QUANTUM COMPUTING
DEMONSTRATION

LUÍS PAULO SANTOS

JANUARY, 2021

BRIEF HISTORICAL OVERVIEW

- **Quantum systems** evolve in a **state space exponentially larger than the number of parameters** require to define each state

- This **exponential complexity** hinders the simulation of large quantum system using classical computers
  but simultaneously **enables quantum parallelism**

- *"**Nature isn't classical**, goddamn it! And if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy. "*

[Richard Feynman, 1981]

BRIEF HISTORICAL OVERVIEW

- In **1985** Deutsch developed a model of a **quantum Turing machine,** a theoretical basis for quantum computing

- In **1994** Shor has shown that efficient ($O(log^3(N))$) **factorization of prime numbers** is possible on quantum computers;
  It hasn't been shown that classical polylogarithmic algorithms for factorization don't exist, although none is known

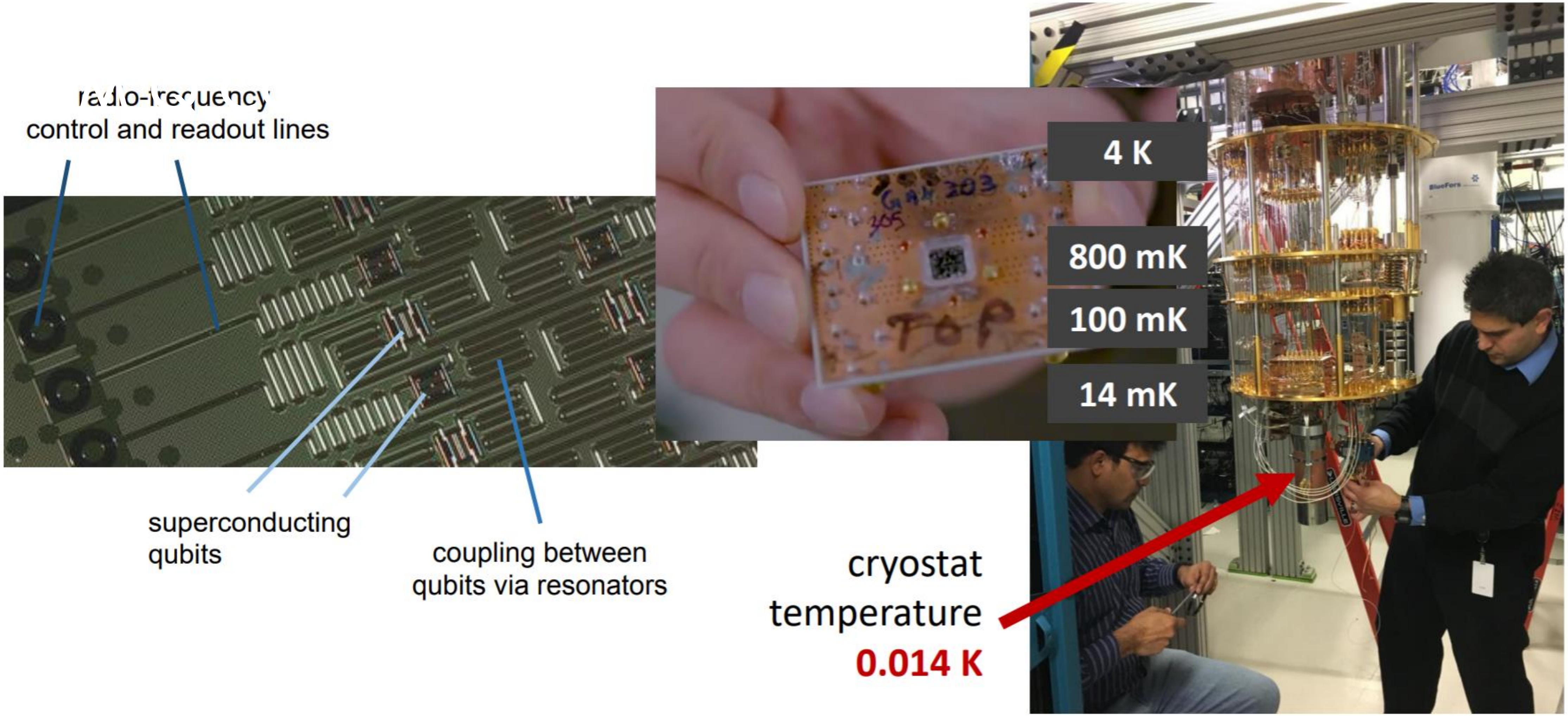
- In **1996** Grover proposed a **search** algorithm on **unstructured databases** with complexity **$O(\sqrt{N})$** , quadratically better than classical searches ($O(N)$)

BRIEF HISTORICAL OVERVIEW

- NISQ (Noisy Intermediate Scale Quantum) era:
  - Noisy qubits
  - Noisy q-gates
  - 20 .. 50 qubits (100 seem feasible)[1]
  - Limited connectivity among qubits
  - Limited coherence time (~100 usec)

---

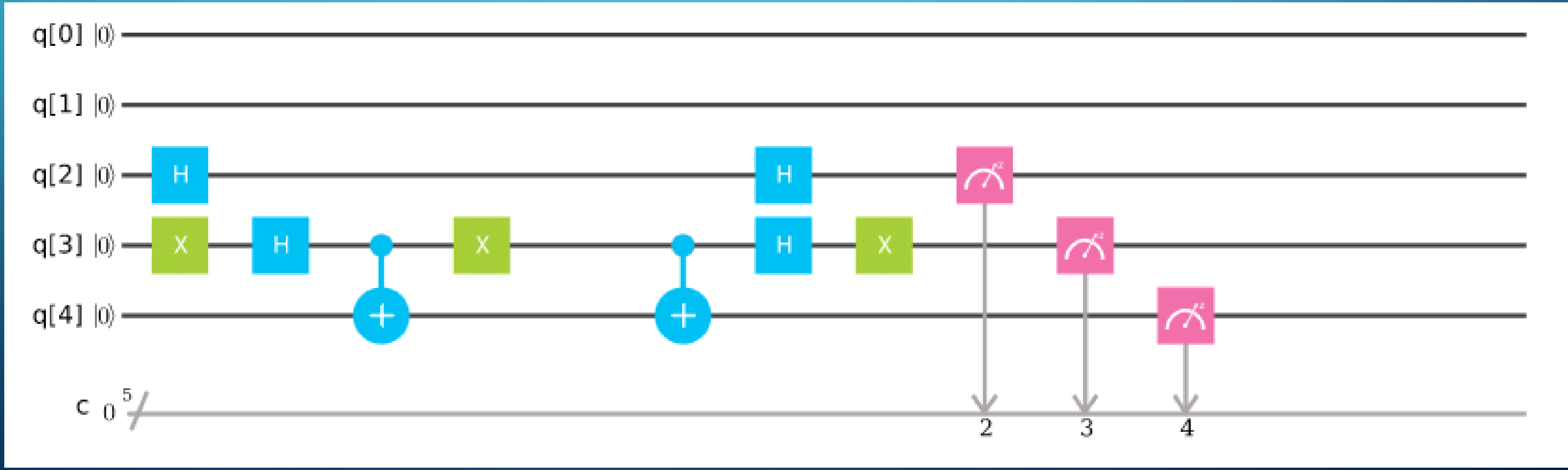
[1] Adiabatic quantum computers can reach 2000 qubits (D-Wave 2000Q System), but operate based on the simulated annealing algorithm and the adiabatic theorem, requiring the modelling of optimization problems as physical Hamiltonians



“Demonstration of a quantum error detection code using a square lattice of four superconducting qubits”, A.D. Córcoles et al., **Nat. Comm.**, 6:6979 (2015)

QUANTUM CIRCUIT MODEL

- Quantum computers can represent an **exponentially large number of states** due to **quantum parallelism**
- The **quantum circuit model generalizes** the **binary logic gates model** used in classical computers: **quantum gates** operate on **quantum states**



#1 - QUBIT

- A classical bit's value is uniquely and deterministically either 0 or 1

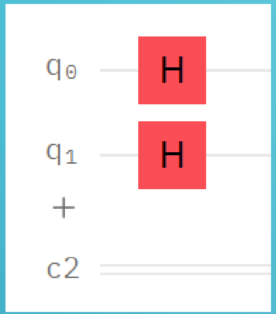
$$b \in \{0,1\}$$

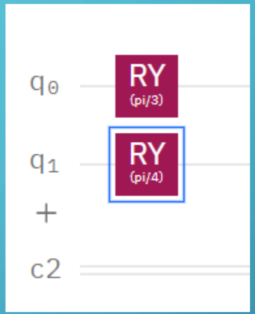
- A **quantum state** is a linear combination **(superposition) of the basis states:**

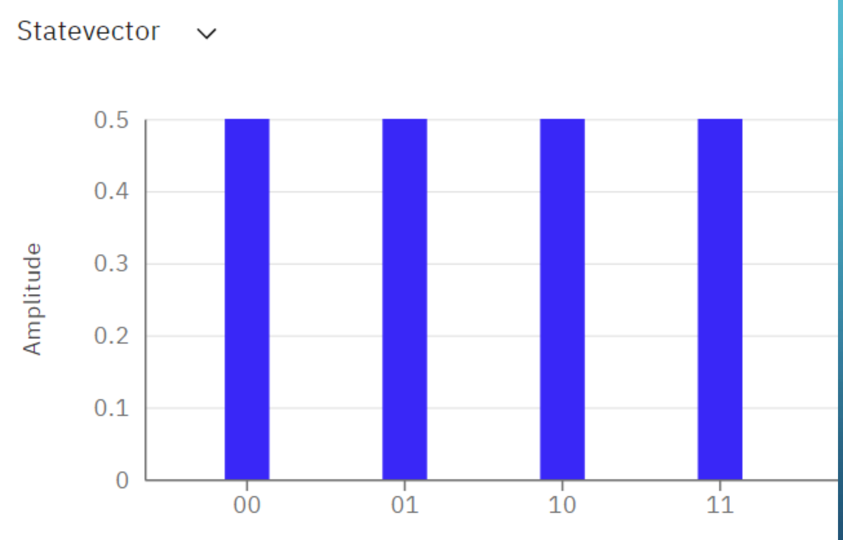
$$|q\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle; \;\; \alpha_0, \alpha_1 \in \mathbb{C}, \;\; \sum_{i=0}^{1} |\alpha_i|^2 = 1$$

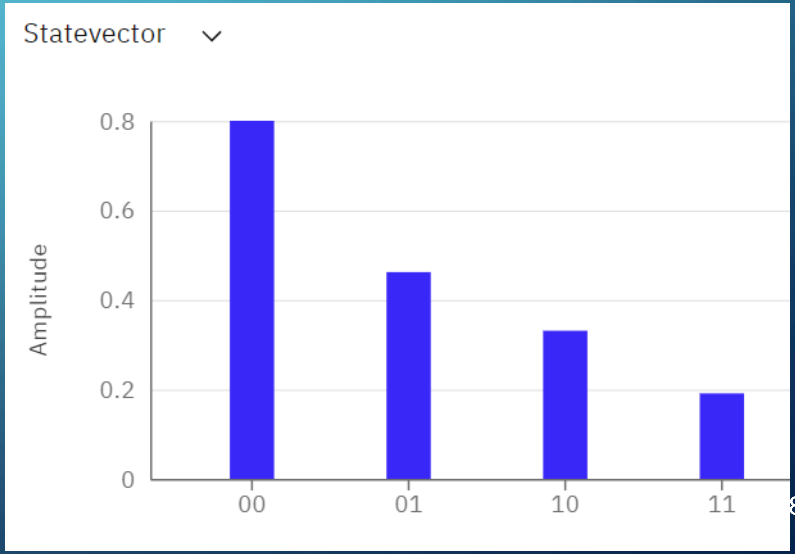
- A qubit can be in both basis states simultaneously, and **any quantum operation** on the qubit **operates over both states**
- A qubit can behave like a classical bit by setting one of the weights α_i to 1 and the quantum machine can behave as a classical computer

IBM Q EXPERIENCE - QUBIT









#1 - QUBIT

- A superposition of *n* qubits is a linear combination of *2ⁿ* states:

$$\left|q^{\otimes n}\right\rangle \equiv |\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle\,, \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

- **any quantum operation** on the *n* qubits superposition **operates over all 2^n states**

#2 - MEASUREMENT

- Measurement of a quantum register **yields a classic state**

  $\text{measurement}\left(|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle\right) = |i\rangle$, with probability $|\alpha_i|^2$

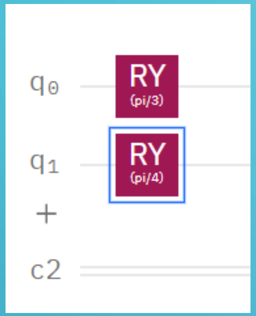
- The **quantum superposition collapses into the measured state**, losing all information on the α_i's

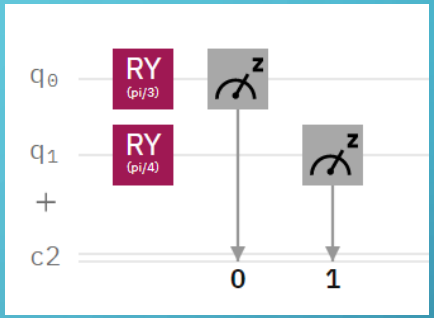
  any further reading will return the same state $|i\rangle$

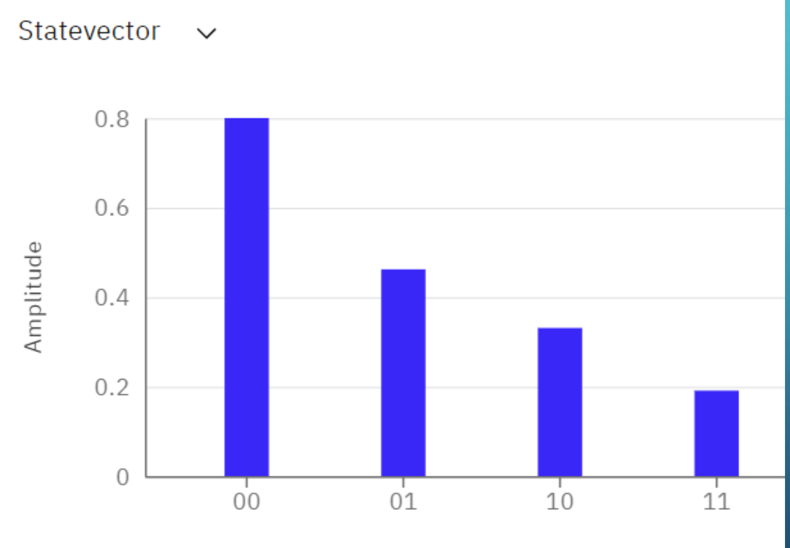
- No intermediate result can be accessed (debugging has to be rethought)

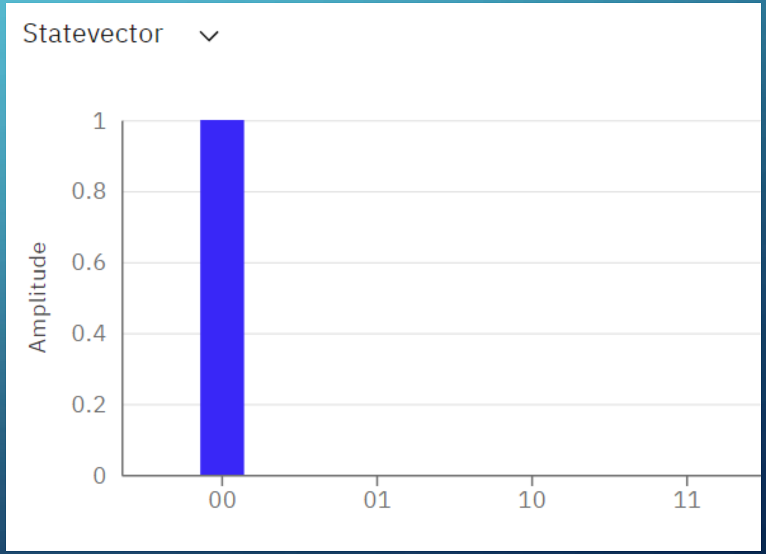
- The α_i's cannot be accessed directly, i.e., they cannot be measured

IBM Q EXPERIENCE - MEASUREMENT









#3 – UNITARY TRANSFORMATIONS

- Physical laws require all **quantum transitions** to be **unitary:**

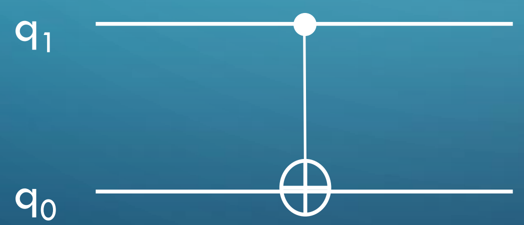
$$|\Psi'\rangle = \mathrm{U}|\Psi\rangle \Rightarrow U^{-1} = U^{\dagger},\ U^{\dagger}U = I$$

- This also implies means that the **transformation** is **reversible:**

  given the outputs the inputs can be known!

Example: CNOT gate (invert qubit q_0 if control qubit q_1 is 1):

q_1	q_0	q_1	q_0
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



$$|\Psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

$$\begin{bmatrix}\alpha_0\\ \alpha_1\\ \alpha_3\\ \alpha_2\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix}$$

$$|\Psi'\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_3|10\rangle + \alpha_2|11\rangle$$

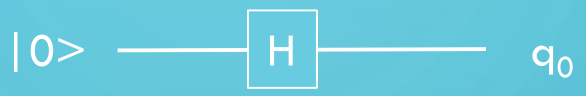
#3 – UNITARY TRANSFORMATIONS

- Unitary transformations have a **number of outputs equal to the number of inputs**
- **Classical** boolean **gates are not reversible**
- Quantum gates:
  - NOT (X gate): $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
  - Rotation (phase shift): $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$
  - CNOT: $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

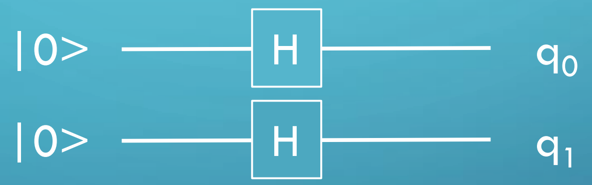
Toffoli (CCNOT): $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

#3 – UNITARY TRANSFORMATIONS (HADAMARD)

- The Hadamard gate is often used to prepare uniform superpositions
  - Hadamard: $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$



$$|q_0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$$

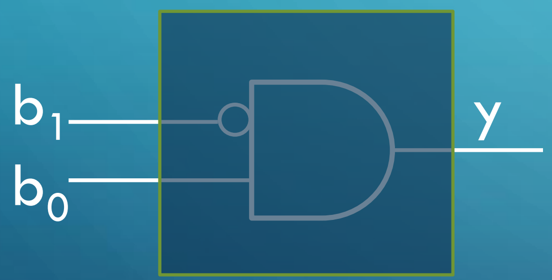


$$|q_1 q_0\rangle = \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right) \otimes \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right)\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{bmatrix} = \frac{1}{2}[|00\rangle + |01\rangle + |10\rangle + |11\rangle]$$

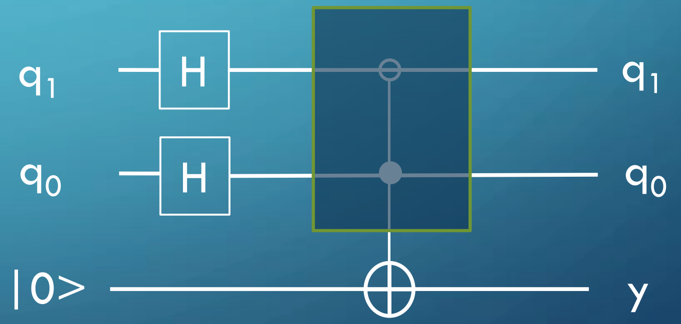
#4 - QUANTUM PARALLELISM

- An *n*-qubits register represents $N=2^n$ states simultaneously
- A quantum algorithm operates over the N states simultaneously
- Quantum parallelism is exponential on the number of qubits

Example: what is the key encoded in the circuit?

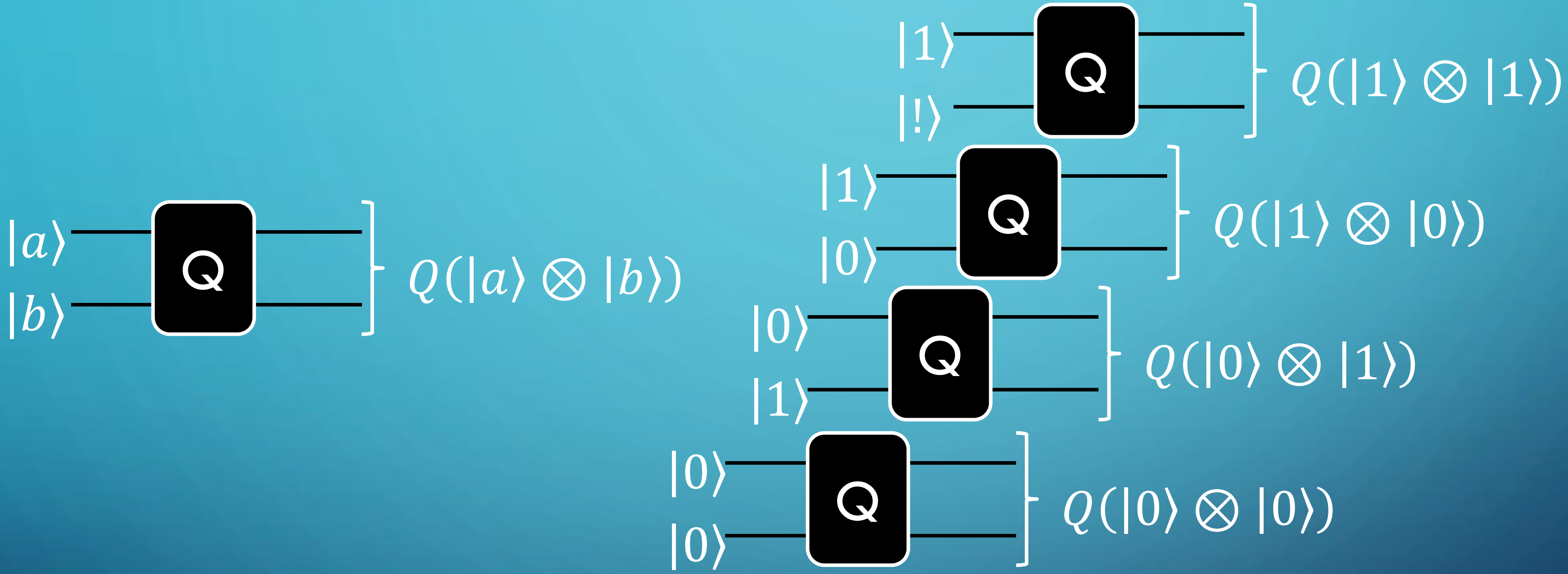


4 executions are required to iterate over the 4 possible candidates



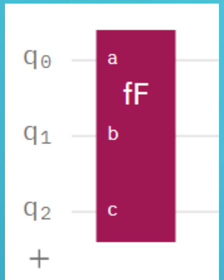
1 execution is enough to encode the solution in $|q_1\ q_0\ y>$, but …

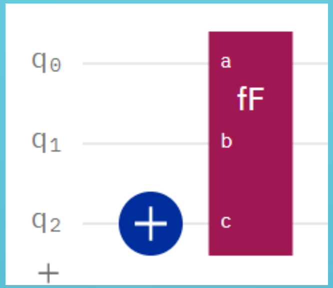
#4 - QUANTUM PARALLELISM

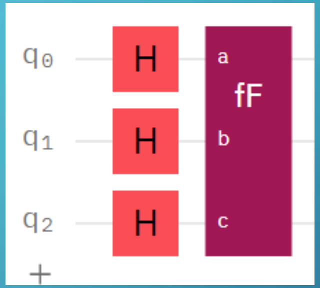


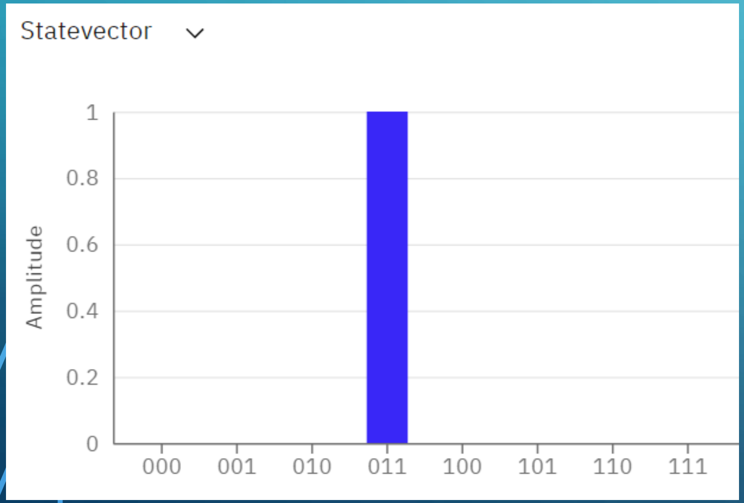
$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \Longrightarrow \hat{Q}|\Psi\rangle = \hat{Q}\left(\sum_{i=0}^{2^n-1} \alpha_i |i\rangle\right)$$

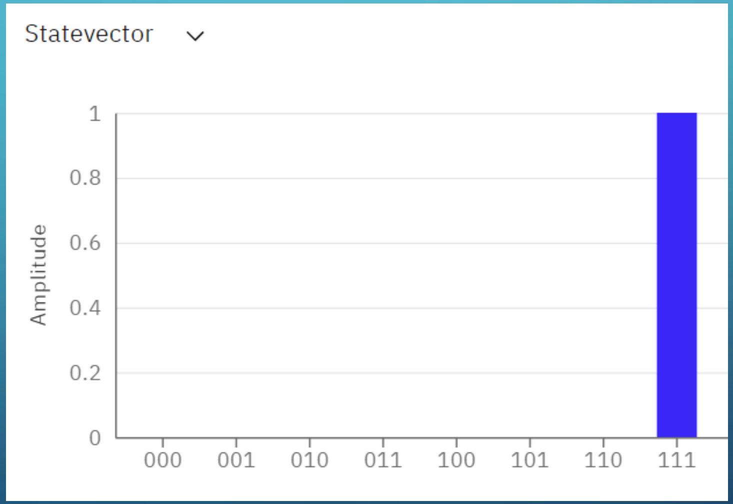
IBM Q EXPERIENCE – QUANTUM PARALLELISM

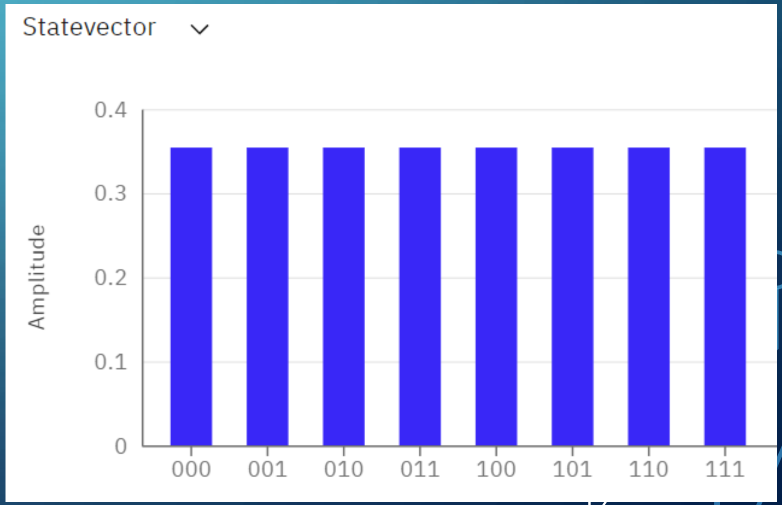












#4 - QUANTUM PARALLELISM

- Resembles data parallelism: **the same algorithm** is **simultaneously applied to all possible states**, but **without replication of resources**
- Caveat: when a **measurement** is performed to access the result, only **a single state is read**, and this is **stochastically selected**
- **Information on all other states is lost**
- This irreversible loss of information means that even though the **computation evolves on an exponentially large state space**, we only have **access to a very limited portion of it**

#5 - NO-CLONING THEOREM

- **Quantum information cannot be copied!**
- There is no unitary transformation that copies one arbitrary quantum superposition in one register to another register:

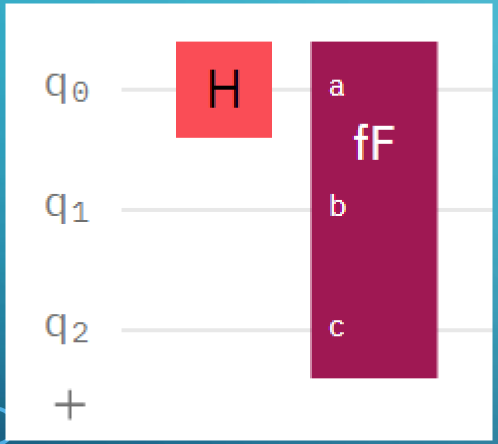
$$|R\rangle|Q\rangle \longrightarrow U|R\rangle|Q\rangle = |R\rangle|R\rangle$$

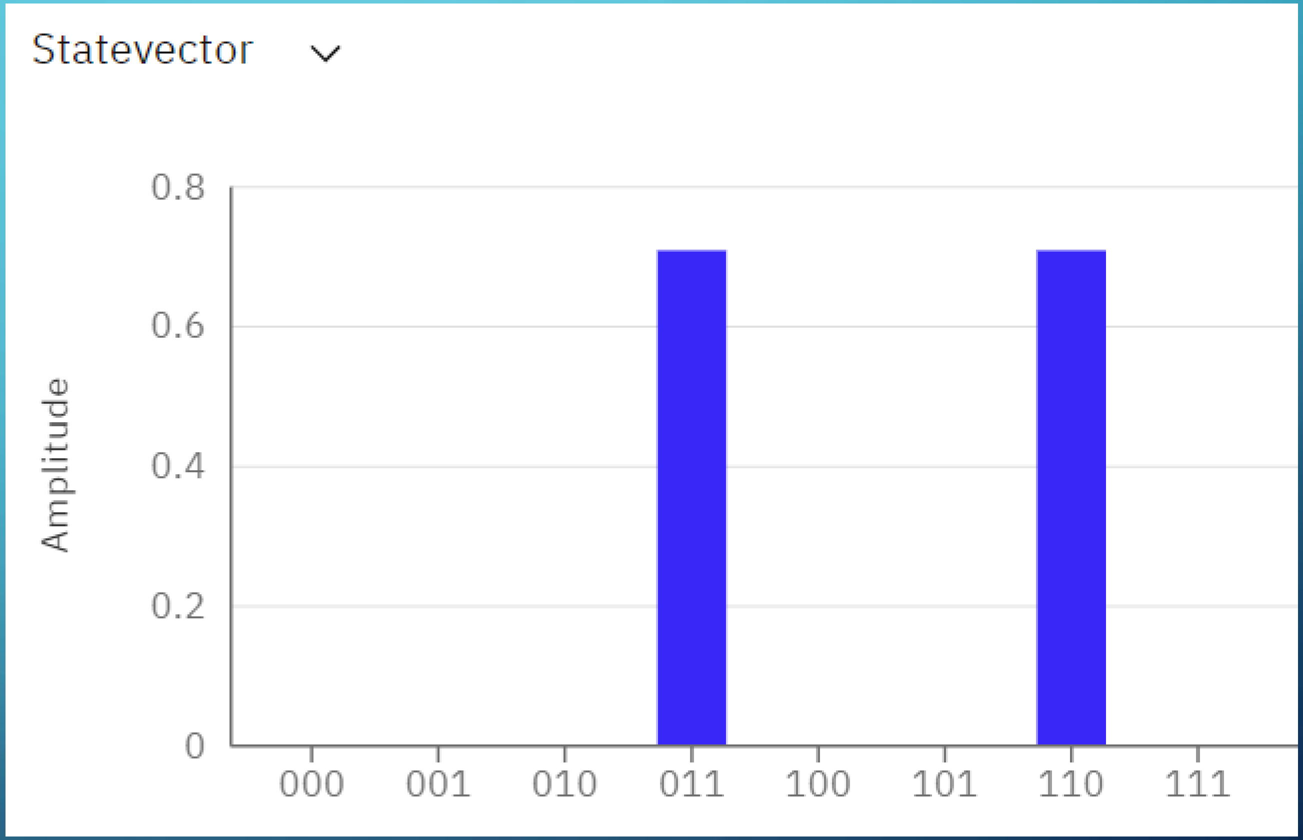
- **Copying intermediate results** into temporary storage (variables) is thus **impossible**

#6 – INITIAL STATE

- Quantum algorithms require that **quantum registers are initialized to some known state**
- This **initial state** is referred to as the **ground state** and usually made to be the **basis state** $|0\rangle$
- **Loading data** to the quantum registers may in many cases require a number of gates (computation) larger than the number of gates necessary to execute the intended algorithm, **offseting the quantum advantage**

MEASUREMENTS ON A SIMULATOR





MEASUREMENTS ON A REAL SYSTEM