

Bits quânticos

Adenilton Silva

8 de setembro de 2020

Seção 1

Bits quânticos

Bits quânticos

qubits

- ▶ Um **bit quântico** é um vetor unitário complexo bidimensional.

$$|v\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \text{ onde } || |v\rangle || = 1$$

Bits quânticos

qubits

- ▶ Um **bit quântico** é um vetor unitário complexo bidimensional.

$$|v\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \text{ onde } || |v\rangle || = 1$$

- ▶ O conjunto $\{|0\rangle, |1\rangle\}$ é uma base ortonormal denominada **base computacional**.

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ e } |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Combinação linear

- ▶ Um **ket** $|x\rangle$ representa um vetor.

Combinação linear

- ▶ Um **ket** $|x\rangle$ representa um vetor.
- ▶ $|v\rangle$ é uma **combinação linear** dos vetores $|v_1\rangle, \dots, |v_n\rangle$ se

$$|v\rangle = \sum_{i=1}^n a_i |v_i\rangle$$

.

Combinação linear

- ▶ Um **ket** $|x\rangle$ representa um vetor.
- ▶ $|v\rangle$ é uma **combinação linear** dos vetores $|v_1\rangle, \dots, |v_n\rangle$ se

$$|v\rangle = \sum_{i=1}^n a_i |v_i\rangle$$

.

- ▶ O **espaço gerado** por um conjunto de vetores S é formado por todas as combinações lineares de vetores em S .

Combinação linear

- ▶ Um **ket** $|x\rangle$ representa um vetor.
- ▶ $|v\rangle$ é uma **combinação linear** dos vetores $|v_1\rangle, \dots, |v_n\rangle$ se

$$|v\rangle = \sum_{i=1}^n a_i |v_i\rangle$$

.

- ▶ O **espaço gerado** por um conjunto de vetores S é formado por todas as combinações lineares de vetores em S .
- ▶ Um conjunto de vetores $S = \{|s_i\rangle\}_{i=1}^n$ é **linearmente dependente** se existirem coeficientes a_i não todos nulos tais que $\sum_{i=1}^n a_i |s_i\rangle = 0$.

Combinação linear

- ▶ Um **ket** $|x\rangle$ representa um vetor.
- ▶ $|v\rangle$ é uma **combinação linear** dos vetores $|v_1\rangle, \dots, |v_n\rangle$ se

$$|v\rangle = \sum_{i=1}^n a_i |v_i\rangle$$

.

- ▶ O **espaço gerado** por um conjunto de vetores S é formado por todas as combinações lineares de vetores em S .
- ▶ Um conjunto de vetores $S = \{|s_i\rangle\}_{i=1}^n$ é **linearmente dependente** se existirem coeficientes a_i não todos nulos tais que $\sum_{i=1}^n a_i |s_i\rangle = 0$.
- ▶ Uma **base** de um espaço S é um conjunto de vetores que gera S e é linearmente independente.

Produto interno

- ▶ Um **produto interno** $\langle v_1 | v_2 \rangle$ é uma função que recebe pares de vetores e retorna um número complexo e satisfaz as propriedades:
 1. $\langle v | v \rangle$ é um número real não negativo;
 2. $\langle v_1 | v_2 \rangle = \overline{\langle v_2 | v_1 \rangle}$
 3. $\langle v_1 | (a | v_2 \rangle + b | v_3 \rangle) = a \langle v_1 | v_2 \rangle + b \langle v_1 | v_3 \rangle$

Bases ortonormais

- Dois vetores $|v_1\rangle, |v_2\rangle$ são **ortogonais** se $\langle v_1 | v_2 \rangle = 0$.

Bases ortonormais

- ▶ Dois vetores $|\nu_1\rangle, |\nu_2\rangle$ são **ortogonais** se $\langle \nu_1 | \nu_2 \rangle = 0$.
- ▶ Um conjunto $\{|\beta_1\rangle, \dots, |\beta_n\rangle\}$ é **ortonormal** se para todo i, j $\langle \beta_i | \beta_j \rangle = \delta_{ij}$, onde

$$\delta_{ij} = \begin{cases} 1, & \text{se } i = j, \\ 0, & \text{se } i \neq j \end{cases}.$$

Bits quânticos

qubits

- ▶ O conjunto $\{|0\rangle, |1\rangle\}$ é uma base ortonormal denominada base computacional.
- ▶ Escolhendo a base compucional,

$$a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}.$$

Bits quânticos

qubits

- ▶ O conjunto $\{|0\rangle, |1\rangle\}$ é uma base ortonormal denominada base computacional.
- ▶ Escolhendo a base compucional,

$$a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}.$$

- ▶ Seja $|v\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$, definimos o bra $|v\rangle^\dagger = \langle v| = [\overline{a_1}, \dots, \overline{a_n}]$
- ▶ $\langle v_1|v_2\rangle = \langle v_1| |v_2\rangle$

Superposição

1. Um bit quântico $|v\rangle$ está em superposição em relação a base computacional se $|v\rangle = a|0\rangle + b|1\rangle$ com a e b diferentes de zero.

Superposição

1. Um bit quântico $|v\rangle$ está em superposição em relação a base computacional se $|v\rangle = a|0\rangle + b|1\rangle$ com a e b diferentes de zero.
2. Qual a quantidade de informação que pode ser armazenada em um qubit?

Medição

- ▶ Não podemos visualizar o estado $a|0\rangle + b|1\rangle$ de um qubit, para obter informações é necessário realizar uma medição.

Medição

- ▶ Não podemos visualizar o estado $a|0\rangle + b|1\rangle$ de um qubit, para obter informações é necessário realizar uma medição.
- ▶ Medições possuem um efeito computacional, pois alteram o estado de um qubit.

Medição

- ▶ Não podemos visualizar o estado $a|0\rangle + b|1\rangle$ de um qubit, para obter informações é necessário realizar uma medição.
- ▶ Medições possuem um efeito computacional, pois alteram o estado de um qubit.
- ▶ Para realizar a medição de um estado $|v\rangle$ devemos
 1. Escolher uma base $\{|u\rangle, |u^\perp\rangle\}$.
 2. Escrever o estado como uma combinação linear dos elementos da base

$$|v\rangle = a|u\rangle + b|u^\perp\rangle$$

Medição

- ▶ Não podemos visualizar o estado $a|0\rangle + b|1\rangle$ de um qubit, para obter informações é necessário realizar uma medição.
- ▶ Medições possuem um efeito computacional, pois alteram o estado de um qubit.
- ▶ Para realizar a medição de um estado $|v\rangle$ devemos
 1. Escolher uma base $\{|u\rangle, |u^\perp\rangle\}$.
 2. Escrever o estado como uma combinação linear dos elementos da base

$$|v\rangle = a|u\rangle + b|u^\perp\rangle$$

3. Realizar a medição obtendo

$$\begin{cases} |u\rangle, & \text{com probabilidade } |a|^2 \\ |u^\perp\rangle, & \text{com probabilidade } |b|^2 \end{cases}$$

Medição

- ▶ Após a medição o bit quântico irá colapsar para o resultado da medição.

Medição

- ▶ Após a medição o bit quântico irá colapsar para o resultado da medição.
- ▶ Ao realizar uma medição de um qubit $|\nu\rangle = a|0\rangle + b|1\rangle$.

$$\begin{cases} |0\rangle, & \text{com probabilidade } |a|^2, \text{ após a medição } |\nu\rangle = |0\rangle \\ |1\rangle, & \text{com probabilidade } |b|^2, \text{ após a medição } |\nu\rangle = |1\rangle \end{cases}$$

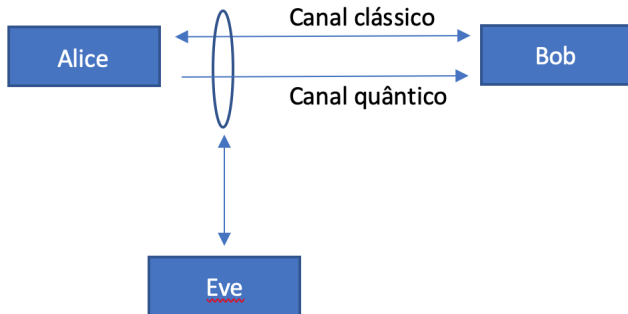
Bits quânticos representam probabilidades?

- ▶ $|v\rangle = a|0\rangle + b|1\rangle$ não representa uma distribuição de probabilidades.
- ▶ $|v\rangle = a|0\rangle + b|1\rangle$ é um estado definido.

Seção 2

Protocolo de distribuição de chaves

Um protocolo para distribuição de chaves privadas



- ▶ Alice e Bob desejam criar uma chave (cadeia binária) secreta.

BB84

- ▶ Alice gera aleatoriamente dois strings binários de comprimento n a e b .

- ▶ Alice gera aleatoriamente dois strings binários de comprimento n a e b .
- ▶ Para cada $a_i b_i$ Alice cria o estado quântico $|v_{a_i b_i}\rangle$, onde

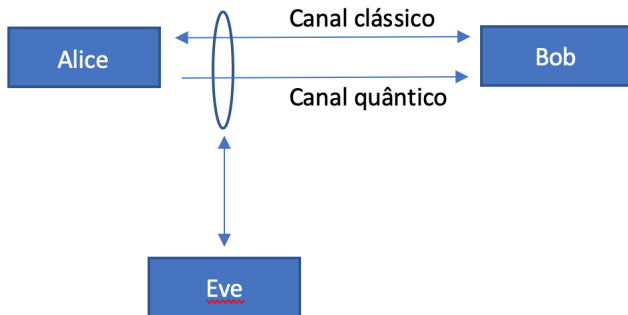
$$\begin{aligned} |v_{00}\rangle &= |0\rangle \\ |v_{10}\rangle &= |1\rangle \\ |v_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |v_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{1}$$

- ▶ Para recuperar o string a é necessário possuir os qubits e o string b (para determinar a base em que será realizada a medição).

- ▶ Alice envia apenas os qubits para Bob.
- ▶ Para cada qubit Bob escolhe aleatoriamente uma das bases $\{|0\rangle, |1\rangle\}$ ou $\{|+\rangle, |-\rangle\}$ para realizar a medição.
- ▶ Bob informa a Alice a base utilizada e ele mantém apenas os bits em que as bases coincidem.
- ▶ Bob e Alice checam através do canal clássico se uma fração dos bits coincidem.

BB84

Como Eve pode interceptar os dados?



Seção 3

O espaço dos bits quânticos

Fase global

- ▶ $a|0\rangle + b|1\rangle$ e $a'|0\rangle + b'|1\rangle$ representam o mesmo estado se

$$a|0\rangle + b|1\rangle = c(a'|0\rangle + b'|1\rangle),$$

onde $c = e^{i\theta}$.

- ▶ $c = e^{i\theta}$ é denominado **fase global**.
- ▶ Existe uma diferença entre o espaço dos qubits e o espaço vetorial complexo onde os qubits são representados.

Fase relativa

- ▶ A fase relativa de um bit quântico é o número $e^{i\phi}$ que satisfaz $a/b = e^{i\phi}|a|/|b|$.
- ▶ Estados com fases relativas diferentes representam diferentes qubits.
- ▶ $e^{i\theta}|v1\rangle$ e $|v1\rangle$ representam o mesmo estado.
- ▶ $1/\sqrt{2}(e^{i\theta}|0\rangle + |1\rangle)$ e $1/\sqrt{2}(|0\rangle + |1\rangle)$ representam qubits diferentes.

Exemplos de qubits

$$\begin{aligned}|+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\|-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\|i\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle) \\|-i\rangle &= \frac{1}{\sqrt{2}} (|0\rangle - i|1\rangle)\end{aligned}$$

Seção 4

Representação geométrica de um qubit

Esfera de Bloch

- ▶ Um qubit $e^{i\phi_1}a|0\rangle + e^{i\phi_2}b|1\rangle$ pode ser descrito como $a|0\rangle + e^{i\phi}b|1\rangle$.
- ▶ Como $|a|^2 + |b|^2 = 1$ existe um θ onde $\cos(\theta) = a$ e $\sin(\theta) = b$.
- ▶ Logo $a|0\rangle + e^{i\phi}b|1\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$.

Esfera de Bloch

- O estado $\cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$ pode ser representado em uma esfera.

