Computação Quântica

Rodrigo Minetto

Instituto de Computação - Unicamp

ra049243@ic.unicamp.br

Apresentação

- Introdução
- Conceitos
- Tecnologias para Construção de Computadores Quânticos
- Algoritmos Quânticos
- Computador Quântico x Computador Clássico
- Conclusões

Introdução

↪ Problemas de propagação de ondas em antenas de telefonia móvel, seqüenciamento genético, previsão de clima e renderização de filmes e imagens pertencem a diferentes áreas da ciência e têm em comum a complexidade de cálculos e necessidade de supercomputadores para resolvê-los.

↪ Computadores quânticos, dispositivos que usam as leis da mecânica quântica para processar informações, provocam na atualidade grande entusiasmo por suas potenciais capacidades de processamento, devido ao paralelismo quântico, matematicamente demonstradas.

↪ Este estudo tem por objetivo dar uma visão geral desse novo paradigma de computação: a computação quântica.

Conceitos

↪ A mecânica clássica, não se aplica aos movimentos de objetos muito pequenos. Surge então a teoria da mecânica quântica que descreve o comportamento da matéria em seus componentes básicos tal como átomos, moléculas e núcleos.

↪ Determinar o estado de um sistema quântico corresponde a especificar probabilidades de encontrar determinados valores para as grandezas fisícas mensuráveis.

↪ Existe uma incerteza intrínsica (incerteza de Heisenberg) que descreve matematicamente o sistema como uma superposição coerente de estados distintos, esta incerterza diz que não se pode medir com segurança as propriedades básicas do comportamento subatômico.

Conceitos

$\hookrightarrow$ A estrutura básica de informação na computação clássica é o bit, a estrutura análoga na computação quântica é o $quantum\ bit$ ou $bit\ quântico$, também conhecido com $qubit$.

Um qutib é um estado quântico $|\psi\rangle$ da forma

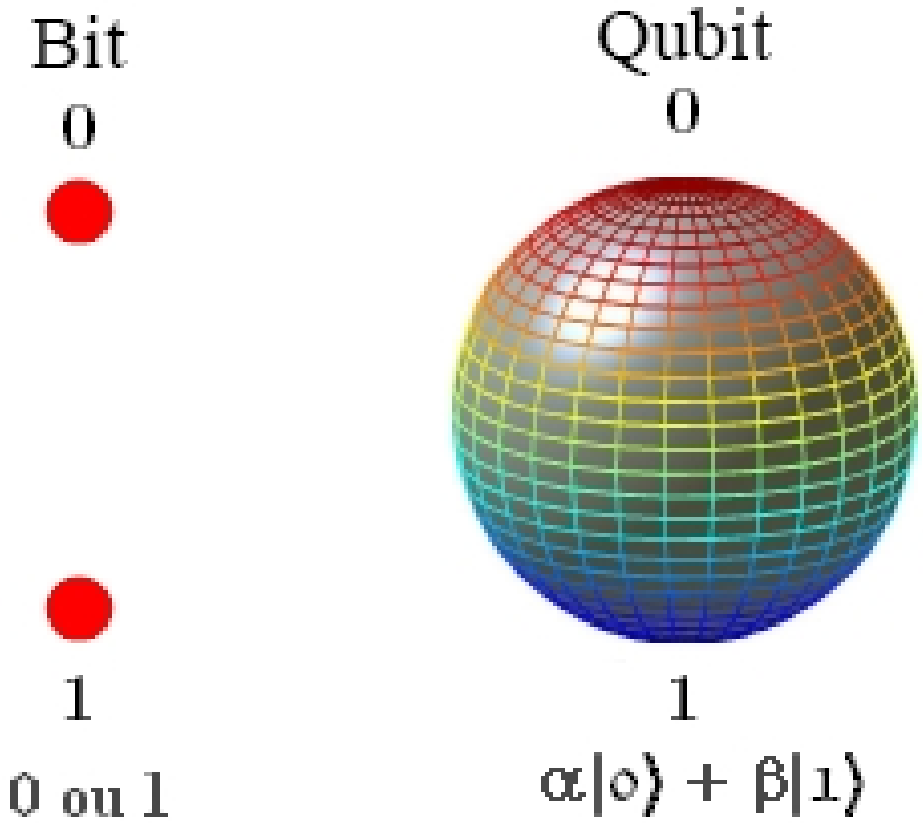
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

onde α e $\beta \in \mathbb{C}$. Ou seja, o qubit $\psi\rangle$ pode colapsar na base $|0\rangle$ com probabilidade α^2, ou na base $|1\rangle$ com probabilidade β^2.

$\hookrightarrow$ Na mecânica quântica, no entanto, qualquer objeto que tenha dois estados diferentes, possui necessariamente diversos outros estados possíveis denominados sobreposições, dos quais resultam a existência de ambos os estados em graus variáveis.

Conceitos

Representação de um Bit e Qubit



Conceitos

$\hookrightarrow$ A porta lógica quântica mais simples é a porta NOT. Esta porta lógica, denotada por Q-NOT, atua sobre um único qubit, e troca o estado

$$\text{Q-NOT}|0\rangle = |1\rangle \qquad \text{Q-NOT}|1\rangle = |0\rangle \tag{2}$$

A matriz de transformação para esta operação é dada por

$$\text{Q-NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3}$$

$$\text{Q-NOT}(|0\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle \tag{4}$$

onde $|0\rangle$ e $|1\rangle$ são definidos como os vetores $(1,0)^T$ e $(0,1)^T$ respectivamente. O conjunto $(|0\rangle, |1\rangle)$ forma uma base do espaço de Hilbert associado com o qubit, que é chamada de base computacional.

Conceitos

↪ A porta lógica quântica XOR atua diferente da sua respectiva porta lógica clássica.

$$\text{Q-XOR}|00\rangle = |00\rangle \qquad \text{Q-XOR}|01\rangle = |01\rangle \tag{5}$$

$$\text{Q-XOR}|10\rangle = |11\rangle \qquad \text{Q-XOR}|11\rangle = |10\rangle \tag{6}$$

↪ A porta XOR quântica, é a única porta de dois qubits necessária para se construir qualquer outra.

↪ Uma consequência importante do fato das transformações quânticas serem unitárias é que elas são reversíveis.

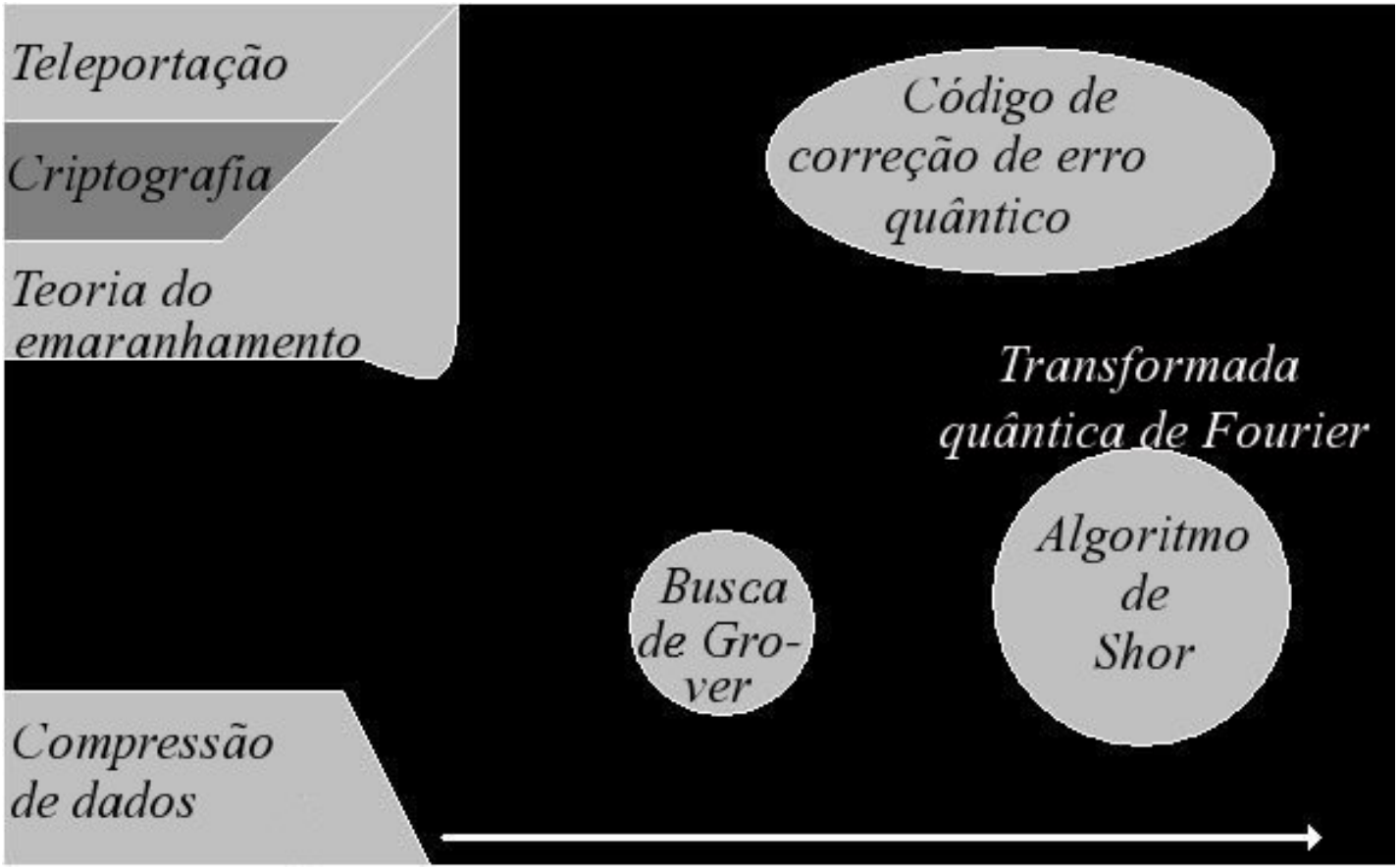
Tecnologias para Construção de Computadores Quânticos

$\hookrightarrow$ As três abordagens para a implementação de um computador quântico, que estão sendo investigadas, são:

- Armadilha de Íons
- Eletrodinâmica Quântica de Cavidade ou Polarização de Fótons
- Ressonância Magnética Nuclear

Algoritmos Quânticos

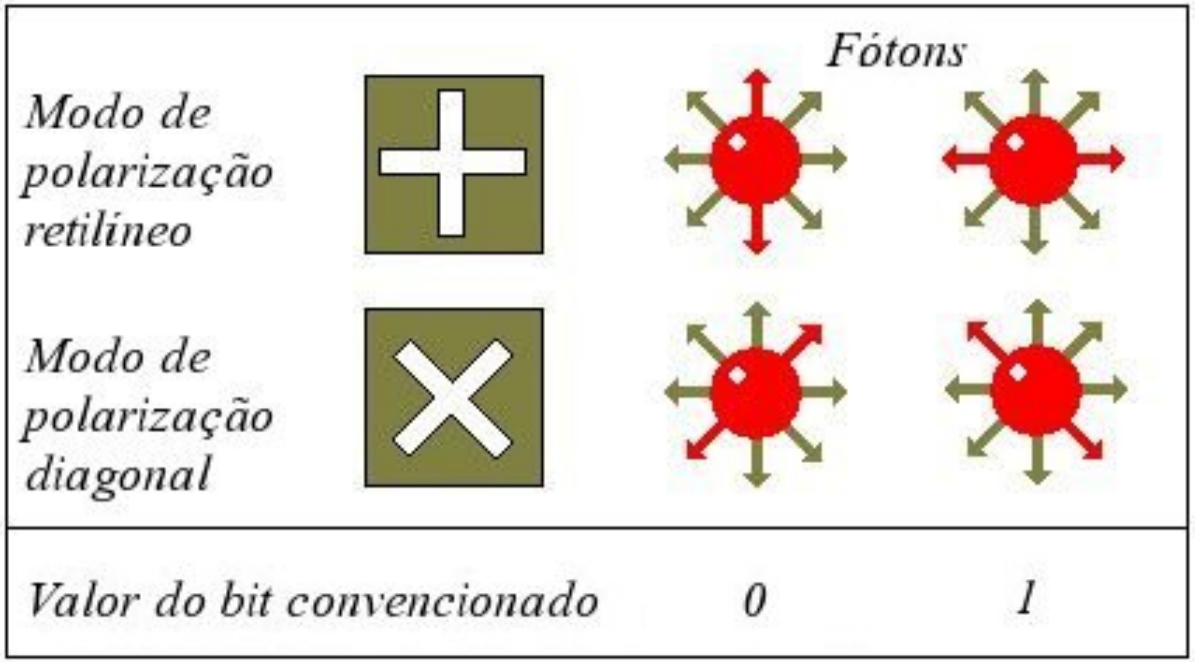
↪ Os algoritmos quânticos mais conhecidos podem ser vistos na figura abaixo:



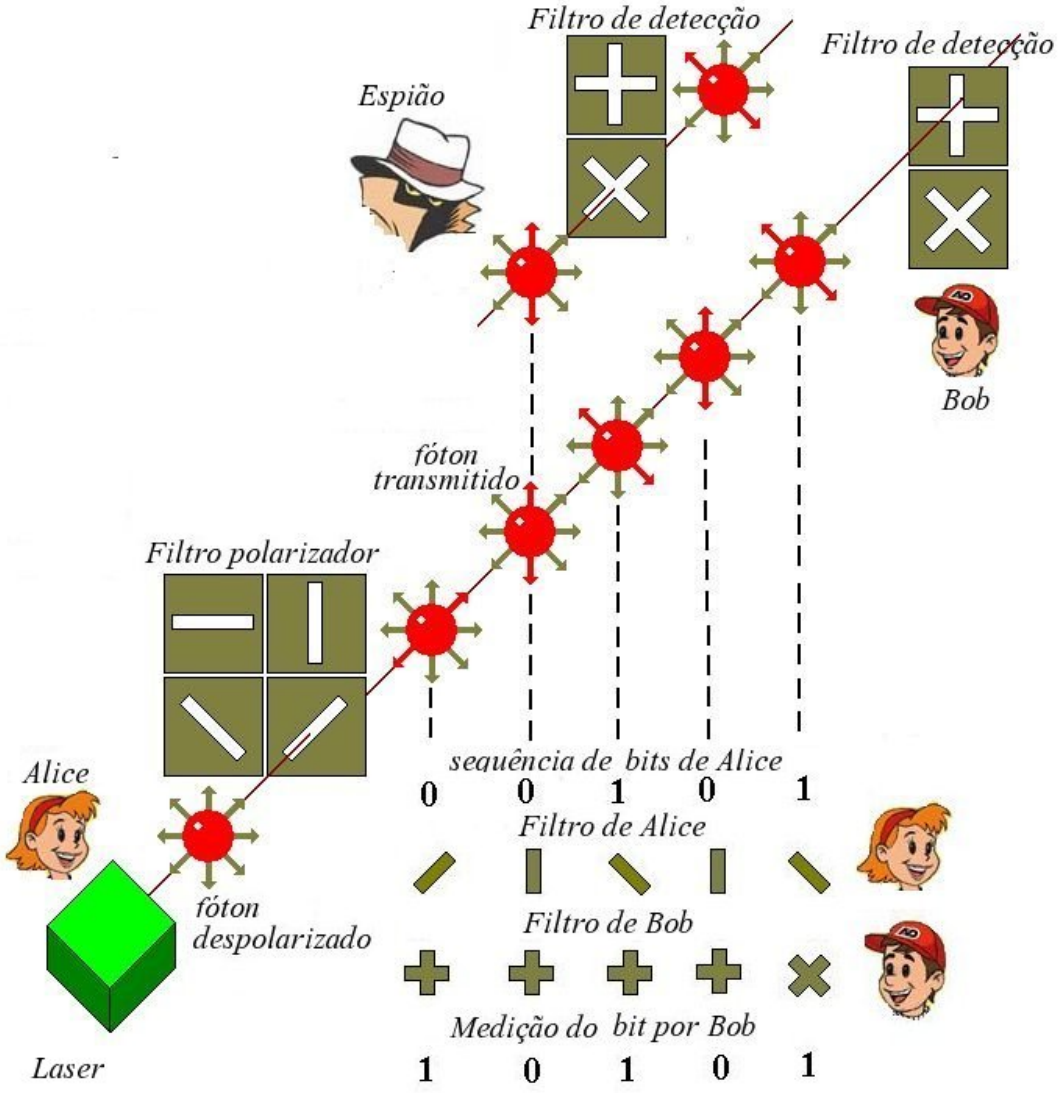
Algoritmos Quânticos

↪ A criptografia quântica é interessante por poder detectar se algum intruso interceptou a transmissão

Polarização dos fotóns

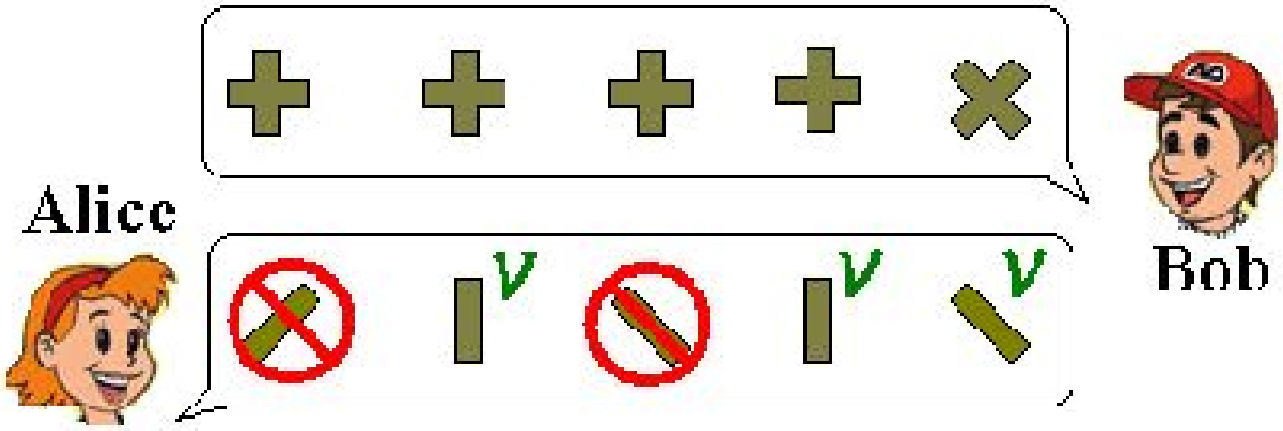


Algoritmos Quânticos



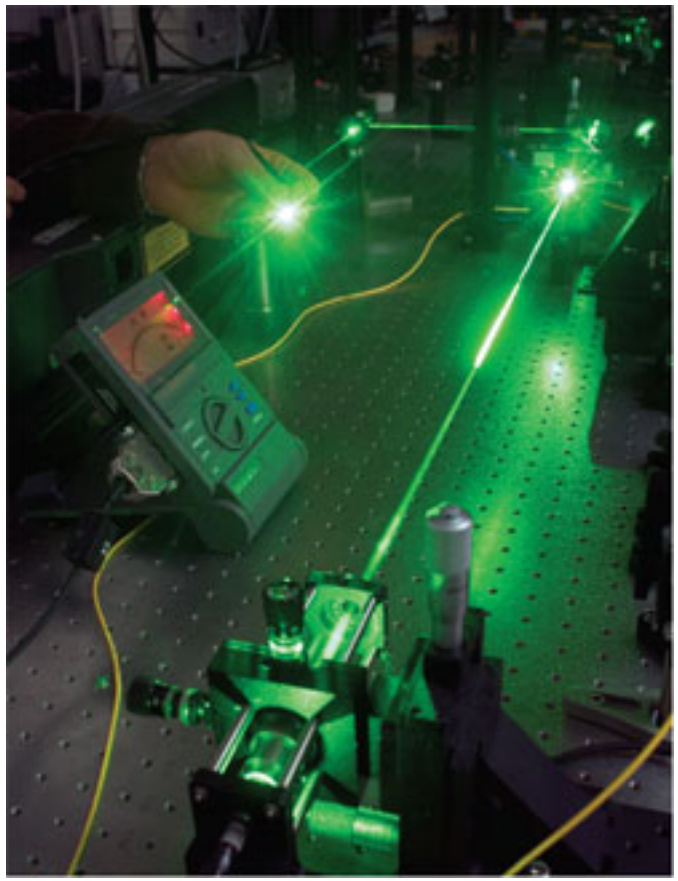
Algoritmos Quânticos

$\hookrightarrow$ Diálogo não necessariamente secreto para determinar a chave criptográfica que serve como entrada de dados para um algoritmo usado para criptografar e decifrar a mensagem.



Algoritmos Quânticos

↪ Um polarizador de fótons para envio de chave criptográfica sendo testado em um laboratório



Computador Quântico x Computador Clássico

$\hookrightarrow$ Um computador clássico com três bits de memória pode apenas armazenar três caracteres (uns ou zeros). Um computador quântico pode armazenar 16 valores analógicos em pares para formar 8 números complexos.

Tabela 1: Probabilidade de retorno de uma sequência de 3-bits caso seja efetuada uma medição.

Estado	Amplitude	Probabilidade
*	$a + ib$	$(a^2 + b^2)$
000	$0.37 + i0.04$	0.14
001	$0.11 + i0.18$	0.04
010	$0.09 + i0.31$	0.10
011	$0.30 + i0.30$	0.18
100	$0.35 + i0.43$	0.31
101	$0.40 + i0.01$	0.16
110	$0.09 + i0.12$	0.02
111	$0.15 + i0.16$	0.05

Conclusões

↪ Ainda não está claro para a tecnologia presente se será possível suportar um computador quântico no futuro.

↪ Embora os computadores quânticos possam ser ordens de grandeza mais rápidos que os computadores clássicos, estes ainda, não podem solucionar problemas que os computadores clássicos não conseguem resolver tendo memória e processamento suficientes.

↪ E finalmente, é importante conhecer os limites de nossas abilidades experimentais em controlar a natureza no nível quântico, e as investigações nesta área fundamental justificam todos os esforços na direção da computação quântica.