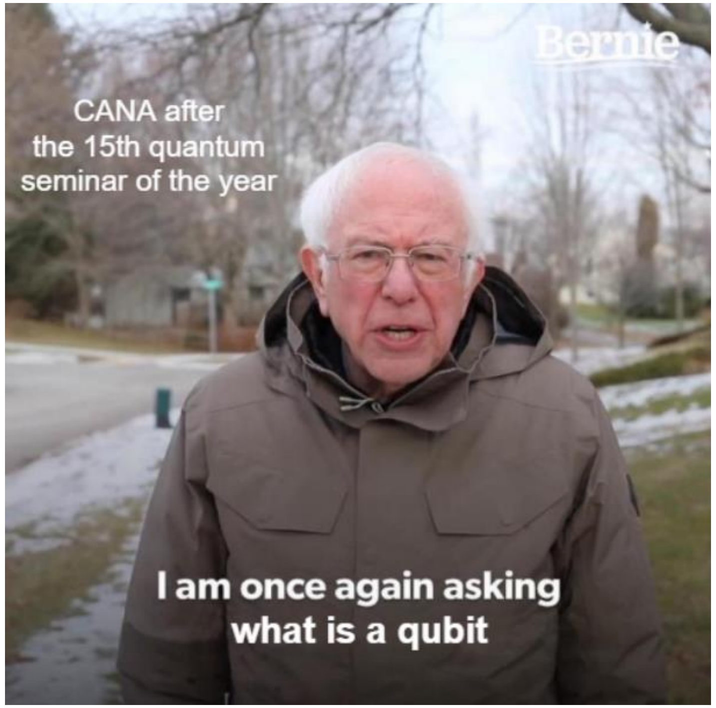
Introduction to Quantum Computing

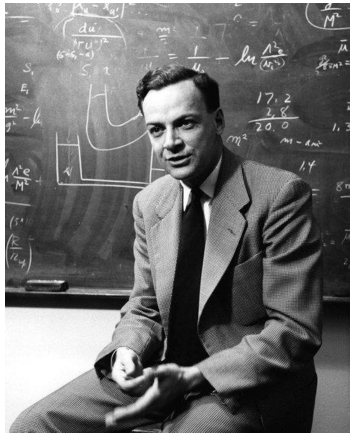


Ugo Nzongani

CANA Seminar

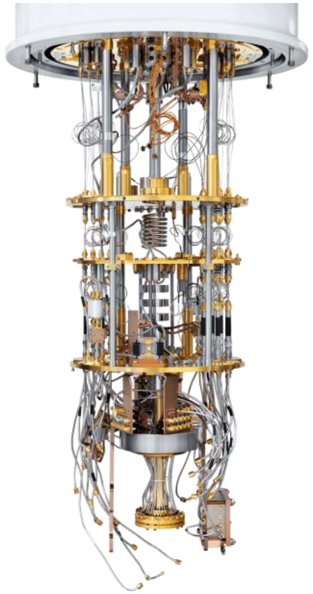
Why?

- Efficient simulation of quantum systems: Feynman (1981)



“Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical”

- Breakthrough: Shor’s algorithm (1994)
  - *Exponential speedup for factoring large numbers*



- Other potential applications:
  - *Optimization*
  - *Communication*
  - *Finance*
  - *Material and drug design*

How?

Quantum mechanics phenomena

- *Superposition: a quantum bit can be 0 and 1 at the same time*

- *Entanglement: correlation of information*

- *Interference: amplify correct solutions*

Measurement: *we only have access to one state of the superposition*

Notations

Dirac notation: « ket » ▶ $|\cdot\rangle =$ column vector

« bra » ▶ $\langle\cdot| =$ row vector

Tensor product $\otimes$:

Vectors

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} c \\ d \end{bmatrix} \\ b \begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

Matrices

$$\begin{pmatrix} A_0 & A_1 \\ A_2 & A_3 \end{pmatrix} \otimes \begin{pmatrix} B_0 & B_1 \\ B_2 & B_3 \end{pmatrix} = \begin{pmatrix} A_0 \begin{pmatrix} B_0 & B_1 \\ B_2 & B_3 \end{pmatrix} & A_1 \begin{pmatrix} B_0 & B_1 \\ B_2 & B_3 \end{pmatrix} \\ A_2 \begin{pmatrix} B_0 & B_1 \\ B_2 & B_3 \end{pmatrix} & A_3 \begin{pmatrix} B_0 & B_1 \\ B_2 & B_3 \end{pmatrix} \end{pmatrix}$$

Quantum bit

A qubit is a two-level quantum system described by a 2D complex vector evolving in an Hilbert space $\mathcal{H}$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

with $(\alpha, \beta) \in \mathbb{C}^2$ and $|\alpha|^2 + |\beta|^2 = 1$.

Before measurement

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

After measurement

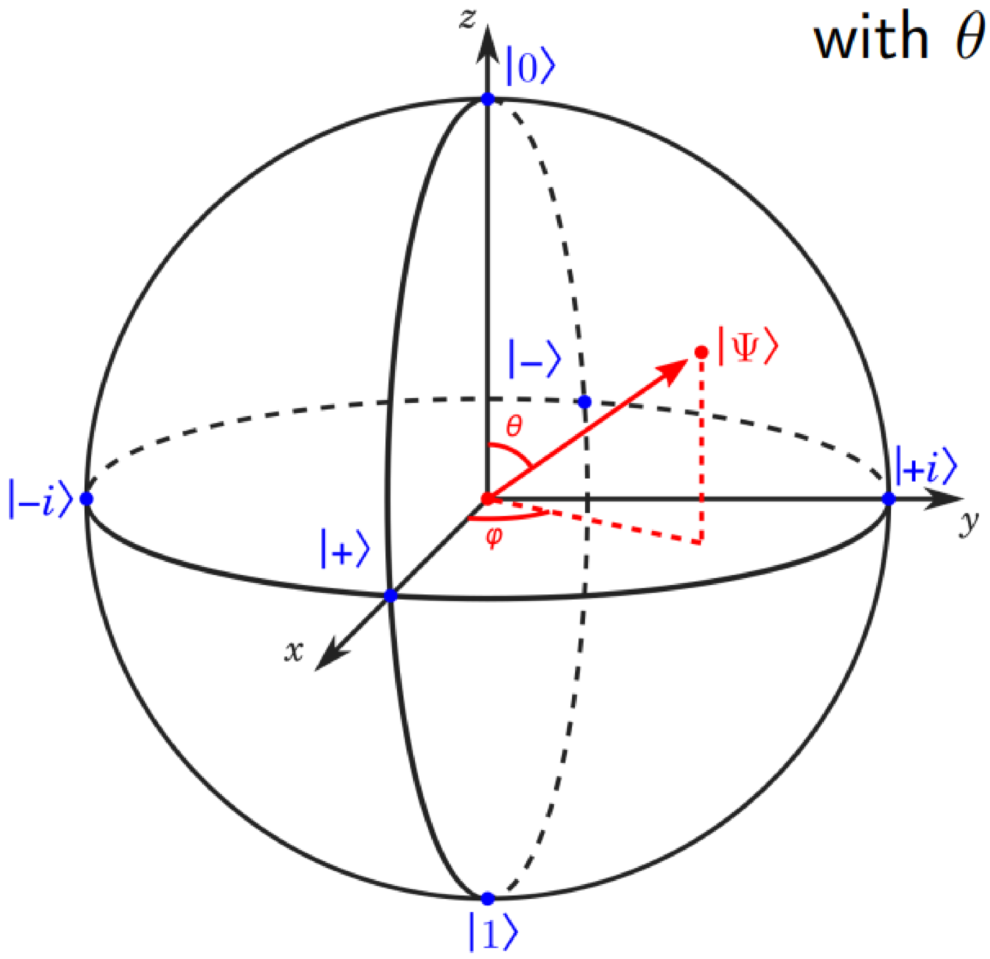
$$p(0) = |\alpha|^2 \longrightarrow |\psi\rangle = |0\rangle$$

$$p(1) = |\beta|^2 \longrightarrow |\psi\rangle = |1\rangle$$

Bloch Sphere

A qubit state can be expressed as: $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$

with $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$



Bloch Sphere

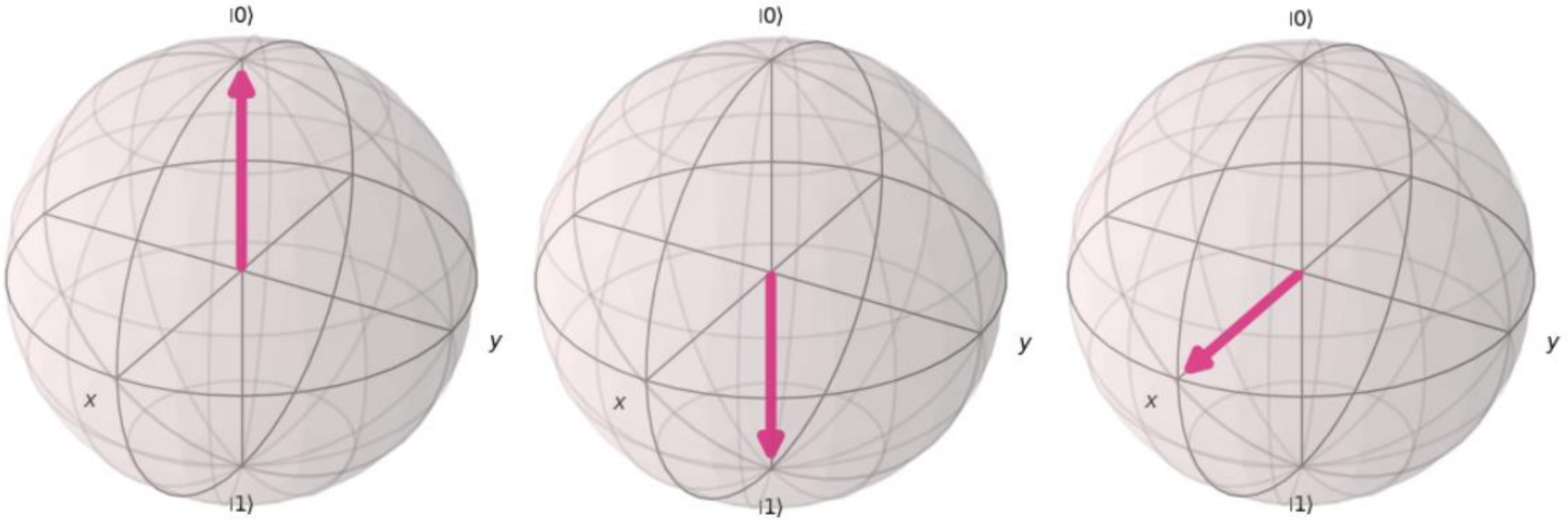


Figure 1: $|0\rangle$, $|1\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Quantum registers

A register of n qubits can represent 2^n states: $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ with $\sum_x |\alpha_x|^2 = 1$

Computational basis $B_n = \{|x\rangle \,|x \in \{0,1\}^n\}$: $|0_2\rangle = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, |1_2\rangle = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, |(2^n-1)_2\rangle = \begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$

$|x\rangle$:x−th canonical basis vector of $\mathbb{R}^{2^n}$

Each state of B_n is a tensor product of n qubits:

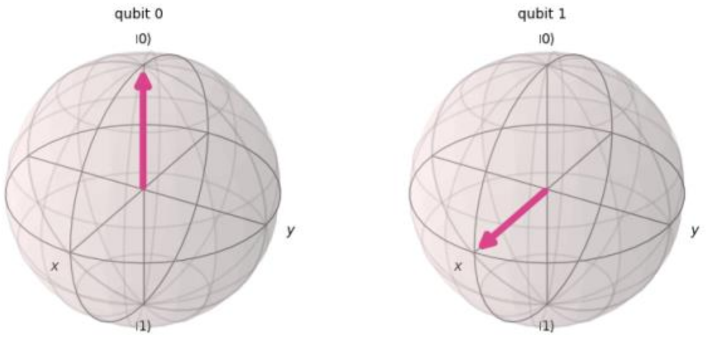
$$|01\cdots0\rangle = |0\rangle \otimes |1\rangle \otimes \cdots \otimes |0\rangle$$

Measuring the n qubits makes the state collapse to a single classical state

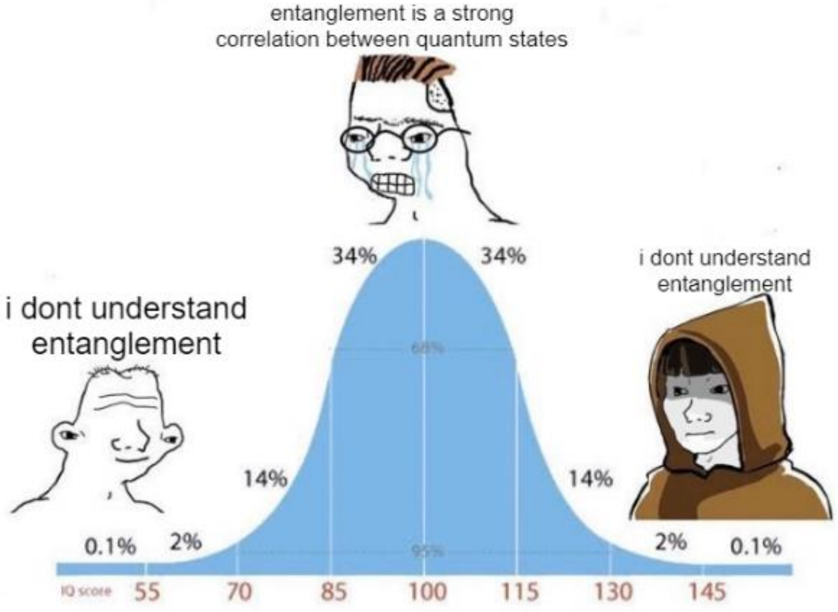
Entanglement

- Separable state: $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

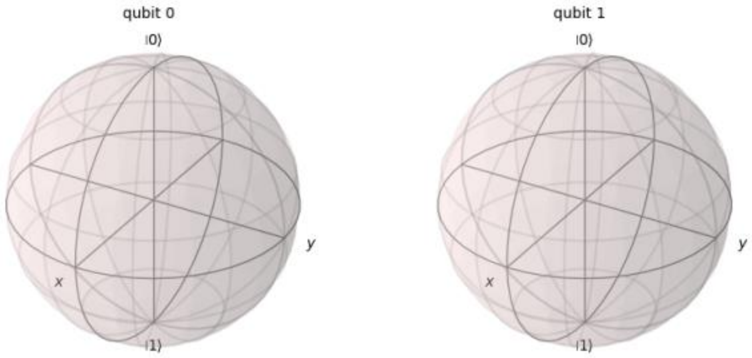
$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



- Non-separable (entangled) state: $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$



$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{or} \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$



Unitary operations

- We manipulate qubits with unitary matrices (gates): $|\psi'\rangle = U\,|\psi\rangle$

$$UU^\dagger = U^\dagger U = I \quad \text{with} \quad U^\dagger = U^{*\,T}$$

- Unitaries:
  - Norm preserving
  - Reversibility (no loss of information)

Some examples

Bit-flip gate:

$$X = \begin{array}{cc} |0\rangle & |1\rangle \\ \end{array}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$$

Phase-flip gate:

$$Z = \begin{array}{cc} |0\rangle & |1\rangle \\ \end{array}$$
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

Some examples

Hadamard gate:

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

$$\begin{tikzcd} |0\rangle \arrow[d, bend left, "H"] \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \arrow[u, bend left, "H"] \end{tikzcd}$$

$$\begin{tikzcd} |1\rangle \arrow[d, bend left, "H"] \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \arrow[u, bend left, "H"] \end{tikzcd}$$

Hadamard transform on $|k\rangle, k \in \{0,1\}^n$:

$$H^{\otimes n} |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{k \cdot x} |x\rangle$$

with $k \cdot x = k_1 x_1 \oplus \cdots \oplus k_n x_n \in \{0,1\}$

Some examples

Controlled-NOT gate:

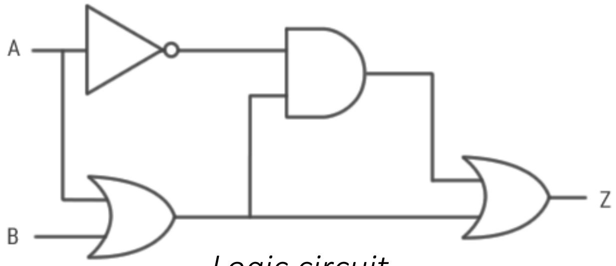
$$C_X = \begin{array}{c} \\ \\ \end{array}\begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array}$$

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

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |11\rangle \\ |11\rangle &\mapsto |10\rangle \end{aligned}$$

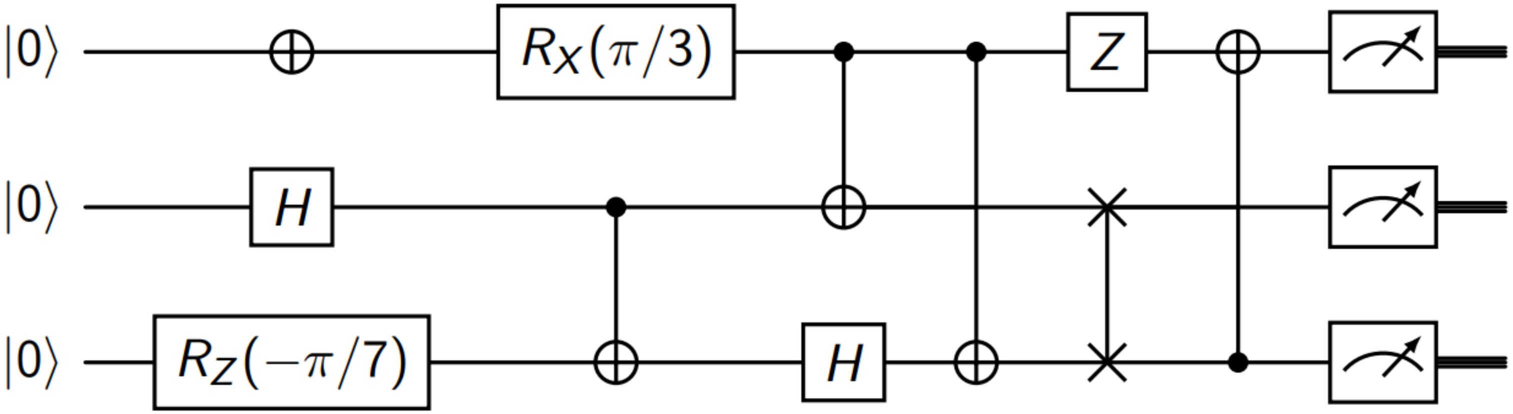
« Entangling gate »

Quantum circuits

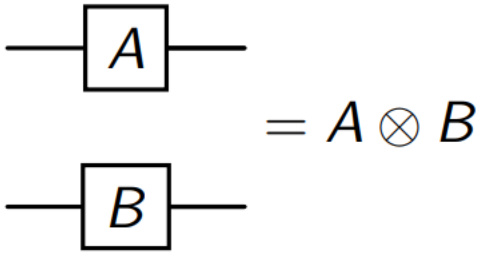


Logic circuit

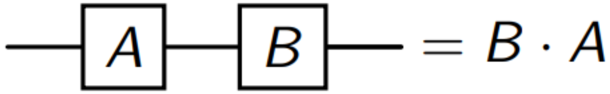
- Time goes from left to right
- Each qubit corresponds to a wire
- Number of qubit: *size*
- Execution time: *depth*
- Efficient circuit: number of gates scales at most polynomially with the number of qubits



Parallel operations



Sequential operations



Quantum circuits

Let's construct U such that: $U|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$|0\rangle$ ———————

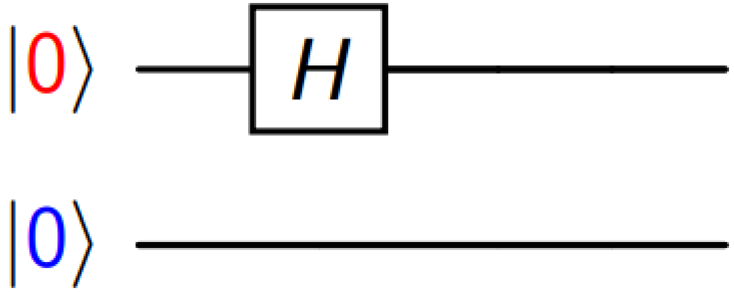
$|0\rangle$ ———————

Current state: $|0\rangle \otimes |0\rangle$

Unitary built: $U = I_4$

Quantum circuits

Let's construct U such that: $U|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

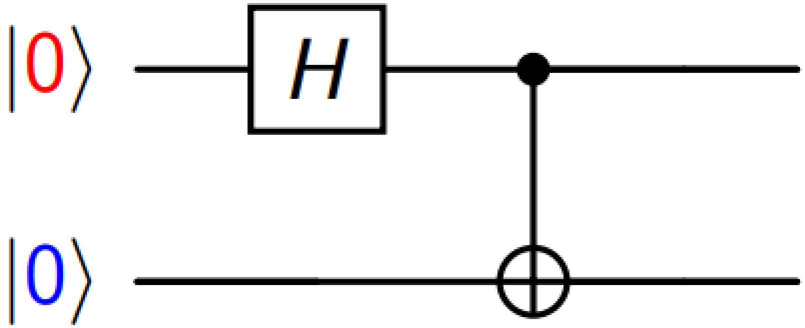


Current state: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

Unitary built: $U = H \otimes I_2$

Quantum circuits

Let's construct U such that: $U|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



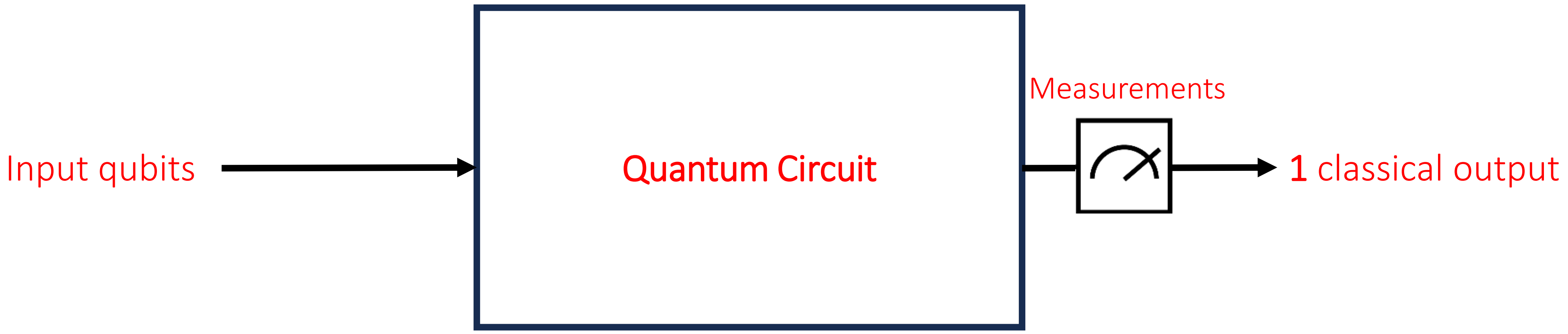
Current state: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Unitary built: $U = C_X(H \otimes I_2)$

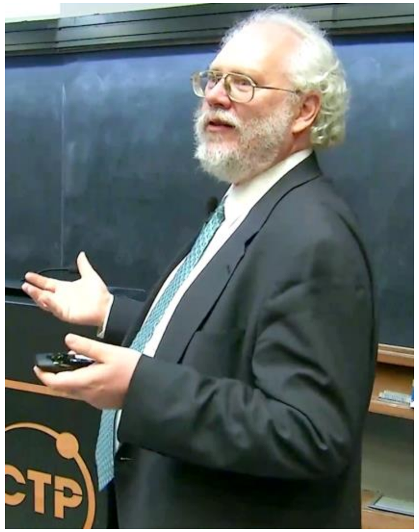
Quantum algorithms

Main idea:

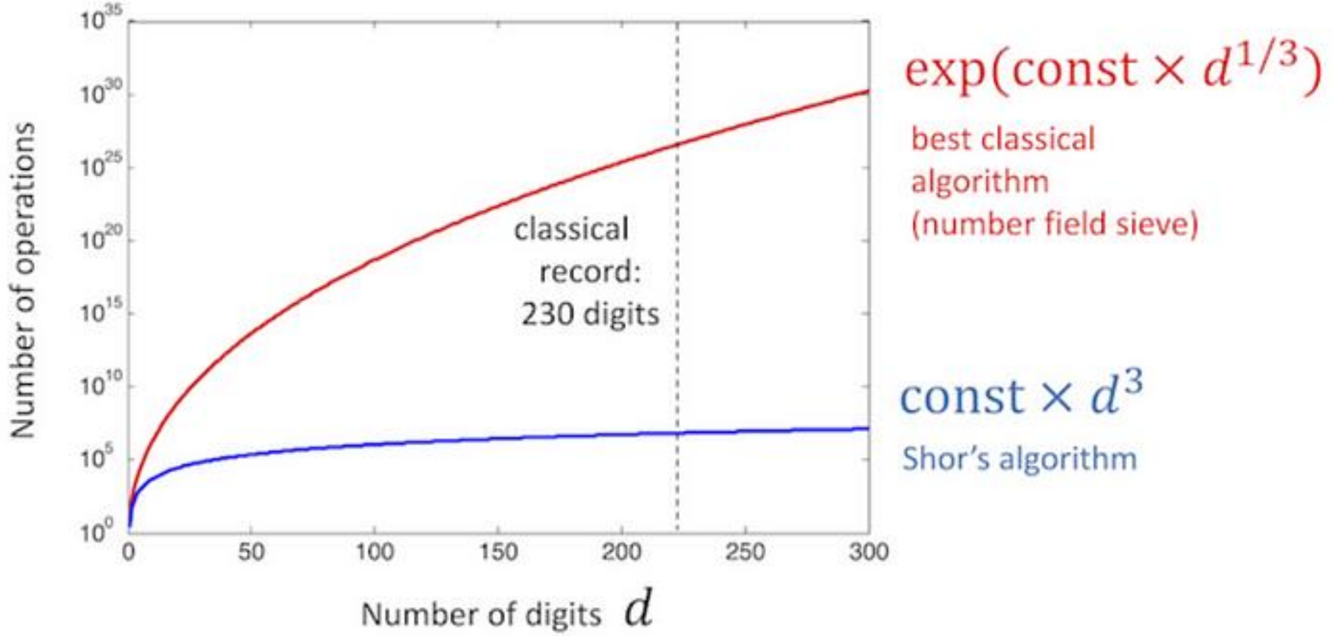
1. Each state encodes a potential solution
2. Use constructive/destructive interferences to modify the measurement probabilities of good/bad solutions
3. Measure the qubits and repeat this process to obtain a representative probability distribution over the states



Shor's algorithm

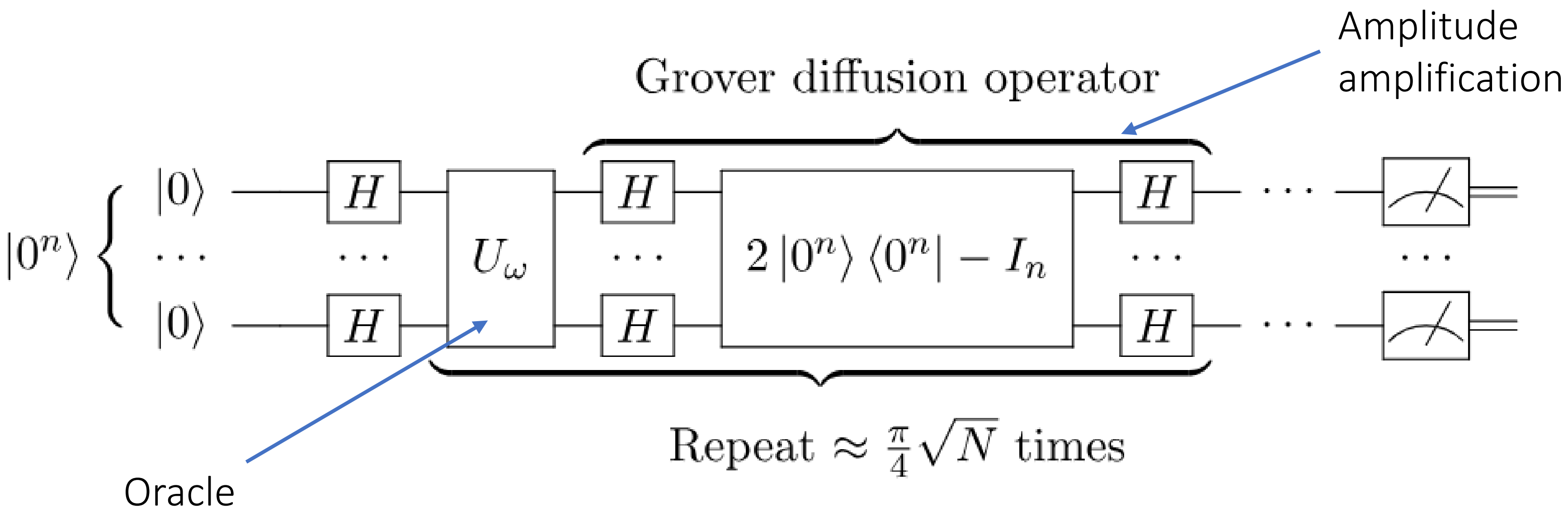


- Efficient factoring algorithm: $N = p \times q$
  - Reduces factoring to period finding
  - Makes use of Quantum Fourier Transform
  - Breaks RSA encryption
  - Shor's algorithm: $O(\log(N)^3)$
  - Best classical algorithm (General Number Field Sieve): $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$



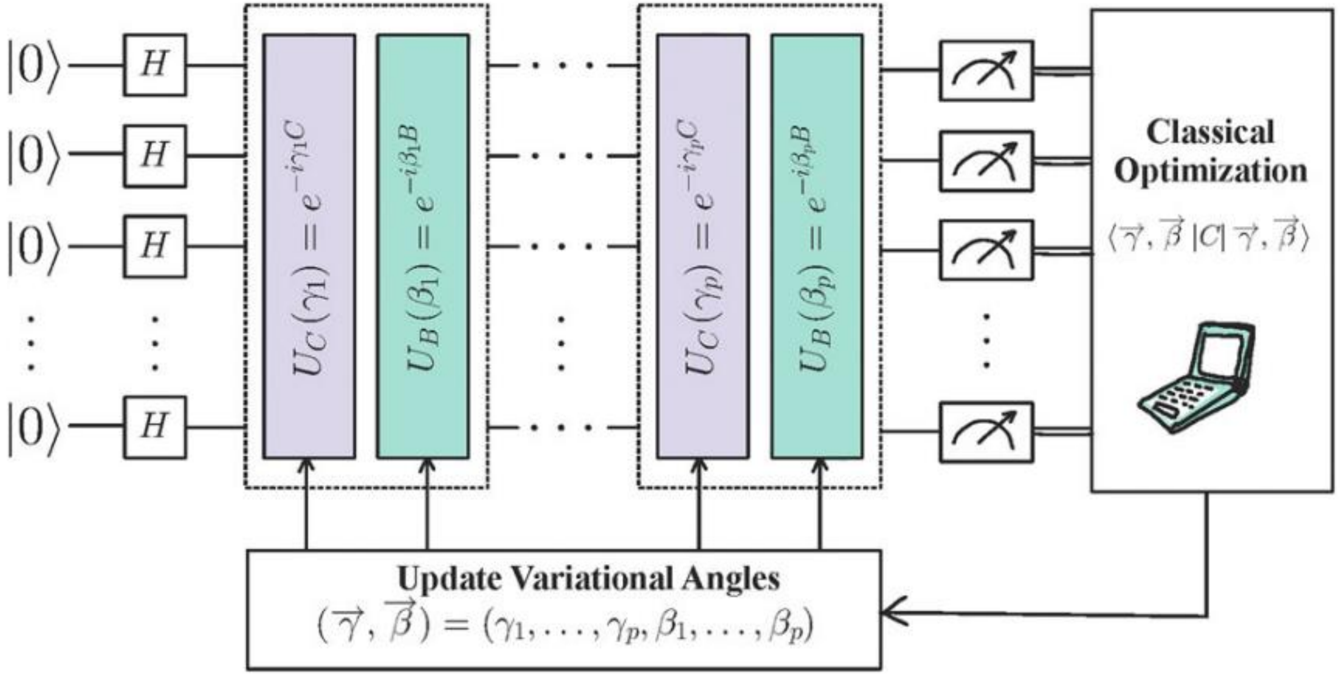
Grover's search

- Unstructured search:
  - Uses an oracle to mark the correct state by flipping its phase
  - Performs amplitude amplification to boost the probability of the correct state
  - Classical approach: worst case 2^n queries
  - Grover: $2^{n/2}$ queries



Variational Quantum Algorithms

- Find the ground (minimum energy) state of a quantum system
- Parametrized quantum circuit
- Set of parameters optimized classically



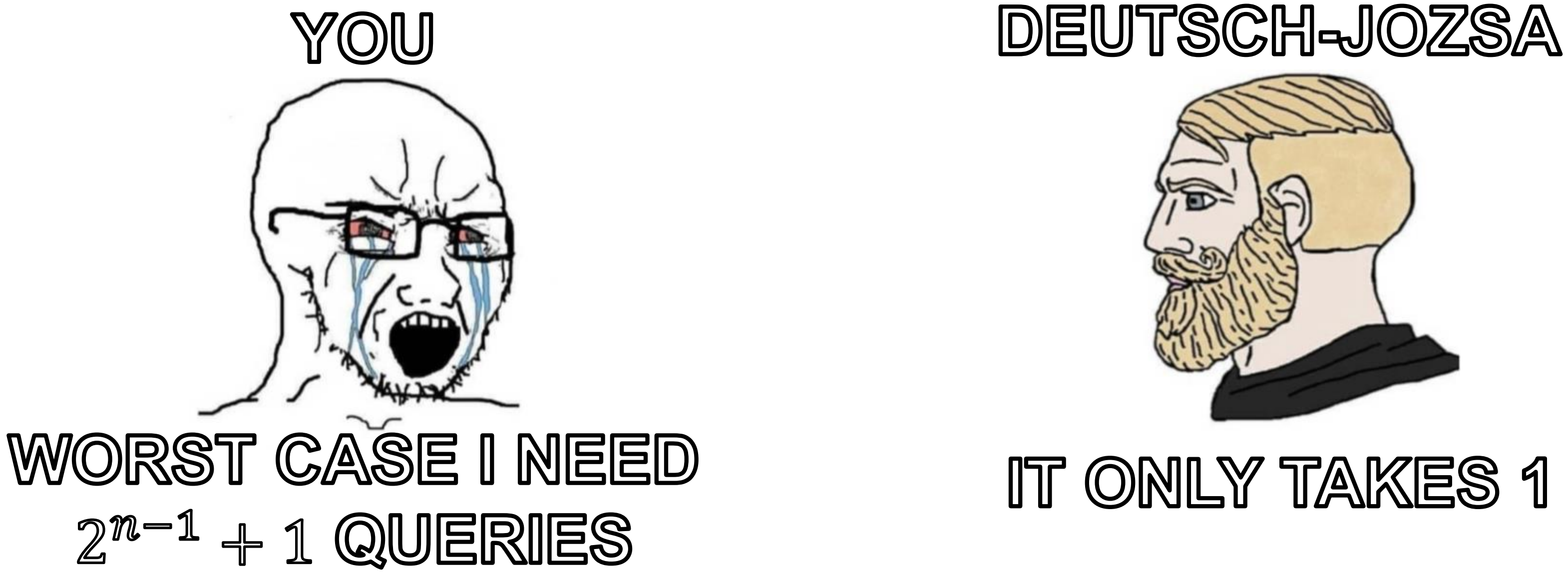
Quantum Approximate Optimization Algorithm (QAOA) circuit

Deutsch-Jozsa

Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be constant or balanced:

- $constant: \forall x, f(x) = a$ with $a \in \{0,1\}$
- $balanced: Card(\{x \mid f(x) = 0\}) = Card(\{x \mid f(x) = 1\})$

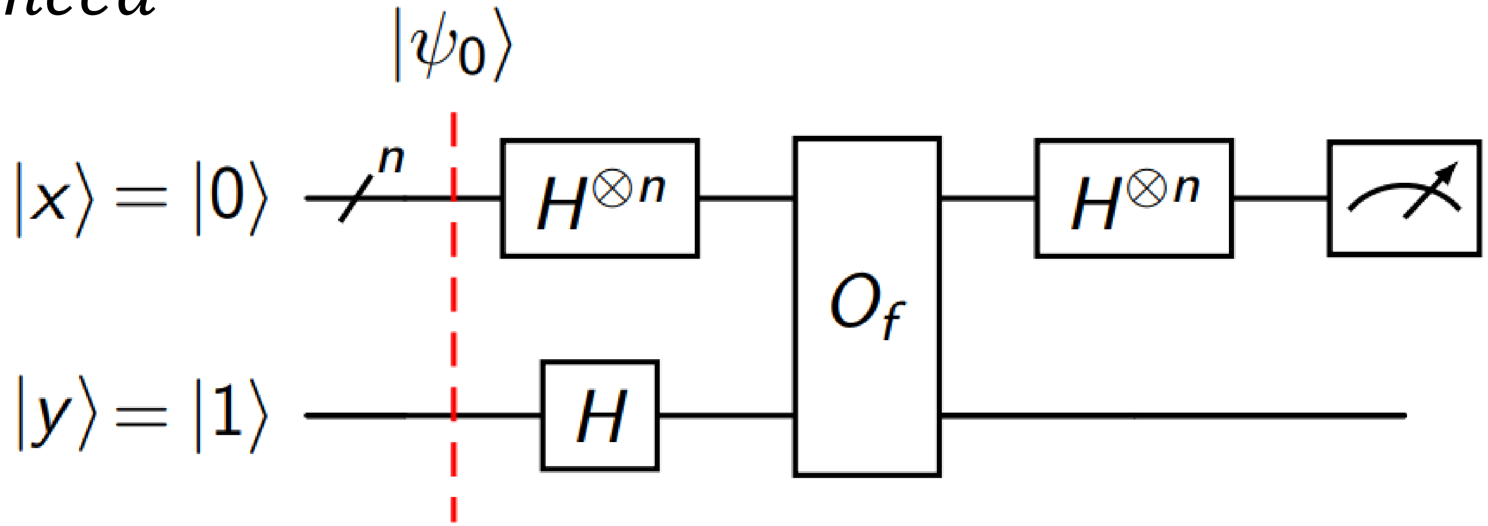
Problem: Determine if f is constant or balanced by querying f



Deutsch-Jozsa

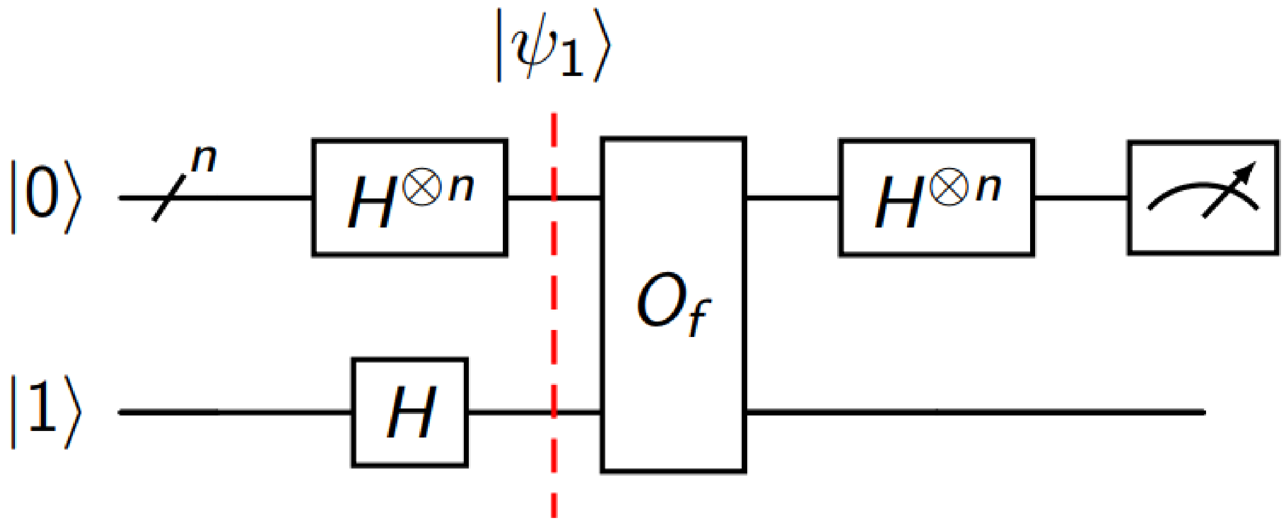
Measurement outcomes:

- $00 \cdots 00$: f *is constant*
- *Otherwise*: f *is balanced*



Initial state: $|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$

Deutsch-Jozsa

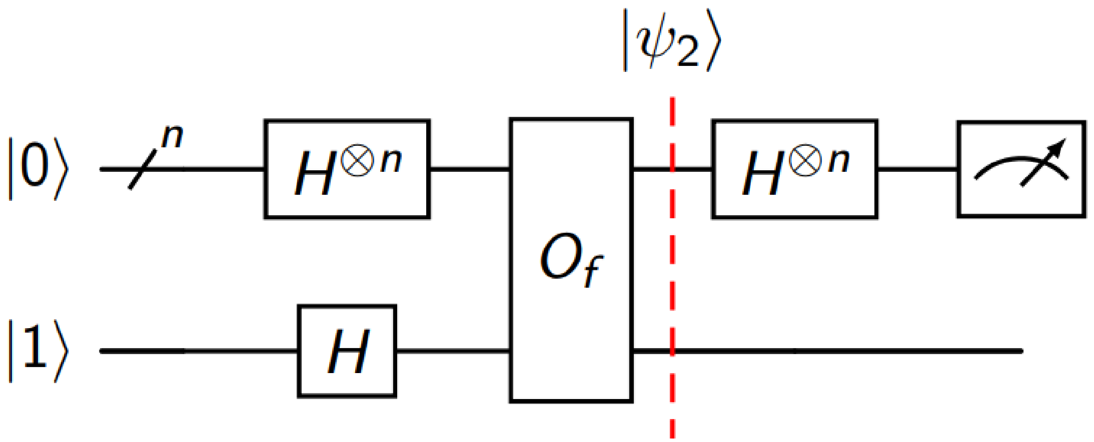


State: $$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Deutsch-Jozsa

State:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}} \underbrace{(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)}$$



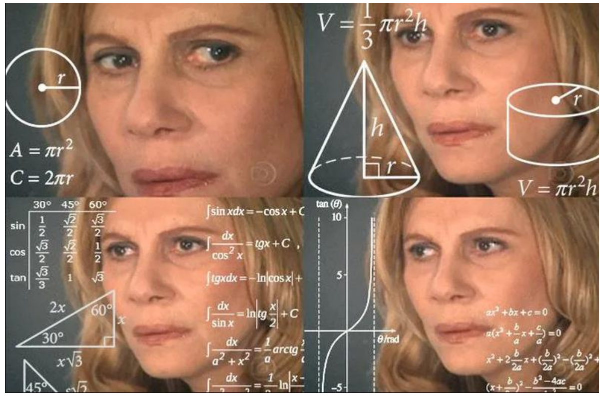
Oracle $O_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus x\rangle$

A	B	A ⊕ B
0	0	0
1	0	1
0	1	1
1	1	0

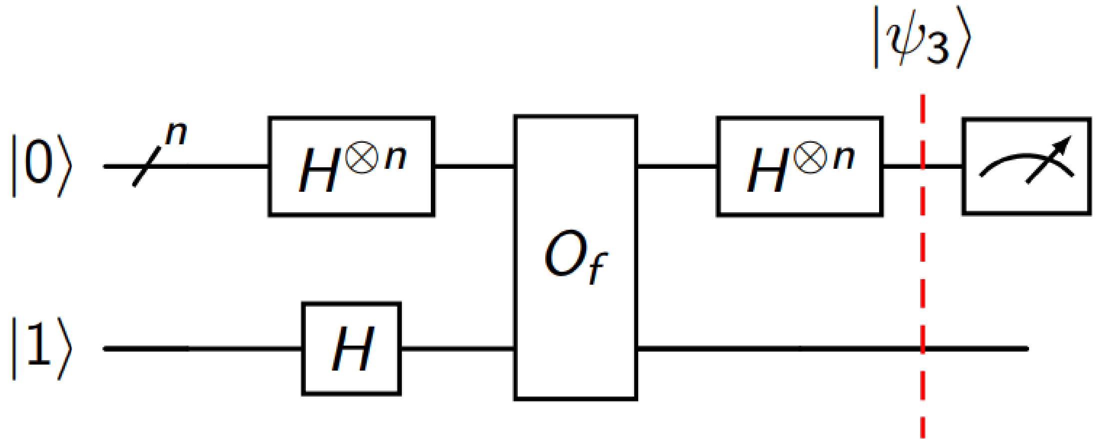
$$|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = \begin{cases} |0\rangle - |1\rangle & \text{if } f(x) = 0 \\ |1\rangle - |0\rangle & \text{if } f(x) = 1 \end{cases}$$

$$= (-1)^{f(x)} \cdot (|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



Deutsch-Jozsa



State:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H\,|x\rangle \otimes |y\rangle$$

Hadamard transform

$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \boxed{\left(\frac{1}{\sqrt{2^n}} \sum_{k\in\{0,1\}^n} (-1)^{x\cdot k}\,|k\rangle \right)} \otimes |y\rangle$$

$$= \frac{1}{2^n} \sum_{k\in\{0,1\}^n} |k\rangle \left(\sum_{x\in\{0,1\}^n} (-1)^{x\cdot k + f(x)} \right) \otimes |y\rangle$$

Deutsch-Jozsa

Final state before measurement:

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{k\in\{0,1\}^n} |k\rangle \left(\sum_{x\in\{0,1\}^n} (-1)^{x\cdot k+f(x)} \right) \otimes |y\rangle$$

The probability of measuring $|0\rangle^{\otimes n}$ is:

$$p(0) = \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \right|^2$$

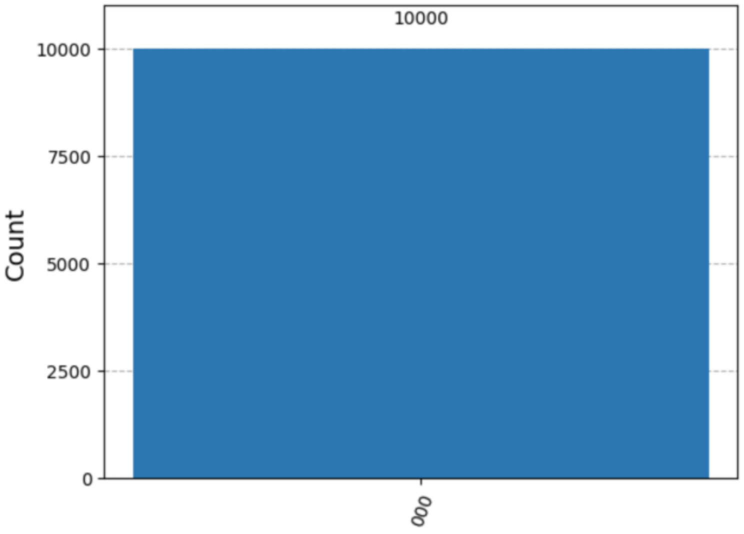
Thus:

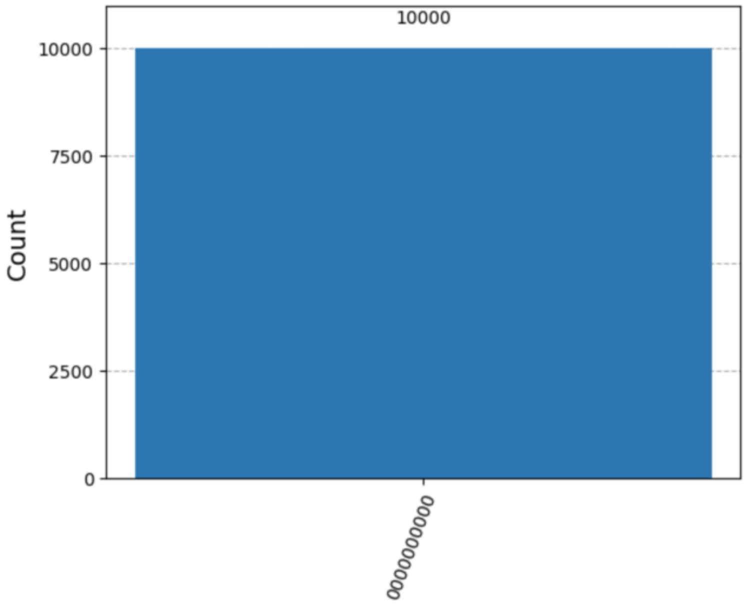
$$p(0) = \begin{cases} 1 \text{ if } f \text{ is constant} \\ 0 \text{ if } f \text{ is balanced} \end{cases}$$

Execution on IBM device: f constant

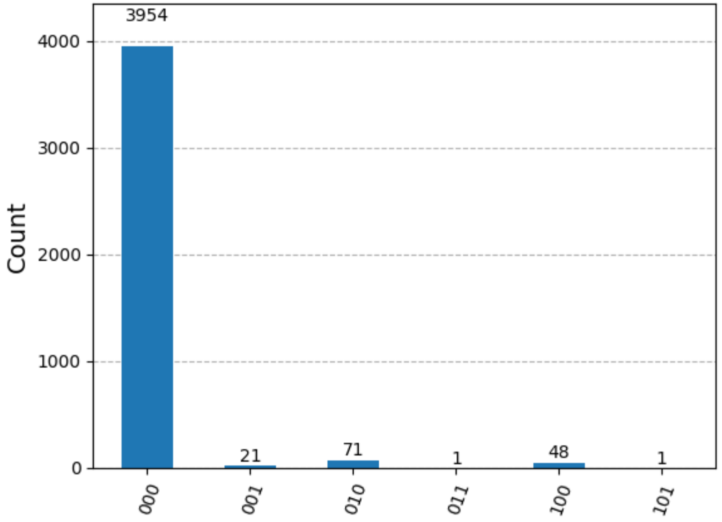
$n = 3\ qubits$ | $n = 10\ qubits$

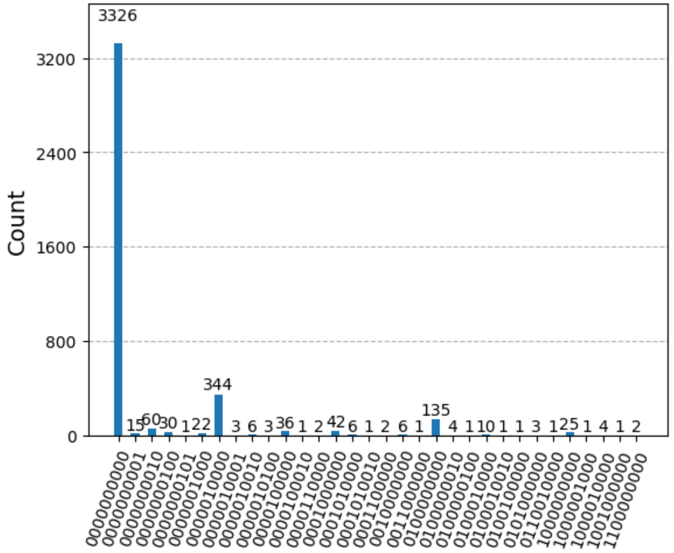
QPU Simulator:





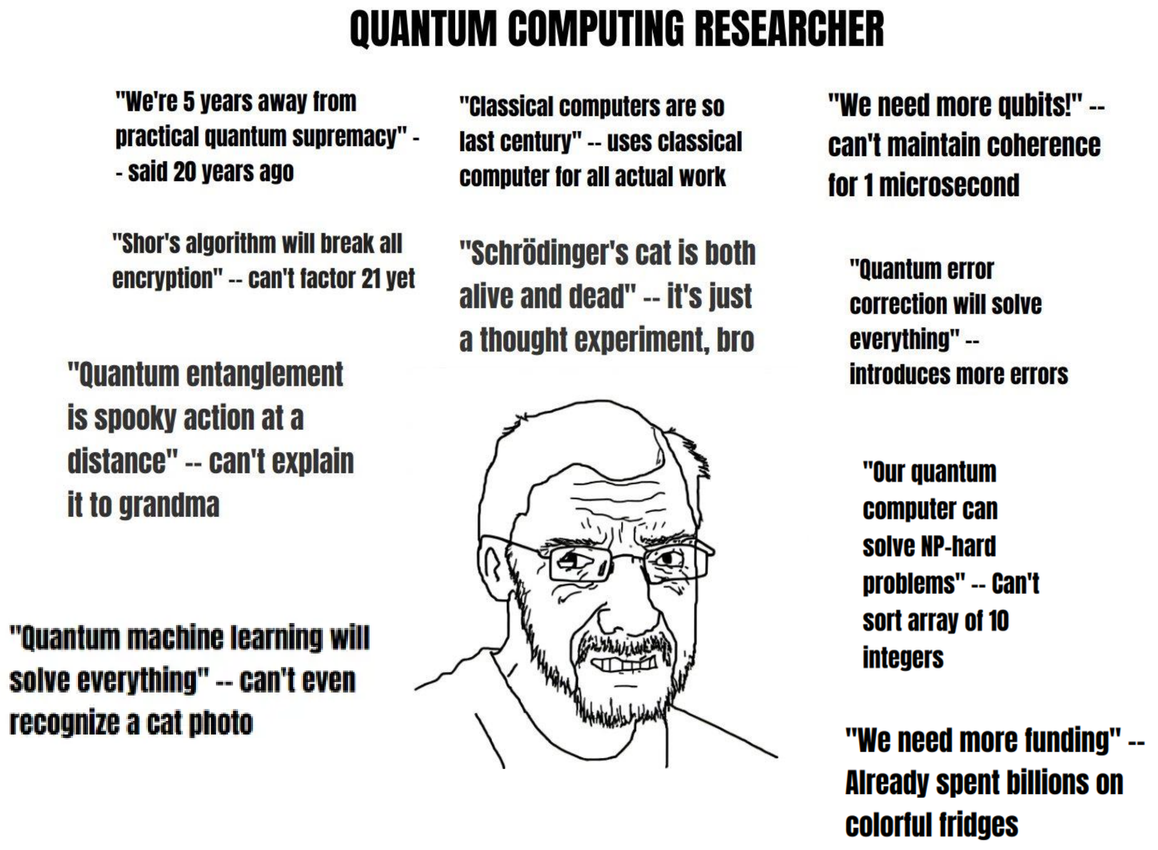
QPU:





Takeaways

- Quantum computing makes use of
  - *Superposition, Entanglement, Interference*
- Real world applications
  - *Drug discovery, Materials science*
  - *Optimization, Cryptography, ML*
- Noisy Intermediate-Scale Quantum (NISQ) era
  - *Major hardware challenges*
  - *French Startups:*



QUANDELA	ALICE & BOB	PASQAL	C12 QUANTUM ELECTRONICS
Photonic qubits	*Superconducting qubits (cat qubit)*	*Neutral atom qubits*	*Carbon nanotube qubits*

Thank you

INTRODUCTION
TO
QUANTUM COMPUTING
CANA
SEMINAR
INTRODUCTION
TO QUANTUM
INFORMATION