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
  - Saltos Quânticos

Fim?

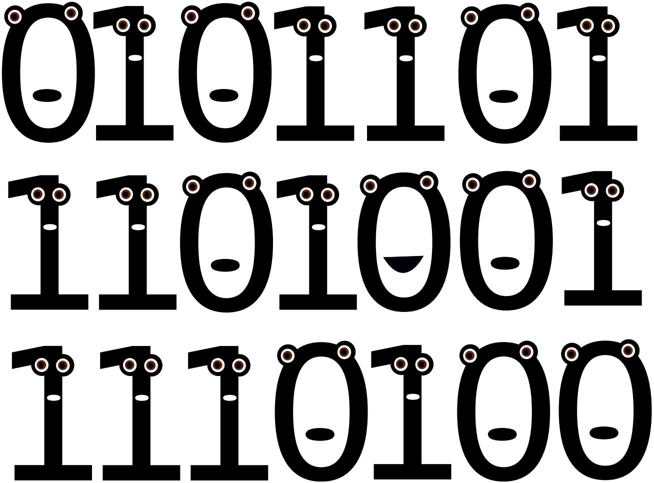
Supremacia Quântica

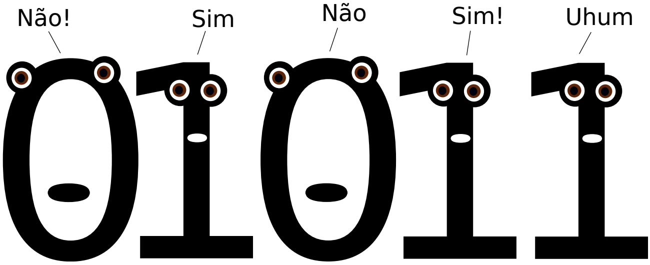
Material

Bibliografia

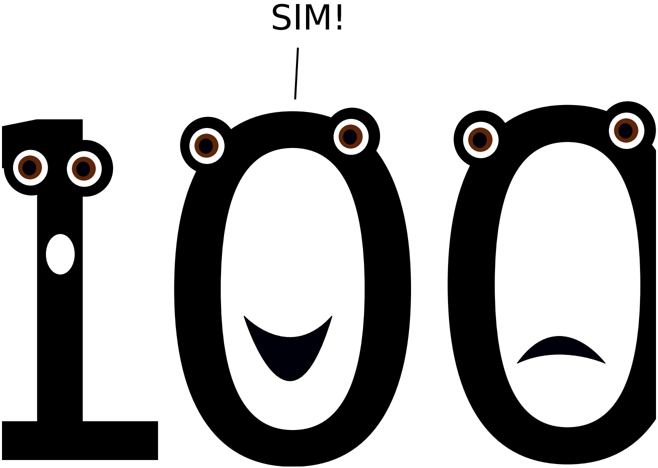
Computação Digital

0100101100001010101010110101010111111011010111001111110010101010000101100000111000001010001011001001
1001000110111001101001010000101011011011101011011000110110101100010010011011000000011101111101010010
0111001110011100000001100010111111001000010100110100101110001001100010100001101001010001111011101100 1
0011000101010001000100110010111111010111010001110100011110000000111100010011010101100110000011001011
1011100000011100110001110110011101000101010010010000100111101101101011110111001111001110101000100011
1010000001011001000000010110100110011110111111100101100101010000000100010011011011100101001010011101010
1011011010010101010111110000011011111011001111101000101101001010011010000111010110101010110100001101
1000110000000101110000001001101110101000101011011010100101110110100011111110001111011101110011111110100
1001100000000000000001110111010010110000010000011101011001001011011111010011011010110110010111001010 1
1100011100000010101110001110010001011101011101111111011001010000110010000111011000110001000101101111 1
0110100110000011000110100101100010011001110111111101111101111111111000110100011010000100100001010011
0001100000101000111110101111101011010010000100010100011011101100100110010110000001101101001101101001
0100100001111110101101101001011111010111011010100111010001011000110110101000111111010011100111000100
0001101101010110111000011111110000111100110100011011011100011111000000110011100010010011100100000001 1
0010111111001100110101001011010000110001011110110111000011010010011000000110101111111000110011100001
1101000000000101101101111000011000101110000110011000000100000011110101101110011100000111111011111101 10
1010001100010000111001101101100001110001011010011010111010001101111111100111001011101000000110001101
1001111101101010110010110101010000001010111100011000111000000001100011101100100010011011010001000001000
0010111100110011000000110111010000101101111100101010011100100110010110000111110010000000111111101100101
0111100100101100011000010011000010111111101101010100000111100100000000000100001001111111100000110010 0
1011111100111101110000000010110010110001010110111000101000000100001111011111100100111000011101000001 1
0111101000000110111010111111010010110000101101101001010111100110011001110101110111101100100011011010
0011101010000001001110110101110011111001100001001000010110000001111010001100011111111010011000001101111
0100101110101111111000000100110001011001011110101010000110110110110110011001111100000110100101101111101
0101001010111111100100101100100101111101110101000110010011011011100110000010001101001000111110011010 0
1010110011000011100000001000111101101101001100100100111100001100001110110100011110001110010010111001 1
0100001001101000000000100110100011110111011111011101010101110011111111011010111011001100001000010110 0
0110000001110001000110110111010100100101111001000101100111010110010000110001000011000000110001000010 0
0101100001100111101101100100100000000110011011111010101011101010001000011110001100101001110100010100 1
0011100111010010010001001000100110000101101011100011111001011011011011111111001111100010000101111001
0011100011111100100010000101111011010010011111011111000101001100101000101011101010000100100100101111
0101011110101100000010100111000000001000010110011000100000011100000110010001101101110010100110001011 00
0101100001110100110110100100110100000101010001001111011001000101100110111010010000011001001100111100
1000011011110111000001111110101001110000101001001111101110000011010000100101010111011110100101010110
0011000101000011100001110011100110001100000100011011101011001001100011011000100011000110101011101101
1110000101101110000100100100000000000111000110110110011011110001101110000000111110100110011011001110 1
1110111010011100011010000101110000111110101100100110010100000110111111101001000101111111110110111100 0
0010110111111100111100010110010011110001010100010010111101100101010100111100010011101101000101101000
1111100100001100110010011000000111111110011000000010101010001011010101000010001001110101100000010001
1001100101001111110001001110011001010101111011110100110000110010110011100011000101100011001001011001 1
1101101001101110000101010110110011011111011111011100011001101100001111010010001001010101100010110100 01
0001100100010111100001000101000101100101010111100011011000011011010100111101101011000101110010101111
1011011011000001101101010011111010101001111000100110110011001010110011110110111111000111110110000111
1011001111001101001101110011110111101011111111011010101100110110111011111100010011100001000101111010 10
1010001101001101010101011001111111110100101011110010101010110011000101011101111100001111011110110111
0101110110000001011101101101001110010011001000111000011010110010101011110000111011111111000001001101
0001110011101011011001010100101101101001101000011010101100111011111001010111010100000101111010001001
1110101010100010101010110101001011101110011010011110000110011111111010110111100001001111000000001111 0
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

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

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 ($q_0 \in Q$)
- 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

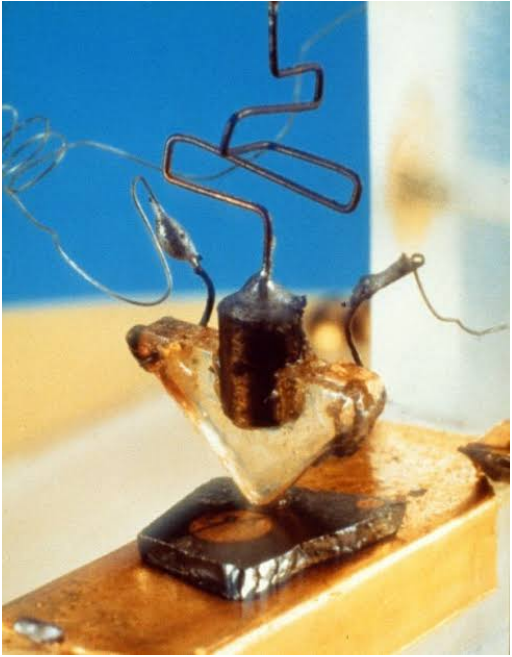
1912 - 1954

A Tese de Church-Turing

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

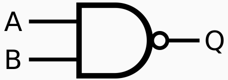
Definição. (***Complexidade Assintótica***)
Seja $f : X \subseteq \mathrm{R}_+ \to \mathrm{C}$ e $g(x) : X \subseteq \mathrm{R}_+ \to \mathrm{R}_+$ dizemos que

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



Transistor

Portas Lógicas



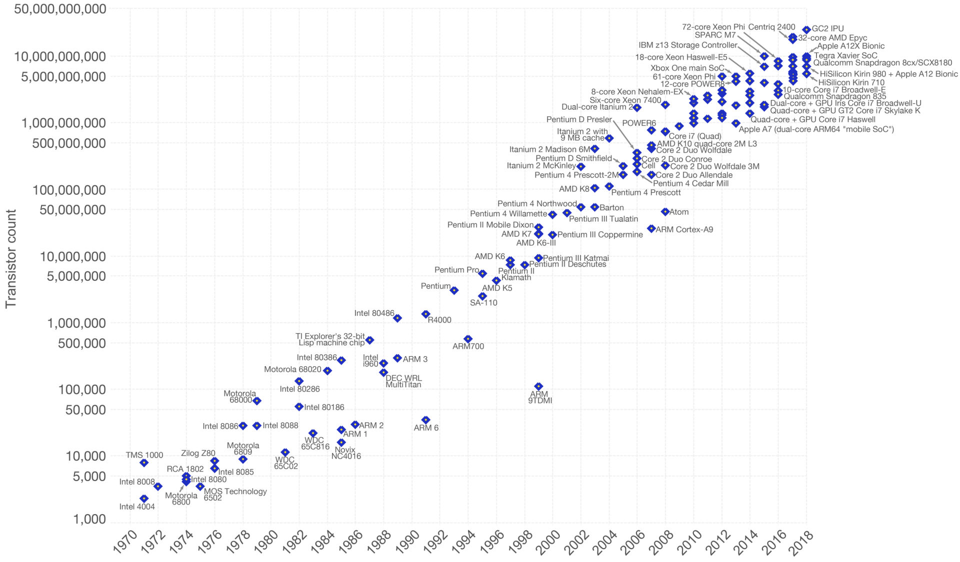
Arquitetura de Von Neuman

John Von
Neuman
1903 - 1957

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

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

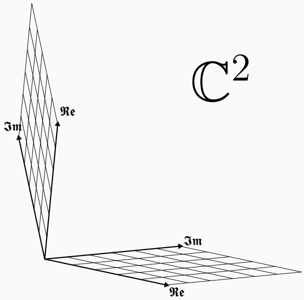
Computação Quântica

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.

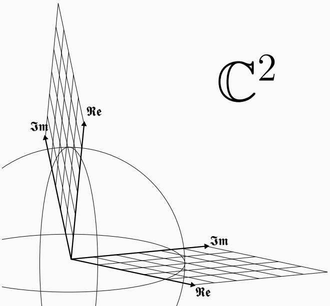
$$|\Psi\rangle \in \mathrm{C}^2 \qquad\qquad (\mathbf{x} \in \mathrm{C}^2)$$



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***)

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

Definição. (*Base Computacional*)
A *Base Computacional* é determinada pelos estados ortogonais $|0\rangle$ e $|1\rangle$, definidos por

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

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:

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

Postulados

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!

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.

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

Postulado. (*Medida*)

Trapped-ion

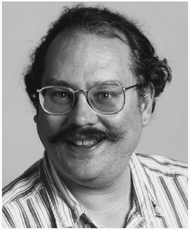
Oi íon aprisionado

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

Teorema da não-clonagem

Teorema. (***Não-Clonagem***)
Não é possível fazer uma cópia de um estado quântico.

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:

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

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

Por outro lado:

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

$\blacksquare$

Fótons

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

Caminhadas Quânticas

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

Computação Topológica

Nós

Nós

Ânions

Ânions

Computação Adiabática

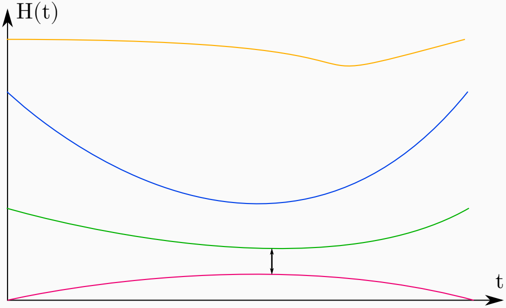
Equação de Pauli

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

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.