

Dia:

01/12

Às 09h



eu vou estar na INOVA 2021!

Trilha: Tecnologias inovadoras



O que é um computador quântico?

Gabriel de Moraes Coutinho

Confira a programação completa em:
www.inova.mg.gov.br

INOVA²⁰²¹
4ª SEMANA DE INOVAÇÃO

Realização



Correalização



1 | O que é a computação quântica?

2 | Para que serve?

3 | Desafios e perspectivas

1 | O que é a computação quântica?

2 | Para que serve?

3 | Desafios e perspectivas

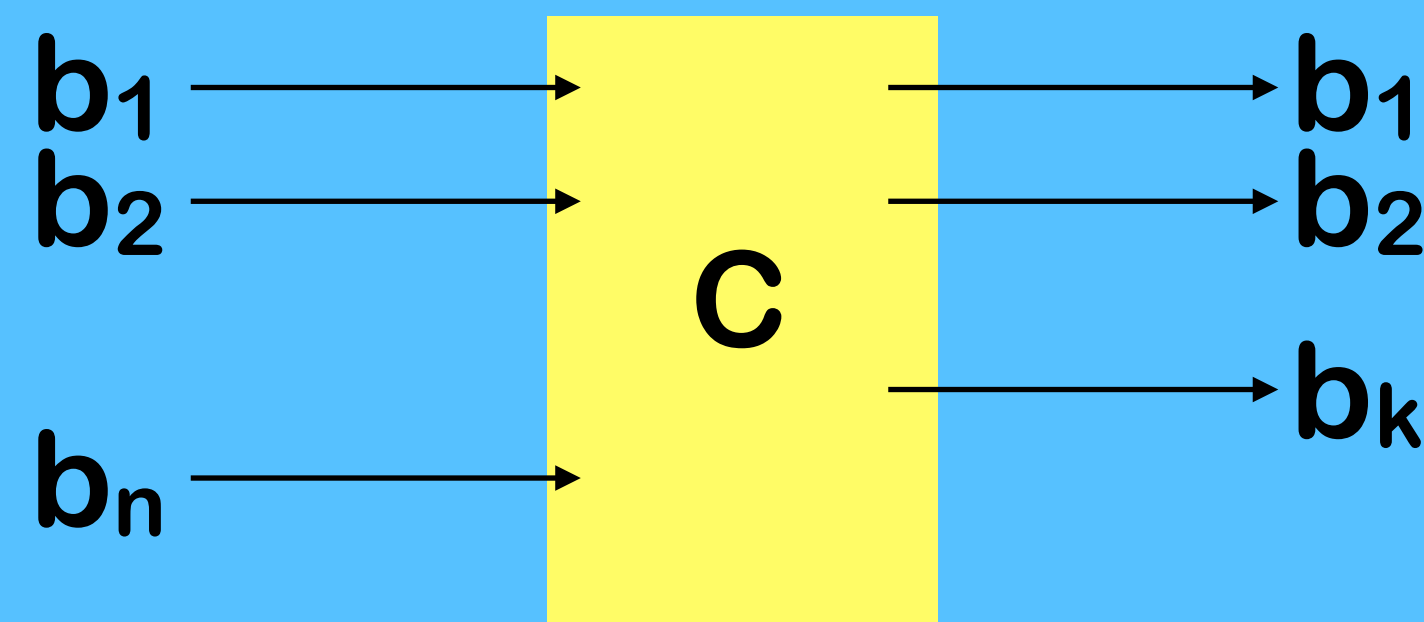
teoria da informação clássica...

bit

um bit corresponde ao conjunto $\{0,1\}$

pode estar no estado $\{0,1\}$ ou no estado $\{0,1\}$

circuito



teoria da informação quântica... aka álgebra linear

qubit

um qubit corresponde ao espaço vetorial $\mathbb{C}^2$

um estado de um qubit é qualquer subespaço de dimensão 1 — ou seja, uma “reta”

exemplos

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\alpha \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$\alpha \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\alpha \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

teoria da informação quântica... aka álgebra linear

qubit

um qubit corresponde ao espaço vetorial $\mathbb{C}^2$

um estado de um qubit é qualquer subespaço de dimensão 1 — ou seja, uma “reta”

exemplos

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\alpha \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$\alpha \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\alpha \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\alpha \begin{pmatrix} i \\ 0 \end{pmatrix}$$

$$\alpha \begin{pmatrix} i \\ -1 \end{pmatrix}$$

$$\alpha \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$\alpha \begin{pmatrix} 0 \\ 1 + i \end{pmatrix}$$

teoria da informação quântica... aka álgebra linear

qubit

um qubit corresponde ao espaço vetorial $\mathbb{C}^2$

um estado de um qubit é qualquer subespaço de dimensão 1 — ou seja, uma “reta”

na prática...

spin de um elétron

polarização de um fóton

<https://en.wikipedia.org/wiki/Qubit>

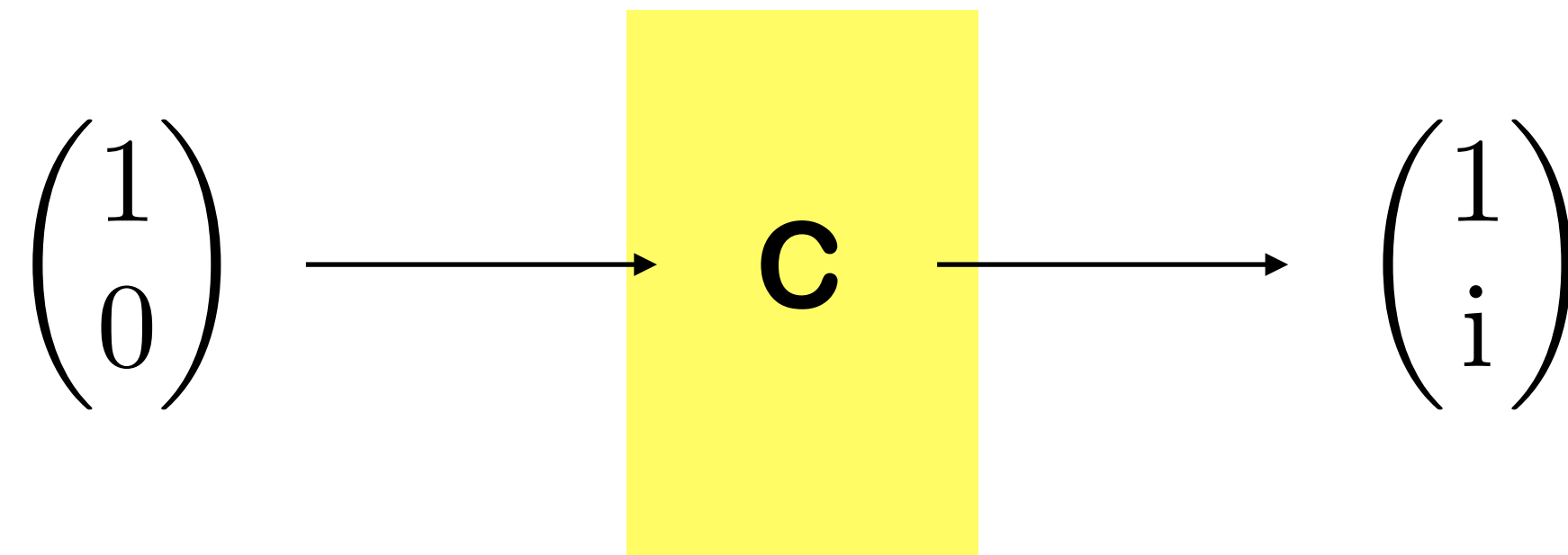
teoria da informação quântica... aka álgebra linear

circuito quântico

corresponde à multiplicação por certas matrizes

exemplos

$$\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ i \end{pmatrix}$$



teoria da informação quântica... aka álgebra linear

medições

um qubit só pode ser observado em dois estados

$$\alpha \begin{pmatrix} 1 \\ i \end{pmatrix} \quad \text{calcule} \quad \begin{cases} \frac{|1|^2}{|1|^2 + |i|^2} = \frac{1}{2} \\ \frac{|i|^2}{|1|^2 + |i|^2} = \frac{1}{2} \end{cases}$$

pode ser observado com probabilidade $\begin{cases} 1/2 \text{ em } \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1/2 \text{ em } \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{cases}$

teoria da informação quântica... aka álgebra linear

medições

um qubit só pode ser observado em dois estados

$$\alpha \begin{pmatrix} 1+i \\ -1 \end{pmatrix} \text{ calcule } \begin{cases} \frac{|1+i|^2}{|1+i|^2 + |-1|^2} = \frac{2}{3} \\ \frac{|-1|^2}{|1+i|^2 + |-1|^2} = \frac{1}{3} \end{cases}$$

pode ser observado com probabilidade $\begin{cases} 2/3 \text{ em } \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1/3 \text{ em } \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{cases}$

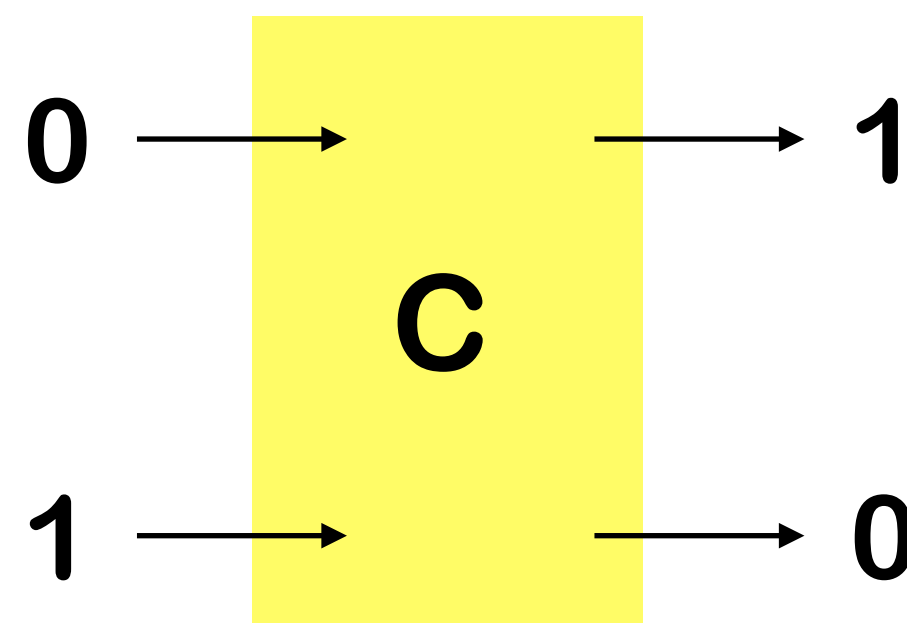
como simular computação clássica

faça a correspondência

$$\text{bit 0} \longrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ ou } |0\rangle$$

$$\text{bit 1} \longrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ ou } |1\rangle$$

circuito bit-flip



$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

mas as possibilidades vão muito além...

criando uma superposição...

$\begin{pmatrix} 1 \\ i \end{pmatrix}$ pode ser observado em $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

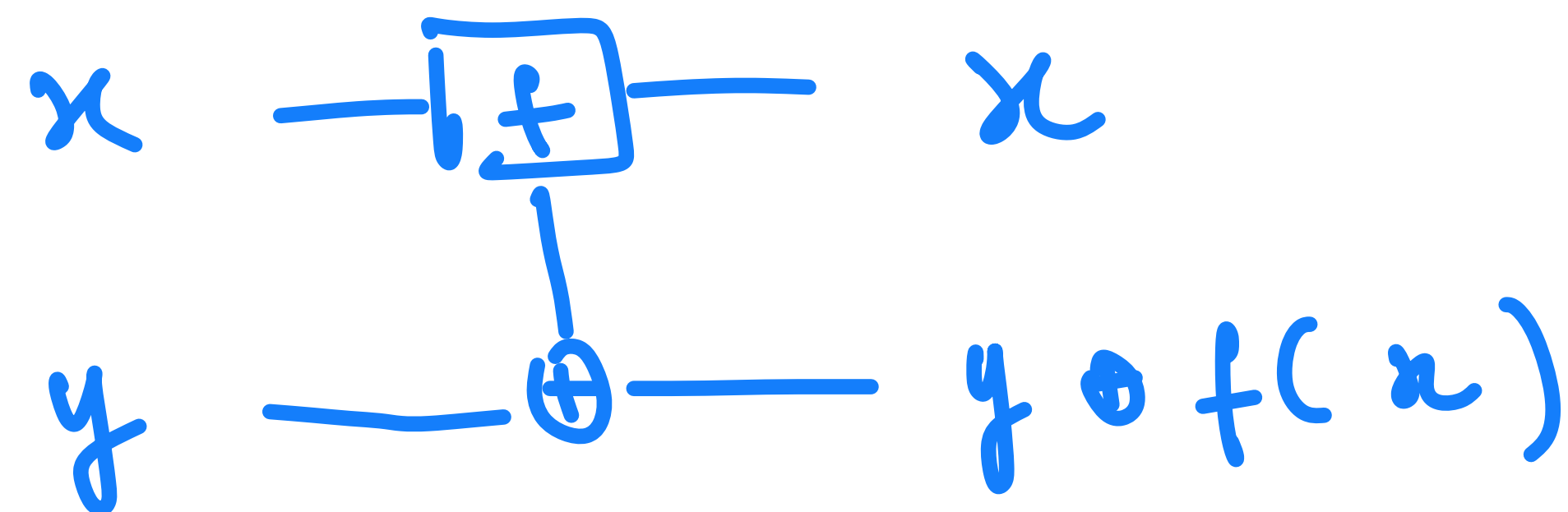
$$\begin{pmatrix} 1 \\ i \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} i \\ 1 \end{pmatrix}$$

**podemos realizar 2 bit flips
de uma vez só (mais ou menos)**

Função: $f: \{0,1\} \rightarrow \{0,1\}$

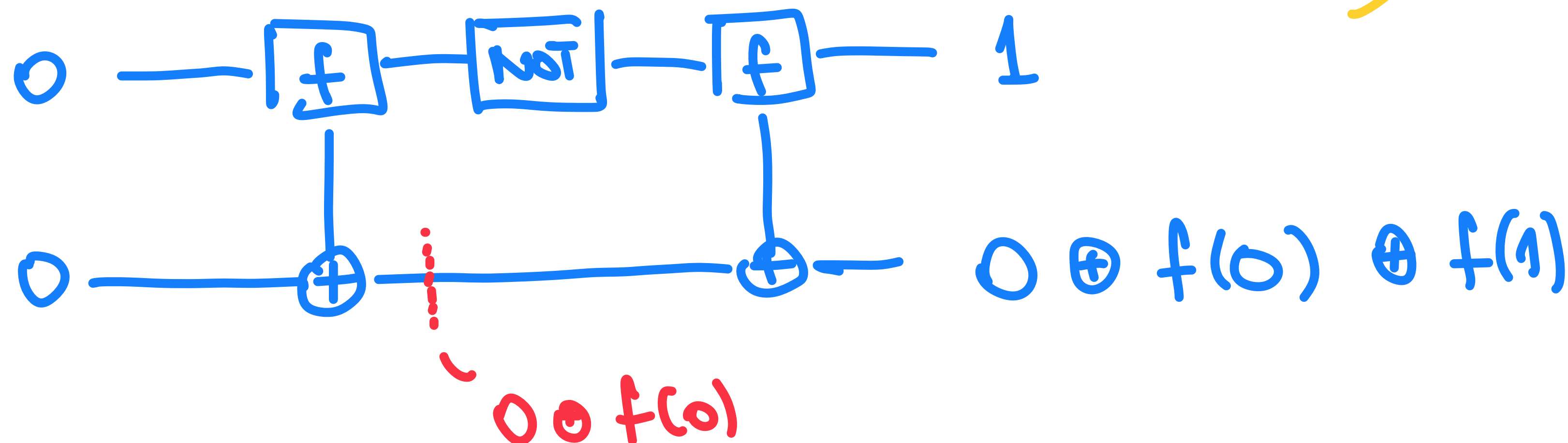
$x, y = 0$ ou 1

Circuito clássico:

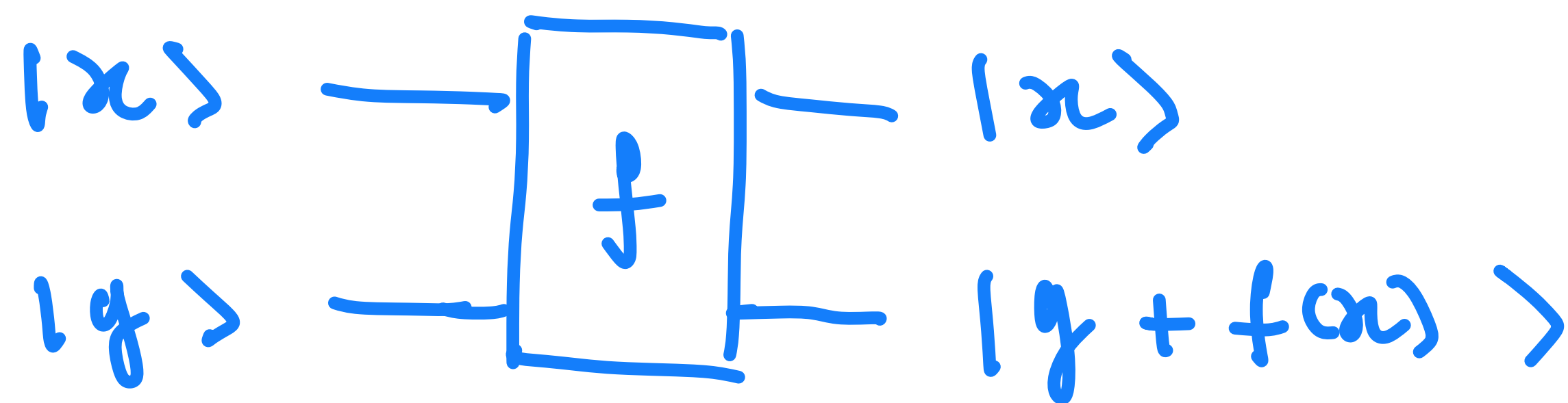


Como calcular $f(0) \oplus f(1)$?

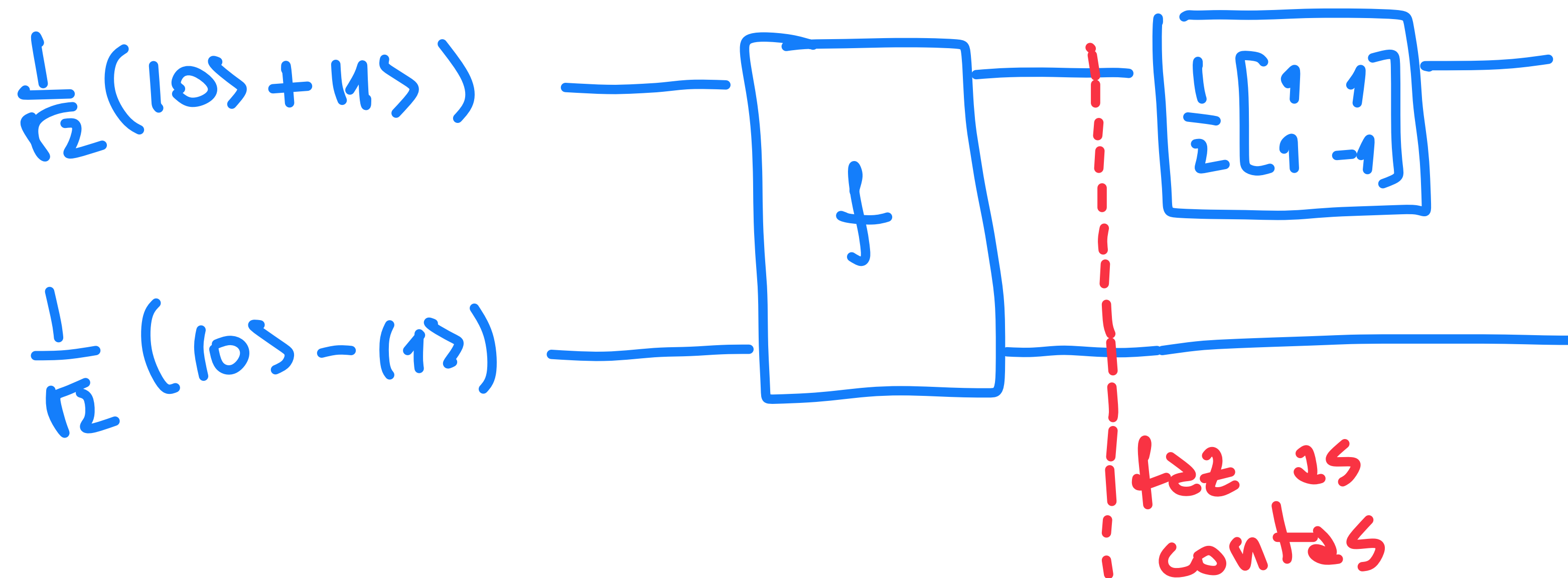
chamada
2 vezes.



Circuito quântico: $x=0$ ou 1 , então $|x\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
 $|0\rangle$ $|1\rangle$



Como calcular $f(0) \oplus f(1)$?



$\left\{ \begin{array}{l} |0\rangle \text{ se } f(0) \oplus f(1) = 0 \\ |1\rangle \text{ se } f(0) \oplus f(1) = 1 \end{array} \right.$

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

1 | O que é a computação quântica?

2 | Para que serve?

3 | Desafios e perspectivas

**simulação de sistemas
físicos**

“criptografia” quântica

**algoritmos quânticos
para tarefas difíceis**

simulação de sistemas físicos

possível em qualquer computador clássico

complexidade exponencial

muitos recursos são usados exclusivamente para isso

eficiente em qualquer computador quântico

“criptografia” quântica

**qualquer sistema de criptografia de chave pública
é baseado em hipóteses de complexidade não
demonstradas**

RSA: baseado na dificuldade de fatorar inteiros.

**apenas (alguns) sistemas de criptografia de
chave privada são comprovadamente seguros**

“criptografia” quântica

é possível codificar a chave privada como propriedades de um sistema quântico

qualquer observação altera o sistema

os usuários podem identificar a presença de intrusos no canal de comunicação

algoritmos quânticos

um computador quântico terá dois botões...

computador quântico

Shor

Grover

Shor

utiliza superposição para encontrar os fatores primos de um número

quebra o RSA (e qualquer sistema baseado em fatoração ou logaritmo discreto)

precisa de “muitos” qubits

difícil construir em alguns modelos de computação

Grover

problema: dada uma função $f : \{0,1\}^n \rightarrow \{0,1\}$,
achar a única entrada cujo valor é = 1.

classicamente, é preciso testar $2^n - 1$ vezes

o algoritmo de Grover tem complexidade $O(2^{n/2})$

para qualquer!! função f

algoritmos quânticos

computador quântico

Shor

ganho exponencial para
fatoração e logaritmo discreto

Grover

ganho quadrático para
qualquer problema

algoritmos para resolver:

sistemas lineares, com aplicação em aprendizado de máquina

otimização adiabática, com aplicação em redes neurais

1 | O que é a computação quântica?

2 | Para que serve?

3 | Desafios e perspectivas

**decoerência
e correção de erros**

escalabilidade

inicialização arbitrárias

**implementação de
qualquer porta**

leitura / medições

decoerência - o maior obstáculo

interação com o meio faz com que qubits colapsem e percam seus estados

em alguns modelos, os qubits resistem apenas por poucos micro-segundos

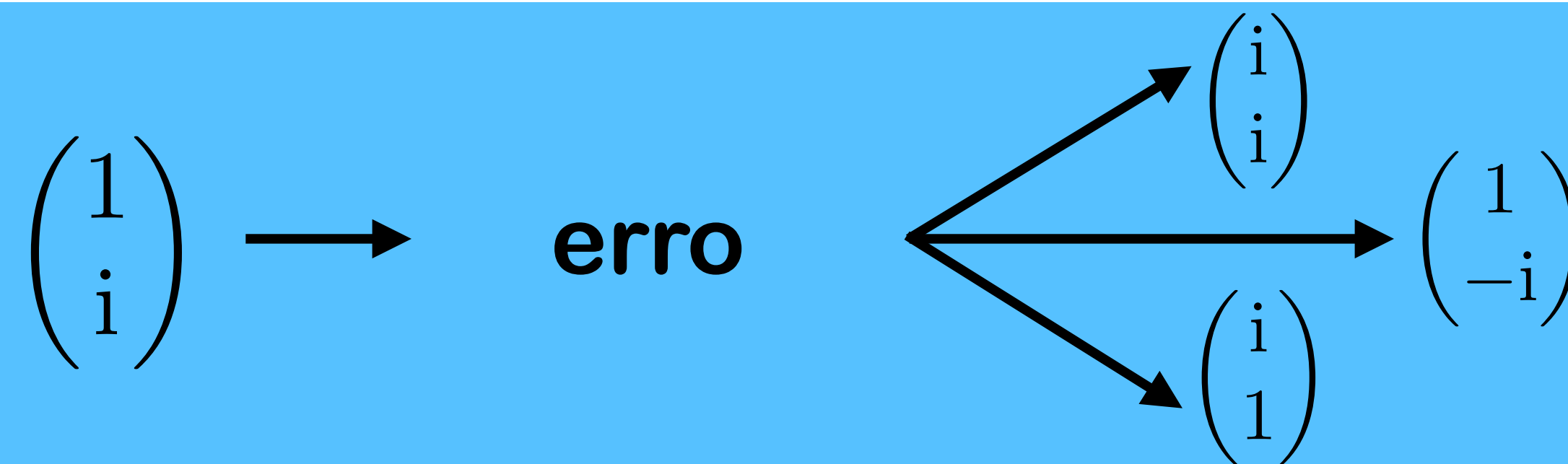
em outros, precisam ser resfriados a temperaturas da ordem de micro-Kelvins

correção de erros

classicamente...

$0 \longrightarrow 000 \xrightarrow{\text{erro}} \begin{matrix} 100 \\ 010 \\ 001 \end{matrix}$

$1 \longrightarrow 111 \xrightarrow{\text{erro}} \begin{matrix} 011 \\ 101 \\ 110 \end{matrix}$

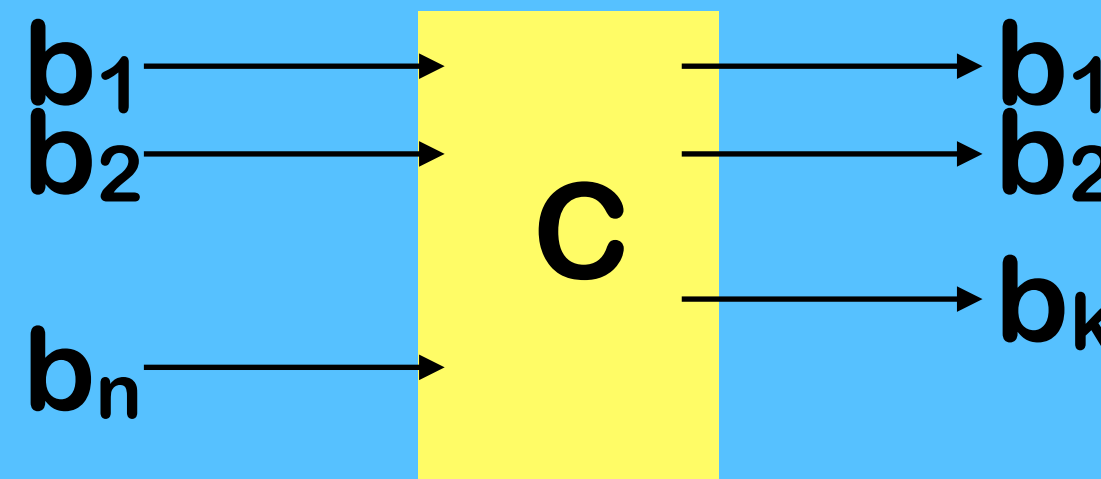


códigos corretores quânticos precisam de > 9 vezes o número de qubits utilizados

escalabilidade

a montagem do circuito impede que certas “ligações” sejam feitas

circuito



o computador da IBM não permite que certas portas “quânticas” usem mais do que 5 qubits

operações arbitrárias

classicamente, qualquer circuito pode ser construído com

AND ; OR & NOT

em computação quântica, também temos um conjunto universal de portas

mas o problema de construção / minimização de circuitos é muito mais difícil

RSA-576	174	576	US\$10,000	December 3, 2003	Jens Franke <i>et al.</i> , University of Bonn
RSA-180 ^[b]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University ^[11]
RSA-190 ^[b]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	US\$20,000	November 2, 2005	Jens Franke <i>et al.</i> , University of Bonn
RSA-200 ^[b] ?	200	663		May 9, 2005	Jens Franke <i>et al.</i> , University of Bonn
RSA-210 ^[b]	210	696		September 26, 2013 ^[12]	Ryan Propper
RSA-704 ^[b]	212	704	US\$30,000	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA-220 ^[b]	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA-230 ^[b]	230	762		August 15, 2018	Samuel S. Gross, Noblis, Inc. 
RSA-232 ^[b]	232	768		February 17, 2020 ^[13]	N. L. Zamarashkin, D. A. Zheltkov and S. A. Matveev.
RSA-768 ^[b]	232	768	US\$50,000	December 12, 2009	Thorsten Kleinjung <i>et al.</i> ^[14]
RSA-240 ^[b]	240	795		Dec 2, 2019 ^[15]	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA-250 ^[b]	250	829		Feb 28, 2020 ^[16]	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA-260	260	862			
RSA-270	270	895			
RSA-896	270	896	US\$75,000 ^[d]		
RSA-280	280	928			
RSA-290	290	962			
RSA-300	300	995			
RSA-309	309	1024			
RSA-1024	309	1024	US\$100,000 ^[d]		
RSA-310	310	1028			
RSA-320	320	1061			
RSA-330	330	1094			
RSA-340	340	1128			
RSA-350	350	1161			

QUANTUM?

perspectivas

**os mais otimistas ainda falam em 10 anos para
aplicações de impacto**

perspectivas

**os mais otimistas ainda falam em 10 anos para
aplicações de impacto**

mas há 5 anos eles falavam em 30...

perspectivas

**os mais otimistas ainda falam em 10 anos para
aplicações de impacto**

mas há 5 anos eles falavam em 30...

tem gente que não acredita

perspectivas

os mais otimistas ainda falam em 10 anos para aplicações de impacto

mas há 5 anos eles falavam em 30...

tem gente que não acredita (Gil Kalai e outros)

e muita gente que acredita:

**IBM, Google, D-Wave, Microsoft, USA!, China!!!,
venture capitalists, universidades, bancos, etc.**

perspectivas

1959 | Feynman descreve a possibilidade

1984 | Esquema de criptografia quântica

1994 | Algoritmo de Shor

2001 | Fatoração de 15 usando 7 qubits (péssima arquitetura)

2009 | 2 qubits usando matéria condensada em Yale

2011 | Computador da D-Wave com 128 qubits - polêmico!

2011 | Fatoração de 143 usando 4 qubits

2012 | Breakthroughs na IBM usando supercondutividade

2012 | Multi-universidades: 2 qubits a temperatura ambiente

2012 | Primeira startup

2013 | Google entra no jogo

2014 | NSA investindo \$80 milhões para quebrar o RSA

2016 | Computador da IBM disponível para mim e para você

2017 - 2020 | muita coisa nova acontecendo todo dia

perspectivas

2017 | D-Wave (quantum annealer), com 2000 qubits

2017 | Computador da IBM com 17 (e depois 50) qubits, duram pouco

2017 | Microsoft desenvolve a Q Sharp

2018 | Oxford: nova técnica para encapsular qubits

2018 | Google: 72-qubit quantum chip

2018 | USA: National Quantum Initiative Act

2019 | Google anuncia supremacia quântica (polêmica com IBM)

2020 | Qubits de estado sólido coerentes 10.000 vezes mais longo

2020 | Processador quantico sílica: 1.5 Kelvin

2020 | Supremacia quântica na China: 76 qubits (100 trilhões)

2021 | China: rede de comunicação + supremacia com fótons

2021 | Japão: comunicação quantica 600km

2021 | Harvard: simulador operando com 256 qubits

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication

perguntas?

Gabriel Coutinho | gabriel@dcc.ufmg.br