

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

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

Fim?

Salto Quântico

Supremacia Quântica

Material

Bibliografia

Computação Digital

010010110000101010101011010101111101010110011111001010101000010110000011100001010001011001001
10010001011100110100101000010101010101010101000101010100001001001010000000110111101010010
011100111001100000001100010111110010000101001010001011000100110000101000101000101101101001
00110001010100010001001010010111101011100001110000111000000011100010010101010000011001011
1011100000011100110001101100111010001010100100100001001111011011011110110011100110101000100011
10100000101100100000001010100110011110111110010100101000000100010011011011001010010100111010
1011011010010101010111100000110111101001010100010100101001101000011101011010101010100001101
1000110000001011100000100110110101000101010101001011101000011111100001110110111001111110100
10011000000000000000111011101001010000010000011010100100101011110100101010101010010110010101
1100011100000101011100011001000010110101101111101100101000011001000011011000110001000101011111
0101001100000100001010010100010001001100111101111011111100010100001010000100100000100001010011
000100000010100011110101111010101001000010001010001101110110010011001011000000101101001010101001
01001000011111010101010010011110101110100111010001010001010101000011110100110011000100100100
0001010101010111000011111100001110011010001010111000111100000100111000100100111001000000011
00101111100110010101010100101010000110001011110101110000101001001100000001010111110001100110001
110100000000010101011110000110001011000001001100000111010101110011001100110000000111101111010
101000110001000011001010111000011100001011010001101011010001100111110011001101000000110001101
1001111010101010011001010101000001010110001100011000000010001101000000100101010001000010000
00101111001100110000010101100000101011110010101001110010011001011000000111100100000011101101001
01111001001010001100001001100001011111010101010000011100100000000010000100111111000001100100
10111110011101110000000010100101100010101011000101000001000011101111100100111000011010000011
01111010000001010110101111010010100000101010100101011100100110011010111101100100010101010
0011010100000100110101010111001110011000100000100000111010001100001111010011000001101111
01001011010111110000010010001010010111010101000010101101010100010011110000010100101011101
010100101011111001001010010010111101101010001100100101011100110000001000110100100011110010010
1010110011000011100000001000111010110100110010010011100001100001110101000111000110010010110011
010000101010000000010011010001110110111101101010101100111111011010101010001100001000010100
0110000011100010001101011101010010010111001000101001110101100100001100010000110000001100010000100
01011000011001111010100100100000011001011110101010110101000100001110001100101001110100010001
00110001110100100100010001000100110000111010110001010101111100111110011110001000010111001
001100001111100100010000010111010100100111011110001001100101000101011010000100100101111
0101011101010000010001110000000100001100110001000001100000110010001010111001001100010100
0101000001101001010100100101000001010100010011101100100010100101011000100000100100110011001
100001011101110000011110101001110000101001001111011000001010000100101011101010010101010
00110001010000111000011100111001100011000001000101110101100100110001101100010001100010101010101
1110000101011100001001001000000000110001010101001011100010111000010011100001001011001101
11101110011100011100001011000011110101001001100100000101010000101010100001000100111010100010001
00101001010011110001001110010010101110111010011000011001010011000110001000101001010011
1010100101011000010101010100101111011110100011001010000111010010000010010101000101010001
00010010001011100001000101000101001010101100011011000010101010001110101010001010100101011
101010110000010101010011110101001110001001100110010010011101011110001111010000111
101001110011001010110011101110101111101010101001101101111000100111000010001011101010
1010001010010101010101001111110100101011001001010110011000101011110000101011110110111
01011101000000101110101010011100100110010001100001101010010101110000101011111100000001001
00011100110101010100101010010101010011010110001010111000101011100010101110001010110001001
1110101010000101010101010010101110011001001110000110011111101010110000010111000000001110
111100001100101001010100010011100001110101010101010011100110101010100001001001001101011101
000111101011110010010010100101000001110100101001000000010001010111010000000100001001001010
101111110100001111011000011001111100000101000010000000010101000100100111111010111001001100011

0101101

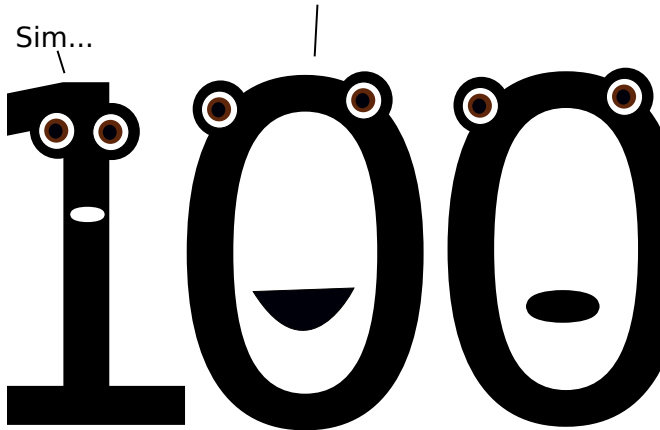
1101001

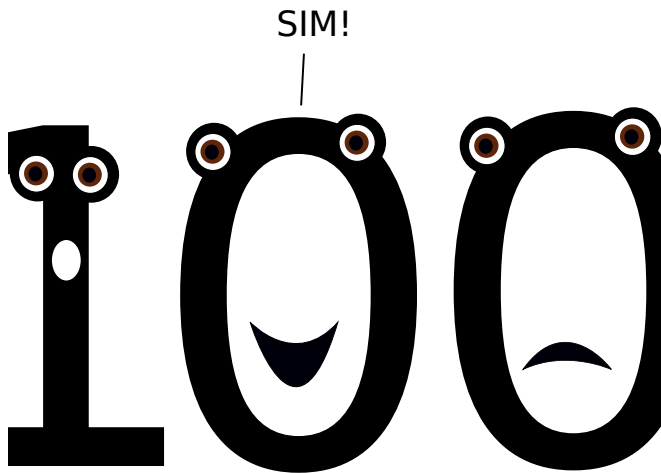
1110100



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 $00\dots0 = 0$ e $11\dots1 = 2^n - 1$.

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 e um cabeçote de leitura

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

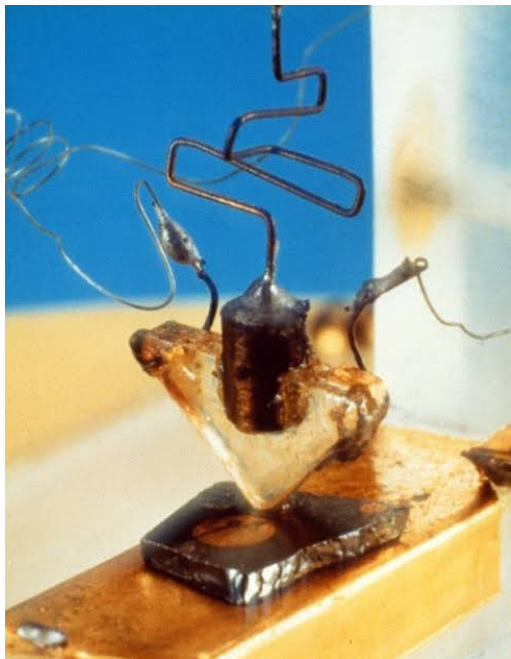
Toda função que seria naturalmente computável pode ser computada por uma Máquina de Turing

Alan Turing

Definição. (*Complexidade Assintótica*)

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

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





Arquitetura de Von Neuman



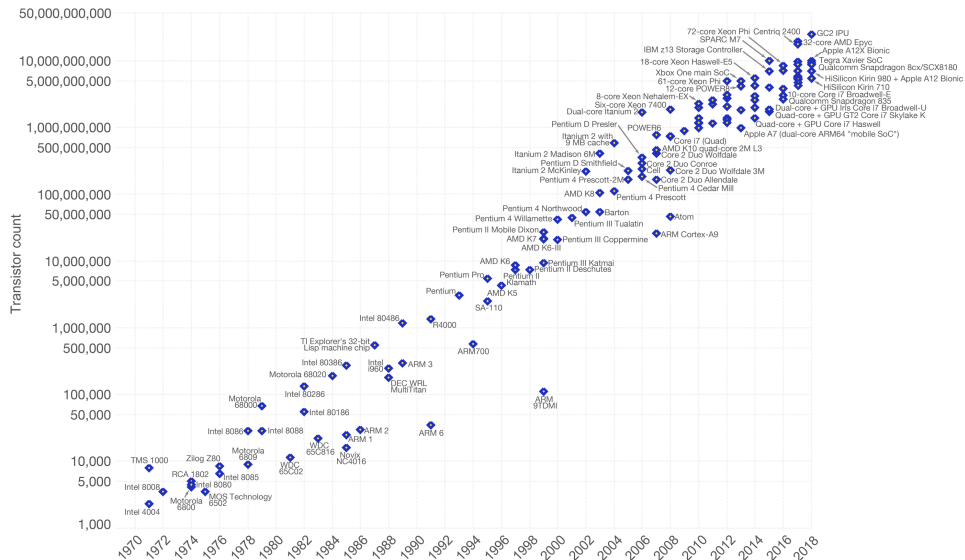
John Von

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 by the author Max Roser.



Gordon Moore

Intel, 1965

Computação Quântica



Richard Feynman

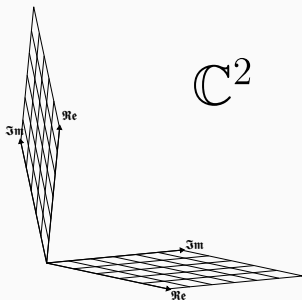
1918 - 1988

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.

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



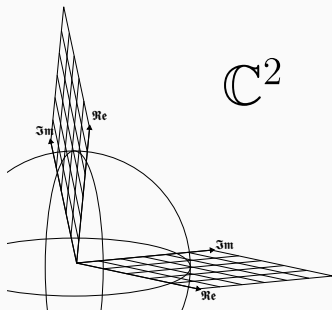
Postulados

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.

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

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



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*)

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

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

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:

$$\begin{aligned} (|\Psi\rangle \otimes |\Phi\rangle)^\dagger &= \langle\Psi| \otimes \langle\Phi| & (\mathbf{x} \otimes \mathbf{y})^\dagger &= \mathbf{x}^\dagger \otimes \mathbf{y}^\dagger \\ |\Psi\Phi\rangle^\dagger &= \langle\Phi\Psi| \end{aligned}$$

Existem outras, mas essas duas são as mais interessantes pra 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*)

Construímos vetores de *qubits* (registradores) através da composição:

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

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

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

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

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

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Uma nota sobre reversibilidade

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

O Princípio de Landau.

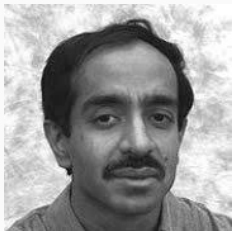
$$\Delta S > KT \log 2$$

Postulado. (*Medida*)

Trapped-ion

Oi íon aprisionado

Algoritmo de Grover



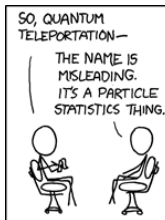
Lov Grover

Bell Labs

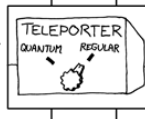
Algoritmo de Shor



Peter Shor
MIT



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



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. (*Não-Clonagem*)

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

Teorema da não-clonagem

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 $|\Phi\Phi\rangle$:

$$\begin{aligned}\langle\Psi\Psi|\Phi\Phi\rangle &= \langle\xi\Psi|U^\dagger U|\Phi\xi\rangle \\ &= \langle\xi\Psi|\Phi\xi\rangle\end{aligned}$$

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

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

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

Portanto:

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



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

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

Computação Topológica

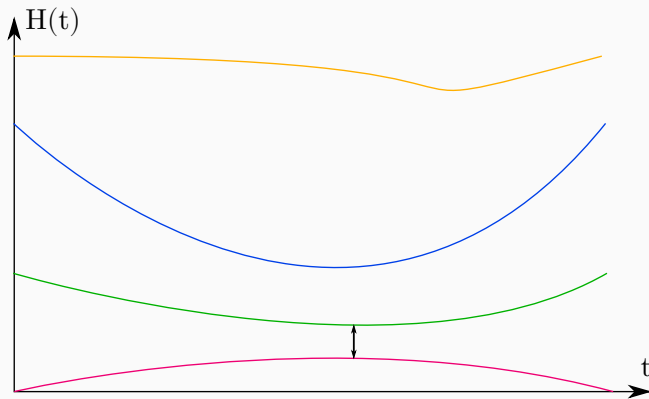
Computação Adiabática

Equação de Pauli

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

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

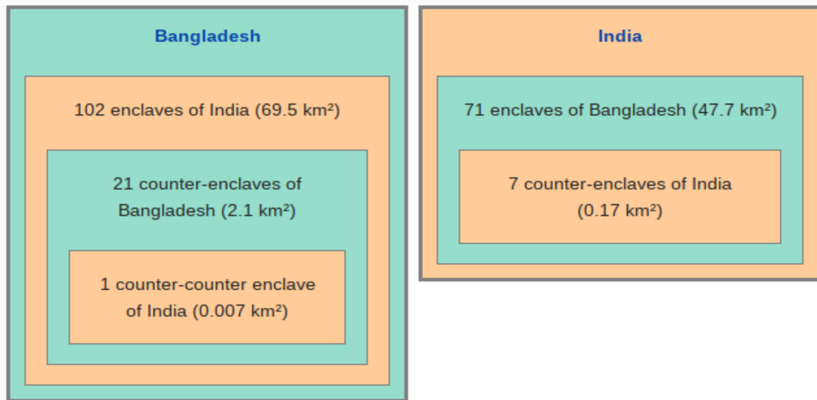
Têmpera Quântica

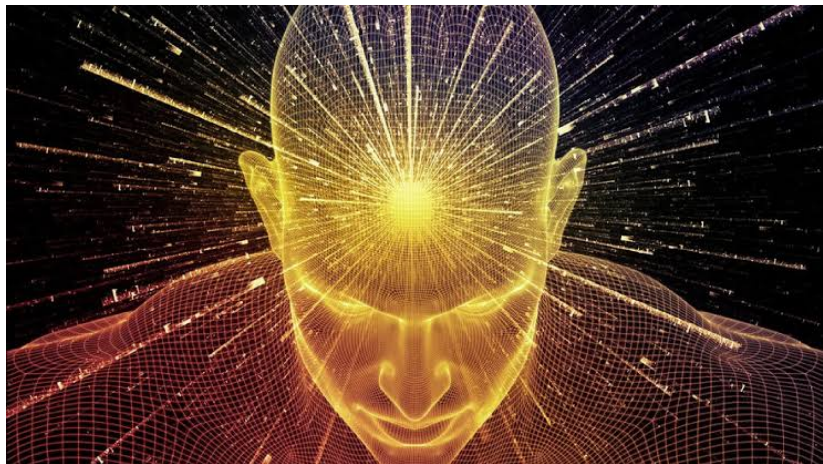


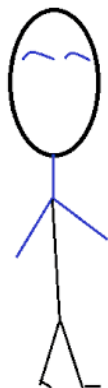
Fim?

Saltos Quânticos



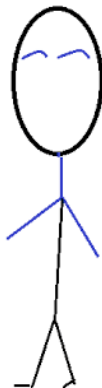






What about the efforts of Google, IBM, Microsoft, Intel, Alibaba, Rigetti, D-wave QuantumCircuits, IonQ, NIST, Atos,... to reach very stable qubits and demonstrate quantum supremacy?

They will all fail



Don't even expect false-positivity for high quality encoded qubits



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.

- The Quantum Algorithm Zoo
- Quanta Magazine

Obrigado



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
