Computação Quântica: introdução

Ricardo Mendes Ribeiro

March 25, 2021

Sistema

Vamos considerar um sistema com spin $S = \hbar\sqrt{s(s+1)}$ $\qquad (s = \frac{1}{2})$

Podemos designar as suas componentes segundo z como:

$$S_z = +\frac{1}{2}\hbar \qquad |+\frac{1}{2}\rangle \qquad |+\rangle \qquad |1\rangle \qquad |\uparrow\rangle$$
$$S_z = -\frac{1}{2}\hbar \qquad |-\frac{1}{2}\rangle \qquad |-\rangle \qquad |0\rangle \qquad |\downarrow\rangle$$

Um estado genérico pode ser descrito por:

$$|z\rangle = a_\uparrow|\uparrow\rangle + a_\downarrow|\downarrow\rangle$$

em que $|a_\uparrow|^2 + |a_\downarrow|^2 = 1$ e, em particular, podemos escolher

$$|z\rangle \equiv |\theta\rangle = \cos\theta|\uparrow\rangle + \sin\theta|\downarrow\rangle$$

Temos o nosso sistema descrito na base S_z, com os vectores da base $|\uparrow\rangle, |\downarrow\rangle$.

Mudanças de base

Podemos querer descrever o nosso sistema na base S_x com os vectores da base $|\rightarrow\rangle, |\leftarrow\rangle$, representando $S_x = +\frac{1}{2}\hbar$ e $S_x = -\frac{1}{2}\hbar$, respectivamente. Vamos ter as seguintes conversões:

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \qquad |\uparrow\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\leftarrow\rangle\right)$$

$$|\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right) \qquad |\downarrow\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\leftarrow\rangle\right)$$

Mudanças de base

Da mesma maneira, podemos querer descrever o nosso sistema na base S_y com os vectores da base $|\nearrow\rangle, |\swarrow\rangle$, representando $S_y = +\frac{1}{2}\hbar$ e $S_y = -\frac{1}{2}\hbar$, respectivamente.
Vamos ter as seguintes conversões:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + i|\downarrow\rangle\right) \qquad |\uparrow\rangle = \frac{1}{\sqrt{2}}\left(|\nearrow\rangle + |\swarrow\rangle\right)$$

$$|\swarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - i|\downarrow\rangle\right) \qquad |\downarrow\rangle = \frac{1}{i\sqrt{2}}\left(|\nearrow\rangle - |\swarrow\rangle\right)$$

Logo, se uma partícula tem o spin em z: $|\psi\rangle = |\uparrow\rangle$, então o seu estado na base em x será:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\leftarrow\rangle\right)$$

e tem 50% de probabilidade de medir $S_x = +\frac{1}{2}\hbar$ e 50% de probabilidade de medir $S_x = -\frac{1}{2}\hbar$.

Transformação para uma base genérica

no plano xy, fazendo um ângulo ϕ com o eixo dos x:

$$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle \pm e^{i\phi}|\downarrow\rangle\right)$$

- O eixo dos x corresponde a fazer $\phi = 0$
- O eixo dos y corresponde a fazer $\phi = \frac{\pi}{2}$

Criptografia Quântica

- Transmitir uma mensagem sem que ninguém a não ser o destinatário a possa decifrar
- Pode-se fazer codificando uma mensagem com uma chave que só o que envia e o destinatário conhecem
- O problema fica então reduzido a enviar uma chave segura para o receptor da mensagem

Chave de encriptação

Escrita em binário

Mensagem	1	0	0	1	1	0	1	0	0	$\cdots$
Chave	1	1	0	1	1	1	1	0	1	$\cdots$
Mensagem encriptada	0	1	0	0	0	1	0	0	1	$\cdots$

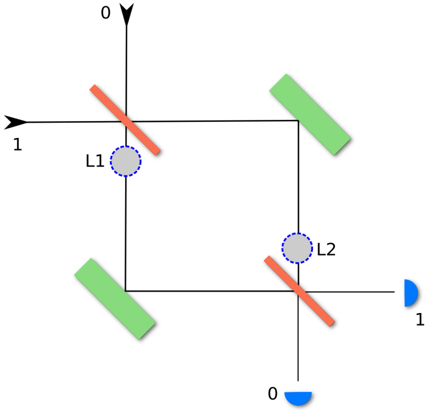
Obtém-se a mensagem encriptada usando o *ou-exclusivo*:

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \oplus 0 = 1 \qquad 1 \oplus 1 = 0$$

Método perfeitamente seguro se:

- A chave é realmente aleatória
- A chave só é usada uma vez
- A chave é do tamanho da mensagem

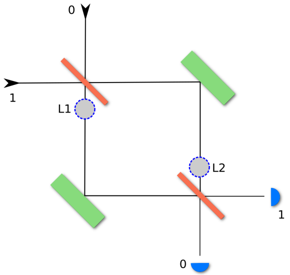
Exemplo de montagem



Se $L1 \neq L2$, destrói a interferência.

Protocolo

1. O emissor envia um conjunto de 0s e 1s gerados aleatoriamente, escolhendo (também aleatoriamente) accionar ou não o dispositivo L1 para cada bit que envia.
2. Para cada bit recebido, o receptor também escolhe accionar ou não o dispositivo L2.
3. Então, receptor e emissor comparam por um canal aberto quais as posições em quem cada um tinha os dispositivos L1 e L2, para cada bit transmitido, e escolhem só aqueles em que tinham na mesma posição, de modo a ficarem os dois com um conjunto de 0s e 1s idêntico.
4. Depois é necessário fazer uma verificação de que ninguém tentou apanhar a chave através de alguma escuta.
   Assim, o receptor envia uma parte da chave que recebeu por canal aberto para o emissor (por exemplo, a primeira metade); este compara os números com os que enviou; se forem iguais, podem usar a outra metade da chave, porque ninguém a interceptou; se forem diferentes, sabem que não podem usar a chave, e que o canal está comprometido.



	bit enviado	L1	L2	bit recebido	Serve?
1	0	sim	não	1	não
2	1	sim	sim	1	sim
3	1	não	não	1	sim
4	1	não	sim	0	não
5	0	não	não	0	sim
⋮	⋮	⋮	⋮	⋮	

Quantum bit: qubit

Podemos associar o estado:

$$|\uparrow\rangle \equiv |1\rangle \text{ a um bit 1}$$

e o estado

$$|\downarrow\rangle \equiv |0\rangle \text{ a um bit 0}$$

A um estado genérico

$$|\psi\rangle = a_1|1\rangle + a_0|0\rangle$$

chamamos qubit, ou quantum bit.

Num computador clássico, os bits estão num estado bem definido: 0 ou 1.

Num computador quântico, os qubits estão numa sobreposição de estados.

Representação de números

Faz-se como nos computadores clássicos: associando qubits.

$$|5\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle \equiv |1\rangle|0\rangle|1\rangle \equiv |101\rangle$$

(São três formas de representar a mesma coisa.)

Qualquer inteiro $0 < N \leq 2^n - 1$ pode ser representado por n qubits:

$$|n\rangle = |b_{n-1}\rangle|b_{n-2}\rangle \cdots |b_1\rangle|b_0\rangle$$

Mas em geral, um estado será uma sobreposição desses 2^n estados:

$$|\psi\rangle = a_0|000\rangle + a_1|100\rangle + a_2|010\rangle + a_3|001\rangle + a_4|110\rangle + a_5|011\rangle + a_6|101\rangle + a_7|111\rangle$$

$$|\psi\rangle = \sum_{i=0}^{n-1} a_i|b^i_{n-1} b^i_{n-2} \cdots b^i_1 b^i_0\rangle$$

Para n qubits, precisamos de guardar 2^n números para definir o estado!

Quantum Logic Gates

As operações em computação quântica são implementadas por quantum logic gates

Os *gates* mais simples são os que se aplicam a 1 só qubit.

X-gate

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$$

Hadamard-gate muda de base:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Exemplo de um *gate* que se aplica a dois qubits:

cNOT-gate o primeiro qubit controla o resultado

$$\mathrm{cNOT}(|0\rangle|0\rangle) = |0\rangle|0\rangle \qquad \mathrm{cNOT}(|0\rangle|1\rangle) = |0\rangle|1\rangle$$

$$\mathrm{cNOT}(|1\rangle|0\rangle) = |1\rangle|1\rangle \qquad \mathrm{cNOT}(|1\rangle|1\rangle) = |1\rangle|0\rangle$$

Procedimento

Temos um sistema de n qubits $|\psi\rangle$

Inicializa-se o sistema significa colocá-lo num dos estados possíveis, por exemplo $|101\rangle$
Pode ser uma sobreposição de estados, logo à partida.

Aplicam-se as diversas operações cada operação O_i transforma o estado anterior noutro

$$O_1|\psi\rangle \rightarrow |\psi'\rangle$$
$$O_2|\psi'\rangle \rightarrow |\psi''\rangle$$
$$\ldots$$
$$O_f|\psi^{(n)}\rangle \rightarrow |\psi_f\rangle$$

Equivale a fazer

$$O_f \cdots O_2 O_1|\psi\rangle \rightarrow |\psi_f\rangle$$

Procedimento (cont.)

Leitura dos valores no fim temos de ler o valor dos qubits. Mas a leitura implica destruir o estado. Se o estado obtido é $|\psi_f\rangle = a_1|10011\rangle + a_2|00011\rangle + a_3|10111\rangle + a_4|10001\rangle$, em cada medida obtemos apenas um dos vectores, com probabilidade $|a_1|^2$ para $|10011\rangle$, $|a_2|^2$ para $|00011\rangle$, etc.

Repete-se o procedimento para obter estatística. Repetindo muitas vezes os passos todos, de modo a chegar sempre ao mesmo vector final, as medidas vão ter a distribuição estatística dada pelas probabilidades $|a_i|^2$; donde podemos obter o vector estado final.

A computação quântica é em geral probabilística.

As operações têm de ser feitas na ordem: não pode haver *if-then*, porque para isso teríamos de ler o qubit antes do fim do cálculo, e destruíamo-lo.

Tem de haver uma forma de programação diferente para um computador quântico.

Problemas tipo para um computador quântico

1. Problemas em que a única forma de os resolver é por tentar adivinhar a solução e testar
2. Problemas onde há n possibilidades para verificar (n grande)
   Computador clássico $t \propto (n+1)/2$
   Computadoir quântico $t \propto \sqrt{n}$
3. Problemas onde todas as possibilidades demoram o mesmo tempo a verificar
4. Problemas onde não há pistas da solução: tanto dá fazer tentativas aleatórias como ordenadas

Exemplo: factorização de inteiros.