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

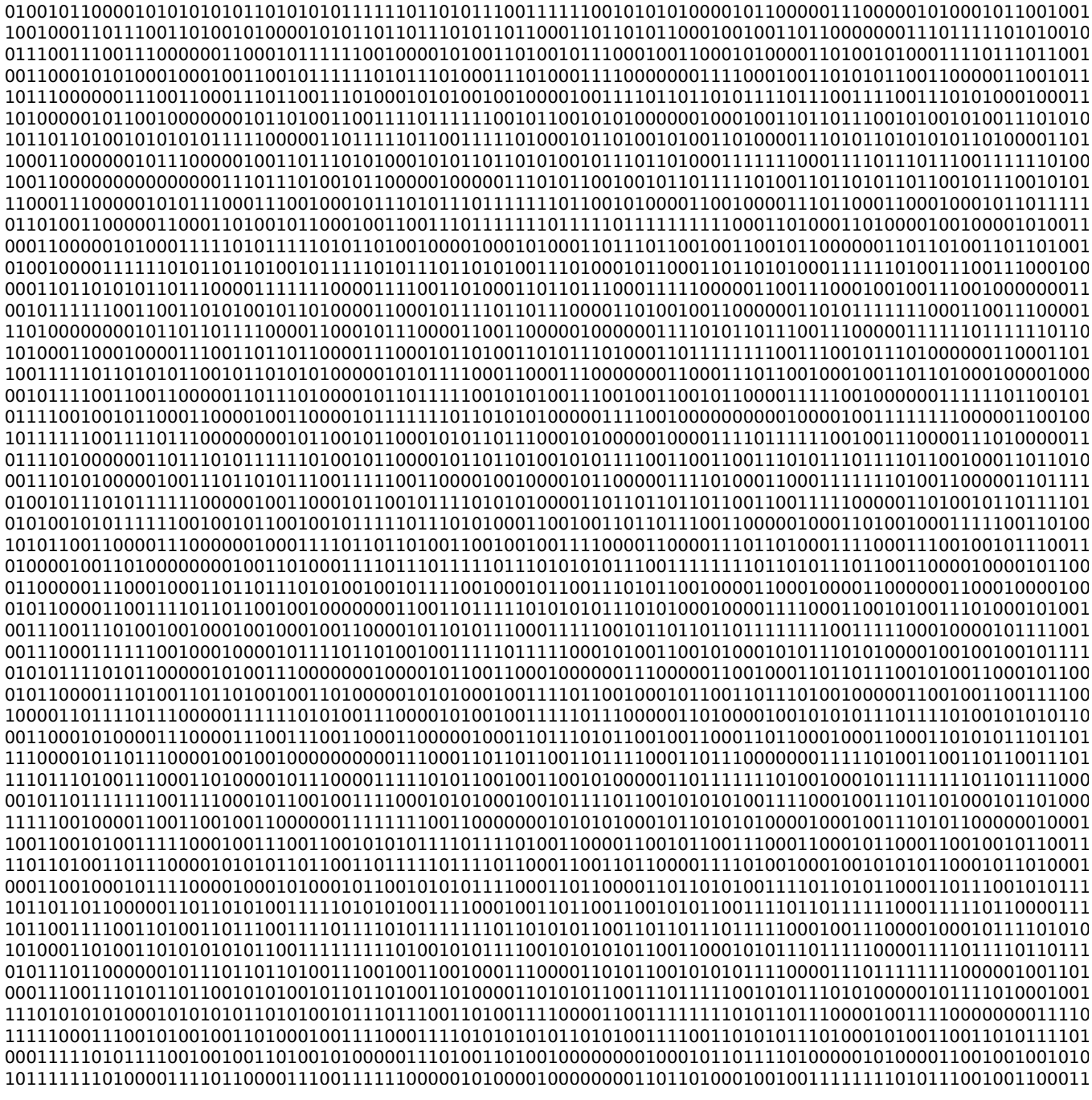
- Computação Quântica
  - Fenômenos Quânticos
  - Postulados
  - Trapped-ion
  - Algoritmos
  - Teletransporte Quântico
  - Teorema da não-clonagem
  - Fótons
  - Caminhadas Quânticas
- Computação Topológica
  - Nós
  - Ânions
- Computação Adiabática
  - Teorema Adiabático
  - Têmpera Quântica

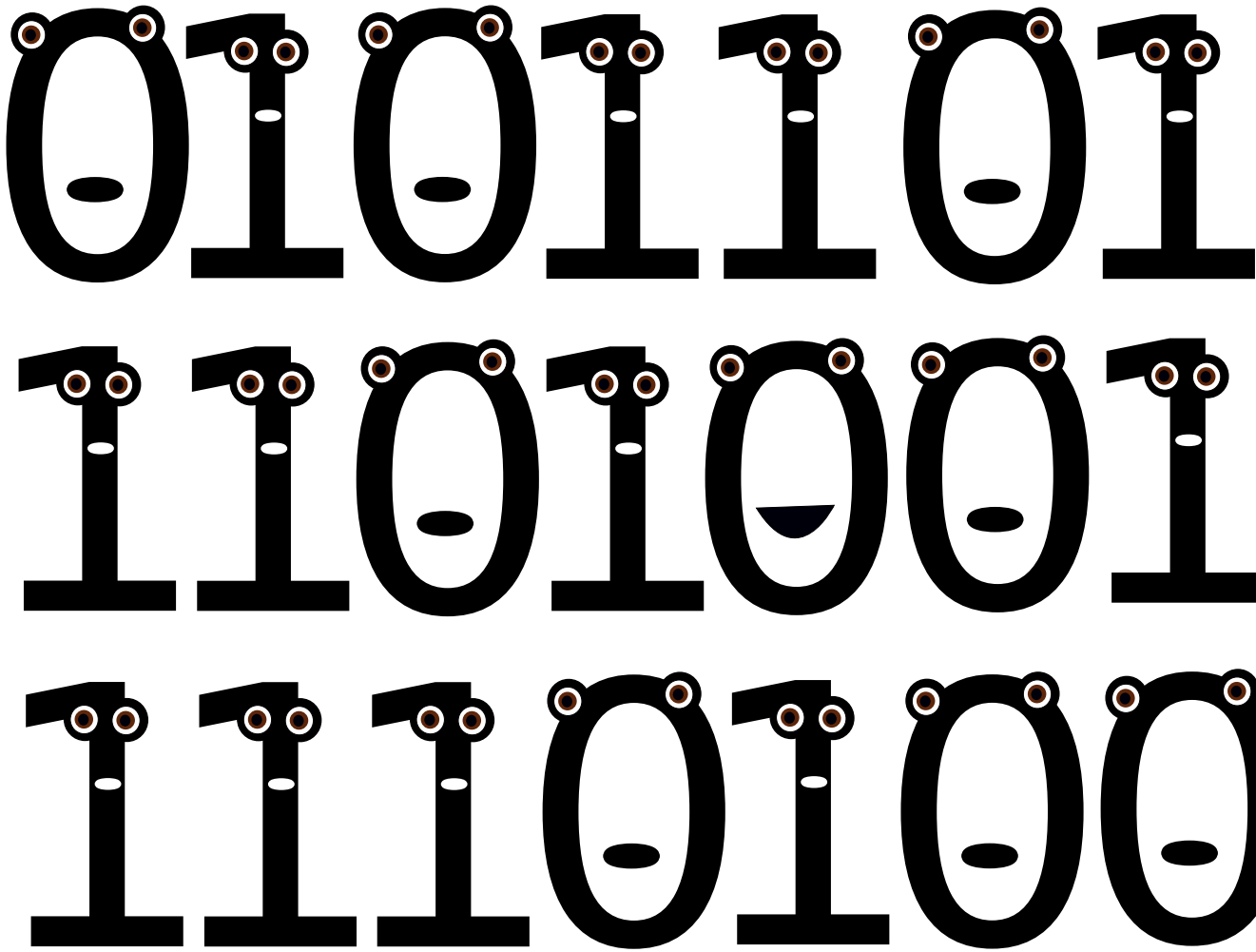
Parte III

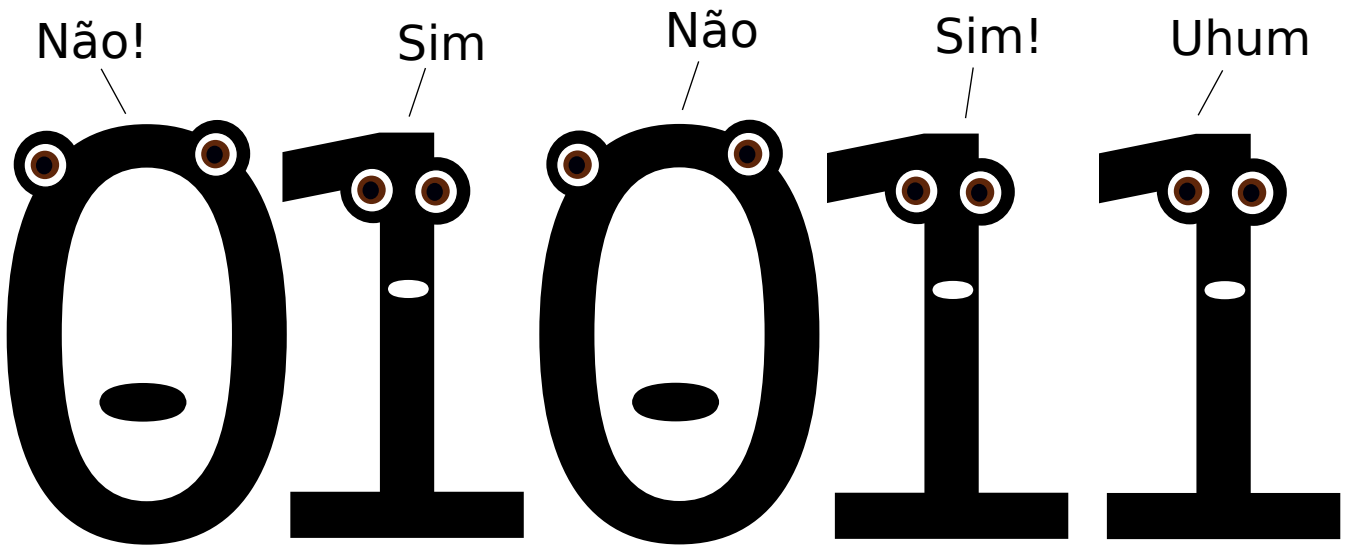
Fim?

- Saltos Quânticos
- Supremacia Quântica
- Material
- Bibliografia

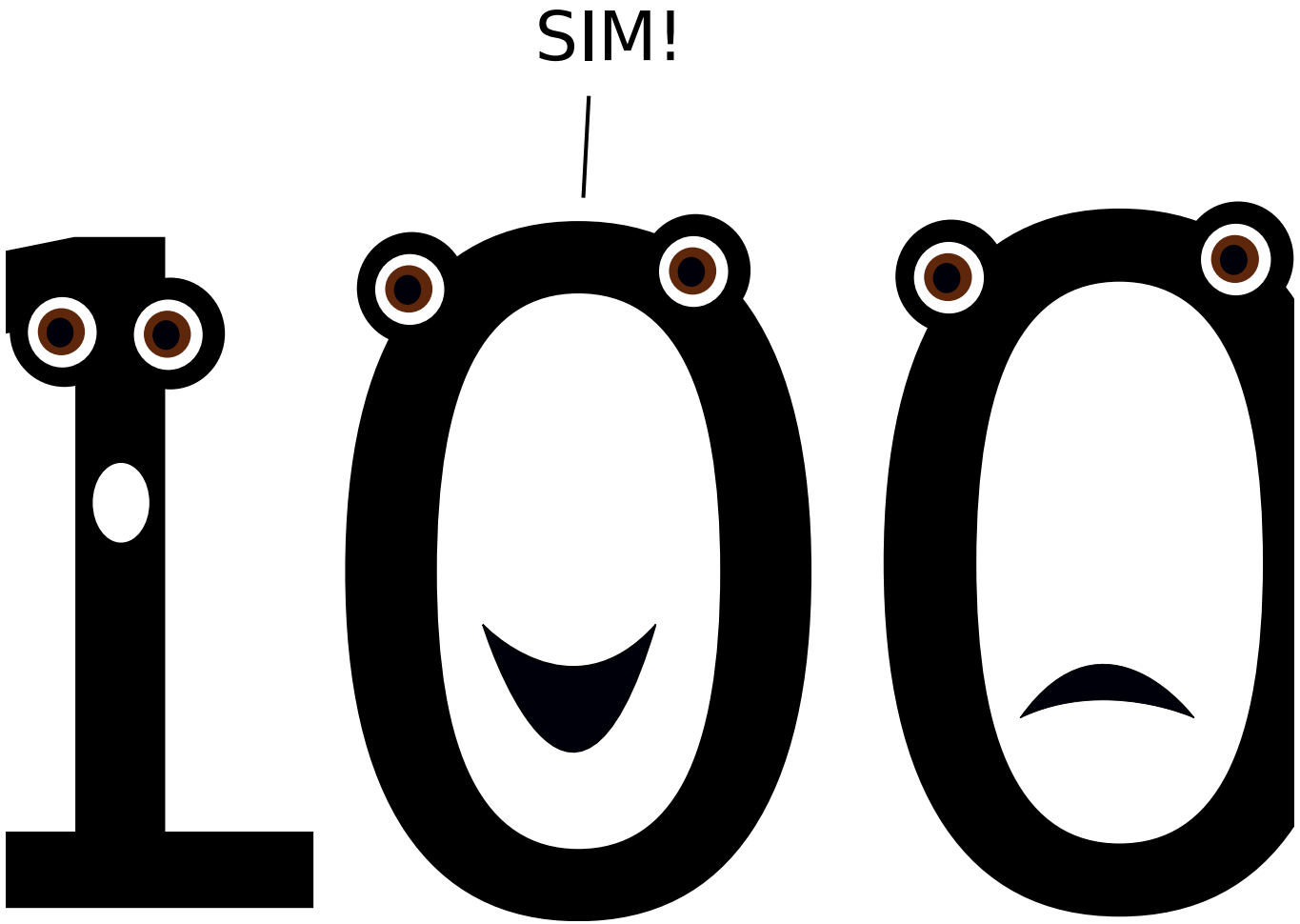
Computação Digital






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 Z_2
- Realizamos operações *Booleanas* com eles: $\neg$, $\wedge$, $\vee$, $\oplus$.
- Formam vetores em 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:

$a \vee (b \vee c) = (a \vee b) \vee c$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	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 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, $\delta : Q/\Omega \times \Gamma \to Q \times \Gamma \times \{\uparrow, \downarrow\}$

Alonzo Church

1903 - 1955

Alan Turing

1912 - 1954

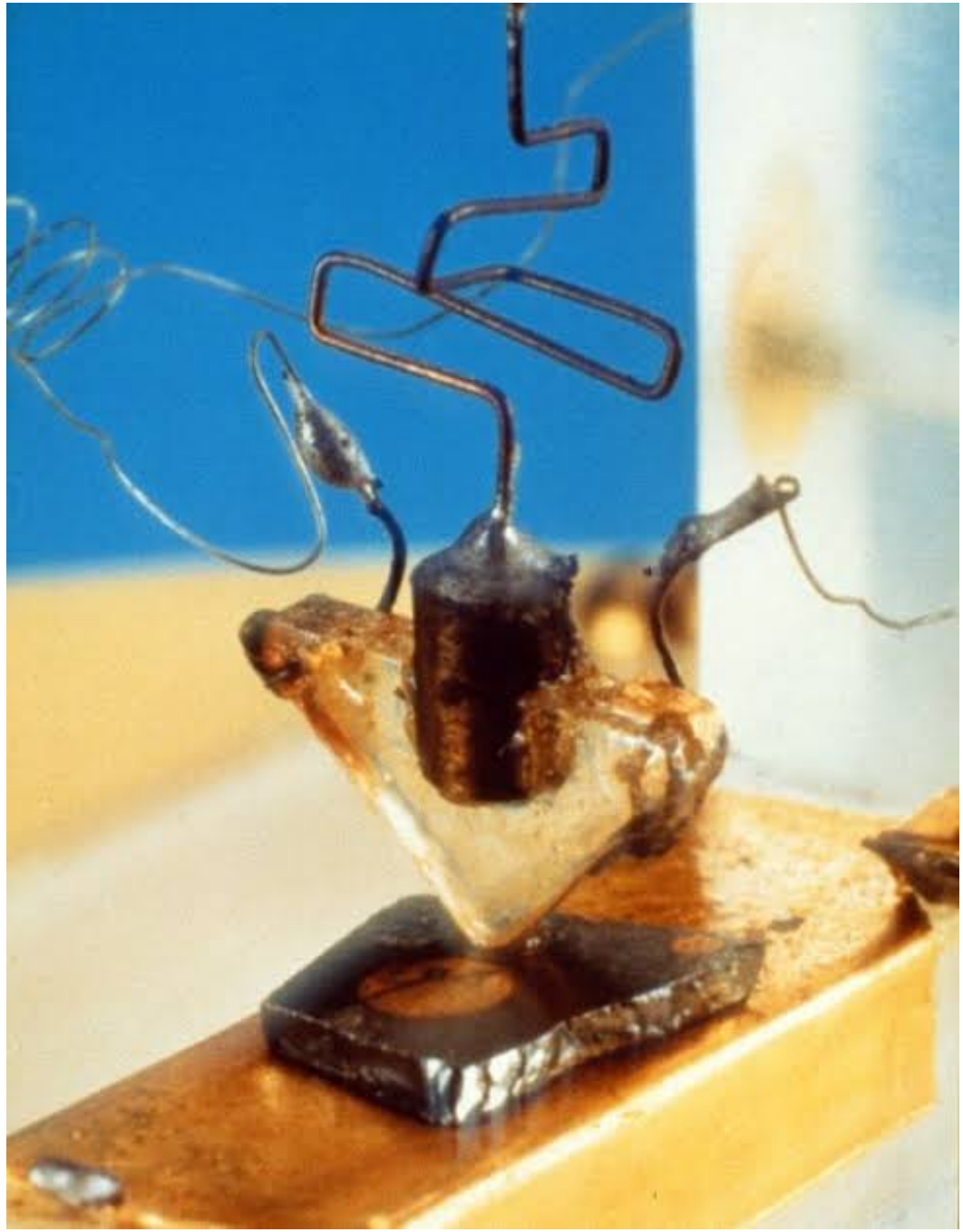
A Tese de Church-Turing

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

Alan Turing

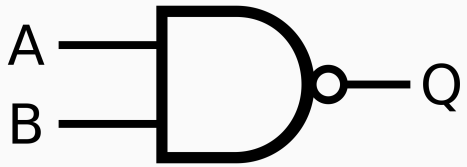
Definição. (***Complexidade Assintótica***)
Seja $f : X \subseteq \mathrm{R}_+ \to \mathrm{C}$ e $g : X \subseteq \mathrm{R}_+ \to \mathrm{R}_+$ dizemos que

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



Transistor

Portas Lógicas



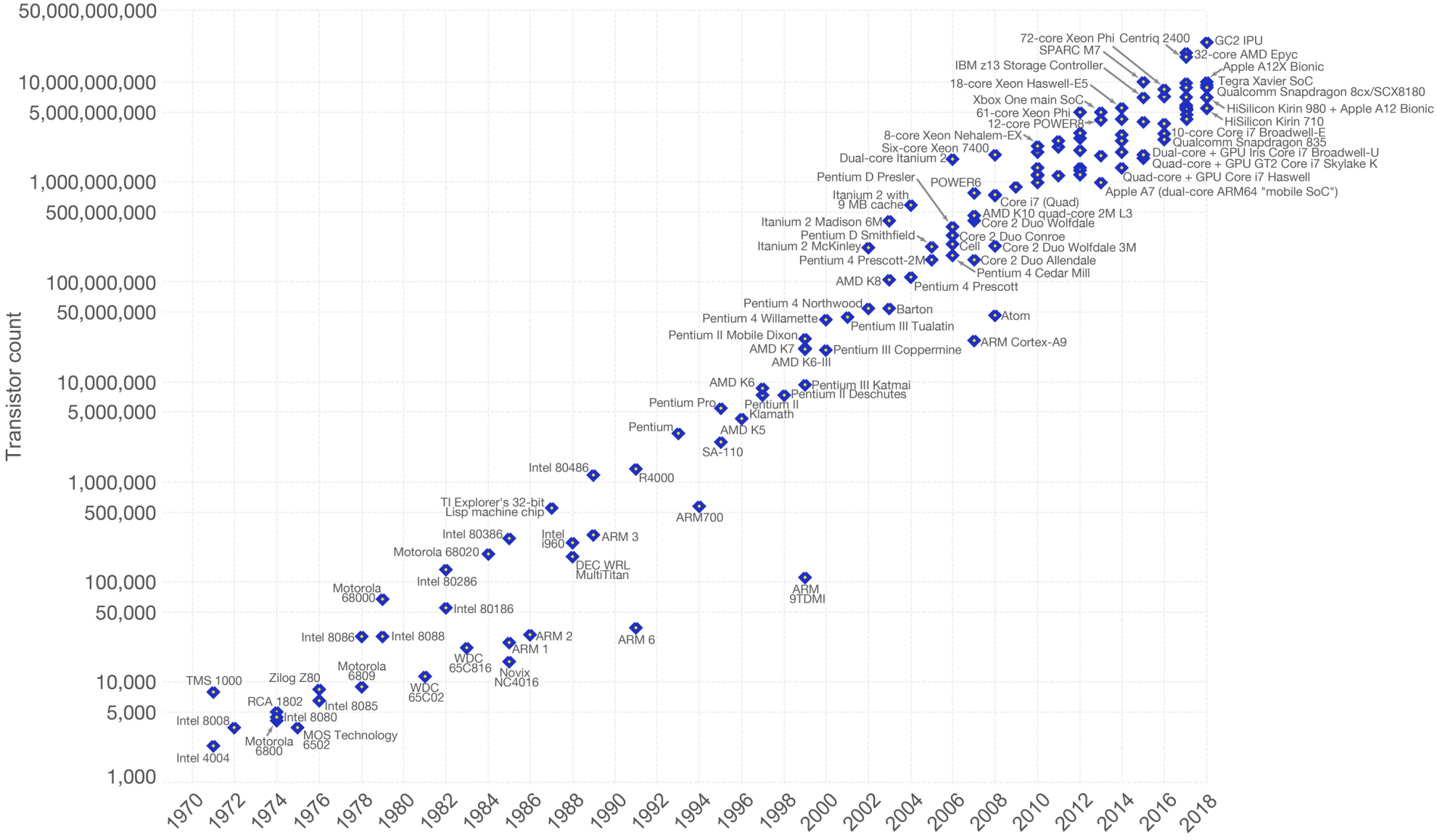
Arquitetura de Von Neuman

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.

Lei de Moore

Gordon Moore

Intel, 1965

Computação Quântica

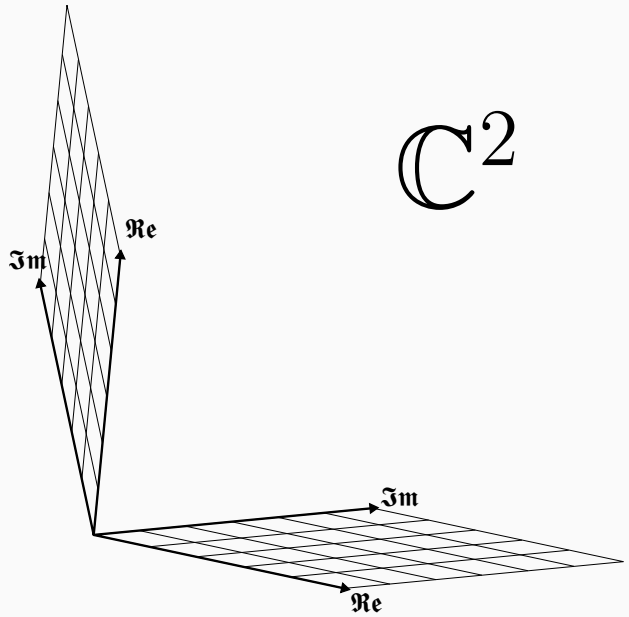
Fenômenos Quânticos

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.

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



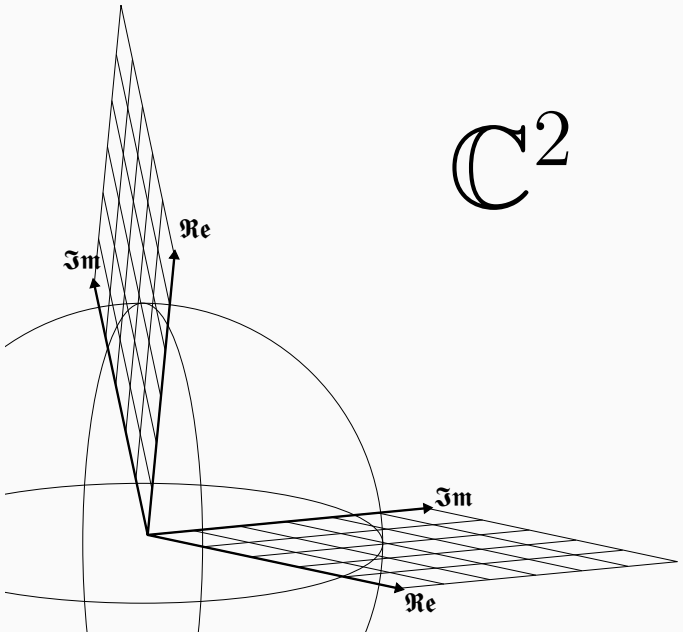
$$\mathbb{C}^2$$

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.

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

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



$$\mathbb{C}^2$$

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 :(

Postulados

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:

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

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:

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

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 $U^\dagger U = I$.

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

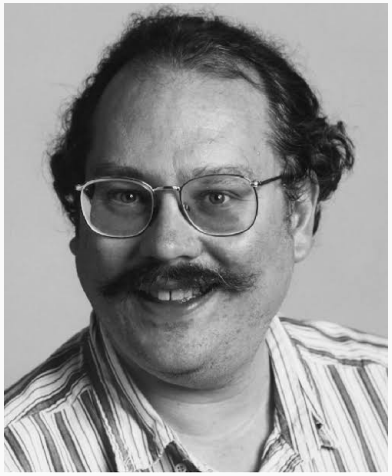
Oi íon aprisionado

Algoritmo de Grover

Lov Grover

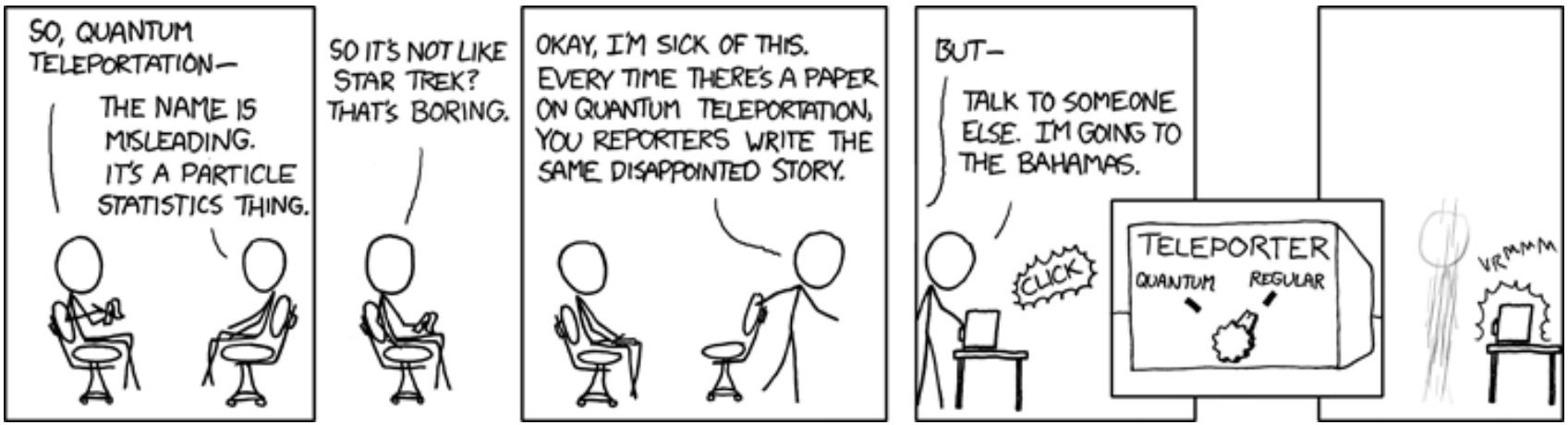
Bell Labs

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

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

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

Computação Topológica

Nós

Nós

Ânions

Ânions

Computação Adiabática

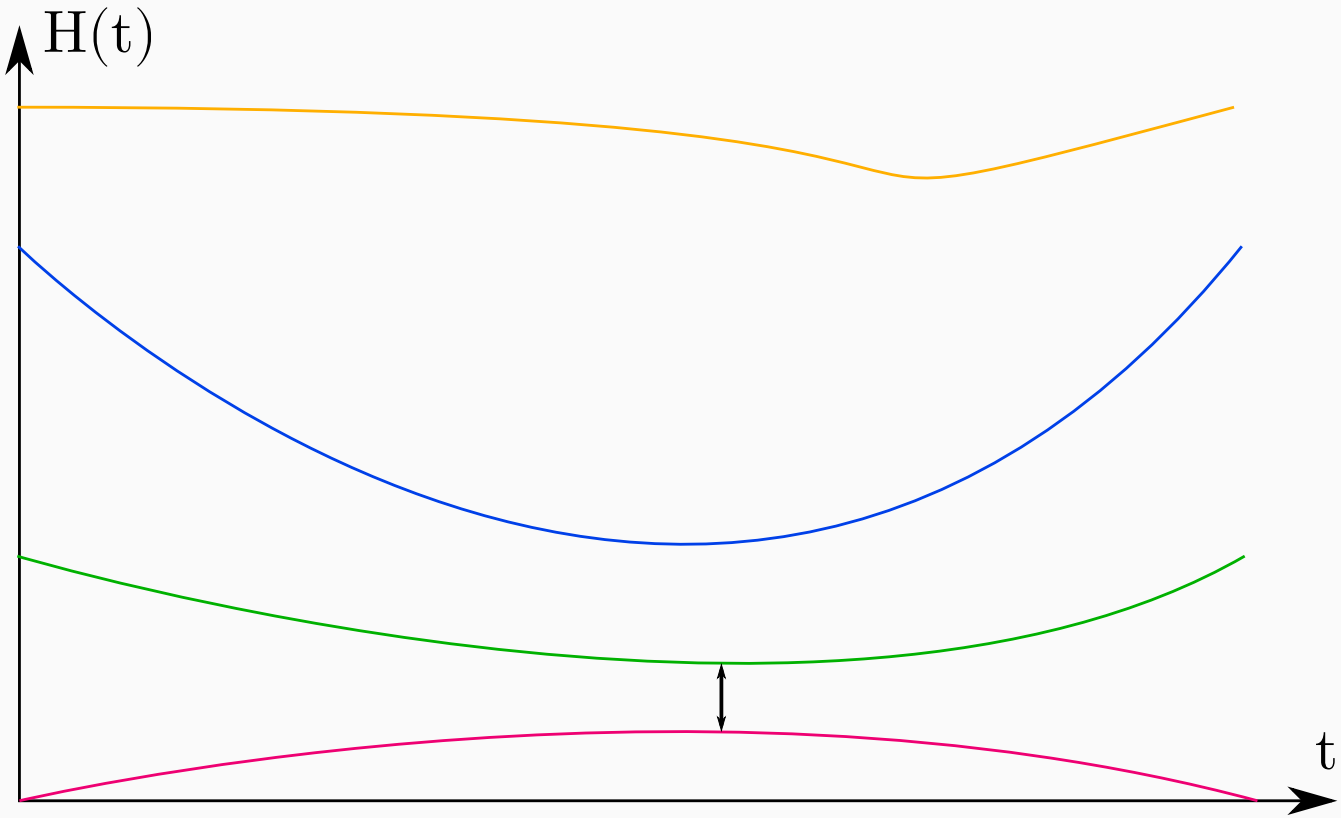
Equação de Pauli

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

Têmpera Quântica

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

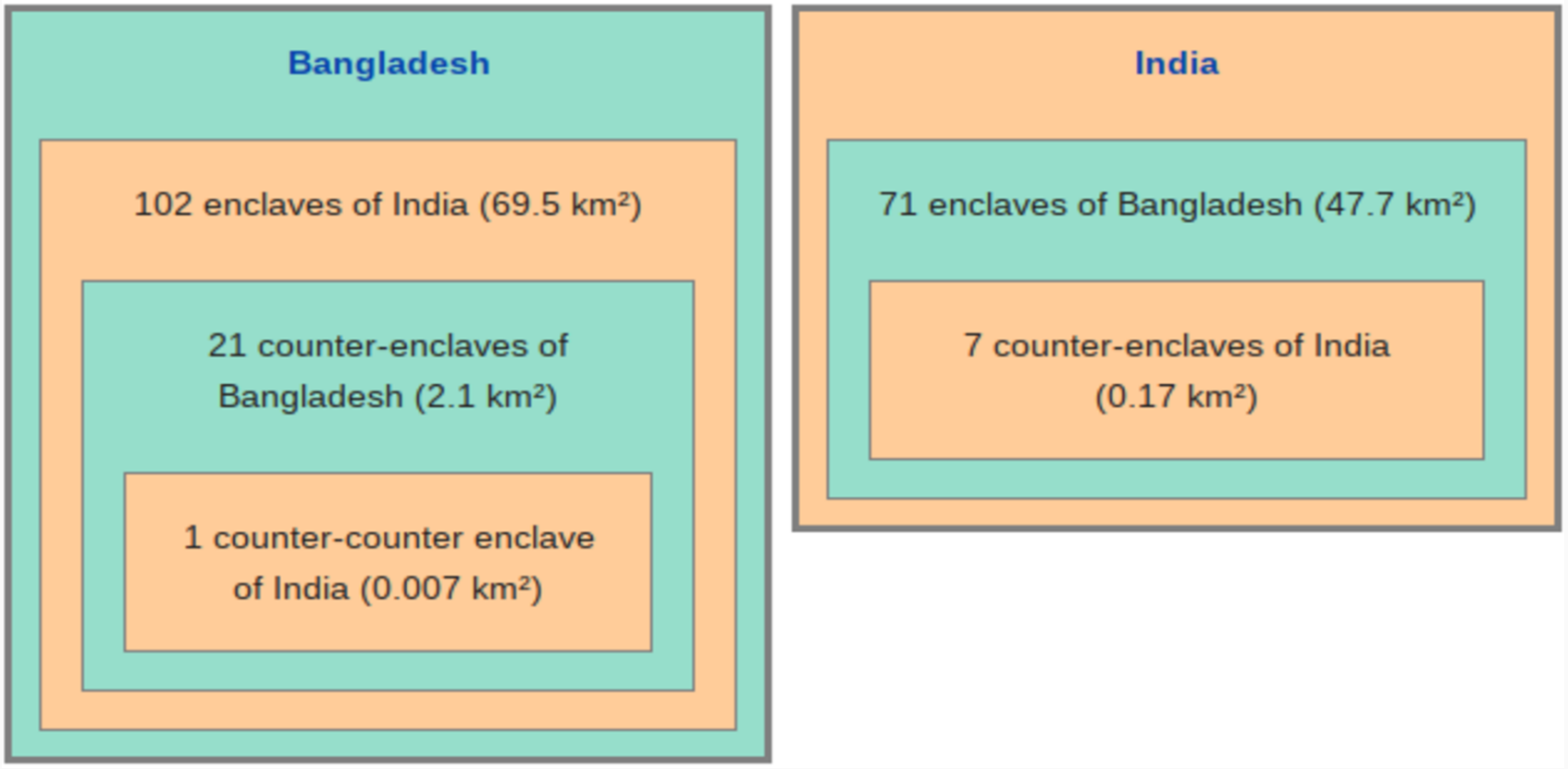
Têmpera Quântica

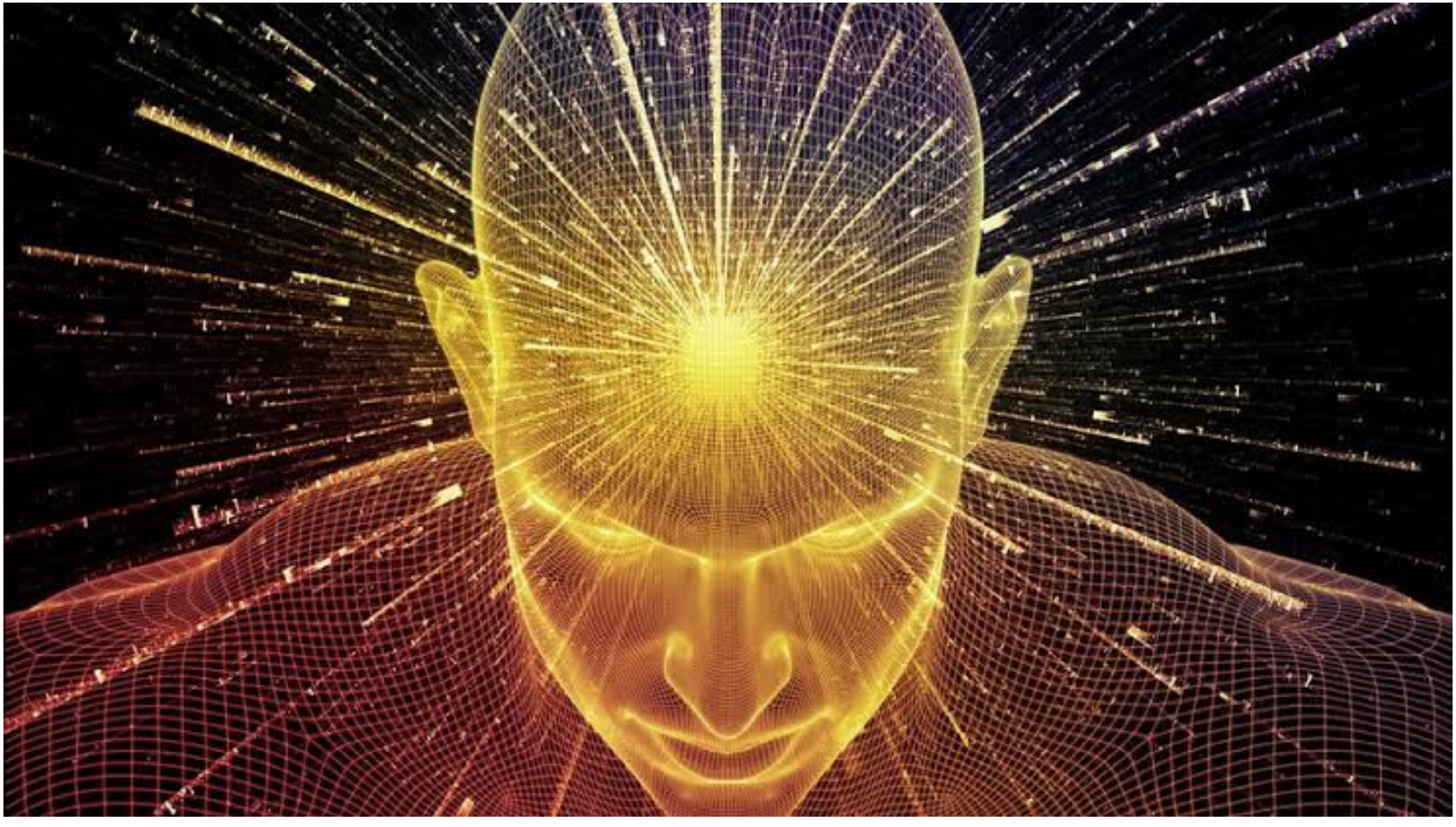


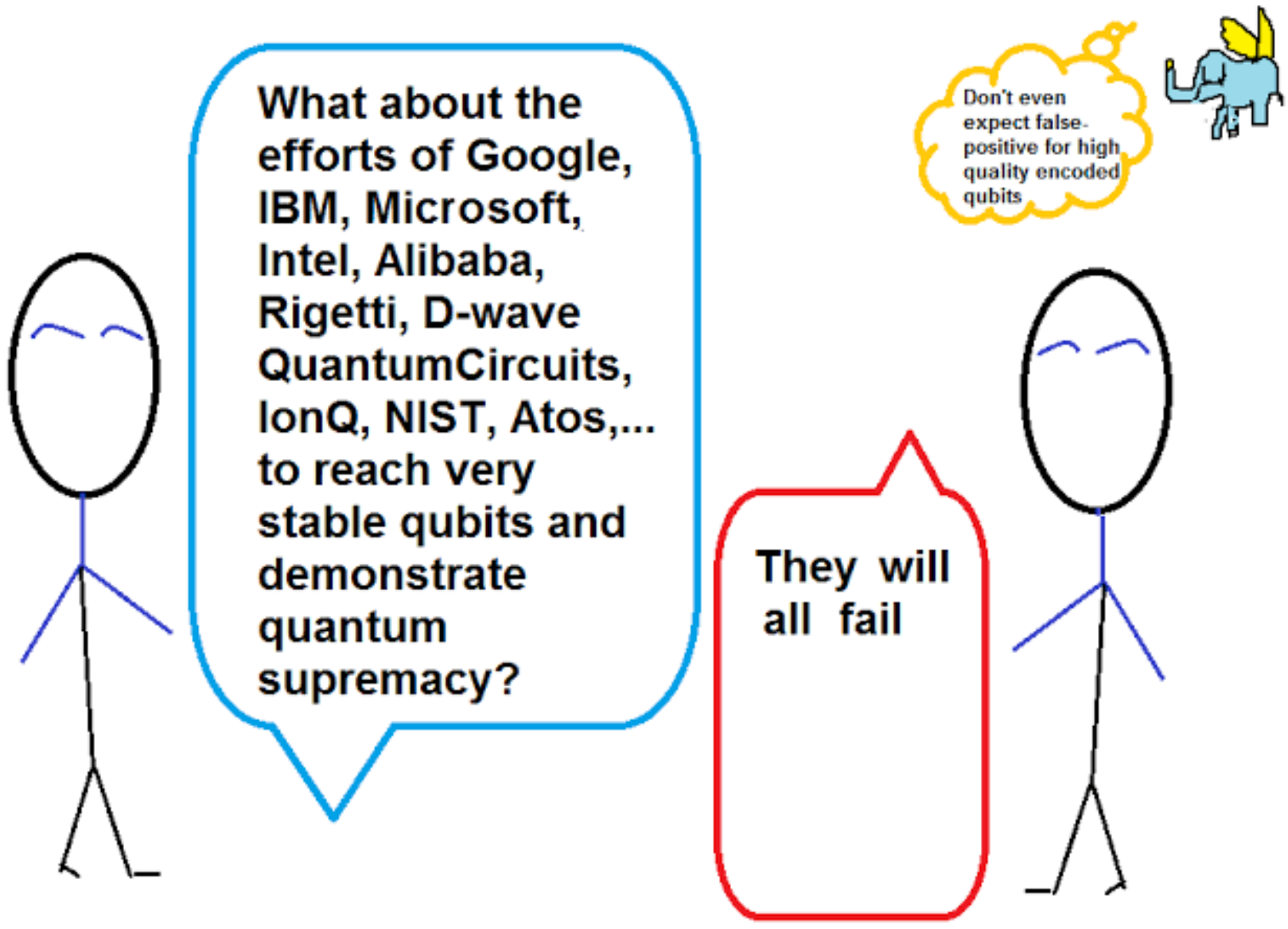
Fim?

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

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.

Supremacia Quântica

Material

- The Quantum Algorithm Zoo
- Quanta Magazine

Obrigado

Bibliografia

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