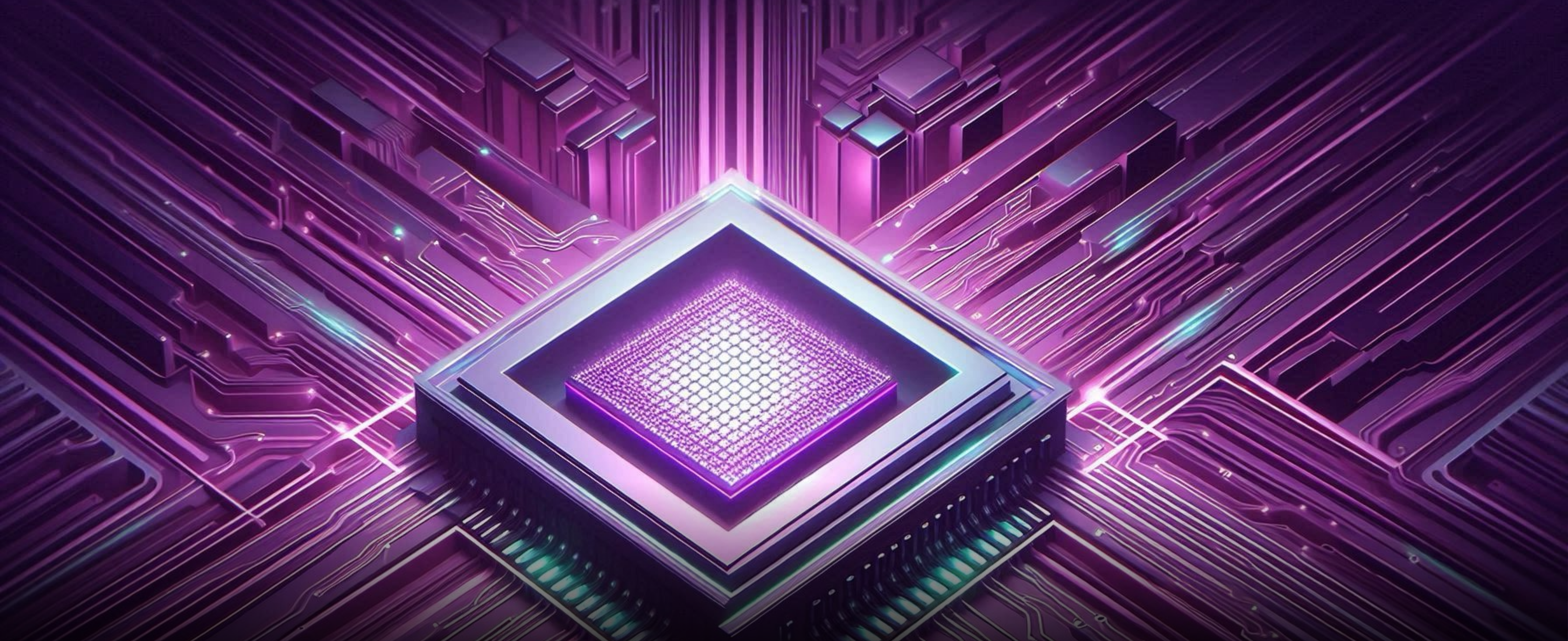


QUANTUM COMPUTING

Gabriele Gabrielli

28 February 2025 – Credit Decision @ Qred

1980s: Theoretical foundations proposed by Richard Feynman and David Deutsch

1998: First 2-qubit quantum computer

2016: IBM makes 5-qubit quantum computer accessible via cloud

2019: Google 53-qubit

2021: IBM 127-qubit

2022: IBM 433-qubit

2023: IBM 1,121-qubit

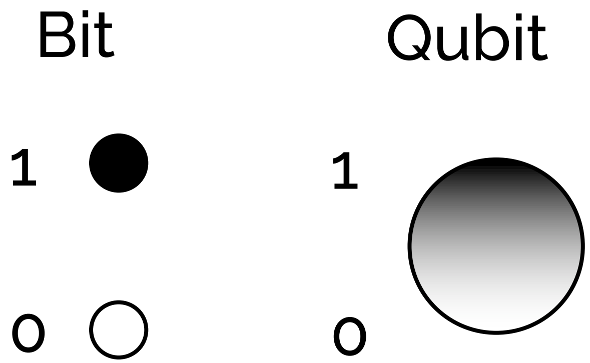
December 2024: Google's Willow: 105-qubit with error correction

February 2025: Microsoft's Majorana 1: first topological processor

2027: IBM 10.000-qubit

QUBIT

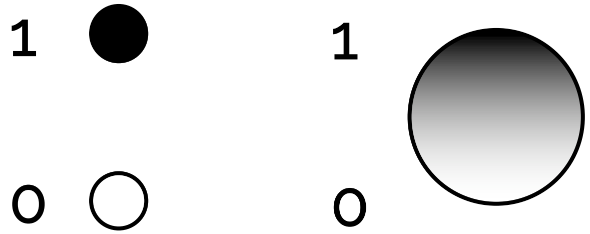
Oversimplified
definition:



QUBIT

Oversimplified definition:

Bit Qubit



State superposition:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{where } |\alpha|^2 + |\beta|^2 = 1$$

Entanglement:

$$|\psi\Phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

COMPUTATION

Initialization of the qubits

Entanglement

Actual computation with Quantum Circuits - Unitary Operations

Measurement (superposition collapse)

Error correction

COMPUTATION

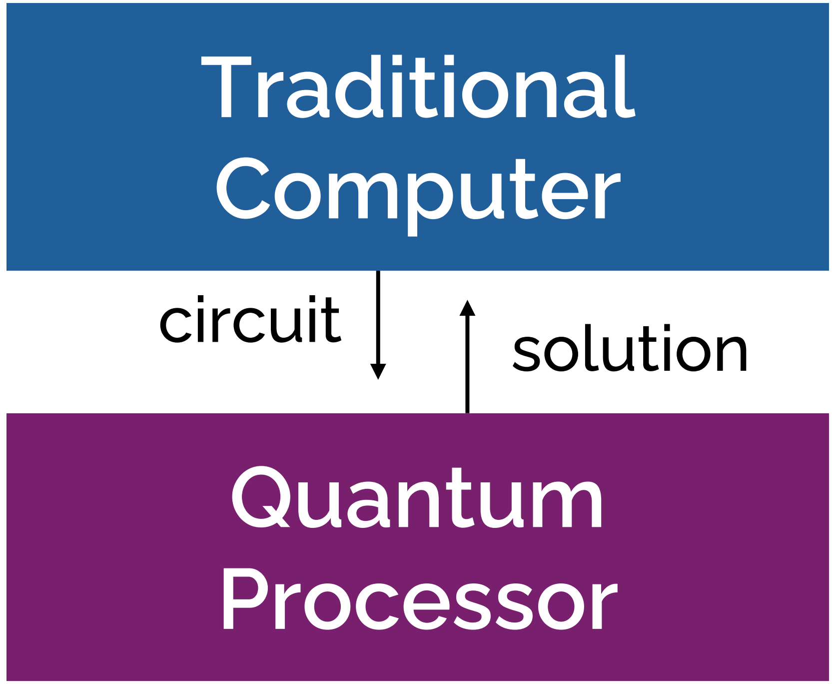
Initialization of the qubits

Entanglement

Actual computation with Quantum Circuits - Unitary Operations

Measurement (superposition collapse)

Error correction



COMPUTATION

Goal of the quantum algorithm (implemented in the circuit): make the probability of the solution state as high as possible.

$$|\psi\rangle = p_1|00000000\rangle + p_2\,|00000001\rangle + \ldots + p_{solution}\,|00101110\rangle + \ldots + p_{256}\,|11111111\rangle$$

When the measurement occurs, the qubits will *likely* assume the value of the solution.

This *likely* is mildly ‘enforced’ by error correction.

COMPUTATION

The only operations allowed in quantum circuits are the unitary operations.

Unitary operations are matrices applied to the vector of the probability amplitudes of one or more entangled qubits.

A matrix is unitary if its inverse is equal to its conjugate transposed.

Operator	**Gate(s)**		**Matrix**
Pauli-X (X)	$\boxed{X}$	$\oplus$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
Pauli-Y (Y)	$\boxed{Y}$		$\begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$
Pauli-Z (Z)	$\boxed{Z}$		$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$
Hadamard (H)	$\boxed{H}$		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$
Phase (S, P)	$\boxed{S}$		$\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$
$\pi/8$ (T)	$\boxed{T}$		$\begin{bmatrix}1 & 0\\0 & e^{i\pi/4}\end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$
Controlled Z (CZ)	$\boxed{Z}$		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$
SWAP			$\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$

DEMO

Logic AND gate

~

Quantum Toffoli gate

CLASSIC ALGORITHMS

Classic algorithms theory measure the efficiency by counting the number of operations to get a certificate verification for a certain problem.

Possible Solution → Algorithm → Certificate

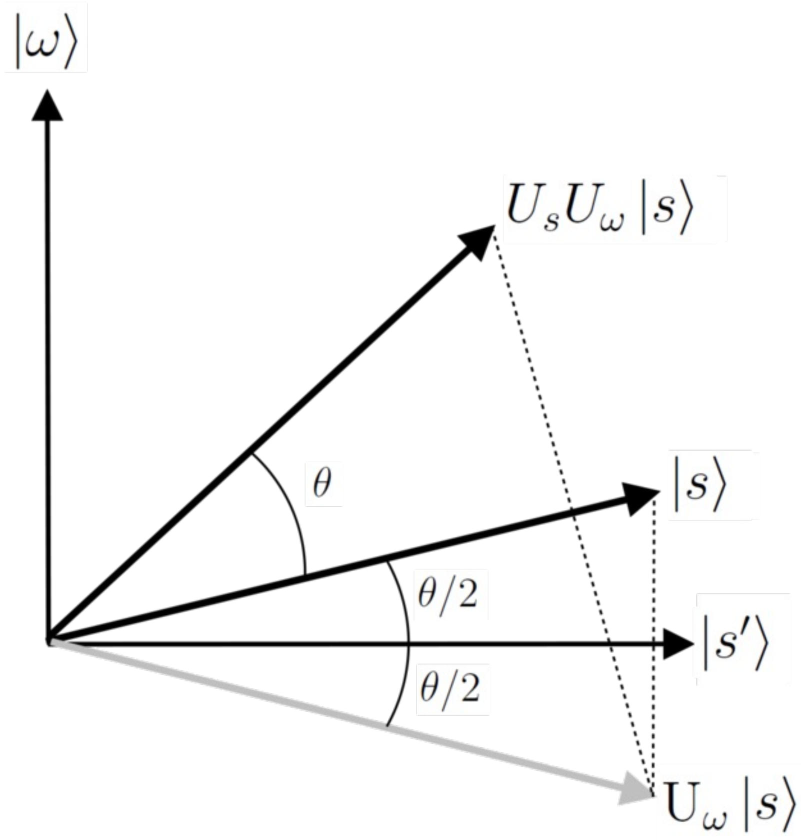
Verification is usually easier (i.e. less computationally expensive) than the solving procedure.

GROVER ALGORITHM

The classic algorithm (providing verification certificate) must be converted into a quantum circuit.

The qubits must be enaugh to represent the total space of solutions. That is, each state in the superposition is a different possible solution.

The grover algorithm circuit apply the verificaton circuit to the whole solution space, rising the probability for that state.



GROVER ALGORITHM

Grover Algorithm uses **quantum parallelization** to apply the validation certificate algorithm to all the possible solution.

$$|\psi\rangle = p_1|00000000\rangle + p_2\,|00000001\rangle + \ldots + p_{solution}\,|00101110\rangle + \ldots + p_{256}\,|11111111\rangle$$

Using Grover Algorithm, the new complexity is the square root of the original complexity. One year of classic computation last than 2 minutes in quantum computation.