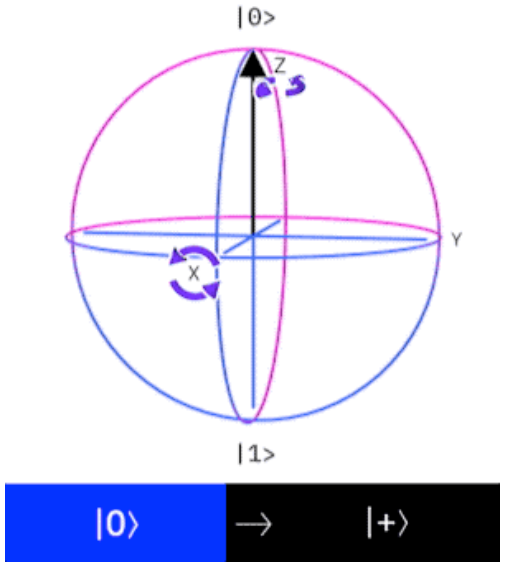
T



$T^\dagger$

Hadamard (H) Gate: Superposition

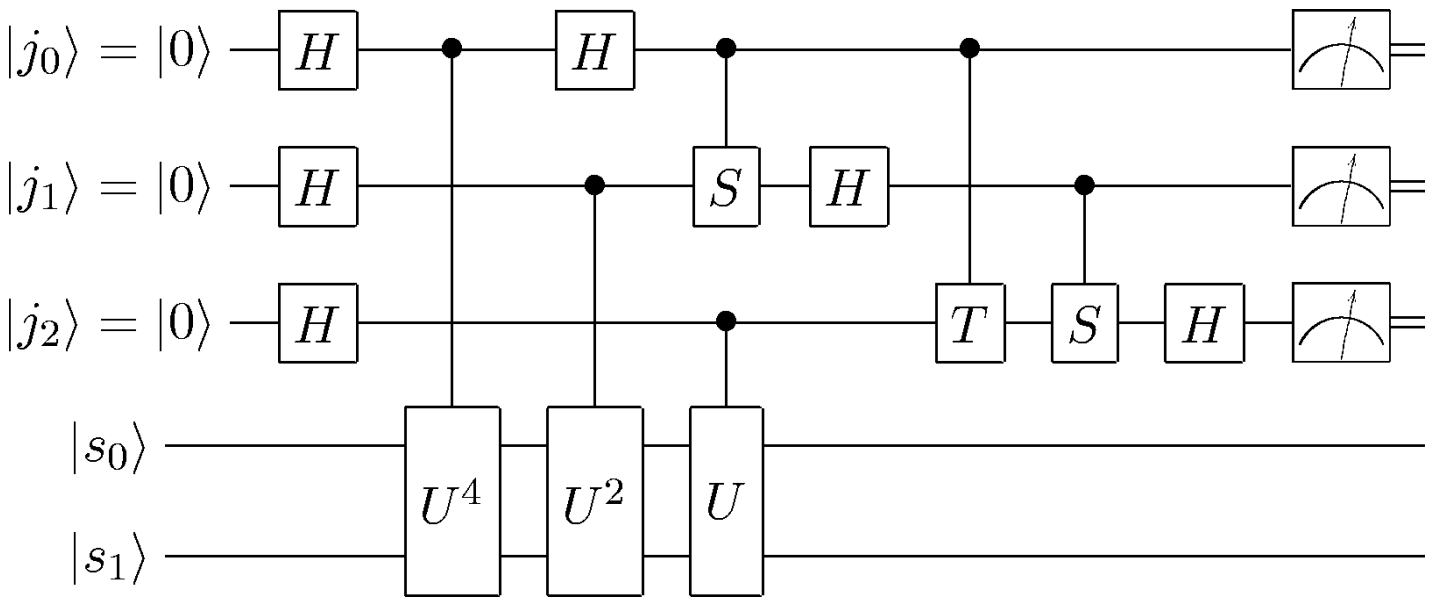




$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Quantum Circuits

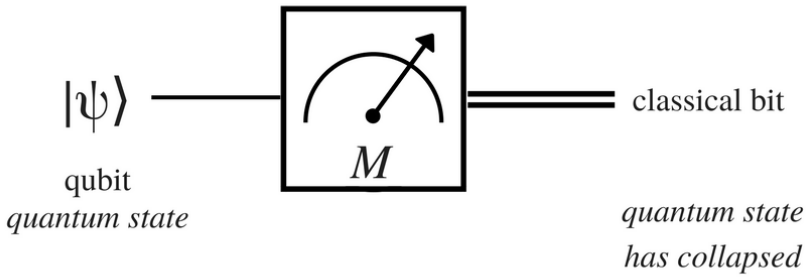


- Time flows left to right.
- Quantum gates (operators) are applied sequentially to qubit states, with result shown on the right.
- Measurement:
  - Double line represents classical bit.
  - Measurement is in the standard basis

Any quantum transformation can be realized in terms of the basic gates of the standard circuit model.

Measurement

- A **measurement** can be done by a projection of each $|\psi\rangle$ in the basis states, namely $|0\rangle$ and $|1\rangle$.
- Measurement can be done in any orthonormal and linear combination of states $|0\rangle$ and $|1\rangle$.
- Measurement changes the state of the system and can not provide a snapshot of the entire system.



Quantum noise and error

Quantum decoherence: the process in which quantum particles and systems can decay, collapse or change, converting into single states measurable by classical physics.

- Intentionally triggered by measuring qubits to send results back via bits.
- Unintentionally triggered due to environmental factors – undesirable!

Noise: anything that affects our quantum system in an undesirable way

Source of noise	**What is it?**
Coherent noise	Imperfect quantum gates causing over- or under-rotations, resulting in outcomes different to the desired
Incoherent noise	Loss of quantum properties in a qubit due to interaction with its environment
State preparation and measurement	Imperfections in preparing initial quantum states and measuring quantum states
Projection noise	The non-deterministic nature of quantum computers resulting in fluctuations in measurement outcomes

Quantum error mitigation

- **Quantum error mitigation:** tools and methods that allow us to evaluate accurate expectation values from noisy, shallow depth quantum circuits, even before the introduction of fault tolerance.

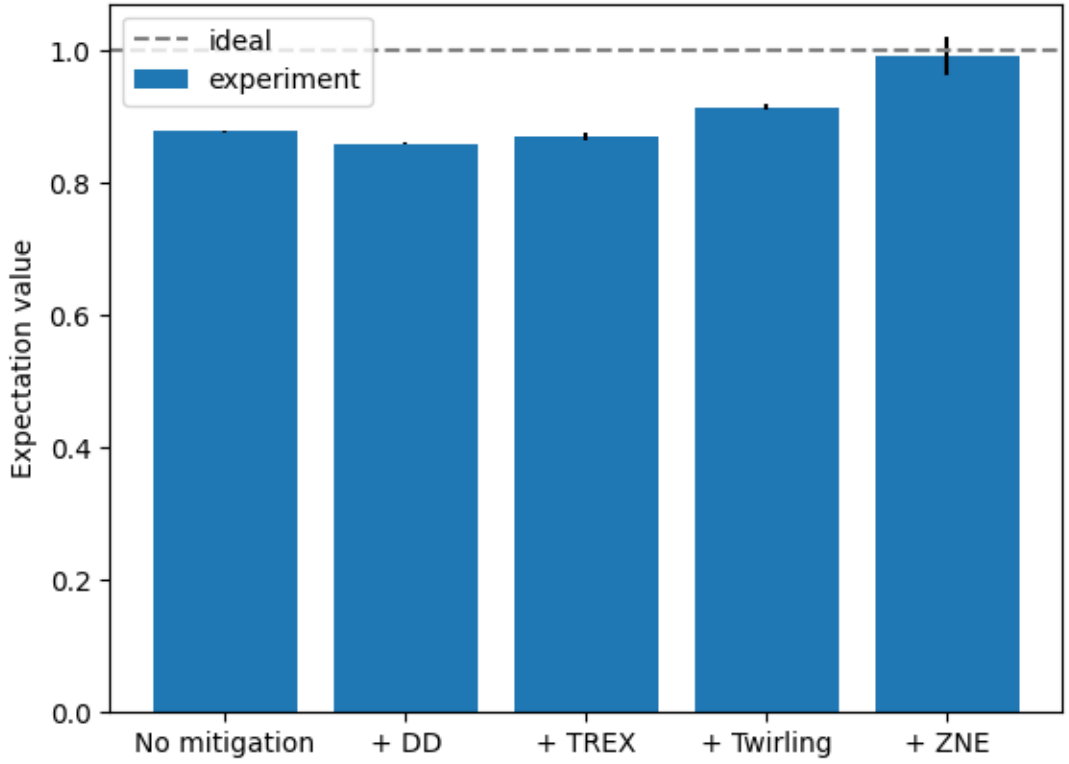
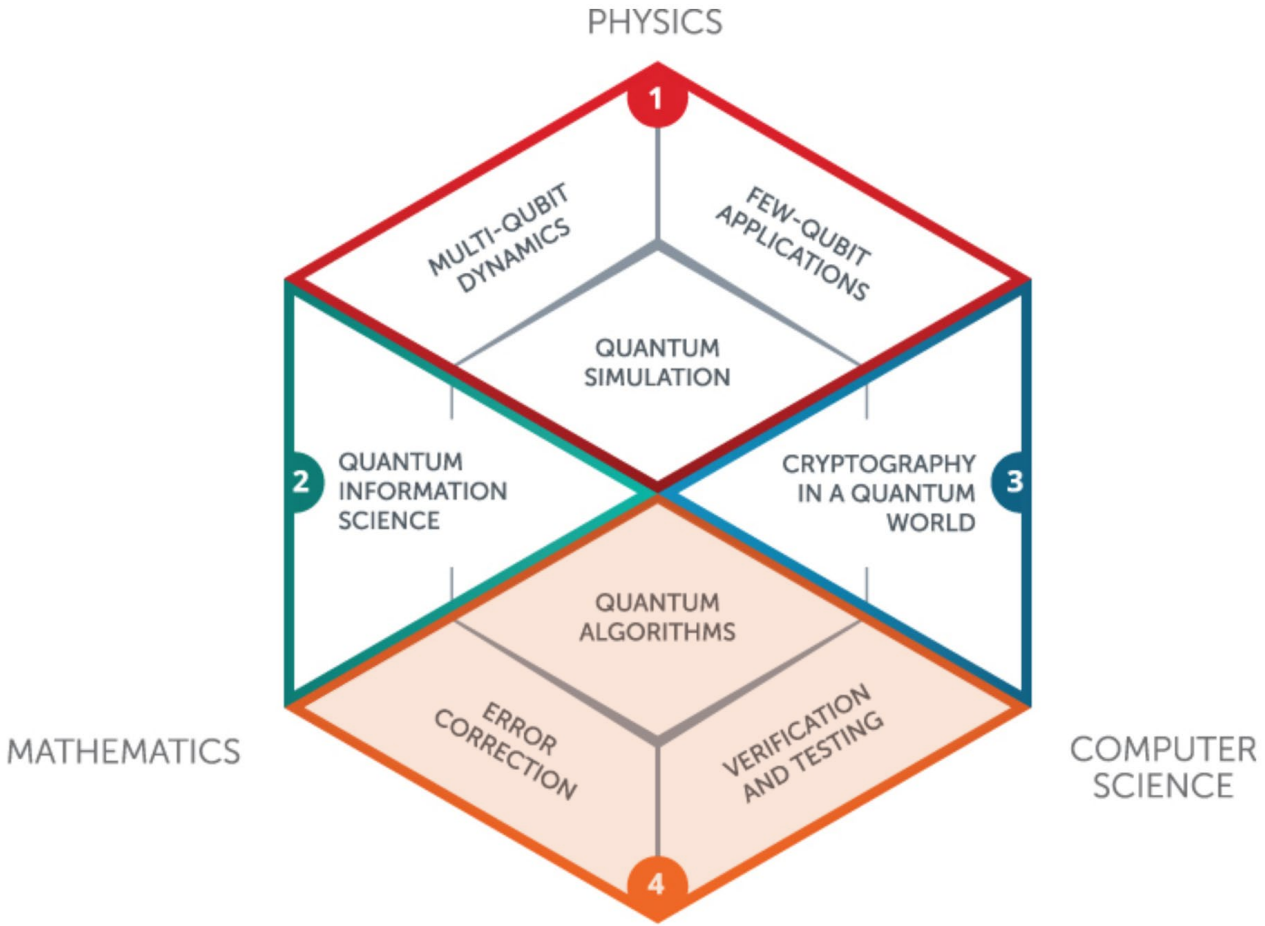


Fig: 50-qubit EfficientSU2 circuit experiment using quantum error mitigation and suppression techniques vs no mitigation (source: IBM, 2025)

Quantum algorithms

A quantum algorithm consists of three basic steps:

- Encoding of the data, which could be classical or quantum, into the state of a set of input qubits.
- A sequence of quantum gates applied to this set of input qubits.
- Measurements of one or more of the qubits at the end to obtain a classically interpretable result.



Classes of Quantum Algorithms

Class	Problem/Algorithm	Paradigms used
Inverse Function Computation	Grover's Algorithm	GO
	Bernstein-Vazirani	n.a.
Number-theoretic Applications	Shor's Factoring Algorithm	QFT
Algebraic Applications	Linear Systems	HHL
	Matrix Element Group Representations	QFT
	Matrix Product Verification	GO
	Subgroup Isomorphism	QFT
	Persistent Homology	GO, QFT
Graph Applications	Quantum Random Walk	n.a.
	Minimum Spanning Tree	GO
	Maximum Flow	GO
	Approximate Quantum Algorithms	SIM
Learning Applications	Quantum Principal Component Analysis (PCA)	QFT
	Quantum Support Vector Machines (SVM)	QFT
	Partition Function	QFT
Quantum Simulation	Schrödinger Equation Simulation	SIM
	Transverse Ising Model Simulation	VQE
Quantum Utilities	State Preparation	n.a.
	Quantum Tomography	n.a.
	Quantum Error Correction	n.a.

Algorithmic Paradigms:

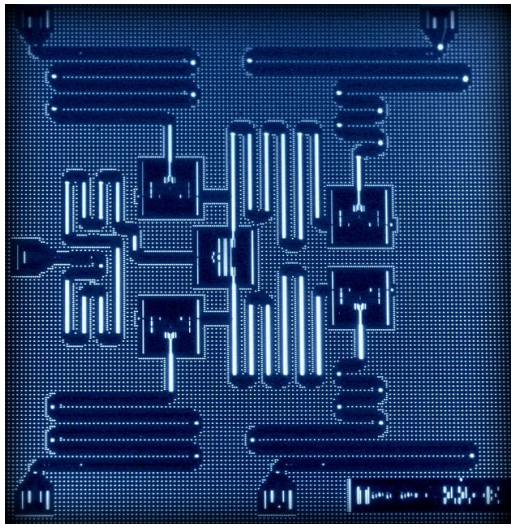
- Quantum Fourier Transform (QFT)
- Grover Operator (GO)
- Harrow-Hassidim-Lloyd (HHL)
- Variational Quantum Eigenvalue (VQE)
- Hamiltonian simulation (SIM)

Requirements for a Quantum Computer

1. A scalable physical system with well characterized qubits
2. The ability to initialize the state of the qubits to a simple state
3. Long decoherence times, much longer than the gate operation time
4. A "universal" set of quantum gates
5. A qubit-specific measurement capability

<u>Two criteria requiring the possibility to transmit information:</u>

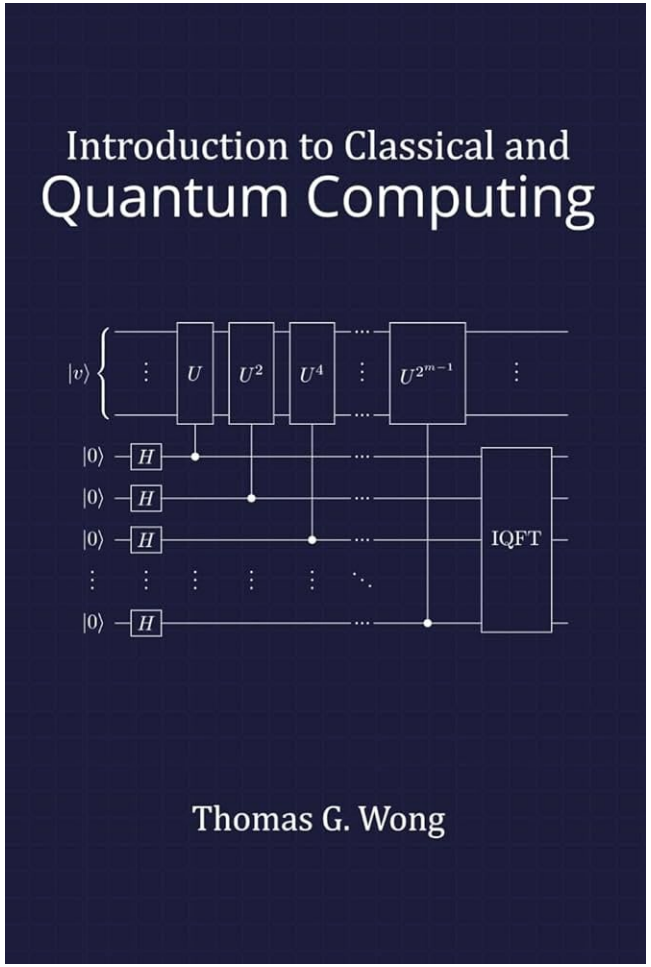
1. The ability to interconvert stationary and flying qubits.
2. The ability to faithfully transmit flying qubits between specified locations.

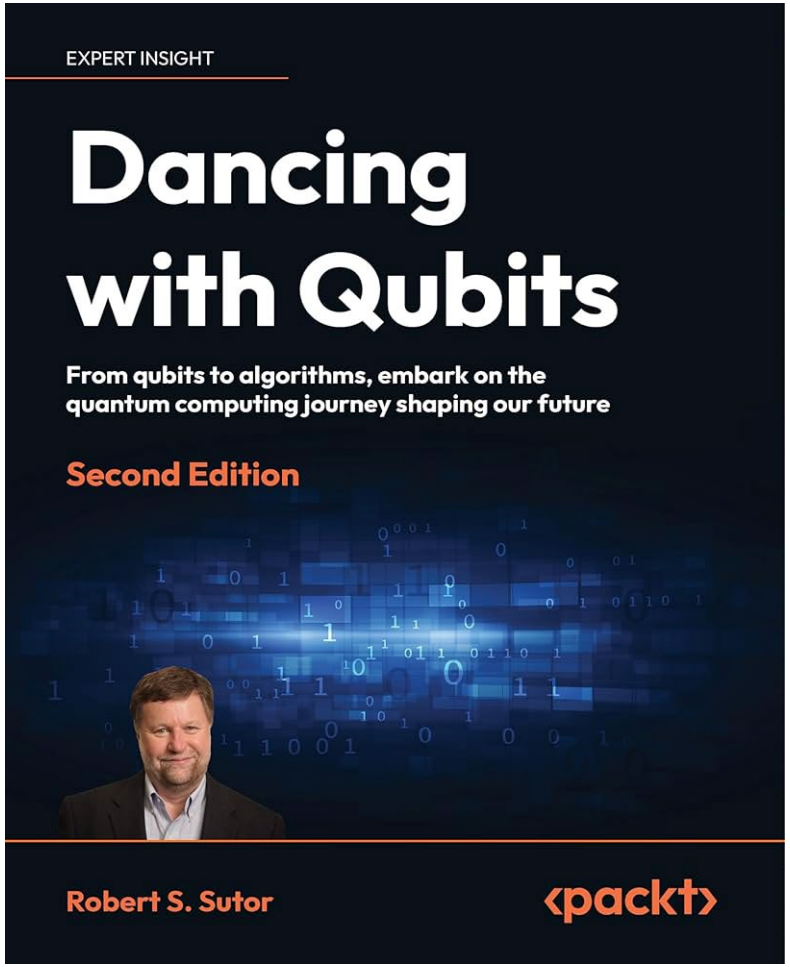


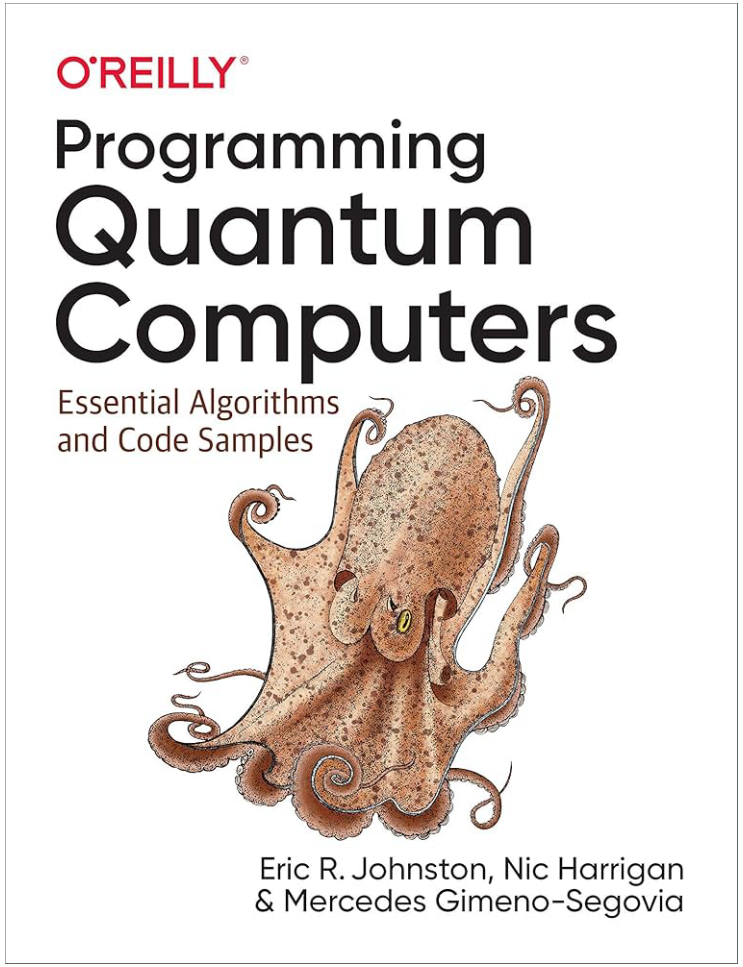
Layout of IBM's five superconducting quantum bit device. (credit: IBM Research)

DiVincenzo, D. P. (2000). The physical implementation of quantum computation. *Fortschritte der Physik: Progress of Physics*, *48*(9‐11), 771-783.

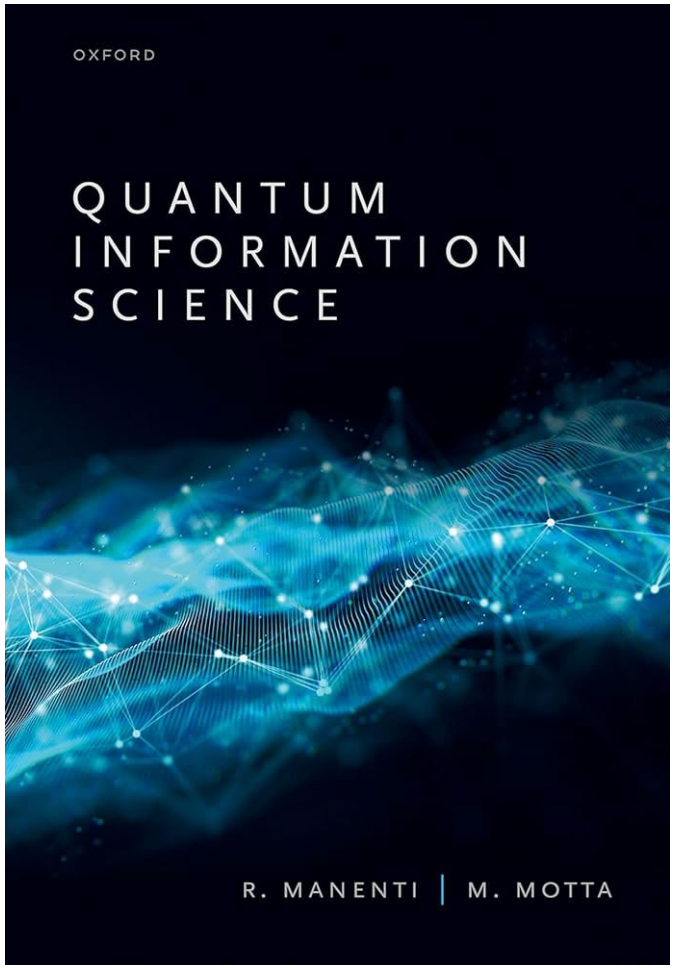
Introductory Books

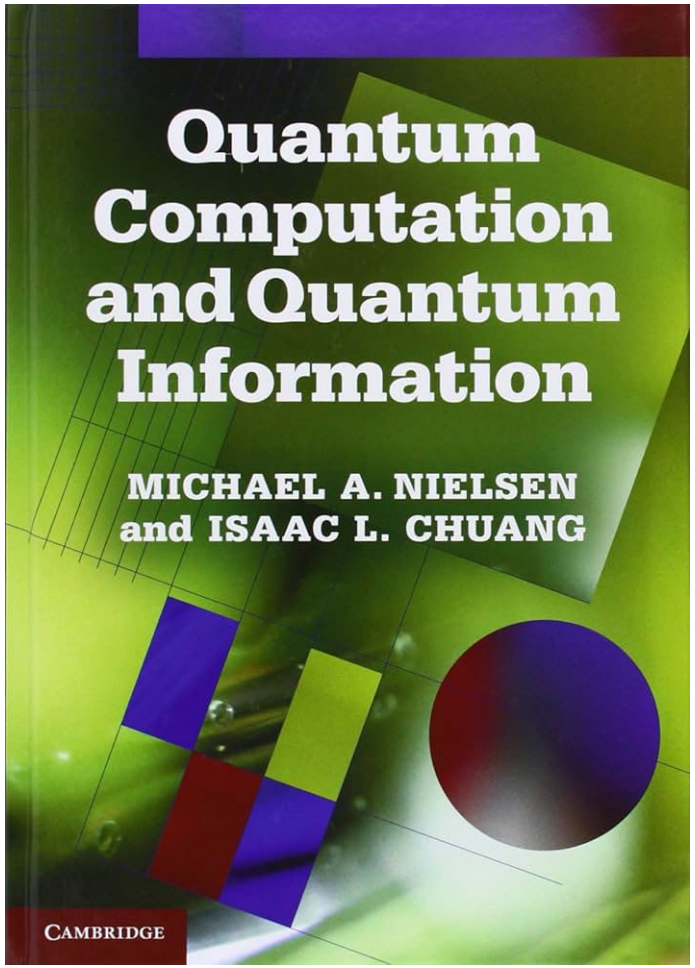




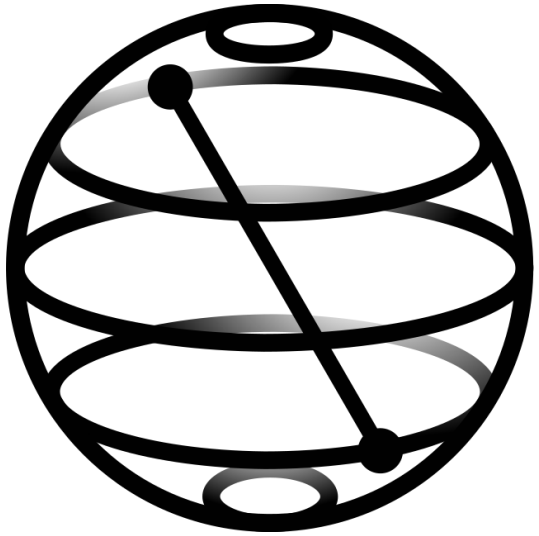


Comprehensive Books





Qiskit



- Qiskit is an open-source framework developed by IBM.
  - Based on Python Easy to integrate with other tools and Python libraries.
  - Access to Quantum Hardware: Execution on quantum hardware through IBM Quantum Experience.
- Advantages:
  - Active Community
  - Access to Quantum Hardware
  - Educational Environment

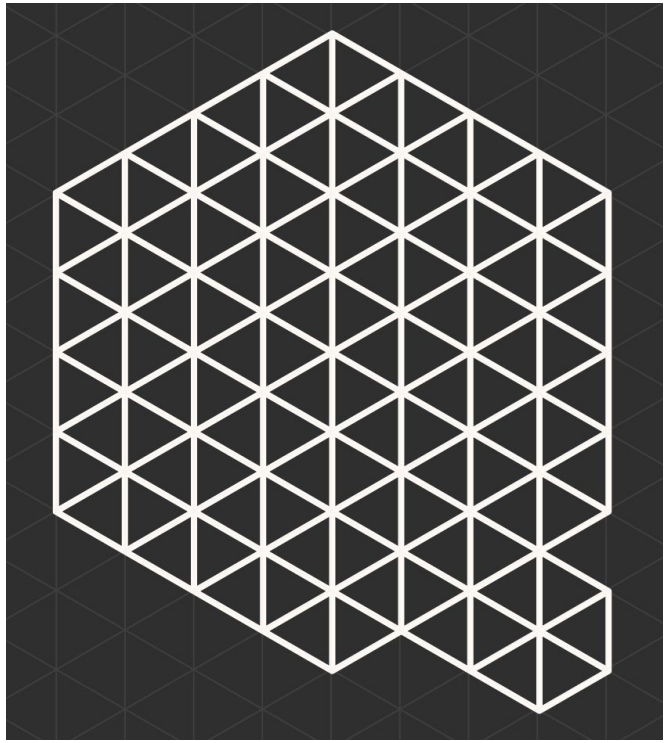
Cirq

- Cirq is an open-source library developed by Google
- Based on Python
  - Easy to integrate with other tools and Python libraries.
- Focus on Real Hardware: Specifically designed to optimize circuits that can be executed on hardware like Google's Sycamore quantum processor.

PyQuil

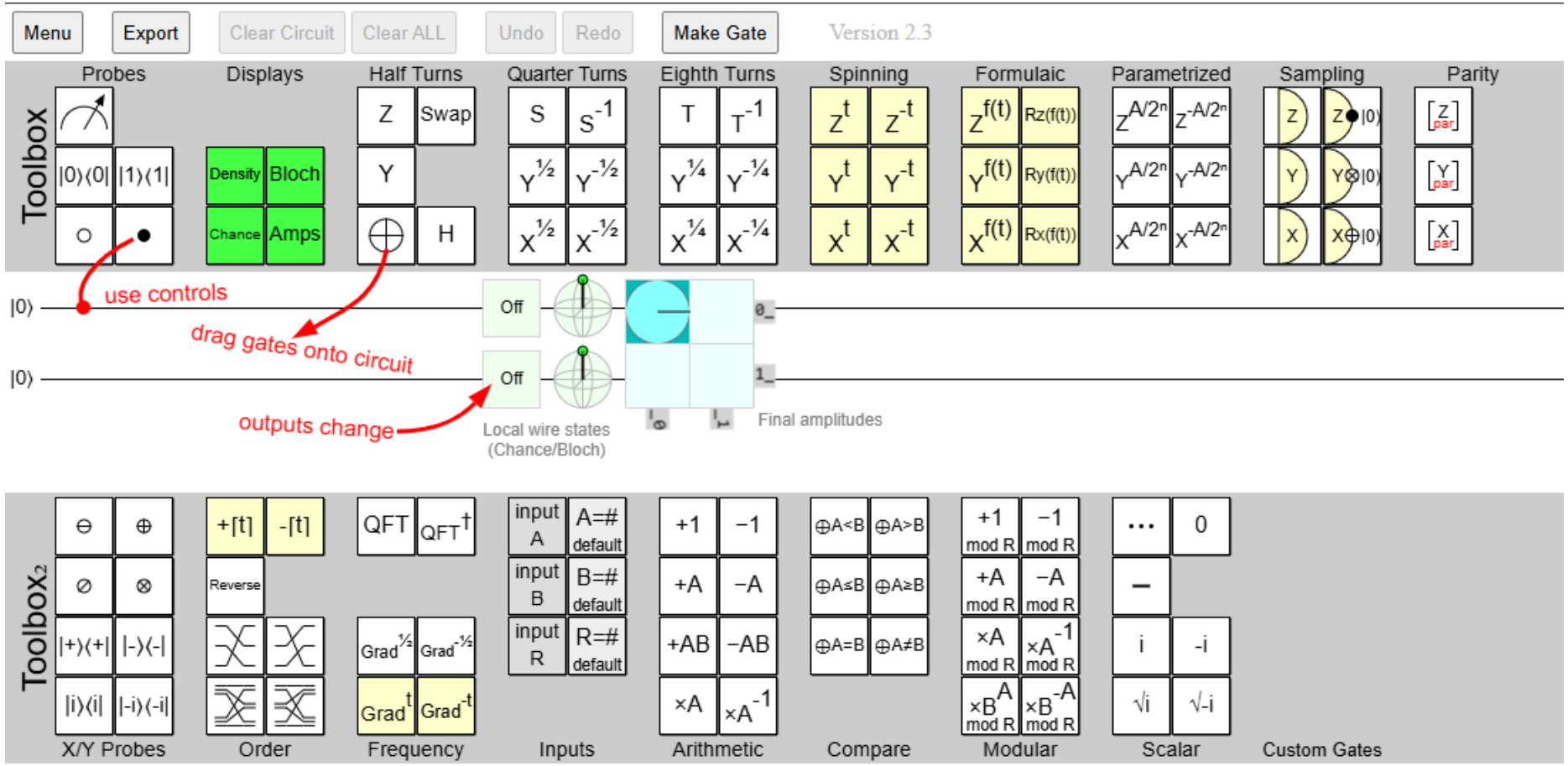
- PyQuil is a Python library developed by Rigetti Computing.
- Based on Python Easy to integrate with other tools and Python libraries.
- Allows the execution of quantum circuits on real hardware through Rigetti's Forest SDK and AWS Braket.
- Suitable for academic research, education, and the development of industrial quantum applications.
- Active Community and Resources:
  - Extensive documentation, practical examples, and active support from the quantum community.

Q#



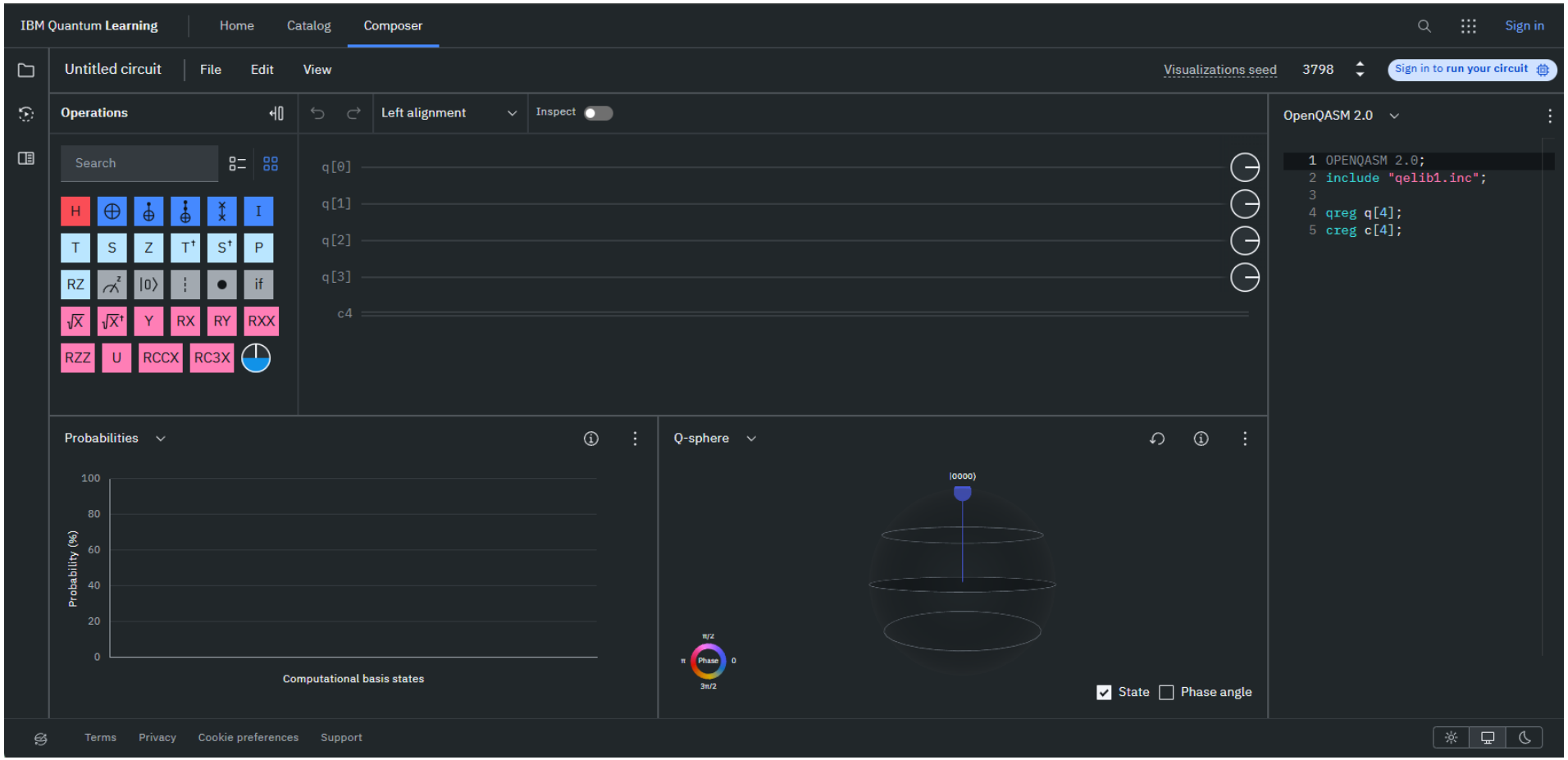
- Q# (Q-sharp) is a programming language developed by Microsoft.
- Integration with .NET and Python: Allows combining quantum programming with classical languages, facilitating the management of mixed tasks.
- Q# provides an environment for developing quantum applications.
- Possibility to run algorithms on real quantum hardware through Microsoft Azure cloud.

Quirk



https://algassert.com/quirk

IBM Composer



https://quantum.ibm.com/composer/files/new

https://quantum.cloud.ibm.com/composer

The present and the future of Quantum