

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

Temperatura Adiabática

Fim?

Material

Bibliografia

Computação Digital

010010110000101010101010101011110101011001111100101010000101100000111000001010001011001001
100100001011100110100101000010101010101010101000101010101000100101010000000110111101010010
01110011100111000000110001011111001000010100101000101100010011000010100101000111011011001
0011000101010001000100110010111110101110100011101000111000000001110001001101010100110000011001011
10111000000011100110001110100110100010101001001000010011110110101011101100111100111001101000100011
1010000010110010000000101010011001110111110010110010100000010001001010101100101001010011101010
101010101001010101011110000011011110100111101000101010010100110100001110101010101010100001101
100010000000101100000100110101000010101010100010110101000111110000111011011001111010011110100
1001100000000000000110101010010100000100000111010100100101101111010011010101100101110010101
1100011100000101011000111001000101101011101111010010100001100100001110100011000100010101111
0110100110000011000101001011000100110011101111011110111111000110100011010000100100001010011
0001100000101000111101011110101001000010001010001101110100100110010110000001010100101101001
0100100001111101010101001011101011101001011000010100010100010101010001111010001110011000100
000101010101011100001111110000111001100001010111000111100000110011000100100111001000000011
00101111100100101010010101000011000101110101110000101001001100000001010111100010011100001
1101000000010101011110000110001011100001001100000100000011101010111001100000001110111110110
10100011000100001110010101100001100010100101011101000101111110101100101101000000011000101
10011110101010100101010101000001010111000110001110000000110001101100100010010101000100001000
0010111100110011000001011101000010101111001010011100100110010110000111100100000011110100101
0111100100110001100001010000101111101010100000111001000000010000100111111000001010010
1011111000111011100000000101001010001010101100010100000100001111011110010011100000111010000011
0111101000000101010111110100101000010101001001011100110011001010101110100100010101010
001101010000010011010101011100110001001000010100000111010001100011111010011000001010111
010010110101111000000100010100101110101000010101010101001100111110000010100101011101
01010010101111100100101001001011101010100010010010101110011000001000101001000111100110100
101010100001100000010001110101010011001001001110000110000111010100011100011100100101110011
01000010010100000000100101000111011011101010101010111011010101010011000100000100010100
01000001100010001010101010100100101110010001010011010110010000110001000011000100001000
0101000010011010101001001000000100101111010101010100010000111000100100101010101000100101001
001100110100100100010001000100110000101010111000111100101010101011101011110001000010111001
00110000111110010001000010111010100010011101111000100100100010101010000010010010010111
01010111010100000101001100000001000010100100010000001100000110010001010101100100100010100
010100001101001010100100101000001010000100111010010001010010111010010000010010010011001100
1000011011101100000111110101001110000101001001110111000001010000100101010110111010010101010
00110001010000111000011100110011000110000100010101010100100110010010001000110001000101010101
11000001010110000010010010000000001100010101001011100010111000000011110100110010100110101
11011010010100011000010100000111101010010010010010000010101010001000010001101010100000010001
001010111110011110001010010011100010100001001011101001010100111001001010101000010101000
1111001000010010010010100000011111100110000000101010000101010100001000010001101010100000010001
10010010010111100010011100100101010101010001001010011000100001000100100100101010011
110101001010100000101010101001011110111010001001010100001110100100010010101000101010001
00011001000101110000100010100010100101011100010100001010101001110101010001011001010111
1010111000001101010010111101010011100101001110010100111001001010111100011110101000011101000011
101000101001010101010100111111010010101110010101010100110001001010111000001010111010101
010110100000010101010100111001001001000011000010101001010101100001010111110000010010101
000110011010101001010010100101010101010101000010101010111001010101110010101011100000101010001001
1101010101000010101010101001011101100110100011001010100001110100100010010101000101010001
1111100011100100100101000100111000111010101010101001110011010101010000100001001100110101
0001111010111001001001010010100001110101010010000000100010101110100000100001001001001010
1011111101000011101100001110011110000010100001000000001010100010010011111010111001001100011

0101101

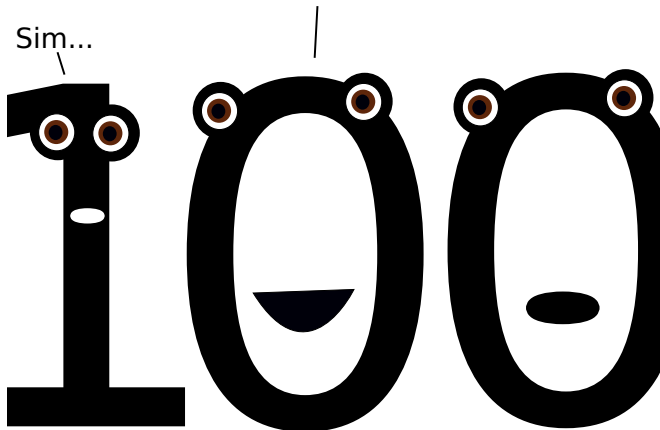
1101001

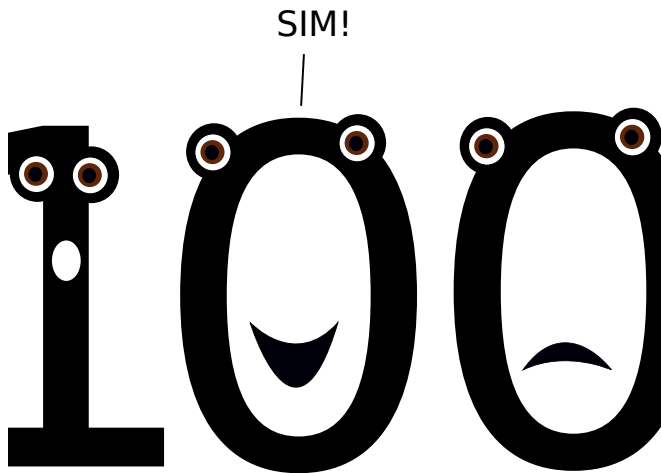
1110100



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



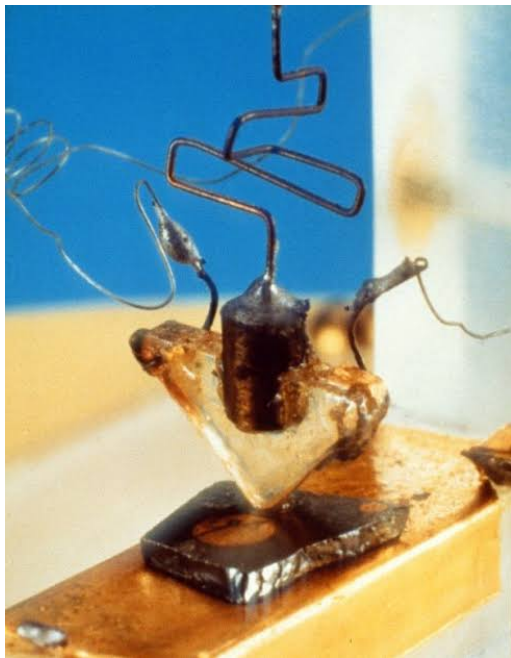
Alonzo Church



Alan Turing

Definição. (*Complexidade Assintótica*)

Seja um problema com entrada de tamanho n , ...





Arquitetura de Von Neuman



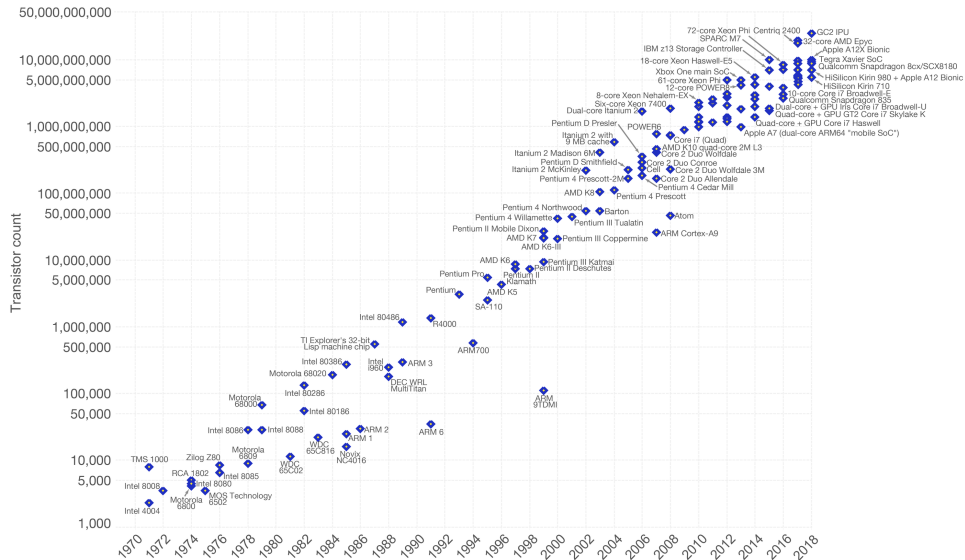
John Von

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.



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at [OurWorldInData.org](https://www.ourworldindata.org). There you find more visualizations and research on this topic.

Licensed under [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) by the author Max Roser.



Gordon Moore
Intel, 1965



Richard Feynman

1918 - 1988

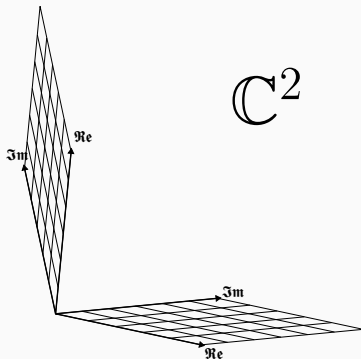
Computação Quântica

Postulados

Postulado. (*Representação*)

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

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

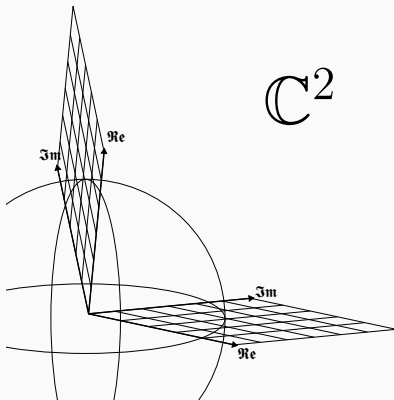


Postulados

Postulado. (*Representação*)

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

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



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*)

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

Definição. (*Base Computacional*)

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

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

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*)

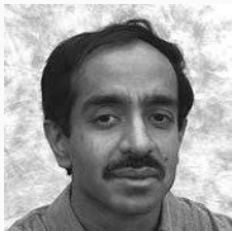
A evolução de um sistema se dá por meio de operadores unitários U

Uma nota sobre reversibilidade

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

Oi íon aprisionado

Algoritmo de Grover



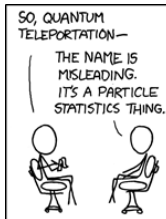
Lov Grover

Bell Labs

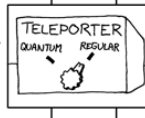
Algoritmo de Shor



Peter Shor
MIT



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



Teorema. (*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 $|\Psi(t)\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$ qualquer, isto é:

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

Assim:

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

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

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

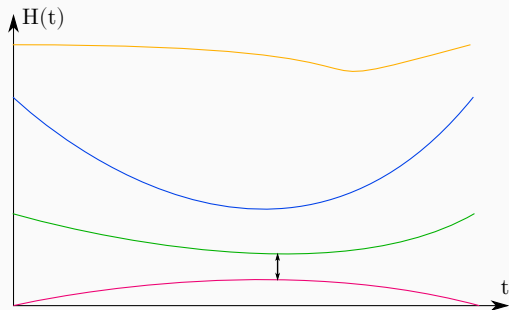
$$H |\Psi(t)\rangle = i\hbar \frac{\partial |\Psi(t)\rangle}{\partial t}$$

Teorema Adiabático

Teorema Adiabático

Teorema Adiabático

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



Fim?



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

