# Computação Quântica

Luís Soares Barbosa

Mestrado em Engenhara Física
Universidade do Minho

**Folha de Exercícios 1**

**Questão** 1

Uma computação pode ser vista como uma operação sobre sequências de símbolos sobre um dado alfabeto.

1. Quantas sequências de comprimento $n$, formadas apenas por zeros e uns, existem?
2. Uma sequência binária é dita de paridade par (respectivamente, ímpar) se contém um número par (respectivamente, ímpar) de ocorrências do símbolo 1. Quantas sequências binárias de comprimento $n$ e paridade par existem?
3. O conceito de distância de Hamming fornece uma medida de similaridade entre duas sequências binárias, definindo-se como o número de posições em diferem. O peso de Hamming define-se como o número de ocorrências de 1 na sequência. Quantas sequências binárias de comprimento $n$ têm peso $p$?
4. Uma função Booleana sobre sequências binárias de comprimento $n$ é uma função que atribui um valor Booleano a cada sequência desse tipo. Quantas funções destas existem?

**Questão** 2

O adjunto de um operador $U$ é o único operador que satisfaz a igualdade

$$\begin{aligned} (U^\dagger|w\rangle, |v\rangle) &= (|w\rangle, U|v\rangle) \quad \text{na habitual notação de Dirac} \\ \langle U^\dagger w|v\rangle &= \langle w|Uv\rangle \end{aligned}$$

1. Mostre que $UV^\dagger \;=\; V^\dagger U^\dagger$
2. Mostre que $U^{\dagger\dagger} \;=\; U$
3. Concretamente, podemos definir $U^\dagger$ através da igualdade

   $$\langle i|U^\dagger|j\rangle \;=\; \overline{\langle j|U|i\rangle}$$

   Que podemos concluir daqui sobre a matriz que o representa?

**Questão** 3

Recorde que um operador $U$ é unitário (respectivamente, Hermitiano) se $U^\dagger = U^{-1}$ (respectivamente, $U = U^\dagger$).

1. Verifique que um operador unitário é reversível.
2. Mostre que os valores próprios de um operador Hermitiano são sempre números reais.
3. Mostre que a norma quadrada de qualquer valor próprio de um operador unitário é 1.

**Questão** 4

Recorde a definição de um espaço de Hilbert. Uma das suas propriedades é o facto de o produto interno $\langle - | - \rangle$ ser *conjugado linear* no primeiro argumento.

1. Mostre que é *linear* no segundo argumento.
2. Mostre que se assumirmos, ao invés, que o produto interno é linear no primeiro argumento, como aparece em alguns livros, então terá de ser conjugado linear no segundo.

**Questão** 5

Recorde a porta de Hadamard $H$ frequentemente usada para introduzir sobreposições uniformes. Mostre que $H$ pode ser escrita como

1. $\frac{1}{\sqrt{2}}\left((|0\rangle + |1\rangle)\langle 0| \; + \; (|0\rangle - |1\rangle)\langle 1|\right)$
2. $\frac{1}{\sqrt{2}}(X + Z)$

**Questão** 6

O produto *externo* $|u\rangle\langle v|$ pode ser visto como uma transformação linear quer em $V$ quer em $V^*$.

1. Calcule o valor da sua aplicação a um valor de qualquer destes espaços vectoriais.
2. Mostre que, dada uma base ortonormal $\{|e_i\rangle \mid i \in \underline{n}\}$, para um espaço $V$, qualquer operador que mapeie os vectores de base $|e_i\rangle$ em vectores $|u_i\rangle$ pode ser escrito como uma soma de produtos externos. A notação $\underline{n}$ designa o segmento incial do natural $n$, i.e., $\{1, 2 \cdots n\}$.
3. Se o conjunto dos vectores $|u_i\rangle$ formarem eles próprios uma base ortonormada para $V$, o efeito do operador acima será mapear uma base na outra. Calcule
$$\sum_i |e_i\rangle\langle e_i|$$
4. Usando a importante relação calculada acima, mostre que qualquer vector $|u\rangle$ em $V$ pode ser escrito como
$$|u\rangle \; = \; \sum_i \alpha_i |e_i\rangle$$
onde $\alpha_i = \langle e_i | u\rangle$ são as amplitudes de $|u\rangle$.
5. Calcule o adjunto de um produto externo, i.e., $(|u\rangle\langle v|)^\dagger$.

**Questão** 7

O traço de um operador linear pode ser definido como o somatório da diagonal da matriz que o representa, i.e.,

$$\mathsf{tr}(U) \; = \; \sum_k \langle k|U|k\rangle \; = \; \sum_k U_{k,k}$$

(em rigor, $\sum_k \langle e_k|U|e_k\rangle \; = \; \sum_k U_{k,k}$ para $|e_0\rangle|e_1\rangle \cdots$ uma base ortonormada; porquê?)

Mostre que este operador converte produtos *externos* em produtos *internos*.

**Questão** 8

Recorde as portas de Pauli

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

que desempenham um papel importante em computação quântica. Em particular, qualquer operador sobre um qubit pode ser expresso como uma combinação linear de portas de Pauli.

1. Escreve cada uma delas com recurso ao produto externo.
2. Mostre que são operadores unitários e Hermitianos.
3. Mostre que o efeito de encapsular uma porta $Z$ (respectivamente, uma porta $X$) num *golden pattern*, i.e., entre duas portas de Hadamard, uma porta de Hadamard é converter um *phase-flip* (respectivamente, um *bit-flip*) num *bit-flip* (respectivamente, num *phase-flip*) , i.e.,
$$HZH \;=\; X \qquad \text{e} \qquad HXH \;=\; Z$$
4. Mostre que $P^2 = I$ para qualquer porta de Pauli.
5. Mostre que as portas de Pauli são anti-comutativas, i.e., e.g. $XY = -YX$, $XZ = -ZX$ e $YZ = -ZY$.
6. Explique por que razão os operadores $X$, $Y$ e $Z$ correspondem a *rotações* na esfera de Bloch ao longo dos eixos $x$, $y$ e $z$, respectivamente.

**Questão** 9

Diz-se que um operador unitário $S$ *estabiliza* um estado quântico representado por um vector $|v\rangle$ se

$$S|v\rangle \;=\; |v\rangle$$

1. Mostre que o conjunto de estabilizadores de $|v\rangle$ formam um grupo, recordando que um *grupo* em álgebra é um conjunto equipado com uma operação binária, associativa, com elemento neutro e inversa.
2. Indique estabilizadores para os seguintes estados: $|+\rangle$, $|-\rangle$, $|0\rangle$, $|1\rangle$, $|i\rangle$ e $|-i\rangle$.
3. Que estados são estabilizados pela identidade $I$? E por $-I$?

**Questão** 10

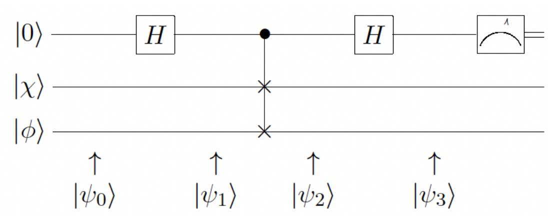
Como facilmente pode verificar, em lógica proposicional não existe nenhuma operação unária que quando composta consigo própria produza o operador de negação. Considere, contudo, o seguinte operador

$$sqX \;=\; \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$$

1. Mostre que este operador tem exactamente esse comportamento.
2. Mostre que é um operador unitário (e corresponde, portanto, a uma operação fisicamente admissível).
3. Mostre que pode ser reescrito como
$$\frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\frac{\pi}{4}} & e^{-i\frac{\pi}{4}} \\ e^{-i\frac{\pi}{4}} & e^{i\frac{\pi}{4}} \end{bmatrix}$$

**Questão** 11

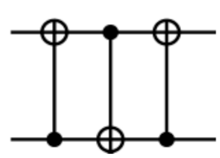
Considere o seguinte circuito:




1. Calcule o valor de cada um dos estados quânticos intermédios representados na figura.
2. Se o resultado da medição for 0 (i.e., o primeiro qubit for $|0\rangle$ no final), qual será o estado quântico dos dois qubits seguintes?
3. Qual será a probabilidade dessa medida ser 0?

**Questão** 12

Considere o seguinte circuito:



1. Construa a sua representação matricial e indique o seu propósito.
2. Mostre que a porta correspondente pode ainda escrita como

$$\frac{I \otimes I + X \otimes X + Y \otimes Y + Z \otimes Z}{2}$$

   onde $I, X, Y, Z$ são as portas de Pauli.

**Questão** 13

Mostre que ao desenhar um circuito de controlo de uma porta $Z$ é indiferente fazer o controlo pelo primeiro ou pelo segundo qubit. Será que este facto pode ser generalizado a outras portas?

**Questão** 14

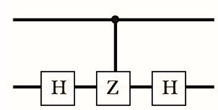
Como sabe, qualquer porta quântica unária $Q$ origina uma porta binária $C_Q$ em que a aplicação de $Q$ ao segundo qubit é condicionada pelo valor do primeiro qubit. O operador correspondente pode ser escrito como

$$C_Q|x\rangle|y\rangle \;=\; |x\rangle \otimes Q^x|y\rangle$$

1. Mostre que o operador $C_Q$ é unitário sempre que $Q$ o fôr.

2. Calcule a representação matricial de $C_Z$ onde $Z$ é uma das portas de Pauli definida por $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

3. O circuito seguinte implementa o operador $CNOT$ que constitui a versão controlada da porta $X$.




Preencha as reticências na seguinte prova desse facto, completando de forma clara e completa as justificações de cada passo.

$$\begin{array}{ll}
 & CNOT|x\rangle|y\rangle \\
= & \qquad \{ \; \cdots \; \} \\
 & |x\rangle \otimes X^x|y\rangle \\
= & \qquad \{ \; X = HZH \; \} \\
 & |x\rangle \otimes (HZH)^x|y\rangle \\
= & \qquad \{ \; \cdots \; \} \\
 & |x\rangle \otimes HZ^xH|y\rangle \\
= & \qquad \{ \; \cdots \; \} \\
 & I \otimes H \cdot C_Z \cdot I \otimes H
\end{array}$$

**Questão** 15

Considere a seguinte porta quântica operando sobre 3 qubits:

$$|abc\rangle \;\mapsto\; |a, b, c \oplus (a \wedge b)\rangle$$

1. Construa a sua representação matricial.
2. Proponha uma representação gráfica na linguagem dos circuitos que traduza para esta porta e justifique a sua escolha.