Quantum gates

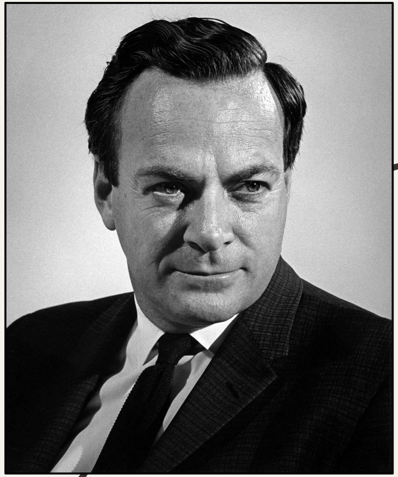
Anna Cristina Cavallari Inacio

Table of contents

01
Introduction

How quantum computing came to be

- **Paul Benioff,** published a paper describing a quantum model of the Turing machine
- **Richard Feynman,** proposes the existence of a quantum computer
- Several teams of researchers starting developing quantum computers (Bell labs, Nasa, IBM, Google)
- Quantum supremacy: **Google IA** and its 54 qubit bits QPU



02
Quantum bits

Classic bits

- Binary digit that is the fundamental state for storing information
- Assumes the value **0 or 1**
- Transformed by logic gates

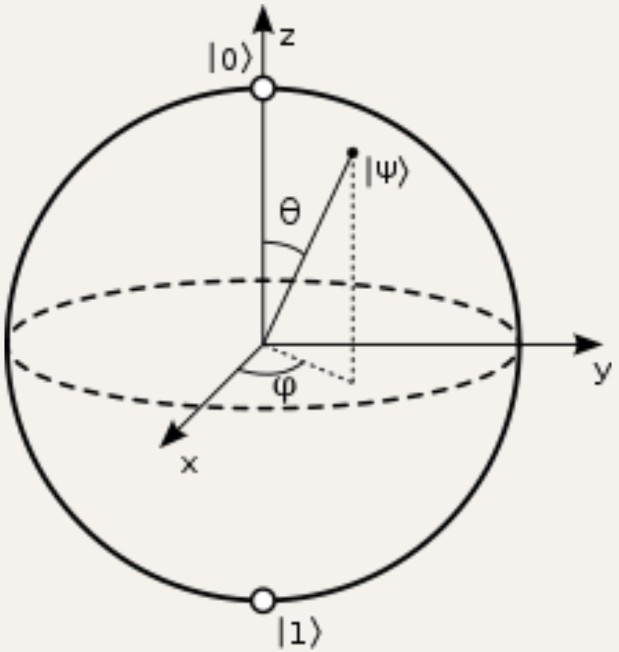
- **NOT:** flips the state of the bit, changing 0 to 1 and 1 to 0
- **OR:** returns 1 if one of the entries is equal to 1
- **AND:** returns 1 only if both entries are equal to the value 1

Quantum bits: Qubits

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

- The state of a qubit is a vector in a two-dimensional complex vector space
- the states are computational basis states that form an orthonormal basis for this vector space

Bloch sphere representation

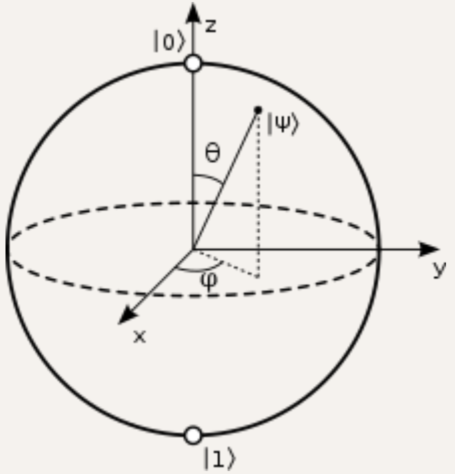


$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + \exp i\varphi \sin\frac{\theta}{2}\,|1\rangle$$

Measurement

- We must determine the alignment of its spin with respect to the z-axis
- The result of a measuring is a probability

$$|\alpha|^2 \qquad |\beta|^2$$



03
Quantum gates

Quantum gates

- Quantum gates are **unitary operators** described as unitary matrices relative to some basis.

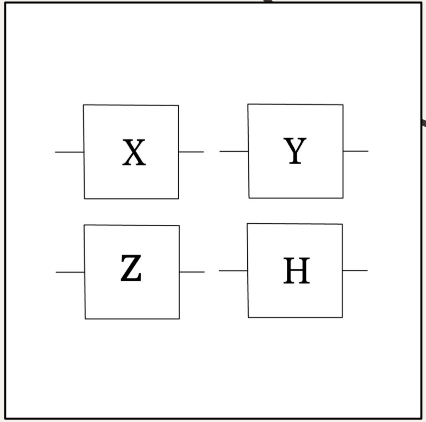
$$U^{\dagger} |\psi_f\rangle = U^{\dagger}U = |\psi_i\rangle$$

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

- We can undo a gate using the output qubit to obtain the initial one

Single qubit logic gates

$$Basis : \{|0\rangle, |1\rangle\}$$



Pauli gates

- X gate or quantum NOT gate
- It "negates" the computational basis states

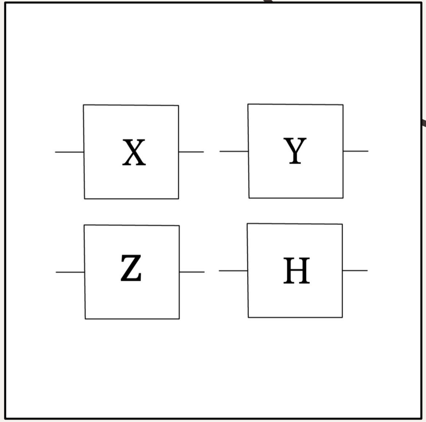
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

Single qubit logic gates

$$Basis : \{|0\rangle, |1\rangle\}$$

Pauli gates



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

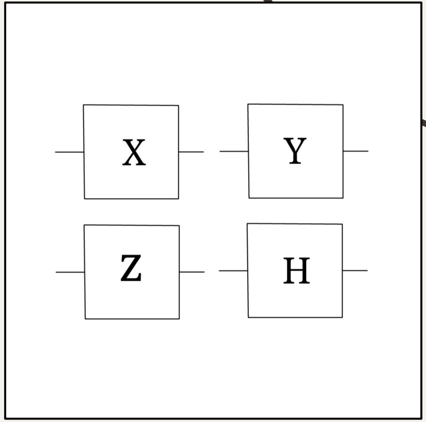
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$Y|\psi\rangle = i\alpha|1\rangle - i\beta|0\rangle$$

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

Single qubit logic gates

$$Basis : \{|0\rangle, |1\rangle\}$$



Hadarmad gate

- Transforms the computational basis into a superposition state

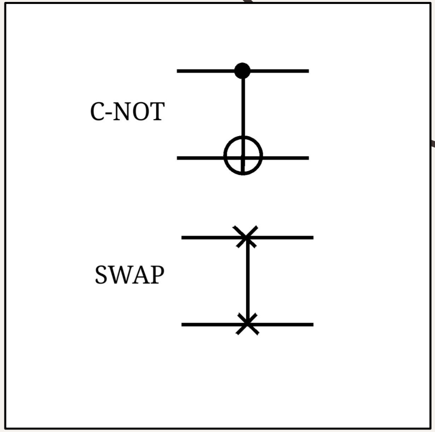
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

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

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Two-qubit logic gates

$$Basis : \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$



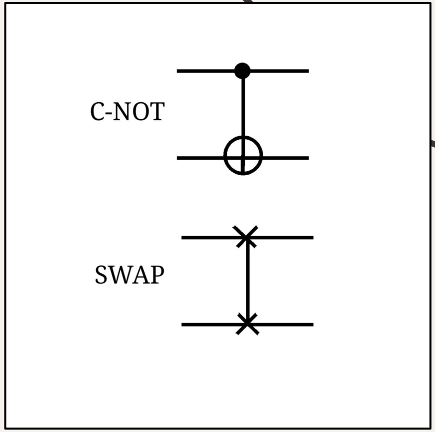
Controlled-NOT gate

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$U_{CNOT} : |00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, \\ |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |10\rangle$$

Two-qubit logic gates

$$Basis : \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$



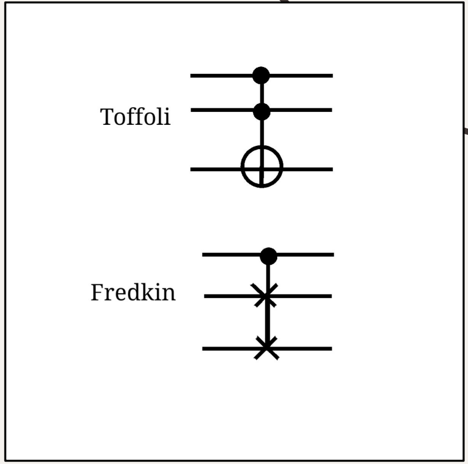
SWAP gate

$$U_{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_{SWAP} \, |\psi_1, \psi_2\rangle = |\psi_2, \psi_1\rangle$$

Three-qubit logic gates

$$Basis : \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

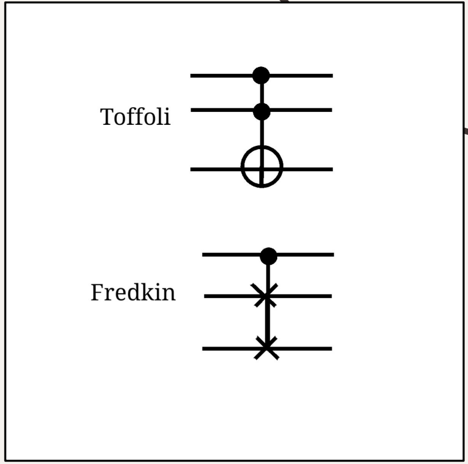


Toffoli gate

$$U_{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Three-qubit logic gates

$$Basis : \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$



Fredkin gate

$$U_{CSWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

04
Quantum circuits

Series

- If several gates act upon the **same subset of qubits**, then those gates must be applied sequentially

$$C \bullet B \bullet A$$

Parallel

- If adjacent gates act on **independent subsets of the qubits,** those gates are applied simultaneously in parallel

$$A \otimes B$$

$$\mathbb{I}_{2^i} \otimes U \otimes \mathbb{I}_{2^k}$$

Conditionally

- If a subset of qubits **controls what gate is to be applied** to some other subset, the gates are applied conditionally

$$A \oplus B$$

Complexity of quantum circuits

- It can be characterized in: **width, size, and length**

- For a quantum circuit to be considered efficient in performing a computation, any of the complexity parameters has to only grow as a **polynomial function**

- For quantum computing advance, the complexity needed to achieve some computation must be significantly less than the need to achieve the same computation classically

05
Final considerations

Final considerations

- Understanding quantum gates is really important for comprehending more complexes subjects in the area
- Quantum gates are also used in quantum information and cryptography
- There are other challenges in building quantum computers besides thinking about algorithms and logic circuits, such as designing efficient hardware.

Appendix

Quantum computer hardware

Quantum computer hardware