**Traballo Fin de Grao**

# ALGORITMO DE COMPUTACIÓN CUÁNTICA PARA OPTIMIZACIÓN

Pablo Rivas Pidre

Curso 2024/2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

**Traballo Fin de Grao**

# ALGORITMO DE COMPUTACIÓN CUÁNTICA PARA OPTIMIZACIÓN

Pablo Rivas Pidre

Xulio, 2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

# Traballo proposto

| |
|---|
| **Área de Coñecemento: Matemática Aplicada** |
| **Título: Algoritmo de computación cuántica para optimización** |
| **Breve descrición do contido** |
| **Neste traballo abordarase o estudo da arte computacional e a computación cuántica, explorando o funcionamento das computadoras e as portas cuánticas. O traballo céntrase na análise e comprensión do algoritmo de optimización cuántica VQE (Variational Quantum Eigensolver), unha ferramenta clave para resolver problemas complexos nesta área.** |
| **Recomendacións** |
| |
| **Outras observacións** |
| |

# Índice

## Resumo

Na área da computación cuántica, existe un gran interese no aproveitamento das propiedades cuánticas para resolver problemas de optimización pola súa potencial vantaxe fronte aos métodos clásicos. Neste traballo introdúcense os fundamentos da computación cuántica, tanto os elementos básicos —o cúbit e o $p$-cúbit— como as portas cuánticas e o proceso de medición. A continuación, formúlanse problemas de optimización mediante hamiltonianos e descríbense os modelos QUBO e Ising. Explórase a computación adiabática (teorema adiabático) e introdúcese o Quantum Approximate Optimization Algorithm (QAOA). Detállase a arquitectura híbrida clásico-cuántica do Variational Quantum Eigensolver (VQE), os seus métodos de optimización variacional e as súas aplicacións prácticas. Finalmente, compárase o rendemento da computación clásica fronte á cuántica a través das clases de complexidade, discútese a vantaxe cuántica e explóranse as futuras liñas de investigación matemática nesta área.



## Abstract

In the field of quantum computing, there is considerable interest in leveraging quantum properties to solve optimization problems, due to their potential advantage over classical methods. This thesis introduces the fundamentals of quantum computing, covering both basic elements —the qubit and the $p$-qubit— as well as quantum gates and the measurement process. It then explores how optimization problems can be modeled using Hamiltonians, with particular focus on the QUBO and Ising models. The work delves into adiabatic quantum computing (adiabatic theorem) and presents the Quantum Approximate Optimization Algorithm (QAOA). It also details the hybrid classical–quantum architecture of the Variational Quantum Eigensolver (VQE), its variational optimization techniques, and practical applications. Finally, the performance of classical versus quantum computing is compared through complexity classes, the notion of quantum advantage is discussed, and future lines of mathematical research in this area are explored.

# Introdución

A computación cuántica é un área relativamente nova dentro da computación baseada nos principios da mecánica cuántica para abordar problemas que resultan intratables para os ordenadores clásicos. O obxectivo deste traballo é explicar os conceptos básicos que sustentan a computación cuántica e analizar algúns dos principais algoritmos no ámbito da optimización. Asúmese que o lector posúe coñecementos previos en álxebra lineal e en conceptos básicos de computación clásica, como o modelo de máquinas de Turing e a teoría da complexidade algorítmica.

No primeiro capítulo introdúcense os conceptos de cúbit e $p$-cúbit, describindo o formalismo matemático subxacente, os estados de superposición, o produto tensorial de espazos de Hilbert e o entrelazamento. A continuación, explícanse os circuítos cuánticos, presentándose as principais portas lóxicas de un e varios cúbits (como CNOT, SWAP e CCNOT) e o proceso de medición, que permite extraer a información dos sistemas cuánticos.

O segundo capítulo céntrase nos algoritmos cuánticos aplicados á optimización. Descríbese o hamiltoniano dun sistema cuántico e preséntanse os modelos QUBO e Ising, empregados na formulación de problemas combinatorios. Ademais, expónse o teorema adiabático, que xustifica a computación cuántica adiabática, e analízase o Quantum Approximate Optimization Algorithm (QAOA), ilustrando como se aplica en contextos reais.

O terceiro capítulo está dedicado ao algoritmo Variational Quantum Eigensolver (VQE), un dos algoritmos híbridos máis relevantes da computación cuántica actual. Abórdanse os seus fundamentos teóricos, o funcionamento da arquitectura híbrida clásica-cuántica e as súas aplicacións prácticas na actualidade.

Por último, o cuarto capítulo compara a computación clásica coa cuántica. Explícanse as clases de complexidade máis relevantes en ambos campos, discútese o concepto de vantaxe cuántica e analízanse as perspectivas futuras da computación cuántica, destacando o papel que ten a investigación matemática na súa evolución.

Ao longo do traballo, emprégase unha metodoloxía formal baseada en definicións matemáticas

rigorosas con exemplos ilustrativos cando é necesario. Por último, cabe destacar que a notación empregada neste traballo prioriza a claridade e a comprensión para quen se achega por primeira vez a esta disciplina. Este enfoque é especialmente axeitado para estudantes e investigadores con formación en matemáticas aplicadas, sen depender do coñecemento previo de física cuántica.

# Capítulo 1

# Introdución á computación cuántica

## 1.1. O concepto de cúbit e p-cúbit

### 1.1.1. Introdución á notación *braket*

O elemento básico da computación cuántica é o cúbit como unidade de información elemental. Para definilo, consideramos o plano complexo $\mathbb{C}^2$, que é un $\mathbb{C}$-espazo vectorial de dimensión dous. Ademais, introducimos a notación "*braket*" de Dirac:

$$\langle z| = \begin{pmatrix} \overline{z_1} & , & \overline{z_2} \end{pmatrix}, \quad |w\rangle = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}, \quad \text{para todo } \mathbf{z}, \mathbf{w} \in \mathbb{C}^2.$$

Desta forma, podemos entender o produto escalar de $\mathbf{z}$ e $\mathbf{w}$ como o produto matricial dos elementos $\langle z|$ e $|w\rangle$.

O produto escalar habitual en $\mathbb{C}^2$ defínese como:

$$\langle | \rangle : (\mathbf{z}, \mathbf{w}) \in \mathbb{C}^2 \times \mathbb{C}^2 \to \langle \mathbf{z} | \mathbf{w} \rangle = \sum_{j=1}^{2} \overline{z_j} w_j \in \mathbb{C}.$$

En particular, o par $(\mathbb{C}^2, \langle | \rangle)$ é un espazo de Hilbert.

Os vectores da base canónica

$$\mathbf{e_1} = |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathbf{e_2} = |2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

forman unha base ortonormal co respectivo produto escalar

Por definición de base, todo elemento $\Psi \in \mathbb{C}^2$ exprésase de forma única como combinación lineal dos elementos da base $B = \{\mathbf{e_1}, \mathbf{e_2}\} = \{|1\rangle, |2\rangle\}$. É dicir, existen $\alpha, \beta \in \mathbb{C}$ únicos tales que $|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle$.

### 1.1.2. Definición de cúbit

**Definición 1.1. (cúbit).** Denomínanse *cúbits* aos elementos unitarios do espazo $\mathbb{C}^2$, é dicir, aos elementos $|\Psi\rangle \in \mathbb{C}^2$ que satisfacen

$$\| \, |\Psi\rangle \, \| = \sqrt{\langle \Psi | \Psi \rangle} = 1.$$

Os elementos $|1\rangle, |2\rangle$ denomínanse *estados básicos computacionais*. Por tanto, un cúbit pódese expresar como combinación lineal destes estados básicos computacionais:

$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle, \quad \text{con} \quad |\alpha|^2 + |\beta|^2 = 1.$$

Como se verá máis adiante, o resultado de medir un cúbit $\Psi$ será un dos estados base $|1\rangle$ ou $|2\rangle$, con certas probabilidades determinadas polos coeficientes $\alpha$ e $\beta$. En concreto, a posibilidade de obter o resultado asociado a $|1\rangle$ é $|\alpha|^2$, e a de obter o resultado asociado a $|2\rangle$ é $|\beta\rangle$.

Cómpre destacar que, cando se mide un cúbit, non se accede directamente aos valores de $\alpha$ e $\beta$, senón que se obtén un dos posibles resultados observables. A interpretación e formalización precisa da medición cuántica será tratada con máis detalle na Sección 1.2.4 posterior.

### 1.1.3. Estados básicos e superposición

**Definición 1.2. (Estados básicos e superposición).** Dise que un cúbit $|\Psi\rangle$ está nun *estado básico* se se expresa como

$$|\Psi\rangle = \sum_{j \in \{1,2\}} \alpha_j |j\rangle$$

onde existe $k \in \{1, 2\}$ tal que $|\alpha_k| = 1$ e $\alpha_j = 0$ para todo $j \neq k$. En caso contrario, dise que o cúbit está nunha *superposición de estados*.

Esta definición esténdese, facendo as modificacións correspondentes, ao caso de sistemas con múltiples cúbits.

**Exemplo 1.3.** Un cúbit con estado en superposición é $|+\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle$, xa que ao medir o seu estado obtemos $|1\rangle$ ou $|2\rangle$ con probabilidade $\frac{1}{2}$ en ambos casos. Como explicamos antes, un cúbit é un vector unitario $\mathbb{C}^2$, que queda caracterizado polas súas coordenadas nos estados básicos $\alpha, \beta \in \mathbb{C}$, polo que farían falta catro parámetros reais para describir un. Sen embargo, a condición de normalización $|\alpha|^2 + |\beta|^2 = 1$ elimina un destes parámetros. Para ver isto explicitamente expresamos $\alpha$ e $\beta$ en forma polar de Euler:

$$\alpha = r_\alpha e^{i\theta_\alpha} \in \mathbb{C}, \qquad \beta = r_\beta e^{i\theta_\beta} \in \mathbb{C}.$$

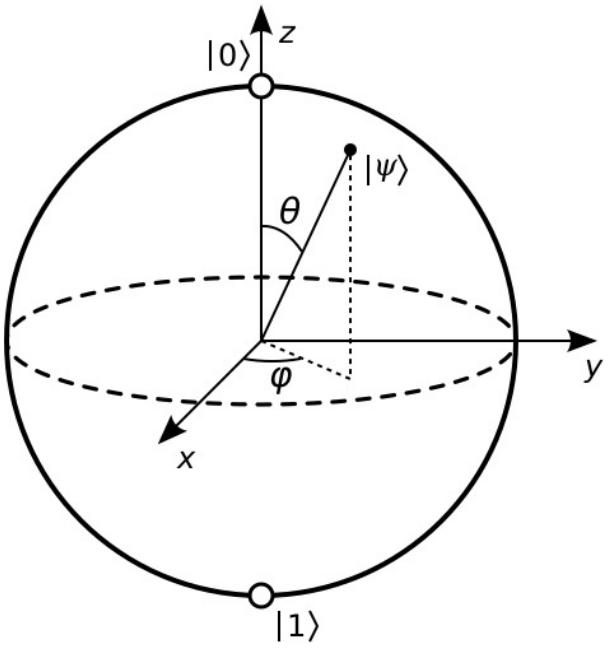



Figura 1.1: Esfera de Bloch. Fonte: Wikimedia Commons.

A condición de normalización $|\alpha|^2 + |\beta|^2 = r_\alpha^2 + r_\beta^2 = 1$ permítenos parametrizar os módulos como $r_\alpha = \cos\left(\frac{\theta}{2}\right)$ e $r_\beta = \text{sen}\left(\frac{\theta}{2}\right)$, para algún $\theta \in [0, \pi]$. Substituíndo na expresión do cúbit:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right) e^{i\theta_\alpha}|1\rangle + \text{sen}\left(\frac{\theta}{2}\right) e^{i\theta_\beta}|2\rangle, \quad \text{sendo} \quad \theta \in [0, \pi] \quad \text{e} \quad \theta_\alpha, \theta_\beta \in [0, 2\pi]$$

Podemos sacar factor común $e^{i\theta_\alpha}$ e eliminalo (posto que non ten efectos observables):

$$|\Psi\rangle = e^{i\theta_\alpha}\left(\cos\left(\frac{\theta}{2}\right)|1\rangle + e^{i(\theta_\beta - \theta_\alpha)}\,\text{sen}\left(\frac{\theta}{2}\right)|2\rangle\right) = \cos\left(\frac{\theta}{2}\right)|1\rangle + e^{i(\theta_\beta - \theta_\alpha)}\,\text{sen}\left(\frac{\theta}{2}\right)|2\rangle,$$

Desta forma, denotando por $\varphi = \theta_\beta - \theta_\alpha \in [0, 2\pi]$, temos que:

$$|\Psi\rangle = |\Psi(\theta, \varphi)\rangle = \cos\left(\frac{\theta}{2}\right)|1\rangle + e^{i\varphi}\,\text{sen}\left(\frac{\theta}{2}\right)|2\rangle.$$

**Exemplo 1.4.** Podemos identificar os parámetros $\theta \in [0, \pi]$ e $\varphi \in [0, 2\pi]$ con puntos da esfera unidade en $\mathbb{R}^3$, coñecida como *esfera de Bloch* (ver a Figura 1.1) mediante a relación:

$$(x, y, z) = (sen(\theta)cos(\varphi), sen(\theta)sen(\varphi), cos(\theta))$$

Cando $\theta = 0$ ou $\theta = \pi$, entón $sen(\theta) = 0$ e o valor de $\varphi$ non altera as coordenadas: para $\theta = 0$ obtense sempre $(0, 0, 1)$ e para $\theta = \pi$ sempre $(0, 0, -1)$. Isto explica como $(0, 0, 1) \equiv (\theta = 0, \varphi$ calquera) e de forma análoga no polo sur.

Os seguintes estados correspóndense con posicións concretas na esfera de Bloch:

- $|\Psi\rangle = cos(0)|1\rangle + e^{i\varphi} sen(0)|2\rangle = |1\rangle$ corresponde ao polo norte da esfera de Bloch, o punto $(0,0,1) \equiv (0,\varphi)$.
- $|\Psi\rangle = cos(\frac{\pi}{2})|1\rangle + e^{i\varphi} sen(\frac{\pi}{2})|2\rangle = |2\rangle$ corresponde ao polo sur da esfera de Bloch, o punto $(0,0,-1) \equiv (\pi,\varphi)$.
- $|\Psi\rangle = cos(\frac{\pi}{4})|1\rangle + e^{i0} sen(\frac{\pi}{4})|2\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle = |+\rangle$ corresponde ao punto $(1,0,0) \equiv (\frac{\pi}{2},0)$ no eixo x.
- $|\Psi\rangle = cos(\frac{\pi}{4})|1\rangle + e^{i\pi} sen(\frac{\pi}{4})|2\rangle = \frac{2}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|2\rangle = |-\rangle$ corresponde ao punto $(-1,0,0) \equiv (\frac{\pi}{2},\pi)$ no eixo x.
- $|\Psi\rangle = cos(\frac{\pi}{4})|1\rangle + e^{i\frac{\pi}{2}} sen(\frac{\pi}{4})|2\rangle = \frac{1}{\sqrt{2}}|1\rangle + i\frac{1}{\sqrt{2}}|2\rangle = |+i\rangle$ corresponde ao punto $(0,1,0) \equiv (\frac{\pi}{2},\frac{\pi}{2})$ no eixo y.
- $|\Psi\rangle = cos(\frac{\pi}{4})|1\rangle + e^{i\frac{3\pi}{2}} sen(\frac{\pi}{4})|2\rangle = \frac{1}{\sqrt{2}}|1\rangle - i\frac{1}{\sqrt{2}}|2\rangle = |-i\rangle$ corresponde ao punto $(0,-1,0) \equiv (\frac{\pi}{2},\frac{3\pi}{2})$ no eixo y.

**Exemplo 1.5.** Podemos identificar os parámetros $\theta \in [0,\pi]$ e $\varphi \in [0,2\pi)$ con puntos na esfera unidad en $\mathbb{R}^3$ (esfera de Bloch) mediante

$$(x,y,z) \;=\; (\operatorname{sen}\theta\cos\varphi,\ \operatorname{sen}\theta\operatorname{sen}\varphi,\ \cos\theta).$$

Obsérvese que, cando $\theta = 0$ ou $\theta = \pi$, entón $\operatorname{sen}\theta = 0$ e o valor de $\varphi$ non altera as coordenadas: para $\theta = 0$ obtense sempre $(0,0,1)$ e para $\theta = \pi$ sempre $(0,0,-1)$. Isto explica como $(0,0,1) \equiv (\theta = 0,\ \varphi \text{ calquera})$ e de forma análoga no pólo sur.

Cando $\theta = 0$ ou $\theta = \pi$, entón $\operatorname{sen}\theta = 0$ e o punto non depende de $\varphi$: para $\theta = 0$ sempre obtense $(0,0,1)$ e para $\theta = \pi$ sempre $(0,0,-1)$, de xeito que calquera $\varphi$ con $\theta = 0$ leva ao mesmo punto norte e de forma análoga ao punto sur.

Os seguintes estados corresponden a posicións concretas na esfera de Bloch:

- Para $\theta = 0$ calquera $\varphi$,

$$|\Psi\rangle = \cos(0)|1\rangle + e^{i\varphi}\operatorname{sen}(0)|2\rangle = |1\rangle,$$

  que corresponde ao pólo norte $(0,0,1)$.

- Para $\theta = \pi$ calquera $\varphi$,

$$|\Psi\rangle = \cos(\pi)|1\rangle + e^{i\varphi}\operatorname{sen}(\pi)|2\rangle = -|1\rangle \sim |2\rangle,$$

  que corresponde ao pólo sur $(0,0,-1)$ (a fase global non modifica o punto na esfera).

- $\theta = \frac{\pi}{2}, \varphi = 0$:

$$|\Psi\rangle = \cos\left(\tfrac{\pi}{4}\right)|1\rangle + e^{i0}\,\mathrm{sen}\left(\tfrac{\pi}{4}\right)|2\rangle = \tfrac{1}{\sqrt{2}}|1\rangle + \tfrac{1}{\sqrt{2}}|2\rangle = |+\rangle,$$

  corresponde a $(1, 0, 0)$.

- $\theta = \frac{\pi}{2}, \varphi = \pi$:

$$|\Psi\rangle = \cos\left(\tfrac{\pi}{4}\right)|1\rangle + e^{i\pi}\,\mathrm{sen}\left(\tfrac{\pi}{4}\right)|2\rangle = \tfrac{1}{\sqrt{2}}|1\rangle - \tfrac{1}{\sqrt{2}}|2\rangle = |-\rangle,$$

  corresponde a $(-1, 0, 0)$.

- $\theta = \frac{\pi}{2}, \varphi = \frac{\pi}{2}$:

$$|\Psi\rangle = \cos\left(\tfrac{\pi}{4}\right)|1\rangle + e^{i\frac{\pi}{2}}\,\mathrm{sen}\left(\tfrac{\pi}{4}\right)|2\rangle = \tfrac{1}{\sqrt{2}}|1\rangle + i\,\tfrac{1}{\sqrt{2}}|2\rangle = |+i\rangle,$$

  corresponde a $(0, 1, 0)$.

- $\theta = \frac{\pi}{2}, \varphi = \frac{3\pi}{2}$:

$$|\Psi\rangle = \cos\left(\tfrac{\pi}{4}\right)|1\rangle + e^{i\frac{3\pi}{2}}\,\mathrm{sen}\left(\tfrac{\pi}{4}\right)|2\rangle = \tfrac{1}{\sqrt{2}}|1\rangle - i\,\tfrac{1}{\sqrt{2}}|2\rangle = |-i\rangle,$$

  corresponde a $(0, -1, 0)$.

Os sistemas físicos con múltiples cúbits descríbense mediante o produto tensorial de espazos de Hilbert. Como os cúbits individuais son elementos do espazo de Hilbert $\mathbb{H} := \mathbb{C}^2$, un sistema con $p$-cúbits represéntase no espazo tensorial $\mathbb{C}^{2^p} \equiv \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.

### 1.1.4. Definición de $p$-cúbit

**Definición 1.6. (p-cúbit).** Un *p-cúbit* é un elemento unitario do espazo $\mathbb{C}^{2^p}$, é dicir, un elemento $|\Psi\rangle \in \mathbb{C}^{2^{\otimes p}}$ que satisfai:

$$\| \, |\Psi\rangle \, \| = \sqrt{\langle \Psi | \Psi \rangle} = 1.$$

Para describir sistemas cuánticos con múltiples cúbits, é fundamental entender o concepto de produto tensorial. Sexan $(\mathbb{H}^A, \langle \, | \, \rangle^A)$ e $(\mathbb{H}^B, \langle \, | \, \rangle^B)$ dous espazos de Hilbert. Defínese o produto tensorial $\mathbb{H}^A \otimes \mathbb{H}^B$ como o espazo vectorial complexo xerado polas aplicacións $\psi : \mathbb{H}^A \times \mathbb{H}^B \to \mathbb{C}$ que son antilineais e continuas. Dados $|\varphi\rangle \in \mathbb{H}^A$ e $|\Psi\rangle \in \mathbb{H}^B$, a aplicación correspondente defínese como:

$$|\varphi\rangle \otimes |\Psi\rangle \colon \mathbb{H}^A \times \mathbb{H}^B \to \mathbb{C}, \quad (\xi, \eta) \mapsto \langle \xi | \varphi \rangle^A \langle \eta | \Psi \rangle^B$$

onde $|\varphi\rangle \otimes |\Psi\rangle$ pertence ao espazo $\mathbb{H}^A \times \mathbb{H}^B$, e adoita escribirse como $|\varphi \otimes \Psi\rangle$.

O produto escalar no espazo tensorial defínese unicamente a partir dos produtos escalares nos factores, de modo que cumpra que se $|\varphi_1\rangle, |\varphi_2\rangle \in \mathbb{H}^A$ e $|\Psi_1\rangle, |\Psi_2\rangle \in \mathbb{H}^B$, entón:

$$\langle \varphi_1 \otimes \Psi_1 \,|\, \varphi_2 \otimes \Psi_2 \rangle := \langle \varphi_1 | \varphi_2 \rangle^A \cdot \langle \Psi_1 | \Psi_2 \rangle^B.$$

e esténdese por linealidade no segundo argumento e antilinealidade no primeiro a todo $\mathbb{H}^A \times \mathbb{H}^B$.

Tomando dúas bases ortonormais $\{|e_a\rangle\} \subset \mathbb{H}^A$ e $\{|f_b\rangle\} \subset \mathbb{H}^B$, constrúese unha base ortonormal do espazo tensorial mediante os vectores $\{|e_a\rangle \otimes |f_b\rangle\}$. Calquera vector $|\Psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ pode escribirse como:

$$|\Psi\rangle = \sum_{a,b} \Psi_{ab} \, |e_a \otimes f_b\rangle, \quad \text{con} \quad \sum_{a,b} |\Psi_{ab}|^2 < \infty,$$

onde a norma e o produto escalar quedan definidos como:

$$\| |\Psi\rangle \|^2 = \langle \Psi | \Psi \rangle = \sum_{a,b} |\Psi_{ab}|^2, \qquad \text{respectivamente} \qquad \langle \Psi | \Phi \rangle = \sum_{a,b} \overline{\Psi_{ab}} \, \Phi_{ab}.$$

**Proposición 1.7.** *Dadas dúas bases ortonormais $\{|e_a\rangle\} \subset \mathbb{H}^A$ e $\{|f_b\rangle\} \subset \mathbb{H}^B$, o conxunto $\{|e_a\rangle \otimes |f_b\rangle\}$ forma unha base ortonormal de $\mathbb{H}^A \otimes \mathbb{H}^B$ e, para espazos vectoriais de dimensión finita $\mathbb{H}^A$ e $\mathbb{H}^B$ tense que:*

$$\dim(\mathbb{H}^A \otimes \mathbb{H}^B) = \dim \mathbb{H}^A \cdot \dim \mathbb{H}^B.$$

Dado un espazo de Hilbert complexo $\mathbb{H}$ podemos identificar calquera base ortonormal $\{|e_j\rangle\} \subset \mathbb{H}$ coa base canónica de $\mathbb{C}^n$.

Queremos extender esta identificación ao produto tensorial de dous espazos de Hilbert $\mathbb{H}^A \otimes \mathbb{H}^B$, con $\dim(\mathbb{H}^X) = n_X < \infty$, para $X \in \{A, B\}$. Sexan $\{|e_a\rangle\} \subset \mathbb{H}^A$ e $\{|f_b\rangle\} \subset \mathbb{H}^B$ dúas bases ortonormais. Se identificamos $\mathbb{H}^X \simeq \mathbb{C}^{n_X}$, con $X \in \{A, B\}$, pódese establecer un isomorfismo $\mathbb{H}^A \otimes \mathbb{H}^B \simeq \mathbb{C}^{n_A n_B}$ identificando a base $\{|e_a \otimes f_b\rangle\} \subset \mathbb{H}^A \otimes \mathbb{H}^B$ coa base canónica en $\mathbb{C}^{n_A n_B}$.

Cada vector canónico de $\mathbb{C}^{n_A n_B}$ ten todas as compoñentes nulas, excepto a que ocupa a posición $(a-1)n_B + b$, onde vale 1. A continuación móstranse algúns exemplos e a forma xenérica:

$$|e_1 \otimes f_1\rangle = \begin{pmatrix} 1 \\ 2 \\ \vdots \\ \vdots \\ n_A n_B \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}, \quad |e_1 \otimes f_2\rangle = \begin{pmatrix} 1 \\ 2 \\ \vdots \\ \vdots \\ n_A n_B \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}, \ldots,$$

$$|e_a \otimes f_b\rangle = \begin{pmatrix} 1 \\ \vdots \\ \vdots \\ (a-1)n_B + b \\ \vdots \\ \vdots \\ n_A n_B \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |e_{n_A} \otimes f_{n_B}\rangle = \begin{pmatrix} 1 \\ 2 \\ \vdots \\ \vdots \\ n_A n_B \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 1 \end{pmatrix}$$

Así, un vector xenérico $|\Psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ pode escribirse como:

$$|\Psi\rangle = \sum_{a=1}^{n_A} \sum_{b=1}^{n_B} \Psi_{ab} |e_a \otimes f_b\rangle = \begin{pmatrix} 1 \\ \vdots \\ (a-1)n_B + b \\ \vdots \\ n_A n_B \end{pmatrix} \begin{pmatrix} \Psi_{11} \\ \vdots \\ \Psi_{ab} \\ \vdots \\ \Psi_{n_A n_B} \end{pmatrix}$$

Para o caso dun sistema cuántico composto por dous cúbits e $\mathbb{H}^A = \mathbb{H}^B = \mathbb{C}^2$ coas bases ortonormais:

$$\{|e_a\rangle\} = \{|f_b\rangle\} = \{|1\rangle, |2\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

*Observación* 1.8. Ao estar traballando con bases ortonormais estándar en espazos $\mathbb{C}^n$, o produto tensorial coincide co denominado *produto de Kronecker*, que representa explicitamente en coordenadas a operación $\otimes$. Supongamos que temos dous estados:

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle, \quad |\phi\rangle = \beta_1|1\rangle + \beta_2|2\rangle$$

O produto tensorial destes dous estados cálculase desta forma:

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \end{pmatrix} = \alpha_1\beta_1|11\rangle + \alpha_1\beta_2|12\rangle + \alpha_2\beta_1|21\rangle + \alpha_2\beta_2|22\rangle \in (\mathbb{C}^2)^{\otimes 2} \equiv \mathbb{C}^4$$

Así, se ten que o produto de dous estados cuánticos representados por 1-cúbit é un estado cuántico de 2-cúbits:

$$|\alpha_1\beta_1|^2 + |\alpha_1\beta_2|^2 + |\alpha_2\beta_1|^2 + |\alpha_2\beta_2|^2 = |\alpha_1|^2(|\beta_1|^2 + |\beta_2|^2) + |\alpha_2|^2(|\beta_1|^2 + |\beta_2|^2) = |\alpha_1|^2 + |\alpha_2|^2 = 1$$

Para $\mathbb{H}^A \otimes \mathbb{H}^B \simeq \mathbb{C}^4$ temos a base ortonormal:

$$\{|e_A \otimes f_B\rangle\} = \{|11\rangle, |12\rangle, |21\rangle, |22\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Por tanto un 2-cúbit $\Psi \in \mathbb{C}^4$ pode expresarse como combinación dos catro estados básicos anteriores:

$$|\Psi\rangle = \alpha_{11}|11\rangle + \alpha_{12}|12\rangle + \alpha_{21}|21\rangle + \alpha_{22}|22\rangle, \quad \text{con} \quad |\alpha_{11}|^2 + |\alpha_{12}|^2 + |\alpha_{21}|^2 + |\alpha_{22}|^2 = 1$$

De forma análoga ao caso dun único cúbit, non podemos obter o estado cuántico dun 2-cúbit (valores de $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$), senón que obtemos o estado $|11\rangle$ con probabilidade $|\alpha_{11}^2|$, o estado $|12\rangle$ con probabilidade $|\alpha_{12}^2|$, etc.

Para $\mathbb{H}^A = \mathbb{H}^B = \mathbb{H}^C = \mathbb{C}^2$, $\mathbb{H}^A \otimes \mathbb{H}^B \otimes \mathbb{H}^C \simeq \mathbb{C}^8$ temos a base ortonormal:

$$\{|e_A \otimes f_B \otimes g_c\rangle\} = \{|111\rangle, |112\rangle, |121\rangle, |122\rangle, |211\rangle, |212\rangle, |221\rangle, |222\rangle\}$$

Por tanto, un 3-cúbit $\Psi \in \mathbb{C}^4$ pode expresarse como:

$$|\Psi\rangle = \alpha_{111}|111\rangle + \alpha_{112}|112\rangle + \alpha_{121}|121\rangle + \alpha_{122}|122\rangle + \alpha_{211}|211\rangle + \alpha_{212}|212\rangle + \alpha_{221}|221\rangle + \alpha_{222}|222\rangle,$$
$$\text{con} \quad |\alpha_{111}|^2 + |\alpha_{112}|^2 + |\alpha_{121}|^2 + |\alpha_{122}|^2 + |\alpha_{211}|^2 + |\alpha_{212}|^2 + |\alpha_{221}|^2 + |\alpha_{222}|^2 = 1$$

*Notación* 1.9. Segundo aumentamos o número de p-cúbits dun sistema cuántico faise máis tedioso traballar con esta notación. Por este motivo hai outras notacións que simplifican a escritura. Un p-cúbit $|\Psi\rangle \in \mathbb{C}^{2^p}$ pode expresarse como combinación lineal de $2^p$ estados básicos:

$$|\Psi\rangle = \sum_{\vec{j} \in \{1,2\}^p} \alpha_{\vec{j}} |\vec{j}\rangle, \quad \text{con} \sum_{\vec{j} \in \{1,2\}^p} |\alpha_{\vec{j}}|^2 = 1$$

Ao traballar con sistemas cuánticos cun gran número de bits, é útil identificar os estados básicos do sistema utilizando a súa representación binaria. Se numeramos os $2^p$ estados básicos 1 a $2^p$:

$$\begin{aligned}
|1\rangle_p &= |0 \cdot 2^{p-1} + 0 \cdot 2^{p-2} + \cdots + 0 \cdot 2^1 + 0 \cdot 2^0\rangle_p = |00 \cdots 000\rangle, \\
|2\rangle_p &= |0 \cdot 2^{p-1} + 0 \cdot 2^{p-2} + \cdots + 0 \cdot 2^1 + 1 \cdot 2^0\rangle_p = |00 \cdots 001\rangle, \\
|3\rangle_p &= |0 \cdot 2^{p-1} + 0 \cdot 2^{p-2} + \cdots + 1 \cdot 2^1 + 0 \cdot 2^0\rangle_p = |00 \cdots 010\rangle, \\
|4\rangle_p &= |0 \cdot 2^{p-1} + 0 \cdot 2^{p-2} + \cdots + 1 \cdot 2^1 + 1 \cdot 2^0\rangle_p = |00 \cdots 011\rangle, \\
&\vdots \\
|2^p - 1\rangle_p &= |1 \cdot 2^{p-1} + 1 \cdot 2^{p-2} + \cdots + 1 \cdot 2^1 + 0 \cdot 2^0\rangle_p = |11 \cdots 110\rangle, \\
|2^p\rangle_p &= |1 \cdot 2^{p-1} + 1 \cdot 2^{p-2} + \cdots + 1 \cdot 2^1 + 1 \cdot 2^0\rangle_p = |11 \cdots 111\rangle,
\end{aligned}$$

Dado $j \in \{1, ..., 2^p\}$, $|j\rangle_p = |\vec{j}\rangle = |\vec{j_1}...\vec{j_p}\rangle$ onde o bit $\vec{j_1}$ é o máis significativo (pois multiplica a $2^p$). Así, o estado cuántico dun $p$-cúbit $|\Psi\rangle$ pódese expresar como:

$$|\Psi\rangle = \sum_{\vec{j}\in\{0,1\}^p} \alpha_{\vec{j}}|\vec{j}\rangle = \sum_{j=1}^{2^p} \alpha_j |j\rangle_p$$

### 1.1.5. Estado produto e entrelazamento

**Definición 1.10. (Estado produto e entrelazamento).** Un $p$-cúbit $|\Psi\rangle \in (\mathbb{C}^2)^{\otimes p}$ é un *estado produto* se pode escribirse como o produto tensorial de $p$ estados de 1-cúbit $\{|\Psi_k\rangle\}_{k=1}^p$:

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \cdots \otimes |\Psi_p\rangle = \bigotimes_{k=1}^{p} |\Psi_k\rangle$$

En caso contrario, diremos que o estado está *entrelazado*.

*Observación* 1.11. Pódese comprobar que un 2-cúbit $|\Psi\rangle = \alpha_{11}|11\rangle + \alpha_{12}|12\rangle + \alpha_{21}|21\rangle + \alpha_{22}|22\rangle$ pódese expresar como o produto tensorial de dous 1-cúbit se, e soamente se, cumpre a condición de entrelazamento:

$$\alpha_{11}\alpha_{22} = \alpha_{12}\alpha_{21}$$

Isto implica que o conxunto de estados cuánticos representables con $q$-cúbits é máis amplo que o conxunto de estados produto de $q$ estados de 1-cúbit.

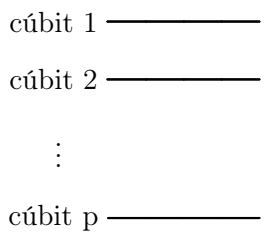
**Exemplo 1.12.** O 2-cúbit $|\Psi\rangle = \frac{1}{2}|11\rangle + \frac{1}{2}|12\rangle + \frac{1}{2}|21\rangle + \frac{1}{2}|22\rangle$ é un estado produto, xa que cumpre a condición de entrelazamento. De feito, pódese escribir como:

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle, \quad \text{onde} |\Psi_1\rangle = |\Psi_2\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle$$

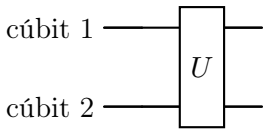
Por outro lado, o 2-cúbit $|\Psi\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|22\rangle$ está entrelazado, xa que non cumpre a condición (por tanto, non pode escribirse como o produto tensorial de dous 1-cúbit.

## 1.2. Circuítos cuánticos

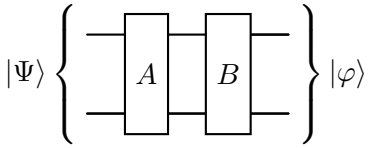
O elemento fundamental para describir e executar algoritmos cuánticos é o circuíto cuántico. Un circuíto é unha rutina computacional composta por unha secuencia ordenada de portas lóxicas, medicións e reinicios cuánticos. Nos circuítos cuánticos, cada cúbit represéntase cunha liña horizontal, de forma que o cúbit 1 se indica na liña superior e o resto enuméranse en orde descendente.



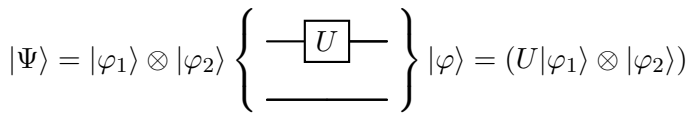

As operacións ou portas cuánticas represéntanse sobre estas liñas, actuando sobre os cúbits indicados. A dirección de lectura é de esquerda a dereita (xa que cada operación se corresponde cunha matriz unitaria), polo que a secuencia de portas lóxicas representa o fluxo temporal das operacións.



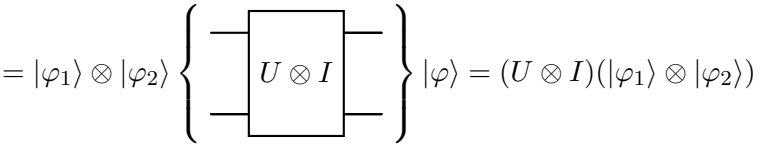

**Exemplo 1.13.** No seguinte circuíto primeiro aplicamos a porta A ao 2-cúbit $|\Psi\rangle$ e despois a porta B ao 2-cúbit $A|\Psi\rangle$. Obtemos entón $|\varphi\rangle = BA|\Psi\rangle$.




No seguinte circuíto aplicamos a porta U ao cúbit $|\varphi_1\rangle$ (enténdese que no resto aplicamos o operador identidade). Obtemos entón $|\varphi\rangle = (U|\varphi_1\rangle \otimes |\varphi_2\rangle)$.




Este circuíto é equivalente ao anterior: $(U|\varphi_1\rangle \otimes |\varphi_2\rangle) = (U \otimes I)(|\varphi_1\rangle \otimes |\varphi_2\rangle)$.




### 1.2.1. Portas lóxicas cuánticas de 1 cúbit

**Definición 1.14. (Porta lóxica para un cúbit).** Denomínase *porta lóxica para un cúbit* a unha matriz unitaria $U \in \mathcal{M}_{2\times 2}(\mathbb{C})$ con $U^\dagger U = UU^\dagger = I$. Esta condición garante que son operadores lineais reversibles que non alteran a norma do estado cuántico.

*Observación* 1.15. O feito de que dous estados cuánticos difiran nunha fase global é indistinguible ao ser medidos. En termos da esfera de Bloch, isto implica que

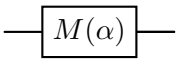
$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle \quad \text{e} \quad |\varphi\rangle = e^{i\theta}(\alpha|1\rangle + \beta|2\rangle)$$

presentan os mesmos resultados ao ser medidos, xa que $|e^{i\theta}| = 1$. Desta forma, dada unha porta lóxica $U$, non se observan diferenzas entre $U|\Psi\rangle$ e $U|\varphi\rangle$.

As portas lóxicas máis importantes para un só cúbit expresadas en termos dos estados básicos $\{|1\rangle, |2\rangle\}$ son as seguintes:

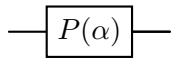
- Factor de fase (Phase-factor)

$$M(\alpha) := e^{i\alpha}1 = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$




- Desprazamento de fase (Phase-shift)

$$P(\alpha) := |1\rangle\langle 1| + e^{i\alpha}|2\rangle\langle 2| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + e^{i\alpha}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

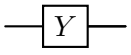



- Matriz de Pauli X (Pauli-X o Q-NOT):

$$X \equiv \sigma_x := |1\rangle\langle 2| + |2\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

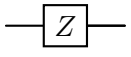

- Matriz de Pauli Y (Pauli-Y):

$$Y \equiv \sigma_y := -i|1\rangle\langle 2| + i|2\rangle\langle 1| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$




- Matriz de Pauli Z (Pauli-Z):

$$Z \equiv \sigma_z := |1\rangle\langle 1| - |2\rangle\langle 2| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



- Porta de Hadamard:

$$H := \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$$


**Exemplo 1.16.** Certas portas lóxicas correspóndense con movementos ríxidos da esfera de Bloch. No caso da porta Pauli-X:

$$|1\rangle \text{ —[X]— } |2\rangle \text{ transforma } |\Psi(0,\varphi)\rangle \text{ en } |\Psi(\pi,\varphi)\rangle$$

$$|+\rangle \text{ —[X]— } |+\rangle \text{ deixa invariante } \left|\Psi\left(\frac{\pi}{2},0\right)\right\rangle$$

$$|-\rangle \text{ —[X]— } |-\rangle \text{ deixa invariante } \left|\Psi\left(\frac{\pi}{2},\pi\right)\right\rangle$$

$$|+i\rangle \text{ —[X]— } |-i\rangle \text{ transforma } \left|\Psi\left(\frac{\pi}{2},\frac{\pi}{2}\right)\right\rangle \text{ en } \left|\Psi\left(\frac{\pi}{2},\frac{3\pi}{2}\right)\right\rangle$$

$$|-i\rangle \text{ —[X]— } |+i\rangle \text{ transforma } \left|\Psi\left(\frac{\pi}{2},\frac{3\pi}{2}\right)\right\rangle \text{ en } \left|\Psi\left(\frac{\pi}{2},\frac{\pi}{2}\right)\right\rangle$$

Desta forma, a porta Pauli-X correspóndese cunha rotación de 180° con respecto ao eixo X na esfera de Bloch. Analogamente, a porta Pauli-Y cunha rotación de 180° con respecto ao eixo Y, a porta Pauli-Z cunha rotación de 180° con respecto ao eixo Z e a porta de Hadamard cunha rotación de 180° con respecto ao eixo X+Z.

Todas as portas cuánticas pódense expresar mediante unha matriz parametrizada que describe de forma xeral calquera operador unitario. Ademais, é posible aproximar calquera matriz unitaria cun nivel de precisión arbitrario utilizando unha secuencia finita de portas $H$, $P(\pi/4)$ e $CNOT$.

$$U(\theta,\varphi,\lambda) = \begin{pmatrix} e^{-i(\varphi+\lambda)/2}cos(\theta/2) & -e^{-i(\varphi-\lambda)/2}sen(\theta/2) \\ e^{i(\varphi-\lambda)/2}sen(\theta/2) & e^{-i(\varphi+\lambda)/2}cos(\theta/2) \end{pmatrix}$$

### 1.2.2. Portas lóxicas cuánticas para múltiples cúbits

De modo análogo ao caso dun cúbit, unha porta lóxica para un circuíto con $p$ cúbits coma un operador unitario.

**Definición 1.17. (porta lóxica para un p-cúbit).** Denomínase *porta lóxica para un p-cúbit* a calquera matriz $U \in \mathbb{M}_{2^p \times 2^p}(\mathbb{C})$ tal que $U^\dagger U = UU^\dagger = I_{2^p}$, onde $U^\dagger$ representa a matriz conxugada complexa de $U$.

A construción de portas lóxicas para múltiples cúbits realízase mediante o produto tensorial de portas lóxicas para un ou varios cúbits. Na observación 1.11, establecíamos unha regra para obter o produto tensorial de dous cúbits; esta operación pode estenderse ao caso de operadores lóxicos sobre cúbits.

**Definición (Produto de Kronecker).** Dadas dúas matrices $A \in \mathcal{M}_{m\times n}(\mathbb{C})$ e $B \in \mathcal{M}_{p\times q}(\mathbb{C})$ defínese o *produto de Kronecker* $A \otimes B \in \mathcal{M}_{mp\times nq}(\mathbb{C})$ como:

$$A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ a_{21}B & \cdots & a_{2n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$$

É fundamental coñecer algunhas propiedades do produto tensorial para describir portas lóxicas definidas sobre sistemas formados por varios cúbits.

**Proposición 1.18.** *Dados $A, B \in \mathcal{M}_{m\times m}$, $C, D \in \mathcal{M}_{n\times n}$, $u, v \in \mathbb{C}^m$, $w, x \in \mathbb{C}^n$ e $a, b \in \mathbb{C}$. Entón:*

1. $(A \otimes C)(B \otimes D) = AB \otimes CD$
2. $(A \otimes C)(u \otimes w) = Au \otimes Cw$
3. $(u + v) \otimes w = u \otimes w + v \otimes w$
4. $u \otimes (w + x) = u \otimes w + u \otimes x$
5. $(au) \otimes (bw) = ab(u \otimes w)$
6. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

Ao facer o produto tensorial dun operador lineal A consigo mesmo n veces, úsase a notación:

$$A^{\otimes n} := \underbrace{A \otimes \cdots \otimes A}_{n \text{ veces}}$$

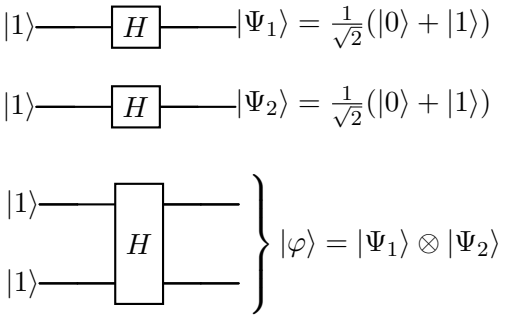
**Corolario 1.19.** *Sexan $U \in \mathcal{M}_{2^p\times 2^p}(\mathbb{C})$ e $V \in \mathcal{M}_{2^q\times 2^q}(\mathbb{C})$ dous operadores unitarios. Entón:*

1. *$U \otimes V$ é un operador unitario no espazo $\mathcal{M}_{2^{p+q}\times 2^{p+q}}$*
2. *Para calquera par de estados $|\Psi\rangle_p$ e $|\varphi\rangle_q$, temos:*

$$(U \otimes V)(|\Psi\rangle_p \otimes |\varphi\rangle_q) = (U|\Psi\rangle_p \otimes V|\varphi\rangle_q)$$

**Exemplo 1.20.** Se consideramos un circuíto cuántico formado por dous cúbits que están inicialmente no estado $|1\rangle \otimes |1\rangle$ e aplicamos a porta de Hadamard, $H^{\otimes 2} = H \otimes H$, sobre cada cúbit, tense:

$$|\varphi\rangle := H^{\otimes 2}(|1\rangle \otimes |1\rangle) = (H|1\rangle) \otimes (H|1\rangle)$$




Vexamos que os dous circuítos anteriores son equivalentes.

No primeiro circuíto estamos calculando $(H|1\rangle) \otimes (H|1\rangle)$:

$$\begin{aligned}(H|1\rangle) \otimes (H|1\rangle) &= \left(\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)\right) \\ &= \frac{1}{2}|1\rangle \otimes |1\rangle + \frac{1}{2}|1\rangle \otimes |2\rangle + \frac{1}{2}|2\rangle \otimes |1\rangle + \frac{1}{2}|2\rangle \otimes |2\rangle \\ &= \frac{1}{\sqrt{2^2}}(|11\rangle + |12\rangle + |21\rangle + |22\rangle) = \frac{1}{\sqrt{2^2}} \sum_{\vec{j} \in \{1,2\}^2} |\vec{j}\rangle = \frac{1}{\sqrt{2^2}} \sum_{j=1}^{2^2} |j\rangle_2\end{aligned}$$

No segundo circuíto estamos calculando $H^{\otimes 2}|11\rangle$. Como:

$$H^{\otimes 2} = H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Entón:

$$H^{\otimes 2}|00\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}(|11\rangle + |12\rangle + |21\rangle + |22\rangle)$$

Este procedemento xeneralízase facilmente a p-cúbits. Se o sistema se atopa inicialmente no estado $|1\rangle^{\otimes p}$, entón:

$$H^{\otimes p}|\vec{0}\rangle = H^{\otimes p}|0\rangle^{\otimes p} = (H|0\rangle)^{\otimes p} = \left(\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)\right)^{\otimes p} = \frac{1}{\sqrt{2^p}} \sum_{\vec{j} \in \{1,2\}^p} |\vec{j}\rangle = \frac{1}{\sqrt{2^p}} \sum_{j=1}^{2^p} |j\rangle_p$$

recuperando desta forma unha superposición uniforme dos $n = 2^p$ estados básicos do sistema formado por $p$-cúbits.

### 1.2.3. Portas cuánticas compostas: CNOT, SWAP, CCNOT

En sistemas con múltiples cúbits, non todas as portas lóxicas poden ser representadas polo produto tensorial de portas individuais. A continuación descríbense algunhas das máis relevantes:

**1. Porta CNOT (NOT controlada)** Esta porta actúa en sistemas 2-cúbit, onde un é o cúbit de control e o outro, o obxectivo. Se o cúbit de control é $|1\rangle$, a porta non altera ao cúbit obxectivo; se é $|2\rangle$, invirte o estado $|1\rangle \leftrightarrow |2\rangle$ no cúbit obxectivo. Adoitan incluírse dous subíndices para indicar cal é o cúbit e cal o obxectivo. Por exemplo, $CNOT_{12}$ indica que o primeiro cúbit é o de control e o segundo o obxectivo, e $CNOT_{21}$ ao revés.

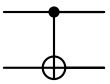
- Porta $CNOT_{12}$:

$$\begin{aligned}
CNOT_{12}|11\rangle &= CNOT_{12}(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |1\rangle = |11\rangle,\\
CNOT_{12}|12\rangle &= CNOT_{12}(|1\rangle \otimes |2\rangle) = |1\rangle \otimes |2\rangle = |12\rangle,\\
CNOT_{12}|21\rangle &= CNOT_{12}(|2\rangle \otimes |1\rangle) = |2\rangle \otimes |1\rangle = |21\rangle,\\
CNOT_{12}|22\rangle &= CNOT_{12}(|2\rangle \otimes |2\rangle) = |2\rangle \otimes |2\rangle = |22\rangle.
\end{aligned}$$

E ten a matriz asociada:

$$CNOT_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Notación para a porta $CNOT_{12}$:



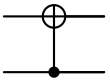
- Porta $CNOT_{21}$:

$$\begin{aligned}
CNOT_{21}|11\rangle &= CNOT_{21}(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |1\rangle = |11\rangle,\\
CNOT_{21}|12\rangle &= CNOT_{21}(|1\rangle \otimes |2\rangle) = |2\rangle \otimes |2\rangle = |22\rangle,\\
CNOT_{21}|21\rangle &= CNOT_{21}(|2\rangle \otimes |1\rangle) = |2\rangle \otimes |1\rangle = |21\rangle,\\
CNOT_{21}|22\rangle &= CNOT_{21}(|2\rangle \otimes |2\rangle) = |1\rangle \otimes |2\rangle = |12\rangle.
\end{aligned}$$

E ten a matriz asociada:

$$CNOT_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Notación para a porta $CNOT_{21}$:



**2. Porta SWAP** Esta porta actúa sobre sistemas de 2-cúbits (aínda que pode estenderse a máis cúbits) intercambiando os valores de ambos cúbits en calquera estado cuántico, de forma que os dixitos dos estados base permútanse entre si.

$$\begin{aligned} \text{SWAP}|11\rangle &= |11\rangle, \\ \text{SWAP}|12\rangle &= |12\rangle, \\ \text{SWAP}|21\rangle &= |21\rangle, \\ \text{SWAP}|22\rangle &= |22\rangle. \end{aligned}$$

E ten matriz asociada:

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

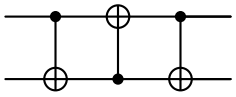
Notación para a porta SWAP:

Vexamos como actúa a porta SWAP sobre o produto tensorial de dous estados $|\Psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle$ e $|\varphi\rangle = \beta_1|1\rangle + \beta_2|2\rangle$:

$$\begin{aligned} \text{SWAP}(|\Psi\rangle \otimes |\varphi\rangle) &= \text{SWAP}((\alpha_1|1\rangle + \alpha_2|2\rangle) \otimes (\beta_1|1\rangle + \beta_2|2\rangle)) \\ &= \text{SWAP}(\alpha_1\beta_1|11\rangle + \alpha_1\beta_2|12\rangle + \alpha_2\beta_1|21\rangle + \alpha_2\beta_2|22\rangle) \\ &= \alpha_1\beta_1|11\rangle + \alpha_1\beta_2|21\rangle + \alpha_2\beta_1|12\rangle + \alpha_2\beta_2|22\rangle \\ &= (\beta_1|1\rangle + \beta_2|2\rangle) \otimes (\alpha_1|1\rangle + \alpha_2|2\rangle) = |\varphi\rangle \otimes |\Psi\rangle. \end{aligned}$$

Ademais, a porta SWAP pode implementarse como a composición $\text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12}$:

$$\begin{aligned} \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12}|11\rangle &= \text{CNOT}_{12}\text{CNOT}_{21}|11\rangle = \text{CNOT}_{12}|11\rangle = |11\rangle, \\ \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12}|12\rangle &= \text{CNOT}_{12}\text{CNOT}_{21}|12\rangle = \text{CNOT}_{12}|22\rangle = |21\rangle, \\ \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12}|21\rangle &= \text{CNOT}_{12}\text{CNOT}_{21}|22\rangle = \text{CNOT}_{12}|12\rangle = |12\rangle, \\ \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12}|22\rangle &= \text{CNOT}_{12}\text{CNOT}_{21}|21\rangle = \text{CNOT}_{12}|21\rangle = |22\rangle. \end{aligned}$$



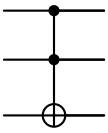
**3. Porta CCNOT (NOT dobremente controlada** Actúa en sistemas 3-cúbit, de forma que se os dous primeiros cúbits son iguais a $|1\rangle$, invértese o terceiro; en caso contrario, non altera o estado:

$$\begin{aligned}
\text{CCNOT}|111\rangle &= |111\rangle,\\
\text{CCNOT}|112\rangle &= |112\rangle,\\
\text{CCNOT}|121\rangle &= |121\rangle,\\
\text{CCNOT}|122\rangle &= |122\rangle,\\
\text{CCNOT}|211\rangle &= |211\rangle,\\
\text{CCNOT}|212\rangle &= |212\rangle,\\
\text{CCNOT}|221\rangle &= |222\rangle,\\
\text{CCNOT}|222\rangle &= |221\rangle.
\end{aligned}$$

E ten matriz asociada:

$$\text{CCNOT} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

Notación para a porta CCNOT:



Outra maneira de definir a porta CCNOT é mediante a seguinte expresión:

$$\text{CCNOT}(|x\rangle \otimes |y\rangle \otimes |z\rangle) = |x\rangle \otimes |y\rangle \otimes |z \otimes (x \cdot y)\rangle,$$

onde $x, y, z \in \{0, 1\}$ e $\otimes$ denota a suma módulo 2. Este comportamento implica que, se o terceiro cúbit está inicialmente no estado $|1\rangle$, o seu valor final será $x \cdot y$, reproducindo así a operación lóxica clásica AND.

$$\text{CCNOT}(|x\rangle \otimes |y\rangle \otimes |0\rangle) = |x\rangle \otimes |y\rangle \otimes |x \cdot y\rangle,$$

### 1.2.4. Medición cuántica

A diferenza do caso dos ordenadores clásicos, nos que podemos acceder ao valor dos bits directamente, nun ordenador cuántico non se ten acceso sen restricións ao estado cuántico dun determinado cúbit. A única forma de acceder á información sobre o estado cuántico é mediante unha porta de medida (que devolve resultados de natureza probabilista).

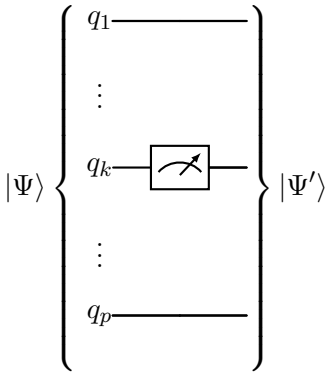
**Definición 1.21. (Porta de medida).** Dado un $p$-cúbit $|\Psi\rangle = \sum_{\vec{j}\in\{1,2\}} \alpha_{\vec{j}}|\vec{j}\rangle$, unha *porta de medida* sobre o cúbit k proporciona:

- O valor 0, cunha probabilidade:
$$\sum_{\vec{j}\in\{1,2\}^p : j_k=1} |\alpha_{\vec{j}}|^2$$
- O valor 1, cunha probabilidade:
$$\sum_{\vec{j}\in\{1,2\}^p : j_k=2} |\alpha_{\vec{j}}|^2$$

Tras a medición, o estado cuántico resultante $|\Psi'\rangle$ depende do valor medido $x \in \{1,2\}$, e vén dado por:

$$|\Psi'\rangle = \sum_{\vec{j}\in\{1,2\}^p \,:\, j_k=x} \frac{\alpha_{\vec{j}}}{\sqrt{\sum_{\vec{j}\in\{1,2\}^p \,:\, j_k=x} |\alpha_{\vec{j}}|^2}} |\vec{j}\rangle$$

O estado cuántico resultante colapsa, tras a medición, a unha combinación lineal dos estados básicos que son coherentes co resultado da medición (os estados $|\vec{j}\rangle$ tales que $j_k = x$). Os coeficientes desta combinación lineal normalízanse para obter un vector unitario.




**Exemplo 1.22.** Consideremos o estado $|\Psi\rangle = \alpha_{11}|11\rangle + \alpha_{12}|12\rangle + \alpha_{21}|21\rangle + \alpha_{22}|22\rangle$.

- Se se mide o primeiro cúbit, o resultado é:

- O valor 0, con probabilidade $|\alpha_{11}|^2 + |\alpha_{12}|^2$ e o estado resultante é:

$$|\Psi'\rangle = \frac{\alpha_{11}|11\rangle + \alpha_{12}|12\rangle}{\sqrt{|\alpha_{11}|^2 + |\alpha_{12}|^2}}$$

- O valor 1, con probabilidade $|\alpha_{21}|^2 + |\alpha_{22}|^2$ e o estado resultante é:

$$|\Psi'\rangle = \frac{\alpha_{21}|21\rangle + \alpha_{22}|22\rangle}{\sqrt{|\alpha_{21}|^2 + |\alpha_{22}|^2}}$$

- Se se mide o segundo cúbit, o resultado é:

  - O valor 0, con probabilidade $|\alpha_{11}|^2 + |\alpha_{21}|^2$ e o estado resultante é:

$$|\Psi'\rangle = \frac{\alpha_{11}|11\rangle + \alpha_{21}|21\rangle}{\sqrt{|\alpha_{11}|^2 + |\alpha_{21}|^2}}$$

  - O valor 1, con probabilidade $|\alpha_{12}|^2 + |\alpha_{22}|^2$ e o estado resultante é:

$$|\Psi'\rangle = \frac{\alpha_{12}|12\rangle + \alpha_{22}|22\rangle}{\sqrt{|\alpha_{12}|^2 + |\alpha_{22}|^2}}$$

*Observación* 1.23. Consideremos o exemplo anterior. Se medimos o primeiro cúbit do estado $|\Psi\rangle = \alpha_{11}|11\rangle + \alpha_{12}|12\rangle + \alpha_{21}|21\rangle + \alpha_{22}|22\rangle$ a probabilidade de obter 0 é $|\alpha_{11}|^2 + |\alpha_{12}|^2$ e o resultado tras a medición é:

$$|\Psi'\rangle = \frac{\alpha_{11}|11\rangle + \alpha_{12}|12\rangle}{\sqrt{|\alpha_{11}|^2 + |\alpha_{12}|^2}}$$

A continuación, se medimos o segundo cúbit, obtemos o valor 0 con probabilidade $\frac{|\alpha_{11}|^2}{|\alpha_{11}|^2+|\alpha_{12}|^2}$ e o estado post-medición é:

$$|\Psi''\rangle = |11\rangle$$

Por tanto, a probabilidade conxunta de obter o estado $|11\rangle$ tras as dúas medicións é:

$$(|\alpha_{11}|^2 + |\alpha_{12}|^2)\frac{|\alpha_{11}|^2}{|\alpha_{11}|^2 + |\alpha_{12}|^2} = |\alpha_{11}|^2$$

Vexamos se a orde na que se realizan as medicións altera este resultado. Supongamos que medimos primeiro o segundo cúbit en primeiro lugar. A probabilidade de obter o valor 0 é $|\alpha_{11}|^2 + |\alpha_{21}|^2$ e o resultado tras a medición é:

$$|\Psi'\rangle = \frac{\alpha_{11}|11\rangle + \alpha_{21}|21\rangle}{\sqrt{|\alpha_{11}|^2 + |\alpha_{21}|^2}}$$

A continuación, se medimos o primeiro cúbit, obtemos o valor 0 con probabilidade $\frac{|\alpha_{11}|^2}{|\alpha_{11}|^2+|\alpha_{21}|^2}$ e o estado post-medición é:

$$|\Psi''\rangle = |11\rangle$$

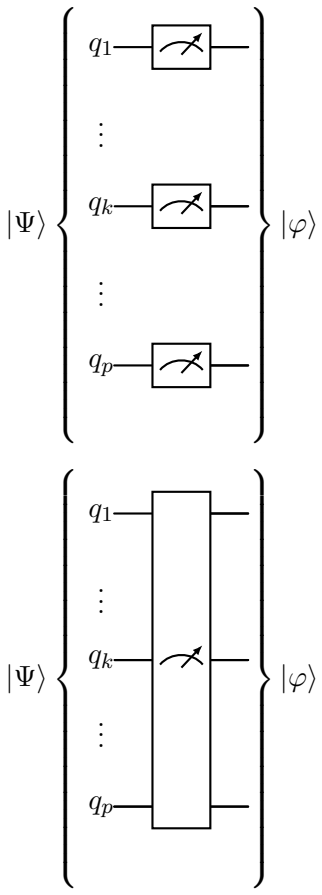
Por tanto, a probabilidade de obter o estado $|11\rangle$ tras as dúas medicións é:

$$(|\alpha_{11}|^2 + |\alpha_{21}|^2)\frac{|\alpha_{11}|^2}{|\alpha_{11}|^2 + |\alpha_{21}|^2} = |\alpha_{11}|^2$$

Desta forma, a orde das medicións non afecta nin ao estado final nin á probabilidade. Ademais, esta propiedade pódese xeneralizar a sistemas de múltiples cúbits. Dado un $p$-cúbit:

$$|\Psi\rangle = \sum_{\vec{j}\in\{1,2\}^p} \alpha_{\vec{j}}|\vec{j}\rangle$$

aplicar portas de medida sobre cada un dos $p$ cúbits, en calquera orde, dá como resultado o estado $|\vec{j}\rangle$ con probabilidade $|\alpha_{\vec{j}}|^2, \forall\ \vec{j} \in \{1,2\}^p$. En consecuencia, os circuítos cuánticos que só se diferencian na orde das medicións son equivalentes. Deste xeito, un circuíto que mide cada cúbit por separado e un que realiza todas as medicións ao mesmo tempo son equivalentes:




No primeiro circuíto, cada cúbit $q_i$ mídese cunha porta de medida na súa liña (poderíase ler en calquera orde porque cada medición actúa sobre un cúbit distinto). En cambio, no segundo, mídese simultaneamente un bloque de $p$ cúbits. Como non hai dependencia entre as medicións, ambas representacións son equivalentes.

**Exemplo 1.24.** Para exemplificar a medida en 2-cúbits, considérese o seguinte caso. Sexan os estados

$$|\Psi\rangle = \frac{1}{2}|11\rangle + \frac{1}{2}|12\rangle + \frac{1}{2}|21\rangle + \frac{1}{2}|22\rangle, \quad |\varphi\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|22\rangle$$

Para estudar a medida nestes $p$-cúbits, denotamos por $Pr_{|\Psi\rangle}(Q_k \overset{M}{=} x)$, que indica a probabilidade de que o cúbit $k \in \{1, \dots, p\}$ do $p$-cúbit $|\Psi\rangle$ tome o valor $x \in \{1, 2\}$

- Caso 1: Estado produto $|\Psi\rangle$.

$$Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 1) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$
$$Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 2) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$
$$Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 1) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$
$$Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 2) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$

  A continuación, se medimos o segundo cúbit e obtemos o valor 1, o estado post-medición é:

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}|12\rangle + \frac{1}{\sqrt{2}}|22\rangle$$

  E temos, que a distribución da probabilidade do primeiro cúbit non cambia:

$$Pr_{|\Psi'\rangle}(Q_1 \overset{M}{=} 1) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$
$$Pr_{|\Psi'\rangle}(Q_1 \overset{M}{=} 2) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

- Caso 2: Estado entrelazado $|\varphi\rangle$.

$$Pr_{|\varphi\rangle}(Q_1 \overset{M}{=} 1) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$
$$Pr_{|\varphi\rangle}(Q_2 \overset{M}{=} 2) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$
$$Pr_{|\varphi\rangle}(Q_1 \overset{M}{=} 1) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$
$$Pr_{|\varphi\rangle}(Q_2 \overset{M}{=} 2) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$$

  A continuación, se medimos o segundo cúbit e obtemos o valor 1, o estado post-medición é:

$$|\varphi'\rangle = |22\rangle$$

E temos, que a distribución da probabilidade do primeiro cúbit si que cambia, a medida sobre un dos cúbits afecta directamente ao estado do outro:

$$Pr_{|\varphi'\rangle}(Q_1 \overset{M}{=} 1) = 1$$
$$Pr_{|\varphi'\rangle}(Q_1 \overset{M}{=} 2) = 2$$

*Observación* 1.25. Dado un 2-cúbit $|\Psi\rangle$, podemos determinar se é un estado entrelazado empregando probabilidades condicionadas:

- Se $|\Psi\rangle$ pódese expresar como o produto tensorial de dous 1-cúbit (é dicir, non está entrelazado), tense que:

$$Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} x) = Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} x | Q_1 \overset{M}{=} y), \quad \forall x, y \in \{1, 2\}$$

- En cambio, se:

$$\exists x, y \in \{1, 2\}, \text{ tal que } \quad Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} x) \neq Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} x | Q_1 \overset{M}{=} y),$$

  entón $|\Psi\rangle$ non se pode expresar como produto tensorial de dous 1-cúbit (é dicir, está entrelazado).

Demostremos isto. Supongamos que $|\Psi\rangle$ é un 2-cúbit que se pode expresar como produto tensorial de dous 1-cúbits:

$$|\Psi\rangle = (\alpha_1|1\rangle + \alpha_2|2\rangle) \otimes (\beta_1|1\rangle + \beta_2|2\rangle) = \alpha_1\beta_1|11\rangle + \alpha_1\beta_2|12\rangle + \alpha_2\beta_1|21\rangle + \alpha_2\beta_2|22\rangle$$

Tense que:

$$Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 1) = |\alpha_1\beta_1|^2 + |\alpha_1\beta_2|^2 = |\alpha_1|^2 \implies |\Psi'\rangle = \frac{\alpha_1\beta_1|11\rangle + \alpha_1\beta_2|12\rangle}{\sqrt{Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 1)}}$$
$$Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 2) = |\alpha_2\beta_1|^2 + |\alpha_2\beta_2|^2 = |\alpha_2|^2 \implies |\Psi'\rangle = \frac{\alpha_2\beta_1|21\rangle + \alpha_2\beta_2|22\rangle}{\sqrt{Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 2)}}$$
$$Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 1) = |\alpha_1\beta_1|^2 + |\alpha_2\beta_1|^2 = |\beta_1|^2 \implies |\Psi'\rangle = \frac{\alpha_1\beta_1|11\rangle + \alpha_2\beta_1|21\rangle}{\sqrt{Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 1)}}$$
$$Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 2) = |\alpha_1\beta_2|^2 + |\alpha_2\beta_2|^2 = |\beta_2|^2 \implies |\Psi'\rangle = \frac{\alpha_1\beta_2|12\rangle + \alpha_2\beta_2|22\rangle}{\sqrt{Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 2)}}$$

Entón:

$$Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 1 | Q_1 \overset{M}{=} 1) = \frac{|\alpha_0\beta_0|^2}{Pr_{|\Psi\rangle}(Q_1 \overset{M}{=} 1)} = |\beta_0|^2 = Pr_{|\Psi\rangle}(Q_2 \overset{M}{=} 1)$$

*Observación* 1.26. (O principio de non clonación). Como ao realizar medicións destrúese o estado cuántico, sería útil realizar unha copia ou clon do estado para poder recuperalo tras as operacións. Sen embargo, isto non é posible, xa que non existe unha matriz unitaria $U \in \mathcal{M}_{2^{2^p}\times 2^{2^p}}$ que transforme o estado $|\Psi\rangle \otimes |0\rangle_p$ no estado $|\Psi\rangle \otimes |\Psi\rangle_p$. Supongamos que si existe e temos:

$$U(|\Psi\rangle \otimes |0\rangle_p) = |\Psi\rangle \otimes |\Psi\rangle, \quad U(|\varphi\rangle \otimes |0\rangle_p) = |\varphi\rangle \otimes |\varphi\rangle \quad \text{para calquera para de } p\text{-cúbits } |\Psi\rangle \text{ e } |\varphi\rangle$$

Entón:

$$\begin{aligned}\langle\varphi|\Psi\rangle = \langle\varphi|\Psi\rangle\langle 0|_p|0\rangle_p = \langle\varphi|\Psi\rangle \otimes (\langle 0|_p|0\rangle_p) = (\langle\varphi| \otimes \langle 0|_p) \otimes (|\Psi\rangle \otimes |0\rangle_p) \\ = (\langle\varphi| \otimes \langle 0|_p)U^\dagger U(|\Psi\rangle \otimes |0\rangle_p) = (\langle\varphi| \otimes \langle\varphi|)(|\Psi\rangle \otimes |\Psi\rangle) = \langle\varphi|\Psi\rangle^2\end{aligned}$$

E isto só se cumpre se $\langle\varphi|\Psi\rangle \in \{1, 0\}$, o cal é unha contradición con que $|\Psi\rangle$ e $|\varphi\rangle$ sexan arbitrarios.

Aínda que non se pode clonar un determinado cúbit, si se pode realizar unha copia limitada que axuda a replicar información para aumentar a probabilidade de éxito dos algoritmos que se empreguen. É posible construír unha matriz unitaria $C_p \in \mathcal{M}_{2^{2^p}\times 2^{2^p}}(\mathbb{C}),$ con $p \geq 1$ tal que:

$$\text{Dado } |a'\rangle = \sum_{\vec{j},\vec{k}\in\{1,2\}^p} a'_{\vec{j}\vec{k}}|\vec{j}\vec{k}\rangle \in \mathbb{C}^{2^{2^p}}, \quad \text{tense } C_p|a'\rangle = |b\rangle \quad \text{onde } b_{\vec{j}\vec{k}} = a'_{\vec{j}\otimes(\vec{j}\otimes\vec{k})}.$$

Se $|a'\rangle = |a\rangle \otimes |0\rangle_p$, entón: $a_{\vec{j}} = a'_{\vec{j}\vec{0}} = b_{\vec{j}\vec{j}}$. Así, temos que a propabilidade de obter $|\vec{j}\vec{j}\rangle$ ao medir $|b\rangle$ e a mesma que a de obter $|\vec{j}\rangle$ ao medir $|a\rangle$. Desta forma, se $|a\rangle = |\vec{i}\rangle$, con $\vec{i} \in \{1, 2\}^p$ é un estado básico, tense que $|b\rangle = |a\rangle \otimes |a\rangle$. Sen embargo, se $|a\rangle$ non é un estado básico, non se ten por que cumprir $C_p(|a\rangle \otimes |0\rangle_p) = |a\rangle \otimes |a\rangle$. Por exemplo:

$$\text{Se } |a\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle, \quad \text{entón} \quad C_1(|a\rangle \times |0\rangle) = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|22\rangle \neq |a\rangle \otimes |a\rangle = \frac{1}{2}\sum_{\vec{j}\in\{1,2\}^p} |\vec{j}\rangle$$

# Capítulo 2

# Algoritmos cuánticos para optimización

Os algoritmos cuánticos nos problemas de optimización teñen como obxectivo atopar o estado óptimo dun sistema cuántico entre un conxunto de posibles solucións. Estes problemas baséanse na minimización (respectivamente maximización) dunha función coñecida como obxectivo que está asociada á enerxía dun sistema físico.

Por este motivo, introdúcese o operador hamiltoniano que describe a enerxía do sistema. Tense que o seu estado fundamental (o de menor enerxía) contén a solución óptima do problema.

## 2.1. O hamiltoniano dun sistema cuántico

Para resolver un problema de optimización de $p$ variables binarias, en primeiro lugar, defínese unha función obxectivo $f$. Esta función asóciase a un operador que describe a enerxía do sistema e que se coñece como *hamiltoniano*.

Partimos dun estado inicial de $H$, $|\Psi_0\rangle$, que é sinxelo de construír (por exemplo, unha superposición uniforme ou un *ansatz* básico) e o estado obxectivo, $|\Psi_1\rangle$, é o estado fundamental de $H$ (que codifica a solución óptima do problema).

Existen dous enfoques principais para aproximarse ao estado obxectivo:

1. Método adiabático (explicado máis en detalle na Sección 2.4): tómase un hamiltoniano inicial $H_0$ con estado inicial $|H_0\rangle$ e defínese unha evolución ao hamiltoniano final $H$. Se a evolución é suficientemente lenta, o sistema mantense no estado de mínima enerxía en todo momento, polo que ao final do proceso o estado do sistema está moi próximo ao estado fundamental de $H$, $\Psi_1$.
2. Método variacional (explicado máis en detalle nas Seccións 2.5, 3): tómase un estado me-

diante un circuíto cuántico que depende dun conxunto de parámetros. A evolución defínese a partir dunha combinación dos hamiltonianos $H_0$ e $H$. Mídese a enerxía esperada $\langle\Psi|H|\Psi\rangle$ do sistema e axústanse os parámetros cun algoritmo clásico para minimizar esa enerxía, aproximando así o estado tomado inicial ao estado fundamental $\Psi_1$.

Para transformar un problema de optimización de $p$ variables, nun definido no espazo de Hilbert de dimensión $2^p$, partimos da ecuación de Schrödinger que describe a evolución unitaria:

$$i\hbar\frac{\partial}{\partial t}|\Psi\rangle(t) = H|\Psi\rangle(t), \tag{2.1}$$

onde $\hbar$ é a constante de Planck reducida.

Se o hamiltoniano $H$ é independente do tempo, tense que a solución da ecuación de Schrödinger 2.1 é:

$$|\Psi\rangle(t) = \exp(-\frac{i}{\hbar}tH)|\Psi\rangle(0)$$

e, por ser $H$ autoadxunto (é igual ao seu conxugado trasposto: $H = H^\dagger$), o operador $\exp(-\frac{i}{\hbar}tH)$ é unitario. O obxectivo é que, tras a evolución (por exemplo en $t = T$ no método adiabático), $|\Psi(T)\rangle$ se aproxime a $|\Psi_1\rangle$.

Como un problema con $p$ variables binarias represéntase con $p$ cúbits, ao transportalo ao espazo de Hilbert, o hamiltoniano do problema terá dimensión $2^p \times 2^p$. Este feito fai inviable almacenar todos os coeficientes de $H$. Sen embargo, é posible traballar coa súa avaliación sobre estados $|\Psi\rangle$, pois é posible implementar operacións como $\exp(iH)|\Psi\rangle$ mediante o produto de portas cuánticas (matrices unitarias).

## 2.2. O modelo QUBO

Un problema común de optimización é o coñecido como tipo QUBO (*Quadratic Unconstrained Binary Optimization*):

$$\text{Dado } Q \in \mathcal{M}_{p\times p}(\mathbb{R}), \text{ atopar un vector } \vec{x} \in \{0,1\}^p \text{ que minimiza } \vec{x}^t Q\vec{x}.$$

Ao tratarse dun problema de optimización de combinatoria, no peor dos casos, haberá que avaliar e comparar as $2^p$ combinacións binarias posibles de $\vec{x}$. Dita solución pode expresarse como un vector de $p$ bits (ceros e uns). Empregaremos a notación indicada en Notación 1.9, por exemplo, o vector $\vec{j} = |100\rangle$ como solución dun problema QUBO con $p = 3$.

Na computación clásica, dado que a solución do problema correspóndese cun vector de $p$ bits, definir o problema só require $p^2$ coeficientes, que se corresponden cos valores da matriz $Q$.

En contraposición, no enfoque cuántico o rexistro reside nun estado $|\Psi\rangle \in (\mathbb{C}^2)^{\otimes p}$, que se expresa como combinación lineal dos estados base $|\vec{j}\rangle$, con $j \in \{0,1\}^p$, da mesma dimensión $2^p$.

## 2.3. O modelo Ising

O modelo Ising é un modelo de ferromagnetismo da mecánica estatística. Utilízase para describir partículas que interaccionan entre si e se sitúan nunha malla. Para estudar a evolución do sistema cuántico é necesario definir o seu hamiltoniano (o que permitirá, por exemplo, calcular o seu estado de mínima enerxía).

Se consideramos $p$ partículas situadas nos vértices V dun grafo, tal que as súas interaccións se representan polas aristas E. Temos que cada partícula $j$ posúe un spin $s_j \in \{-1, 1\}$, de forma que $\vec{s} = (s_j)_{j \in V}$ é a *configuración de spin*. A enerxía correspondente a esa configuración do sistema vén dada pola expresión:

$$H|\vec{s}\rangle = -\sum_{(i,j)\in E} J_{ij} s_i s_j - \sum_{j \in V} h_j s_j$$

onde $J_{ij}$ representa a interacción entre as partículas dos vértices $i$ e $j$, e $(h_j)_{j\in V}$ é un campo magnético externo que actúa sobre cada partícula do grafo.

Desta forma, podemos converter un problema QUBO ao modelo Ising empregando o cambio de variable:

$$x_j = \frac{1 - s_j}{2}$$

Desde a perspectiva cuántica, cada configuración de spin $\vec{s} \in \{-1, 1\}^p$ asóciase a un estado $|\vec{s}\rangle \in (\mathbb{C}^2)^{\otimes p}$. Deste xeito, aplicando sobre $|\vec{s}\rangle$ o hamiltoniano adecuado, obtense a enerxía do sistema. No caso do sistema Ising, o hamiltoniano pódese expresar como unha combinación de produtos tensoriais de matrices unitarias como:

$$H|\vec{s}\rangle = -\sum_{(i,j)\in E} J_{ij} \bigotimes_{k=1}^{p} M_{ij}^k - \sum_{j=1} h_j \bigotimes_{k=1}^{p} M_j^k$$

$$\text{onde} \qquad M_{ij}^k = \begin{cases} \sigma_z & \text{se } k = i \text{ ou } k = j, \\ I & \text{noutro caso} \end{cases}, \qquad M_j^k = \begin{cases} \sigma_z & \text{se } k = j, \\ I & \text{noutro caso} \end{cases}$$

e $\sigma_z$ é a matriz de Pauli $Z$ e $I$ é a matriz identidade de dimensión $2 \times 2$.

Entón o hamiltoniano descríbese como unha suma de matrices unitarias e esta descomposición permite construír circuítos cuánticos sobre os que se poden aplicar algoritmos cuánticos. Calquera hamiltoniano con interaccións locais admite unha formulación deste tipo. Ademais, a identidade de Trotter-Suzuki permite a aproximación da suma anterior polo produto de matrices unitarias (facilitando a súa implementación como circuíto cuántico):

$$e^{it\sum_j H_j} = \lim_{m\to\infty} \left( \prod_j e^{\frac{iH_j}{m}} \right)^m . \tag{2.2}$$

## 2.4. Teorema adiabático e computación cuántica adiabática

A computación cuántica adiabática baséase no teorema adiabático, que foi formulado por Born e Fock, e establece que, se un sistema cuántico evoluciona de xeito suficientemente lento no tempo, este permanece no seu estado de mínima enerxía (estado fundamental) durante toda a evolución.

Desta maneira, se se coñece o estado de mínima enerxía $|\Psi_0\rangle$ dun hamiltoniano inicial $H_0$ e se quere calcular o estado de mínima enerxía doutro hamiltoniano $H_1$, pódese interpolar entre ambos hamiltonianos e definir un novo que depende do tempo:

$$H(t) = \left(1 - \frac{t}{T}\right) H_0 + \frac{t}{T} H_1, \quad \text{con } 0 \leq t \leq T.$$

Segundo o teorema, se o tempo total $T$ é suficientemente grande, entón o sistema evolucionará desde o estado inicial $|\Psi_0\rangle$ ata un estado moi próximo ao estado fundamental de $H_1$, que contén a solución do problema que se quere resolver.

Canto máis pequena é a separación enerxética existente entre os dous estados de menor enerxía do hamiltoniano (coñecida como *gap*), maior ten que ser o tempo total $T$ para garantir unha correcta evolución adiabática.

Outro enfoque distinto á computación baseada en portas lóxicas (na que se inclúen os algoritmos que se tratan neste traballo) é a *computación cuántica adiabática*, que emprega este principio como mecanismo de cálculo.

Esta relación inversamente proporcional entre o *gap* e o tempo total requerido T é a base das máquinas cuánticas adiabáticas como as chamadas *quantum annealers* (ou *máquinas de temple cuántico*), como a desenvolvida pola compañía D-Wave. Estas máquinas utilízanse para atopar o estado fundamental dun hamiltoniano asociado ao problema de optimización.

Aínda que non se inclúen exemplos baseados neste modelo no traballo, algunhas aplicacións que teñen os quantum annealers na actualidade son:

- Problemas Lineais de Enteros Mixtos (MILP), cun esquema híbrido clásico-cuántico aplicados á optimización dunha refinería.
- Problemas reais como o tempo de difusión ou a planificación de talleres.
- Métodos híbridos inspirados na xeración de columnas en Investigación Operativa.
- Problemas NP-completos en hipergrafos e instancias aleatorias.
- Clasificación binaria e adestramento de clasificadores a gran escala.

- Avaliación de funcións de partición e mostreo de estados de Gibbs.
- Estudo das transicións de fase, condicións adiabáticas e tempo de colisión en cadeas de Markov.

## 2.5. *Quantum Approximate Optimization Algorithm* (QAOA)

O algoritmo *Quantum Approximate Optimization Algorithm* (QAOA) baséase na idea do algoritmo cuántico adiabático (ver Sección 2.4), onde un hamiltoniano evoluciona ao longo do tempo. En lugar diso, neste caso substitúese o tempo por un parámetro $\alpha \in [0,1]$, que define unha interpolación entre dous hamiltonianos:

$$H(\alpha) = (1-\alpha)H_0 + \alpha H,$$

sendo $H_0$ o hamiltoniano inicial e $H$ o hamiltoniano que codifica o problema a resolver. A evolución xerada por $H(\alpha)$ vén dada por $e^{-iH(\alpha)}$.

Para poder aproximar esta evolución dependente de $\alpha$, divídese o intervalo $[0,1]$ en pequenos segmentos nos que se supón que $H(\alpha)$ é constante (de xeito análogo á definición dunha integral de Riemann). Deste xeito, cada segmento define un operador unitario (que se pode implementar como unha porta cuántica) e a evolución total pódese expresar mediante unha descomposición tipo Trotter (ver ecuación 2.2) como produto de exponenciais.

A implementación do algoritmo comeza cun estado inicial $|\Psi_0\rangle$, ao que se lle aplica o hamiltoniano inicial $H_0$ e que actúa aplicándolle a porta Pauli-$X$ a cada un dos cúbits. A continuación, en cada un dos $p$ pasos aplícanse dous operadores exponenciais: un xerado por $H$ con parámetros $\vec{\gamma} = (\gamma_k)$ e outro xerado por $H_0$ con parámetros $\vec{\beta} = (\beta_k)$ e con $k \in \{1, \dots, p\}$. Así, obtense o estado final:

$$|\Psi\rangle_{\vec{\beta},\vec{\gamma}} = \left( \prod_{k \in \{p, p-1, \dots, 1\}} e^{-i\beta_k H_0} e^{-i\gamma_k H} \right) |\Psi_0\rangle.$$

Ao realizar a medición deste estado final, a probabilidade de que sexa a solución óptima aumenta grazas ao deseño dos parámetros $\vec{\beta}$ e $\vec{\gamma}$. A obtención dos valores óptimos dos parámetros lévase a cabo cun algoritmo de optimización clásico resolvendo o problema:

$$(\vec{\beta}^*, \vec{\gamma}^*) = \arg\max_{\vec{\beta},\vec{\gamma}} \langle \Psi|_{\vec{\beta},\vec{\gamma}} H |\Psi\rangle_{\vec{\beta},\vec{\gamma}}.$$

Para realizar esta elección adoitan empregarse técnicas de optimización como o de descenso de gradiente, temple simulado ou estratexias que parten desde múltiples puntos iniciais.

Este algoritmo foi deseñado nun inicio para resolver problemas de optimización combinatoria, nos que se busca a solución óptima entre un conxunto finito pero moi amplo de posibilidades. Moitos destes problemas inclúense na clase NP-completos.

O QAOA compórtase como unha versión discretizada do temple cuántico (ou *Quantum Annealing*), que é un proceso de optimización no que se busca o mínimo global dunha función obxectivo a través de flutuacións cuánticas. No temple cuántico, o sistema parte dunha superposición uniforme de todos os estados posibles e evoluciona segundo a ecuación de Schrödinger (2.1). As flutuacións cuánticas producen o efecto túnel, que permite que un estado poida cruzar barreiras de potencial e escapar de mínimos locais. Se a variación do hamiltoniano é suficientemente lenta, o sistema permanece próximo ao estado fundamental en cada instante; en cambio, se é rápida, pódense producir transicións con maior probabilidade de acadar o estado fundamental do hamiltoniano final.

A semellanza estrutural entre o QAOA e o temple cuántico permite entender o primeiro como unha versión programable mediante portas cuánticas deste último. Discretizar a evolución do sistema e controlala mediante parámetros $\beta_k, \gamma_k$ facilita empregar posteriormente os procesos de optimización clásicos.

Na actualidade, a potencia de QAOA en comparación á computación clásica ou outros algoritmos cuánticos continúa sendo obxecto de estudo. Por exemplo, se o número de parámetros que hai que determinar no algoritmo (coñecido como profundidade) é $p = 1$, non existe unha forma eficiente de simular QAOA de forma clásica. Sen embargo, isto non implica que non existan algoritmos clásicos que poidan resolver os mesmos problemas eficientemente. Ademais, o rendemento de QAOA depende en grande medida do problema específico. Por exemplo, no problema de corte máximo dun grafo requírense centos de cúbits para que sexa competitivo fronte a métodos clásicos (como se pode ver en [6]). Esta limitación motivou o desenvolvemento de variantes do algoritmo para resolver o problema concreto en máquinas cun número de cúbits baixo, que aínda así permiten obter resultados útiles en certos contextos (como se pode ver en [21], [22]).

# Capítulo 3

# Algoritmo *Variational Quantum Eigensolver* (VQE)

## 3.1. Fundamentos do algoritmo VQE.

O algoritmo VQE (*Variational Quantum Eigensolver*) está deseñado para calcular o menor autovalor $E_0$ e o seu autovector asociado dun hamiltoniano $H$. Este método baséase no *principio variacional* que establece que, para todo estado $|\Psi\rangle$:

$$\langle\Psi|H|\Psi\rangle \geq E_0\langle\Psi|\Psi\rangle$$

Para atopar o estado que minimiza a enerxía (que é o menor autovalor $E_0$), introdúcese unha representación parametrizada do estado (coñecida como *ansatz*) que permite recorrer un subespazo do espazo de Hilbert $(\mathbb{C}^2)^{\otimes n}$. A elección deste *ansatz* é determinante para o rendemento do algoritmo e, por tanto, para a converxencia do método.

## 3.2. Arquitectura híbrida e optimización.

Un dos obxectivos fundamentais da mecánica cuántica é o cálculo do menor autovalor dun hamiltoniano e do seu autovector asociado. Isto é clave, por exemplo, para determinar o estado fundamental dun sistema físico.

Unha das vantaxes que ten o VQE é que pode empregar representacións parametrizadas que os ordenadores clásicos non poden simular eficientemente. Existe un exemplo no que o crecemento do algoritmo é polinómico respecto ao tamaño do rexistro en cúbits (como se pode ver en [15]).

Debido a que o algoritmo require optimizar os parámetros do *ansatz* para minimizar a enerxía esperada, é fundamental empregar un método de optimización axeitado. Ademais, debido á natureza estocástica intrínseca das medicións en mecánica cuántica, cómpre repetir os experimentos múltiples veces para estimar os valores esperados con precisión suficiente (como se pode ver na Subsección 4.1.2).

O algoritmo VQE (*Variational Quantum Eigensolver*) permite aproximar o estado fundamental dun hamiltoniano mediante a minimización do valor esperado da enerxía ($\langle\Psi|H|\Psi\rangle$). O enfoque híbrido deste algoritmo híbrido é similar ao de QAOA na idea de combinar parte cuántica e clásica. Sen embargo, no VQE deseñase o *ansatz* para aproximar directamente o estado fundamental, mentres que en QAOA este defínese alternando evolucións do tipo $e^{-i\beta_k H_0}$ e $e^{-i\gamma_k H}$ sobre o estado inicial $H_0$ (como se pode ver na Sección 2.5).

O algoritmo VQE (*Variational Quantum Eigensolver*) permite aproximar o autovector correspondente ao estado fundamental mediante a minimización do valor esperado da enerxía ($\langle\Psi|H|\Psi\rangle$). Para levar a cabo esta tarefa, propónse unha representación parametrizada do estado (coñecida como *ansatz*) que permite recorrer un subespazo do espazo de Hilbert asociado ao problema.

Este algoritmo combina, por unha banda, un sistema cuántico para xerar os estados e calcular os valores esperados, e por outra, a optimización dos parámetros do *ansatz* mediante un algoritmo de computación clásica. Polo tanto, inclúese no enfoque de computación híbrida.

Non obstante, existen algúns desafíos para empregar este algoritmo, especialmente ao empregar técnicas de optimización baseadas no cálculo de gradientes. No espazo de optimización existen múltiples mínimos locais que o VQE non evita, dificultando a obtención do estado fundamental. Ademais, existen rexións nas que os gradientes son practicamente nulos (coñecidas como *barren plateaus*), o que dificulta aínda máis o proceso de optimización (como se pode ver en [1], [5], [9]).

Como alternativa, proponse algoritmos evolutivos como o QPSO (*Quantum Particle Swarm Optimization*), que ofrecen mellor rendemento en espazos de optimización complexos (como se pode ver en [19]).

## 3.3. Aplicacións do algoritmo VQE.

Tanto o algoritmo VQE como as súas variacións, aplícanse a numerosos problemas de interese en física e química. Entre os seus principais campos de aplicación destacan:

- Problemas de física nuclear (como se pode ver en [12]).

- Problemas de estrutura nuclear (como se pode ver en [16]).
- Problemas de física de altas enerxías (como se pode ver en [2], [3]).
- Estudos de espectroscopía vibracional e vibrónica (como se pode ver en [7], [11]).
- Predición de propiedades de reacciones fotoquímicas (como se pode ver en [14]).
- Análise de sistemas periódicos (como se pode ver en [20]).
- Resolución de ecuacións de Schrödinger non lineais (como se pode ver en [10]).
- Estudo de estados cuánticos, como os buratos negros Schwarzschild-de Ditter ou cosmoloxía Kantowski-Sachs (como se pode ver en [8]).

# Capítulo 4

# Computación clásica fronte a computación cuántica

Neste capítulo compararemos a computación clásica e a cuántica dende distintas perspectivas co obxectivo de entender os seus respectivos límites e capacidades.

## 4.1. Clases de complexidade

En primeiro lugar analizaremos os recursos computacionais (tempo e memoria) que requiren os problemas para a súa resolución, é dicir, da súa complexidade. A pesar de que esta está asociada ao algoritmo que se empregue, existen indicios de que hai problemas que son máis difíciles de forma intrínseca.

### 4.1.1. Complexidade clásica

Os algoritmos e problemas pódense clasificar segundo os recursos computacionais que requiren para ser resoltos en función do tamaño dos datos de entrada. Os problemas de decisión que se poden resolver en tempo polinómico nun ordenador clásico (*máquina de Turing determinista*) inclúense na *clase de complexidade computacional P* (tempo polinómico).

Por outro lado, os problemas cuxa solución pódese verificar en tempo polinómico ou, equivalentemente, os que unha *máquina de Turing non determinista* (que pode estar en varios estados á vez) pode determinar a súa solución, inclúense na *clase de complexidade* NP. Unha das grandes incógnitas da informática na actualidade é se P = NP.

Dentro da clase NP, os problemas aos que calquera outro problema da clase pódese reducir

en tempo polinómico inclúense na subclase *NP-completo* (tempo polinómico non determinista completo). Por outro lado, os problemas de decisión L tales que cada problema de NP pode transformarse neles en tempo polinómico, inclúense na subclase *NP-difícil* (tempo polinómico non determinista difícil). Tense que a clase NP-completo é un subconxunto de NP-difícil, mentres que ao revés non o é necesariamente.

Os problemas para os que se pode verificar que unha solución proposta é válida ou non en tempo polinómico inclúense na *clase de complexidade co-NP*.

Por outra banda, os problemas de decisión que requiren unha cantidade de memoria polinómica para resolverse pertencen á *clase PSPACE*. Adoita existir unha relación directamente proporcional entre a complexidade temporal e espacial dos problemas.

A *clase de complexidade #P* inclúe aos problemas de conteo, aqueles que consisten en determinar cantas solucións teñen e non en se existe algunha ou non. Esta é unha subclase de PSPACE.

Finalmente, os problemas que se poden resolver en tempo polinómico, pero cunha certa probabilidade de erro, inclúense na *clase BPP* (*"Bounded Error Probabilistic Polynomial time"*). Aos algoritmos desta clase permíteselles unha probabilidade de erro máxima de $1/2 + \epsilon$ (sendo $\epsilon$ unha cantidade positiva).

### 4.1.2. Complexidade cuántica

Para estudar os ordenadores cuánticos, defínense novas clases de complexidade que abordan as capacidades e limitacións dos ordenadores cuánticos.

A *clase de complexidade BQP (Bounded Error Quantum Polynomial time)* é a versión análoga da clase BPP clásica. Inclúe os algoritmos que se executan en tempo polinómico en función do tamaño de entrada e tales que devolven a solución do problema cunha alta probabilidade (xeneralmente, $\geq 2/3$). Dise que un problema é *BQP-completo* se, ademais de pertencer a BQP, calquera outro problema desta clase pódese reducir a el e resolvelo en tempo polinómico.

A *clase de complexidade QMA (Quantum-Merlin-Arthur)* inclúe os problemas de decisión cuxas solucións poden ser verificadas con alta probabilidade en tempo polinómico en función do tamaño de entrada. Existe un estado cuántico (*testigo cuántico*) para cada problema tal que, cando se introduce como entrada, o verificador cuántico conclúe cunha resposta. Se esta é afirmativa, entón existe un estado cuántico que o verificador acepta cunha probabilidade $\geq 2/3$, mentres que se é negativa, calquera estado será rexeitado coa mesma probabilidade. É a versión análoga da *clase MA (Merlin-Arthur)* clásica.

A *clase de complexidade DQC1 (De 1 Cúbit Limpio)* inclúe os problemas de decisión que poden resolverse cunha máquina de *cúbits limpios* en tempo polinómico cunha alta probabilidade (polo menos 2/3) (como se pode ver en [17]). Iníciase cun único cúbit no estado puro cero e $n$ cúbits no estado máximo mesturado. A continuación, aplícase a calquera circuíto cuántico de tamaño polinómico, medindo unicamente o cúbit puro. Este proceso pódese repetir un número polinómico de veces.

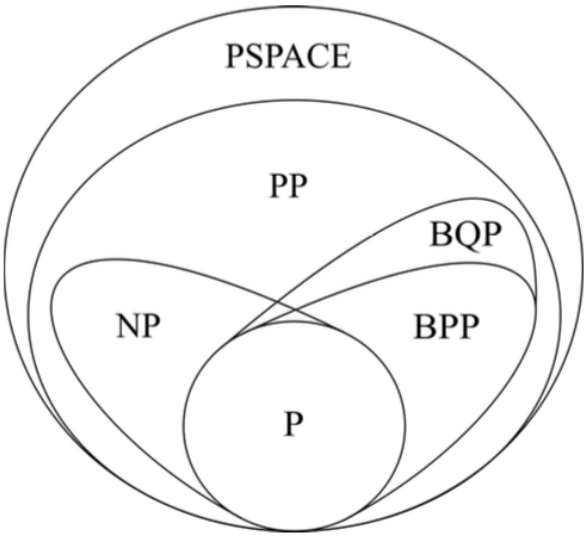



Figura 4.1: Relación entre clases de complexidade clásica e cuántica. Adaptado de [6], Figura AN.1.

## 4.2. A vantaxe cuántica

A *vantaxe cuántica* (chamada inicialmente *supremacía cuántica*) enténdese como a capacidade dos ordenadores cuánticos para resolver problemas que son intratables para os clásicos ou requiren un tempo desorbitado. Considérase que existe esta vantaxe cando o dispositivo cuántico resolve un problema, incluíndo a preparación da entrada e a extracción da saída, nun tempo razoable e o mellor algoritmo clásico coñecido non o consegue. O tempo razoable dáse cando ao tomar unha entrada de gran tamaño, o dispositivo cuántico pode resolvelo, mentres que o clásico non.

Se nos referimos a algoritmos, estamos tratando un concepto matemático (libre de restricións materiais), mentres que os ordenadores cuánticos son obxectos físicos (suxeitos a restricións). Desta forma, a comparación debe ter en conta tanto o modelo teórico do algoritmo como as posibles limitacións na súa implementación práctica.

Comparar a complexidade dos algoritmos non adoita ser sempre trivial. Aínda que para algúns algoritmos clásicos existen cotas inferiores para a complexidade, na maioría dos casos isto non é así. Desta forma, a vantaxe enténdese como a comparación cos mellores algoritmos clásicos coñecidos en cada momento. Isto provoca o proceso de *descuantización* (como se pode ver en [4]), que describe a aparición de melloras nos algoritmos clásicos para reducir ou eliminar a suposta vantaxe e impulsa avances tanto no campo cuántico como no clásico.

Moitos algoritmos cuánticos adoitan empregar caixas negras coñecidas como *oráculos* que devolven respostas instantáneas a partir da entrada. Estes oráculos poden enmascarar a complexidade real do problema e determinar se este é cuántico ou clásico tampouco é doado. En certos casos, poden ser simulados clasicamente con facilidade e noutros esixen unha capacidade cuántica inevitable (como se pode ver en [18]).

Para que o *hardware* sexa escalable, requírese un gran número de cúbits con alta fiabilidade e interconexión entre eles. Os ordenadores cuánticos están suxeitos a erros físicos como o ruído e a decoherencia (perda das propiedades cuánticas), feito que limita a lonxitude dos circuítos. Ademais, reducir o tempo de execución adoita requirir máis recursos ou calibracións. Por este motivo, a vantaxe práctica adoita darse en problemas de dimensión moderada, nos que o custo de preparar a entrada ou extraer a saída non anula o beneficio en tempo.

Todas estas reflexións conducen á cuestión de se merece a pena ou non o investimento de recursos na computación cuántica. Sen embargo, aínda que a obtención dun avance significativo na práctica poida tardar en materializarse, o esforzo na investigación xa produciu beneficios suficientes para que compense seguir investindo, por exemplo:

- No ámbito tecnolóxico, impulsáronse progresos en supercondutores e sistemas de refrixeración a moi baixas temperaturas.
- No ámbito da física, profundizouse na comprensión dos principios da mecánica cuántica.
- No ámbito das matemáticas, desenvolvéronse numerosos algoritmos clásicos inspirados nos cuánticos que resultan útiles, especialmente na deceleración da lei de Moore.

## 4.3. O futuro da computación cuántica

A comparación anterior entre a computación clásica e a cuántica adoita ser ambigua. Cada unha ten un propósito distinto e os resultados óptimos xorden de empregalos de forma complementaria.

En calquera caso, considérase que no futuro existirá unha vantaxe cuántica realista. Existen

algúns ámbitos como a optimización de funcións e a resolución de problemas de combinatoria nos que a computación cuántica resulta especialmente axeitada.

Numerosos centros de investigación na actualidade dispoñen de superordenadores en liña para executar subrutinas dentro de algoritmos clásicos. De xeito análogo, é previsible que nun futuro tamén conten con ordenadores cuánticos en liña para realizar cálculos concretos. Desta forma, poderán empregarse como recursos complementarios cando o problema o xustifique.

No ámbito industrial, xa existen empresas que proporcionan servizos de computación cuántica en liña como IBM, Google, Amazon, D-Wave ou Rigetti. Estes servizos deséñanse para executar circuítos ou algoritmos cuánticos breves para minimizar os erros. Ademais, requirirán un algoritmo clásico que coordine o traballo.

Outra liña de desenvolvemento diríxese á creación de QPUs (procesadores cuánticos "analóxicos") deseñados para abordar tarefas de optimización de problemas en campos como a química, a física ou a bioloxía. Estes dispositivos servirán para aproveitar a natureza cuántica dos fenómenos a simular, o que conlevará unha maior eficiencia na súa resolución.

Non obstante, a adopción de QPUs en ámbitos domésticos ou en instalacións de pequena escala non é probable. Os requisitos de infraestrutura e o alto custo supoñen un obstáculo. Así mesmo, nun futuro podería producirse algún avance que reduza estes inconvenientes, do mesmo xeito que os semicondutores revolucionaron a computación clásica.

## 4.4. A investigación matemática na computación cuántica

En España existe unha rede colaborativa denominada Quantum Spain [1] que se dedica a construír un ordenador cuántico de alto rendemento e accesible en liña. O obxectivo é que tanto empresas como entidades públicas poidan traballar cos novos algoritmos cuánticos e poidan xerar bibliotecas de algoritmos cuánticos aplicables a problemas reais.

Entre os principais grupos de investigación en computación cuántica destacan:

- O grupo QUANTIC [2] no Centro Nacional de Supercomputación (BSC-CNS) en Barcelona, especializado en cúbits superconductores.
- O grupo de QUANTIA [3] da Universidade de Zaragoza, centrado en algoritmos de optimización cuántica aplicados a problemas industriais e científicos.

[1] `https://quantumspain-project.es/`
[2] `https://www.bsc.es/discover-bsc/organisation/scientific-structure/quantic`
[3] `https://quantumspain-project.es/ia-cuantica-para-aplicaciones-cientificas-e-industriales/`

- O proxecto Basque Quantum [4] promovido pola Fundación Basca para a ciencia (Ikerbasque), que traballa no desenvolvemento de infraestrutura cuántica.
- O EHU Quantum Center [5] da universidade do País Vasco (UPV/EHU), dedicado á investigación en fundamentos de mecánica cuántica, algoritmos cuánticos e á formación de novos investigadores.
- Outros como o ICREA en Cataluña, a Universidade do País Vasco (UPV/EHU), o BCAM no País Vasco ou o CESGA en Galicia.

Non obstante, a participación de matemáticos especializados na computación cuántica é limitada nalgunhas rexións como Galicia. Aínda así, destaca o Laboratorio de Investigación e Desenvolvemento en Intelixencia Artificial (LIDIA) da Facultade de Informática de A Coruña, que inclúe esta temática entre as súas áreas de traballo.

Proximamente, o CESGA incorporará un ordenador cuántico no marco do Polo de Tecnoloxías Cuánticas de Galicia. Esta infraestrutura permitirá ampliar o acceso dos investigadores galegos á tecnoloxía cuántica.

[4] https://www.ikerbasque.net/es/noticias/presentacion-del-proyecto-basque-quantum
[5] https://www.ehu.eus/es/web/quantum-center

# Bibliografía


[1] Eric R. Anschuetz and Behzad T. Kiani. Quantum variational algorithms are swamped with traps. *Nature Communications*, 13(1):7760, 2022. doi:10.1038/s41467-022-35364-5.

[2] Steven D. Bass and Eliahu Zohar. Quantum technologies in particle physics. *Philosophical Transactions of the Royal Society A*, 380, 2022. URL: https://royalsocietypublishing.org/doi/10.1098/rsta.2021.0072, doi:10.1098/rsta.2021.0072.

[3] Christian W. Bauer, Zohreh Davoudi, A. Baha Balantekin, Tanmoy Bhattacharya, Marcela Carena, Wibe A. de Jong, Patrick Draper, Aida El-Khadra, Nathan Gemelke, Masanori Hanada, Dmitri Kharzeev, Henry Lamm, Yingsheng Y. Li, Junyu Liu, Mikhail Lukin, Yannick Meurice, Christopher Monroe, Benjamin Nachman, Guido Pagano, John Preskill, Enrico Rinaldi, Alessandro Roggero, David I. Santiago, Martin J. Savage, Irfan Siddiqi, George Siopsis, Daniel Van Zanten, Nathan Wiebe, Yuta Yamauchi, Karam Yeter-Aydeniz, and Silvia Zorzetti. Quantum simulation for high-energy physics. *PRX Quantum*, 4:027001, 2023. URL: https://link.aps.org/doi/10.1103/PRXQuantum.4.027001, doi:10.1103/PRXQuantum.4.027001.

[4] J. Cotler, Hsin-Yuan Huang, and J. R. McClean. Revisiting dequantization and quantum advantage in learning tasks, 2021. arXiv preprint arXiv:2112.00811. URL: http://arxiv.org/abs/2112.00811, arXiv:2112.00811.

[5] Diego Faílde, José D. Viqueira, Miguel M. Juane, and Adrián Gómez. Using differential evolution to avoid local minima in variational quantum algorithms. arXiv preprint, 2023. URL: https://doi.org/10.48550/arXiv.2303.12186.

[6] L. Gyongyosi and S. Imre. A survey on quantum computing technology. *Computer Science Review*, 31:51–71, 2019. URL: https://www.sciencedirect.com/science/article/pii/S1574013718301709.

[7] Soran Jahangiri, Juan Miguel Arrazola, Nicolas Quesada, and Alejandro Delgado. Quantum algorithm for simulating molecular vibrational excitations. *Physical Chemistry Chemical*

*Physics*, 22:25528–25537, 2020. URL: http://dx.doi.org/10.1039/D0CP03593A, doi:10.1039/D0CP03593A.

[8] Anosh Joseph, Toby White, Varun Chandra, and Michael McGuigan. Quantum computing of schwarzschild-de sitter black holes and kantowski-sachs cosmology, 2022. arXiv:2202.09906, doi:10.48550/arXiv.2202.09906.

[9] A. Kulshrestha and I. Safro. Beinit: Avoiding barren plateaus in variational quantum algorithms. In *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 197–203, 2022. doi:10.1109/QCE53715.2022.00039.

[10] Michael Lubasch, Jaewoo Joo, Pierre Moinier, Martin Kiffner, and Dieter Jaksch. Variational quantum algorithms for nonlinear problems. *Physical Review A*, 101(1):010301, 2020. URL: https://link.aps.org/doi/10.1103/PhysRevA.101.010301, doi:10.1103/PhysRevA.101.010301.

[11] Erik Lötstedt, Kaoru Yamanouchi, Takuya Tsuchiya, and Yuji Tachikawa. Calculation of vibrational eigenenergies on a quantum computer: Application to the fermi resonance in $co_2$. *Physical Review A*, 103(6):062609, 2021. URL: https://link.aps.org/doi/10.1103/PhysRevA.103.062609, doi:10.1103/PhysRevA.103.062609.

[12] Richard Miceli and Michael McGuigan. Effective matrix model for nuclear physics on a quantum computer. In *2019 New York Scientific Data Summit (NYSDS)*, pages 1–4, 2019. doi:10.1109/NYSDS.2019.8909693.

[13] Giacomo Nannicini. An introduction to quantum computing, without the physics, 2020. arXiv preprint arXiv:1708.03684v5. URL: https://arxiv.org/abs/1708.03684v5, arXiv:1708.03684v5.

[14] Kazuya Omiya, Yuto O. Nakagawa, Shumpei Koh, Wataru Mizukami, Qian Gao, and Ryohei Kobayashi. Analytical energy gradient for state-averaged orbital-optimized variational quantum eigensolvers and its application to a photochemical reaction. *Journal of Chemical Theory and Computation*, 18(2):741–748, 2022. doi:10.1021/acs.jctc.1c00877.

[15] A. Peruzzo, J. McClean, P. Shadbolt, M. H. Yung, X. Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5:4213, 2014. URL: https://pubmed.ncbi.nlm.nih.gov/25055053, doi:10.1038/ncomms5213.

[16] Adam M. Romero, Jonathan Engel, Ho Lun Tang, and Sophia E. Economou. Solving nuclear structure problems with the adaptive variational quantum algorithm. *Physical Review C*, 105(6):064317, 2022. doi:10.1103/PhysRevC.105.064317.

[17] Peter W. Shor and Stephen P. Jordan. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Information and Computation*, 8(8):681–714, 2008. doi:10.26421/QIC8.8-9-1.

[18] E. Stoudenmire and X. Waintal. Grover's algorithm offers no quantum advantage, 2023. arXiv preprint arXiv:2303.11317. URL: http://arxiv.org/abs/2303.11317, arXiv:2303.11317.

[19] Jianjun Sun, Chuen-Horng Lai, and Xiao-Jun Wu. *Particle Swarm Optimisation: Classical and Quantum Perspectives*. Numerical Analysis and Scientific Computing Series. Chapman & Hall/CRC, 2012. URL: https://doi.org/10.1201/b11579.

[20] Naoki Yoshioka, Takashi Sato, Yuto O. Nakagawa, Yusuke Y. Ohnishi, and Wataru Mizukami. Variational quantum simulation for periodic materials. *Physical Review Research*, 4(1):013052, 2022. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.4.013052, doi:10.1103/PhysRevResearch.4.013052.

[21] L. Zhou, S. T. Wang, S. Choi, H. Pichler, and M. D. Lukin. Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. *Physical Review X*, 10(2):021067, 2020. URL: https://link.aps.org/doi/10.1103/PhysRevX.10.021067, doi:10.1103/PhysRevX.10.021067.

[22] Z. Zhou, Y. Du, X. Tian, and D. Tao. Qaoa-in-qaoa: Solving large-scale maxcut problems on small quantum machines. *Physical Review Applied*, 19(2):024027, 2023. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.19.024027, doi:10.1103/PhysRevApplied.19.024027.