Computação Quântica

Caio Quinta Naiane Yanachi Renan Alves

MAC5742/0219 - Introdução à Programação Concorrente, Paralela e Distribuída
Prof Alfredo Goldman - 1º Semestre/2017

Tópicos

- Contexto histórico
- Conceitos básicos
- Algoritmos
- Atualmente
- Perspectivas

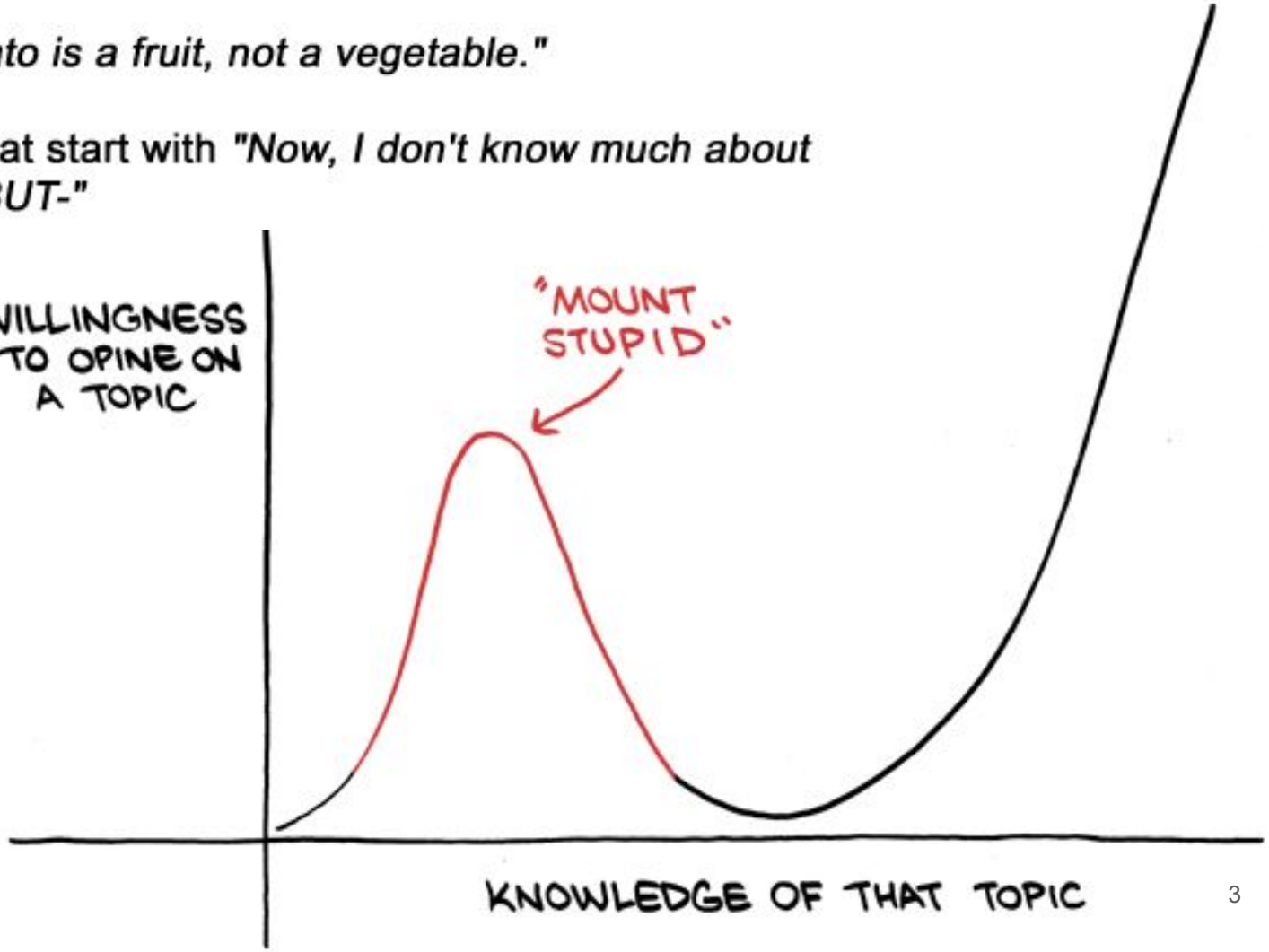
Phrases uttered atop Mount Stupid:

- *"Historically, the Amazons would cut off their right breast so they could shoot a bow and arrow."*

- *"The American Civil War really had nothing to do with slavery."*

- *"Biologically, tomato is a fruit, not a vegetable."*

- 99% of phrases that start with *"Now, I don't know much about quantum physics, BUT-"*



Contexto Histórico

- Primeira Menção: Feynman, 1981, afirma que é possível criar uma máquina capaz de tirar vantagens da mecânica quântica para simulações físicas.
- Deutsch, 1984, escreve um artigo com um modelo teórico para um computador quântico.
- 1994, Shor divulga o seu Algoritmo para fatoração de grandes números.
- 2010, D-Wave lança o primeiro computador quântico comercial: o D-Wave One.

Conceitos Básicos

Qubit

- Unidade básica da computação quântica
- Abstração das propriedades físicas subjacentes
  - Superposição
  - Emaranhamento
- Valores básicos:
  - $|0\rangle$ (“zero ket”) : ao ser medido obtém-se bit clássico 0
  - $|1\rangle$ (“um ket”) : ao ser medido obtém-se bit clássico 1

Superposição

- O qubit pode estar em uma combinação linear de $|0\rangle$ e $|1\rangle$
- $2^{(-½)}$ $(|0\rangle + |1\rangle)$ é um qubit em superposição
- Ao ser medido, pode resultar em um 0 ou 1 clássico com 50% de probabilidade

Superposição

Emaranhamento

- Emaranhamento é uma propriedade que um sistema com dois ou mais qubits pode apresentar
- Apesar do resultado de medição individual de cada qubit não ser determinado, ao medir um qubit há correlação com o resultado do segundo
- Exemplo: 2^(-1) (|00⟩ + |11⟩)
  - Medir um qubit pode resultar em 0 ou em 1
  - Se a primeira medição resultar em 0 a segunda também resultará

Portas lógicas

- Operações que transformam os estados dos qubits
- Exemplos:
- Porta X, conhecida como NOT pois altera $|0\rangle$ para $|1\rangle$ e vice-versa
- Porta de Hadamard: utilizada para formar superposições
- CNOT: semelhante ao XOR, utilizada para formar emaranhamentos

Algoritmos

Deutsch-Jozsa: Problema

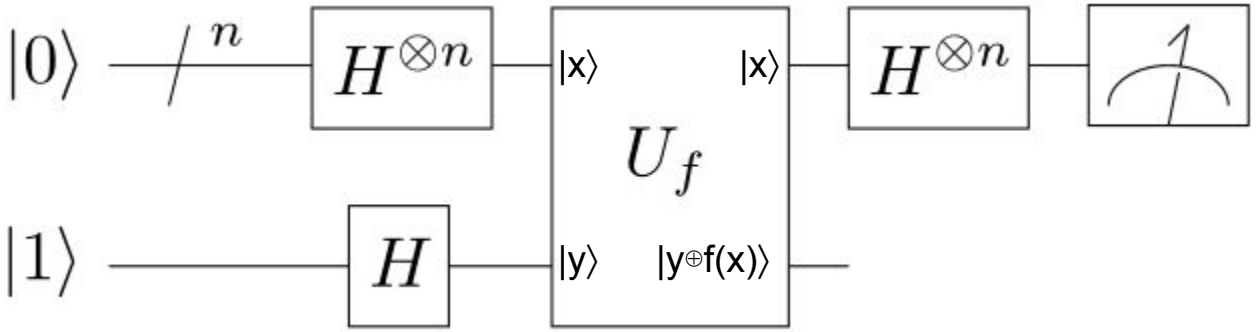
- Feito para demonstrar poder da computação quântica
- Não é um problema de realidade prática

Enunciado:

- Dado um oráculo de uma função f: $\{0, 1\}^n \rightarrow \{0,1\}$, responder se f é constante ou balanceada
- É prometido que f seja constante ou balanceada

Deutsch-Jozsa: Resolução

- Algoritmo clássico: necessita $2^{n-1}+1$ consultas ao oráculo
- Algoritmo quântico: necessita de 1 consulta ao oráculo
  - N qubits são inicializados em $|0\rangle$, e 1 qubit em $|1\rangle$
  - Porta de Hadamard coloca os qubit em superposição
  - Operador U_f utiliza o oráculo para calcular $|y \oplus f(x)\rangle$
  - Medição da saída será 0 se a função for constante

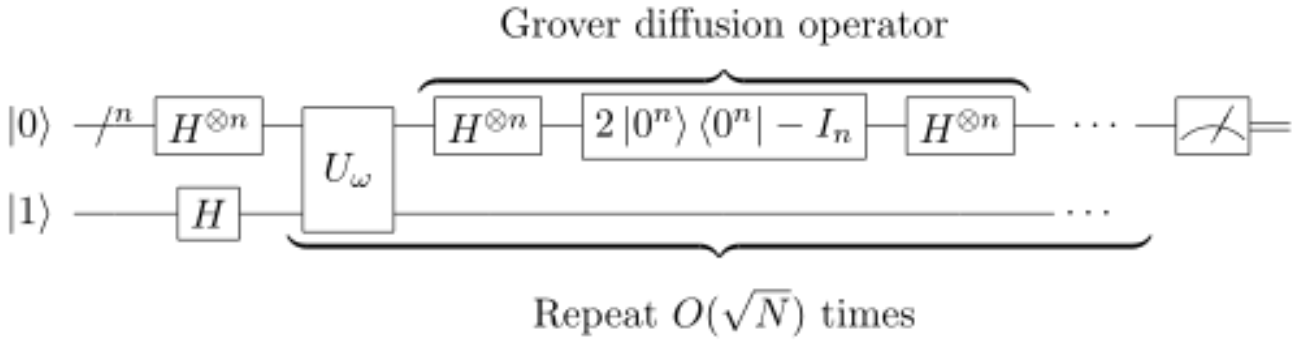


Busca de Grover

- A busca de Grover é um algoritmo de busca para listas não ordenadas, bancos de dados, etc.
- Algoritmo probabilístico capaz de efetuar uma busca em tempo assintótico $O(\sqrt{N})$, oferecendo um speedup quadrático sobre o limite de $O(N)$ em um computador convencional.

Busca de Grover

- Iteração de Grover: Consiste em uma função caixa-preta oráculo e um operador que são repetidos O(√N) vezes para encontrar a resposta com maior probabilidade.



Algoritmo de Shor - Introdução

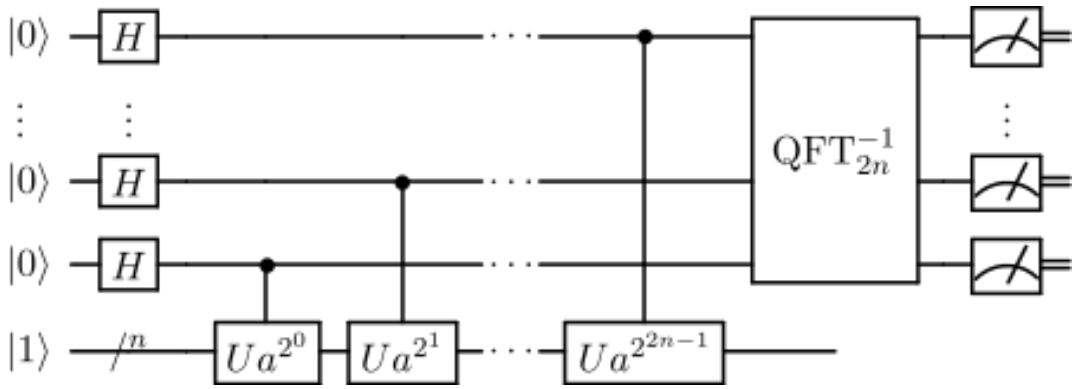
- Objetivo: Fatorar grandes inteiros em tempo polinomial.
- Complexidade: O((logN)^3) e utiliza 3logN qubits
- Faz uso da superposição quântica para chegar a um resultado com alta probabilidade.
- Capaz de quebrar uma criptografia de chave pública RSA.
- O maior número fatorado utilizando esse algoritmo foi 21 em 2012 devido as limitações tecnológicas atuais.

Algoritmo de Shor - Explicação Breve

- Seja N = p x q, p e q primos, existe uma única fatoração possível.
- Para x < N e a sequência: x mod N, x^2 mod N, x^3 mod N... existe um período em que ela começa a repetir, t.q, esse período divide (p-1).(q-1).
- Ex.: N = 15 temos p=3,q=5. Tome x = 2 e temos a sequência 2,4,8,1,2,4,8,1 com periodo igual 4. Logo (p-1).(q-1) = 2 x 4 = 8 e é divisível por 4.

Algoritmo de Shor

- Encontrar o período de N.
- Problema: O período pode ser tão grande quanto N, razão pela qual não existem algoritmos convencionais.
- Solução proposta utiliza uma superposição quântica para encontrar o período.



Comunicação

- Não é possível copiar, mover ou teleportar a informação, sem que o original seja destruído
- Segurança
- Criptografia
  - Fótons
  - QKD

Atualmente

D-Wave 2000Q™ System

D-Wave 2000Q™ System

- 2048 qubits e 5600 couplers
- Consome 25 kW (Super Computador 2500 kW)
- Preço: 15 milhões de dólares

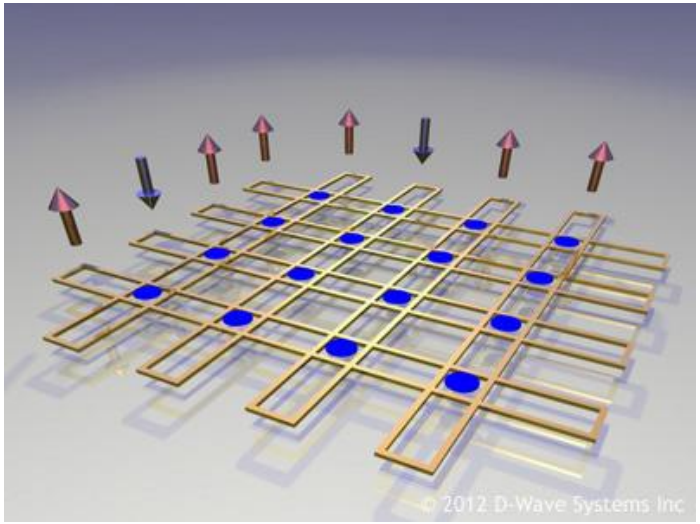
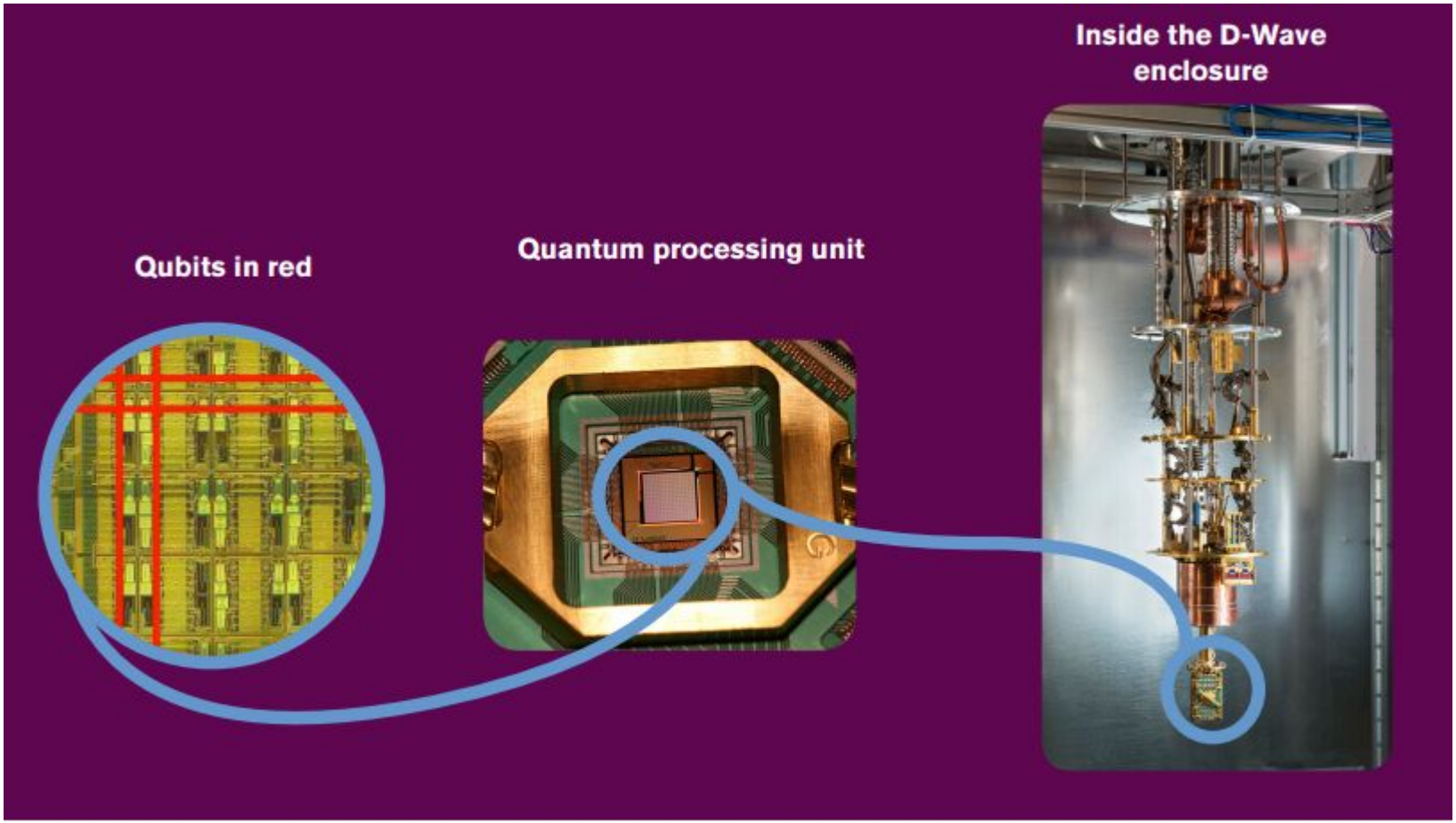


Fig: 8 qubits loops (dourados) e 16 couplers (pontos azuis)

Fonte:
https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware

D-Wave 2000Q™ System



D-Wave 2000Q™ System

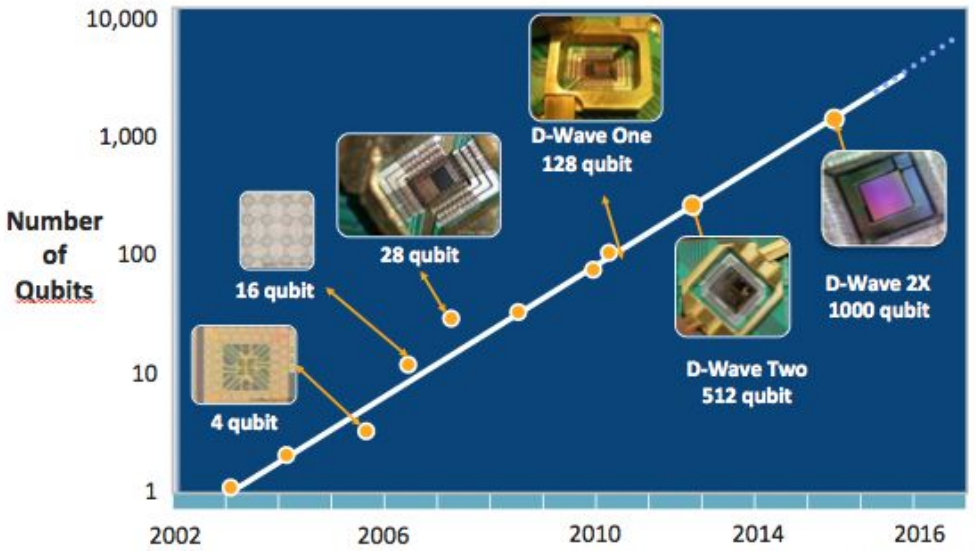
- Acesso via Cloud
  - API's disponíveis em: C/C++, Python, and MATLAB
- D-Wave tools:
  - Qsage: "translator" para problemas de otimização
  - ToQ: Constraint Satisfaction Problems
  - Qbsolv: Open-Source - hybrid partitioning optimization solver
- Escrever as Quantum Machine Instructions (QMIs) diretamente.

Fonte:
https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware

Perspectivas

Perspectivas

- Lei de Rose: Nos últimos 8 anos o número de qubits dobrou a cada ano. A expectativa é que até 10000 qubits não seja necessário um redesign do processador, apenas adicionar novos qubits



Perspectivas

- Canada's Quantum Valley: Em 2013 o fundador da BlackBerry criou um fundo de investimento de 100 milhões de dólares para empresas que empreguem aplicações práticas em física quântica.
- Criado o Institute for Quantum Computing, University of Waterloo - Canadá.
- Objetivo de ser o maior polo de Pesquisa Quântica no Mundo

Fonte:
https://uwaterloo.ca/institute-for-quantum-computing/news/quantum-technologies-priority-canada

Perspectivas

- 18 Empresas que já estão trabalhando na área, entre elas:
  - Google: Supercomputador da D-Wave em um laboratório em conjunto com a Nasa e desenvolvimento de chips próprios.
  - Microsoft: Centro de pesquisa para desenvolvimento de algoritmos Quânticos (vagas disponíveis :): https://www.microsoft.com/en-us/research/group/quantum-architectures-and-computation-group-quarc/
  - Intel: Fez um investimento de 50 milhões na Qutech, um centro de pesquisa em computação quântica.

Fonte: https://www.cbinsights.com/blog/quantum-computing-corporations-list/#head12

Perspectivas

- Miniaturização das memórias estáticas
- Memória quântica
- Menor unidade de armazenamento: um átomo!

Fonte: http://www.nature.com/news/magnetic-hard-drives-go-atomic-1.21599