Quantum Computing

Introduction to quantum algorithms with PennyLane

André Sequeira
HASLab, INESC TEC
Department of Informatics, University of Minho
andre.m.sequeira@inesctec.pt

INESCTEC

Universidade do Minho

Quantum programming languages?

In these classes, we use quantum software development kits.

- SDKs usually provide Python or C++ interfaces.
- Classical instructions build quantum circuits.
- The same workflow connects simulation with hardware execution.

Our toolkit: PennyLane.

Quantum companies and software kits

Company	Software
IBM	**Qiskit**
Google	**Cirq**
QunaSys	**Qulacs**
Xanadu	**PennyLane**, Strawberry Fields
Quandela	**Perceval** photonic computing
Quantinuum	**TKET / pytket**

Selected companies and frameworks. Frameworks can support multiple hardware providers.
Official documentation: Qiskit, Cirq, Qulacs, PennyLane, Strawberry Fields, Perceval, TKET.

A wider ecosystem

Quantum processors

IBM, Google, Rigetti, IQM, IonQ, Quantinuum, QuEra, Pasqal, Xanadu, Quandela

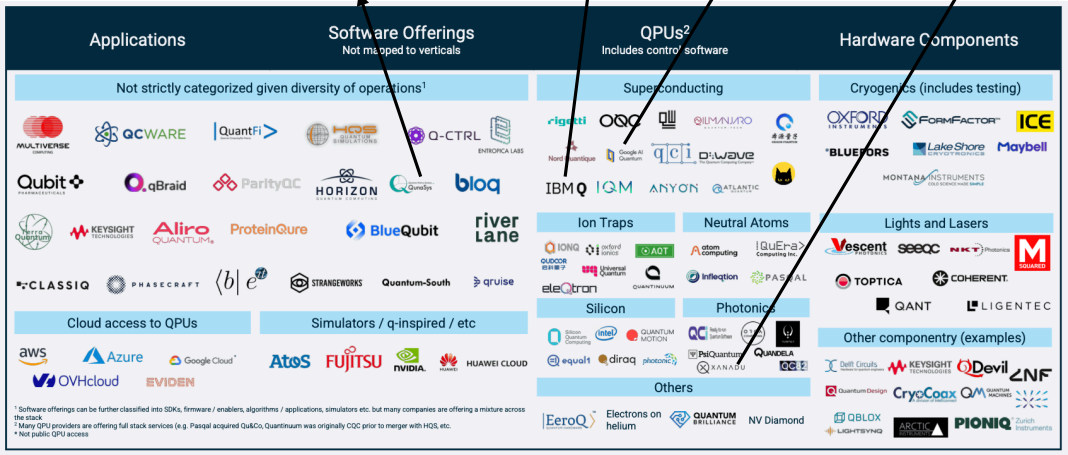
Cloud access

AWS, Microsoft Azure, Google Cloud

Enabling technologies

Control electronics, cryogenics, lasers and simulation tools

Quantum technology companies



The unit of quantum information

What is a qubit?

The classical bit

The unit of information in a classical computer.

$$0 \quad \text{or} \quad 1$$

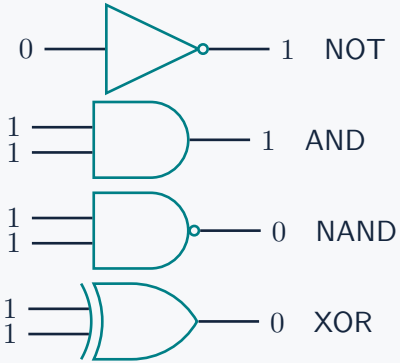
A bit has one of two possible values.

Classical logic gates

How do we manipulate bits?

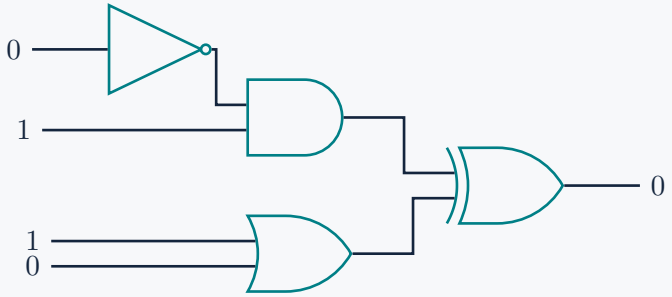
Logic gates map input bits to output bits.

NAND alone forms a universal gate set for classical computation.



A deterministic classical circuit

A fixed input produces a fixed output.



$$\big((\neg 0) \wedge 1\big) \oplus (1 \vee 0) = 1 \oplus 1 = 0$$

Bits and qubits

Classical bit

The unit of information in a classical computer.

$$0 \quad \text{or} \quad 1$$

Classical logic gates act

deterministically.

Quantum bit

The unit of information in a quantum computer.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

But a qubit can be more than a basis state.

A qubit is a linear combination

Classical bit

0 or 1

Computational basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

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

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

A superposition of the two basis states.

Quantum measurement is probabilistic

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

At the end of a computation, measurement returns a classical outcome.

For one qubit, the computational-basis outcome is 0 or 1.

Is a qubit just a probabilistic bit?

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

Quantum measurement produces probabilistic outcomes.

Does that make a qubit equivalent to a classical random bit?

Complex amplitudes can interfere

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad \alpha, \beta \in \mathbb{C}$$

A qubit carries complex amplitudes.

Amplitudes can reinforce or cancel one another before measurement.

This interference is the key distinction from a classical random bit.

Amplitudes determine probabilities

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

$$\alpha, \beta \in \mathbb{C}$$

Computational-basis measurement

$$P_{|0\rangle} = |\alpha|^2, \qquad P_{|1\rangle} = |\beta|^2$$

$$P_{|0\rangle} + P_{|1\rangle} = 1$$

Do the two probabilities always add up to one?

A valid qubit has unit norm

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

$$\alpha, \beta \in \mathbb{C}$$

Computational-basis measurement

$$P_{|0\rangle} = |\alpha|^2, \qquad P_{|1\rangle} = |\beta|^2$$

$$P_{|0\rangle} + P_{|1\rangle} = 1$$

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad \boxed{|\alpha|^2 + |\beta|^2 = 1}$$

A normalized complex vector yields a classical bit with probabilities $|\alpha|^2$ and $|\beta|^2$.

How do we manipulate a qubit?

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

$$\alpha, \beta \in \mathbb{C}$$

Computational-basis measurement

$$P_{|0\rangle} = |\alpha|^2, \qquad P_{|1\rangle} = |\beta|^2$$

$$P_{|0\rangle} + P_{|1\rangle} = 1$$

Quantum logic gates must preserve valid quantum states.

Quantum gates preserve vector length

A gate must preserve normalization.

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

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \longmapsto \quad |\psi'\rangle = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}$$

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

Unitary matrices are quantum gates

Unitary transformations preserve the norm of a state.

$$\boxed{U^\dagger U = I}$$

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

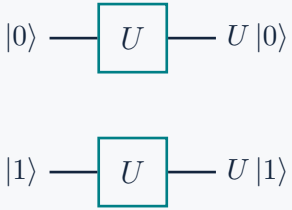
$U^\dagger$ is the conjugate transpose of U.

Matrices and circuit notation

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad U^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}, \qquad U^\dagger U = I$$

Quantum gates compose into quantum circuits.

Each wire represents a qubit.



Gates act linearly on superpositions



$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \qquad U = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

$$|\psi'\rangle = U|\psi\rangle = U\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = U\begin{pmatrix}\alpha\\ 0\end{pmatrix} + U\begin{pmatrix}0\\ \beta\end{pmatrix}$$

$$= \alpha U|0\rangle + \beta U|1\rangle = \begin{pmatrix}a\alpha + b\beta\\ c\alpha + d\beta\end{pmatrix} = \begin{pmatrix}\alpha'\\ \beta'\end{pmatrix}.$$

U acts on each term of the superposition.

Exercise: valid quantum gates

Verify whether each matrix is unitary.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Compute the conjugate transpose and check $U^\dagger U = I$.

Solution: all three matrices are unitary

$$A = A^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad AA^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$B = B^\dagger = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad BB^\dagger = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$C = C^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad CC^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I.$$

Each matrix is also Hermitian: $U = U^\dagger$.

The Pauli gates

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



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



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



The Pauli matrices X, Y and Z are single-qubit gates.

Exercise: Pauli gates on basis states

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



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



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



What does each gate do to $|0\rangle$ and $|1\rangle$?

Use matrix-vector multiplication for all six cases.

How the Pauli gates act

X	$X\|0\rangle = \|1\rangle$	$X\|1\rangle = \|0\rangle$	Bit flip (NOT)
Y	$Y\|0\rangle = i\|1\rangle$	$Y\|1\rangle = -i\|0\rangle$	Bit flip with complex phases
Z	$Z\|0\rangle = \|0\rangle$	$Z\|1\rangle = -\|1\rangle$	Phase flip on $\|1\rangle$

Z changes the relative phase of a superposition.

What about this matrix?

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

Are its columns orthogonal? Is $M^\dagger M = I$?

$$M^\dagger M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \neq I$$

Changing one sign gives the Hadamard gate.

The Hadamard gate

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

$$H = H^\dagger, \qquad HH^\dagger = I$$



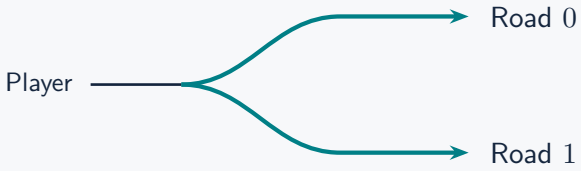
$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

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

Hadamard creates superpositions from computational-basis states.

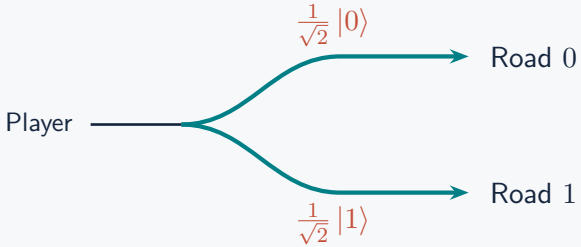
Two roads in a game

Imagine your favourite game character choosing a road.



A classical player tests one road at a time.

A superposition of the two roads



Hadamard assigns an amplitude to each road in the metaphor.

Is a superposition enough to find the correct road?

Superposition alone is not enough

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

$$P(0) = P(1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

If only one road is correct, measurement succeeds with probability $1/2$.

Exercise: the H–Z–H circuit



Compute the state after each gate.

What outcome will a computational-basis measurement return?

First create a superposition, then a phase flip

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

$$Z\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

The probabilities are unchanged. The relative phase has changed.

The final Hadamard produces interference

$$
\begin{aligned}
H\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) &= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] \\
&\quad - \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\
&= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle - \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle \\
&= |1\rangle\,.
\end{aligned}
$$

Amplitudes cancel and reinforce



Amplitude of $|0\rangle$

$$\frac{1}{2} - \frac{1}{2} = 0$$

Amplitude of $|1\rangle$

$$\frac{1}{2} + \frac{1}{2} = 1$$

In the road metaphor, the phase operation marks a route and interference changes the final probabilities.

The marking rule must be supplied by the problem. The circuit does not discover it for free.

A recurring pattern in quantum algorithms



Superposition

Manipulation of amplitudes and phases

Interference

Arrange interference so that useful answers become more likely.

Our gate set so far

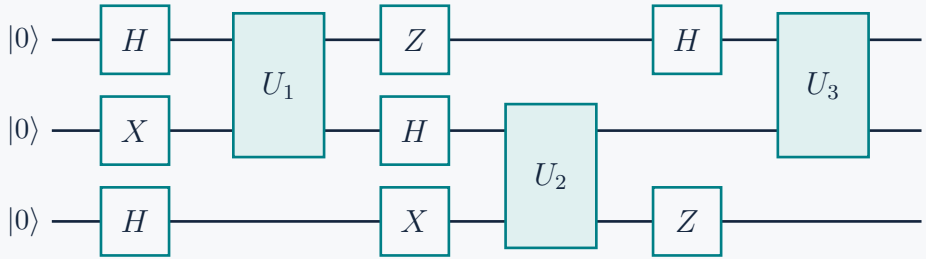
$$\{H, X, Y, Z\}$$

Is this enough?

So far, every gate acts on one qubit.

Beyond single-qubit gates

Combine single-qubit gates with gates that couple two qubits.



U_1, U_2, U_3: generic two-qubit unitary gates.

Each large box acts jointly on the two wires it spans. Read the circuit from left to right.