Encontros Matemáticos apresenta

Computação Quântica

Pedro Maciel Xavier
pedromxavier@poli.ufrj.br

19 de novembro de 2019

IM-UFRJ

Parte I

Computação Digital

- O Bit
- Álgebra Booleana
- Complexidade e Computabilidade
- Transistor
- Portas Lógicas
- Arquitetura de Von Neuman
- Lei de Moore

Parte II

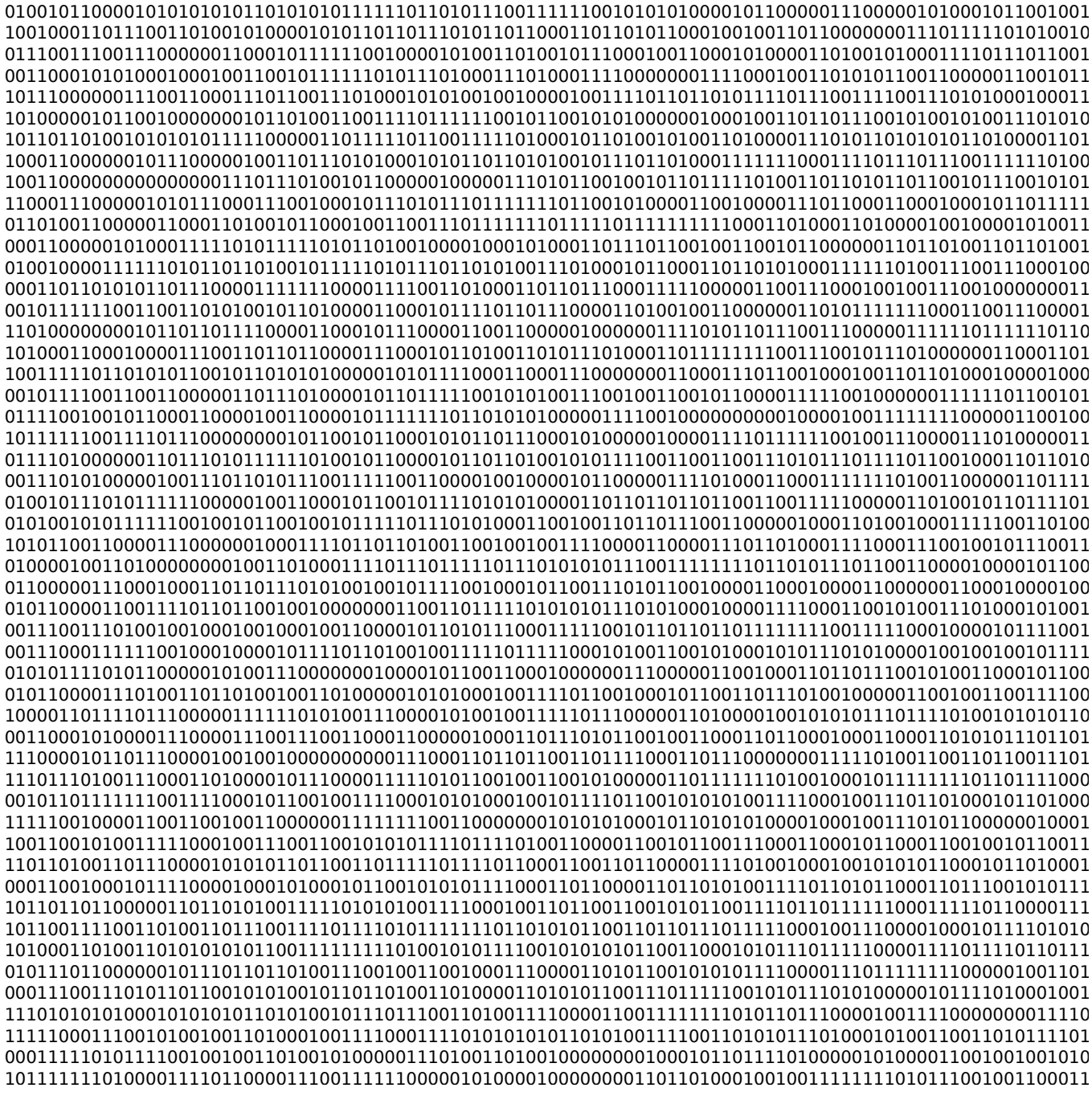
- Computação Quântica
  - Postulados
  - Trapped-ion
  - Algoritmos
  - Teletransporte Quântico
  - Teorema da não-clonagem
  - Fótons
  - Caminhadas Quânticas
- Computação Topológica
  - Nós
  - Ânions
- Computação Adiabática
  - Teorema Adiabático
  - Têmpera Quântica
  - Saltos Quânticos

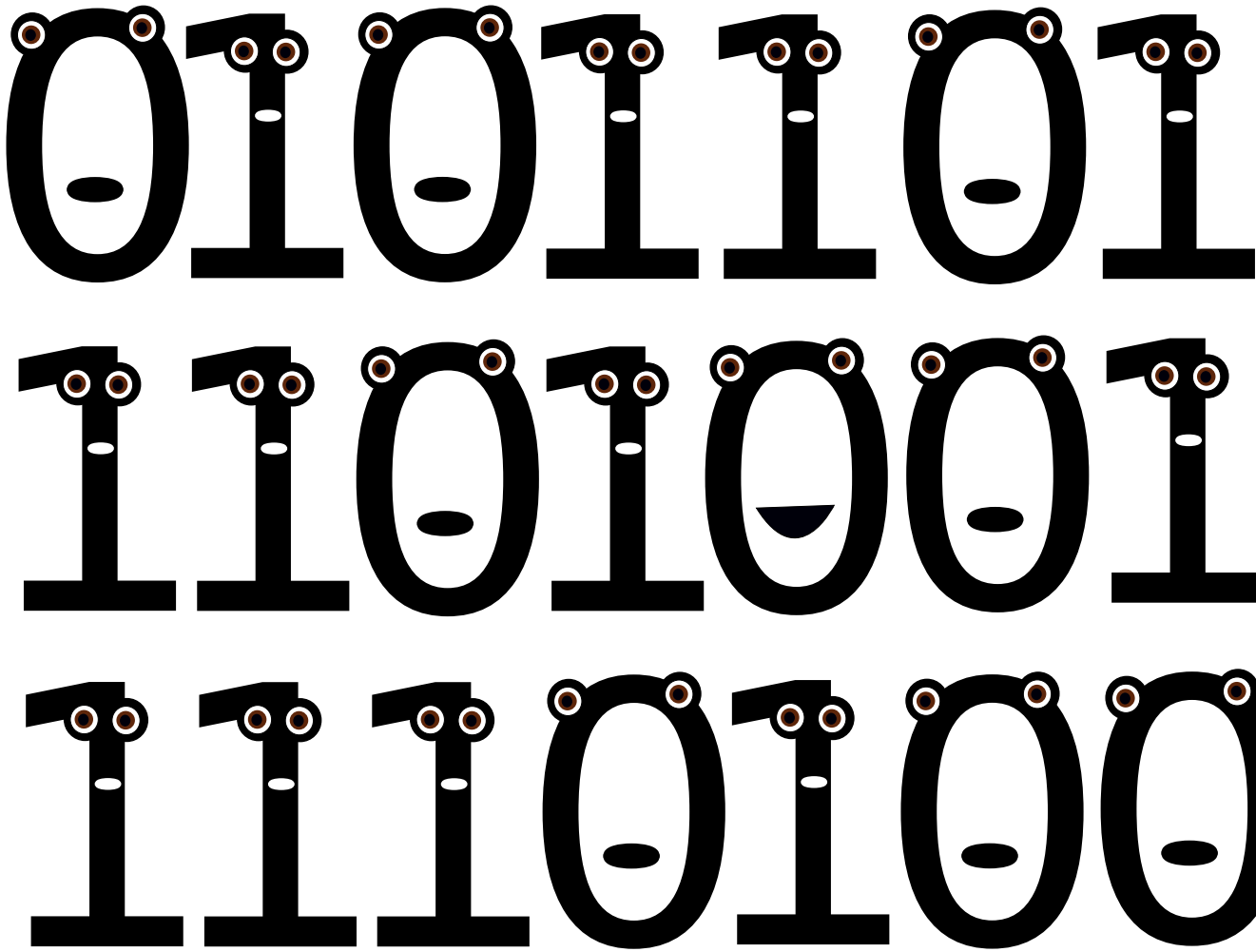
Parte III

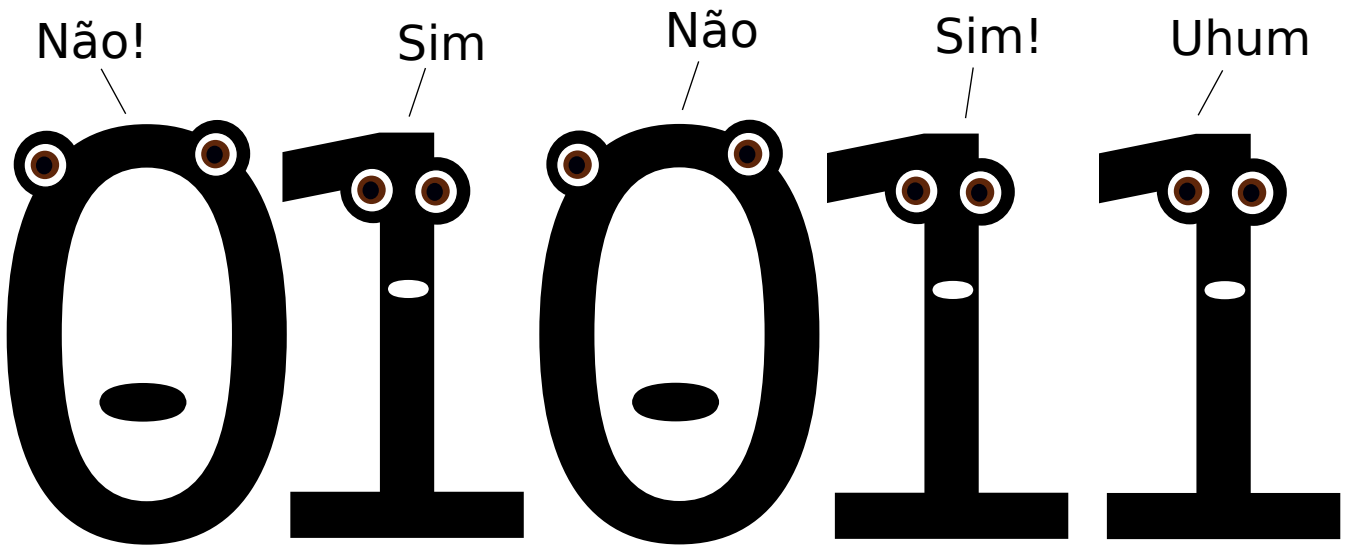
Fim?

- Supremacia Quântica
- Material
- Bibliografia

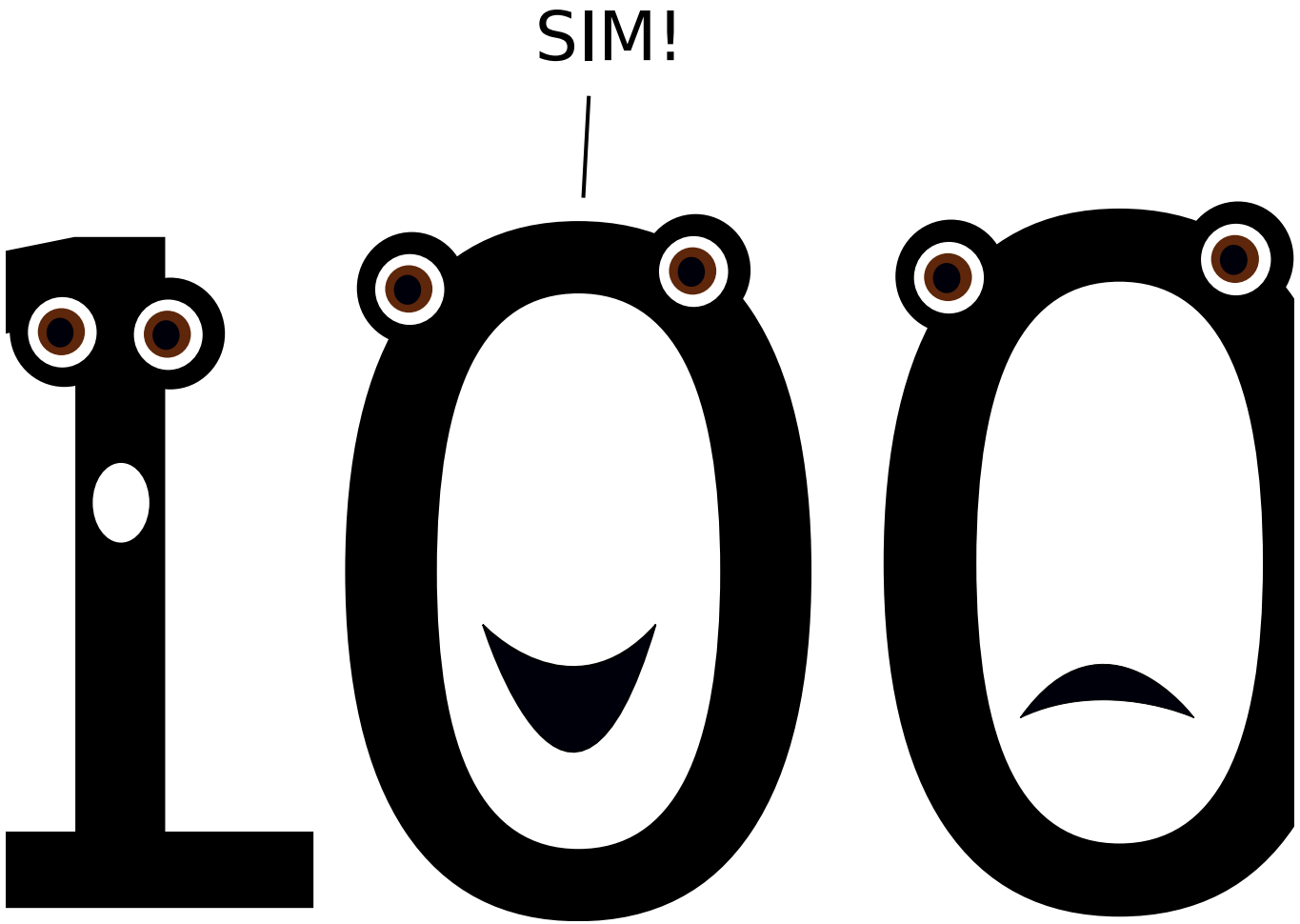
Computação Digital






Não!
Sim
Não
Sim!
Uhum
01011


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 $\mathbb{Z}_2$
- Realizamos operações *Booleanas* com eles: $\neg$, $\wedge$, $\vee$, $\oplus$.
- Formam vetores em $\mathbb{Z}_2^n$, onde cada $\vec{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_2^n$ 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:

$a \vee (b \vee c) = (a \vee b) \vee c$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	associatividade
$a \vee b = a \vee a$	$a \wedge b = b \wedge a$	comutatividade
$a \vee 0 = a$	$a \wedge 1 = a$	identidade
$a \vee \neg a = 1$	$a \wedge \neg a = 0$	complemento
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	distributividade
$a \vee (a \wedge b) = a$	$a \wedge (a \vee b) = a$	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

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

Alonzo Church

1903 - 1955

Alan Turing

1912 - 1954

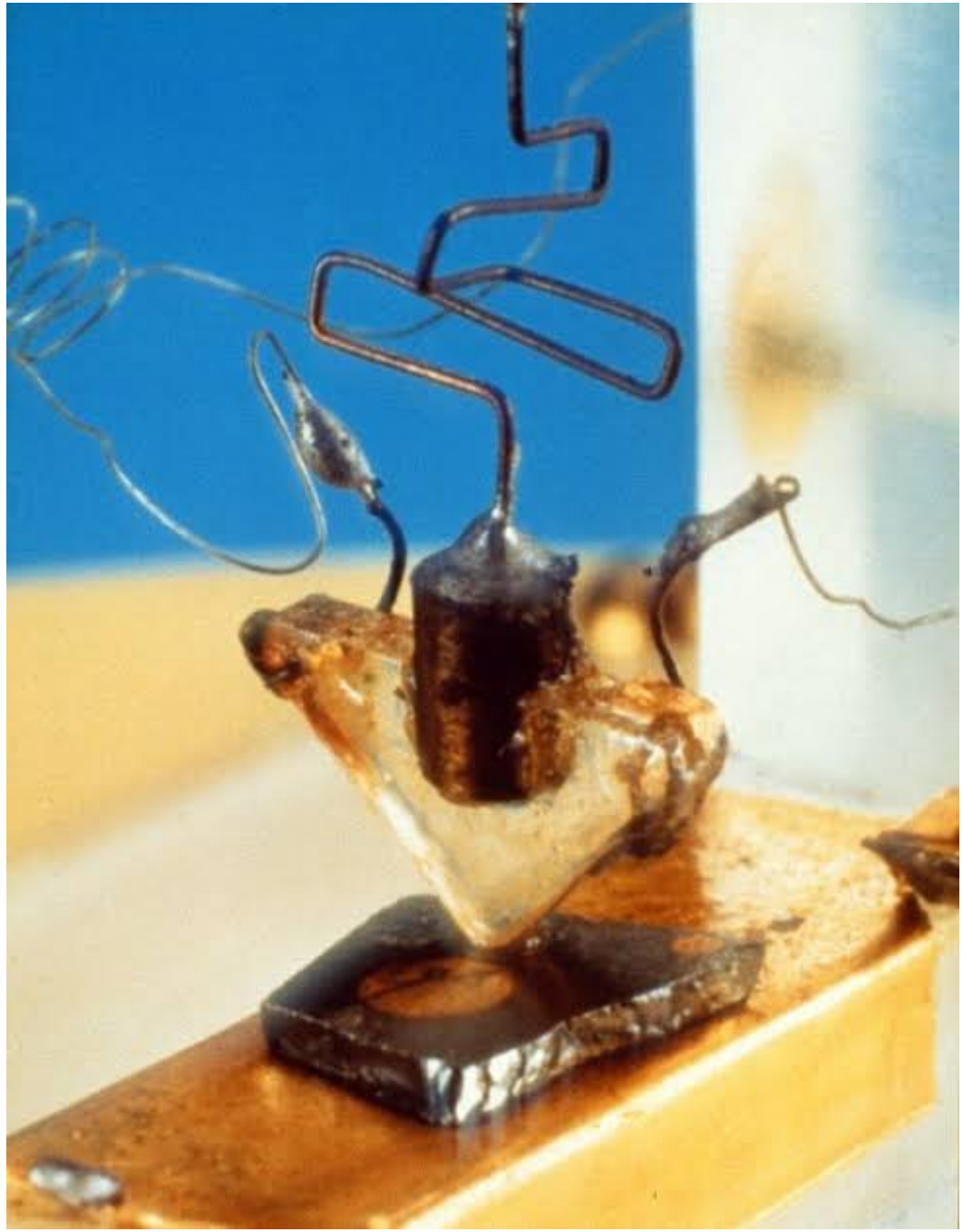
A Tese de Church-Turing

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

Alan Turing

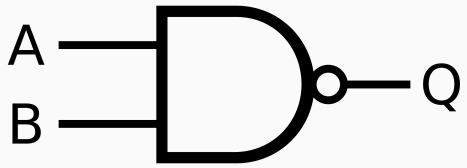
Definição. (***Complexidade Assintótica***)
Seja $f : X \subseteq \mathbb{R}_+ \to \mathbb{C}$ e $g(x) : X \subseteq \mathbb{R}_+ \to \mathbb{R}_+$ dizemos que

$$f(x) = O(g(x)) \iff \exists M, x_0$$



Transistor

Portas Lógicas



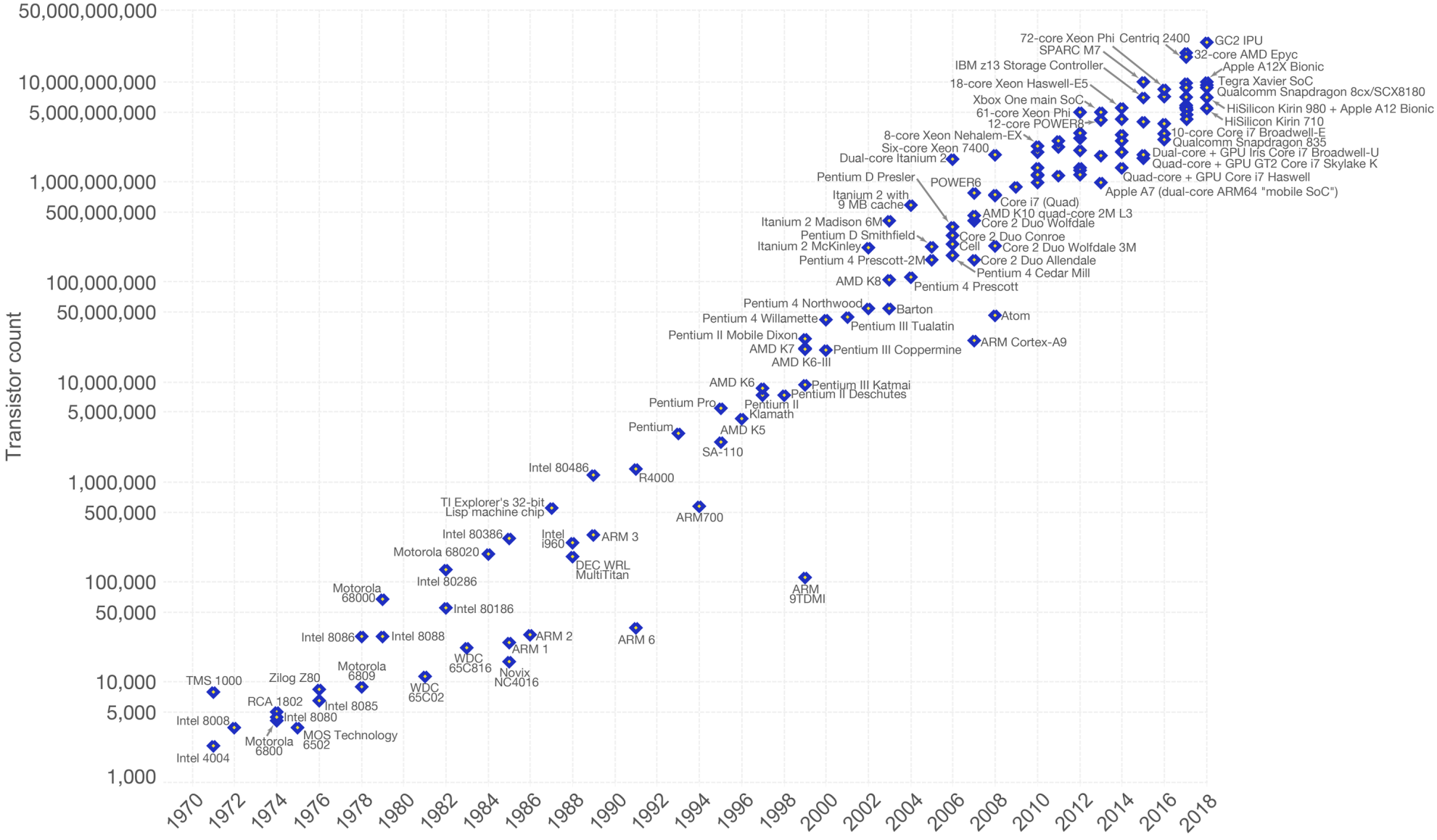
Arquitetura de Von Neuman

John Von Neuman

1903 - 1957

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

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.

Gordon Moore

Intel, 1965

Fenômenos Quânticos

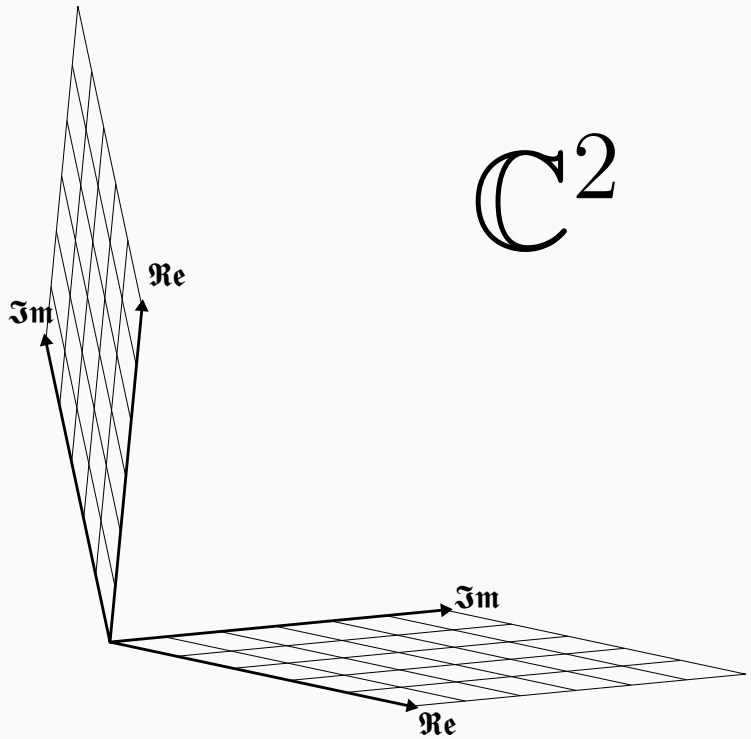
Richard Feynman

1918 - 1988

Computação Quântica

Postulado. (***Representação***)

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

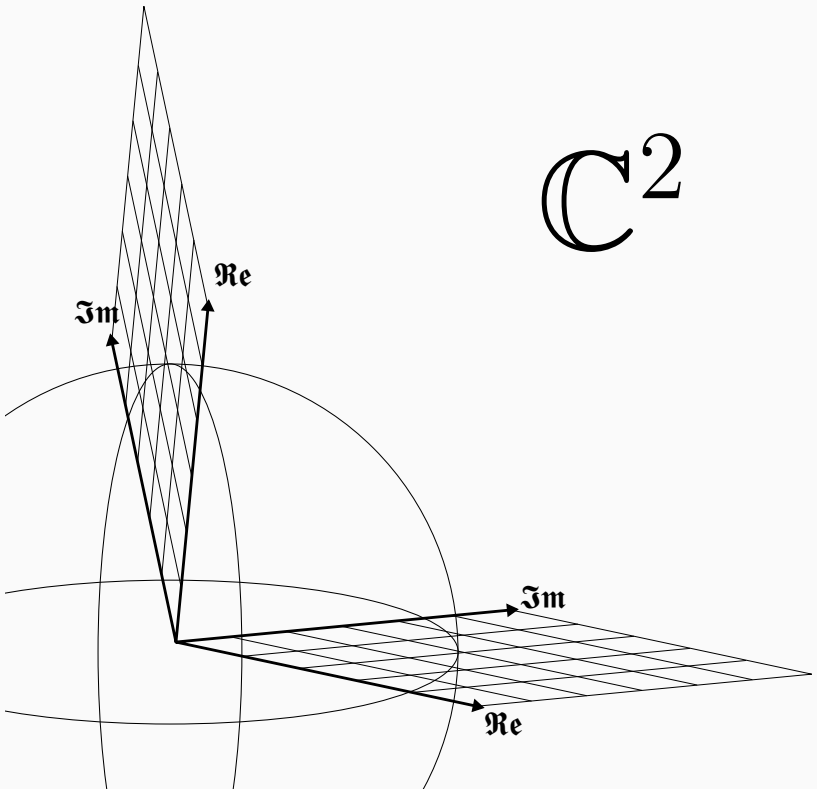


$$\mathbb{C}^2$$

Postulado. (***Representação***)

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

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



Postulados

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:

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

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

Postulados

Postulado. (***Evolução***)
A evolução de um sistema se dá por meio de operadores unitários U

Uma nota sobre reversibilidade

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

Trapped-ion

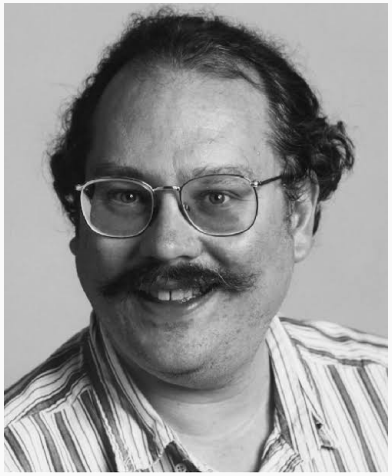
Oi íon aprisionado

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

Teorema da não-clonagem

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 $|\Psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle$ qualquer, isto é:

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

Assim:

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

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

Teorema da não-clonagem

Por outro lado:

$$\begin{aligned}
|\Psi\rangle \otimes |\Psi\rangle =& (\alpha |\uparrow\rangle + \beta |\downarrow\rangle) \otimes (\alpha |\uparrow\rangle + \beta |\downarrow\rangle) \\
=& \alpha^2 |\uparrow\uparrow\rangle + \alpha\beta(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) + \beta^2 |\downarrow\downarrow\rangle \\
\neq& \alpha |\uparrow\uparrow\rangle + \beta |\downarrow\downarrow\rangle
\end{aligned}$$

■

Fótons

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

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

Computação Topológica

Nós

Nós

Ânions

Ânions

Computação Adiabática

Teorema Adiabático

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

Teorema Adiabático

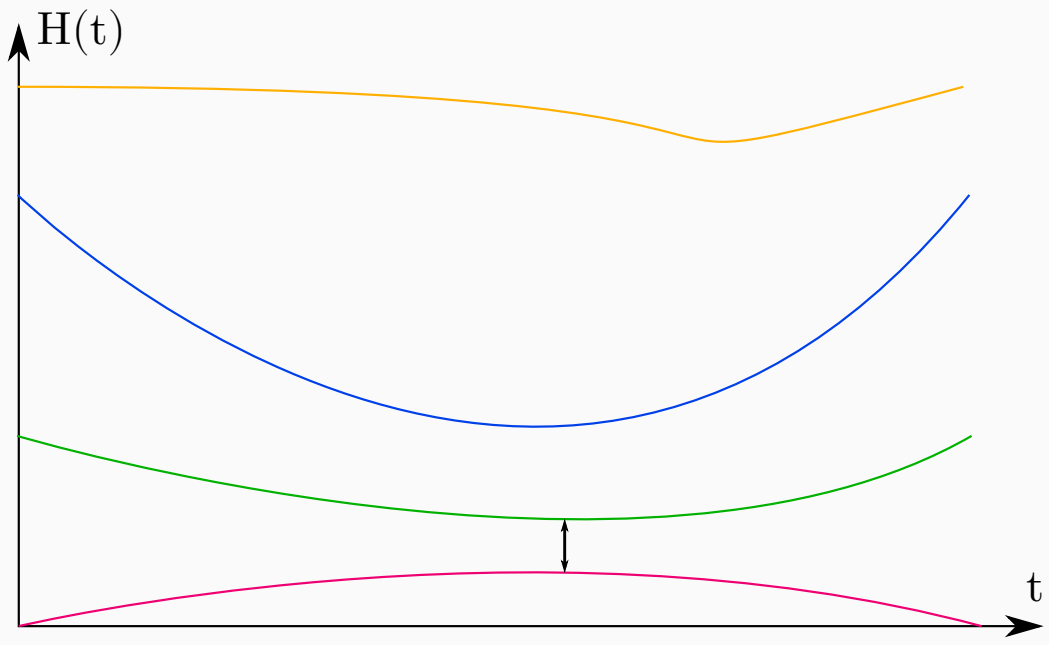
Teorema Adiabático

Teorema Adiabático

Têmpera Quântica

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

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.