**Encontros Matemáticos** apresenta

# Computação Quântica

Pedro Maciel Xavier
pedromxavier@poli.ufrj.br

19 de novembro de 2019

IM-UFRJ

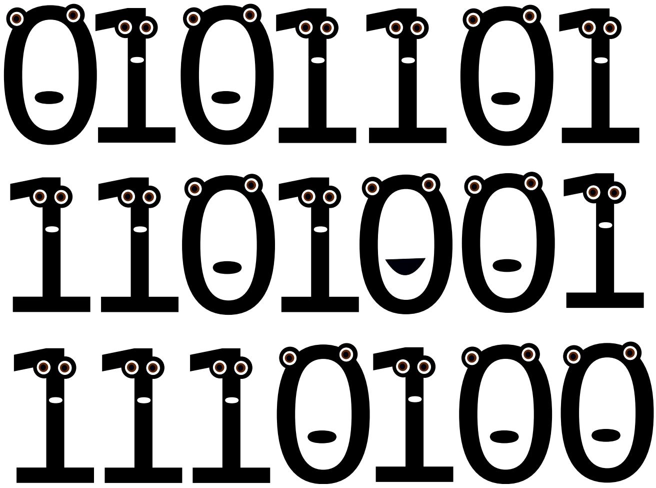
## Parte I

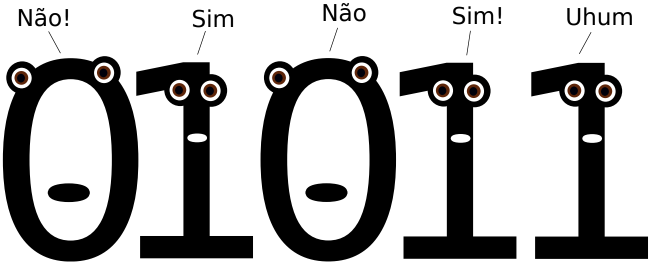
# Parte II

# Parte III

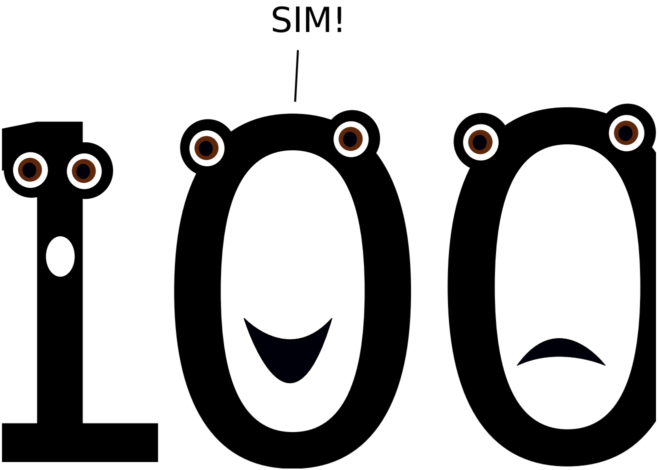
# Computação Digital

0100101100001010101010110101010111111011010111001111111001010101000010110000011100000101000101100100 1
1001000110111001101001010000101011011011101011011000110110101100010010011011000000011101111101010010
0111001110011100000001100010111111001000010100110100101110001001100010100001101001010001111011101100 1
0011000101010001000100110010111111010111010001110100011110000000111100010011010101100110000011001011
1011100000011100110001110110011101000101010010010000100111101101101011110111001111001110101000100011
1010000010110010000000101101001100111101111111001011001010100000010001001101101110010100101001110101 0
1011011010010101010111110000011011111011001111101000101101001010011010000111010110101010110100001101
1000110000001011100000010011011101010001010110110101001011101101000111111100011110111011100111111010 0
1001100000000000000001110111010010110000010000011101011001001011011111010011011010110110010111001010 1
1100011100000101011100011100100010111010111011111110110010100001100100001110110001100010001011011111
0110100110000011000110100101100010011001110111111101111101111111111000110100011010000100100001010011
0001100000101000111110101111101011010010000100010100011011101100100110010110000001101101001101101001
0100100001111110101101101001011111010111011010100111010001011000110110101000111111010011100111000100
0001101101010110111000011111110000111100110100011011011100011111000001100111000100100111001000000011
0010111111001100110101001011010000110001011110110111000011010010011000000110101111111000110011100001
1101000000000101101101111000011000101110000110011000001000000111101011011100111000001111111011111011 0
1010001100010000111001101101100001110001011010010101011101000110111111111001110010111010000001100011 01
1001111101101010110010110101010000001010111100011000111000000001100011101100100010011011010001000010 00
0010111100110011000000110111010000101101111100101010011100100110010110000111110010000000111111011001 01
0111100100101100011000010011000010111111101101010100000111100100000000000100001001111111100000110010 0
1011111100111101110000000001011001011000101011011100010100000100001111011111100100111000011101000001 1
0111101000000110111010111111010010110000101101101001010111100110011001110101110111101100100011011010
0011101010000010011101101011100111110011000010010000101100000111101000110001111111010011000001101111
0100101110101111110000001001100010110010111101010100001101101101101100110011111000001101001011011110 1
0101001010111111001001011001001011111011101010001100100110110111001100000100011010010001111100110100
1010110011000011100000001000111101101101001100100100111100001100001110110100011110001110010010111001 1
0100001001101000000000100110100011110111011111101110101010111001111111101101011101100110000100001011 00
0110000011100010001101101110101001001011110010001011001110101100100001100010000110000001100010000100
0101100001100111101101100100100000000110011011111010101011101010001000011110001100101001110100010100 1
0011100111010010010001001000100110000101101011100011111001011011011011111111001111000100001011110010 1
0011100011111100100010000101111011010010011111011111100010100110010100010101110101000010010010010111 1
0101011110101100000010100111000000010000101100110001000000111000001100100011011011100101001100010110 0
0101100001110100110110100100110100000101010001001111011001000101100110111010010000011001001100111100
1000011011110111000000111111010100111000010100100111110111000001101000010010101011101111010010101011 0
0011000101000011100001110011100110001100000100011011101011001001100011011000100011000110101011101101
1110000010110111000010010010000000000011100011011011001101111000110111000000011111010011001101100111 01
1110111101001110001101000010111000011111010110010011001010000011011111111010010001011111111011011110 00
0010110111111100111100010110010011110001010100010010111101100101010100111100010011101101000101101000
1111100100001100110010011000000111111110011000000001010101000101101010100001000100111010110000001000 1
1001100101001111100010011100110010101011110111101001100001100101100111000110001011000110010010110011
1101101001101110000101010110110011011110111110110001100110110000111010010001001010101100010110100 01
0001100100010111100001000101000101100101010111100011011000011011010100111101101011000101110010101011 1
1011011011000000110110101001111101010100111100010011011001100101011001111011011111110001111101100001 11
1011001111001101001101110011110111101011111110110101010110011011011101111100010011100001000101111010 10
1010001101001101010101011001111111110100101011110010101010110011000101011101111100001111011110110111
0101110110000001011101101101001110010011001000111000011010110010101011110000111011111111000001001101
0001110011101011011001010100101101101001101000011010101100111011111001010111010100000101111010001001
1110101010100010101010110101001011101110011010011110000110011111111010110111100001001111000000001111 0
1111100011100101001001101000100111100011110101010101101010011110011010101110100010100110011010111101
0001111101011110010010011010010100000111010011010010000000010001011011110100000101000011001001001010
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

Sobre os *bits*:

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

# Álgebra Booleana

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

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

# 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 ($q_0 \in Q$)
- $\Gamma$: Alfabeto da fita.
- $\square$: Símbolo vazio.
- $\Sigma$: Alfabeto de entrada da máquina. ($\Sigma \subseteq \Gamma / \{\square\}$)
- $\Omega$: Conjunto dos códigos de parada.
- $\delta$: Função de Transição, $\delta : Q/\Omega \times \Gamma \to Q \times \Gamma \times \{\uparrow, \downarrow\}$

Alonzo Church

1903 - 1955

Alan Turing

1912 - 1954

# A Tese de Church-Turing

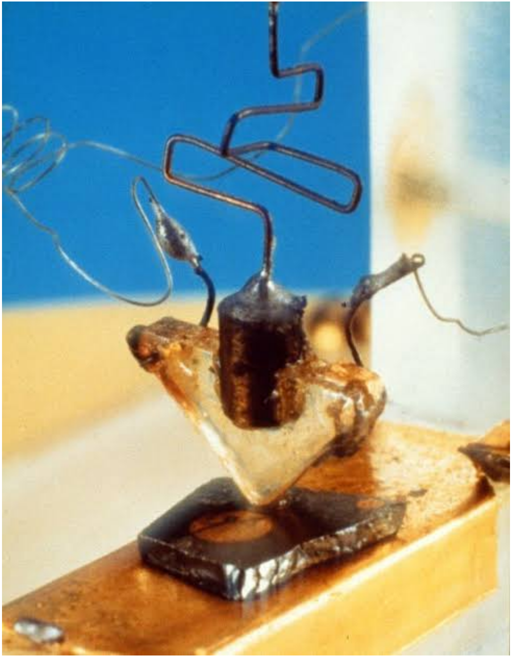
> *Toda função que seria naturalmente computável pode ser computada por uma Máquina de Turing*
>
> Alan Turing

**Definição.** (***Complexidade Assintótica***)

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

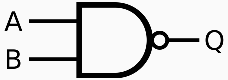
$$f(x) = O(g(x)) \iff \exists M, x_0 |f(x)| \leq Mg(x), \forall x > x_0$$

# Complexidade e Computabilidade



# Transistor

# Portas Lógicas



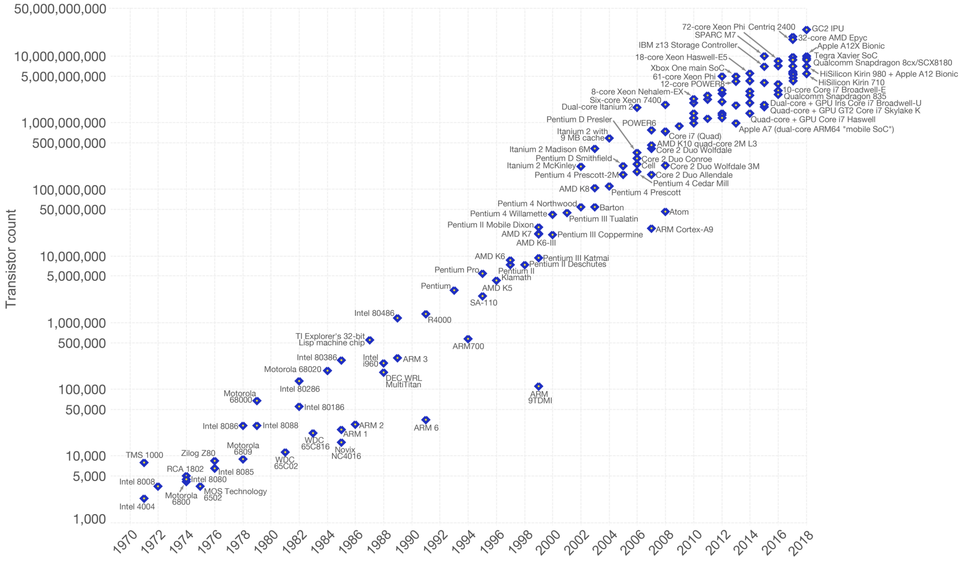
# Arquitetura de Von Neuman

John Von
Neuman
1903 - 1957

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

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.

# Lei de Moore

Gordon Moore

Intel, 1965

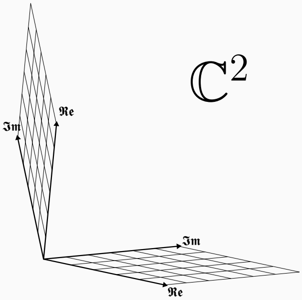
# Computação Quântica

Richard Feynman

1918 - 1988

**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.

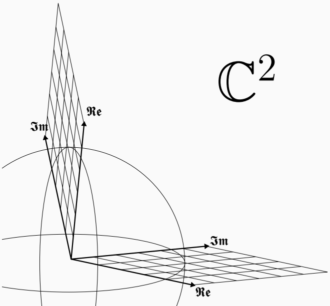
$$|\Psi\rangle \in \mathrm{C}^2 \qquad\qquad (\mathbf{x} \in \mathrm{C}^2)$$



**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.

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

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




$\mathbb{C}^2$

**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 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*)**
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:

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

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.

# 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!

# Postulados

Matriz de Hadamard

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

# Postulados

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

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

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

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

# 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.**

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

# Postulados

**Postulado.** (*Medida*)

# Trapped-ion

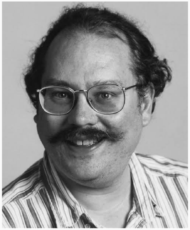
Oi íon aprisionado

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

# 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 $|\Phi\Phi\rangle$:

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

Portanto:

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

■

# Fótons

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

## Caminhadas Quânticas

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

# Computação Topológica

# Nós

# Nós

# Ânions

# Ânions

# Computação Adiabática

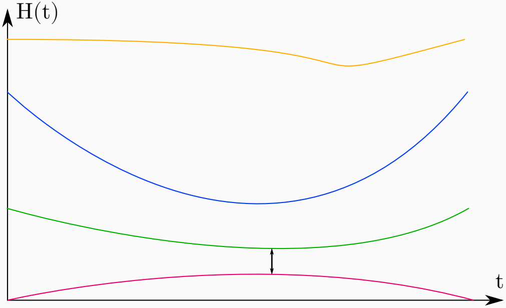
# Equação de Pauli

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

# Têmpera Quântica

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

# Têmpera Quântica



# Fim?

## Supremacia Quântica

# Material

# Bibliografia


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