

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

### 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

Saltos Quânticos

Fim?

Supremacia Quântica

Material

Bibliografia

# Computação Digital

---

010010110000101010101011010101111101010110011111001010101000010110000011100001010001011001001  
10010001011100110100101000010101010101010101000101010100001001001010000000110111101010010  
0111001110011000000011000101111100100001010010100010110001001100001010001010001101110101001  
00110001010100010001001010010111101011100001110000111000000011100010010101010000011001011  
1011100000011100110001101100111010001010100100100001001111011011011110110011100110101000100011  
1010000010110010000000101010011001111011111001010010100000010001001101101100101001010011101010  
10110110100101010101111000001101111010011010100010101001010011010000111010110101010100001101  
100011000000101110000010011011010100010101010100101110100011111100001110110111001111110100  
10011000000000000000111011101001010000010000011010100100101011110100101010101010010110010101  
1100011100000101011100011001000010110101101111101100101000011001000011011000110001000101011111  
01010011000001000010100101000100010011001111011110111111000101000010100001000000100001010011  
00010000001010001111010111101010100100001000101000110111011001001100101100000010101010010101001  
01001000011111010101010010011110101110100111010001010001010101000011110100110011000100100100  
0001010101010111000011111100001110011010001010111000111100000100111000100100111001000000011  
0010111110011001010101010010101000011000101111010111000010100100110000001010111110001100110001  
110100000000010101011110000110001011000001001100000111010101110011001100110000000111101111010  
101000110001000011001010111000011100001011000010101110100011001111100001101110000000110001101  
10011110101010100110010101010000010101100011000110000000100011010100000010010101000100001000  
0010111100110011000001010110000010101111001010100111001001100101100000111100100000011101101001  
0111100100101000110000100110000101111101010101000001110010000000001000010011111100000100100  
10111110011101110000000010100101100010101011000101000001000011101111100100111000011010000011  
011110100000010101101011111010010100000101010100101011100100110011010111101100100010101010  
001101010000010011010101011100111001100010000010100001110100011000011111010011000001101111  
01001011010111110000010010001010010111010101000010101101010100010011110000010100101011101  
010100101011111001001010010010111101101010001100100101011100110000010001101001000111110010010  
1010110011000011100000001000111010110100110010010011100001100001110101000111000110010010110011  
010000101010000000010011010001110110111101101010101100111111011010101010001100001000010100  
0110000011100010001101011101010010010111001000101001110101100100001100010000110000001100010000100  
0101100001100111101010010010000001100110111101010110101000100001110001100101001101000101001  
00110001110100100100010001000101000010100001110010110010101111100111110001000010111001  
001100001111100100010000010111010100100111011110001001100100100010101101000010010010111  
0101011101010000010001100000000100001100010000000110000011001000101011100100110001010010100  
0101000001101001010100100101000001010100010011101100100010100101010000001001001010011001100  
1000010111011100000111101010011100000101000100111101100000101000010010101101010010101010  
00110001010000111000011100111001100011000001000101110101100100110001101100010001100010101010101  
1110000101011100001001001000000000110001010100101011100010111000000011110001001011001101  
110101100111000111000101000001110000111101010010011001010000010111110101000100010111101011000  
00101011111100111100010100100111000101000010011101100101010011110001000111010100001010001  
11110010000110011001001100000001111110011000000010101000010101010000100010011010100000010001  
100110010010011110001000111001100101010111011101001100001100101001100011000100010100110011  
1101010010101100001010101010010111101111010001100101000001001001000010010101000101010001  
0001001000101110000100010100010100101010110001101100001010101001111010101000101011000101011  
101010110000011010100111101010011110101001110001001100110010011101011110001111010000111  
10110011100110011001110011101110101111101010101001101101111000100111000010001011101010  
1010001101001101010101001111111010010101100101010101001100010010101111000011101110110111  
010111011000000101110101010011100100110010001100001101010010101110000101011111100000001001  
0001110011010101010100101001010101001101010100110111000101011100010101110001001011010001001  
1101010100001010101010100101011100110010100111000011001111110101011000000001110100000001110  
111100001100101001010100010011100001110101010101010011100110101010100001001001001101011101  
0001111010111100100100101001010000011101001010010000000100010101110100000001000010010010010  
101111110100001111011000011100111110000010100001000000010101000100100111111010111001001100011

0101101

1101001

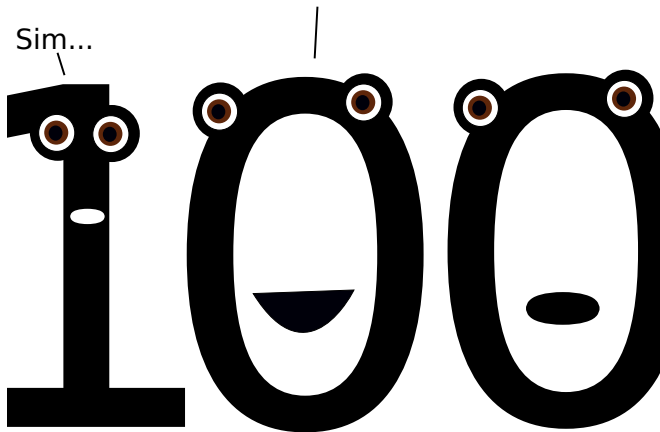
1110100

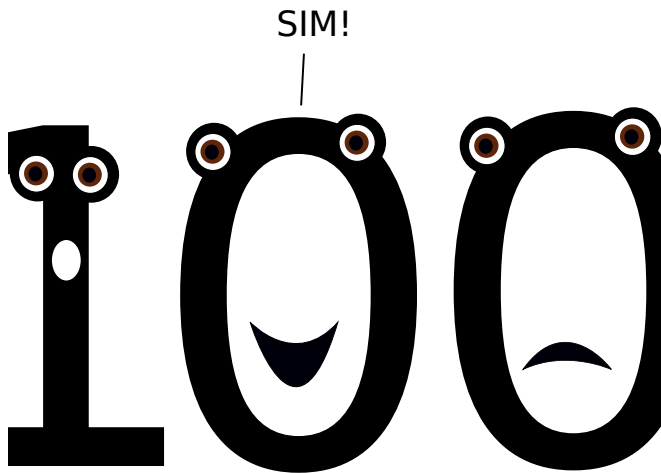




Finalmente! É o meu grande dia!

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  $11\dots 1 = 2^n - 1$ .

## 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 ( $q_0 \in Q$ )

$\Gamma$ : 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,  $\delta : Q / \Omega \times \Gamma \rightarrow Q \times \Gamma \times \{\uparrow, \downarrow\}$



# 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*

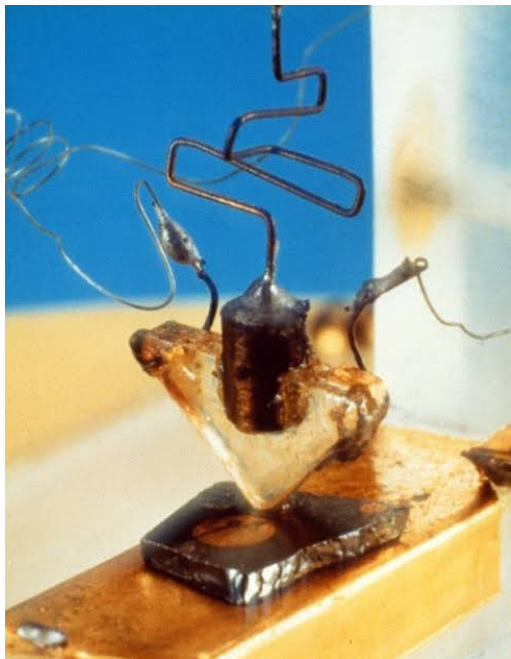
Alan Turing

## 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

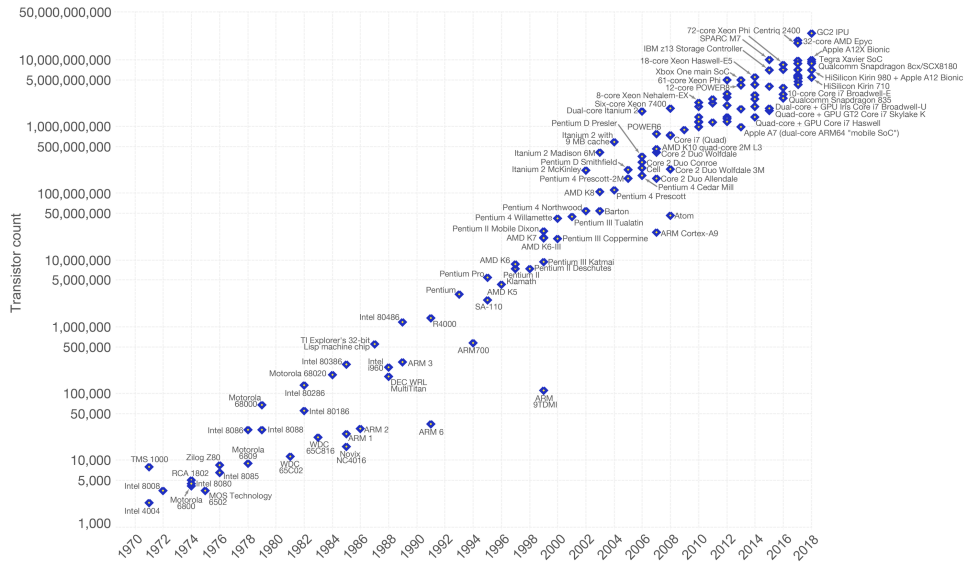
Neuman

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](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

# Computação Quântica

---



Richard Feynman

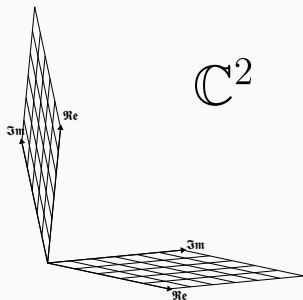
1918 - 1988

# 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.

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



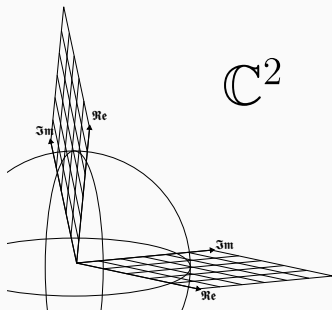
# Postulados

## 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*)

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

## 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*)

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:

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

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!

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

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

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

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



# Uma nota sobre reversibilidade

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

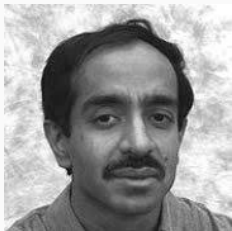
**O Princípio de Landau.**

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

Postulado. (*Medida*)

Oi íon aprisionado

# Algoritmo de Grover

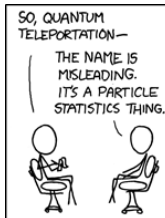


Lov Grover

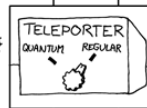
Bell Labs



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  $|\Phi\Phi\rangle$ :

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

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

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

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

Portanto:

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



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

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

# Computação Topológica

---











# Computação Adiabática

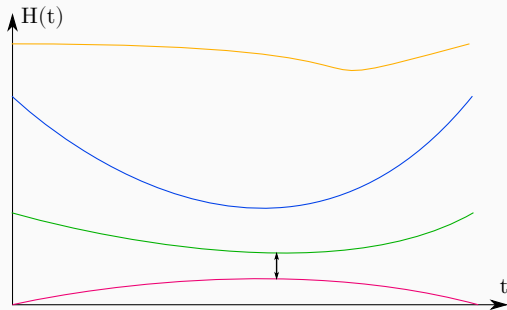
---

## 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?**

---











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

