Encontros Matemáticos apresenta

Computação Quântica

Pedro Maciel Xavier pedromxavier@poli.ufrj.br 19 de novembro de 2019



IM-UFRJ

Parte I

Computação

Álgebra Booleana

Computabilidade

Complexidade

Computação Digital

O Bit

Transistor

Portas Lógicas

Arquitetura de Von Neuman

Lei de Moore

Parte II

Computação Quântica

Fenômenos Quânticos

Postulados

Trapped-ion

Algoritmos

Teletransporte Quântico

Teorema da não-clonagem

Fótons

Caminhadas Quânticas

Computação Topológica

Nós

Ânions

Computação Adiabática

Teorema Adiabático

Têmpera Quântica

Parte III

Fim?

- Saltos Quânticos
- Supremacia Quântica
- Material
- ${\bf Bibliografia}$

Computação

Computabilidade

A Tese de Church-Turing

Toda função que seria naturalmente computável pode ser computada por uma Máquina de Turing

Alan Turing

Computabilidade

Definição. (Máquina de Turing)

É um computador abstrato definido por $(Q, q_0, \Gamma, \Box, \Sigma, \Omega, \delta)$, que possui uma fita e um cabeçote de leitura

Q: Um conjunto não-vazio de estados.

 q_0 : Estado inicial $(q_0 \in Q)$

 Γ : Alfabeto da fita.

□: Símbolo vazio.

 Σ : Alfabeto de entrada da máquina. ($\Sigma \subseteq \Gamma/\{\Box\}$)

 Ω : Conjunto dos códigos de parada.

 $\delta \colon$ Função de Transição, $\delta : Q/\Omega \times \Gamma \to Q \times \Gamma \times \{\uparrow,\downarrow\}$

Computabilidade



Alonzo Church 1903 - 1955



Alan Turing 1912 - 1954

Computabilidade

A Tese de Church-Turing

Toda função que seria naturalmente computável pode ser computada por uma Máquina de Turing

Alan Turing

Definição. (Complexidade Assintótica)

Seja
$$f:X\subseteq\mathbb{R}_+\to\mathbb{C}$$
 e $g:X\subseteq\mathbb{R}_+\to\mathbb{R}_+$ dizemos que

$$f(x) = O(g(x)) \iff \exists M, x_0, \quad |f(x)| \le Mg(x) \quad \forall x > x_0$$

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

5 2 3 1 4

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

5 5 2 3 1 4 1

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

$$5+4$$

$$\boxed{5 \ 2 \ 3 \ 4}$$

$$\boxed{1 \ 2}$$

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

- 5 + 4 + 3
- 5 3 4
- 1 2 3

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

$$5 + 4 + 3 + 2$$

- 5 4
- 1 2 3 4

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

$$5+4+3+2+1=15$$

5

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

$$5 + 4 + 3 + 2 + 1 = 15$$

5

Mas e se a lista tivesse n elementos?

Exemplo. (Ordenação de uma lista)

Dada uma lista de tamanho N=5, fazemos o seguinte: Procuramos o menor elemento, removemos da lista e acrescentamos em uma nova lista, e assim sucessivamente.

$$5 + 4 + 3 + 2 + 1 = 15$$

5

Mas e se a lista tivesse n elementos?

$$T(n) = \frac{n(n+1)}{2} = \frac{n^2 + n}{2}$$
 (complexidade)

Dizemos que este algoritmo tem complexidade $O(n^2)$.

Computação Digital

Álgebra Booleana

Definição. (Álgebra Booleana)

É uma estrutura algébrica $(\Omega, \vee, \wedge, \neg, 0, 1)$, com $0, 1 \in \Omega$, que satisfazem os Axiomas:

Álgebra Booleana



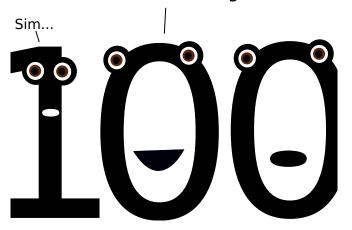
George Boole 1815 - 1864



Augustus De Morgan 1806 - 1871

Não! Sim! Uhum

Finalmente! É o meu grande dia!



SIM!

A problem has been detected and Windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow

PAGE_FAULT_IN_NONPAGED_AREA

for any Windows updates you might need.

these steps: Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

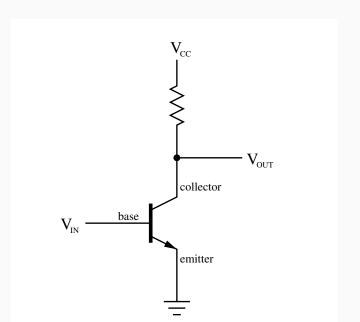
Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c



Transistor



Portas Lógicas

Arquitetura de Von Neuman

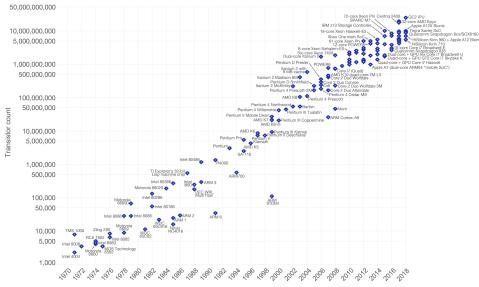


John Von Neuman 1903 - 1957

Moore's Law – The number of transistors on integrated circuit chips (1971-2018)



Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.



Lei de Moore



Gordon Moore Intel, 1965

Computação Quântica

Fenômenos Quânticos



Richard Feynman 1918 - 1988

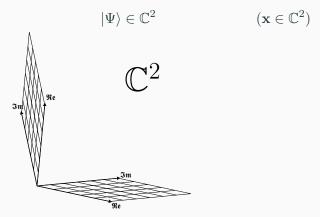
Postulados

Postulado. (Representação)

Um sistema físico isolado está associado a um espaço de Hilbert \mathcal{H} e é, num dado momento no tempo, completamente descrito por um vetor unitário em \mathcal{H} , o estado do sistema.

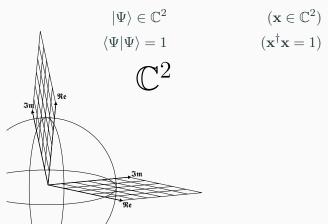
Postulado. (Representação)

Um sistema físico isolado está associado a um espaço de Hilbert \mathcal{H} e é, num dado momento no tempo, completamente descrito por um vetor unitário em \mathcal{H} , o estado do sistema.



Postulado. (Representação)

Um sistema físico isolado está associado a um espaço de Hilbert \mathcal{H} e é, num dado momento no tempo, completamente descrito por um vetor unitário em \mathcal{H} , o estado do sistema.



Postulado. (Composição)

Um sistema é descrito pela composição dos estados que o representam, que se dá através do *produto tensorial*.

$$|\Psi\rangle\otimes|\Phi\rangle\equiv|\Psi\Phi\rangle$$

Definição. (Produto de Kronecker)

É um caso particular do *produto tensorial*, computado da seguinte forma:

$$\mathbf{x} \otimes \mathbf{y} \equiv \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \otimes \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 & y_1 \\ y_2 \\ x_2 & y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 y_1 \\ x_1 y_2 \\ x_2 y_1 \\ x_2 y_2 \end{bmatrix}$$

Ele é bilinear e associativo, mas não é comutativo :(

Definição. (Produto de Kronecker)

Mas nem tudo está perdido. Tem outras propriedades legais também!

Produto misto:

$$U \otimes V \cdot |\Psi\rangle \otimes |\Phi\rangle = U |\Psi\rangle \otimes V |\Phi\rangle \quad \mathbf{A} \otimes \mathbf{B} \cdot \mathbf{x} \otimes \mathbf{y} = \mathbf{A} \cdot \mathbf{B} \otimes \mathbf{x} \cdot \mathbf{y}$$

Transposição:

$$(|\Psi\rangle \otimes |\Phi\rangle)^{\dagger} = \langle \Psi| \otimes \langle \Phi| \qquad (\mathbf{x} \otimes \mathbf{y})^{\dagger} = \mathbf{x}^{\dagger} \otimes \mathbf{y}^{\dagger}$$
$$|\Psi\Phi\rangle^{\dagger} = \langle \Phi\Psi|$$

Existem outras, mas essas duas são as mais interessantes para nós hoje.

Definição. (Base Computacional)

A Base Computacional é determinada pelos estados ortogonais $|0\rangle$ e $|1\rangle,$ definidos por

$$|0\rangle = \begin{bmatrix} 1\\0 \end{bmatrix}$$
$$|1\rangle = \begin{bmatrix} 0\\1 \end{bmatrix}$$

Chamaremos estes estados de qubits!

Definição. (Base Computacional)

Construimos vetores de qubits (registradores) através da composição:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Postulado. (Evolução)

A evolução de um sistema é descrita por um $Hamiltoniano\ H$, representado por uma matriz Hermitiana, isto é, $H=H^{\dagger}$. Assim temos, pela equação de Schrödinger:

$$H|\Psi\rangle = i\hbar \frac{d|\Psi\rangle}{dt} \implies \frac{d|\Psi\rangle}{dt} = \frac{-i}{\hbar}H|\Psi\rangle$$

Sejam $|\Psi(t_k)\rangle$, $|\Psi(t_{k+1})\rangle$ os estados do sistema no tempo t_k e t_{k+1} , respectivamente. Segue que:

$$|\Psi(t_{k+1})\rangle = e^{\frac{-iH}{\hbar}(t_{k+1}-t_k)} |\Psi(t_k)\rangle$$

Postulado. (Evolução)

1. Seja $U = e^{\frac{-iH}{\hbar}(t_{k+1} - t_k)}$ o operador de evolução.

Postulado. (Evolução)

- 1. Seja $U = e^{\frac{-iH}{\hbar}(t_{k+1} t_k)}$ o operador de evolução.
- 2. Sabemos também que $U^{\dagger}=e^{\frac{iH^{\dagger}}{\hbar}(t_{k+1}-t_k)}$.

Postulado. (Evolução)

- 1. Seja $U = e^{\frac{-iH}{\hbar}(t_{k+1} t_k)}$ o operador de evolução.
- 2. Sabemos também que $U^{\dagger}=e^{\frac{iH^{\dagger}}{\hbar}(t_{k+1}-t_k)}$.
- 3. Como a matriz H é Hermitiana, temos que $U^{\dagger}U=I$.

Postulado. (Evolução)

- 1. Seja $U = e^{\frac{-iH}{\hbar}(t_{k+1} t_k)}$ o operador de evolução.
- 2. Sabemos também que $U^{\dagger} = e^{\frac{iH^{\dagger}}{\hbar}(t_{k+1}-t_k)}$.
- 3. Como a matriz H é Hermitiana, temos que $U^{\dagger}U=I$.

Podemos então dizer que a evolução dos sistemas se dá por operadores unitários!

Postulado. (Evolução)

- 1. Seja $U = e^{\frac{-iH}{\hbar}(t_{k+1} t_k)}$ o operador de evolução.
- 2. Sabemos também que $U^{\dagger} = e^{\frac{iH^{\dagger}}{\hbar}(t_{k+1}-t_k)}$.
- 3. Como a matriz H é Hermitiana, temos que $U^{\dagger}U = I$.

Podemos então dizer que a evolução dos sistemas se dá por operadores unitários!

Hora de conhecer alguns deles!

Matriz de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1\\ 1 & -1 \end{bmatrix}$$

$$H |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \qquad = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$$

$$H |1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$$

Porta de Hadamard

$$\begin{array}{c|c} |0\rangle - H - \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle - H - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}$$

Matrizes de Pauli Também conhecidas como σ_1 , σ_2 e σ_3 , respectivamente.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Uma nota sobre reversibilidade

Uma nota sobre reversibilidade

Para toda matriz unitária, como $U^{\dagger}U=UU^{\dagger}=I,$ temos também que $U^{\dagger}=U^{-1}.$

Isso significa que todos os processos quânticos de computação serão **reversíveis!**

Uma nota sobre reversibilidade

O Princípio de Landauer.

O princípio de Landauer estabelece que toda vez que um bit de informação é apagado, o sistema perde energia, que é liberada na forma de calor, com limite inferior

$$E > KT \log 2$$

Onde:

E: Energia dissipada

K: Constante de Boltzmann, $1.380^{-23}J/K$

T: Temperatura ambiente, em Kelvin

Postulado. (Medida)

Trapped-ion

Oi íon aprisionado

Algoritmo de Grover

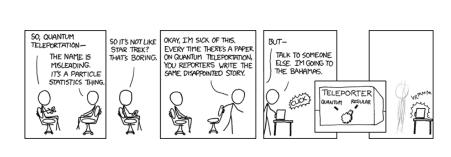


Lov Grover Bell Labs

Algoritmo de Shor



Peter Shor MIT



Teletransporte Quântico

Imagine o teletransporte como um operador

$$\mathcal{T}: |\Psi\rangle \otimes |\xi\rangle \rightarrow |\xi\rangle \otimes |\Psi\rangle$$

Teorema da não-clonagem

Teorema. $(N\tilde{a}o\text{-}Clonagem)$

Não é possível fazer uma cópia de um estado quântico qualquer.

Prova.

Vamos supor que existe um operador unitário U capaz de clonar um estado $|\Psi\rangle$ qualquer, isto é:

$$U(|\Psi\rangle\otimes|\xi\rangle) = |\Psi\rangle\otimes|\Psi\rangle = |\Psi\Psi\rangle$$

Como isso vale para qualquer estado, também é preciso que

$$U(|\Phi\rangle \otimes |\xi\rangle) = |\Phi\rangle \otimes |\Phi\rangle = |\Phi\Phi\rangle$$

Teorema da não-clonagem

Tomando o produto interno entre $|\Psi\Psi\rangle$ e $|\Phi\Phi\rangle$:

$$\langle \Psi \Psi | \Phi \Phi \rangle = \langle \xi \Psi | U^{\dagger} U | \Phi \xi \rangle$$

$$= \langle \xi \Psi | \Phi \xi \rangle$$

$$(\langle \Psi | \otimes \langle \Psi |) \cdot (|\Phi \rangle \otimes |\Phi \rangle) = (\langle \Psi | \otimes \langle \xi |) \cdot (|\Phi \rangle \otimes |\xi \rangle)$$

$$\langle \Psi | \Phi \rangle \otimes \langle \Psi | \Phi \rangle = \langle \Psi | \Phi \rangle \otimes \langle \xi | \xi \rangle$$

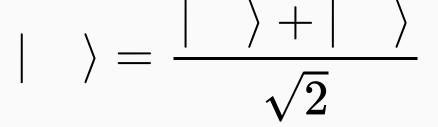
$$\langle \Psi | \Phi \rangle^2 = \langle \Psi | \Phi \rangle$$

Portanto:

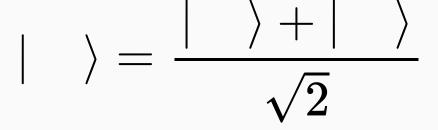
$$\langle \Psi | \Phi \rangle = \begin{cases} 1 \text{ se } |\Psi \rangle = |\Phi \rangle \\ 0 \text{ se } |\Psi \rangle \perp |\Phi \rangle \end{cases}$$

46

Fótons



Caminhadas Quânticas



Computação Topológica

Nós

Nós

$\hat{\mathbf{A}}$ nions

$\hat{\mathbf{A}}$ nions

Computação Adiabática

Computação Adiabática

Equação de Pauli

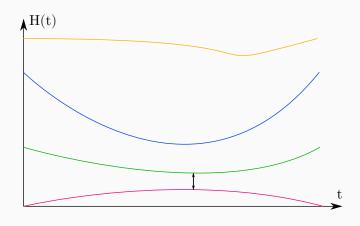
$$\left[\frac{1}{2m}(\vec{\sigma}\cdot(\vec{p}-q\vec{A}))^2+q\phi\right]|\psi\rangle=\mathrm{i}\hbar\frac{\partial}{\partial\mathrm{t}}|\psi\rangle$$

Têmpera Quântica

$$H(t) = -\frac{A(t)}{2} \sum_{i} h_{i} \cdot X |s_{i}\rangle$$

$$+ \frac{B(t)}{2} \left(\sum_{i} h_{i} \cdot Z |s_{i}\rangle + \sum_{i < j} J_{i,j} \cdot Z |s_{i}\rangle \otimes Z |s_{j}\rangle \right)$$

Têmpera Quântica

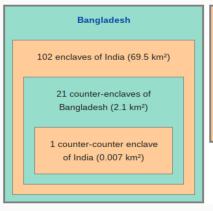


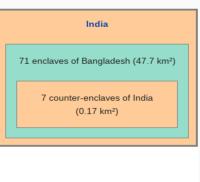
Fim?

Saltos Quânticos

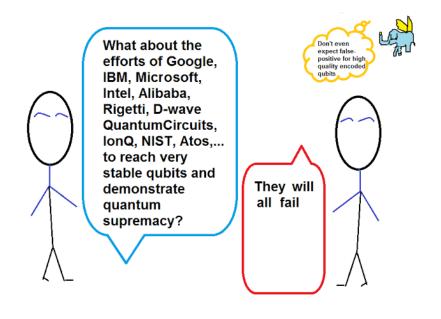


Saltos Quânticos









Supremacia Quântica



Gil Kalai Yale & Huji

Supremacia Quântica

Definição um tanto vaga. (Supremacia Quântica)

Atingir a supremacia quântica significa realizar uma tarefa em um computador quântico que não se possa concretizar no clássico.

Supremacia Quântica

Material

- The Quantum Algorithm Zoo
- Quanta Magazine

Obrigado

Bibliografia



Introduction to topological quantum computation with non-Abelian anyons, FIELD, B. & SIMULA, T., School of Physics and Astronomy, Monash University, Victoria 3800, Australia.



Reprograme o seu DNA na

frequência do Sucesso