



Qubit e a Computação Quântica

Mentor: Tiago Gonçalves

Participantes: Pedro Ramos e Raquel Freixo



ÍNDICE

01

INTRODUÇÃO

Introdução à Computação Quântica

03

CIRCUITOS E ALGORITMOS

Algoritmo Half-Adder
Algoritmo de Deutsch-Jozsa

02

QUBITS E GATES

Diferenças entre Computação Clássica e Computação Quântica

04

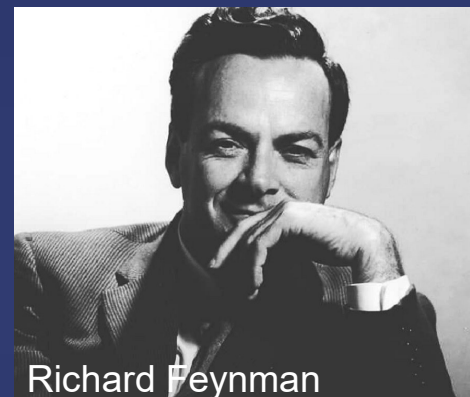
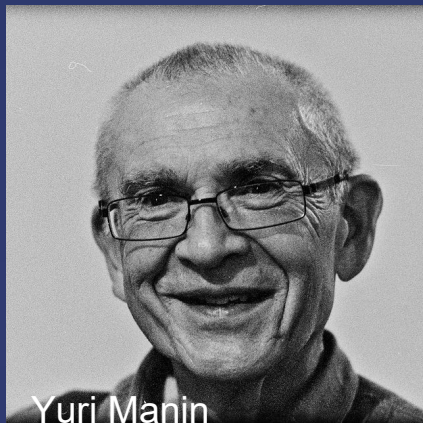
OUTRAS COISAS

Algoritmo de Grover
Protocolo BB84



Computação Quântica

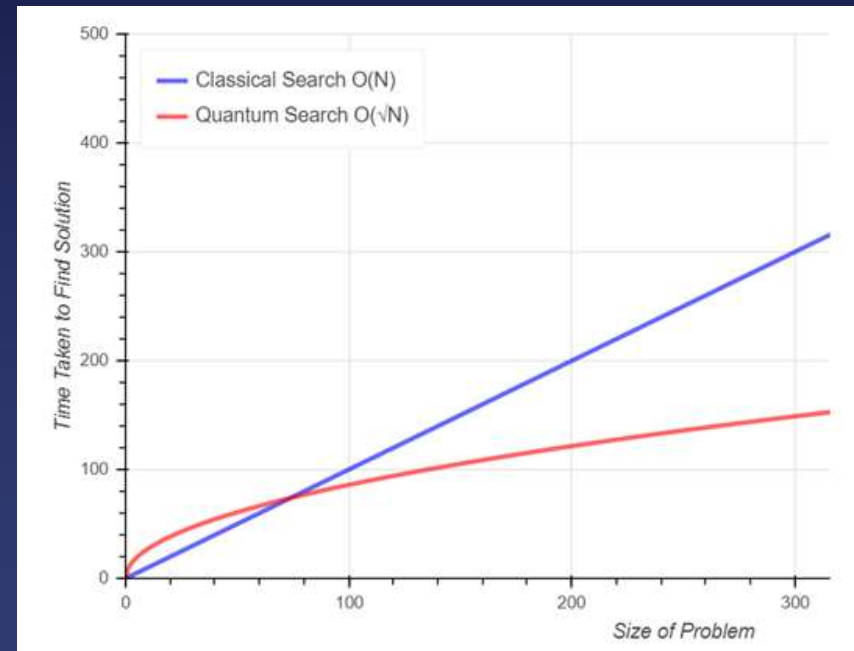
1. A computação quântica teve a sua origem na década de 80 com físicos como Richard Feynman e Yuri Manin, que propuseram que um computador quântico seria capaz de simular coisas impossíveis para um computador clássico
2. Em 1994 a área de estudo foi alvo de um grande e renovado interesse após Peter Shor desenvolver um algoritmo para fatorizar números inteiros
3. Nos últimos anos, a computação tem recebido grande investimento enquanto centros de investigação por todo o mundo tentam alcançar o novo horizonte da tecnologia



Vantagens da Computação Quântica

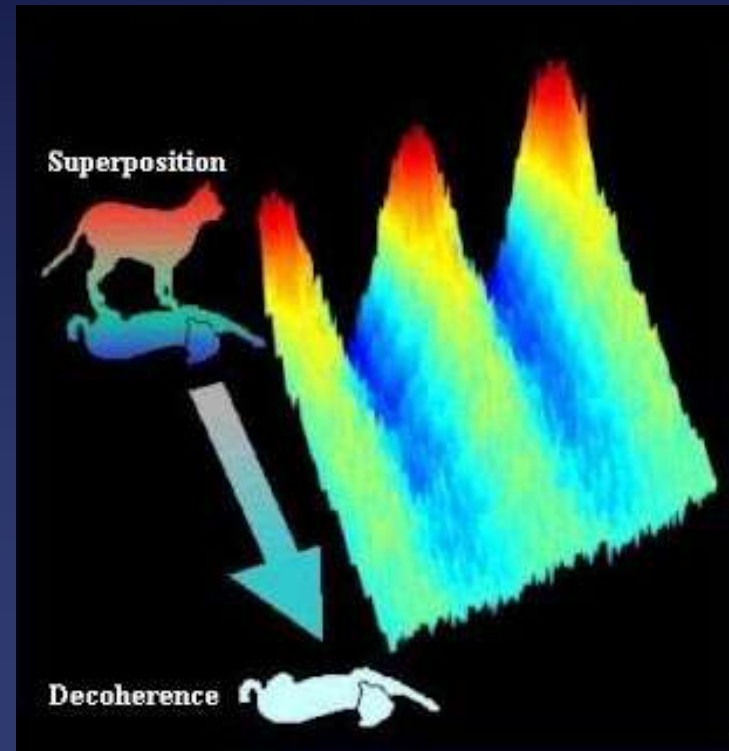
1. Computadores quânticos conseguem executar tarefas com complexidade bastante diferente da de computadores clássicos
2. Algoritmos quânticos são especialmente poderosos em problemas de determinar propriedades globais de funções
3. Estados de sobreposição são uma das grandes razões para o sucesso da computação quântica

$$|\Psi\rangle = \frac{|\text{girafa}\rangle + |\text{leão}\rangle}{\sqrt{2}}$$



Desvantagens da Computação Quântica

1. Escalabilidade
2. Problema da decoerência quântica
3. Material (raro e/ou caro)

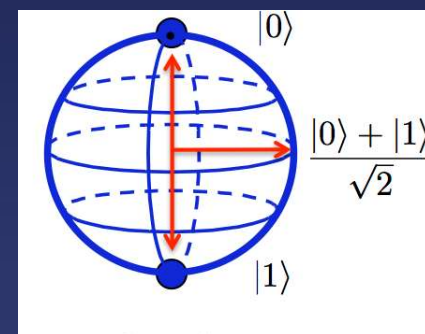


Computação Clássica



Bit Clássico

Computação Quântica



Bit Quântico



Computação Clássica



1. Os bits são a base da computação clássica
2. Os bits são um estado lógico de dois valores possíveis
3. Circuitos clássicos são feitos usando portas lógicas



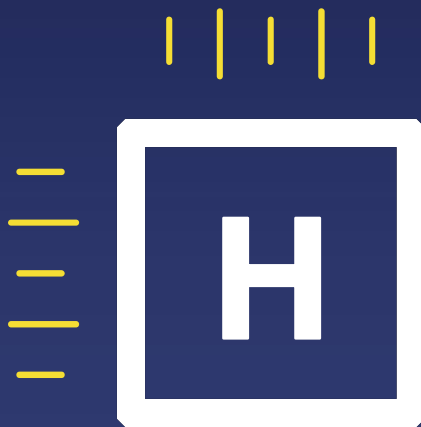
Computação Quântica



1. Os qubits são a base da computação quântica
2. Os qubits são um estado quântico de dois níveis podem estar num estado de sobreposição
3. Circuitos clássicos são feitos usando gates quânticos



Gates



O que são gates?

- No computador quântico, gates são operadores que alteram o estado do qubit
- Ao contrário das portas lógicas clássicas, as gates não executam operações booleanas entre qubits
- Podem ser representadas por matrizes

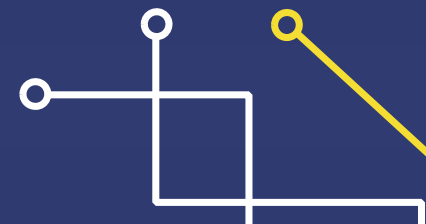
Tipos de Gates

NOT 

CNOT 

TOFFOLI 

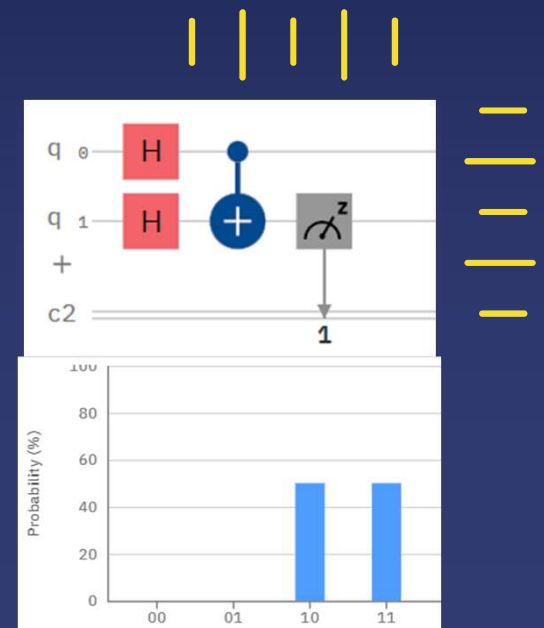
HADAMARD 



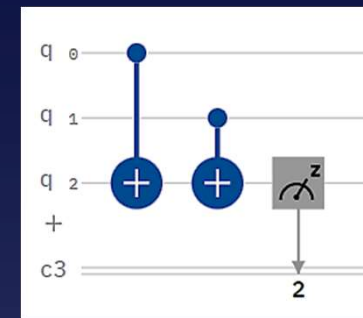
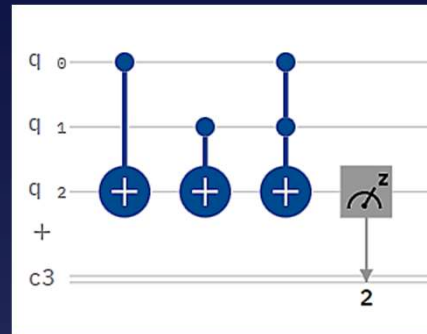
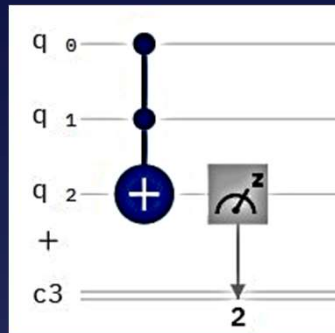
Circuitos Quânticos

O que é um circuito quântico?

- Os computadores quânticos em que nos focamos funcionam com base num modelo de circuito
 - As linhas horizontais representam um qubit
 - Gates são inseridas nas linhas e atuam no respetivo(s) qubit(s)
 - Medições são registadas no registo clássico
- No IBM Quantum Experience é apresentado um histograma com a probabilidade de se medir cada estado



Tipos de Circuitos Quânticos

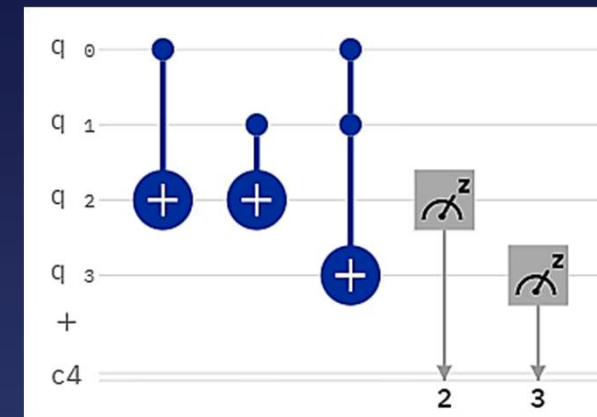


INPUT	AND	OR	XOR
00	0	0	0
01	0	1	1
10	0	1	1
11	1	1	0

Circuito Half-Adder: o que é e como funciona

O que é um circuito Half-Adder?

- É o circuito básico para realizar somas computacionalmente
- São necessários 4 qubits: 2 para input e 2 para guardar o output
- O circuito constrói-se facilmente percebendo que a primeira coluna é igual a uma porta AND e a segunda uma porta XOR

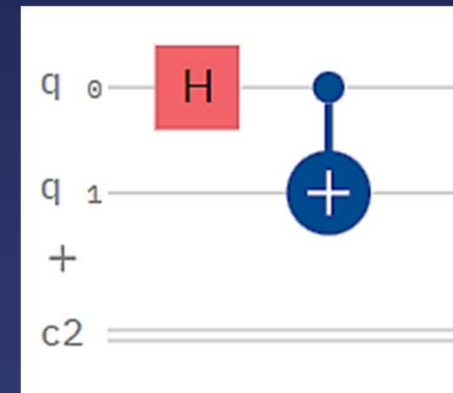


INPUT	OUTPUT
0 0	0 0
0 1	0 1
1 0	0 1
1 1	1 0

Entrelaçamento Quântico

É possível criar estados entrelaçados de dois qubits

- Este circuito coloca dois qubits num estado de Bell
- Os estados de Bell são um conjunto de estados entrelaçados, que têm características especiais relativas à sua medição



Exemplo de um estado de Bell

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



Algoritmo de Deutsch-Jozsa

O que é o problema de Deutsch-Jozsa?

- É-nos dada uma black box que implementa uma função binária
- Sabemos que a função ou é constante ou é balanceada
- O problema é descobrir se a função é constante ou balanceada

$$f: \{0, 1\}^n \rightarrow \{0, 1\}$$




Computação Clássica

- Verificar o output de cada input um a um
- Assim que houver um output que seja diferente dos obtidos até então confirmamos que a função é balanceada
- Se mais de metade dos outputs forem o mesmo então é constante
- É necessário testar no mínimo 2 e no máximo $N/2+1$



Computação Quântica

- 
- Colocar os bits de input num estado de sobreposição de todos os estados da base, usando as gates de Hadamard
 - Depois, passar este estado de sobreposição pelo "Oracle"
 - Depois de passar pelo "Oracle" uma única vez temos a informação necessária para aferir se a função é constante ou balanceada

Implementação do Algoritmo de Deutsch-Jozsa

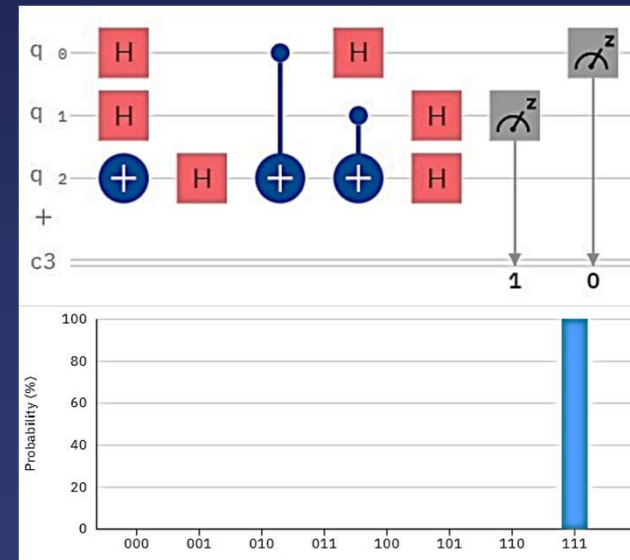
- A função é constante se medirmos $|00\rangle$ com 100% de probabilidade nos dois qubits de input

$$f(0, 0) = 0$$

$$f(0, 1) = 1$$

$$f(1, 0) = 1$$

$$f(1, 1) = 0$$



THANKS!

Mentor: Tiago Gonçalves

Participantes: Pedro Ramos e Raquel Freixo

