

# Computação Quântica

## Parte 1

### Índice

1.	Bits e qubits .....	2
2.	Operadores quânticos .....	7
3.	Porta quântica CNOT: NOT-controlado .....	9
4.	Algoritmo quântico .....	10
5.	Computador quântico × Computador digital .....	11
6.	Problemas indicados para solução via computação quântica.....	13
7.	Referências bibliográficas e links úteis .....	14

## 1. Bits e qubits

- A unidade básica de informação em computadores digitais é o bit. Um bit pode ter os valores lógicos “0” ou “1”.
- Nos computadores digitais, bits são fisicamente representados pela presença ou não de correntes elétricas em componentes eletrônicos dentro dos chips: a presença da corrente indica o estado lógico 1 e a sua ausência o estado lógico 0. Portanto, **os dois valores lógicos de um bit são mutuamente excludentes.**
- Para tratar da unidade básica de informação em computadores quânticos, é necessário recorrer ao conceito de espaço de Hilbert e de esfera de Bloch.
- Um espaço de Hilbert ( $H$ ) é um espaço vetorial complexo provido de uma métrica dada por um produto escalar. Em um espaço vetorial  $H$ , uma combinação linear de dois elementos pertencentes a  $H$ ,  $|\psi_1\rangle$  e  $|\psi_2\rangle$ , também pertence a  $H$ , ou seja:

$$\text{Dados } |\psi_1\rangle \in H \text{ e } |\psi_2\rangle \in H, \text{ então } a|\psi_1\rangle + b|\psi_2\rangle \in H,$$

onde  $a$  e  $b$  são números complexos.

- A unidade de informação quântica é o bit quântico, ou qubit (do inglês **quantum binary digit**), o qual pode assumir os valores lógicos “0”, “1” ou qualquer superposição destes.
- Fisicamente, qubits são representados por qualquer objeto quântico que possua dois auto-estados bem distintos, como estados de polarização de um fóton ou spins nucleares.
- Os auto-estados de um qubit são representados por  $|0\rangle$  e  $|1\rangle$ . O conjunto de auto-estados  $\{|0\rangle, |1\rangle\}$  forma uma base no espaço de Hilbert de duas dimensões, tal que:

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

- O estado genérico de um qubit é representado por:

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

onde  $a$  e  $b$  são números complexos tal que  $a^2 + b^2 = 1$ .

- Este estado genérico pode ser parametrizado por ângulos  $\theta$  e  $\varphi$ , fazendo-se:

$$a = \cos\left(\frac{\theta}{2}\right) \text{ e } b = \exp(j\varphi)\text{sen}\left(\frac{\theta}{2}\right)$$

o que produz:

$$|\psi\rangle = \left[ \cos\left(\frac{\theta}{2}\right) \right] |0\rangle + \left[ \exp(j\varphi)\text{sen}\left(\frac{\theta}{2}\right) \right] |1\rangle$$

- Esta representação permite que o estado de um qubit corresponda a um ponto sobre a superfície de uma esfera. Tal esfera é chamada de esfera de Bloch, a qual é apresentada na sequência.
- Pontos especiais sobre a esfera de Bloch são mostrados na tabela abaixo.

$\theta$	$\varphi$	$ \psi\rangle$	Comentário
0	0	$ 0\rangle$	Pólo Norte da Esfera de Bloch
$\pi$	0	$ 1\rangle$	Pólo Sul da Esfera de Bloch
$\pi/2$	0	$( 0\rangle +  1\rangle)/\sqrt{2}$	Equador, sobre o eixo $x$
$\pi/2$	$\pi/2$	$( 0\rangle + j 1\rangle)/\sqrt{2}$	Equador, sobre o eixo $y$

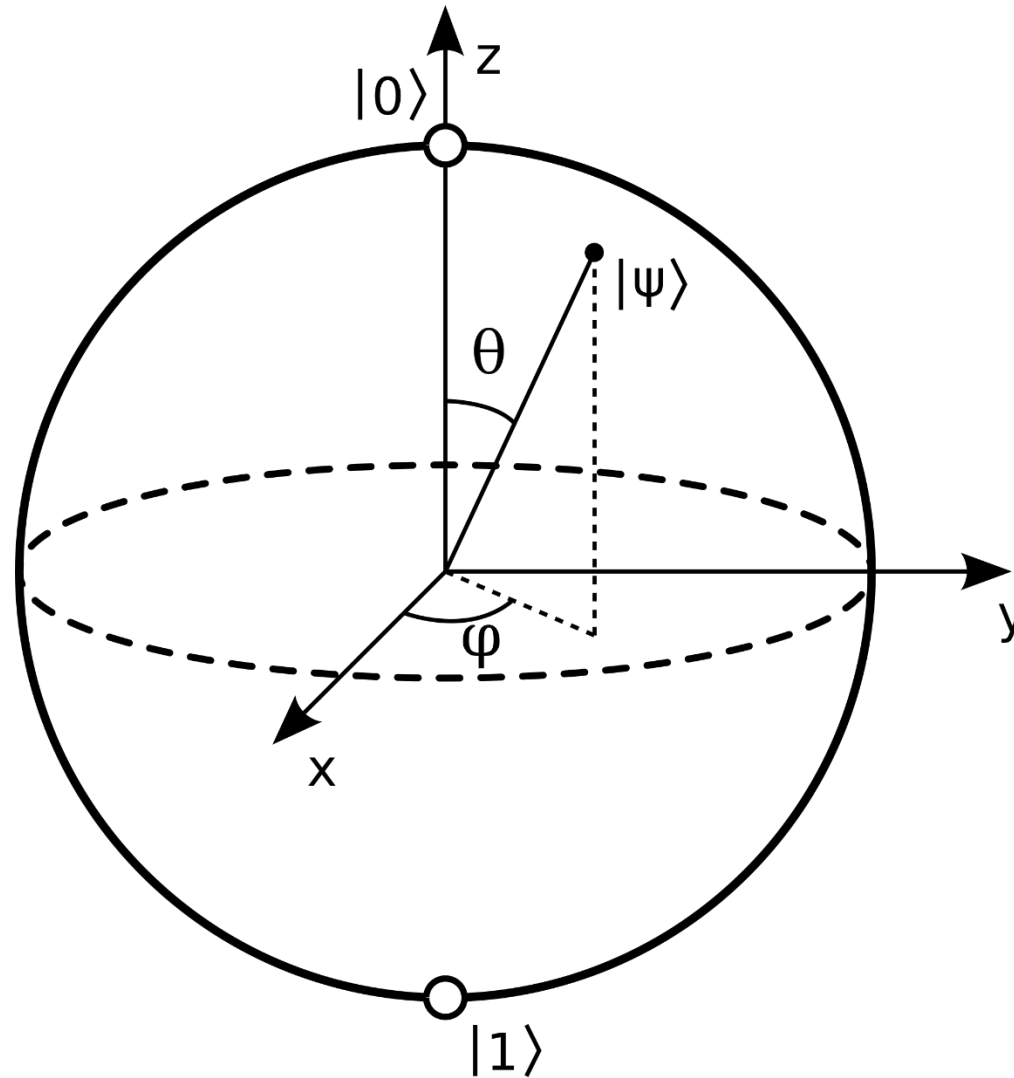


Figura 1 – Esfera de Bloch

- Fica evidenciado, portanto, que **um único qubit pode armazenar uma dentre infinitas informações**, que são todas as combinações lineares possíveis dos números complexos  $a$  e  $b$ , sempre respeitando  $a^2 + b^2 = 1$ . Essas combinações lineares são chamadas de superposições dos auto-estados.
- Não importando em que estado de superposição se encontre um qubit, a leitura de seu valor será sempre  $|0\rangle$  ou  $|1\rangle$ . Isso ocorre porque **a leitura promove o colapso do estado para um dos auto-estados**.
- O estado do qubit vai colapsar em  $|0\rangle$  com probabilidade  $a^2$  e vai colapsar em  $|1\rangle$  com probabilidade  $b^2$ .
- O espaço de Hilbert de dois qubits é expandido pelos vetores formados pelo produto tensorial:  $\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ .
- A representação desses auto-estados é dada por:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}; |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}; |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}; |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

- Prosseguindo com este raciocínio, conclui-se que **um computador quântico com  $n$  qubits em superposição vai ter  $2^n$  auto-estados.**

## 2. Operadores quânticos

- Portas quânticas unárias (que operam sobre um único qubit) são representadas por matrizes  $2 \times 2$  unitárias, sendo capazes apenas de rotacionar o qubit na esfera de Bloch, levando o qubit a um outro estado de superposição.
- Esta é a razão pela qual **toda porta quântica é reversível.**
- Exemplos importantes são as portas de Pauli:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix} \quad \text{e} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

que produzem:

$$X |\psi\rangle = b|0\rangle + a|1\rangle; \quad Y |\psi\rangle = -jb|0\rangle + a|1\rangle \quad \text{e} \quad Z |\psi\rangle = a|0\rangle - b|1\rangle$$

e a porta de Hadamard:

$$H_{ad} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{X + Z}{\sqrt{2}},$$

$$\text{que produz } H_{ad} |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{e} \quad H_{ad} |1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- Com isso, a porta de Hadamard é capaz de produzir uma superposição dos auto-estados quando aplicada a cada um dos auto-estados não-superpostos.
- Como os registradores quânticos vão estar em uma superposição de auto-estados, o **paralelismo quântico é sustentado pelo fato de que uma única porta lógica quântica vai operar simultaneamente sobre todos os auto-estados da superposição.**



### 3. Porta quântica CNOT: NOT-controlado

- Para a implementação da computação quântica, é necessário tomar apenas uma porta quântica de dois qubits: a porta quântica CNOT.
- A porta quântica CNOT é também conhecida como porta NOT-controlado.
- Nesta porta, o estado do qubit alvo muda se e somente se o estado do qubit de controle for igual a 1. A matriz que representa a porta CNOT com controle no primeiro qubit (qubit A) é dada por:

$$\text{CNOT}_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Verifica-se, então que:

$$\begin{array}{ll} \text{CNOT}_A(|00\rangle) = |00\rangle & \text{CNOT}_A(|01\rangle) = |01\rangle \\ \text{CNOT}_A(|10\rangle) = |11\rangle & \text{CNOT}_A(|11\rangle) = |10\rangle \end{array}$$

## 4. Algoritmo quântico

- Um algoritmo quântico, em sua estrutura básica, é composto por:
  1. Especificação de  $n$  qubits;
  2. Aplicação sequencial de  $k$  operadores quânticos sobre quaisquer subconjuntos dos  $n$  qubits;
  3. Medição realizada sobre qualquer subconjunto de qubits.
- Logo, o resultado só pode ser auferido probabilisticamente.
- Múltiplas execuções do mesmo algoritmo (redundância) e estratégias de projeto podem fazer com que a solução se aproxime de um resultado determinístico.

## 5. Computador quântico × Computador digital

- Já foi demonstrado que um computador digital pode ser simulado por um computador quântico. Logo, conclui-se que o computador quântico é ao menos tão poderoso quanto o computador digital.
- Considerando agora a possibilidade de simular um computador quântico empregando um computador digital, cabem as seguintes constatações:
  - ✓ Um computador quântico com  $n$  qubits em superposição vai ter  $2^n$  auto-estados.
  - ✓ Isso implica que cada estado de um registrador quântico é definido por  $2^n$  números complexos.
  - ✓ Cada operador quântico para este computador quântico de  $n$  qubits é descrito por uma matriz  $2^n \times 2^n$  de elementos complexos.
  - ✓ A medida de cada qubit colapsa o estado em superposição para um dos auto-estados, com certa probabilidade.

- Portanto, para simular um algoritmo quântico em um computador digital, é necessário:
  1. Memória suficiente para armazenar as  $2^n$  amplitudes complexas do registrador;
  2. Memória suficiente para armazenar as  $2^n \times 2^n$  amplitudes complexas de cada operador quântico;
  3. Dispor de operações básicas de álgebra matricial;
  4. Usar geradores pseudo-aleatórios para simular os resultados das medidas realizadas.
- Além de uma demanda exponencial por memória, deve-se considerar a imprecisão numérica da representação em ponto flutuante para valores reais e a imprecisão estatística ao empregar-se geradores de números pseudo-aleatórios na computação digital.

- Como um exemplo, supondo que um número real possa ser representado aproximadamente por 4 bytes em um computador digital, **são necessários 8 Gigabytes para representar um estado arbitrário de 30 qubits em superposição**:  $2 \times 2^{30}$  valores em ponto flutuante para as partes real e imaginária dos números complexos, cada qual requerendo 4 bytes.

## 6. Problemas indicados para solução via computação quântica

- O problema deve apresentar 4 propriedades:
  1. O único modo de resolvê-lo é chutar respostas candidatas repetidamente e checar cada uma;
  2. Há um número finito de respostas candidatas;
  3. Cada resposta candidata leva o mesmo tempo para ser checada;
  4. Não há nenhuma dica acerca de qual resposta candidata é melhor.
- Para poder resolver problemas NP-completos usando computação quântica, seria necessário desenvolver portas quânticas não-lineares.

## 7. Referências bibliográficas e links úteis

Links para textos introdutórios e temas correlatos:

- ✓ <http://www.cm.ph.bham.ac.uk/scondintro/qubitsintro.html>
- ✓ <http://en.wikipedia.org/wiki/Qubits>
- ✓ <http://www.quantiki.org/>

DE WOLF, R. “Quantum Computing – Lecture Notes”, Dutch Centre for Mathematics and Computer Science, <http://homepages.cwi.nl/~rdewolf/qcnotes.pdf>, 2014.

HAGAR, A. “Quantum Computing”, The Stanford Encyclopedia of Philosophy, E.N. Zalta (ed.) URL: <http://plato.stanford.edu/archives/spr2011/entries/qt-quantcomp/>, 2011.

NIELSEN, M.A. & CHUANG, I.L. “Quantum Computation and Quantum Information”, Cambridge University Press, 10th Anniversary edition, 2010.

STEANE, A.M. “Quantum Computing”, Reports on Progress in Physics, vol. 61, pp. 117-173, 1998.

VALIRON, B. “Quantum Computation: a Tutorial”, New Generation Computing, vol. 30, no. 4, pp. 271-296, 2012.