A Short Introduction to Quantum Computing

Elías F. Combarro
combarro@gmail.com

University of Oviedo (Oviedo, Spain)

15-17 January 2025 - Ulster University

Universidad de Oviedo

Part I

Introduction: quantum computing... the end of the world as we know it?

In the year 2025

INTERNATIONAL YEAR OF

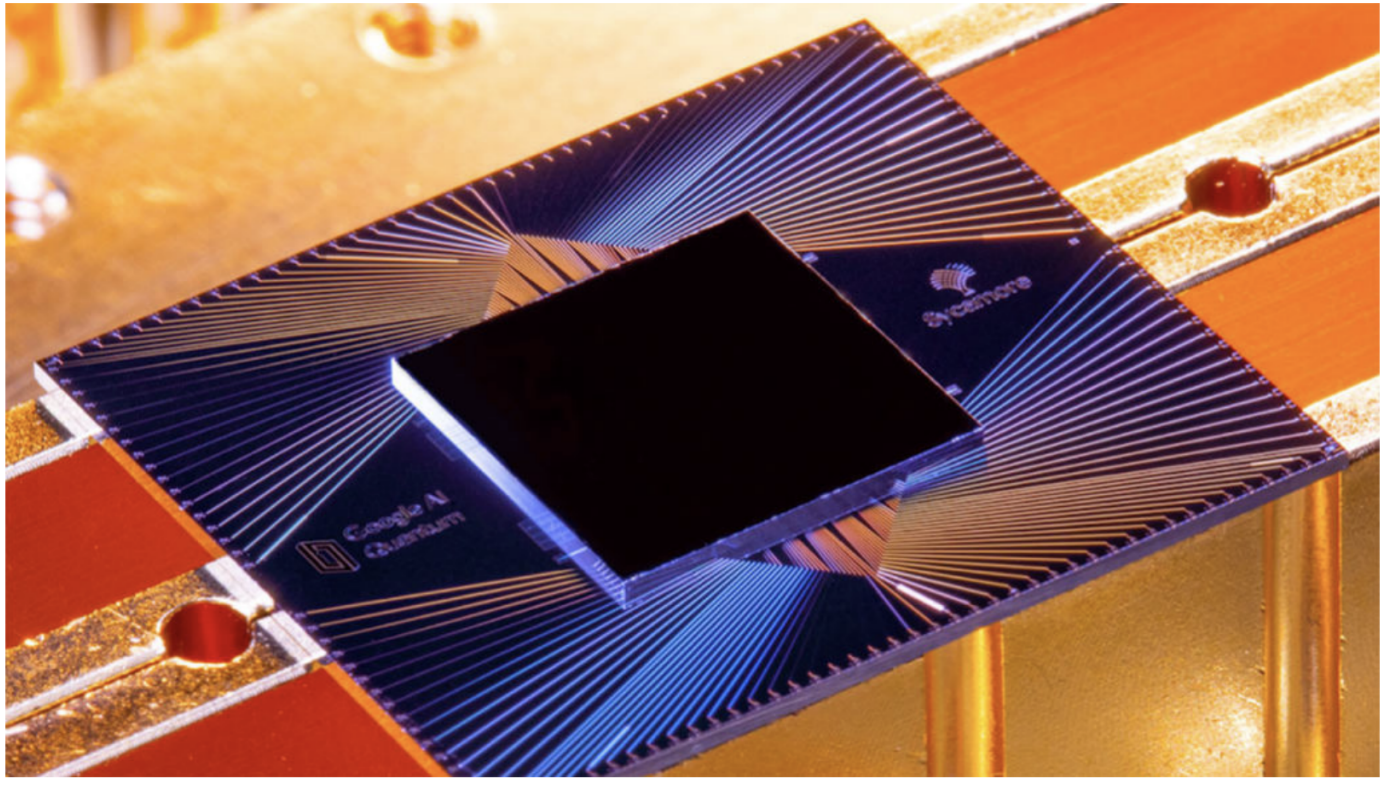
Quantum Science and Technology

I, for one, welcome our new quantum overlords

NEWS QUANTUM PHYSICS

Google officially lays claim to quantum supremacy

A quantum computer reportedly beat the most powerful supercomputers at one type of calculation



Quantum supremacy... yet again

Meet Willow, our state-of-the-art quantum chip

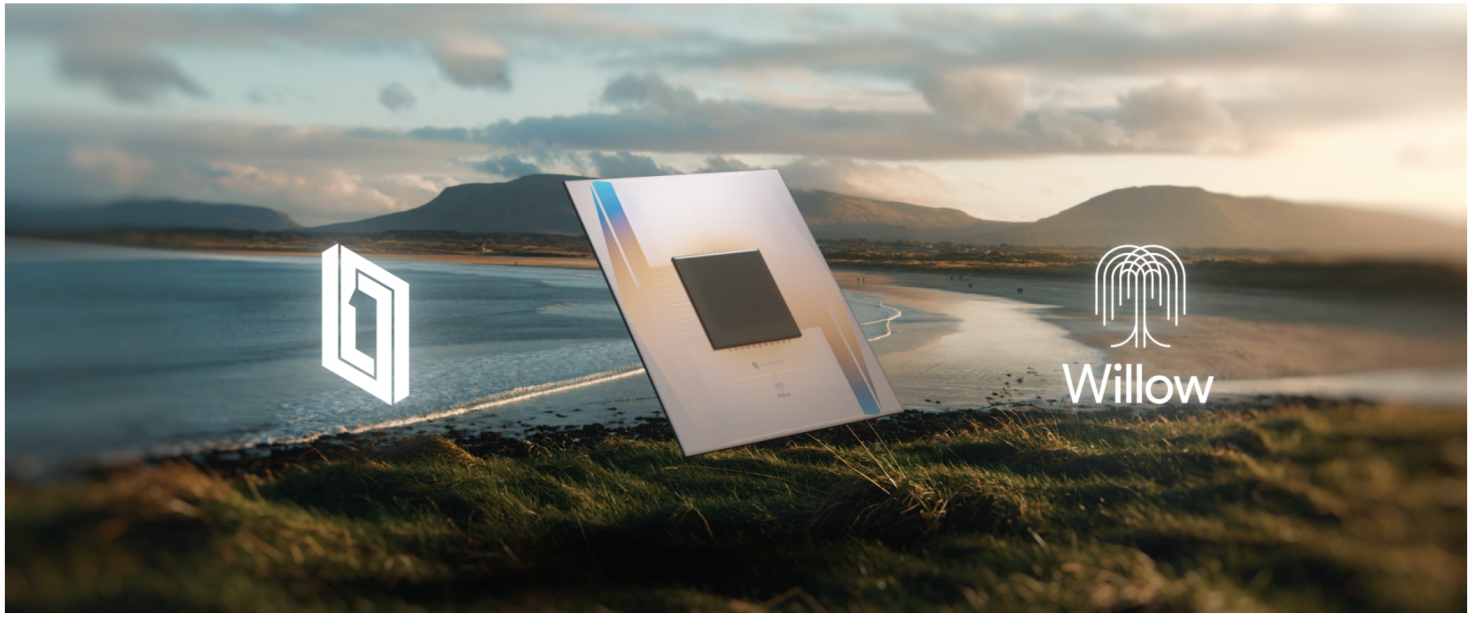
Dec 09, 2024
6 min read

Our new chip demonstrates error correction and performance that paves the way to a useful, large-scale quantum computer

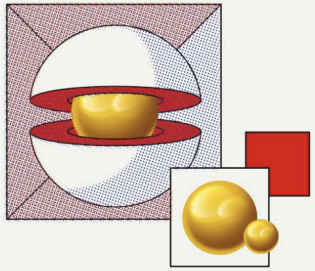
Hartmut Neven
Founder and Lead, Google Quantum AI

Read AI-generated summary

Share



Myths and realities



Palabras clave: computación cuántica, supremacía cuántica, criptografía, inteligencia artificial, simulación.

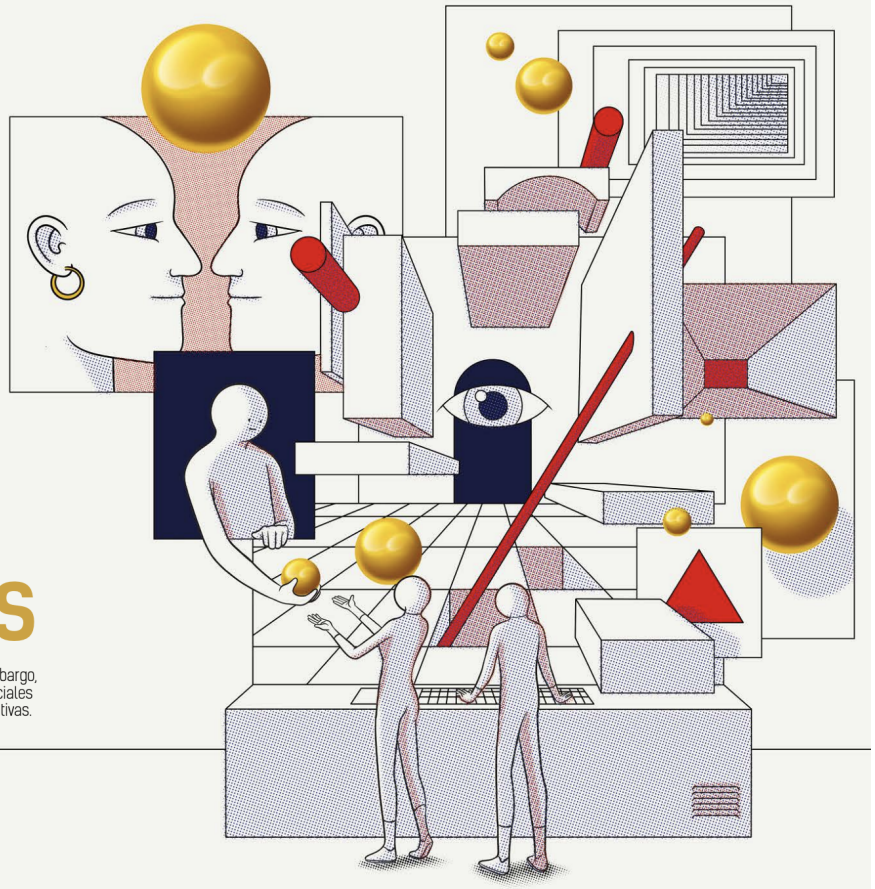
ELÍAS F. COMBARRO

Las verdaderas capacidades de los ordenadores cuánticos

COMPUTACIÓN CUÁNTICA:

MITOS Y REALIDADES

La computación cuántica es una tecnología llamada a transformar nuestra sociedad. Sin embargo, sus verdaderas capacidades son a menudo incomprendidas y mitificadas. Explicar las potenciales aplicaciones de los ordenadores cuánticos ayuda a disipar dudas y a desterrar falsas expectativas.



The true capabilities of quantum computers

QUANTUM COMPUTING: MYTHS AND REALITIES

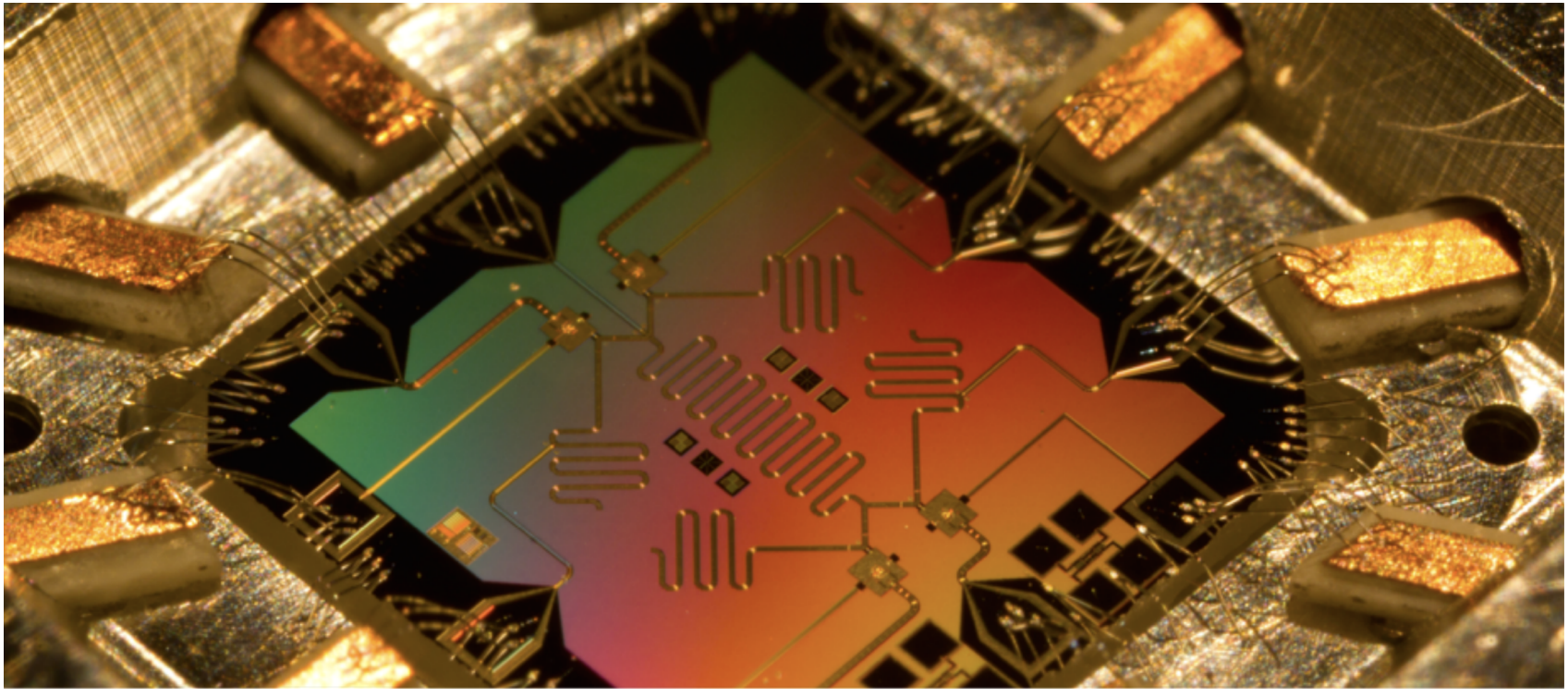
Quantum computing is a technology that is set to transform our society. However, its true capabilities are often misunderstood and mythologized. Explaining the potential applications of quantum computers helps to dispel doubts and banish false expectations.

Keywords: *quantum computing, quantum supremacy, quantum supremacy, cryptography, artificial intelligence, simulation.*

What is quantum computing?

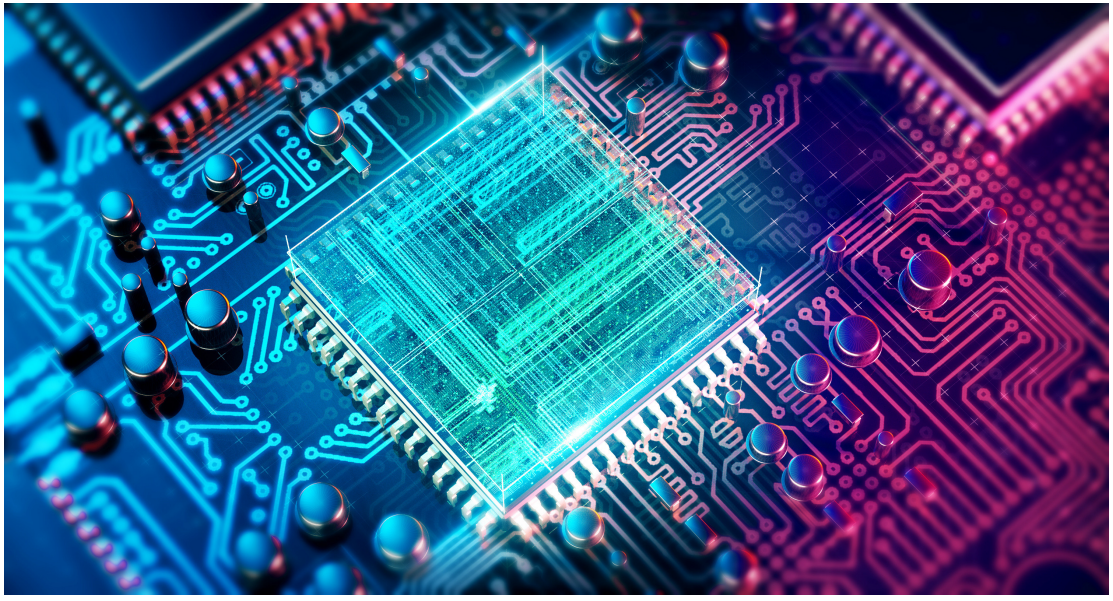
Quantum computing

Quantum computing is a computing paradigm that exploits quantum mechanical properties (superposition, entanglement, interference...) of matter in order to do calculations



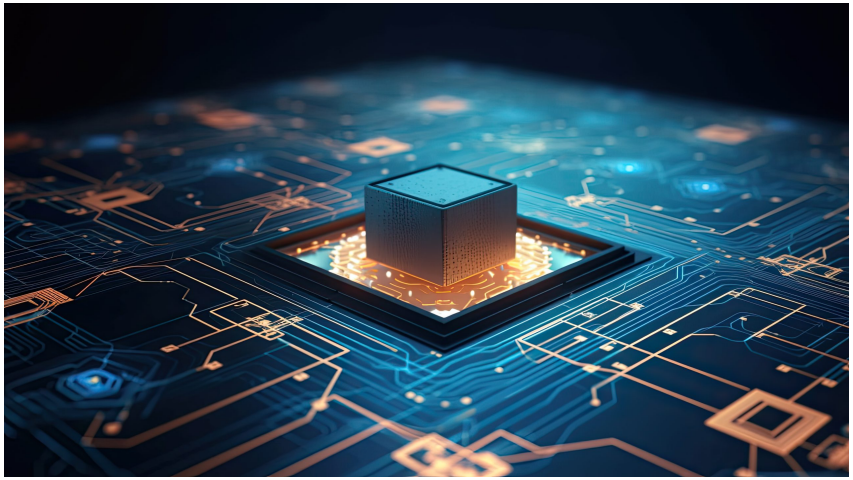
Models of quantum computing

- There are several models of quantum computing (they're all equivalent)
  - Quantum Turing machines
  - **Quantum circuits**
  - Measurement based quantum computing (MBQC)
  - Adiabatic quantum computing
  - Topological quantum computing
- Regarding their **computational capabilities**, they are equivalent to classical models (Turing machines)

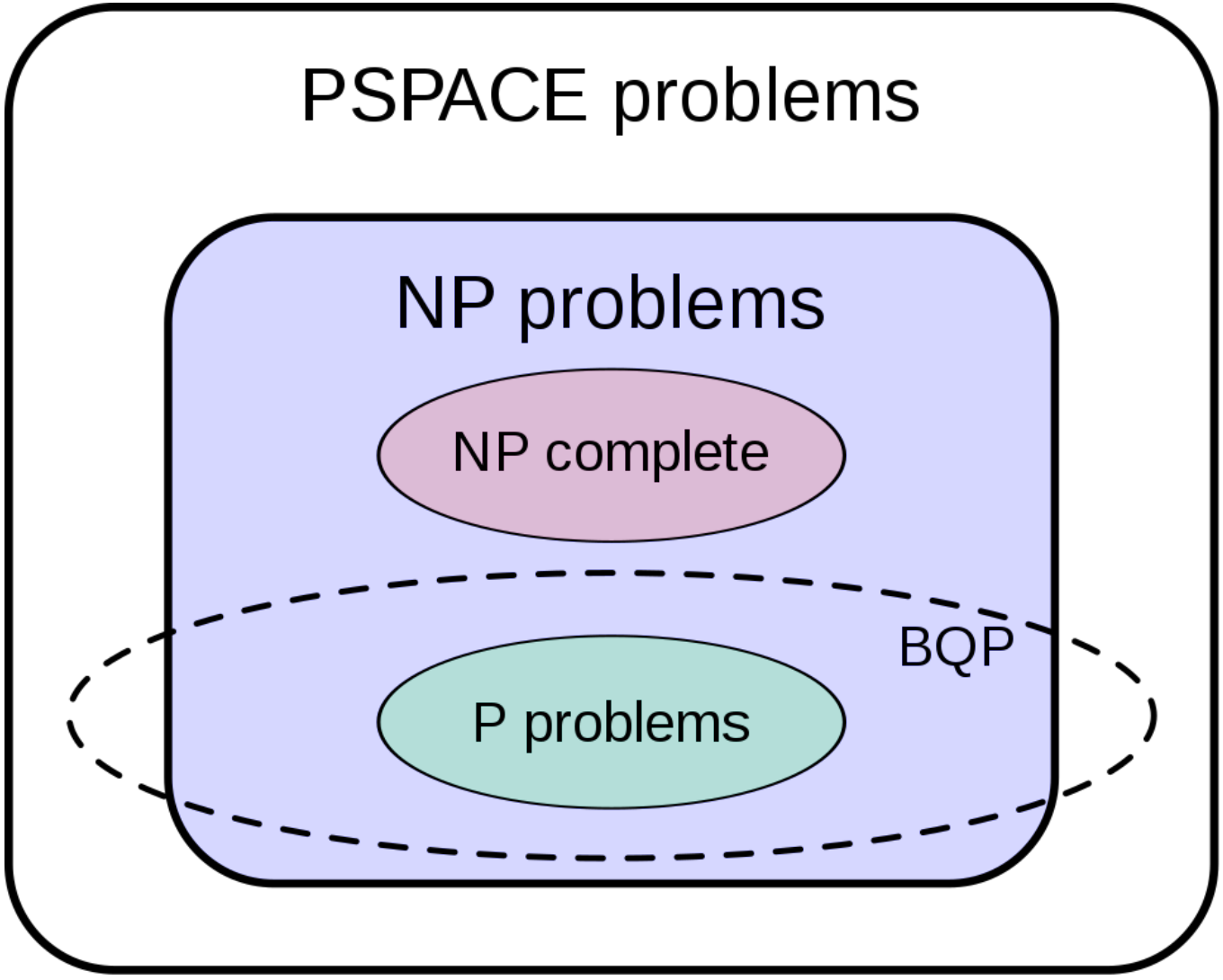


Applications of quantum computing

- Search problems (Grover's algorithm)
- Cryptography (Shor's algorithm, BB84)
- Linear systems of equations (HHL)
- Quantum Machine Learning
- Quantum Optimization
- Simulation
- ...



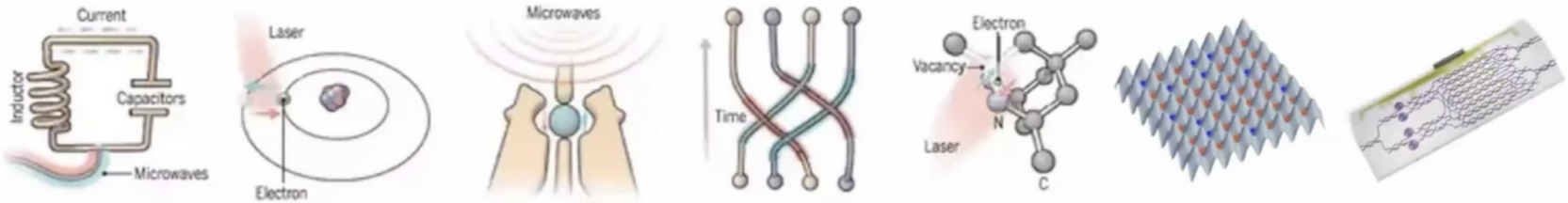
Quantum and classical computational complexity



What technologies are used to build quantum computers?

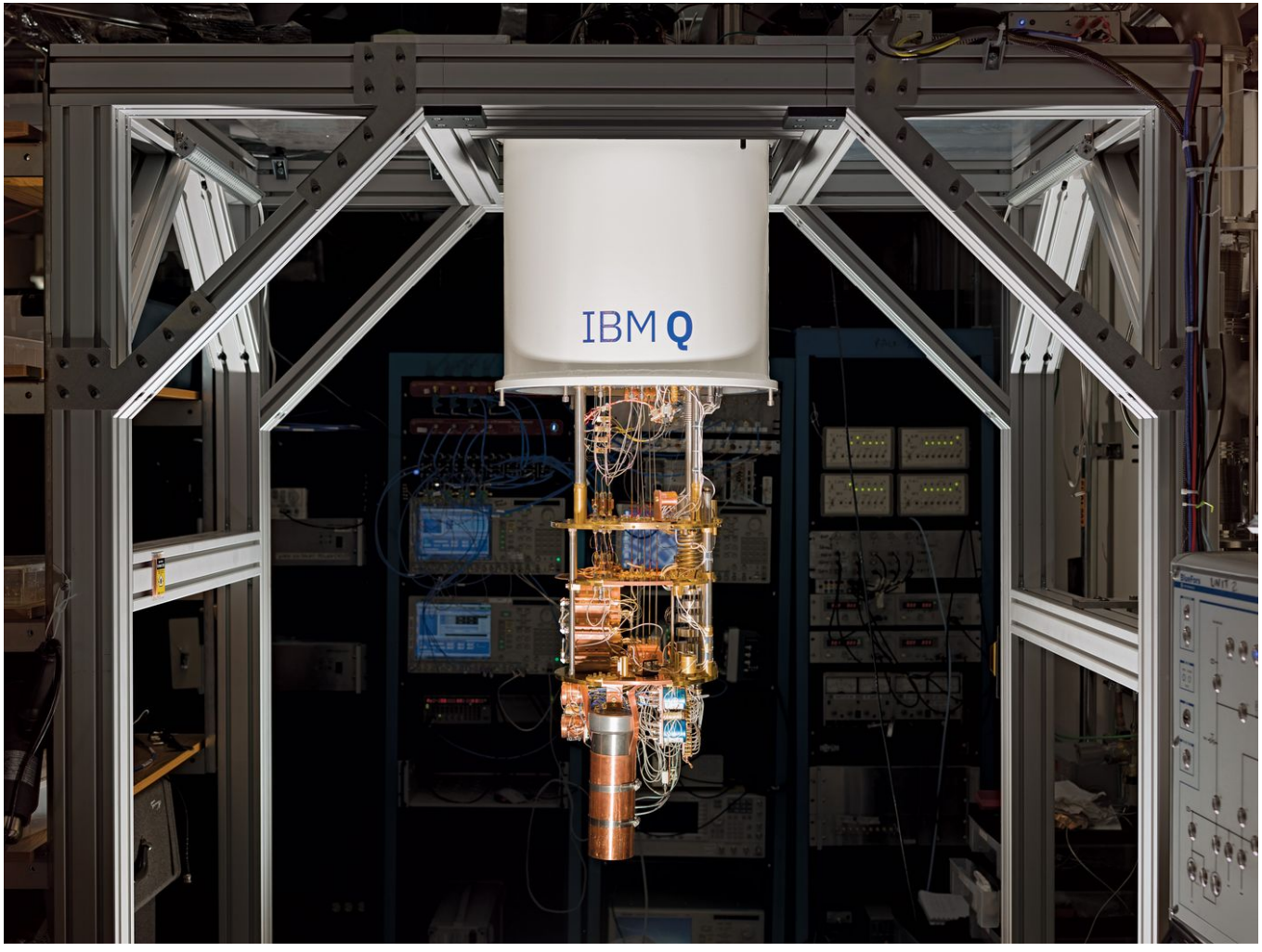
Quantum Technologies

Science, Dec 2016



	Superconducting loops	**Trapped ions**	**Silicon quantum dots**	**Topological qubits**	**Diamond vacancies**	**Neutral atoms**	**Photonics**
	A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into super-position states.	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 superposition states.	These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.	Quasiparticles can be seen in the behavior of electrons channeled through semi-conductor structures. Their braided paths can encode quantum information.	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.	Neutral atoms, like ions, store qubits within electronic states. Interactions through excitation to Rydberg states	Photonic qubits interact via linear elements
Longevity (seconds)	0.00005	>1000	0.03	N/A	10	1	
Logic success rate	99.4%	99.9%	~99%	N/A	99.2%	99%	
Number entangled	9	14	2	N/A	6	20	
Company support	Google, IBM, Rigetti, QCI	IonQ, Honeywell	Intel, HRL	Microsoft	Quantum Diamond Technologies	Atom Computing QuEra	PsiCorp, Xanadu
Pros	Fast working. Build on existing semiconductor industry.	Very stable. Highest achieved gate fidelities.	Stable. Build on existing semiconductor industry.	Greatly reduce errors.	Can operate at room temperature.	Many qubits, 2D and maybe 3D	Linear optical gates, integrated on-chip
Cons	Collapse easily and must be kept cold.	Slow operation. Many lasers are needed.	Only a few entangled. Must be kept cold.	Existence not yet confirmed.	Difficult to entangle.	Lasers needed, spaghetti physics, atoms escape	No memory, not clear how to scale

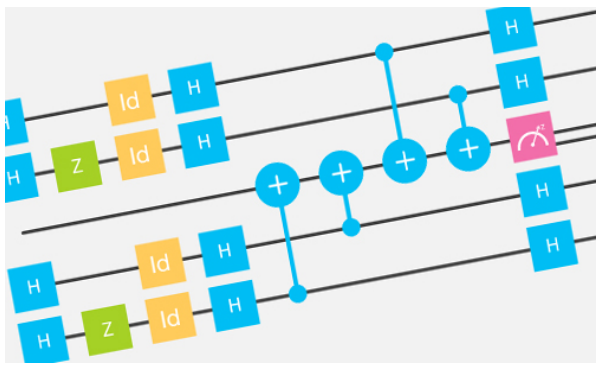
What is a quantum computer like?



The Sounds of IBM: IBM Q

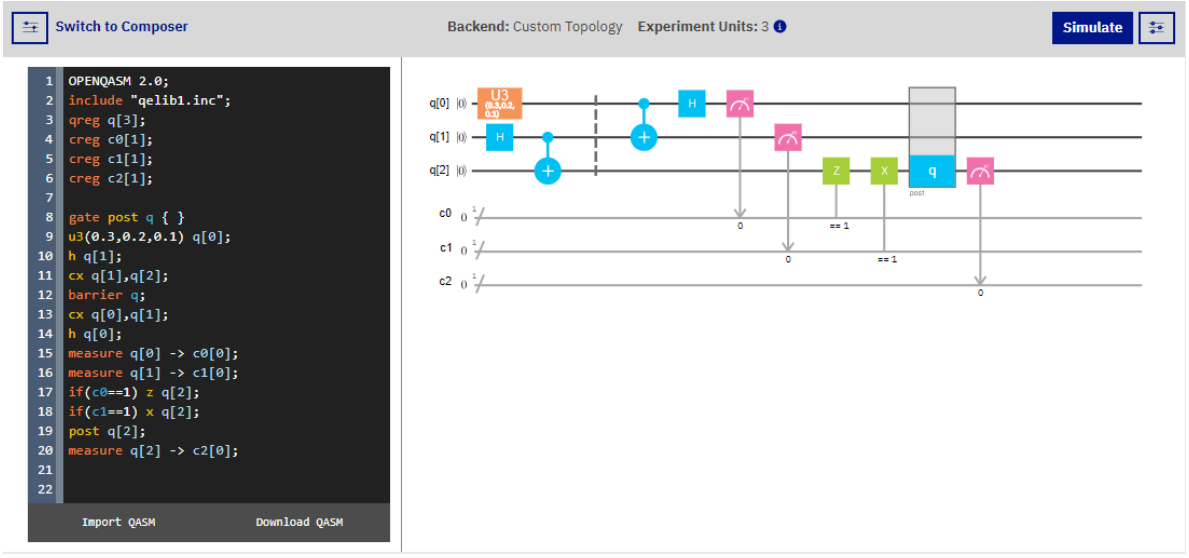
Tools and resources

- Jupyter Notebooks
  - Web application to create and execute notebooks that include code, images, text and formulas
  - They can be used locally (Anaconda, VS Code) or in the cloud (Google Colab...)
- IBM Quantum
  - Free access to **actual quantum computers** (127+ qubits)
  - Programmable with a visual interface and via different languages (Python, qasm)
  - https://quantum.ibm.com/
- Quirk
  - Online simulator (up to 16 qubits)
  - Lots of different gates and visualization options
  - http://algassert.com/quirk



Programming a quantum computer

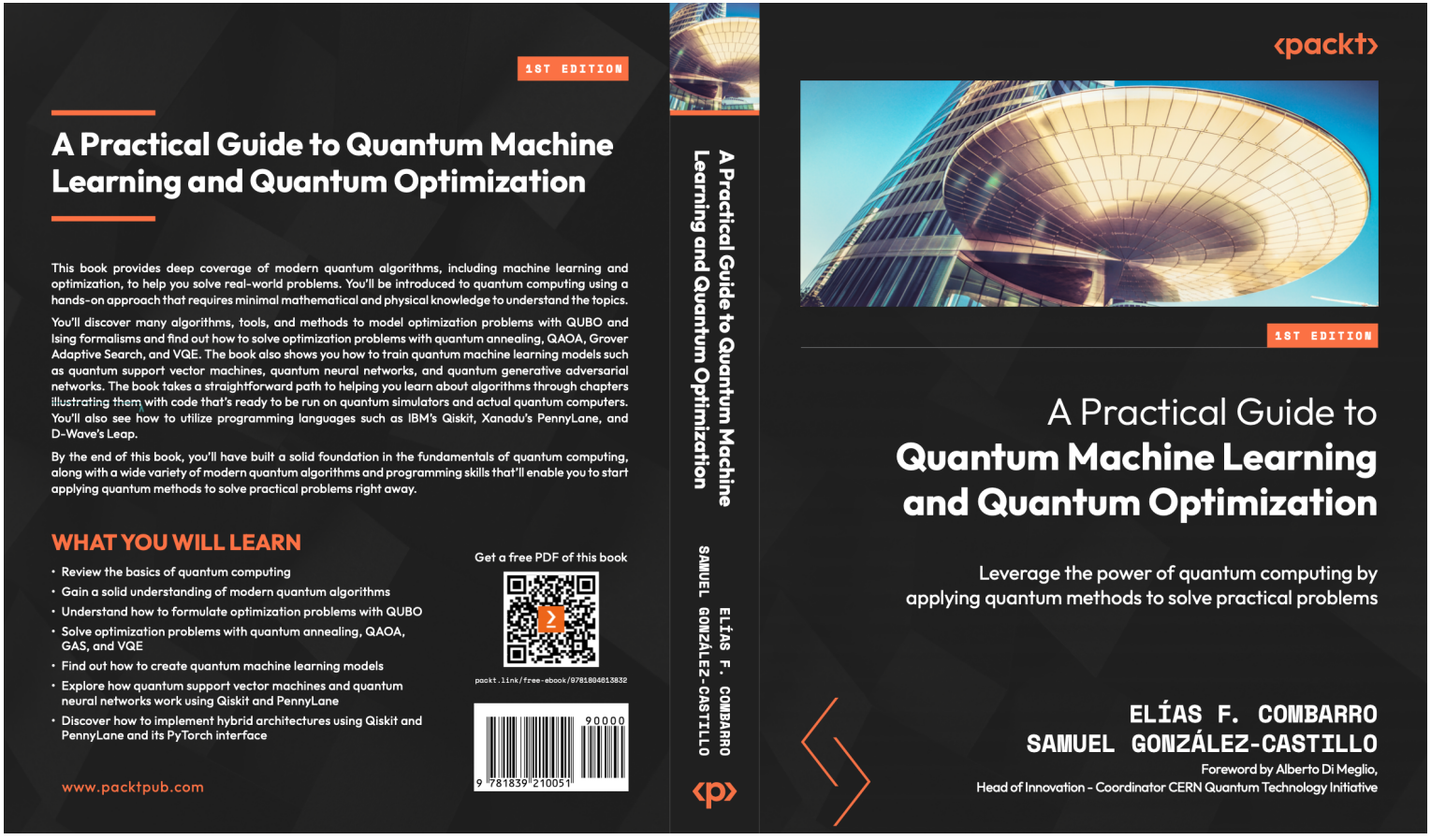
- Different frameworks and programming languages:
  - qasm
  - Qiskit (IBM)
  - Cirq (Google)
  - Forest/pyqil (Rigetti)
  - Q# (Microsoft)
  - Ocean (D-Wave)
  - ...
- Most of them for quantum circuit specification



What are the elements of a quantum circuit?

- Every computation has three elements: data, operations and results
- In quantum circuits:
  - Data = **qubits**
  - Operations = **quantum gates** (unitary transformations)
  - Results = **measurements**

To know more...


1ST EDITION
A Practical Guide to Quantum Machine Learning and Quantum Optimization
This book provides deep coverage of modern quantum algorithms, including machine learning and optimization, to help you solve real-world problems. You'll be introduced to quantum computing using a hands-on approach that requires minimal mathematical and physical knowledge to understand the topics.
You'll discover many algorithms, tools, and methods to model optimization problems with QUBO and Ising formalisms and find out how to solve optimization problems with quantum annealing, QAOA, Grover Adaptive Search, and VQE. The book also shows you how to train quantum machine learning models such as quantum support vector machines, quantum neural networks, and quantum generative adversarial networks. The book takes a straightforward path to helping you learn about algorithms through chapters illustrating them with code that's ready to be run on quantum simulators and actual quantum computers. You'll also see how to utilize programming languages such as IBM's Qiskit, Xanadu's PennyLane, and D-Wave's Leap.
By the end of this book, you'll have built a solid foundation in the fundamentals of quantum computing, along with a wide variety of modern quantum algorithms and programming skills that'll enable you to start applying quantum methods to solve practical problems right away.
WHAT YOU WILL LEARN
• Review the basics of quantum computing
• Gain a solid understanding of modern quantum algorithms
• Understand how to formulate optimization problems with QUBO
• Solve optimization problems with quantum annealing, QAOA, GAS, and VQE
• Find out how to create quantum machine learning models
• Explore how quantum support vector machines and quantum neural networks work using Qiskit and PennyLane
• Discover how to implement hybrid architectures using Qiskit and PennyLane and its PyTorch interface
Get a free PDF of this book
packt.link/free-ebook/9781804613832
9 781839 210051 90000
www.packtpub.com
A Practical Guide to Quantum Machine Learning and Quantum Optimization
ELÍAS F. COMBARRO
SAMUEL GONZÁLEZ-CASTILLO
<p>
<packt>
1ST EDITION
A Practical Guide to
Quantum Machine Learning
and Quantum Optimization
Leverage the power of quantum computing by applying quantum methods to solve practical problems
ELÍAS F. COMBARRO
SAMUEL GONZÁLEZ-CASTILLO
Foreword by Alberto Di Meglio,
Head of Innovation - Coordinator CERN Quantum Technology Initiative

Part II

One-qubit systems: one qubit to rule them all

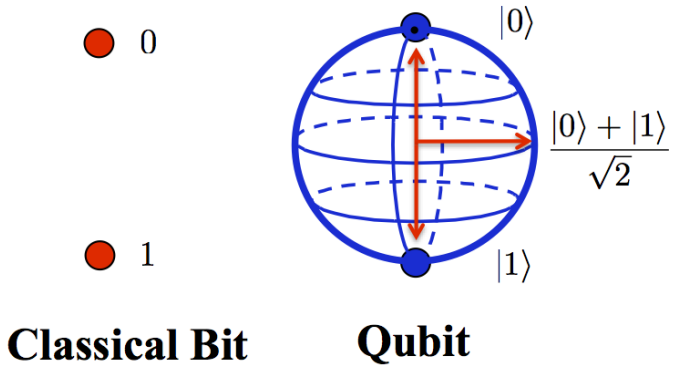
What is a qubit?

- A classical bit can take two different values (0 or 1). It is discrete.
- A qubit can “take” **infinitely** many different values. It is continuous.
- Qubits live in a **Hilbert vector space** with a basis of two elements that we denote $|0\rangle$ y $|1\rangle$.
- A generic qubit is in a **superposition**

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

where α and β are **complex numbers** such that

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



Measuring a qubit

- The way to know the value of a qubit is to perform a measurement. However
  - The result of the measurement is random
  - When we measure, we only obtain one (classical) bit of information
- If we measure the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ we get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.
- Moreover, the new state after the measurement will be $|0\rangle$ or $|1\rangle$ depending of the result we have obtained (wavefunction colapse)
- We cannot perform several independent measurements of $|\psi\rangle$ because we cannot copy the state (**no-cloning theorem**)

What are quantum gates?

- Quantum mechanics tells us that the evolution of an isolated state is given by the Schrödinger equation

$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

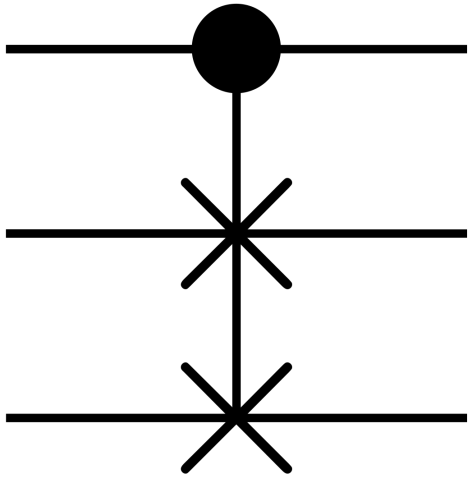
- In the case of quantum circuits, this implies that the operations that can be carried out are given by unitary matrices. That is, matrices U of complex numbers verifying

$$UU^\dagger = U^\dagger U = I$$

  where $U^\dagger$ is the conjugate transpose of U.
- Each such matrix is a possible quantum gate in a quantum circuit

Reversible computation

- As a consequence, all the operations have an inverse: **reversible computing**
- Every gate has the same number of inputs and outputs
- We cannot directly implement some classical gates such as *or*, *and*, *nand*, *xor*...
- But we can simulate any classical computation with small overhead
- Theoretically, we could compute without wasting energy (Landauer's principle, 1961)



One-qubit gates

- When we have just one qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, we usually represent it as a column vector $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$
- Then, a one-qubit gate can be identified with a matrix $U = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ that satisfies

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\overline{a} & \overline{c}\\ \overline{b} & \overline{d}\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

where $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ are the conjugates of complex numbers a, b, c, d.

Action of a one-qubit gate

- A state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is transformed into

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}$$

  that is, into the state $|\psi\rangle = (a\alpha + b\beta)\,|0\rangle + (c\alpha + d\beta)\,|1\rangle$

- Since U is unitary, it holds that

$$|(a\alpha + b\beta)|^2 + |(c\alpha + d\beta)|^2 = 1$$

The *X* or *NOT* gate

- The *X* gate is defined by the (unitary) matrix

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

- Its action (in quantum circuit notation) is

$$|0\rangle \; \boxed{X} \; |1\rangle$$

$$|1\rangle \; \boxed{X} \; |0\rangle$$

  that is, it acts like the classical *NOT* gate
- On a general qubit its action is

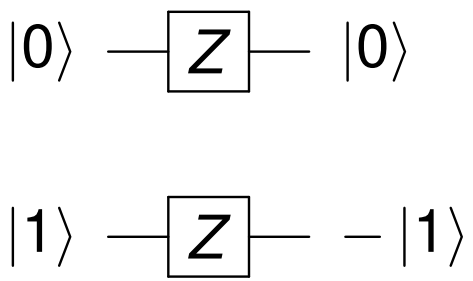
$$\alpha\,|0\rangle + \beta\,|1\rangle \; \boxed{X} \; \beta\,|0\rangle + \alpha\,|1\rangle$$

The Z gate

- The Z gate is defined by the (unitary) matrix

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

- Its action is



The H or Hadamard gate

- The H or Hadamard gate is defined by the (unitary) matrix

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

- Its action is

$$|0\rangle \;\text{—}\boxed{H}\text{—}\; \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$|1\rangle \;\text{—}\boxed{H}\text{—}\; \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- We usually denote

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

and

$$|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Other important gates

- Y gate

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- S gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

- T gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

- The gates X, Y and Z are also called, together with the identity, the Pauli gates. An alternative notation is σ_X, σ_Y, σ_Z.

The Bloch sphere

- A common way of representing the state of a qubit is by means of a point in the surface of the Bloch sphere
- If $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ we can find angles γ, δ, θ such that

$$\alpha = e^{i\gamma} \cos\frac{\theta}{2}$$

$$\beta = e^{i\delta} \sin\frac{\theta}{2}$$

- Since an overall phase is physically irrelevant, we can rewrite

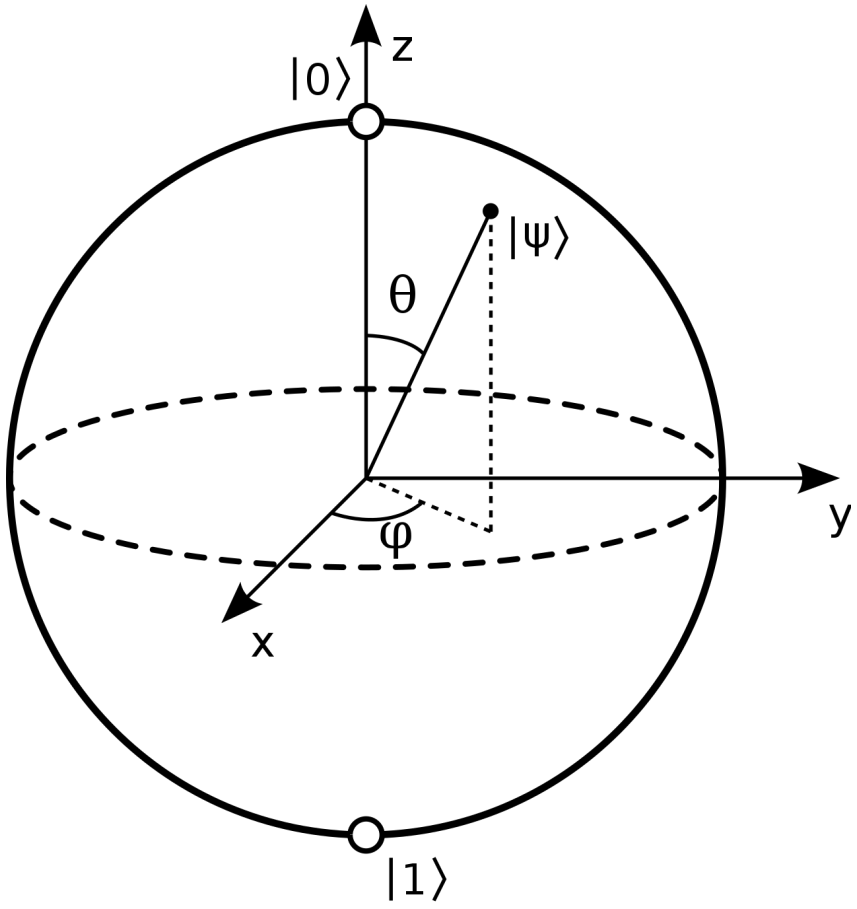
$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi} \sin\frac{\theta}{2}\,|1\rangle$$

with $0 \leq \theta \leq \pi$ and $0 \leq \varphi < 2\pi$.

The Bloch sphere (2)

- From $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ we can obtain spherical coordinates for a point in $\mathbb{R}^3$

$$(\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$



Rotation gates

- We can define the following rotation gates

$$R_X(\theta) = e^{-i\frac{\theta}{2}X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_Y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_Z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

- Notice that $R_X(\pi) \equiv X$, $R_Y(\pi) \equiv Y$, $R_Z(\pi) \equiv Z$, $R_Z(\frac{\pi}{2}) \equiv S$, $R_Z(\frac{\pi}{4}) \equiv T$

Using rotation gates to generate one-qubit gates

- For any one-qubit gate U there exist a unit vector $r = (r_x, r_y, r_z)$ and an angle θ such that

$$U \equiv e^{-i\frac{\theta}{2} r\cdot\sigma} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}(r_x X + r_y Y + r_z Z)$$

- For instance, choosing $\theta = \pi$ and $r = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ we can see that

$$H \equiv e^{-i\frac{\theta}{2} r\cdot\sigma} = -i\frac{1}{\sqrt{2}}(X + Z)$$

- Additionally, it can also be proved that there exist angles α, β and γ such that

$$U \equiv R_Z(\alpha) R_Y(\beta) R_Z(\gamma)$$

Inner product, Dirac's notation and Bloch sphere

- The inner product of two states $|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$ and $|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$ is given by

$$\langle\psi_1|\psi_2\rangle = \begin{pmatrix}\overline{\alpha_1} & \overline{\beta_1}\end{pmatrix} \begin{pmatrix}\alpha_2 \\ \beta_2\end{pmatrix} = \overline{\alpha_1}\alpha_2 + \overline{\beta_1}\beta_2$$

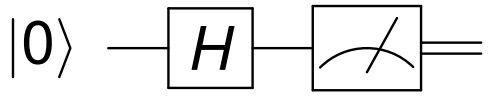
- Notice that $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$
- This allows us to compute

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= \left(\overline{\alpha_1}\langle 0| + \overline{\beta_1}\langle 1|\right)\left(\alpha_2|0\rangle + \beta_2|1\rangle\right) \\ &= \overline{\alpha_1}\alpha_2\langle 0|0\rangle + \overline{\alpha_1}\beta_2\langle 0|1\rangle + \overline{\beta_1}\alpha_2\langle 1|0\rangle + \overline{\beta_1}\beta_2\langle 1|1\rangle \\ &= \overline{\alpha_1}\alpha_2 + \overline{\beta_1}\beta_2\end{aligned}$$

- Orthogonal states are antipodal on the Bloch sphere

Hello, quantum world!

- Our very first quantum circuit!



- After applying the H gate the qubit state is

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

- When we measure, we obtain 0 or 1, each with 50% probability: we have a circuit that generates perfectly uniform random bits!

Part III

Quantum money: crime does not pay

The concept of quantum money

- Proposed by Wiesner circa 1970
- Published in 1983
- Formal security proof in 2013
- Impossible to forge

Quantum banknotes

- A quantum banknote has:
  - A (public) serial number. It's just a bit string.
  - A key (secret, kept by the issuing bank). Another bit string.
  - A quantum register with several qubits (inside the banknote)
- Example:
  - Serial number: 123456789
  - Key: $0-1++1100-$
  - Qubits: $|0\rangle\,|-\rangle\,|1\rangle\,|+\rangle\,|+\rangle\,|1\rangle\,|1\rangle\,|0\rangle\,|0\rangle\,|-\rangle$

Checking a quantum banknote

- The bank can always check if a banknote is legit
- With the serial number, they retrieve the key
- If in a certain position of the key there is:
  - 0 or 1: they measure the qubit and check the result
  - $+$ or $-$: they first apply a H gate and then measure the qubit. For $+$ they should obtain 0 and for $-$ they should obtain 1
- If the banknote is valid, it will pass the test 100% of the times
- If there is a random value in one of the qubits, there is a 50% chance of detecting it

Trying to forge a banknote

- Choosing states at random is not viable:
  - With 10 qubits, the probability of passing the test is under 0.01%
  - With 20 qubits, it is under 0.00001%
- Copying the states is NOT possible (no-cloning theorem)
- A different strategy:
  - Decide at random if H should be applied or not. Measure. Copy the result.
  - The probability of being detected is 25% per qubit:
    - 50% of getting the basis right (will pass the test)
    - If the basis is not right, 50% chance of being detected
  - The uncertainty principle is at work here
- It can be formally proved that no other strategy can work