Encontros Matemáticos apresenta

Computação Quântica

Pedro Maciel Xavier
pedromxavier@poli.ufrj.br

19 de novembro de 2019

IM-UFRJ

Parte I

Parte II

Parte III

Fim?

- Saltos Quânticos
- Supremacia Quântica

Computação

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. (*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.
- $\Box$: Símbolo vazio.
- Σ: Alfabeto de entrada da máquina. ($\Sigma \subseteq \Gamma/\{\Box\}$)
- Ω: Conjunto dos códigos de parada.
- δ: Função de Transição, $\delta : Q/\Omega \times \Gamma \rightarrow Q \times \Gamma \times \{\uparrow, \downarrow\}$

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

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

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

Complexidade

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.

$5 + 4$

5	2	3	4

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

1	2	3	4	5

Complexidade

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.

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

$\boxed{5}$

$\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}$

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.

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

$\boxed{5}$

$\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}$

Mas e se a lista tivesse n elementos?

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

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:

$$
\begin{array}{rrr}
a \vee (b \vee c) = (a \vee b) \vee c & a \wedge (b \wedge c) = (a \wedge b) \wedge c & \text{associatividade} \\
a \vee b = a \vee a & a \wedge b = b \wedge a & \text{comutatividade} \\
a \vee 0 = a & a \wedge 1 = a & \text{identidade} \\
a \vee \neg a = 1 & a \wedge \neg a = 0 & \text{complemento} \\
a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) & a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) & \text{distributividade} \\
a \vee (a \wedge b) = a & a \wedge (a \vee b) = a & \text{absorção}
\end{array}
$$

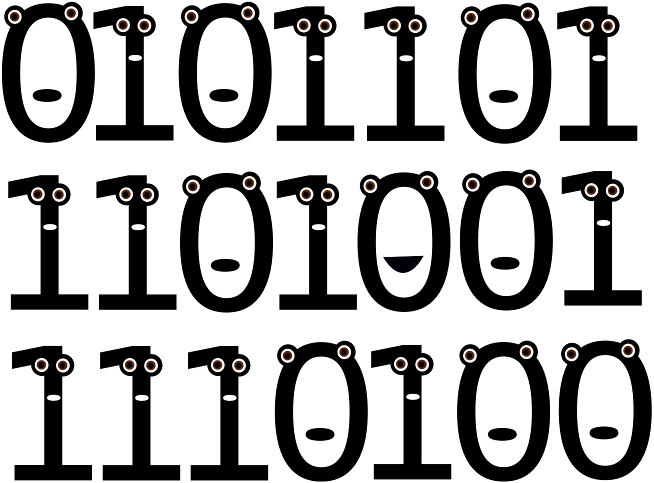
George Boole

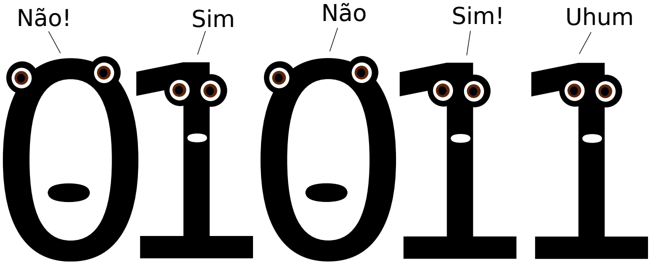
1815 - 1864

Augustus De Morgan

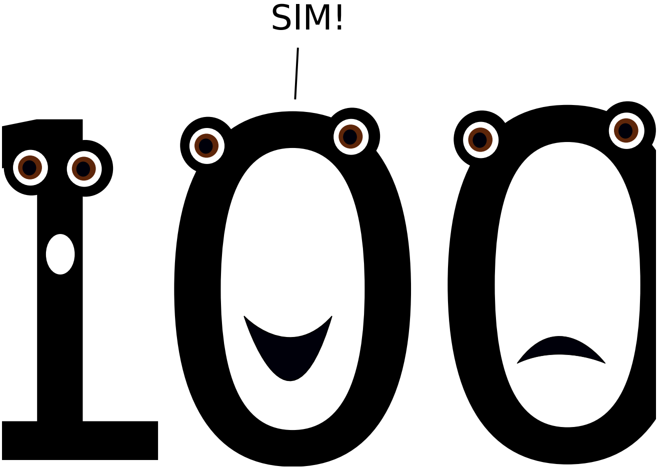
1806 - 1871

0100101100001010101010110101010111111011010111001111110010101010000101100000111000001010001011001001
1001000110111001101001010000101011011011101011011000110110101100010010011011000000011101111101010010
0111001110011100000001100010111111001000010100110100101110001001100010100001101001010001111011101101 001
0011000101010001000100110010111111010111010001110100011110000000111100010011010101100110000011001011
1011100000001110011000111011001110100010101001001000010011110110110101111011100111100111010100010001 1
1010000010110010000000101101001100111101111111001011001010100000001000100110110111001010010100111010 10
1011011010010101010111110000011011111011001111101000101101001010011010000111010110101010110100001101
1000110000000101110000001001101110101000101011011010100101110110100011111110001111011101110011111010 0
1001100000000000000001110111010010110000010000011101011001001011011111010011011010110110010111001010 1
1100011100000010101110001110010001011101011101111111011001010000110010000111011000110001000101101111 1
0110100110000011000110100101100010011001110111111101111101111111111000110100011010000100100001010011
0001100000101000111110101111101011010010000100010100011011101100100110010110000001101101001101101001
0100100001111110101101101001011111010111011010100111010001011000110110101000111111010011100111000100
0001101101010110111000011111110000111100110100011011011100011111000001100111000100100111001000000011
0010111111001100110101001011010000110001011110110111000011010010011000000110101111111000110011100001
1101000000000101101101111000011000101110000110011000001000000111101011011100111000001111111011111110110
1010001100010000111001101101100001110001011010010101110100011011111111100111001011101000000110001101
1001111101101010110010110101010000010101111000110001110000000110001110110010001001101101000100001000
0010111110011001100000110111010000101101111100101010011100100110010110000111110010000001111111011001 01
0111100100101100011000010011000010111111101101010100000111100100000000001000010011111111000001100100
1011111100111101110000000010110010110001010110111000101000001000011110111111001001110000111010000011
0111101000000110111010111111010010110000101101101001010111100110011001110101110111101100100011011010
0011101010000010011101101011100111110011000010010000101100000111101000110001111111010011000001101111
0100101110101111110000001001100010110010111101010100001101101101101100110011111000000110100101101111 01
0101001010111111001001011001001011111011101010001100100110110111001100000010001101001000111110011010 0
1010110011000011100000001000111101101101001100100100111100001100001110110100011110001110010010111001 1
0100001001101000000000100110100011110111011111101110101010111001111111101101011101100110000100001011 00
0110000011100010001101101110101001001011110010001011001110101100100001100010000110000000110001000010 0
0101100001100111101101100100100000000110011011111010101011101010001000011110001100101001110100010100 1
0011100111010010010001001000100110000101101011100011111001011011011011111111001111100010000101111001
0011100011111100100010000101111011010010011111011111100010100110010100010101110101000010010010010111 1
0101011110101100000010100111000000010000101100110001000000111000001100100011011011100101001100010110 0
0101100001110100110110100100110100000101010001001111011001000101100110111010010000011001001100111100
1000011011110111000001111110101001110000101001001111101110000011010000100101010111011110100101010110
0011000101000011100001110011100110001100000100011011101011001001100011011000100011000110101011101101
1110000010110111000010010010000000000111000110110110011011110001101110000000111110100110011011001110 1
1110111101001110001101000010111000011111010110010011001010000011011111111010010001011111111011011110 00
0010110111111100111100010110010011110001010100010010111101100101010100111100010011101101000101101000
1111100100001100110010011000000111111110011000000001010101000101101010100001000100111010110000001000 1
1001100101001111100010011100110010101010111101111010011000011001011001110001100010110001100100101100 11
1101101001101110000101010110110011011111011111011000110011011000011110100100010010101011000101101000 1
0001100100010111100001000101000101100101010111100011011000011011010100111101101011000101110010101011 1
1011011011000000110110101001111101010100111100010011011001100101011001111011011111100011111011000011 1
1011001111001101001101110011110111101011111110110101011001101101110111110001001110000100010111101010
1010001101001101010101011001111111110100101011110010101010110011000101011101111100001111011110110111
0101110110000001011101101101001110010011001000111000011010110010101011110000111011111111100000100110 1
0001110011101011011001010100101101101001101000011010101100111011111001010111010100000101111010001001
1110101010100010101010110101001011101110011010011110000110011111111010110111000010011110000000011110
1111100011100101001001101000100111100011110101010101101010011110011010101110100010100110011010111101
0001111101011110010010011010010100000111010011010010000000001000101101111010000010100001100100100101 0
1011111110100001111011000011100111111000001010000100000000110110100010010011111111010111001001100011


0101101
1101001
1110100


Não!
Sim
Não
Sim!
Uhum

Finalmente! É o meu grande dia!
Sim...


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

O Bit

Definição. (***Anel Booleano***)
Um Anel booleano é um Anel $(\Omega, +, \cdot)$ com as operações $+$ e $\cdot$ definidas por:

$$\begin{aligned} a + b &:= a \oplus b = (\neg a \wedge b) \vee (a \wedge \neg b) \\ a \cdot b &:= a \wedge b \end{aligned}$$

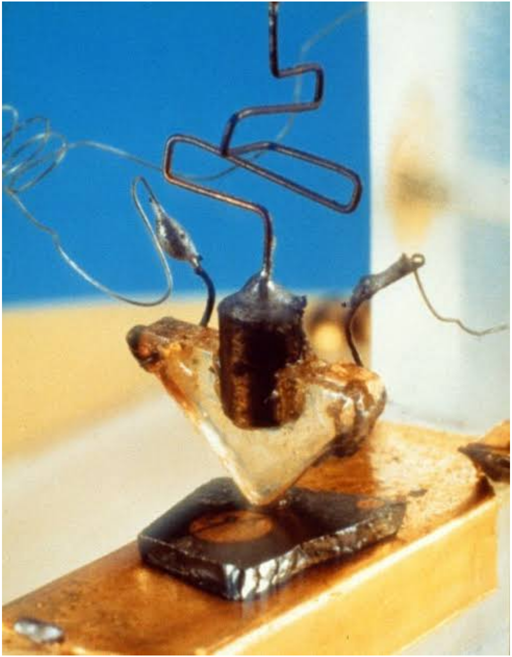
O Bit

Definição. ***(Anel Booleano)***
Um Anel booleano é um Anel $(\Omega, +, \cdot)$ com as operações $+$ e $\cdot$ definidas por:

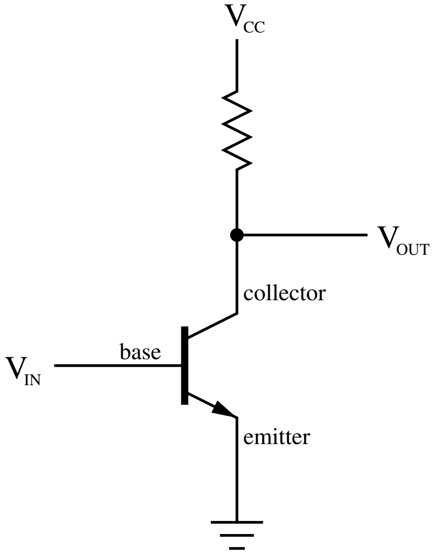
$$a + b := a \oplus b = (\neg a \wedge b) \vee (a \wedge \neg b)$$
$$a \cdot b := a \wedge b$$

É aqui que as contas com *bits* acontecem! Com $\Omega = \mathbb{Z}_2$, seguimos adiante e formamos vetores de *bits* como:

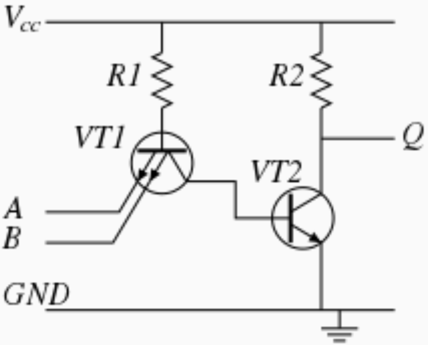
$$\begin{array}{rl}
 & 1 \\
 & 0101 \\
+ & 0100 \\
\hline
 & 1001
\end{array}
\qquad\qquad
\begin{array}{r}
5 \\
4 \\
\hline
9
\end{array}$$

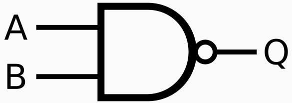


Transistor

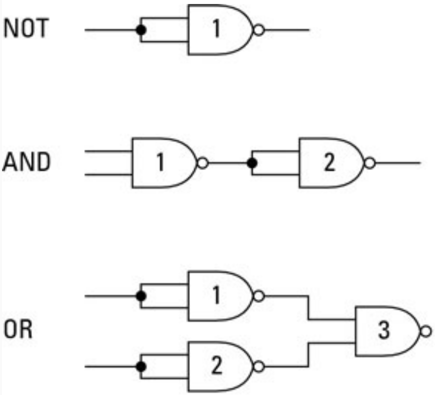


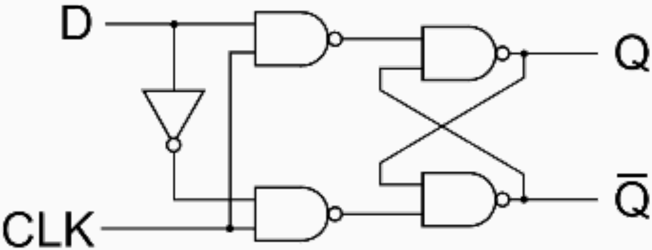
Portas Lógicas





Portas Lógicas




D
CLK
Q
$\overline{Q}$

Arquitetura de Von Neuman

John Von Neuman

1903 - 1957

Lei de Moore

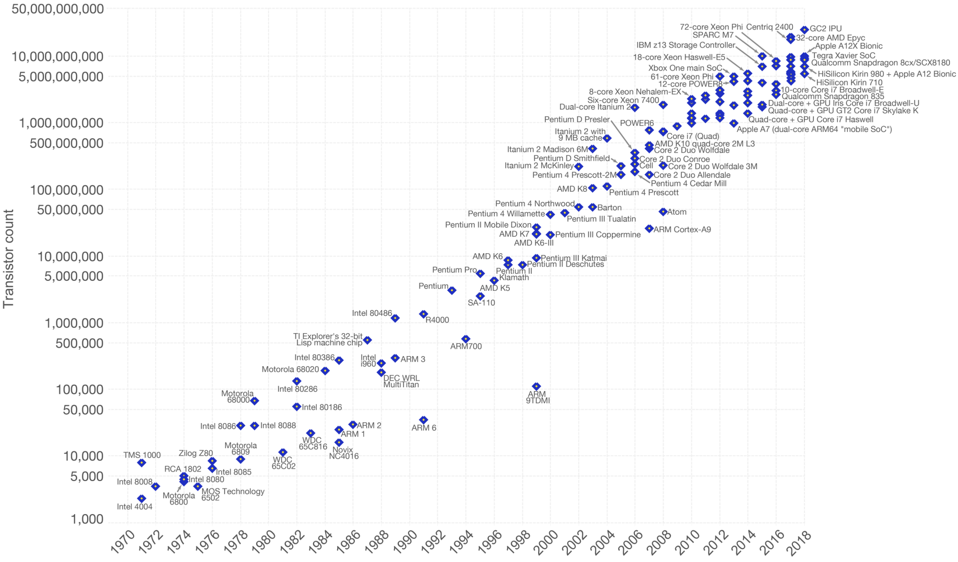
Gordon Moore

Intel, 1965

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

Our World in Data

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. There you find more visualizations and research on this topic.

Computação Quântica

Richard Feynman

1918 - 1988

Fenômenos Quânticos

Superposição

$$|\Psi\rangle = |\quad\rangle + |\quad\rangle$$

Superposição

$$|\Psi\rangle = |\uparrow\rangle + |\downarrow\rangle$$

Superposição

$|\Psi\rangle = |$ 

$\rangle + |$ 

$\rangle$

Fenômenos Quânticos

Superposição

$|\Psi\rangle = |$  $\rangle + |$  $\rangle$

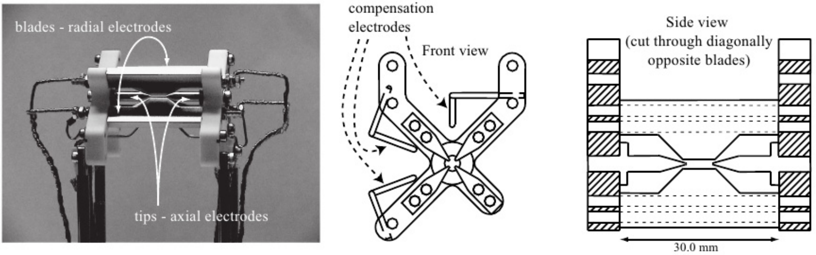
Superposição

$$|\Psi\rangle = |0\rangle + |1\rangle$$

Emaranhamento

O fenômeno do emaranhamento ocorre quando duas partículas distintas tem suas propriedades não somente correlacionadas, mas dependentes. Uma observação realizada em uma das partículas determina o estado da outra.

Trapped-ion



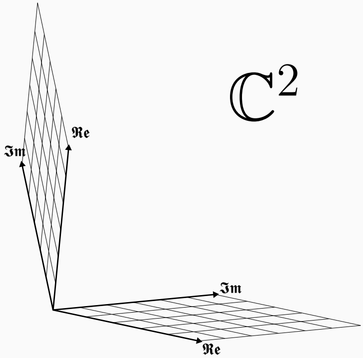
blades - radial electrodes
tips - axial electrodes
compensation electrodes
Front view
Side view
(cut through diagonally opposite blades)
30.0 mm

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.

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

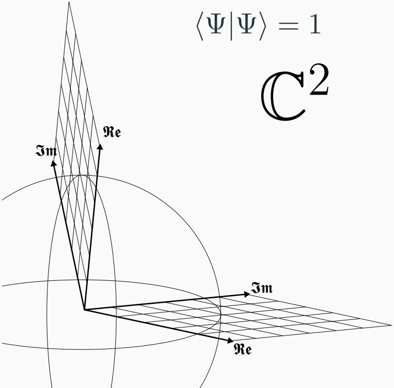


$$\mathbb{C}^2$$

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.

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

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



$$\mathbb{C}^2$$

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:

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

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:

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

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

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:

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

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:

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

Postulados

Postulado. (***Evolução***)

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

Postulados

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 $U^\dagger U = I$.

Postulados

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

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

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

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

Porta de Hadamard

$$|0\rangle \;-\!\boxed{H}\!-\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \;-\!\boxed{H}\!-\; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Postulados

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

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

Postulados

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

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

$$X\left|0\right\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \left|1\right\rangle$$
$$X\left|1\right\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \left|0\right\rangle$$

Não-controlado (CNOT)

Opera como a porta X de Pauli, dependendo do valor de outro *qubit*.

$$CNOT\,|00\rangle = |01\rangle$$
$$CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle$$
$$CNOT\,|11\rangle = |10\rangle$$

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*)

Medidas são descritas por uma coleção de operadores $\{M_i\}$, definida pelos estados da base em relação a qual se quer medir. Por exemplo, para a base computacional $\{|0\rangle, |1\rangle\}$

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Postulado. (*Medida*)

A probabilidade de medir um determinado estado $|i\rangle$ da base, dado um estado $|\Psi\rangle$ é atribuída pelo quadrado da norma da projeção realizada pelo operador M_i. Vejamos:

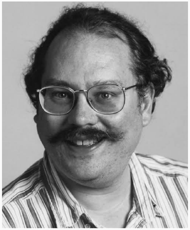
$$\begin{aligned} P(|i\rangle \,|\, |\Psi\rangle) &= ||M_i |\Psi\rangle ||^2 \\ &= (M |\Psi\rangle)^\dagger M_i |\Psi\rangle \\ &= \langle\Psi| M_i^\dagger M_i |\Psi\rangle \end{aligned}$$

Algoritmo de Grover

Lov Grover

Bell Labs

Algoritmo de Shor



Peter Shor

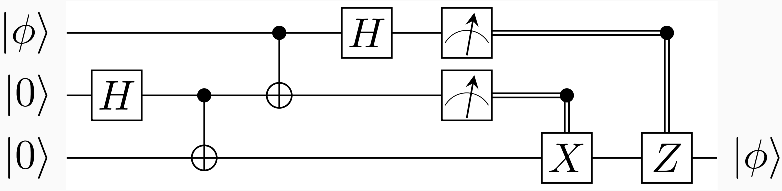
MIT


SO, QUANTUM TELEPORTATION—
THE NAME IS MISLEADING. IT'S A PARTICLE STATISTICS THING.
SO IT'S NOT LIKE STAR TREK? THAT'S BORING.
OKAY, I'M SICK OF THIS. EVERY TIME THERE'S A PAPER ON QUANTUM TELEPORTATION, YOU REPORTERS WRITE THE SAME DISAPPOINTED STORY.
BUT—
TALK TO SOMEONE ELSE. I'M GOING TO THE BAHAMAS.
CLICK
TELEPORTER
QUANTUM
REGULAR
VRMMM

Teletransporte Quântico

Imagine o teletransporte como um operador

$$\mathcal{T} : |\Psi\rangle_A |0\rangle_A |0\rangle_B \to |\xi\rangle \otimes |\Psi\rangle_B$$



Teorema da não-clonagem

Teorema. (***Não-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 $|\Phi\Phi\rangle$:

$$\begin{aligned}
\langle\Psi\Psi|\Phi\Phi\rangle &= \langle\xi\Psi|\, U^{\dagger}U\,|\Phi\xi\rangle \\
&= \langle\xi\Psi|\Phi\xi\rangle \\
(\langle\Psi|\otimes\langle\Psi|)\cdot(|\Phi\rangle\otimes|\Phi\rangle) &= (\langle\Psi|\otimes\langle\xi|)\cdot(|\Phi\rangle\otimes|\xi\rangle) \\
\langle\Psi|\Phi\rangle\otimes\langle\Psi|\Phi\rangle &= \langle\Psi|\Phi\rangle\otimes\langle\xi|\xi\rangle \\
\langle\Psi|\Phi\rangle^2 &= \langle\Psi|\Phi\rangle
\end{aligned}$$

Portanto:

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

$\blacksquare$

Caminhadas Quânticas

Definição. (*Caminhada Aleatória*)
Uma caminhada aleatória é um processo que consiste em, partindo do 0, caminhar sobre a reta dos inteiros ($\mathbb{Z}$) conforme os lançamentos de uma moeda $m_i \in \{-1, 1\}$, de modo que a posição do viajante após N passos será:

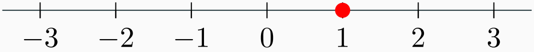
$$\sum_{i=1}^{N} m_i$$

Caminhadas Quânticas

Definição. (***Caminhada Aleatória***)

Uma caminhada aleatória é um processo que consiste em, partindo do 0, caminhar sobre a reta dos inteiros ($\mathbb{Z}$) conforme os lançamentos de uma moeda $m_i \in \{-1, 1\}$, de modo que a posição do viajante após N passos será:

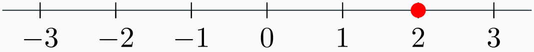
$$\sum_{i=1}^{N} m_i$$



Caminhadas Quânticas

Definição. (***Caminhada Aleatória***)
Uma caminhada aleatória é um processo que consiste em, partindo do 0, caminhar sobre a reta dos inteiros ($\mathbb{Z}$) conforme os lançamentos de uma moeda $m_i \in \{-1, 1\}$, de modo que a posição do viajante após N passos será:

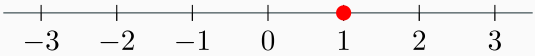
$$\sum_{i=1}^{N} m_i$$



Caminhadas Quânticas

Definição. (*Caminhada Aleatória*)
Uma caminhada aleatória é um processo que consiste em, partindo do 0, caminhar sobre a reta dos inteiros ($\mathbb{Z}$) conforme os lançamentos de uma moeda $m_i \in \{-1, 1\}$, de modo que a posição do viajante após N passos será:

$$\sum_{i=1}^{N} m_i$$



Caminhadas Quânticas

Definição. (*Caminhada Aleatória*)

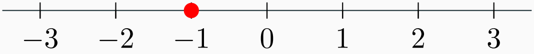
Uma caminhada aleatória é um processo que consiste em, partindo do 0, caminhar sobre a reta dos inteiros ($\mathbb{Z}$) conforme os lançamentos de uma moeda $m_i \in \{-1, 1\}$, de modo que a posição do viajante após N passos será:

$$\sum_{i=1}^{N} m_i$$

Caminhadas Quânticas

Definição. (***Caminhada Aleatória***)
Uma caminhada aleatória é um processo que consiste em, partindo do 0, caminhar sobre a reta dos inteiros ($\mathbb{Z}$) conforme os lançamentos de uma moeda $m_i \in \{-1, 1\}$, de modo que a posição do viajante após N passos será:

$$\sum_{i=1}^{N} m_i$$



Definição. (*Caminhada Quântica*)
Para realizar uma caminhada quântica, temos que preparar um sistema como

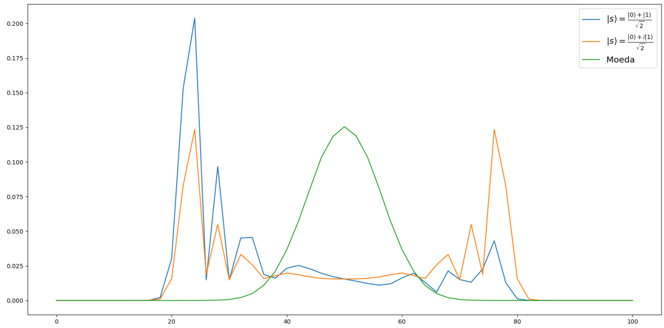
$$|\Psi\rangle = |s\rangle \otimes |x\rangle$$

Onde $|s\rangle$ será nossa "moeda" e $|x\rangle$ a posição da partícula.
Em $|\Psi\rangle$ aplicaremos um operador U definido como:

$$U = |0\rangle\langle 0| \otimes \sum_i |i-1\rangle\langle i| + |1\rangle\langle 1| \otimes \sum_i |i+1\rangle\langle i|$$

$$U|\Psi\rangle = |0\rangle\langle 0|s\rangle \otimes \sum_i |i-1\rangle\langle i|x\rangle + |1\rangle\langle 1|s\rangle \otimes \sum_i |i+1\rangle\langle i|x\rangle$$

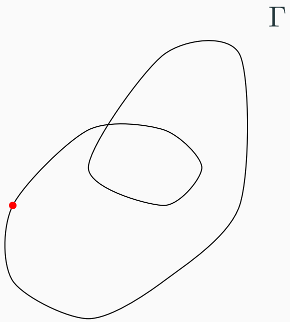
Caminhadas Quânticas



Computação Topológica

Ânions

Em geral, quando partículas como bósons e férmions descrevem uma curva fechada $\Gamma \subset \mathbb{R}^3$, é como se estas jamais tivessem se movido.



Ânions

Imaginem que temos n partículas em posições $\mathbf{x}_i$ distintas de $\mathbb{R}^3$, de modo que seu estado quântico é representado por

$$|x_1 ... x_i ... x_j ... x_n\rangle$$

Trocando duas partículas de posição, temos que

$$|x_1 ... x_j ... x_i ... x_n\rangle = \theta \, |x_1 ... x_i ... x_j ... x_n\rangle \, , \theta \in \mathbb{C}$$

Trocando i por j novamente, voltamos ao estado inicial! Isso significa que $\theta^2 = 1$. Quando $\theta = 1$ temos um bóson, e quando $\theta = -1$, um férmion.

Ânions

Já os ânions se separam em dois grupos: os **Abelianos** e os **não-Abelianos**.
Os interessantes são os **não-Abelianos**!

Computação Adiabática

Equação de Pauli

Seja $\vec{\sigma} = [\sigma_1, \sigma_2, \sigma_3]^T$. A equação a seguir descreve o comportamento de um sistema $|\phi\rangle$ sob um campo magnético.

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

Esse é o Pauli

Wolfgang Pauli

1900 -1958

Teorema Adiabático

Um sistema físico permanece no seu autoestado se uma perturbação atua suficientemente devagar e se há um intervalo entre o autovalor e o restante do espectro do Halmitoniano

Max Born, Vladmir Fock (1928)

Modelo de Ising

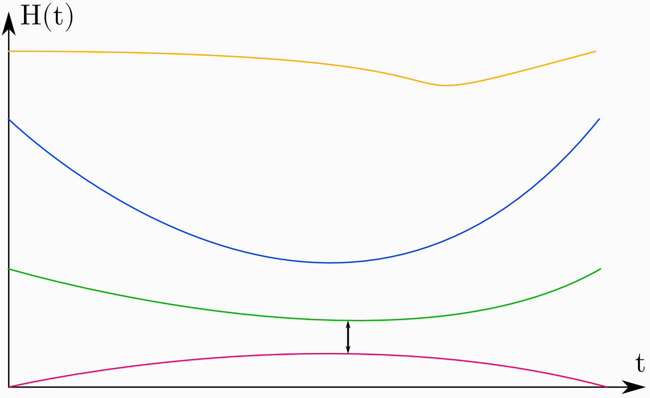
O modelo de Ising foi bolado para descrever as interações ferromagnéticas entre partículas adjacentes. Consiste em um Hamiltoniano dado por:

$$H = \sum_{i} h_i s_i + \sum_{i<j} J_i j s_i s_j$$

Têmpera Quântica

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

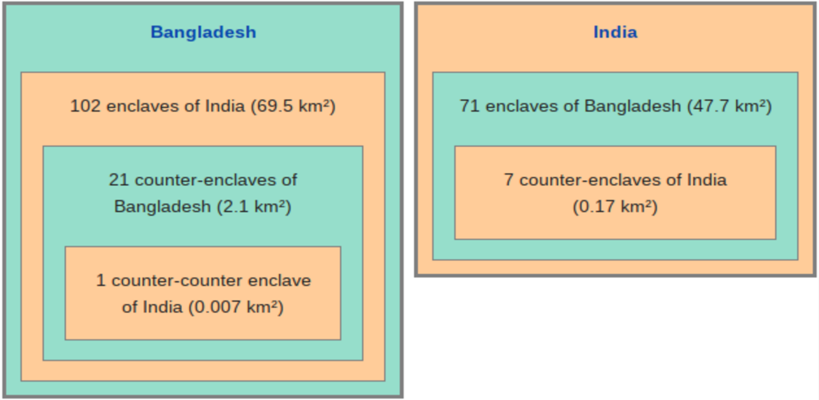
Têmpera Quântica

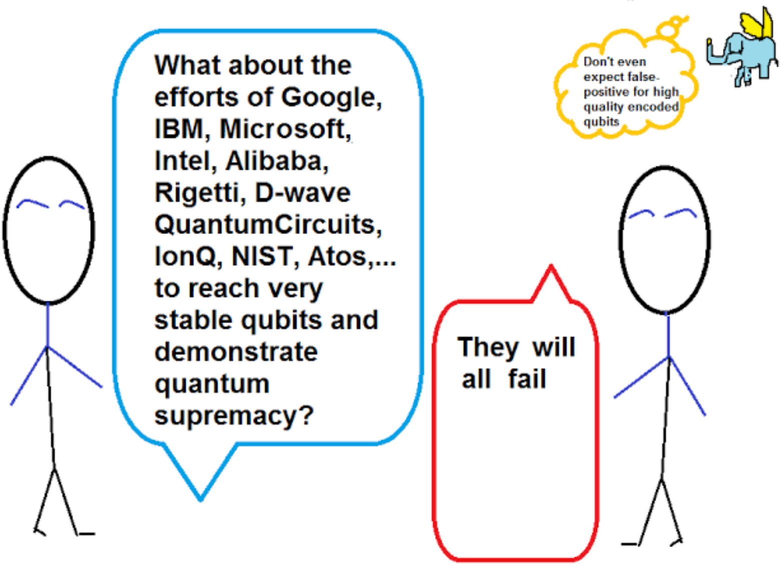


Fim?

Saltos Quânticos

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-positive for high quality encoded qubits

Gil Kalai

Yale & Huji

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.

Reprograme o seu DNA na frequência do Sucesso