

Encontros Matemáticos apresenta

Computação Quântica

Pedro Maciel Xavier

pedromxavier@poli.ufrj.br

19 de novembro de 2019

IM-UFRJ

Computação Digital

O Bit

Álgebra Booleana

Complexidade e Computabilidade

Transistor

Portas Lógicas

Arquitetura de Von Neuman

Lei de Moore

Parte II

Computação Quântica

Postulados

Trapped-ion

Algoritmos

Teletransporte Quântico

Teorema da não-clonagem

Fótons

Caminhadas Quânticas

Computação Topológica

Nós

Ânions

Computação Adiabática

Teorema Adiabático

Têmpera Quântica

Saltos Quânticos

Fim?

Supremacia Quântica

Material

Bibliografia

Computação Digital

010010110000101010101011010101111101010110011111001010101000010110000011100001010001011001001
10010001011100110100101000010101010101010101000101010100001001001010000000110111101010010
011100111001100000001100010111110010000101001010001011000100110000101000101000101101101001
00110001010100010001001010010111101011100001110000111000000011100010010101010000011001011
1011100000011100110001101100111010001010100100100001001111011011011110110011100110101000100011
1010000010110010000000101010011001111011111001010010100000010001001101101100101001010011101010
1011011010010101010111100000110111101001010100010101001010011010000111010110101010100001101
1000110000001011100000100110110101000101010101001011101000011111100001110110111001111110100
1001100000000000000011101101001010000010000011010100100101011110100101010101010010110010101
110001110000010101110001100100001011010110111110100101000011001000011011000110001000101011111
01010011000001000010100101000100010011001111011110111111000101000011010000100100000100011
000100000010100011110101111010101001000010001010001101110100100110010110000001010100101101001
01001000011111010101010010011110101110100111010001010001010101000011110100110011000100100
000101010101010111000011111100001110010100010101011000111100000100111000100100111001000000011
001011111001100101010101001010100001000101111010111000010100100110000001101011111000100110001
110100000000010101011110000110001011000001001100000111010101110011001100110000000111101111010
1010001100010000110010101110000110000101100001010111010001100111110000110111000000011000101
100111101010101001100101010100000101011000100011000000010001101010000010010101000100001000
0010111100110011000001010110000010101111001010100111001001100101100000111100100000001110101001
0111100100101000110000100110000101111101010101000001110010000000001000010011111100000100100
10111110011101110000000010100101100010101011000101000001000011101111100100111000011010000011
01111010000001010110101111101001010000010101010010101110010011001101011110100100010101010
0011010100000100110101010111001110011000100000101000011101000100001111010011000001010111
01001011010111110000010010000101001011101010100001010101010100010011110000010100101011101
01010010101111100100101100100101111011010100011001001010111001100000010001101001000111100100
1010100110000111000000010001110101010011001001001110000110000110101000111000110010010110011
0100001010100000000100110100011101101111010101011100111111010101010101001100001000010100
011000001100010001010101101010010010111001000101001110101100100001100010000110000001100010000100
010100001001111010100100100000011001010111010101010101000100001110001100101001101000010001
001100011101001001000100010001010000110100011110010101010111110011110001000010111001
001100001111100100010000010111010100100111011110001001100100100010101101000010010010111
0101011101010000010001100000000100001100010000000110000011001000101011101001001100010100
01010000110100101010010010100000101010001001110110010001010010101000000100100110011001100
10000101110111000001111010100111000010100100111101100000101000010010101101010010101010
001100010100001110000111001110011000110000010001011101010010011000101010001000100101010101
111000010101110000100100100000000011000101010010101110001011100000001111000100101001101
111011100111000111000010100001111010100100110010000010101000010101010000000001111010101000
00101011111001110001001110010010101110111010011000010010100110001100001000101010011
1010100101011000010101010100101111011110100010010100001101000100000010101000101010001
00010010001011100001000101000101001010101100011010000101010100011101010100010101000101011
1010101100000101010100111101010011100010010100110010010010100111101011110001111010000111
10100111001010010101100111011101010101001010101011100010011100001000101110101010
10100010100101010101010011111110100101011001001010101001100010001010111100001010111010111
010111010000001011101010100111001001100100011000010101100001010111000010101111110000000101
00011001101010101010010100101010100110101100101011100010101110001010111000101011010001001
11101010100001010101010100101011100110010110000100111111101010110000010111000000001110
1111000011001010010101000100111000011101010101010100111001101010101000010010010010101011101
000111101011110010010010100101000001110100101001000000010001010111010000000100001001001010
1011111101000011110100001100111110000010100001000000010101000100100111111010111001001100011

0101101

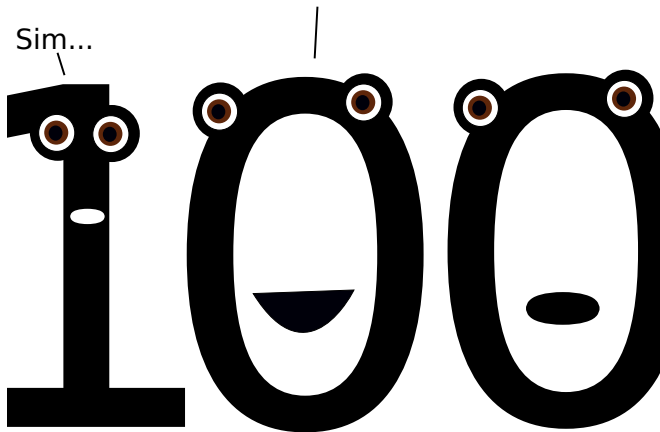
1101001

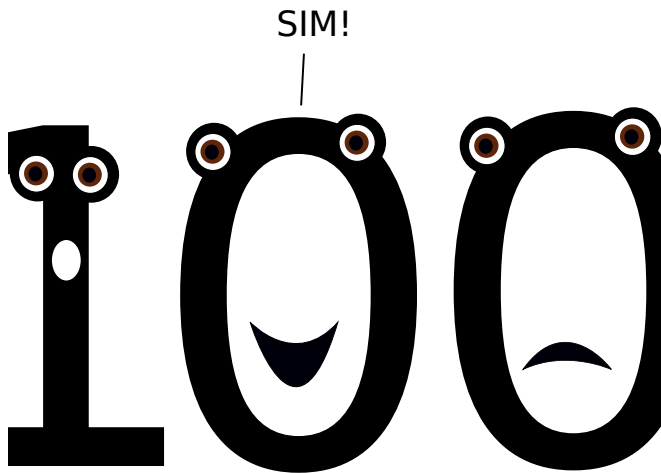
1110100



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

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow 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 for any windows updates you might need.

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

Sobre os *bits*:

- Eles moram em \mathbb{Z}_2
- Realizamos operações *Booleanas* com eles: $\neg, \wedge, \vee, \oplus$.
- Formam vetores em \mathbb{Z}_2^n , onde cada $\vec{a} = (a_1, a_2, \dots, a_n) \in \mathbb{Z}_2^n$ representa um valor entre $00\dots 0 = 0$ e $11\dots 1 = 2^n - 1$.

Álgebra Booleana

Definição. (*Álgebra Booleana*)

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

$$a \vee (b \vee c) = (a \vee b) \vee c \qquad a \wedge (b \wedge c) = (a \wedge b) \wedge c \qquad \text{associatividade}$$

$$a \vee b = a \vee a \qquad a \wedge b = b \wedge a \qquad \text{comutatividade}$$

$$a \vee 0 = a \qquad a \wedge 1 = a \qquad \text{identidade}$$

$$a \vee \neg a = 1 \qquad a \wedge \neg a = 0 \qquad \text{complemento}$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad \text{distributividade}$$

$$a \vee (a \wedge b) = a \qquad a \wedge (a \vee b) = a \qquad \text{absorção}$$

Álgebra Booleana



George Boole
1815 - 1864



Augustus De Morgan
1806 - 1871

A Tese de Church-Turing

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

Alan Turing

Definição. (*Máquina de Turing*)

É um computador abstrato definido por $(Q, q_0, \Gamma, \square, \Sigma, \Omega, \delta)$,
que possui uma fita

Q : Um conjunto não-vazio de estados.

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

Γ : Alfabeto da fita.

\square : Símbolo vazio.

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

Ω : Conjunto dos códigos de parada.

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

Complexidade e Computabilidade



Alonzo Church
1903 - 1955



Alan Turing
1912 - 1954

A Tese de Church-Turing

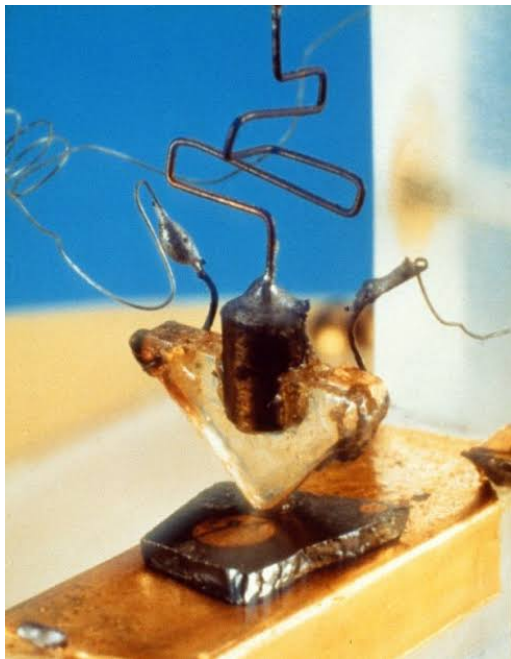
Toda função que seria naturalmente computável pode ser computada por uma Máquina de Turing

Alan Turing

Definição. (*Complexidade Assintótica*)

Seja $f : X \subseteq \mathbb{R}_+ \rightarrow \mathbb{C}$ e $g(x) : X \subseteq \mathbb{R}_+ \rightarrow \mathbb{R}_+$ dizemos que

$$f(x) = O(g(x)) \iff \exists M, x_0$$





Arquitetura de Von Neuman



John Von

Neuman

1903 - 1957

Our World
in Data

Licensed under [CC-BY-SA](#) by the author Max Roser.



Gordon Moore
Intel, 1965



Richard Feynman

1918 - 1988

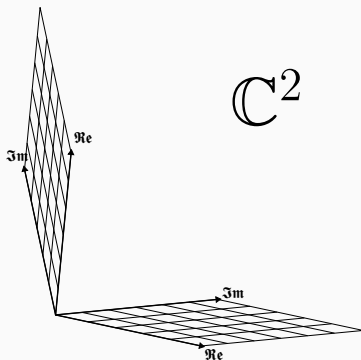
Computação Quântica

Postulados

Postulado. (*Representação*)

$$|\Psi\rangle \in \mathbb{C}^2$$

$$(\mathbf{x} \in \mathbb{C}^2)$$

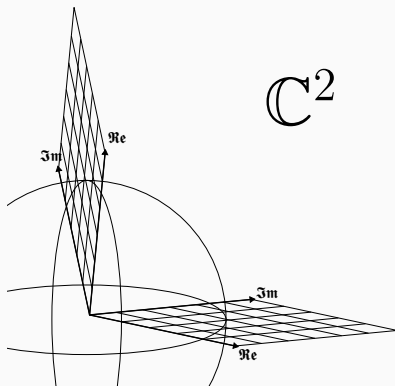


Postulados

Postulado. (*Representação*)

$$|\Psi\rangle \in \mathbb{C}^2 \quad (\mathbf{x} \in \mathbb{C}^2)$$

$$\langle\Psi|\Psi\rangle = 1 \quad (\mathbf{x}^\dagger \mathbf{x} = 1)$$



Postulados

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*)

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax \\ ay \\ bx \\ by \end{bmatrix}$$

Definição. (*Base Computacional*)

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

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

Chamaremos estes estados de *qubits*!

Definição. (*Base Computacional*)

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

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

Postulado. (*Evolução*)

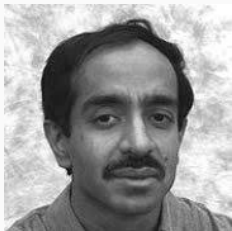
A evolução de um sistema se dá por meio de operadores unitários U

Uma nota sobre reversibilidade

$$\Delta S > KT \log 2$$

Oi íon aprisionado

Algoritmo de Grover



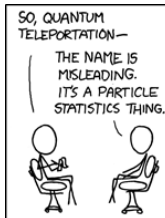
Lov Grover

Bell Labs

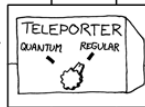
Algoritmo de Shor



Peter Shor
MIT



SO IT'S NOT LIKE STAR TREK? THAT'S BORING.



Teorema da não-clonagem

Teorema. (*Não-Clonagem*)

Não é possível fazer uma cópia de um estado quântico.

Teorema da não-clonagem

Prova.

Vamos supor que existe um operador unitário U capaz de clonar um estado $|\Psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$ qualquer, isto é:

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

Assim:

$$\begin{aligned} |\Psi\rangle \otimes |\xi\rangle &= (\alpha |\uparrow\rangle + \beta |\downarrow\rangle) \otimes |\xi\rangle \\ &= \alpha |\uparrow\rangle \otimes |\xi\rangle + \beta |\downarrow\rangle \otimes |\xi\rangle \end{aligned}$$

$$\begin{aligned} \therefore U(|\Psi\rangle \otimes |\xi\rangle) &= U(\alpha |\uparrow\rangle \otimes |\xi\rangle) + U(\beta |\downarrow\rangle \otimes |\xi\rangle) \\ &= \alpha U(|\uparrow\rangle \otimes |\xi\rangle) + \beta U(|\downarrow\rangle \otimes |\xi\rangle) \\ &= \alpha |\uparrow\uparrow\rangle + \beta |\downarrow\downarrow\rangle \end{aligned}$$

Teorema da não-clonagem

Por outro lado:

$$\begin{aligned} |\Psi\rangle \otimes |\Psi\rangle &= (\alpha |\uparrow\rangle + \beta |\downarrow\rangle) \otimes (\alpha |\uparrow\rangle + \beta |\downarrow\rangle) \\ &= \alpha^2 |\uparrow\uparrow\rangle + \alpha\beta(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) + \beta^2 |\downarrow\downarrow\rangle \\ &\neq \alpha |\uparrow\uparrow\rangle + \beta |\downarrow\downarrow\rangle \end{aligned}$$



$$| \rangle = \frac{| \rangle + | \rangle}{\sqrt{2}}$$

$$| \rangle = \frac{| \rangle + | \rangle}{\sqrt{2}}$$

Computação Topológica

Computação Adiabática

$$H |\Psi(t)\rangle = i\hbar \frac{\partial |\Psi(t)\rangle}{\partial t}$$

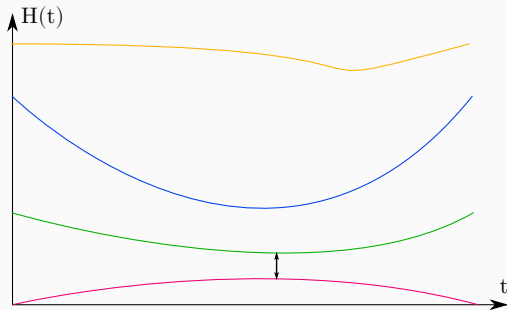
Teorema Adiabático

Teorema Adiabático

Teorema Adiabático

$$H(t) = -\frac{A(t)}{2} \sum_i h_i \cdot X |s_i\rangle \\ + \frac{B(t)}{2} \left(\sum_i h_i \cdot Z |s_i\rangle + \sum_{i < j} J_{i,j} \cdot Z |s_i\rangle \otimes Z |s_j\rangle \right)$$

Têmpera Quântica



Fim?



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

