QUANTUM COMPUTING INTRODUCTION

LUÍS PAULO SANTOS

NOVEMBER, 2018

BRIEF HISTORICAL OVERVIEW

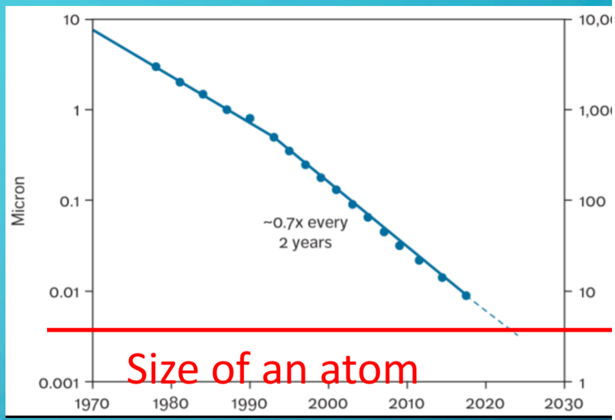
- **Quantum systems** evolve in a **state space exponentially larger than the number of parameters** require to define each state

- 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



- Moore's Law: since 1960 semiconductor size has halved every two years;
- By 2020 circuits will be dominated by quantum effects
- By 2050 circuits will reach the minimum scale at which information can be physically represented
- Is Quantum Computing a natural consequence of Moore's law?

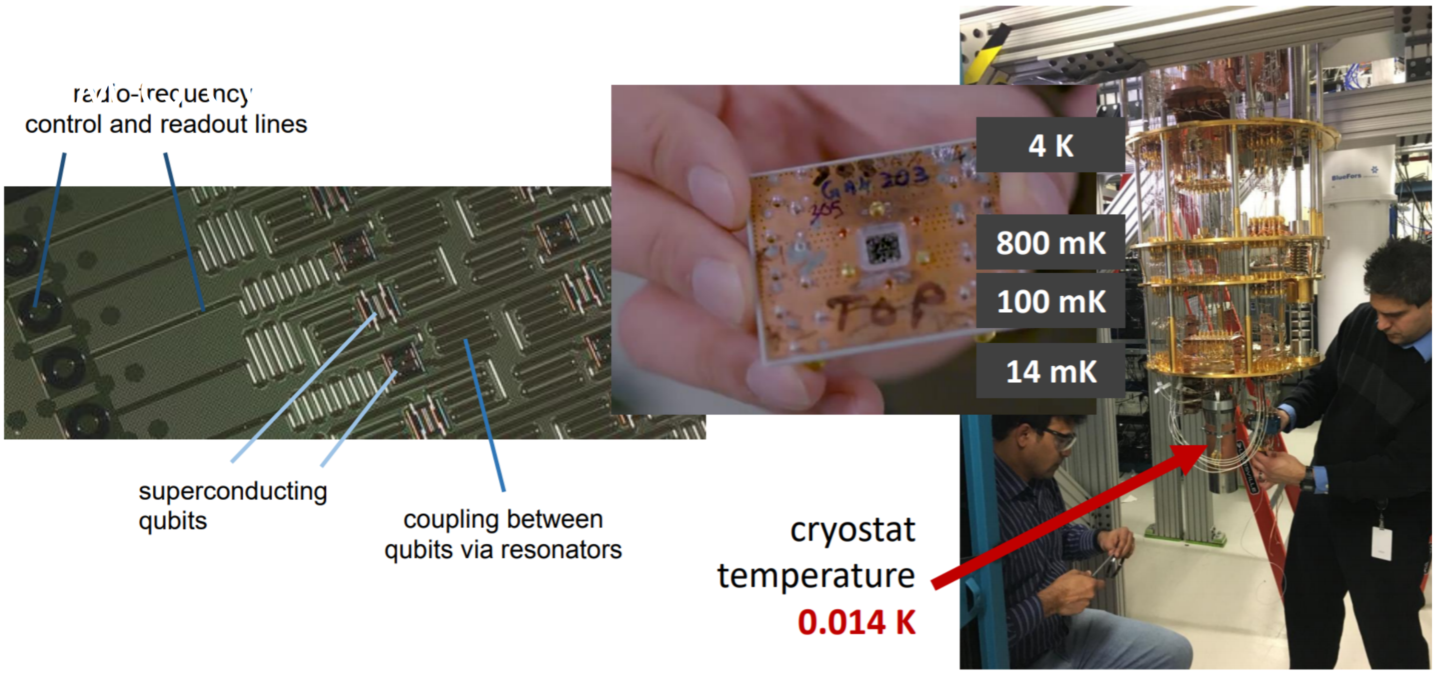
BRIEF HISTORICAL OVERVIEW

- 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)

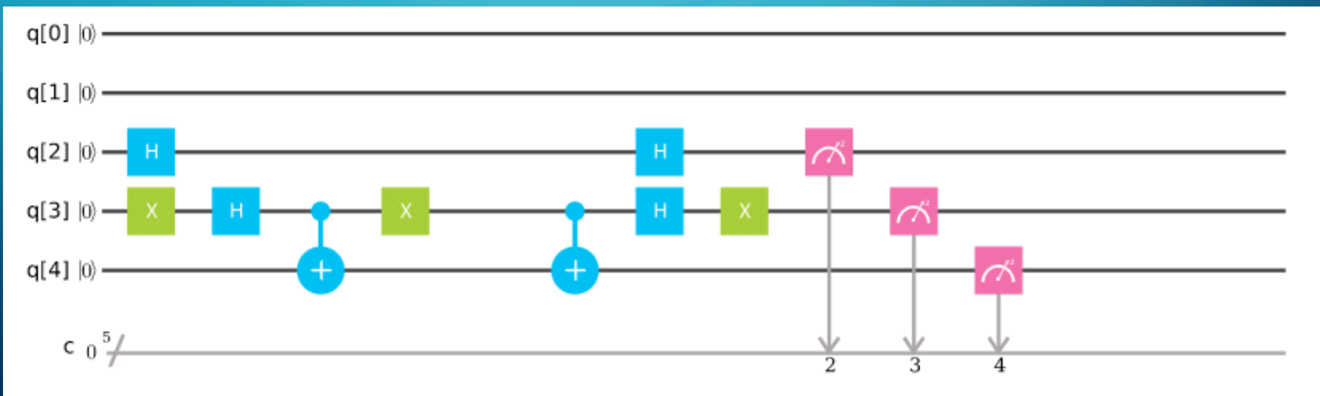
[1] Adiabatic quantum computers can reach 2000 qubits (D-Wave 2000Q System), but operate based on the simulated annealing algorithm and the adiabatic theorem, requiring the modelling of optimization problems as physical Hamiltonians



"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 classic computers: **quantum gates** operate on **quantum states**



QUANTUM COMPUTING PROPERTIES

#1	Qubit	#4	Quantum Parallelism
#2	Measurement	#5	No-Cloning Theorem
#3	Reversible Transitions	#6	Initial State

#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

#1 - QUBIT

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

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

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

#1 - QUBIT

- Example: 2-qubits superposition

- Only n qubits are require to represent $N=2^n$ states

    A classical machine requires $N*n$ bits to represent N states

    Example: 3 qubits can simultaneous represent 8 states
    24 = 8*3 bits are require to represent the 8 states

#2 - MEASUREMENT

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

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

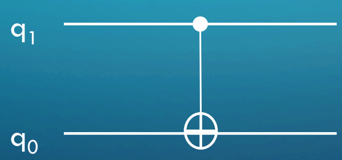
#3 – REVERSIBLE TRANSITIONS

- Physical laws require all **quantum transitions** to be **reversible**; given the outputs the inputs can be known!
- Mathematically, this means that the **transformation** matrix is **unitary**

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

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



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

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

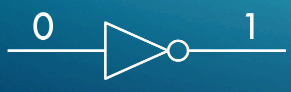
$$|\Psi'\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_3|10\rangle + \alpha_2|11\rangle$$

#3 – REVERSIBLE TRANSITIONS

Under unitary transformations **the Euclidean norm** of the coefficients **is preserved** to be unity – probabilistic model

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,\ \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \Rightarrow |\Psi'\rangle = U|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i' |i\rangle,\ \sum_{i=0}^{2^n-1} |\alpha_i'|^2 = 1$$

While classical circuits are seen as operating over the state,
quantum circuits are thought as operating over the coefficients



classical

quantum

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$$|\Psi'\rangle = \alpha_1|0\rangle + \alpha_0|1\rangle$$

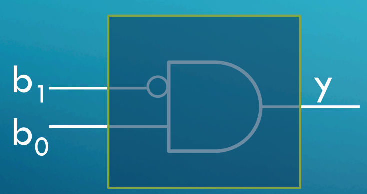
#3 – REVERSIBLE TRANSITIONS

- Unitary transformations have a **number of outputs equal to the number of inputs**
- **Classical** boolean **gates are not reversible**
- Quantum gates:
  - NOT: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
  - Hadamard: $1/\sqrt{2}\ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ 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): $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

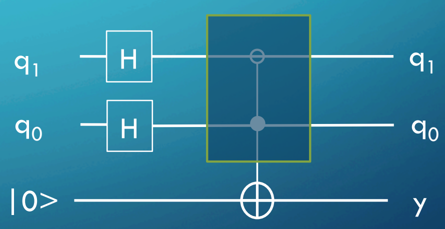
#4 - QUANTUM PARALLELISM

- 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 $|q_1\ q_0\ y\rangle$, but …

#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**

QUANTUM COMPUTING: GROVER'S ALGORITH

LUÍS PAULO SANTOS

NOVEMBER, 2018

- Problem Statement: https://www.youtube.com/watch?v=nZXq28oSSjM
- Quantum Problem Statement: https://www.youtube.com/watch?v=tu6E9XhXMDs
- Grover Algorithm outline: https://www.youtube.com/watch?v=7tc3DCAJC7E (negation and inversion)

PROBLEM STATEMENT: FUNCTION INVERSION

- Let $f:\{0,1,\ldots,2^n-1\}\rightarrow\{0,1\}$, with $\begin{cases} f(x)=0 \ if \ x\neq x^* \\ f(x)=1 \ if \ x=x^* \end{cases}$
- Grover's algorithm returns, with high probability, $x^*: f(x^*)=1$
- On its simplest form requires that there is a single solution x^*
- It has been extended to include multiple (M) solutions, both for the cases where M is known and unknown

PROBLEM STATEMENT EXAMPLE: SEARCH

- Let *v* be a vector (array) with 2^n elements
- Grover's algortihm can be thought as searching for the index of some unique key, *y*, within this vector:

$$\begin{cases} f(x)=0 \ if \ v[x]\neq y \\ f(x)=1 \ if \ v[x]=y \end{cases}$$

CLASSICAL PROBLEM COMPLEXITY

Given that:

- Nothing is known about $f(x)$, i.e., there is no known structure
- The values of $f(x)$ for each x can only be known by evaluating $f(x)$

then a classical solution for finding $x^* : f(x^*)=1$ requires, in the worst case, evaluating all $N=2^n$ values of x; its complexity is $\mathcal{O}(N)$

QUANTUM PROBLEM DEFINITION: ORACLE

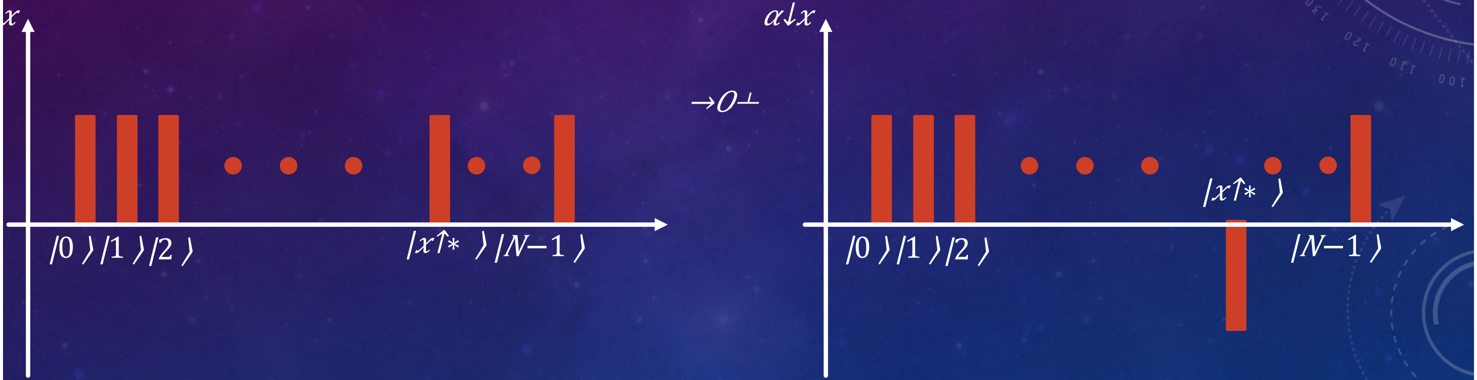
- $f(x)$ becomes the operator O, which is applied to an uniform superposition of all states $|s\rangle = 1/\sqrt{2^n} \sum_{x=0}$
- O is referred to as the "Oracle"
- It negates state $|x^*\rangle$ sign:

$$O|s\rangle = 1/\sqrt{2^n}\left[\sum_{x=0,\, x\neq x^*}^{2^n-1} |x\rangle - |x^*\rangle\right]$$

ORACLE INTERPRETATION

- The oracle negates the sign of the desired state $|x^*\rangle$:

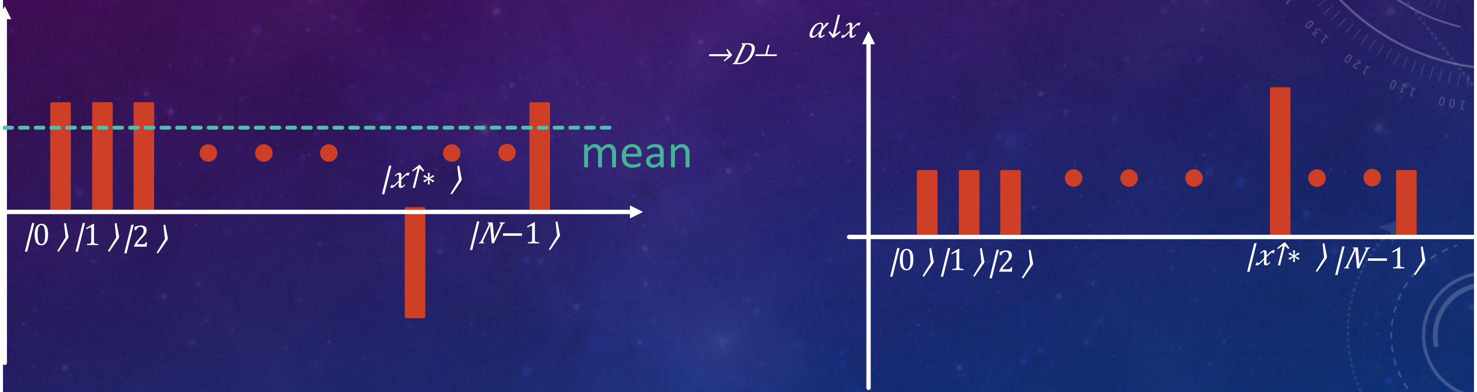
$$O|s\rangle = 1/\sqrt{2^n}\left[\sum_{x=0,\, x\neq x^*}^{2^n-1} |x\rangle - |x^*\rangle\right]$$



The probability of measuring each state doesn't change: $P(x) = |\alpha_x|^2$

GROVER'S DIFFUSION OPERATOR

Grover's diffusion operator D reflects the coefficients over their mean



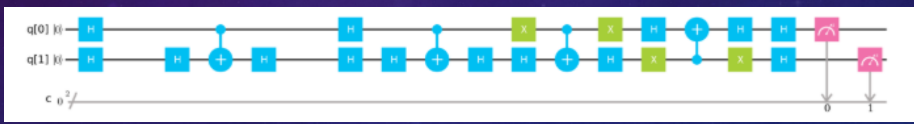
The probability of measuring $|x^*\rangle$ is amplified

QUANTUM PROBLEM COMPLEXITY

- The sequence of operators DO is applied in sequence r times
- The state $\psi^{(r)}$ that maximizes the probablity of measuring $|x^*\rangle$ is given by $\psi^{(r)} = (DO)^r |s\rangle$
- $r = \lceil \sqrt{2^n} \rceil = \lceil \sqrt{N} \rceil$
- The oracle is therefore executed $\mathcal{O}(\sqrt{N})$ times

GROVER IMPLEMENTATION: 2 QUBITS

- According to https://www.youtube.com/watch?v=Uw6zEMSxKvg



- Optimized according to https://www.youtube.com/watch?v=hfxAQtO19Wg