



CITMAga

Las Matemáticas en la era de la Computación Cuántica: nuevas fronteras

Fernando Adrián Fernández Tojo
Francisco Javier Fernández Fernández
Francisco José Pena Brage

24/10/2023



*Unha maneira
de facer Europa.*



Fondos Europeos



Despregamento dunha infraestrutura baseada en tecnoloxías cuánticas da información que permita impulsar a I+D+i en Galicia.

Apoiar a transición cara a una economía dixital.

Operación financiada pola Unión Europea, a través do FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL (FEDER) como parte da resposta da Unión á pandemia da COVID-19

Bajo licencia CC-BY-SA

//... It may turn out to be possible to build small quantum computers, while scaling up to machines large enough to do interesting computations may present fundamental difficulties.

Even if no useful quantum computer is ever built, this research does illuminate the problem of simulating quantum mechanics on a classical computer. //

Peter W. Shor
*Polynomial-Time Algorithms for Prime Factorization
and Discrete Logarithms on a Quantum Computer (1999).*

Índice general

Planteamiento y objetivos	7
I Introducción a la computación cuántica para matemáticos	9
1 El concepto de cúbit y p-cúbit	9
1.1 El concepto de cúbit	9
1.2 El concepto de p -cúbit	13
2 Circuitos cuánticos	20
2.1 Puertas lógicas para cúbits	21
2.2 Puertas lógicas para p -cúbits	24
2.3 Puertas de medida	30
3 Principales algoritmos cuánticos	37
3.1 Transformada de Fourier cuántica (QFT)	37
3.2 Algoritmo de estimación de fase (QPE)	46
3.3 Algoritmo de resolución de sistemas lineales (HHL)	53
3.4 Algoritmo de Shor	59
3.5 Algoritmo de Grover	67
3.6 El enfoque cuántico para problemas de optimización	73
3.6.1 El hamiltoniano de un sistema cuántico	74
3.6.2 El modelo Ising	75
3.6.3 Computación cuántica adiabática	76
3.6.4 Algoritmo QAOA	76
3.6.5 Algoritmo VQE	77
4 Computación clásica y computación cuántica	77
4.1 Clases de complejidad	78
4.1.1 Complejidad clásica	78
4.1.2 Complejidad cuántica	79
4.2 La ventaja cuántica	80
4.3 El futuro de la computación cuántica	83
4.4 El papel de la investigación matemática en la computación cuántica	84

II Algoritmos y líneas de investigación actuales en computación cuántica	86
5 Introducción	86
5.1 Bibliografía y recursos	86
5.2 Planteamiento de las líneas de investigación y problemas	87
6 Lógica, conjuntos y funciones	90
6.1 Búsqueda cuántica	90
6.2 Evaluación de fórmulas	91
6.3 Reconocimiento de patrones	91
6.4 Búsqueda en listas ordenadas	92
6.5 Búsqueda de subconjuntos	93
7 Álgebra y teoría de números	93
7.1 Cálculo de logaritmo discreto	93
7.2 Criterios de primalidad	93
7.3 Verificación del producto de matrices	94
7.4 Problemas de conmutatividad	94
7.5 Rango de una matriz	95
7.6 Subgrupo oculto abeliano	95
7.7 Subgrupo oculto no abeliano	96
7.8 Grupos de unidades	97
7.9 Desplazamiento oculto	97
7.10 Criptografía	97
7.11 Obtención de autovalores	98
8 Geometría y Topología	99
8.1 Análisis cuántico de datos topológicos	99
8.2 Invariantes de nudos	100
8.3 Invariantes de variedades de dimensión tres	100
8.4 Determinación de propiedades de grafos	101
9 Estadística, optimización y simulación numérica	102
9.1 Diferencia estadística	102

9.2	Flujos en redes	103
9.3	Temple simulado (Simulated Annealing, SA)	103
9.4	Temple cuántico (Quantum Annealing, QA)	104
9.5	Algoritmo de Optimización Cuántica Aproximada (QAOA)	104
9.6	Ajuste de mínimos cuadrados	105
9.7	Machine learning y análisis de datos	105
9.8	Análisis financiero	108
9.9	Simulación cuántica y redes de tensores	108
9.10	Computación cuántica adiabática	109
9.11	Ecuaciones diferenciales ordinarias	110
9.12	Ecuaciones en derivadas parciales	111
10	Ordenadores cuánticos, aplicaciones a la industria y casos de uso	111
10.1	Computación cuántica en España	115
10.2	Riesgos y consideraciones éticas	116
	Bibliografía	118
	Índice alfabético	148

Planteamiento y objetivos

Este informe tiene por objetivo principal ofrecer a los profesionales de las matemáticas tanto un punto de entrada al mundo de la computación cuántica como un resumen del estado del arte y los problemas abiertos en diferentes áreas que puedan ser de su interés. Para lograrlo, hemos tenido en cuenta los siguientes principios a la hora de elaborar el informe:

- ◇ **Autocontención:** Se ha intentado eliminar las barreras de entrada a la hora de comprender y poder hacer uso del documento, de modo que la persona que lo lea no tenga que estar familiarizada con la computación cuántica para entenderlo.
- ◇ **Enfoque:** El documento está pensado para matemáticos y el enfoque tomado a la hora de explicar conceptos y plantear líneas de investigación refleja este punto de vista particular. Hemos destacado los aspectos matemáticos de la computación cuántica por encima de otros más enfocados a la física o la ingeniería.
- ◇ **Transversalidad:** La computación cuántica es un campo muy amplio y con muy variadas aplicaciones. Es por ello que hemos intentado recoger una gran diversidad de temas de investigación que puedan ser interesantes a los matemáticos independientemente de su área de trabajo, ofreciendo líneas de investigación cercanas al álgebra, la criptografía, el análisis, la estadística, la optimización, la geometría, la lógica, el cálculo numérico o la matemática aplicada.
- ◇ **Brevidad:** Tener unos objetivos tan amplios conlleva la necesidad de ser breve en la exposición. Se destacan solo los aspectos fundamentales y necesarios, ofreciendo una amplia bibliografía al lector interesado para que pueda profundizar más en los temas de su interés.
- ◇ **Transparencia:** Hay temas concretos en computación cuántica que generan un intenso debate a día de hoy, son fruto de muchas especulaciones o están sujetos a diversos intereses (por ejemplo, la cuestión de la *ventaja cuántica*). Hemos intentado ser transparentes y abiertos con los puntos conflictivos, presentando con claridad los problemas, aportando referencias al respecto y dando nuestra opinión como observadores externos.
- ◇ **Recursos:** Además de la abundante bibliografía, se hace un repaso de los recursos de todo tipo, en especial los electrónicos (páginas web, repositorios, foros, tutoriales, software de diseño de circuitos, simuladores, servicios cuánticos en línea...) disponibles en la actualidad.

Estos principios nos han llevado a dividir el informe en dos partes. La primera es una introducción somera a la computación cuántica pensada para un público objetivo formado por profesionales de las matemáticas. La finalidad de esta parte es que el lector, sin necesidad de acudir a referencias adicionales, adquiera los rudimentos mínimos necesarios

para iniciarse en el mundo de la computación cuántica y sacar mejor provecho de la segunda parte. Para ello hemos incluido abundantes ejemplos y explicaciones que a menudo se omiten en la literatura. También en esta primera parte comparamos la computación cuántica con la clásica y explicamos en qué consiste el concepto de ventaja cuántica.

La segunda parte empieza con una breve exposición de la bibliografía (centrándose en las monografías básicas y en las revisiones bibliográficas especializadas) y los recursos disponibles para informarse, investigar y hacer uso de la computación cuántica. A continuación, se detalla una lista de problemas de interés y algoritmos, descritos de forma somera, con abundantes referencias bibliográficas referentes al estado del arte y, en su caso, los problemas abiertos y tendencias. Estos algoritmos y problemas están clasificados por áreas, pero esta clasificación es por necesidad arbitraria y deficiente, como lo es cualquier intento de subdividir las matemáticas en parcelas. Aún así, pensamos que esta división puede ser de utilidad a la hora de encontrar un problema o algoritmo concreto, algo que no se conseguiría con otro tipo de organización.

Incluimos también en esta segunda parte un resumen de las posibles aplicaciones a la industria y casos de uso de la computación cuántica. Hay que tener en cuenta que, al ser una tecnología muy incipiente y poco distribuida, las aplicaciones actuales son muy limitadas. También ponemos el foco sobre el caso de España, sus instituciones en materia de computación cuántica, sus recursos y sus proyectos abiertos.

Finalmente, hay un índice alfabético de términos que puede ayudar al lector a encontrar aquellas cuestiones que considere de relevancia.

Parte I

Introducción a la computación cuántica para matemáticos

1 El concepto de cúbit y p -cúbit

En esta sección veremos uno de los elementos de la computación cuántica, el concepto de cúbit y p -cúbit. Para ello, nos centraremos en definiciones y propiedades básicas meramente matemáticas sin mencionar las cuestiones relacionadas con la física cuántica subyacentes. Existe una gran cantidad de literatura científica que el lector puede consultar para profundizar al respecto, véase, entre otros, [312, 354]. En nuestro caso en concreto, hemos optado por considerar como referencia principal [306] pues se adapta muy bien al espíritu del documento: introducir la computación cuántica desde un punto de vista matemático sin considerar las cuestiones físicas que la motivan y sustentan.

1.1 El concepto de cúbit

Comencemos presentando el concepto matemático de cúbit y su representación en la esfera de Bloch. Para ello, consideraremos el plano complejo \mathbb{C}^2 como \mathbb{C} -espacio vectorial. Se tendrá que dicho espacio vectorial tiene dimensión dos. Además, los vectores de la base canónica

$$\mathbf{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathbf{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

conforman una base ortonormal con respecto al producto escalar

$$\langle | \rangle : (\mathbf{z}, \mathbf{w}) \in \mathbb{C}^2 \times \mathbb{C}^2 \rightarrow \langle \mathbf{z} | \mathbf{w} \rangle = \sum_{j=0}^1 \bar{z}_j w_j \in \mathbb{C}.$$

En particular, el par $(\mathbb{C}^2, \langle | \rangle)$ es un espacio de Hilbert.

Notación 1.1. Es frecuente, en computación cuántica, emplear las notaciones $\langle z |$ (*bra-vector*) y $|w\rangle$ (*ket-vector*) para denotar los siguientes elementos:

$$\langle z | = \begin{pmatrix} \bar{z}_0 & \bar{z}_1 \end{pmatrix},$$
$$|w\rangle = \begin{pmatrix} w_0 \\ w_1 \end{pmatrix}.$$

De esta forma, la propia notación para el producto escalar de \mathbf{z} por \mathbf{w} , se puede entender como el producto matricial de los elementos $\langle z |$ y $|w\rangle$.

Al comienzo de esta sección empleábamos la notación \mathbf{e}_0 y \mathbf{e}_1 para referirnos a los elementos de la base canónica. A partir de ahora emplearemos la notación $|0\rangle = \mathbf{e}_0$ y $|1\rangle = \mathbf{e}_1$, por ser la que se suele emplear con más frecuencia en el ámbito de la computación cuántica. De esta forma, dado un elemento $\psi \in \mathbb{C}^2$, existirán elementos únicos $\alpha, \beta \in \mathbb{C}$ tales que $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. Identificaremos, sin que por ello cause confusión, los vectores $\psi \in \mathbb{C}^2$ con su correspondiente vector de coordenadas en la base canónica $|\psi\rangle$.

A continuación definiremos uno de los elementos básicos en la computación cuántica, el concepto de cúbit.

Definición 1.2 (cúbit). Diremos que un elemento $|\psi\rangle \in \mathbb{C}^2$ es un *cúbit* si

$$\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle} = 1,$$

esto es, un cúbit es un elemento unitario del espacio \mathbb{C}^2 .

A los elementos $|0\rangle$ y $|1\rangle$ se les suele llamar *estados básicos computacionales*. Teniendo en cuenta lo anterior, un cúbit se podrá expresar como combinación lineal de los estados básicos computacionales, esto es, dado un elemento $|\psi\rangle \in \mathbb{C}^2$, existirán $\alpha, \beta \in \mathbb{C}$ tales que

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle,$$

con

$$|\alpha|^2 + |\beta|^2 = 1.$$

No podemos examinar un cúbit para obtener su estado cuántico (los valores de α y β). En lugar de eso, lo que nos dice la mecánica cuántica es que solamente podemos disponer de una información más restrictiva del estado cuántico. Cuando medimos un cúbit obtenemos el resultado $|0\rangle$ con probabilidad $|\alpha|^2$, o el estado $|1\rangle$ con probabilidad $|\beta|^2$.

Tal y como hemos visto en la sección anterior, un cúbit puede existir en un continuo de estados entre el $|0\rangle$ y $|1\rangle$ hasta que sea observado. Remarquemos que cuando se mide un cúbit, solamente obtenemos el estado $|0\rangle$ o el estado $|1\rangle$ como resultado de dicha medición (probabilística).

Definición 1.3 (Estados básicos y superposición). Diremos que un cúbit $|\psi\rangle$ está en un *estado básico* si $|\psi\rangle = \sum_{j \in \{0,1\}} \alpha_j |j\rangle$ es tal que existe $k \in \{0, 1\}$ de forma que $|\alpha_k| = 1$ y $\alpha_j = 0$ para todo $j \neq k$. En caso contrario, diremos que está en *superposición de estados básicos*.

Esta definición, con las modificaciones correspondientes, será válida para el caso de tener sistemas con múltiples cúbits.


Ejemplo 1.4. El cúbit¹,

$$|+\rangle := \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle,$$

¹Se suele denotar por $|+\rangle := \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$ y por $|-\rangle := \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$.

se encuentra en superposición de estados básicos. Además, al realizar la medición del estado cuántico del mismo, obtenemos

- ◊ el estado $|0\rangle$ el $|1/\sqrt{2}|^2$ por ciento de las veces,
- ◊ el estado $|1\rangle$ el $|1/\sqrt{2}|^2$ por ciento de las veces.

Esto es, tenemos un cincuenta por ciento de probabilidades de que al medir el estado cuántico del cúbit, obtengamos el estado $|0\rangle$ o el estado $|1\rangle$. 

Tal y como comentábamos anteriormente, un cúbit es un elemento de \mathbb{C}^2 , que quedará caracterizado por sus coordenadas en los estados básicos, $\alpha, \beta \in \mathbb{C}$. Puesto que $|\alpha|^2 + |\beta|^2 = 1$, un cúbit quedará parametrizado por $4 - 1 = 3$ números reales que, en última instancia, podremos identificar con la esfera unidad en \mathbb{R}^3 .

En efecto, denotemos por

$$\begin{aligned}\alpha &= r_\alpha e^{i\theta_\alpha} \in \mathbb{C}, \\ \beta &= r_\beta e^{i\theta_\beta} \in \mathbb{C},\end{aligned}$$

a las expresiones en forma polar de Euler de los complejos α y β . De la relación $|\alpha|^2 + |\beta|^2 = 1$ deducimos que

$$r_\alpha^2 + r_\beta^2 = 1.$$

Por lo tanto, existe un elemento $\theta \in [0, \pi/2]$ tal que $r_\alpha = \cos(\theta)$ y $r_\beta = \sin(\theta)$, de forma equivalente, existe un elemento $\theta \in [0, \pi]$ tal que $r_\alpha = \cos(\theta/2)$ y $r_\beta = \sin(\theta/2)$. Tenemos entonces que:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) e^{i\theta_\alpha} |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\theta_\beta} |1\rangle,$$

siendo $\theta \in [0, \pi]$ y $\theta_\alpha, \theta_\beta \in [0, 2\pi]$. En particular,

$$|\psi\rangle = e^{i\theta_\alpha} \left(\cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i(\theta_\beta - \theta_\alpha)} \sin\left(\frac{\theta}{2}\right) |1\rangle \right).$$

En la expresión anterior podemos desprestigiar el término $e^{i\theta_\alpha}$ puesto que no tiene efectos observables (luego analizaremos que quiere decir esto). Por lo tanto, si denotamos por $\varphi = \theta_\beta - \theta_\alpha \in [0, 2\pi]$, tenemos que

$$|\psi\rangle \equiv |\psi(\theta, \varphi)\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle.$$

Los parámetros $\theta \in [0, \pi]$ y $\varphi \in [0, 2\pi]$ se suelen identificar con puntos de la esfera unidad en \mathbb{R}^3 (ver Figura 1.1) que se conoce, en tal caso, como *esfera de Bloch*.

Ejemplo 1.5. Veamos que estados cuánticos se corresponden con los puntos de la esfera $(0, 0, 1)$, $(0, 0, -1)$, $(1, 0, 0)$, $(-1, 0, 0)$, $(0, 1, 0)$ y $(0, -1, 0)$, respectivamente:

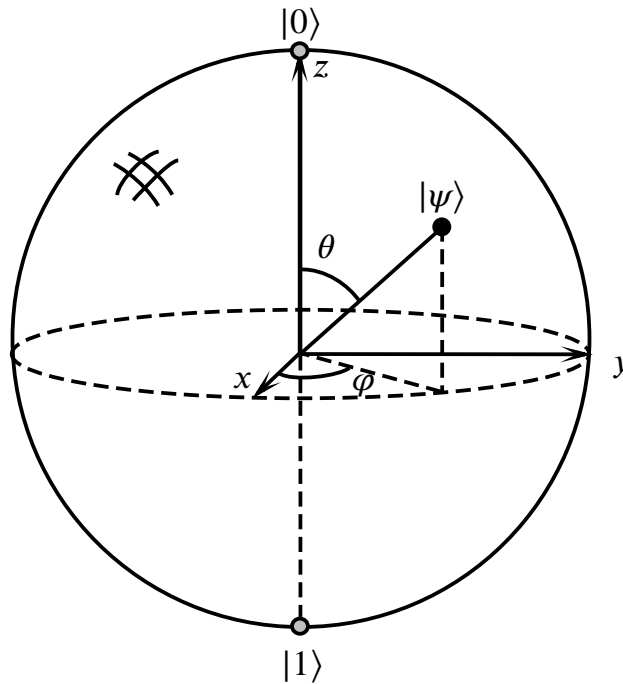


Fig. 1.1. Representación en la esfera de Bloch de un cúbit [312, Figure 1.3]).

1. $(0, 0, 1) \equiv (0, \varphi)$:

$$|\psi\rangle = |\psi(0, \varphi)\rangle = \cos(0) |0\rangle + e^{i\varphi} \sin(0) |1\rangle = |0\rangle.$$

2. $(0, 0, -1) \equiv (\pi, \varphi)$:

$$|\psi\rangle = |\psi(\pi, \varphi)\rangle = \cos\left(\frac{\pi}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\pi}{2}\right) |1\rangle = e^{i\varphi} |1\rangle \equiv |1\rangle.$$

3. $(1, 0, 0) \equiv (\pi/2, 0)$:

$$|\psi\rangle = |\psi(\pi/2, 0)\rangle = \cos\left(\frac{\pi}{4}\right) |0\rangle + e^{i0} \sin\left(\frac{\pi}{4}\right) |1\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle = |+\rangle.$$

4. $(-1, 0, 0) \equiv (\pi/2, \pi)$:


$$|\psi\rangle = |\psi(\pi/2, \pi)\rangle = \cos\left(\frac{\pi}{4}\right) |0\rangle + e^{i\pi} \sin\left(\frac{\pi}{4}\right) |1\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle = |-\rangle.$$

5. $(0, 1, 0) \equiv (\pi/2, \pi/2)$:

$$|\psi\rangle = |\psi(\pi/2, \pi/2)\rangle = \cos\left(\frac{\pi}{4}\right) |0\rangle + e^{i\frac{\pi}{2}} \sin\left(\frac{\pi}{4}\right) |1\rangle = \frac{1}{\sqrt{2}} |0\rangle + i \frac{1}{\sqrt{2}} |1\rangle = |+i\rangle.$$

6. $(0, -1, 0) \equiv (\pi/2, 3\pi/2)$:

$$|\psi\rangle = |\psi(\pi/2, 3\pi/2)\rangle = \cos\left(\frac{\pi}{4}\right) |0\rangle + e^{i\frac{3\pi}{2}} \sin\left(\frac{\pi}{4}\right) |1\rangle = \frac{1}{\sqrt{2}} |0\rangle - i \frac{1}{\sqrt{2}} |1\rangle = |-i\rangle.$$

La identificación geométrica de los estados cuánticos que se corresponden con los puntos anteriores puede resultar de utilidad a la hora de estudiar determinados operadores lógicos en términos de movimientos rígidos de la esfera de Bloch. 

1.2 El concepto de p -cúbit

La estructura matemática básica para expresar sistemas físicos con múltiples cúbits es el producto tensorial de espacios de Hilbert. Anteriormente hemos visto que un cúbit es un elemento del espacio $\mathbb{H} := \mathbb{C}^2$. En el caso de tener un sistema con dos cúbits sus posibles estados estarán en el espacio resultante de hacer el producto tensorial de \mathbb{H} por si mismo, $\mathbb{H} \otimes \mathbb{H} := \mathbb{C}^2 \otimes \mathbb{C}^2$ y así sucesivamente. De esta manera, obtenemos la siguiente definición.

Definición 1.6 (p -cúbit). Diremos que un elemento $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p} = \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 \equiv \mathbb{C}^{2^p}$ es un p -cúbit si $\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle} = 1$. Esto es, un p -cúbit es un elemento unitario del espacio \mathbb{C}^{2^p} .

Para entender el concepto de sistemas cuánticos con múltiples cúbits, veamos algunas nociones básicas del producto tensorial de espacios de Hilbert.

Sean $(\mathbb{H}^A, \langle | \rangle^A)$ y $(\mathbb{H}^B, \langle | \rangle^B)$ dos espacios de Hilbert. Dados $|\varphi\rangle \in \mathbb{H}^A$ y $|\psi\rangle \in \mathbb{H}^B$, definimos

$$\begin{aligned} |\varphi\rangle \otimes |\psi\rangle : \mathbb{H}^A \times \mathbb{H}^B &\rightarrow \mathbb{C} \\ (\xi, \eta) &\rightarrow \langle \xi | \varphi \rangle^A \langle \eta | \psi \rangle^B. \end{aligned}$$

La aplicación anterior es *antilineal*¹ en ξ y η y, además, es continua. Definamos el conjunto de tales aplicaciones de la siguiente forma:

$$\mathbb{H}^A \otimes \mathbb{H}^B := \{ \Psi : \mathbb{H}^A \times \mathbb{H}^B \rightarrow \mathbb{C} : \Psi \text{ es anti-lineal y continua} \}.$$

El espacio anterior es un espacio vectorial sobre \mathbb{C} . Además, dados $|\varphi\rangle \in \mathbb{H}^A$ y $|\psi\rangle \in \mathbb{H}^B$, tenemos que $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ (para simplificar la notación es frecuente emplear la notación $|\varphi \otimes \psi\rangle := |\varphi\rangle \otimes |\psi\rangle$).

Sean ahora $|\varphi_k\rangle \otimes |\psi_k\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$, $k \in \{1, 2\}$, definimos

$$\langle \varphi_1 \otimes \varphi_2 | \psi_1 \otimes \psi_2 \rangle := \langle \varphi_1 | \varphi_2 \rangle^A \langle \psi_1 | \psi_2 \rangle^B.$$

¹También se dice *lineal-conjugada* o *sesquilineal*. Dados dos \mathbb{C} -espacios vectoriales V y W , una aplicación $f : V \rightarrow W$ se dice antilineal si $f(u + v) = f(u) + f(v)$ y $f(\lambda u) = \bar{\lambda} f(u)$, para todo $u, v \in V$ y $\lambda \in \mathbb{C}$.

La aplicación anterior es un producto escalar para vectores de la forma $|\varphi\rangle \otimes |\psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$. Para definir el producto escalar para elementos genéricos $\Psi \in \mathbb{H}^A \otimes \mathbb{H}^B$, consideremos dos bases ortonormales $\{|e_a\rangle\} \subset \mathbb{H}^A$ y $\{|f_b\rangle\} \subset \mathbb{H}^B$ de, respectivamente, \mathbb{H}^A y \mathbb{H}^B . Se tendrá que $\{|e_a\rangle \otimes |f_b\rangle\} \subset \mathbb{H}^A \otimes \mathbb{H}^B$ es un sistema ortonormal ya que

$$\langle e_{a_1} \otimes f_{b_1} | e_{a_2} \otimes f_{b_2} \rangle = \langle e_{a_1} | e_{a_2} \rangle^A \langle f_{b_1} | f_{b_2} \rangle^B = \delta_{a_1 a_2} \delta_{b_1 b_2}.$$

Consideremos ahora un vector $|\Psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ y sean $\xi \in \mathbb{H}^A$, $\eta \in \mathbb{H}^B$. Por un lado (omitiremos los superíndices en los productos escalares sin que por ello se cause confusión),

$$\begin{aligned} \xi &= \sum_a |e_a\rangle \langle e_a | \xi \rangle, \\ \eta &= \sum_b |f_b\rangle \langle f_b | \eta \rangle. \end{aligned}$$

Por otro lado, gracias a la anti-linealidad de la aplicación Ψ ,

$$\begin{aligned} \Psi(\xi, \eta) &= \Psi\left(\sum_a |e_a\rangle \langle e_a | \xi \rangle, \sum_b |f_b\rangle \langle f_b | \eta \rangle\right) = \sum_{a,b} \Psi(|e_a\rangle, |f_b\rangle) \overline{\langle e_a | \xi \rangle} \overline{\langle f_b | \eta \rangle} \\ &= \sum_{a,b} \Psi(|e_a\rangle, |f_b\rangle) \langle \xi | e_a \rangle \langle \eta | f_b \rangle = \sum_{a,b} \Psi(|e_a\rangle, |f_b\rangle) |e_a\rangle \otimes |f_b\rangle (\xi, \eta) \\ &= \left(\sum_{a,b} \Psi(|e_a\rangle, |f_b\rangle) |e_a \otimes f_b\rangle\right) (\xi, \eta). \end{aligned}$$

Tenemos entonces que, dado $|\Psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$,

$$|\Psi\rangle = \sum_{a,b} \Psi(|e_a\rangle, |f_b\rangle) |e_a \otimes f_b\rangle.$$

Podemos entonces definir el producto escalar de dos vectores $|\Psi\rangle$ y $|\Phi\rangle$ de $\mathbb{H}^A \otimes \mathbb{H}^B$ de la siguiente forma:

$$\begin{aligned} \langle \Psi | \Phi \rangle &= \sum_{a_1, b_1} \sum_{a_2, b_2} \overline{\Psi(|e_{a_1}\rangle, |f_{b_1}\rangle)} \Phi(|e_{a_2}\rangle, |f_{b_2}\rangle) \langle e_{a_1} \otimes f_{b_1} | e_{a_2} \otimes f_{b_2} \rangle \\ &= \sum_{a_1, b_1} \sum_{a_2, b_2} \overline{\Psi(|e_{a_1}\rangle, |f_{b_1}\rangle)} \Phi(|e_{a_2}\rangle, |f_{b_2}\rangle). \end{aligned}$$

Habría que comprobar que el producto escalar así definido es realmente un producto escalar y que no depende de la elección de las bases ortonormales para \mathbb{H}^A y \mathbb{H}^B .

Se tiene entonces que el bra-vector asociado a $|\Psi\rangle$ es

$$\langle \Psi | = \sum_{a,b} \overline{\Psi(|e_a\rangle, |f_b\rangle)} \langle e_a \otimes f_b |.$$

Dicho vector actúa sobre un elemento $|\Phi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ como hemos visto antes.

La norma asociada a un elemento $|\Psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$ es, entonces,

$$\|\Psi\|^2 = \langle \Psi | \Psi \rangle = \sum_{a,b} |\Psi(|e_a\rangle, |f_b\rangle)|^2.$$

En particular, dado un elemento $|\Psi \otimes \Phi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$,

$$\| |\Psi \otimes \Phi\rangle \|^2 = \langle \Psi \otimes \Phi | \Psi \otimes \Phi \rangle = \langle \Psi | \Psi \rangle \langle \Phi | \Phi \rangle = \|\Phi\| \|\Psi\|.$$

Se tiene entonces que $\mathbb{H}^A \otimes \mathbb{H}^B$ es un espacio de Hilbert (es importante que las dimensiones de \mathbb{H}^A y \mathbb{H}^B sean finitas). Para nuestros propósitos es suficiente con identificar $\mathbb{H}^A \otimes \mathbb{H}^B$ con

$$\mathbb{H}^A \otimes \mathbb{H}^B = \left\{ \sum_{a,b} \Psi_{ab} |e_a \otimes f_b\rangle : \sum_{a,b} |\Psi_{ab}|^2 < \infty \right\}$$

y las reglas de cálculo,

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

Llegamos entonces al siguiente resultado.

Proposición 1.7 ([354, Proposition 3.2]). *Dadas dos bases ortonormales $\{|e_a\rangle\} \subset \mathbb{H}^A$ y $\{|f_b\rangle\} \subset \mathbb{H}^B$, el conjunto $\{|e_a\rangle \otimes |f_b\rangle\}$ forma una base ortonormal de $\mathbb{H}^A \otimes \mathbb{H}^B$ y, para espacios vectoriales de dimensión finita \mathbb{H}^A y \mathbb{H}^B , tenemos que*

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

Observación 1.8. Dado un espacio de Hilbert complejo \mathbb{H} de dimensión finita n , identificaremos las bases $\{|e_j\rangle\} \subset \mathbb{H}$ con una base en \mathbb{C}^n . Veamos como se translada esta idea al caso de considerar el producto tensorial de dos espacios de Hilbert $\mathbb{H}^A \otimes \mathbb{H}^B$, siendo, $\dim(\mathbb{H}^X) = n_X < \infty$, con $X \in \{A, B\}$. Sean entonces $\{|e_a\rangle\} \subset \mathbb{H}^A$ y $\{|f_b\rangle\} \subset \mathbb{H}^B$ dos bases ortonormales. Consideremos el isomorfismo $\mathbb{H}^X \simeq \mathbb{C}^{n_X}$, con $X \in \{A, B\}$, y veamos como podemos establecer un isomorfismo $\mathbb{H}^A \otimes \mathbb{H}^B \simeq \mathbb{C}^{n_A n_B}$ identificando la base $\{|e_a \otimes f_b\rangle\} \subset \mathbb{H}^A \otimes \mathbb{H}^B$ con la base canónica en $\mathbb{C}^{n_A n_B}$. Para ello, consideraremos la siguiente relación:

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

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

Con lo cual, dado un vector $|\Psi\rangle \in \mathbb{H}^A \otimes \mathbb{H}^B$, tenemos que

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

Ejemplo 1.9. Consideremos ahora el caso de tener un sistema cuántico compuesto por dos cúbits. En este caso, $\mathbb{H}^A = \mathbb{H}^B = \mathbb{C}^2$, con las siguientes bases ortonormales:

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

Con lo cual, para $\mathbb{H}^A \otimes \mathbb{H}^B \simeq \mathbb{C}^4$, tenemos la siguiente base ortonormal:

$$\{|e_a \otimes f_b\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Se tiene, por lo tanto, que un 2-cúbit $|\psi\rangle \in \mathbb{C}^4$ se puede expresar en función de los cuatro estados básicos anteriores:

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle,$$

donde

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

Al igual que en el caso de un cúbit, no podemos examinar el 2-cúbit para obtener su estado cuántico (los valores de α_{00} , α_{01} , α_{10} y α_{11}). Una vez medido el 2-cúbit, obtenemos el estado $|00\rangle$ con probabilidad $|\alpha_{00}|^2$, el estado $|01\rangle$ con probabilidad $|\alpha_{01}|^2$, etc.

En el caso de considerar un 3-cúbit, necesitaremos un tercer espacio $\mathbb{H}^C = \mathbb{C}^2$. En este caso, la base ortonormal será:

$$\{|e_a \otimes f_b \otimes g_c\rangle\} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\},$$

que se corresponde con la base canónica de \mathbb{C}^8 como \mathbb{C} -espacio vectorial. Por lo tanto, un 3-cúbit $|\psi\rangle \in \mathbb{C}^{2^3}$ se puede expresar como:

$$|\psi\rangle = \alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \alpha_{010} |010\rangle + \alpha_{011} |011\rangle \\ + \alpha_{100} |100\rangle + \alpha_{101} |101\rangle + \alpha_{110} |110\rangle + \alpha_{111} |111\rangle,$$

donde

$$|\alpha_{000}|^2 + |\alpha_{001}|^2 + |\alpha_{010}|^2 + |\alpha_{011}|^2 + |\alpha_{100}|^2 + |\alpha_{101}|^2 + |\alpha_{110}|^2 + |\alpha_{111}|^2 = 1. \quad \square$$

Notación 1.10. Observamos que a medida que aumentamos el número de p -cúbits, se hace cada vez más tedioso mantener la notación que hemos estado empleando hasta ahora, en donde detallamos cada uno de los elementos asociados a los estados básicos. Con la finalidad de simplificar la escritura, será frecuente emplear la siguiente notación:

$$\sum_{\vec{j} \in \{0,1\}^3} \alpha_{\vec{j}} |\vec{j}\rangle = \alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \alpha_{010} |010\rangle + \alpha_{011} |011\rangle \\ + \alpha_{100} |100\rangle + \alpha_{101} |101\rangle + \alpha_{110} |110\rangle + \alpha_{111} |111\rangle$$

De esta forma, un p -cúbit $|\psi\rangle \in \mathbb{C}^{2^p}$ se puede expresar como combinación lineal de 2^p estados básicos:

$$|\psi\rangle = \sum_{\vec{j} \in \{0,1\}^p} \alpha_{\vec{j}} |\vec{j}\rangle,$$

donde

$$\sum_{\vec{j} \in \{0,1\}^p} |\alpha_{\vec{j}}|^2 = 1.$$

Otra forma de denotar los estados básicos cuando tengamos circuitos cuánticos con un gran número de cúbits es considerar el desarrollo en binario de la posición que ocupa en la numeración global cada uno de los estados básicos. Supongamos que tenemos un p -cúbit. En este caso, tenemos $n = 2^p$ estados básicos, que numeraremos de 0 a $2^p - 1$ (indicamos cada uno de los estados básicos numerados de 0 a $2^p - 1$ con un subíndice para aclarar que se corresponden con los estados básicos de un sistema formado por p cúbits):

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

En particular, dado $j \in \{0, \dots, 2^{p-1}\}$, $|j\rangle_p = |\vec{j}\rangle$, donde $|\vec{j}\rangle = |\vec{j}_1 \dots \vec{j}_p\rangle$ (\vec{j}_1 es el bit más significativo), siendo $\vec{j} \in \{0, 1\}^p$ tal que

$$j = \sum_{k=1}^p \vec{j}_k 2^{p-k}.$$

Por ejemplo, en el caso de tener $p = 3$ cúbits, el número de estados básicos es $n = 2^3 = 8$:

$$\begin{aligned} |0\rangle_3 &= |000\rangle, \\ |1\rangle_3 &= |001\rangle, \\ |2\rangle_3 &= |010\rangle, \\ |3\rangle_3 &= |011\rangle, \\ |4\rangle_3 &= |100\rangle, \\ |5\rangle_3 &= |101\rangle, \\ |6\rangle_3 &= |110\rangle, \\ |7\rangle_3 &= |111\rangle. \end{aligned}$$

Por lo tanto, las siguientes notaciones son equivalentes:

$$|\psi\rangle = \sum_{\vec{j} \in \{0,1\}^3} \alpha_{\vec{j}} |\vec{j}\rangle = \sum_{j=0}^{2^3-1} \alpha_j |j\rangle_3.$$

De forma general, para un p -cúbit $|\psi\rangle$,

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

Observación 1.11. Alternativamente a la identificación que hemos hecho de los estados básicos en un sistema formado por múltiples cúbits, en la bibliografía, se suele emplear la siguiente regla para la construcción del producto tensorial entre dos estados $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \in \mathbb{C}^2$ y $|\varphi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle \in \mathbb{C}^2$:

$$\begin{aligned} |\psi\rangle \otimes |\varphi\rangle &= \begin{pmatrix} \alpha_0 \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \\ \alpha_1 \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha_0 \beta_0 \\ \alpha_0 \beta_1 \\ \alpha_1 \beta_0 \\ \alpha_1 \beta_1 \end{pmatrix} \\ &= \alpha_0 \beta_0 |00\rangle + \alpha_0 \beta_1 |01\rangle + \alpha_1 \beta_0 |10\rangle + \alpha_1 \beta_1 |11\rangle \in (\mathbb{C}^2)^{\otimes 2} \cong \mathbb{C}^4. \end{aligned}$$

Observar que el producto de dos estados cuánticos representados por 1-cúbit es un estado cuántico de 2-cúbits,

$$\begin{aligned} |\alpha_0 \beta_0|^2 + |\alpha_0 \beta_1|^2 + |\alpha_1 \beta_0|^2 + |\alpha_1 \beta_1|^2 &= |\alpha_0|^2 (|\beta_0|^2 + |\beta_1|^2) + |\alpha_1|^2 (|\beta_0|^2 + |\beta_1|^2) \\ &= |\alpha_0|^2 + |\alpha_1|^2 = 1. \end{aligned}$$

En particular, podemos obtener los estados básicos del espacio \mathbb{C}^4 aplicando la regla anterior para obtener el producto tensorial de los estados básicos del espacio \mathbb{C}^2 . De esta forma, por ejemplo,

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix}.$$

Esta regla que acabamos de describir para la construcción del producto tensorial de dos estados cuánticos se puede trasladar, tal y como veremos, a la construcción del producto tensorial de operadores lógicos.

Observación 1.12. Debemos observar que, aunque el producto tensorial de dos 1-cúbits del espacio \mathbb{C}^2 es 2-cúbit del espacio $(\mathbb{C}^2)^{\otimes 2}$, no todos los estados 2-cúbits de $(\mathbb{C}^2)^{\otimes 2}$ se pueden expresar como producto tensorial de 1-cúbits del espacio \mathbb{C}^2 . Por ejemplo, el estado

$$|\psi\rangle = \frac{1}{2} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle,$$

se puede expresar como el producto tensorial:

$$\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right).$$

Sin embargo, el estado

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

no se puede expresar como el producto tensorial de dos estados, como se verá más adelante. Esta observación nos lleva a la siguiente definición.

Definición 1.13 (Estado producto y entrelazamiento). Un p -cúbit $|\psi\rangle \in (\mathbb{C}^2)^{\otimes p}$ es un *estado producto* si se puede expresar como el producto tensorial de p 1-cúbits $\{|\psi_k\rangle\}_{k=1}^p$:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_p\rangle = \bigotimes_{k=1}^p |\psi_k\rangle.$$

En el caso de que no sea posible expresarlo como producto tensorial de p 1-cúbits, diremos que está *entrelazado*.

Observación 1.14. Se puede comprobar (ver [306, Example 2.9]) que un 2-cúbit $|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$ se puede expresar como el producto tensorial de dos 1-cúbits si y solamente si se cumple la siguiente condición de entrelazamiento:

$$\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}. \quad (1.1)$$

En particular, el conjunto de estados cuánticos que podemos representar con q -cúbits es más grande que el que podemos representar con el producto tensorial de q estados cuánticos de un cúbit.

Ejemplo 1.15. A la vista de la definición anterior, el 2-cúbit

$$|\psi\rangle = \frac{1}{2} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle$$

es un estado producto de dos 1-cúbits ya que cumple la condición de entrelazamiento (1.1). Es más, ya hemos visto que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, donde:

$$|\psi_1\rangle = |\psi_2\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle.$$

Por otro lado, el 2-cúbit

$$|\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

está entrelazado ya que no cumple la condición de entrelazamiento (1.1).



2 Circuitos cuánticos

El elemento fundamental de la computación cuántica es el circuito o algoritmo cuántico cuántico. Un circuito cuántico es una rutina computacional que consiste en una secuencia ordenada de puertas cuánticas lógicas, mediciones y reinicios cuánticos, que pueden estar condicionados por algún tipo de computación clásica en tiempo real. Es importante destacar que, como veremos en la siguiente sección, las operaciones (puertas) que podemos hacer en un ordenador cuántico se corresponden, salvo la medición, con operadores unitarios. En particular, y al contrario de lo que ocurre en computación clásica, las puertas cuánticas son lineales y reversibles. Aunque estas dos propiedades pueden parecer a priori muy restrictivas, un ordenador cuántico universal es Turing-completo [141].

Un circuito cuántico se representa indicando qué operaciones se realizan en cada cúbit o grupo de cúbits. En el caso de que tengamos una computadora cuántica de p cúbits, representamos p líneas (cada una de las cuales representa un cúbit), donde la línea superior indica el cúbit 1 y el resto se numeran en orden creciente (ver Figura 2.1). Las operaciones

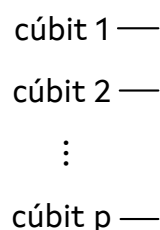


Fig. 2.1. Notación para un conjunto de p cúbits en un circuito cuántico.

o puertas lógicas toman líneas de cúbits como entrada, tienen el mismo número de líneas de cúbits como salida y aplican la matriz unitaria indicada en la puerta al estado cuántico de esos cúbits (ver Figura 2.2). Es importante destacar que los diagramas se leen de

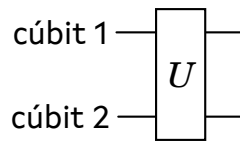


Fig. 2.2. Notación para una puerta lógica U que actúa sobre un 2-cúbit.

izquierda a derecha (debido a que cada operación se corresponde con una matriz unitaria la dirección de lectura no es obvia). Por ejemplo, en el circuito de la Figura 2.3, primero aplicamos la puerta A al 2-cúbit $|\psi\rangle$ y luego aplicamos la puerta B al 2-cúbit $A|\psi\rangle$. Tendremos entonces que $|\varphi\rangle = BA|\psi\rangle$. Cuando tengamos un circuito formado por varios

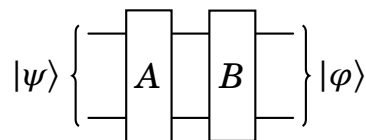


Fig. 2.3. Ejemplo de circuito cuántico con dos puertas lógicas que actúan sobre un 2-cúbit.

cúbits, es posible aplicar una puerta sobre un único cúbit (entendemos que en el resto aplicamos el operador identidad). Por ejemplo, el circuito de la Figura 2.4 es equivalente

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \left\{ \begin{array}{c} \boxed{U} \\ \hline \end{array} \right\} |\varphi\rangle = (U|\varphi_1\rangle \otimes |\varphi_2\rangle)$$

Fig. 2.4. Puerta lógica U actuando sobre el primer cúbit.

al de la Figura 2.5 (en las siguientes secciones detallaremos el producto tensorial de dos operadores).

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \left\{ \begin{array}{c} \boxed{U \otimes I} \\ \hline \end{array} \right\} |\varphi\rangle = (U \otimes I) (|\varphi_1\rangle \otimes |\varphi_2\rangle)$$

Fig. 2.5. Puerta lógica $U \times I$ actuando sobre los dos cúbits.

2.1 Puertas lógicas para cúbits

Las operaciones que podemos hacer sobre estados cuánticos deben satisfacer ciertas condiciones para asegurar que se mantienen las propiedades básicas del estado cuántico.

Definición 2.1 (Puerta lógica para un cúbit). Una puerta lógica para un cúbit es una matriz $U \in \mathcal{M}_{2 \times 2}(\mathbb{C})$ tal que $U^\dagger U = U U^\dagger = I_2$. Esto es, cualquier matriz unitaria es una puerta lógica.

Es importante destacar que todas las puertas lógicas son operadores lineales invertibles que preservan la norma.

Observación 2.2. Recordemos que cuando introducimos la esfera de Bloch comentamos que los estados $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ y $|\varphi\rangle = e^{i\theta}(\alpha|0\rangle + \beta|1\rangle)$ son indistinguibles. Por un lado resulta claro que si medimos el estado $|\psi\rangle$ obtenemos el estado básico $|0\rangle$ con probabilidad $|\alpha|^2$ y el estado $|1\rangle$ con probabilidad $|\beta|^2$. Al medir el estado $|\varphi\rangle$, obtenemos exactamente lo mismo, ya que $|e^{i\theta}| = 1$. Por otro lado, dada una puerta lógica U , tampoco observaremos diferencias visibles entre $U|\psi\rangle$ y $U|\varphi\rangle$.

A continuación listamos las puertas lógicas más importantes para un solo cúbit expresadas en términos de los estados básicos $\{|0\rangle, |1\rangle\}$.

◊ *Factor de fase (Phase-factor):*

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

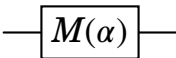


Fig. 2.6. Notación para la puerta Phase-factor.

◊ *Desplazamiento de fase (Phase-shift):*

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

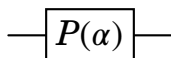


Fig. 2.7. Notación para la puerta Phase-shift.

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

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

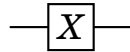


Fig. 2.8. Notación para la puerta Pauli-X.

◊ Matriz de Pauli Y (Pauli-Y):

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

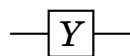


Fig. 2.9. Notación para la puerta Pauli-Y.

◊ Matriz de Pauli Z (Pauli-Z):

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

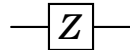


Fig. 2.10. Notación para la puerta Pauli-Z.

◊ Puerta de Hadamard:

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

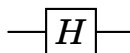



Fig. 2.11. Notación para la puerta de Hadamard.

Ejemplo 2.3. Tal y como comentamos cuando introducimos la esfera de Bloch, ciertas puertas lógicas se corresponden con movimientos rígidos de la esfera de Bloch. Por ejemplo, la puerta Pauli-X sobre los cúbits del Ejemplo 1.5 actúa de la siguiente manera:

◊ $|0\rangle \xrightarrow{X} |1\rangle$ transforma $|\psi(0, \varphi)\rangle$ en $|\psi(\pi, \varphi)\rangle$.

◊ $|+\rangle \xrightarrow{X} |+\rangle$ deja invariante $|\psi(\pi/2, 0)\rangle$.

- ◊ $|-\rangle \xrightarrow{X} |-\rangle$ deja invariante $|\psi(\pi/2, \pi)\rangle$.
- ◊ $|+i\rangle \xrightarrow{X} |-i\rangle$ transforma $|\psi(\pi/2, \pi/2)\rangle$ en $|\psi(\pi/2, 3\pi/2)\rangle$.
- ◊ $|-i\rangle \xrightarrow{X} |+i\rangle$ transforma $|\psi(\pi/2, 3\pi/2)\rangle$ en $|\psi(\pi/2, \pi/2)\rangle$.

En particular, la puerta Pauli-X se corresponde con una rotación de 180° con respecto al eje X en la esfera de Bloch. Análogamente, podemos comprobar que la puerta Pauli-Y se corresponde con una rotación de 180° con respecto al eje Y y que la puerta Pauli-Z se corresponde con una rotación de 180° con respecto al eje Z . En lo que respecta a la puerta de Hadamard, esta se corresponde con una rotación de 180° con respecto al eje $X + Z$. 

Para terminar esta sección en la que analizamos algunas de las puertas más importantes para un cúbit, remarcamos que todas ellas pueden ser representadas, en esencia, por la siguiente matriz parametrizada que describe todo los operadores unitarios [306]:

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

Cualquier matriz unitaria puede ser obtenida empleando la matriz anterior eligiendo de forma apropiada los parámetros θ , φ y λ . Es más (ver [244], [312, Section 4.5]), cualquier matriz unitaria puede ser aproximada con una precisión arbitraria por una secuencia finita compuesta por puertas H , $P(\pi/4)$ y CNOT (ver Sección 2.2).

2.2 Puertas lógicas para p -cúbits

Al igual que en caso de un cúbit, una *puerta lógica* para un circuito formado por p cúbits se puede definir como un operador unitario.

Definición 2.4 (Puerta lógica para un p -cúbit). Una puerta lógica para un p -cúbit es una matriz $U \in \mathcal{M}_{2^p \times 2^p}(\mathbb{C})$ tal que $U^\dagger U = U U^\dagger = I_{2^p}$, siendo U^\dagger la matriz conjugada transpuesta.

Una de las formas más frecuentes de construir puertas lógicas para sistemas formados por varios cúbits es a través del producto tensorial de puertas lógicas para uno o varios cúbits. En la Observación 1.11 establecíamos una regla para obtener el producto tensorial de dos cúbits y avanzábamos que dicha regla se podía extender al caso de considerar operadores lógicos sobre cúbits.

Definición 2.5 (Producto de Kronecker). Sean $A \in \mathcal{M}_{m \times n}(\mathbb{C})$ y $B \in \mathcal{M}_{p \times q}(\mathbb{C})$, definimos el producto de Kronecker $A \otimes B \in \mathcal{M}_{mp \times nq}(\mathbb{C})$ como:

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

Si consideramos la base canónica de los espacios vectoriales $\mathcal{M}_{m \times n}(\mathbb{C})$ y $\mathcal{M}_{p \times q}(\mathbb{C})$, la operación bilineal \otimes definida sobre el producto tensorial $\mathcal{M}_{m \times n}(\mathbb{C}) \otimes \mathcal{M}_{p \times q}(\mathbb{C})$ es simplemente el producto de Kronecker.

A continuación listamos algunas propiedades del producto tensorial que nos resultarán de utilidad a la hora de trabajar con puertas lógicas definidas sobre sistemas formados por múltiples cúbits.

Proposición 2.6. Sean $A, B \in \mathcal{M}_{m \times m}(\mathbb{C})$ y $C, D \in \mathcal{M}_{n \times n}(\mathbb{C})$, $u, v \in \mathbb{C}^m$, $w, x \in \mathbb{C}^n$ y $a, b \in \mathbb{C}$. Se tendrá que:

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. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

Es frecuente cuando queremos hacer el producto tensorial de un operador lineal A por si mismo n veces emplear la notación $A^{\otimes n} = A \otimes \cdots \otimes A$.

Gracias a la proposición anterior podemos asegurar que el producto tensorial de dos puertas unitarias sigue siendo una puerta unitaria.

Corolario 2.7. Sean $U \in \mathcal{M}_{2^p \times 2^p}(\mathbb{C})$ y $V \in \mathcal{M}_{2^q \times 2^q}(\mathbb{C})$ dos operadores unitarios. Entonces,

1. $U \otimes V$ es un operador unitario en el espacio $\mathcal{M}_{2^{p+q} \times 2^{p+q}}(\mathbb{C})$.
2. $(U \otimes V)(|\psi\rangle_p \otimes |\varphi\rangle_q) = (U|\psi\rangle_p) \otimes (V|\varphi\rangle_q)$.

Ejemplo 2.8. Consideremos un circuito cuántico compuesto por dos cúbits que están inicializados al estado cuántico básico $|0\rangle \otimes |0\rangle$ y apliquemos a continuación la puerta $H^{\otimes 2} = H \otimes H$ sobre $|0\rangle \otimes |0\rangle$. Gracias a la proposición anterior:

$$|\varphi\rangle := H^{\otimes 2}(|0\rangle \otimes |0\rangle) = (H|0\rangle) \otimes (H|0\rangle).$$

$$\begin{array}{l}
 |0\rangle \xrightarrow{H} |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 |0\rangle \xrightarrow{H} |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)
 \end{array}
 \quad
 \begin{array}{l}
 |0\rangle \xrightarrow{H^{\otimes 2}} \\
 |0\rangle \xrightarrow{H^{\otimes 2}}
 \end{array}
 \left. \vphantom{\begin{array}{l} |0\rangle \\ |0\rangle \end{array}} \right\} |\varphi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

Fig. 2.12. Dos circuitos equivalentes asociados al producto tensorial de dos puertas de Hadamard.

En particular, los circuitos de la Figura 2.12 son equivalentes.

Para convencernos de que realmente estamos haciendo lo mismo, basta comprobar los cálculos. En el circuito que tenemos a la izquierda lo que estamos haciendo es calcular $(H|0\rangle) \otimes (H|0\rangle)$:

$$\begin{aligned}
 (H|0\rangle) \otimes (H|0\rangle) &= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \\
 &= \frac{1}{2}|0\rangle \otimes |0\rangle + \frac{1}{2}|0\rangle \otimes |1\rangle + \frac{1}{2}|1\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |1\rangle \\
 &= \frac{1}{\sqrt{2}^2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}^2} \sum_{\vec{j} \in \{0,1\}^2} |\vec{j}\rangle = \frac{1}{\sqrt{2}^2} \sum_{j=0}^{2^2-1} |j\rangle_2.
 \end{aligned}$$

En el circuito que tenemos a la derecha calculamos directamente $H^{\otimes 2}|00\rangle$. Ahora bien,

$$\begin{aligned}
 H^{\otimes 2} &= H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \\
 &= \frac{1}{\sqrt{2}} \left(\begin{array}{cc|cc} 1/\sqrt{2} & 1/\sqrt{2} & 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} & 1/\sqrt{2} & -1/\sqrt{2} \\ \hline 1/\sqrt{2} & 1/\sqrt{2} & -1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} & -1/\sqrt{2} & 1/\sqrt{2} \end{array} \right) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.
 \end{aligned}$$

Por lo tanto,

$$H^{\otimes 2}|00\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle),$$

que es precisamente lo que obteníamos anteriormente.


Observamos que la aplicación del producto tensorial de puertas de Hadamard sobre el primer estado básico produce una superposición uniforme de los estados básicos. Esto último es el motivo por el cual se empleará en muchos algoritmos cuánticos.

Podemos generalizar el circuito anterior al caso de considerar p -cúbits inicializados al primer estado básico. En este caso,

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

Por lo tanto,

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

recuperando así una superposición uniforme de los $n = 2^p$ estados básicos del sistema formado por p -cúbits. 

Ejemplo 2.9. Existen puertas para sistemas de múltiples cúbits que no pueden ser representadas como el producto tensorial de puertas de un cúbit. A continuación listamos algunas de las más importantes.

1. *Puerta CNOT* (puerta NOT controlada). La puerta CNOT es una puerta para sistemas de 2-cúbits que tiene un cúbit de control y un cúbit objetivo. Si el cúbit de control es igual a $|0\rangle$ no se hace nada y, en el caso en el que el cúbit de control sea igual a $|1\rangle$, se intercambia $|0\rangle$ por $|1\rangle$ en el cúbit objetivo. Normalmente se incluyen dos subíndices para indicar quien es el cúbit de control y el cúbit objetivo. Por ejemplo, $CNOT_{12}$ indica que el cúbit de control es el primero y el segundo es el objetivo y $CNOT_{21}$ indica que el cúbit de control es el segundo y el primero es el objetivo. Veamos como actúa cada una de ellas sobre los estados básicos de un sistema formado por 2-cúbits.

◇ Puerta $CNOT_{12}$:

$$\begin{aligned} CNOT_{12} |00\rangle &= CNOT_{12}(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle = |00\rangle, \\ CNOT_{12} |01\rangle &= CNOT_{12}(|0\rangle \otimes |1\rangle) = |0\rangle \otimes |1\rangle = |01\rangle, \\ CNOT_{12} |10\rangle &= CNOT_{12}(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle = |11\rangle, \\ CNOT_{12} |11\rangle &= CNOT_{12}(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |0\rangle = |10\rangle. \end{aligned}$$

Se tiene, por lo tanto, la siguiente matriz asociada:

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

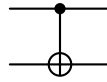


Fig. 2.13. Notación para la puerta $CNOT_{12}$.

◇ Puerta $CNOT_{21}$:

$$CNOT_{21} |00\rangle = CNOT_{21}(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle = |00\rangle,$$

$$CNOT_{21} |01\rangle = CNOT_{21}(|0\rangle \otimes |1\rangle) = |1\rangle \otimes |1\rangle = |11\rangle,$$

$$CNOT_{21} |10\rangle = CNOT_{21}(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |0\rangle = |10\rangle,$$

$$CNOT_{21} |11\rangle = CNOT_{21}(|1\rangle \otimes |1\rangle) = |0\rangle \otimes |1\rangle = |01\rangle.$$

Se tiene, por lo tanto, la siguiente matriz asociada:

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

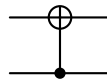


Fig. 2.14. Notación para la puerta $CNOT_{21}$.

2. *Puerta SWAP.* La puerta SWAP es una puerta para sistemas de 2-cúbits (se puede generalizar para sistemas de múltiples cúbits). La actuación de la puerta SWAP sobre un estado cuántico representado por dos cúbits lo transforma en otro estado en donde cada uno de los estados básicos tiene los dígitos permutados:

$$SWAP |00\rangle = |00\rangle,$$

$$SWAP |01\rangle = |10\rangle,$$

$$SWAP |10\rangle = |01\rangle,$$

$$SWAP |11\rangle = |11\rangle.$$

La matriz asociada es, por lo tanto,

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



Fig. 2.15. Notación para la puerta SWAP.

Veamos como actúa la puerta SWAP sobre el producto tensorial de dos estados. Sea $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ y $|\varphi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$. Se tendrá que

$$\begin{aligned} \text{SWAP}(|\psi\rangle \otimes |\varphi\rangle) &= \text{SWAP}((\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle)) \\ &= \text{SWAP}(\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle) \\ &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |10\rangle + \alpha_1\beta_0 |01\rangle + \alpha_1\beta_1 |11\rangle \\ &= (\beta_0 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) = |\varphi\rangle \otimes |\psi\rangle. \end{aligned}$$

La puerta lógica SWAP también se puede obtener aplicando CNOT_{12} , CNOT_{21} y CNOT_{12} de forma iterada. En efecto:

$$\begin{aligned} \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12} |00\rangle &= \text{CNOT}_{12}\text{CNOT}_{21} |00\rangle = \text{CNOT}_{12} |00\rangle = |00\rangle, \\ \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12} |01\rangle &= \text{CNOT}_{12}\text{CNOT}_{21} |01\rangle = \text{CNOT}_{12} |11\rangle = |10\rangle, \\ \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12} |10\rangle &= \text{CNOT}_{12}\text{CNOT}_{21} |11\rangle = \text{CNOT}_{12} |01\rangle = |01\rangle, \\ \text{CNOT}_{12}\text{CNOT}_{21}\text{CNOT}_{12} |11\rangle &= \text{CNOT}_{12}\text{CNOT}_{21} |10\rangle = \text{CNOT}_{12} |10\rangle = |11\rangle. \end{aligned}$$

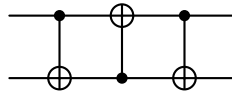


Fig. 2.16. Puerta SWAP expresada en función de puertas CNOT.

3. **Puerta CCNOT** (puerta NOT doblemente controlada). La puerta CCNOT actúa sobre un sistema de 3-cúbits de forma que si el primer y el segundo cúbit son igual a $|1\rangle$, se intercambia el $|0\rangle$ por $|1\rangle$ en el tercer cúbit. En otro caso, no se hace nada:

$$\begin{aligned} \text{CCNOT} |000\rangle &= |000\rangle, \\ \text{CCNOT} |001\rangle &= |001\rangle, \\ \text{CCNOT} |010\rangle &= |010\rangle, \\ \text{CCNOT} |011\rangle &= |011\rangle, \\ \text{CCNOT} |100\rangle &= |100\rangle, \\ \text{CCNOT} |101\rangle &= |101\rangle, \\ \text{CCNOT} |110\rangle &= |111\rangle, \\ \text{CCNOT} |111\rangle &= |110\rangle. \end{aligned}$$

En este caso, la matriz asociada es

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

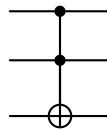



Fig. 2.17. Notación para la puerta CCNOT.

Otra forma de definir la puerta CCNOT es a partir de la siguiente expresión:

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

donde $x, y, z \in \{0, 1\}$ y \oplus representa la suma módulo 2. Observar que si $z = 0$, entonces,

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

esto es, el tercer cúbit se corresponde con la puerta lógica AND. En particular, la puerta CCNOT es la versión cuántica de la puerta lógica clásica AND. Esto es coherente con el hecho de que un ordenador cuántico es Turing-completo. 

2.3 Puertas de medida

Mientras que en un ordenador clásico podemos simplemente leer el estado de los bits, en un ordenador cuántico no tenemos acceso sin restricciones al estado cuántico de un determinado cúbit. La información sobre el estado cuántico es de tipo probabilista y solamente se puede acceder a ella a través de una *puerta de medida*.

Definición 2.10 (Puerta de medida). Dado un p -cúbit $|\psi\rangle = \sum_{\vec{j} \in \{0,1\}^p} \alpha_{\vec{j}} |\vec{j}\rangle$ una puerta de medida en el cúbit k proporciona:

◊ 0 con probabilidad

$$\sum_{\vec{j} \in \{0,1\}^p: \vec{j}_k=0} |\alpha_{\vec{j}}|^2.$$

◊ 1 con probabilidad

$$\sum_{\vec{j} \in \{0,1\}^p: \vec{j}_k=1} |\alpha_{\vec{j}}|^2.$$

Sea $x \in \{0, 1\}$, el valor medido. Después de la medición el estado cuántico resultante es

$$|\psi'\rangle = \sum_{\vec{j} \in \{0,1\}^p: \vec{j}_k=x} \frac{\alpha_{\vec{j}}}{\sqrt{\sum_{\vec{j} \in \{0,1\}^p: \vec{j}_k=x} |\alpha_{\vec{j}}|^2}} |\vec{j}\rangle.$$

El estado cuántico después de la medida colapsa a una combinación lineal de los estados básicos que son coherentes con el resultado de la medición. Esto es, los estados básicos $|\vec{j}\rangle$ tales que $\vec{j}_k = x$. Los coeficientes asociados a la combinación lineal son normalizados para obtener un vector unitario.

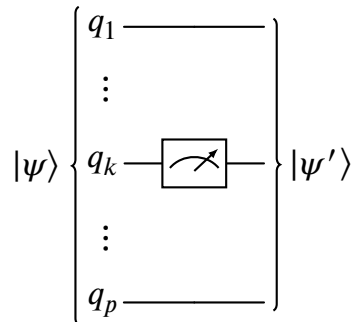


Fig. 2.18. Puerta de medida actuando sobre el cúbit k .

Ejemplo 2.11. Consideremos el estado $\psi = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$. Se tendrá que:

◊ Si medimos el primer cúbit, obtendremos:

✱ El valor 0 con probabilidad $|\alpha_{00}|^2 + |\alpha_{01}|^2$, quedando el siguiente estado resultante después de la medición:

$$|\psi'\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

✱ El valor 1 con probabilidad $|\alpha_{10}|^2 + |\alpha_{11}|^2$, quedando el siguiente estado resultante después de la medición:

$$|\psi'\rangle = \frac{\alpha_{10} |10\rangle + \alpha_{11} |11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}.$$

◊ Si medimos el segundo cúbit, obtendremos:

- ✱ El valor 0 con probabilidad $|\alpha_{00}|^2 + |\alpha_{10}|^2$, quedando el siguiente estado resultante después de la medición:

$$|\psi'\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{10} |10\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{10}|^2}}.$$

- ✱ El valor 1 con probabilidad $|\alpha_{01}|^2 + |\alpha_{11}|^2$, quedando el siguiente estado resultante después de la medición:

$$|\psi'\rangle = \frac{\alpha_{01} |01\rangle + \alpha_{11} |11\rangle}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}}.$$



Observación 2.12. Consideremos el Ejemplo 2.11. Al medir el primer cúbit obtenemos el valor 0 con probabilidad $|\alpha_{00}|^2 + |\alpha_{01}|^2$ y estado resultante tras la medición:

$$|\psi'\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

A continuación, midamos el segundo cúbit. Obtenemos 0 con probabilidad

$$\frac{|\alpha_{00}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2},$$

con estado post-medición

$$|\psi''\rangle = |00\rangle.$$

Así, la probabilidad de llegar al estado $|00\rangle$ después de dos medidas es

$$(|\alpha_{00}|^2 + |\alpha_{01}|^2) \frac{|\alpha_{00}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2} = |\alpha_{00}|^2.$$

Podríamos pensar que el orden en el que medimos los cúbits puede influir en el resultado. Por ejemplo, supongamos que medimos el segundo cúbit en primer lugar. La probabilidad de obtener 0 es $|\alpha_{00}|^2 + |\alpha_{10}|^2$, siendo el estado resultante después de la medida

$$|\psi'\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{10} |10\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{10}|^2}}.$$

A continuación midamos el primer cúbit. Obtenemos el valor 0 con probabilidad

$$\frac{|\alpha_{00}|^2}{|\alpha_{00}|^2 + |\alpha_{10}|^2},$$

con estado post-medición

$$|\psi''\rangle = |00\rangle.$$

Así, la probabilidad de llegar al estado $|00\rangle$ después de dos medidas es

$$(|\alpha_{00}|^2 + |\alpha_{10}|^2) \frac{|\alpha_{00}|^2}{|\alpha_{00}|^2 + |\alpha_{10}|^2} = |\alpha_{00}|^2.$$

Llegamos, por lo tanto, al mismo estado.

Esta observación que acabamos de hacer para el caso particular de considerar un sistema de 2-cúbits, se puede generalizar (ver [306, Proposition 3.6.]). Dado un p -cúbit $|\psi\rangle = \sum_{\vec{j} \in \{0,1\}^p} \alpha_{\vec{j}} |\vec{j}\rangle$, si aplicamos una puerta de medida sobre cada uno de los p cúbits en cualquier orden, obtenemos el estado $|\vec{j}\rangle$ con probabilidad $|\alpha_{\vec{j}}|^2$, para todo $\vec{j} \in \{0,1\}^p$. En particular, son equivalentes los circuitos cuánticos de la Figura 2.19.

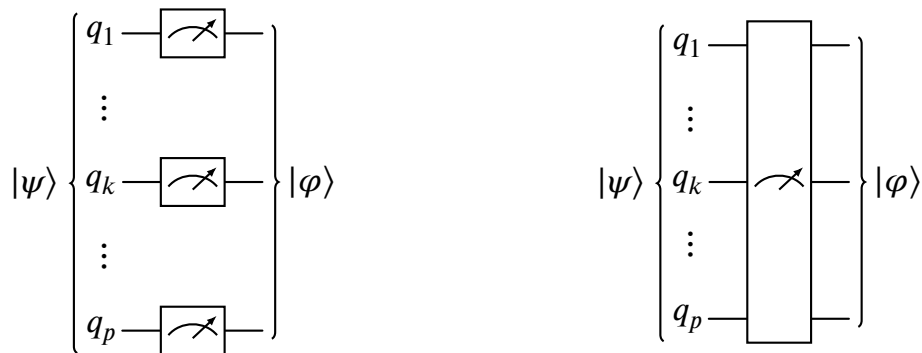


Fig. 2.19. Circuitos cuánticos equivalentes asociados a la medida de un p -cúbit.

Ejemplo 2.13. Volvamos a considerar los 2-cúbits del Ejemplo 1.15, que denotaremos ahora por

$$\begin{aligned} |\psi\rangle &= \frac{1}{2} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle, \\ |\varphi\rangle &= \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle. \end{aligned} \tag{2.1}$$

Para simplificar el desarrollo del ejemplo, denotaremos por $\Pr_{|\psi\rangle}(Q_k \stackrel{M}{=} x)$ la probabilidad de que el cúbit $k \in \{1, \dots, p\}$ del p -cúbit $|\psi\rangle$ tome el valor $x \in \{0, 1\}$. Veamos como influye el entrelazamiento a la hora de realizar medidas sobre los 2-cúbits anteriores.

◊ Comencemos analizando el 2-cúbit $|\psi\rangle$ definido en (2.1). Por un lado,

$$\Pr_{|\psi\rangle}(Q_1 \stackrel{M}{=} 0) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2},$$

$$\Pr_{|\psi\rangle}(Q_1 \stackrel{M}{=} 1) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2},$$

$$\Pr_{|\psi\rangle}(Q_2 \stackrel{M}{=} 0) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2},$$

$$\Pr_{|\psi\rangle}(Q_2 \stackrel{M}{=} 1) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

Supongamos que medimos el segundo cúbit y obtenemos el valor 1, el estado resultante después de la medición es

$$|\psi'\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Por lo tanto,

$$\Pr_{|\psi'\rangle}(Q_1 \stackrel{M}{=} 0) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2},$$

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

Esto es, la probabilidad de que el primer cúbit tome el valor 0 o 1 no cambia después de la primera medida.

◊ Consideremos ahora el 2-cúbit $|\varphi\rangle$ definido en (2.1). Por un lado,

$$\Pr_{|\varphi\rangle}(Q_1 \stackrel{M}{=} 0) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2},$$

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

$$\Pr_{|\varphi\rangle}(Q_2 \stackrel{M}{=} 0) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2},$$

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

Al igual que en el caso anterior, supongamos que medimos el segundo cúbit y obtenemos el valor 1, el estado resultante después de la medición es

$$|\varphi'\rangle = |11\rangle.$$

Por lo tanto,

$$\Pr_{|\varphi'\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 0) = 0,$$

$$\Pr_{|\varphi'\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 1) = 1.$$

Esto es, la probabilidad de que el primer cúbit tome el valor 0 o 1 cambia después de la medida. Esta situación es muy distinta a la anterior y es causada, fundamentalmente, por el hecho de que el 2-cúbit $|\varphi\rangle$ está entrelazado: cuando un p -cúbit está entrelazado, una medida realizada sobre uno de los cúbits afecta a la distribución de probabilidad del resto de cúbits. ✎

Observación 2.14. Lo que hemos observado en el ejemplo anterior para los estados definidos en (2.1) se puede interpretar en términos de probabilidades condicionadas. Sea $|\psi\rangle$ un 2-cúbit,

- ◊ si $|\psi\rangle$ se puede expresar como el producto tensorial de dos 1-cúbits (no está entrelazado), entonces, $\Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} x) = \Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} x | \mathcal{Q}_1 \stackrel{M}{=} y)$, para todo $x, y \in \{0, 1\}$;
- ◊ si existen $x, y \in \{0, 1\}$ tal que $\Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} x) \neq \Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} x | \mathcal{Q}_1 \stackrel{M}{=} y)$, entonces $|\psi\rangle$ no se puede expresar como producto tensorial de dos 1-cúbits (está entrelazado).

En efecto, solo tendremos que demostrar la primera implicación ya que la segunda es la negación de la primera. Supongamos que $|\psi\rangle$ es un 2-cúbit que se puede expresar como el producto tensorial de dos 1-cúbits:

$$\begin{aligned} |\psi\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle. \end{aligned}$$

Se tendrá que

$$\begin{aligned} \Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 0) &= |\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 = |\alpha_0|^2 \Rightarrow |\psi'\rangle = \frac{\alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle}{\sqrt{\Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 0)}}, \\ \Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 1) &= |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = |\alpha_1|^2 \Rightarrow |\psi'\rangle = \frac{\alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle}{\sqrt{\Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 1)}}, \\ \Pr_{|\psi\rangle}(\mathcal{Q}_2 \stackrel{M}{=} 0) &= |\alpha_0\beta_0|^2 + |\alpha_1\beta_0|^2 = |\beta_0|^2 \Rightarrow |\psi'\rangle = \frac{\alpha_0\beta_0 |00\rangle + \alpha_1\beta_0 |10\rangle}{\sqrt{\Pr_{|\psi\rangle}(\mathcal{Q}_2 \stackrel{M}{=} 0)}}, \\ \Pr_{|\psi\rangle}(\mathcal{Q}_2 \stackrel{M}{=} 1) &= |\alpha_0\beta_1|^2 + |\alpha_1\beta_1|^2 = |\beta_1|^2 \Rightarrow |\psi'\rangle = \frac{\alpha_0\beta_1 |01\rangle + \alpha_1\beta_1 |11\rangle}{\sqrt{\Pr_{|\psi\rangle}(\mathcal{Q}_2 \stackrel{M}{=} 1)}}. \end{aligned}$$

Por lo tanto:

$$\Pr_{|\psi\rangle}(\mathcal{Q}_2 \stackrel{M}{=} 0 | \mathcal{Q}_1 \stackrel{M}{=} 0) = \frac{|\alpha_0\beta_0|^2}{\Pr_{|\psi\rangle}(\mathcal{Q}_1 \stackrel{M}{=} 0)} = |\beta_0|^2 = \Pr_{|\psi\rangle}(\mathcal{Q}_2 \stackrel{M}{=} 0).$$

El resto de las identidades se obtienen de forma análoga.

Observación 2.15 (El principio de no clonación). Puesto que al realizar una medida se destruye el estado cuántico, es natural preguntarse si es posible realizar una copia o clon de dicho estado. Si disponemos de dicho clon, podemos realizar las mediciones sobre el mismo sin destruir el estado original o realizar varias mediciones (si disponemos de varios clones) sin necesidad de repetir el circuito cuántico de nuevo. Lamentablemente, esto no es posible. La razón fundamental es que no existe una matriz unitaria que transforme un estado $|\psi\rangle \otimes |0\rangle_p$ en el estado $|\psi\rangle \otimes |\psi\rangle_p$. En efecto, supongamos que existe una matriz unitaria $U \in \mathcal{M}_{2^{2p} \times 2^{2p}}(\mathbb{C})$ tal que

$$U\left(|\psi\rangle \otimes |0\rangle_p\right) = |\psi\rangle \otimes |\psi\rangle, \quad U\left(|\varphi\rangle \otimes |0\rangle_p\right) = |\varphi\rangle \otimes |\varphi\rangle,$$

para cualquier par de p -cúbits $|\psi\rangle$ y $|\varphi\rangle$. Se tendrá entonces que

$$\begin{aligned} \langle\varphi|\psi\rangle &= \langle\varphi|\psi\rangle \langle 0|_p |0\rangle_p = \langle\varphi|\psi\rangle \otimes \left(\langle 0|_p |0\rangle_p\right) = \left(\langle\varphi| \otimes \langle 0|_p\right) \left(|\psi\rangle \otimes |0\rangle_p\right) \\ &= \left(\langle\varphi| \otimes \langle 0|_p\right) U^\dagger U \left(|\psi\rangle \otimes |0\rangle_p\right) = \left(\langle\varphi| \otimes \langle\varphi|\right) \left(|\psi\rangle \otimes |\psi\rangle\right) = \langle\varphi|\psi\rangle^2, \end{aligned}$$

lo cual solamente es cierto si $\langle\varphi|\psi\rangle = 1$ o 0 . Esto contradice el hecho de que $|\psi\rangle$ y $|\varphi\rangle$ son dos p -cúbits arbitrarios.

Es importante destacar que, aunque no es posible clonar un determinado cúbit, si es posible realizar un tipo limitado de copia que puede ayudar a replicar cálculos y amplificar la probabilidad de éxito de los algoritmos después de medir. En efecto, por [266, Theorem 6.1], dado $p \geq 1$, es posible construir una matriz unitaria $C_p \in \mathcal{M}_{2^{2p} \times 2^{2p}}(\mathbb{C})$ tal que, dado un elemento

$$|a'\rangle = \sum_{\vec{j}, \vec{k} \in \{0,1\}^p} a'_{\vec{j}\vec{k}} |\vec{j}\vec{k}\rangle \in \mathbb{C}^{2^{2p}},$$

$C_p |a'\rangle = |b\rangle$, donde:

$$b_{\vec{j}\vec{k}} = a'_{\vec{j}(\vec{j} \oplus \vec{k})}.$$

En particular, si $|a'\rangle = |a\rangle \otimes |0\rangle_p$, entonces,

$$a_{\vec{j}} = a'_{\vec{j}\vec{0}} = b_{\vec{j}\vec{j}}.$$

Esto es, la probabilidad de obtener el estado básico $|\vec{j}\vec{j}\rangle$ al medir $|b\rangle$ es la misma que la de obtener el estado $|\vec{j}\rangle$ al medir $|a\rangle$. Esto último tiene una repercusión muy importante y es que si $|a\rangle = |\vec{i}\rangle$, con $\vec{i} \in \{0,1\}^p$, es un estado básico, entonces $|b\rangle = |a\rangle \otimes |a\rangle$. Notar que esto no contradice el principio de no clonación pues, en el caso en el que $|a\rangle$ no sea un estado básico, no se tiene porqué cumplir que $C_p(|a\rangle \otimes |0\rangle_p) = |a\rangle \otimes |a\rangle$. Por ejemplo, si $|a\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$, entonces $C_1(|a\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \neq |a\rangle \otimes |a\rangle = \frac{1}{2} \sum_{\vec{j} \in \{0,1\}^2} |\vec{j}\rangle$.

El hecho de que no sea posible clonar un cúbit es una diferencia sustancial con respecto a la computación clásica en la cual podemos hacer todas las copias que queramos de un

determinado registro. A cambio de esta pequeña contrariedad, es posible realizar otras operaciones que son difícilmente alcanzables por un ordenador clásico. Destacamos, a modo de curiosidad, la teletransportación cuántica [312, Section 1.3.7] y el paralelismo cuántico [312, Section 1.4.2]. Tanto el principio de no clonación como las dos aplicaciones que acabamos de citar son fáciles de comprobar desde un punto de vista matemático, sin embargo, son difíciles de comprender desde un punto de vista físico.

3 Principales algoritmos cuánticos

En esta sección analizaremos algunos de los algoritmos cuánticos más importantes que luego aparecerán de forma recurrente cuando estudiemos algunos de los principales avances en computación cuántica desde un punto de vista de las matemáticas. Además de los listados en esta sección, existen una gran cantidad de algoritmos cuánticos interesantes que muestran las ventajas de la computación cuántica frente a la clásica. Destacamos, por ejemplo, los algoritmos de CHSH [120], Deutsch-Jozsa [142], Bernstein-Vazirani [55], Simon [374], etc.

3.1 Transformada de Fourier cuántica (QFT)

La Transformada de Fourier Cuántica (QFT por sus siglas en inglés) es la versión cuántica de la Transformada de Fourier Discreta (DFT por sus siglas en inglés) [312, Section 5.1]:

$$\mathbb{C}^n \xrightarrow{DFT} \mathbb{C}^n$$

$$\{x_j\}_{j=0}^{n-1} \mapsto \{y_k\}_{k=0}^{n-1}$$

donde, dado $k \in \{0, \dots, n-1\}$,

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{n-1} x_j \omega_n^{jk},$$

con $\omega_n^{jk} = e^{2\pi ijk/n}$.

La Transformada de Fourier Cuántica será una herramienta fundamental en muchos algoritmos cuánticos, en particular, en el algoritmo de estimación de fase, en el algoritmo HHL y en el algoritmo de factorización de Shor. El mejor algoritmo conocido para calcular la Transformada de Fourier Discreta es de orden de complejidad $O(n2^n)$, sin embargo, la Transformada Cuántica de Fourier es de orden $O(n^2)$. Es decir, se requieren exponencialmente más operaciones para calcular la Transformada de Fourier en un ordenador clásico que para implementar la transformada de Fourier cuántica en un ordenador cuántico. Lamentablemente, no podemos emplear la Transformada de Fourier Cuántica en muchas de las aplicaciones que requieren de la Transformada de Fourier Discreta. Uno de los motivos

es que no podemos acceder directamente a las amplitudes de todos los estados básicos en un circuito cuántico. A pesar de ello, será una herramienta crucial en algoritmos cuánticos como el HHL o el de Shor que sí suponen una ventaja frente a los mejores algoritmos clásicos conocidos.

Para definirla, emplearemos la Notación 1.10.

Definición 3.1 (QFT). Dado un sistema cuántico formado por p cúbits, definimos la *Transformada de Fourier Cuántica* como el siguiente operador unitario:

$$U_{QFT} := \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} \sum_{j=0}^{2^p-1} \omega_{2^p}^{jk} |k\rangle_p \langle j|_p, \quad (3.1)$$

donde

$$\omega_{2^p}^{jk} = e^{2\pi ijk/2^p}.$$

Observación 3.2. Veamos como actúa el operador unitario (3.1) sobre un p -cúbit $|X\rangle = \sum_{l=0}^{n-1} x_l |l\rangle_p$, donde $n = 2^p$. Se tendrá que:

$$U_{QFT} |X\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x_l \omega_n^{jk} |k\rangle_p \langle j|l\rangle_p = \sum_{k=0}^{n-1} \left(\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j \omega_n^{jk} \right) |k\rangle_p,$$

donde hemos usado la relación $\langle j|l\rangle_p = \delta_{jl}$, para todo $l, j \in \{0, \dots, n-1\}$. Esto es,

$$U_{QFT} |X\rangle = |Y\rangle,$$

con

$$|Y\rangle = \sum_{k=0}^{n-1} y_k |k\rangle_p,$$

siendo

$$y_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j \omega_n^{jk}.$$

Ejemplo 3.3. Consideremos un sistema cuántico formado por un único cúbit. Se tendrá que

$$U_{QFT} = \frac{1}{\sqrt{2}} \sum_{k=0}^1 \sum_{j=0}^1 \omega_2^{jk} |k\rangle |j\rangle = \frac{1}{\sqrt{2}} (\omega_2^{00} |0\rangle \langle 0| + \omega_2^{01} |1\rangle \langle 0| + \omega_2^{10} |0\rangle \langle 1| + \omega_2^{11} |1\rangle \langle 1|),$$


donde:

$$\begin{aligned} \omega_2^{00} &= e^{i0} = 1, \\ \omega_2^{01} &= e^{i0} = 1, \end{aligned}$$

$$\begin{aligned}\omega_2^{10} &= e^{i0} = 1, \\ \omega_2^{11} &= e^{i\pi} = -1.\end{aligned}$$

Por lo tanto,

$$U_{QFT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

que coincide con la puerta de Hadamard que hemos definido anteriormente. 

Veamos como podemos diseñar un algoritmo que calcule la Transformada de Fourier Cuántica (QFT) en un sistema de p cúbits ($n = 2^p$), para ello, consideremos un estado básico arbitrario $|X\rangle = |l\rangle_p$, con $l \in \{0, \dots, n-1\}$. Observar que, entonces,

$$|X\rangle = \underbrace{0}_{x_0} |0\rangle_p + \dots + \underbrace{1}_{x_l} |l\rangle_p + \dots + \underbrace{0}_{x_{n-1}} |x\rangle_{n-1},$$

de donde $\sum_{j=0}^{n-1} x_j \omega_n^{jk} = \omega_n^{lk}$. Por lo tanto,

$$U_{QFT} |X\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega_n^{lk} |k\rangle_p = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp\left(2\pi i l \frac{k}{2^p}\right) |k\rangle_p.$$

Ahora bien, gracias a la Notación 1.10, dado $k \in \{0, \dots, n-1\}$,

$$|k\rangle_p = |\vec{k}\rangle = |\vec{k}_1 \dots \vec{k}_p\rangle,$$

donde $\vec{k} \in \{0, 1\}^p$ es tal que $k = \sum_{j=1}^p \vec{k}_j 2^{p-j}$. Así,

$$\begin{aligned}U_{QFT} |X\rangle &= \frac{1}{\sqrt{n}} \sum_{\vec{k} \in \{0,1\}^p} \exp\left(2\pi i l \sum_{j=1}^p \frac{\vec{k}_j 2^{p-j}}{2^p}\right) |\vec{k}\rangle \\ &= \frac{1}{\sqrt{n}} \sum_{\vec{k} \in \{0,1\}^p} \exp\left(2\pi i l \sum_{j=1}^p \frac{\vec{k}_j}{2^j}\right) |\vec{k}\rangle \\ &= \frac{1}{\sqrt{n}} \sum_{\vec{k} \in \{0,1\}^p} \left(\prod_{j=1}^p \exp\left(2\pi i l \frac{\vec{k}_j}{2^j}\right)\right) |\vec{k}_1 \dots \vec{k}_p\rangle \tag{3.2} \\ &= \frac{1}{\sqrt{n}} \bigotimes_{j=1}^p \left(\exp\left(2\pi i l \frac{0}{2^j}\right) |0\rangle + \exp\left(2\pi i l \frac{1}{2^j}\right) |1\rangle\right) \\ &= \frac{1}{\sqrt{n}} \bigotimes_{j=1}^p \left(|0\rangle + \exp\left(\frac{2\pi i}{2^j} l\right) |1\rangle\right).\end{aligned}$$

Tal y como veremos, para implementar la QFT solamente necesitaremos dos tipos de puertas lógicas:

◊ *Puerta de Hadamard:*

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

que también se puede representar de la siguiente forma (que se adapta mejor a nuestros propósitos):

$$H |x\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2}x\right) |1\rangle \right), \quad x \in \{0, 1\}.$$

◊ *Puerta de rotación parametrizada controlada de 2 cúbits:* Dado un elemento $j \in \{1, \dots, p\}$, definimos la puerta de rotación parametrizada como

$$RT_j = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^j}\right) \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{C}).$$

Obsérvese que $RT_j = P(2\pi i/2^j)$, donde $P(\alpha)$ es la puerta Phase-shift que hemos introducido en la Sección 2.1. Ahora, introducimos como cúbit de control el segundo y denotamos por $CRT_j \in \mathcal{M}_{2^2 \otimes 2^2}(\mathbb{C})$ a la puerta controlada de la Figura 3.1. Vea-

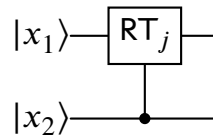


Fig. 3.1. Notación para la puerta CRT_j .

mos como actúa la puerta controlada CRT_j sobre los estados básicos de un sistema formado por dos cúbits:

$$CRT_j |00\rangle = |00\rangle,$$

$$CRT_j |01\rangle = (RT_j |0\rangle) \otimes |1\rangle = |0\rangle \otimes |1\rangle = |01\rangle,$$

$$CRT_j |10\rangle = |10\rangle,$$

$$CRT_j |11\rangle = ((RT_j |1\rangle) \otimes |1\rangle) = \left(\exp\left(\frac{2\pi i}{2^j}\right) |1\rangle \right) \otimes |1\rangle = \exp\left(\frac{2\pi i}{2^j}\right) |11\rangle.$$

A la vista de lo anterior observamos que

$$CRT_j |0x_2\rangle = |0x_2\rangle, \quad \forall x_2 \in \{0, 1\},$$

$$CRT_j |1x_2\rangle = \exp\left(\frac{2\pi i}{2^j}x_2\right) |1x_2\rangle, \quad \forall x_2 \in \{0, 1\}. \quad (3.3)$$

Por lo tanto, la matriz asociada a la puerta CRT_j es la siguiente

$$CRT_j := \left(\begin{array}{c|c} I_2 & 0 \\ \hline 0 & RT_j \end{array} \right) \in \mathcal{M}_{2^2 \times 2^2}(\mathbb{C}).$$

En el algoritmo que presentaremos a continuación aparecerán variaciones de la puerta controlada CRT_j (que seguiremos denotando de la misma forma sin que por ello cause confusión) consistentes en modificar el cúbit de control $|x_2\rangle$ a un cúbit de control genérico $|x_k\rangle$ en un sistema de p cúbits (ver Figura 3.2). En este caso, la

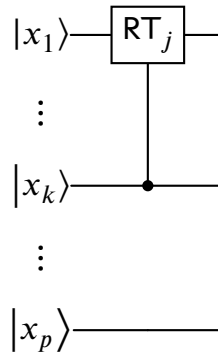


Fig. 3.2. Puerta CRT_j con cúbit de control genérico $|x_k\rangle$ en un sistema de p cúbits.

actuación de la puerta CRT_j con cúbit de control $|x_k\rangle$ es la siguiente:

$$\begin{aligned} CRT_j |0x_2x_3 \dots x_k\rangle &= |0x_2x_3 \dots x_k\rangle, \quad \forall x_2, \dots, x_k \in \{0, 1\}, \\ CRT_j |1x_2x_3 \dots x_k\rangle &= \exp\left(\frac{2\pi i}{2^j} x_k\right) |1x_2x_3 \dots x_k\rangle, \quad \forall x_2, \dots, x_k \in \{0, 1\}. \end{aligned} \quad (3.4)$$

Estamos ya en disposición de describir el algoritmo que calcula la Transformada de Fourier Cuántica (QFT).

Algoritmo 3.4 (QFT). Sea $|l\rangle_p = |\vec{l}\rangle = |\vec{l}_1 \dots \vec{l}_p\rangle$, con $l \in \{0, \dots, n - 1\}$, un estado básico de un sistema de p cúbits.

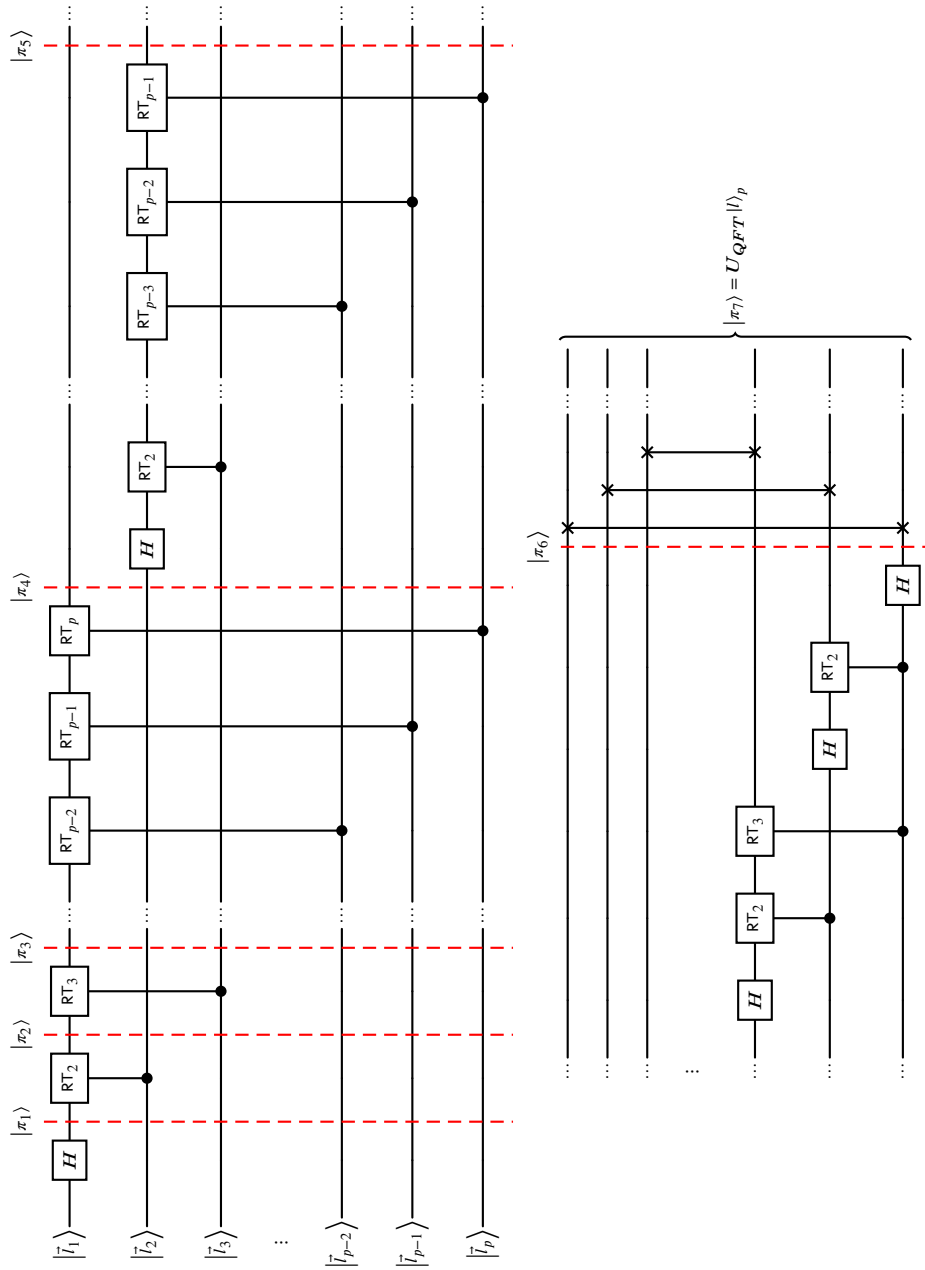


Fig. 3.3. Algoritmo para el cálculo de la QFT.

Analicemos cada una de las partes en las que hemos dividido el algoritmo anterior.

◊ Cálculo de $|\pi_1\rangle$.

$$\begin{aligned} |\pi_1\rangle &= (H \otimes I_2 \otimes I_2 \otimes \cdots \otimes I_2 \otimes I_2 \otimes I_2) \left| \vec{l}_1 \vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i \vec{l}_1}{2}\right) |1\rangle \right) \otimes \left| \vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle. \end{aligned}$$

◊ Cálculo de $|\pi_2\rangle$ y $|\pi_3\rangle$. Para calcular $|\pi_2\rangle$ emplearemos la expresión de la puerta controlada CRT_2 para 2 cúbits (3.3):

$$\begin{aligned} |\pi_2\rangle &= (\text{CRT}_2 \otimes I_2 \otimes \cdots \otimes I_2 \otimes I_2 \otimes I_2) |\pi_1\rangle \\ &= \frac{1}{\sqrt{2}} \left(\text{CRT}_2 \left| 0 \vec{l}_2 \right\rangle \right) \otimes \left| \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle + \frac{1}{\sqrt{2}} \exp\left(\frac{2\pi i \vec{l}_1}{2}\right) \left(\text{CRT}_2 \left| 1 \vec{l}_2 \right\rangle \right) \\ &\quad \otimes \left| \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle \\ &= \frac{1}{\sqrt{2}} \left| 0 \vec{l}_2 \right\rangle \otimes \left| \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle + \frac{1}{\sqrt{2}} \exp\left(\frac{2\pi i \vec{l}_1}{2}\right) \exp\left(\frac{2\pi i \vec{l}_2}{2^2}\right) \left| 1 \vec{l}_2 \right\rangle \\ &\quad \otimes \left| \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i \vec{l}_2}{2^2} + \frac{2\pi i \vec{l}_1}{2}\right) |1\rangle \right) \otimes \left| \vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle. \end{aligned}$$

Análogamente, para calcular $|\pi_3\rangle$, emplearemos la expresión para la puerta controlada CRT_3 de 3 cúbits cuya expresión se deduce de la fórmula genérica (3.4):

$$\begin{aligned} |\pi_3\rangle &= (\text{CRT}_3 \otimes \cdots \otimes I_2 \otimes I_2 \otimes I_2) |\pi_1\rangle \\ &= \frac{1}{\sqrt{2}} \left(\text{CRT}_3 \left| 0 \vec{l}_2 \vec{l}_3 \right\rangle \right) \otimes \left| \vec{l}_4 \dots, \vec{l}_p \right\rangle + \frac{1}{\sqrt{2}} \exp\left(\frac{2\pi i \vec{l}_2}{2^2} + \frac{2\pi i \vec{l}_1}{2}\right) \left(\text{CRT}_3 \left| 1 \vec{l}_2 \vec{l}_3 \right\rangle \right) \\ &\quad \otimes \left| \vec{l}_4 \dots, \vec{l}_p \right\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i \vec{l}_3}{2^3} + \frac{2\pi i \vec{l}_2}{2^2} + \frac{2\pi i \vec{l}_1}{2}\right) |1\rangle \right) \otimes \left| \vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(2\pi i \sum_{k=1}^3 \frac{\vec{l}_k}{2^k}\right) |1\rangle \right) \otimes \left| \vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} \sum_{k=1}^3 \vec{l}_k 2^{p-k}\right) |1\rangle \right) \otimes \left| \vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p \right\rangle. \end{aligned}$$

◊ Cálculo de $|\pi_4\rangle$. Repitiendo el mismo razonamiento que hemos hecho anteriormente,

$$\begin{aligned} |\pi_4\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} \sum_{k=1}^p \vec{l}_k 2^{p-k}\right) |1\rangle \right) \otimes |\vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} l\right) |1\rangle \right) \otimes |\vec{l}_2 \vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p\rangle. \end{aligned}$$

◊ Cálculo de $|\pi_5\rangle$. Lo primero que haremos será aplicar una puerta de Hadamard en el segundo cúbit:

$$\begin{aligned} &(I_2 \otimes H \otimes I_2 \dots \otimes I_2 \otimes I_2 \otimes I_2) |\pi_3\rangle \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2} \vec{l}_2\right) |1\rangle \right) \\ &\quad \otimes |\vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p\rangle. \end{aligned}$$

Ahora, aplicando de forma reiterada al resultado anterior las puertas controladas CRT_k , con $k = 2, \dots, p-1$, sobre el segundo cúbit y tomando como control, respectivamente, los cúbits $3, 4, \dots, p$, obtenemos que:

$$\begin{aligned} |\pi_5\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(2\pi i \sum_{k=2}^p \frac{\vec{l}_k}{2^{k-1}}\right) |1\rangle \right) \\ &\quad \otimes |\vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p\rangle. \end{aligned}$$

Ahora bien,

$$\begin{aligned} \exp\left(2\pi i \sum_{k=2}^p \frac{\vec{l}_k}{2^{k-1}}\right) &= \exp\left(2\pi i \frac{1}{2^{p-1}} \sum_{k=2}^p \vec{l}_k 2^{p-k}\right) \\ &= \exp\left(2\pi i \frac{1}{2^{p-1}} \left(\sum_{k=1}^p \vec{l}_k 2^{p-k} - \vec{l}_1 2^{p-1}\right)\right) \\ &= \exp\left(\frac{2\pi i}{2^{p-1}} l\right) \exp\left(-2\pi i \vec{l}_1\right) = \exp\left(\frac{2\pi i}{2^{p-1}} l\right). \end{aligned}$$

Por lo tanto,

$$\begin{aligned} |\pi_5\rangle &= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^{p-1}} l\right) |1\rangle \right) \\ &\quad \otimes |\vec{l}_3 \dots \vec{l}_{p-2} \vec{l}_{p-1} \vec{l}_p\rangle. \end{aligned}$$

- ◊ Cálculo de $|\pi_6\rangle$. El razonamiento es completamente análogo al anterior. Se obtiene que:

$$|\pi_6\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^{p-1}} l\right) |1\rangle \right) \otimes \dots \\ \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^2} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^1} l\right) |1\rangle \right).$$

- ◊ Cálculo de $|\pi_7\rangle$ (estado final). Observamos que la diferencia entre $|\pi_6\rangle$ y (3.2) es el orden en el que se realizan los productos tensoriales. Para recuperar el orden adecuado, se aplican las puertas SWAP que están detalladas en el algoritmo. Finalmente:

$$|\pi_7\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^1} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^2} l\right) |1\rangle \right) \otimes \dots \\ \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^{p-1}} l\right) |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left(\frac{2\pi i}{2^p} l\right) |1\rangle \right) \\ = \frac{1}{\sqrt{n}} \bigotimes_{j=1}^p \left(|0\rangle + \exp\left(\frac{2\pi i}{2^j} l\right) |1\rangle \right).$$

Observación 3.5 (Sobre la Transformada de Fourier Cuántica Inversa (QFT⁻¹)). Hemos visto que, dado un estado básico $|l\rangle_p$ de un sistema de p cúbits, la Transformada de Fourier Cuántica viene dada por la siguiente expresión ($n = 2^p$):

$$U_{QFT} |l\rangle_p = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \omega_n^{lk} |k\rangle_p = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \exp\left(2\pi i \frac{lk}{n}\right) |k\rangle_p.$$

Con lo cual,

$$U_{QFT} = \frac{1}{\sqrt{n}} \begin{pmatrix} \omega_n^{00} & \omega_n^{10} & \omega_n^{20} & \dots & \omega_n^{(n-3)0} & \omega_n^{(n-2)0} & \omega_n^{(n-1)0} \\ \omega_n^{01} & \omega_n^{11} & \omega_n^{21} & \dots & \omega_n^{(n-3)1} & \omega_n^{(n-2)1} & \omega_n^{(n-1)1} \\ \omega_n^{02} & \omega_n^{12} & \omega_n^{22} & \dots & \omega_n^{(n-3)2} & \omega_n^{(n-2)2} & \omega_n^{(n-1)2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \omega_n^{0(n-3)} & \omega_n^{1(n-3)} & \omega_n^{2(n-3)} & \dots & \omega_n^{(n-3)(n-3)} & \omega_n^{(n-2)(n-3)} & \omega_n^{(n-1)(n-3)} \\ \omega_n^{0(n-2)} & \omega_n^{1(n-2)} & \omega_n^{2(n-2)} & \dots & \omega_n^{(n-2)(n-2)} & \omega_n^{(n-2)(n-2)} & \omega_n^{(n-1)(n-2)} \\ \omega_n^{0(n-1)} & \omega_n^{1(n-1)} & \omega_n^{2(n-1)} & \dots & \omega_n^{(n-3)(n-1)} & \omega_n^{(n-2)(n-1)} & \omega_n^{(n-1)(n-1)} \end{pmatrix}.$$

Resulta claro que la matriz anterior es simétrica, por lo tanto, para calcular su inversa, lo único que tenemos que hacer es conjugar sus elementos. Así, si denotamos por $U_{QFT^{-1}} := (U_{QFT})^{-1} = U_{QFT}^\dagger$, tenemos que

$$U_{QFT^{-1}} |k\rangle_p = \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} \exp\left(-2\pi i \frac{lk}{n}\right) |l\rangle_p.$$

Para construir un algoritmo que calcule la Transformada de Fourier Cuántica Inversa simplemente hacemos las inversas de las operaciones del Algoritmo 3.3 en orden opuesto (recordemos que, dadas dos matrices invertibles A y B , $(AB)^{-1} = B^{-1}A^{-1}$). Por ejemplo, supongamos que tenemos un sistema de 3 cúbits, el Algoritmo 3.3 en este caso quedaría el circuito de la Figura 3.4. Resulta claro que la inversa de la operación SWAP es ella misma y

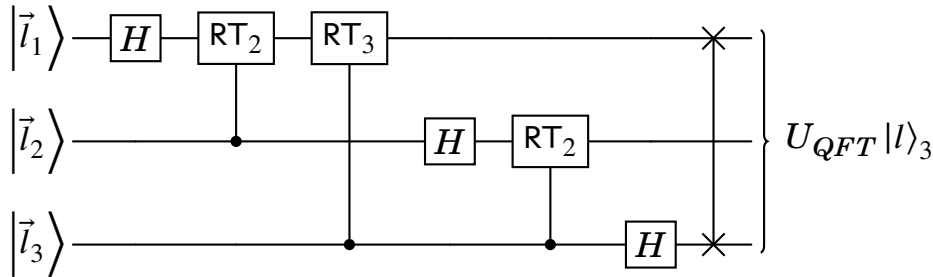


Fig. 3.4. QFT en un sistema de 3 cúbits.

lo mismo ocurre con la puerta de Hadamard. En lo que respecta a las puertas controladas, si denotamos por

$$RS_j = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(-\frac{2\pi i}{2^j}\right) \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{C})$$

y por $CRS_j \in \mathcal{M}_{2^2 \otimes 2^2}(\mathbb{C})$ a la correspondiente puerta controlada, observamos que

$$CRS_j CRT_j = I_4.$$

En efecto:

$$CRS_j CRT_j |00\rangle = CRS_j |00\rangle = |00\rangle,$$

$$CRS_j CRT_j |01\rangle = CRS_j |01\rangle = |01\rangle,$$

$$CRS_j CRT_j |10\rangle = CRS_j |10\rangle = |10\rangle,$$

$$CRS_j CRT_j |11\rangle = \exp\left(\frac{2\pi i}{2^j}\right) CRS_j |11\rangle = \exp\left(\frac{2\pi i}{2^j}\right) \exp\left(-\frac{2\pi i}{2^j}\right) |11\rangle = |11\rangle.$$

Por lo tanto, el algoritmo que calcula la Transformada de Fourier Cuántica Inversa de un sistema de 3 cúbits es el que se muestra en la Figura 3.5.

3.2 Algoritmo de estimación de fase (QPE)

El *algoritmo de estimación de fase* (QPE por sus siglas en inglés) [312, Section 5.2], es un algoritmo cuántico básico que se emplea en muchas aplicaciones como por ejemplo el algoritmo HHL que veremos en la siguiente sección. La idea básica del algoritmo consiste, dado un operador unitario U , en estimar la fase θ de un autovalor $\lambda = e^{2\pi i\theta}$ asociado a un autoestado $|\psi\rangle$:

$$U |\psi\rangle = e^{2\pi i\theta} |\psi\rangle.$$

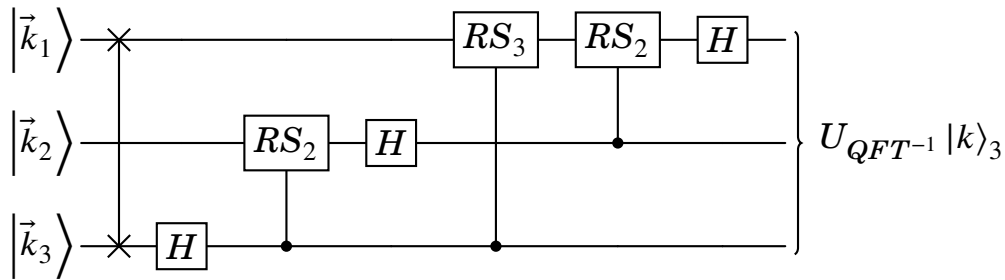


Fig. 3.5. QFT^{-1} en un sistema de 3 cúbits.

El algoritmo de estimación de fase emplea dos registros. El primer registro contiene t cúbits inicializados al estado $|0\rangle$. La elección del parámetro t dependerá de la precisión con la que queremos estimar θ y de la probabilidad de que el algoritmo tenga éxito (hablaremos sobre esto al final de la sección). El segundo registro que necesitaremos está formado por el número de cúbits necesarios para almacenar $|\psi\rangle$ (supondremos que es p). Pasamos a continuación a describir y analizar el algoritmo.

Algoritmo 3.6 (Algoritmo QPE). Sea U un operador unitario y $|\psi\rangle$ un autoestado. Se trata de calcular θ tal que $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$.

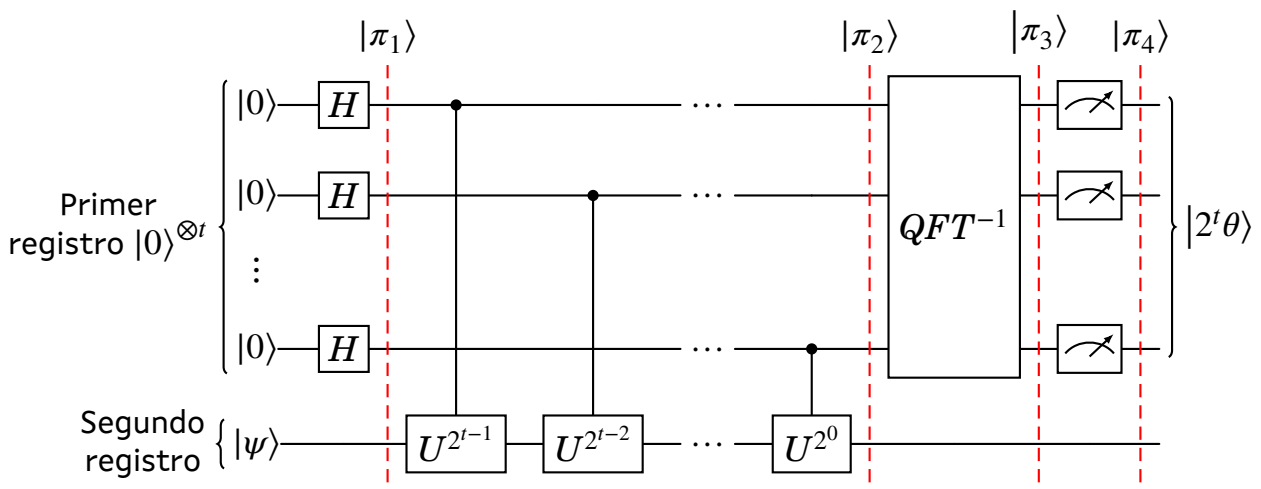


Fig. 3.6. Algoritmo QPE.

Analicemos cada una de las partes en las que hemos dividido el algoritmo anterior.

- ◊ Cálculo de $|\pi_1\rangle$. Aplicamos la puerta $H^{\otimes t}$ sobre el primer registro y la identidad sobre el segundo.

$$|\pi_1\rangle = \left(H^{\otimes t} |0\rangle^{\otimes t} \right) \otimes \psi = \frac{1}{\sqrt{2^t}} (|0\rangle + |1\rangle)^{\otimes t} \otimes |\psi\rangle.$$

- ◊ Cálculo de $|\pi_2\rangle$. Se aplican las puertas controladas al segundo registro. Obsérvese que, puesto que $e^{2\pi i\theta}$ es un autovalor asociado al autoestado $|\psi\rangle$, dado $j \in \{0, \dots, t-1\}$,

$$U^{2^j} |\psi\rangle = e^{2\pi i 2^j \theta} |\psi\rangle.$$

Así,

$$\begin{aligned} |\pi_2\rangle &= \left(CU^{2^0} \dots CU^{2^{t-2}} CU^{2^{t-1}} \right) \left(\frac{1}{\sqrt{2^t}} (|0\rangle + |1\rangle)^{\otimes t} \otimes |\psi\rangle \right) \\ &= \frac{1}{\sqrt{2^t}} \left(CU^{2^0} \dots CU^{2^{t-2}} \right) CU^{2^{t-1}} \left((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)^{\otimes(t-1)} \otimes |\psi\rangle \right) \\ &= \frac{1}{\sqrt{2^t}} \left(CU^{2^0} \dots CU^{2^{t-2}} \right) CU^{2^{t-1}} \left(|0\rangle \otimes (|0\rangle + |1\rangle)^{\otimes(t-1)} \otimes |\psi\rangle + |1\rangle \right. \\ &\quad \left. \otimes (|0\rangle + |1\rangle)^{\otimes(t-1)} \otimes |\psi\rangle \right) \\ &= \frac{1}{\sqrt{2^t}} \left(CU^{2^0} \dots CU^{2^{t-2}} \right) \left(|0\rangle \otimes (|0\rangle + |1\rangle)^{\otimes(t-1)} \otimes |\psi\rangle + e^{2\pi i 2^{t-1} \theta} |1\rangle \right. \\ &\quad \left. \otimes (|0\rangle + |1\rangle)^{\otimes(t-1)} \otimes |\psi\rangle \right) \\ &= \frac{1}{\sqrt{2^t}} \left(CU^{2^0} \dots CU^{2^{t-2}} \right) \left((|0\rangle + e^{2\pi i 2^{t-1} \theta} |1\rangle) \otimes (|0\rangle + |1\rangle)^{\otimes(t-1)} \otimes |\psi\rangle \right). \end{aligned}$$

Repitiendo el mismo razonamiento para el resto de puertas controladas,

$$\begin{aligned} |\pi_2\rangle &= \frac{1}{\sqrt{2^t}} \left(|0\rangle + e^{2\pi i 2^{t-1} \theta} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 2^{t-2} \theta} |1\rangle \right) \otimes \dots \\ &\quad \otimes \left(|0\rangle + e^{2\pi i 2^0 \theta} |1\rangle \right) \otimes |\psi\rangle. \end{aligned}$$

Analicemos la expresión anterior en el caso particular de considerar $t = 3$. Se tendrá que

$$\begin{aligned} |\pi_2\rangle &= \frac{1}{\sqrt{2^3}} \left(|0\rangle + e^{2\pi i 2^2 \theta} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 2^1 \theta} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 2^0 \theta} |1\rangle \right) \otimes |\psi\rangle \\ &= \frac{1}{\sqrt{2^3}} \left(|0\rangle + e^{2\pi i 2^2 \theta} |1\rangle \right) \\ &\quad \otimes \left(|00\rangle + e^{2\pi i 2^0 \theta} |01\rangle + e^{2\pi i 2^1 \theta} |10\rangle + e^{2\pi i (2^1 + 2^0) \theta} |11\rangle \right) \otimes |\psi\rangle \\ &= \frac{1}{\sqrt{2^3}} \left(|000\rangle + e^{2\pi i 2^0 \theta} |001\rangle + e^{2\pi i 2^1 \theta} |010\rangle + e^{2\pi i (2^1 + 2^0) \theta} |011\rangle + e^{2\pi i 2^2 \theta} |100\rangle \right. \\ &\quad \left. + e^{2\pi i (2^2 + 2^0) \theta} |101\rangle + e^{2\pi i (2^2 + 2^1) \theta} |110\rangle + e^{2\pi i (2^2 + 2^1 + 2^0) \theta} |111\rangle \right) \otimes |\psi\rangle \\ &= \frac{1}{\sqrt{2^3}} \left(e^{2\pi i (0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0) \theta} |000\rangle + e^{2\pi i (0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) \theta} |001\rangle \right. \end{aligned}$$

$$\begin{aligned}
& + e^{2\pi i(0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0)\theta} |010\rangle + e^{2\pi i(0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0)\theta} |011\rangle \\
& + e^{2\pi i(1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0)\theta} |100\rangle + e^{2\pi i(1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0)\theta} |101\rangle \\
& + e^{2\pi i(1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0)\theta} |110\rangle + e^{2\pi i(1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0)\theta} |111\rangle \Big) \otimes |\psi\rangle \\
& = \left(\frac{1}{\sqrt{2^3}} \sum_{k=0}^{2^3-1} e^{2\pi i k \theta} |k\rangle_3 \right) \otimes |\psi\rangle.
\end{aligned}$$

Para el caso general,

$$|\pi_2\rangle = \left(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i k \theta} |k\rangle_t \right) \otimes |\psi\rangle.$$

◊ Cálculo de $|\pi_3\rangle$. Se aplica la Transformada de Fourier Inversa al primer registro. Así,

$$\begin{aligned}
|\pi_3\rangle & = \left(U_{QFT^{-1}} \left(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i k \theta} |k\rangle_t \right) \right) \otimes |\psi\rangle \\
& = \left(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i k \theta} U_{QFT^{-1}} |k\rangle_t \right) \otimes |\psi\rangle \\
& = \left(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} \exp(2\pi i k \theta) \frac{1}{\sqrt{2^t}} \sum_{l=0}^{2^t-1} \exp\left(-2\pi i \frac{lk}{2^t}\right) |l\rangle_t \right) \otimes |\psi\rangle \\
& = \left(\frac{1}{2^t} \sum_{k=0}^{2^t-1} \sum_{l=0}^{2^t-1} \exp\left(\frac{2\pi i k}{2^t} (2^t \theta - l)\right) |l\rangle_t \right) \otimes |\psi\rangle.
\end{aligned}$$

◊ Cálculo de $|\pi_4\rangle$. Empezamos midiendo el primer registro. Aquí es donde el algoritmo presenta su mayor limitación. Distinguiamos los siguientes casos:

✱ Supongamos que existe un elemento $l \in \{0, \dots, 2^t-1\}$ tal que $2^t \theta = l$ ($\theta = l/2^t$). En este caso,

$$|\pi_2\rangle = \left(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} \exp\left(2\pi i \frac{lk}{2^t}\right) |k\rangle_t \right) \otimes |\psi\rangle = (U_{QFT} |l\rangle_t) \otimes |\psi\rangle,$$

de donde,

$$|\pi_3\rangle = \left(U_{QFT^{-1}} U_{QFT} |l\rangle_t \right) \otimes |\psi\rangle = |l\rangle_t \otimes |\psi\rangle = |2^t \theta\rangle_t \otimes |\psi\rangle.$$

Con lo cual, al realizar la medida en el primer registro, obtenemos el estado básico $|2^t \theta\rangle_t$ con probabilidad uno, recuperando así el valor exacto de θ .

- ✱ Caso general. Sea $b \in [0, 2^t - 1] \cap \mathbb{Z}$ tal que $b/2^t = 0.b_1 \dots b_t$ es la mejor aproximación de t bits de θ menor o igual a θ . Se tendrá entonces que $\delta := \theta - b/2^t \in [0, 2^{-t}]$. La idea fundamental es que, al aplicar el algoritmo de estimación de fase, obtenemos un resultado próximo a b con alta probabilidad, lo cual nos permite, en última instancia, estimar θ .

Ahora bien, recordemos que al aplicar la Transformada de Fourier Inversa sobre el primer registro obtenemos

$$\sum_{l,k=0}^{2^t-1} \frac{1}{2^t} \exp \left(2\pi i k \left(\theta - \frac{l}{2^t} \right) \right) |l\rangle_t.$$

Consideremos ahora la siguiente reenumeración de los estados básicos:

$$|(b+l)(\text{mod } 2^t)\rangle_t.$$

con $l = -2^{t-1} + 1, \dots, 2^{t-1}$. Se tendrá que la expresión anterior admite la siguiente formulación:

$$\sum_{l=-2^{t-1}+1}^{2^t-1} \frac{1}{2^t} \left(\sum_{k=0}^{2^t-1} \exp \left(2\pi i k \left(\theta - \frac{(b+l)}{2^t} \right) \right) \right) |(b+l)(\text{mod } 2^t)\rangle_t, \quad (3.5)$$

donde hemos empleado el hecho de que, dados $b \in [0, 2^t - 1] \cap \mathbb{Z}$ y $l = -2^{t-1} + 1, \dots, 2^{t-1}$, existe $a \in \mathbb{Z}$ tal que

$$\begin{aligned} \exp \left(2\pi i k \frac{b+l}{2^k} \right) &= \exp \left(2\pi i k \left(a + \frac{(b+l)(\text{mod } 2^t)}{2^k} \right) \right) \\ &= \exp(2\pi i k a) \exp \left(2\pi i k \frac{(b+l)(\text{mod } 2^t)}{2^t} \right) \\ &= \exp \left(2\pi i k \frac{(b+l)(\text{mod } 2^t)}{2^t} \right). \end{aligned}$$

Denotemos ahora por α_l a la amplitud del estado básico $|(b+l)(\text{mod } 2^t)\rangle_t$. Se tendrá que α_l se puede expresar como la suma parcial de una serie geométrica:

$$\alpha_l := \frac{1}{2^t} \sum_{k=0}^{2^t-1} \exp \left(2\pi i \left(\theta - \frac{(b+l)}{2^t} \right) \right)^k = \frac{1}{2^t} \left(\frac{1 - \exp(2\pi i (2^t \delta - l))}{1 - \exp(2\pi i (\delta - \frac{l}{2^t}))} \right).$$

Supongamos que el resultado final después de la medida es el estado básico $|m\rangle_t$. Estamos interesados en acotar la probabilidad de obtener un estado básico $|m\rangle_t$ tal que $|m - b| > r$, donde $r \in \mathbb{N}$ es la tolerancia deseada.

Por ejemplo, supongamos que $t = 3$, que $b = 2 \in [0, 2^3 - 1]$ y que $r = 1$. Tendremos que (3.5) admite la siguiente expresión:

$$\alpha_{-3} |7\rangle_3 + \alpha_{-2} |0\rangle_3 + \alpha_{-1} |1\rangle_3 + \alpha_0 |2\rangle_3 + \alpha_1 |3\rangle_3 + \alpha_2 |4\rangle_3 + \alpha_3 |5\rangle_3 + \alpha_4 |6\rangle_3.$$

Por lo tanto, los estados básicos tales que distan de $b = 2$ una cantidad mayor o igual a $r + 1$ son $|7\rangle_3, |0\rangle_3, |4\rangle_3, |5\rangle_3$ y $|6\rangle_3$. Con lo cual,

$$\begin{aligned} \Pr(|m - b| > r) &= |\alpha_{-3}|^2 + |\alpha_{-2}|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 \\ &= \sum_{l=-2^{t-1}+1}^{-(r+1)} |\alpha_l|^2 + \sum_{l=(r+1)}^{2^{t-1}} |\alpha_l|^2, \end{aligned}$$

pudiéndose demostrar que la última igualdad sigue siendo válida en el caso general.

Ahora, puesto que $|1 - \exp(i\varphi)| \leq 2$ para todo $\varphi \in \mathbb{R}$,

$$|\alpha_l| \leq \frac{2}{2^t |1 - \exp(2\pi i (\delta - l/2^t))|}.$$

Dado un elemento $\varphi \in [-\pi, \pi]$ tenemos que $|1 - \exp(i\varphi)| \geq 2|\varphi|/\pi$, de donde, puesto que $-\pi \leq 2\pi(\delta - l/2^t) \leq \pi$, obtenemos,

$$|\alpha_l| \leq \frac{1}{2^{t+1}(\delta - l/2^t)} = \frac{1}{2(2^t\delta - l)}.$$

Así, si tenemos en cuenta además que $0 \leq 2^t\delta \leq 1$, llegamos a la siguiente acotación:

$$\begin{aligned} \Pr(|m - b| > r) &\leq \frac{1}{4} \left(\sum_{l=-2^{t-1}+1}^{-(r+1)} \frac{1}{(l - 2^t\delta)^2} + \sum_{l=(r+1)}^{2^{t-1}} \frac{1}{(l - 2^t\delta)^2} \right) \\ &\leq \frac{1}{4} \left(\sum_{l=-2^{t-1}+1}^{-(r+1)} \frac{1}{l^2} + \sum_{l=(r+1)}^{2^{t-1}} \frac{1}{(l-1)^2} \right) \\ &\leq \frac{1}{2} \sum_{l=r}^{2^{t-1}-1} \frac{1}{l^2} = \frac{1}{2} \left(\frac{1}{r^2} + \sum_{l=r+1}^{2^{t-1}-1} \frac{1}{l^2} \right) \leq \frac{1}{2} \left(\frac{1}{r^2} + \int_r^{2^{t-1}-1} \frac{1}{l^2} dl \right). \end{aligned}$$

Ahora, puesto que r es un número natural, tienen sentido las siguientes acotaciones:

$$\begin{aligned} \frac{1}{2} \left(\frac{1}{r^2} + \sum_{l=r+1}^{2^{t-1}-1} \frac{1}{l^2} \right) &\leq \frac{1}{2} \left(\frac{1}{r^2} + \int_r^{2^{t-1}-1} \frac{1}{l^2} dl \right) \\ &= \frac{1}{2} \left(\frac{1}{r^2} + \frac{1}{r} - \frac{1}{2^{t-1}-1} \right) \leq \frac{r+1}{2r^2}, \end{aligned}$$

de donde llegamos a que $\Pr(|m - b| > r) \leq \frac{r+1}{2r^2}$.

Supongamos que queremos aproximar θ con una precisión de 2^{-n} . En particular, debemos tomar $r = 2^{t-n} - 1$ ($b + r + 1 = b + 2^{t-n} \simeq 2^t + \theta 2^{t-n} = 2^t(\theta + 2^{-n})$). Tomemos $t = n + q$ ($q = t - n$) cúbits en el primer registro del algoritmo, siendo

q un número entero positivo a determinar, se tendrá, entonces que $r = 2^q - 1$, con lo cual:

$$\Pr(|m - b| > r) \leq \frac{2^p}{2(2^q - 1)^2} \Rightarrow \Pr(|m - b| \leq r) \geq 1 - \frac{2^q}{2(2^q - 1)^2}.$$

En resumen, dado $\epsilon > 0$ un número real y $n > 0$ un número entero, si queremos aproximar θ con una precisión de n bits y con probabilidad de éxito superior a $1 - \epsilon$, debemos tomar q tal que

$$\frac{2^q}{2(2^q - 1)^2} \leq \epsilon.$$

Podemos tomar entonces

$$q = \left\lceil \frac{\ln \left(\frac{4\epsilon + \sqrt{8\epsilon + 1} + 1}{4\epsilon} \right)}{\ln(2)} \right\rceil.$$

Con lo cual, el número de cúbits para el primer registro será

$$t = n + \left\lceil \frac{\ln \left(\frac{4\epsilon + \sqrt{8\epsilon + 1} + 1}{4\epsilon} \right)}{\ln(2)} \right\rceil.$$

Destacamos que en el algoritmo anterior es necesario conocer el autoestado asociado a U . En el caso de que esto no sea posible, remitimos al lector a [312, Section 5.2.1]. El lector también podrá observar en la mencionada referencia que la estimación de t es distinta a la nuestra. Esto se debe a que el autor hace la acotación $\frac{1}{2} \sum_{l=r}^{2^{t-1}-1} \frac{1}{l^2} \leq \frac{1}{2} \int_{r-1}^{2^{t-1}-1} \frac{1}{r} dr$ que, a nuestro juicio, no es cierta cuando $r = 1$ (la integral no es convergente). Es por ello que separamos el primer sumando de la suma que sería el que, eventualmente, nos podría dar el problema de que la integral no fuese convergente. En cualquier caso, la cota propuesta en este trabajo mejora a la propuesta en [312].

Notación 3.7. Con la finalidad de simplificar la descripción del algoritmo HHL que veremos en la siguiente sección, establezcamos la siguiente notación para el algoritmo de estimación de fase:

$$U_{QPE} \left(|0\rangle^{\otimes t} \otimes |\psi\rangle \right) = \left(\frac{1}{2^t} \sum_{k=0}^{2^t-1} \sum_{l=0}^{2^t-1} \exp \left(\frac{2\pi i k}{2^t} (2^t \theta - l) \right) |l\rangle_t \right) \otimes |\psi\rangle.$$

Recordemos que al medir el primer registro, lo que obtenemos es una aproximación $\tilde{\theta}$ de $2^t \theta$, siendo θ tal que $U |\psi\rangle = e^{2\pi i \theta} |\psi\rangle$. La construcción del operador U_{QPE}^{-1} se puede realizar de forma análoga a la que hemos visto para el operador U_{QFT} . Recordemos por último que, en el caso de que exista un elemento $l \in \{0, \dots, 2^t - 1\}$ tal que $2^t \theta = l$ ($\theta = l/2^t$), entonces, $U_{QPE} \left(|0\rangle^{\otimes t} \otimes |\psi\rangle \right) = |2^t \theta\rangle \otimes |\psi\rangle$.

3.3 Algoritmo de resolución de sistemas lineales (HHL)

El *algoritmo HHL* (Harrow-Hassidim-Lloyd [202]) consiste en, dada una matriz hermitiana $A \in \mathcal{M}_{N \times N}(\mathbb{C})$, con $N = 2^{n_b}$, y un vector unitario $b \in \mathcal{M}_{N \times 1}(\mathbb{C})$, estimar el valor de $x \in \mathcal{M}_{N \times 1}(\mathbb{C})$ tal que $Ax = b$. El interés de este algoritmo resulta más evidente cuando, en lugar de conocer el valor de la solución x directamente, lo que necesitamos es estimar el valor de $x^\dagger M x$, para alguna matriz M . En tal caso, cuando A es dispersa, el algoritmo HHL presenta una mejora exponencial en el orden de complejidad frente al mejor algoritmo clásico [202]. Esto es, el algoritmo HHL presenta un orden de complejidad de $O(d^4 \kappa^2 \log(N)/\epsilon)$, donde d es el número de entradas distintas de cero por fila en la matriz A , κ es el condicionamiento de A y ϵ es la precisión deseada en los cálculos. Sin embargo, el algoritmo de Gradiente Conjugado, que se puede considerar como el mejor algoritmo clásico para resolver sistemas lineales con matrices dispersas, tiene un orden de complejidad de $O(Nd\kappa \log(1/\epsilon))$ [347].

En esta sección introduciremos el algoritmo cuántico HHL en el caso más simple de aplicación. Remitimos al lector a la referencia [202] para el caso general que mencionábamos en el párrafo anterior.

Supongamos que A admite la siguiente descomposición espectral:

$$A = \sum_{j=0}^{N-1} \lambda |u_j\rangle \langle u_j|,$$

donde, dado $j = 0, \dots, N-1$, $\lambda_j \in \mathbb{R}$ es un autovalor y $|u_j\rangle$ es un autoestado unitario asociado a λ_j . Se tendrá entonces que

$$A^{-1} = \sum_{j=0}^{N-1} \lambda_j^{-1} |u_j\rangle \langle u_j|.$$

Supongamos ahora que $|b\rangle$ se puede expresar de la siguiente forma:

$$|b\rangle = \sum_{j=0}^{N-1} b_j |u_j\rangle,$$

siendo $b_j \in \mathbb{C}$, para todo $j = 0, \dots, N-1$, tales que $\sum_{j=0}^{N-1} |b_j|^2 = 1$. Resulta claro que, en el caso en el que

$$\sum_{j=0}^{N-1} |\lambda_j^{-1} b_j|^2 = 1,$$

la solución x es un vector unitario que se puede expresar de la siguiente forma:

$$|x\rangle = A^{-1} |b\rangle = \sum_{j=0}^{N-1} \lambda_j^{-1} b_j |u_j\rangle.$$

En el caso en el que A no sea hermitiana, se considera el sistema lineal $\tilde{A}\tilde{x} = \tilde{b}$, donde

$$\tilde{A} = \begin{pmatrix} 0 & A \\ A^\dagger & 0 \end{pmatrix}, \quad \tilde{b} = \begin{pmatrix} b \\ 0 \end{pmatrix} \quad y \quad \tilde{x} = \begin{pmatrix} 0 \\ x \end{pmatrix}.$$

Algoritmo 3.8 (Algoritmo HHL). Dada una matriz hermitiana $A \in \mathcal{M}_{2^{n_b} \times 2^{n_b}}(\mathbb{C})$ y un vector unitario $b \in \mathcal{M}_{2^{n_b} \times 1}(\mathbb{C})$, se trata de calcular $|x\rangle = A^{-1}|b\rangle$. Denotaremos por n_l al número de cúbits que empleamos en el primer registro del algoritmo de estimación de fase.

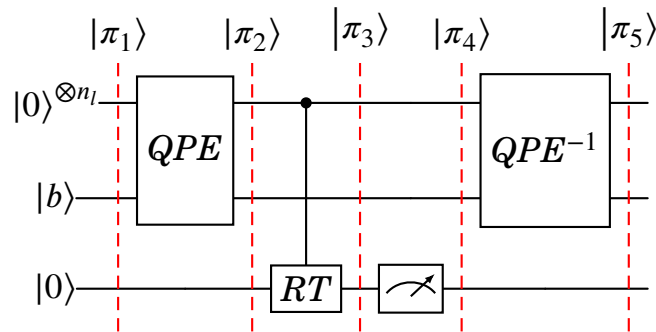


Fig. 3.7. Algoritmo HHL.

Analicemos ahora cada una de las fases en las que hemos dividido el algoritmo anterior.

- ◇ Cálculo de $|\pi_1\rangle$. Se corresponde con la etapa de inicialización del algoritmo. Puesto que $b \in \mathcal{M}_{N \times 1}(\mathbb{C})$ es un vector unitario, lo podemos identificar con un n_b -cúbit que denotaremos por $|b\rangle$. Por lo tanto,

$$|\pi_1\rangle = |0\rangle^{\otimes n_l} \otimes |b\rangle \otimes |0\rangle = \left(\sum_{j=0}^{N-1} b_j |0\rangle^{\otimes n_l} \otimes |u_j\rangle \right) \otimes |0\rangle.$$

- ◇ Cálculo de $|\pi_2\rangle$. Para poder aplicar el algoritmo de estimación de fase, necesitamos un operador unitario. Consideremos entonces el operador unitario $U = e^{iAt}$, donde $t \in \mathbb{R}$, con $t > 0$ (no confundir con la variable entera que hemos empleado para identificar el número de cúbits en el primer registro para el algoritmo de estimación de fase). Se tendrá que

$$e^{iAt} = \sum_{j=0}^{N-1} e^{i\lambda_j t} |u_j\rangle \langle u_j| = \sum_{j=0}^{N-1} e^{2\pi i \frac{\lambda_j t}{2\pi}} |u_j\rangle \langle u_j|.$$

Con lo cual,

$$|\pi_2\rangle = \left(\sum_{j=0}^{N-1} b_j U_{QPF} \left(|0\rangle^{\otimes n_l} \otimes |u_j\rangle \right) \right) \otimes |0\rangle.$$

Por simplicidad en la descripción del algoritmo, supondremos que la aproximación del algoritmo de estimación de fase es exacta:

$$U_{QPF} \left(|0\rangle^{\otimes n_l} \otimes |u_j\rangle \right) = |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle,$$

donde $\tilde{\lambda}_j = 2^{n_l} \lambda_j t / (2\pi)$. Por lo tanto,

$$|\pi_2\rangle = \left(\sum_{j=0}^{N-1} b_j |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \right) \otimes |0\rangle = \sum_{j=0}^{N-1} b_j |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \otimes |0\rangle.$$

- ◊ Cálculo de $|\pi_3\rangle$. Aplicamos una rotación al *cúbit auxiliar* $|0\rangle$, basada en los elementos del primer registro:

$$|\pi_3\rangle = \sum_{j=0}^{N-1} b_j |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \otimes \left(\left[1 - \frac{C^2}{\tilde{\lambda}_j^2} \right]^{1/2} |0\rangle + \frac{C}{\tilde{\lambda}_j} |1\rangle \right),$$

donde C es una constante de normalización que debe ser elegida lo mayor posible, con la finalidad de maximizar la probabilidad de obtener el estado $|1\rangle$, véase $|C|^2/|\tilde{\lambda}_j|^2$, cuando midamos el cúbit auxiliar.

- ◊ Cálculo de $|\pi_4\rangle$. Veamos por qué es interesante obtener el estado $|1\rangle$ en el cúbit auxiliar (de hecho, en el caso de obtener el cúbit $|0\rangle$ descartamos el resultado y volvemos a repetir el algoritmo hasta que salga el cúbit $|1\rangle$). En este caso:

$$\begin{aligned} |\pi_4\rangle &= \sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|C|^2 |b_j|^2}{|\tilde{\lambda}_j|^2}}} b_j \frac{C}{\tilde{\lambda}_j} |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \otimes |1\rangle \\ &= \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|C|^2 |b_j|^2}{|\tilde{\lambda}_j|^2}}} b_j \frac{C}{\tilde{\lambda}_j} |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \right) \otimes |1\rangle. \end{aligned}$$

- ◊ Calculemos $|\pi_5\rangle$, para ello, tenemos que aplicar $U_{QPE^{-1}}$ sobre los dos primeros registros:

$$|\pi_5\rangle = \left(U_{QPE^{-1}} \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|C|^2 |b_j|^2}{|\tilde{\lambda}_j|^2}}} b_j \frac{C}{\tilde{\lambda}_j} |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \right) \right) \otimes |1\rangle$$

$$\begin{aligned}
 &= \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|C|^2 |b_j|^2}{|\tilde{\lambda}_j|^2}}} b_j \frac{C}{\tilde{\lambda}_j} U_{QPE^{-1}} |\tilde{\lambda}_j\rangle_{n_l} \otimes |u_j\rangle \right) \otimes |1\rangle \\
 &= \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|C|^2 |b_j|^2}{|\tilde{\lambda}_j|^2}}} b_j \frac{C}{\tilde{\lambda}_j} |0\rangle^{\otimes n_l} \otimes |u_j\rangle \right) \otimes |1\rangle \\
 &= |0\rangle^{\otimes n_l} \otimes \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|b_j|^2}{|\lambda_j|^2}}} \frac{b_j}{\lambda_j} |u_j\rangle \right) \otimes |1\rangle = |0\rangle^{\otimes n_l} \otimes |x\rangle \otimes |1\rangle.
 \end{aligned}$$

Obsérvese que, en el caso en el que

$$\sum_{j=0}^{N-1} |\lambda_j^{-1} b_j|^2 \neq 1,$$

el algoritmo nos proporciona en el segundo registro la solución x normalizada:

$$|\pi_5\rangle = |0\rangle^{\otimes n_l} \otimes \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{\sum_{j=0}^{N-1} \frac{|b_j|^2}{|\lambda_j|^2}}} \frac{b_j}{\lambda_j} |u_j\rangle \right) \otimes |1\rangle.$$

Esto se pondrá de manifiesto en el siguiente ejemplo.

Ejemplo 3.9. Consideremos el sistema lineal $Ax = b$, donde

$$A = \begin{pmatrix} 1 & -1/3 \\ -1/3 & 1 \end{pmatrix} \quad y \quad b = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

La solución de dicho sistema es

$$x = \begin{pmatrix} 9/8 \\ 3/8 \end{pmatrix}.$$

Si la normalizamos, lo que nos debería proporcionar el algoritmo HHL es

$$|x\rangle = \frac{1}{\sqrt{(9/8)^2 + (3/8)^2}} \frac{9}{8} |0\rangle + \frac{1}{\sqrt{(9/8)^2 + (3/8)^2}} \frac{3}{8} |1\rangle = \frac{3}{\sqrt{10}} |0\rangle + \frac{1}{\sqrt{10}} |1\rangle.$$

Vamos ahora con la aplicación del algoritmo HHL en este caso en concreto. Por un lado, los autovalores de la matriz A son $\lambda_0 = 2/3$ y $\lambda_1 = 4/3$, siendo los autovectores

asociados:

$$u_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad y \quad u_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

En particular,

$$b = \sum_{j=0}^1 \frac{1}{\sqrt{2}} u_j.$$

Para almacenar b solamente necesitamos un cúbit ($b = |0\rangle$), por lo que $n_b = 1$. Para almacenar los autovalores asociados, tomaremos $t = 3\pi/4$. En este caso, tomando $n_l = 2$,

$$\tilde{\lambda}_0 = \frac{2^{n_l} \lambda_0 t}{2\pi} = 1 = |01\rangle_2, \quad \tilde{\lambda}_1 = \frac{2^{n_l} \lambda_1 t}{2\pi} = 2 = |10\rangle_2.$$

◊ Inicialización:

$$\begin{aligned} |\pi_1\rangle &= |00\rangle \otimes |0\rangle \otimes |0\rangle = |00\rangle \otimes \left(\frac{1}{\sqrt{2}} |u_0\rangle + \frac{1}{\sqrt{2}} |u_1\rangle \right) \otimes |0\rangle \\ &= \left(\frac{1}{\sqrt{2}} |00\rangle \otimes |u_0\rangle + \frac{1}{\sqrt{2}} |00\rangle \otimes |u_1\rangle \right) |0\rangle. \end{aligned}$$

◊ Aplicamos el algoritmo de estimación de fase:

$$|\pi_2\rangle = \left(\frac{1}{\sqrt{2}} |01\rangle \otimes |u_0\rangle + \frac{1}{\sqrt{2}} |10\rangle \otimes |u_1\rangle \right) \otimes |0\rangle.$$

◊ Rotación del cúbit auxiliar. Tal y como hemos visto en el algoritmo, los coeficientes asociados a $|0\rangle$ y $|1\rangle$ después de la rotación en el cúbit auxiliar son $\sqrt{1 - C^2/\tilde{\lambda}_j^2}$ y $C/\tilde{\lambda}_j$. En particular, $C \leq \tilde{\lambda}_j$, $j = 0, 1$. Puesto que $\min\{\tilde{\lambda}_0, \tilde{\lambda}_1\} = 1$, tomamos $C = 1$ (valor que maximiza la probabilidad de obtener el cúbit $|1\rangle$ después de la medición del cúbit auxiliar). Obtenemos entonces que:

$$|\pi_3\rangle = \frac{1}{\sqrt{2}} |01\rangle \otimes |u_0\rangle \otimes (0|0\rangle + 1|1\rangle) + \frac{1}{\sqrt{2}} |10\rangle \otimes |u_1\rangle \otimes \left(\frac{\sqrt{3}}{2} |0\rangle + \frac{1}{2} |1\rangle \right).$$

◊ Supongamos que al medir el cúbit auxiliar obtenemos el estado $|1\rangle$:

$$|\pi_4\rangle = \left(\frac{2}{\sqrt{5}} |01\rangle \otimes |u_0\rangle + \frac{1}{\sqrt{5}} |10\rangle \otimes |u_1\rangle \right) \otimes |1\rangle.$$

- ◊ Aplicamos U_{QPE}^{-1} a los dos primeros registros:

$$\begin{aligned}
 |\pi_5\rangle &= \left(\frac{2}{\sqrt{5}} |00\rangle \otimes |u_0\rangle + \frac{1}{\sqrt{5}} |00\rangle \otimes |u_1\rangle \right) \otimes |1\rangle \\
 &= |00\rangle \otimes \left(\frac{2}{\sqrt{5}} |u_0\rangle + \frac{1}{\sqrt{5}} |u_1\rangle \right) \otimes |1\rangle \\
 &= |00\rangle \otimes \left(\frac{2}{\sqrt{5}} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) + \frac{1}{\sqrt{5}} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) \otimes |1\rangle \\
 &= |00\rangle \otimes \left(\frac{3}{\sqrt{10}} |0\rangle + \frac{1}{\sqrt{10}} |1\rangle \right) \otimes |1\rangle = |00\rangle \otimes |x\rangle \otimes |1\rangle.
 \end{aligned}$$



Observación 3.10. Es importante destacar que para alcanzar la mejora exponencial que hemos comentado al comienzo de la sección, es necesario lo siguiente:

- ◊ Poder acceder a los elementos de la matriz A de forma eficiente a través de una función (también conocido como oráculo en la literatura).
- ◊ La matriz A debe ser dispersa o, en su defecto, debe poderse descomponer como producto de matrices dispersas.
- ◊ El condicionamiento de A , κ , tiene que escalar como $\text{polilog}(N)$.

A la vista del ejemplo que hemos presentado, el algoritmo tiene tres características que dificultan su aplicación práctica:

- ◊ La preparación del estado $|b\rangle$. Este es un problema abierto y en el trabajo original no se desarrolla lo suficiente.
- ◊ Extracción de la solución. Puesto que la solución viene dada en un estado cuántico $|x\rangle$, la extracción de la información del valor de cada una de las componentes es un problema en sí mismo. Los autores proponen que puede ser empleado para calcular el valor esperado de cierto operador, pero no proporcionan un procedimiento de medida para ello.
- ◊ El condicionamiento de A tiene que escalar a lo sumo $\text{polilog}(N)$, lo cual es una condición muy restrictiva que limita el rango de aplicación del algoritmo.

En [119] se propone una mejora del algoritmo original que intenta dar respuesta a las cuestiones anteriores que dificultan la aplicación práctica del algoritmo HHL. Adicionalmente, proponen la aplicación a un cierto problema relacionado con el electromagnetismo en el que usan el método de Elementos Finitos para obtener la matriz asociada al problema.

En un trabajo más reciente [108], los autores mejoran el algoritmo de HHL en lo que respecta al orden de complejidad empleando una técnica general para implementar cualquier operador con una representación adecuada en series de Fourier o Chebyshev. Esto último les permite eludir el algoritmo de estimación de fase.

3.4 Algoritmo de Shor

El *algoritmo de Shor* es uno de los principales algoritmos en computación cuántica [369]. El propósito último del algoritmo de Shor es encontrar la descomposición en factores primos de un número entero. Teóricamente, mejora sustancialmente el tiempo de cálculo con respecto al mejor algoritmo clásico conocido, al ser el orden de complejidad

$$O((\log N)^2(\log \log N)(\log \log \log N)),$$

mientras que la complejidad del mejor algoritmo clásico conocido es

$$O\left(e^{(\log N)^{1/3}(\log \log N)^{2/3}}\right).$$

Esto supone una ventaja sustancial a la hora de factorizar números grandes. Lamentablemente, el número de cúbits necesarios para factorizar números grandes está lejos de la capacidad de los ordenadores cuánticos actuales.

El algoritmo de Shor consta de una parte clásica (que se realiza en un ordenador convencional) y de una parte cuántica. Será, lógicamente, en la parte cuántica en donde se ponga de manifiesto la ventaja con respecto a los algoritmos clásicos. Comencemos estableciendo algunos resultados y definiciones básicas que nos ayudarán a la hora de describir el algoritmo.

Teorema 3.11 (Teorema de la factorización única). *Dado un número entero N no negativo, existe una única factorización de N como producto de potencias de números primos:*

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}.$$

Al problema de encontrar la factorización anterior se le suele denotar por PFP (por sus siglas en inglés).

Definición 3.12 (Orden multiplicativo). Dado un número entero $N \in (1, \infty) \cap \mathbb{Z}$ y $x \in (1, N) \cap \mathbb{Z}$ tal que $\text{mcd}(x, N) = 1$, diremos que $r \in (0, \infty) \cap \mathbb{Z}$ es el orden multiplicativo de x módulo N , y lo denotaremos por $O_N(x)$, si

$$O_N(x) = \min \{r \in (0, \infty) \cap \mathbb{Z} : x^r \equiv 1 \pmod{N}\}.$$

Teorema 3.13 (Representación de un número racional como una fracción continua). *Todo número racional positivo ξ se puede expresar de la siguiente forma:*

$$\xi = [a_0; a_1, \dots, a_K],$$

donde a_0 es un número entero no negativo, a_1, \dots, a_K son enteros positivos y $[a_0; a_1, \dots, a_K]$ representa la siguiente fracción continua:

$$[a_0; a_1, \dots, a_K] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\dots + \frac{1}{a_K}}}}}$$

Observación 3.14. (ver [276, Section 7]) Dado un número racional positivo ξ , podemos calcular los elementos de la fracción continua asociada $[a_0; a_1, \dots, a_K]$ mediante la siguiente relación de recurrencia, que siempre finaliza si ξ es racional:

$$\begin{cases} a_0 = \lfloor \xi \rfloor, \\ \xi_0 = \xi - a_0. \end{cases} \quad \text{Si } \xi_n \neq 0 : \quad \begin{cases} a_{n+1} = \left\lfloor \frac{1}{\xi_n} \right\rfloor, \\ \xi_{n+1} = \frac{1}{\xi_n} - a_{n+1}. \end{cases} \quad (3.6)$$

Llamaremos a cada elemento $\xi_k = [a_0; a_1, \dots, a_k]$, con $0 \leq k \leq K$ *convergente k -ésimo*. Se tendrá además que cada uno de los convergentes k -ésimos se puede expresar como $\xi_k = p_k/q_k$, donde p_k y q_k son dos números enteros tales que $\text{mcd}(p_k, q_k) = 1$. Dichos elementos p_k y q_k se obtienen mediante la siguiente relación de recurrencia

$$\begin{aligned} p_0 &= a_0, \\ q_0 &= 1, \\ p_1 &= a_1 a_0 + 1, \\ q_1 &= a_1, \\ &\vdots \\ p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned} \quad (3.7)$$

Pasamos entonces a describir el algoritmo de Shor para obtener la factorización de un número entero $N > 1$.

◊ **Paso 1.** Parte clásica del algoritmo de Shor.

※ **Paso 1.1.** Seleccionamos un número entero aleatorio x tal que $1 < x < N$.

※ **Paso 1.2.** Calculamos $d = \text{mcd}(x, N)$. Si $d > 1$, ya hemos encontrado un factor de N (la probabilidad de que esto ocurra es pequeña para números grandes). En caso contrario ($d = 1$), pasamos a la parte cuántica.

◊ **Paso 2.** Parte cuántica del algoritmo de Shor. Consiste en obtener un estado cuántico a partir del cual podemos obtener el valor de $r = O_N(x)$. Denotemos dicho estado cuántico por $|\tilde{w}\rangle_t$, donde $\tilde{w} \in \{0, \dots, 2^t - 1\}$, siendo $t = 2 \lceil \log_2(N) \rceil$.

◊ **Paso 3.** Parte clásica del algoritmo de Shor.

※ **Paso 3.1.** Extraemos información del valor de r a partir del estado cuántico obtenido en el **Paso 2**. Para ello, supuesto \tilde{w} es distinto de cero (en el caso de que $\tilde{w} = 0$ ejecutamos de nuevo la parte cuántica del algoritmo de Shor), definimos $\xi := \tilde{w}/2^t$. Ahora, para $k = 1$, calculamos p_k y q_k empleando las fórmulas de recurrencia (3.6)-(3.7). Si $x^{q_k} \equiv 1 \pmod{N}$, entonces $r = q_k$. En caso contrario, pasamos a $k = k + 1$. Si terminamos con los posibles valores de k y no obtenemos ningún resultado, volvemos a lanzar la parte cuántica.

※ **Paso 3.2.** Comprobamos si r es par y, en el caso de que sea así, comprobamos si $x^{r/2} + 1 \not\equiv 0 \pmod{N}$. Si alguna de las dos condiciones falla, volvemos al **Paso 1**.

※ **Paso 3.3.** Calculamos

$$\begin{aligned} d_1 &= \text{mcd}(x^{r/2} + 1, N), \\ d_2 &= \text{mcd}(x^{r/2} - 1, N). \end{aligned}$$

Como $2|r$ y $x^{r/2} + 1 \not\equiv 0 \pmod{N}$, se tiene que:

$$x^r - 1 = (x^{r/2} + 1)(x^{r/2} - 1) \equiv 0 \pmod{N},$$

de donde deducimos que d_1 y d_2 son factores no triviales de N (que es precisamente el propósito del algoritmo).

Algoritmo 3.15 (Parte cuántica del algoritmo de Shor). Dado un número entero $N \in (1, \infty) \cap \mathbb{Z}$ y un elemento $x \in (1, N) \cap \mathbb{Z}$, consideramos el siguiente algoritmo cuántico:

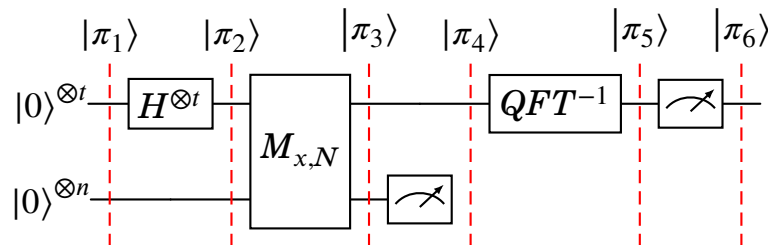


Fig. 3.8. Parte cuántica del algoritmo de Shor.

Analicemos a continuación cada una de las fases en las que hemos dividido el algoritmo anterior.

◊ Cálculo de $|\pi_1\rangle$. Dado $n = \lceil \log_2(N) \rceil$ y $t = 2n$ tenemos que $|\pi_1\rangle = |0\rangle^{\otimes t} \otimes |0\rangle^{\otimes n}$.

◊ Cálculo de $|\pi_2\rangle$. Aplicamos la puerta de Hadamard a cada uno de los cúbits del primer registro:

$$|\pi_2\rangle = \left(H^{\otimes t} |0\rangle^{\otimes t} \right) \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_t \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_t \otimes |0\rangle_n.$$

◊ Cálculo de $|\pi_3\rangle$. Definamos el siguiente operador unitario:

$$M_{x,N} : |j\rangle_t \otimes |k\rangle_n \rightarrow M_{x,N} (|j\rangle_t \otimes |k\rangle_n) := |j\rangle_t \otimes |k + x^j \bmod N\rangle_n.$$

Se tendrá entonces que

$$|\pi_3\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} M_{x,N} (|j\rangle_t \otimes |0\rangle_n) = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_t \otimes |x^j \bmod N\rangle_n.$$

Veamos como queda el estado $|\pi_3\rangle$ en el caso particular de considerar $N = 3$. En este caso, $n = 2$ y $t = 4$. Tomando $x = 2$,

$$\begin{aligned} |\pi_3\rangle = \frac{1}{\sqrt{2^4}} & \left(|0\rangle_4 \otimes |1\rangle_2 + |1\rangle_4 \otimes |2\rangle_2 + |2\rangle_4 \otimes |1\rangle_2 + |3\rangle_4 \otimes |2\rangle_2 + |4\rangle_4 \otimes |1\rangle_2 \right. \\ & + |5\rangle_4 \otimes |2\rangle_2 + |6\rangle_4 \otimes |1\rangle_2 + |7\rangle_4 \otimes |2\rangle_2 + |8\rangle_4 \otimes |1\rangle_2 + |9\rangle_4 \otimes |2\rangle_2 \\ & + |10\rangle_4 \otimes |1\rangle_2 + |11\rangle_4 \otimes |2\rangle_2 + |12\rangle_4 \otimes |1\rangle_2 + |13\rangle_4 \otimes |2\rangle_2 + |14\rangle_4 \otimes |1\rangle_2 \\ & \left. + |15\rangle_4 \otimes |2\rangle_2 \right), \end{aligned}$$

observamos la siguiente periodicidad:

$$\begin{aligned} |\pi_3\rangle = \frac{1}{\sqrt{2^4}} & \left[(|0\rangle_4 + |2\rangle_4 + |4\rangle_4 + |6\rangle_4 + |8\rangle_4 + |10\rangle_4 + |12\rangle_4 + |14\rangle_4) \otimes |1\rangle_2 \right. \\ & \left. + (|1\rangle_4 + |3\rangle_4 + |5\rangle_4 + |7\rangle_4 + |9\rangle_4 + |11\rangle_4 + |13\rangle_4 + |15\rangle_4) \otimes |2\rangle_2 \right]. \end{aligned}$$

Por lo tanto, detallar de forma precisa el resultado de la medición del segundo registro, requiere expresar de forma conveniente la periodicidad que se observa en el ejemplo anterior. En este caso, es posible expresarla de forma simple puesto que $r = O_5(2) = 2$ que, en particular es una potencia de 2. En efecto,

$$|\pi_3\rangle = \frac{1}{\sqrt{2^4}} \sum_{b=0}^{2-1} \left(\sum_{a=0}^{\frac{2^4}{2}-1} |a \cdot 2 + b\rangle_4 \right) \otimes |x^b \bmod 3\rangle_2.$$

Con el fin de simplificar la descripción del algoritmo, supondremos que r es una potencia de 2 (en el ejemplo veremos que ocurre si esto no es así). En este caso,

$$|\pi_3\rangle = \frac{1}{\sqrt{2^t}} \sum_{b=0}^{r-1} \left(\sum_{a=0}^{\frac{2^t}{r}-1} |ar + b\rangle_t \right) \otimes |x^b \bmod N\rangle_n,$$

donde los elementos $|x^b \bmod N\rangle_n$, con $b = 0, \dots, r - 1$, son todos distintos entre si, no aparecen elementos repetidos.

- ◊ Cálculo de $|\pi_4\rangle$. Supongamos que al medir el segundo registro obtenemos el estado $|x^{b_0} \bmod N\rangle_n$ para algún valor $b_0 \in \{0, \dots, r-1\}$. Se tendrá entonces que:

$$|\pi_4\rangle = \sqrt{\frac{r}{2^t}} \left(\sum_{a=0}^{\frac{2^t}{r}-1} |ar + b_0\rangle_t \right) \otimes |x^{b_0} \bmod N\rangle_n.$$

Puesto que el resto de operaciones las haremos con el primer registro y con la finalidad de aligerar la notación, a partir de este momento no tendremos en cuenta el segundo registro en la descripción del algoritmo. Por lo tanto, consideraremos la siguiente notación:

$$|\pi_4\rangle = \sqrt{\frac{r}{2^t}} \sum_{a=0}^{\frac{2^t}{r}-1} |ar + b_0\rangle_t.$$

- ◊ Cálculo de $|\pi_5\rangle$. Tenemos que aplicar la Transformada de Fourier Cuántica Inversa:

$$\begin{aligned} |\pi_5\rangle &= U_{QFT^{-1}} |\pi_4\rangle = \sqrt{\frac{r}{2^t}} \sum_{a=0}^{\frac{2^t}{r}-1} U_{QFT^{-1}} |ar + b_0\rangle_t \\ &= \sqrt{\frac{r}{2^t}} \sum_{a=0}^{\frac{2^t}{r}-1} \left(\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \exp(-2\pi i j(ar + b_0)/2^t) |j\rangle_t \right) \\ &= \frac{1}{\sqrt{r}} \left(\sum_{j=0}^{2^t-1} \left[\frac{r}{2^t} \sum_{a=0}^{\frac{2^t}{r}-1} \exp\left(-\frac{2\pi i j a}{\frac{2^t}{r}}\right) \right] \exp(-2\pi i j b_0/2^t) |j\rangle_t \right). \end{aligned}$$

Ahora bien, denotemos por $M = 2^t/r$ y analicemos el término que está entre corchetes:

$$\frac{1}{M} \sum_{a=0}^{M-1} \exp\left(-\frac{2\pi i j a}{M}\right) = \frac{1}{M} \sum_{a=0}^{M-1} \exp\left(-\frac{2\pi i j}{M}\right)^a. \quad (3.8)$$

Observamos que:

- ✱ Si j es un múltiplo de M , entonces, $\exp(-2\pi i j/M) = 1, \forall a \in \{0, \dots, M-1\}$, de donde se deduce que la suma (3.8) es igual a 1.
- ✱ Si j no es múltiplo de M , entonces podemos calcular el valor de la suma (3.8) empleando la técnica estándar y obtenemos:

$$\frac{1 - \exp(-2\pi i j)}{1 - \exp(-2\pi i j/M)} = 0.$$

Teniendo en cuenta lo anterior,

$$|\pi_4\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp(-2\pi i k b_0/r) \left| \frac{k 2^t}{r} \right\rangle_t.$$

- ◊ Cálculo de $|\pi_6\rangle$. Se tendrá que tras la medición del estado $|\pi_4\rangle$ obtenemos el estado

$$|\pi_6\rangle = \left| \frac{k_0 2^t}{r} \right\rangle_t,$$

para algún valor de $k_0 \in \{0, \dots, r-1\}$ (obsérvese que las probabilidades asociadas a cada uno de los estados básicos que aparecen son las mismas, no ocurre lo mismo en el caso en el que r no sea una potencia de 2). Si $\tilde{w} := k_0 2^t / r = 0$, no tenemos información sobre r y debemos repetir el algoritmo cuántico. Si $\tilde{w} \neq 0$, podemos extraer cierta información sobre r del estado que obtenemos tras la medición.

Ejemplo 3.16 (Aplicación del algoritmo de Shor para factorizar $N = 21 = 7 \cdot 3$). Seguimos los pasos que hemos indicado en el algoritmo:

- ◊ **Paso 1.** Parte clásica del algoritmo de Shor.

- ✳ **Paso 1.1.** Seleccionamos un número entero aleatorio x tal que $1 < x < N$. Por ejemplo, consideremos $x = 2$ ($O_{21}(2) = 6$, que es un número par, además, $x^3 + 1 \pmod{21} = 9$ por lo que el algoritmo de Shor debería funcionar).

- ✳ **Paso 1.2.** Calculamos $d = \text{mcd}(2, 21) = 1$. Pasamos a la parte cuántica del algoritmo.

- ◊ **Paso 2.** Parte cuántica del algoritmo de Shor.

- ✳ Cálculo de $|\pi_1\rangle$. En este caso, $n = 5$, por lo tanto, $t = 10$ y, entonces,

$$|\pi_1\rangle = |0\rangle^{\otimes 10} \otimes |0\rangle^{\otimes 5} = |0\rangle_{10} \otimes |0\rangle_5.$$

- ✳ Cálculo de $|\pi_2\rangle$:

$$|\pi_2\rangle = \frac{1}{\sqrt{2^{10}}} \sum_{j=0}^{2^{10}-1} |j\rangle_{10} \otimes |0\rangle_5.$$

- ✳ Cálculo de $|\pi_3\rangle$:

$$\begin{aligned} |\pi_3\rangle &= \frac{1}{\sqrt{2^{10}}} \sum_{j=0}^{2^{10}-1} |j\rangle_{10} \otimes |2^j \pmod{21}\rangle_5 \\ &= (|0\rangle_{10} \otimes |1\rangle_5 + |1\rangle_{10} \otimes |2\rangle_5 + |2\rangle_{10} \otimes |4\rangle_5 + |3\rangle_{10} \otimes |8\rangle_5 + |4\rangle_{10} \otimes |16\rangle_5 \\ &\quad + |5\rangle_{10} \otimes |11\rangle_5 + |6\rangle_{10} \otimes |1\rangle_5 + |7\rangle_{10} \otimes |2\rangle_5 + |8\rangle_{10} \otimes |4\rangle_5 + |9\rangle_{10} \otimes |8\rangle_5 \\ &\quad + |10\rangle_{10} \otimes |16\rangle_5 + |11\rangle_{10} \otimes |1\rangle_5 + \dots) / \sqrt{2^{10}}. \end{aligned}$$

Reagrupando términos:

$$\begin{aligned}
 |\pi_3\rangle &= (|0\rangle_{10} + |6\rangle_{10} + \dots + |1020\rangle_{10}) \otimes |1\rangle_5 \\
 &\quad + (|1\rangle_{10} + |7\rangle_{10} + \dots + |1021\rangle_{10}) \otimes |2\rangle_5 \\
 &\quad + (|2\rangle_{10} + |8\rangle_{10} + \dots + |1022\rangle_{10}) \otimes |4\rangle_5 \\
 &\quad + (|3\rangle_{10} + |9\rangle_{10} + \dots + |1023\rangle_{10}) \otimes |8\rangle_5 \\
 &\quad + (|4\rangle_{10} + |10\rangle_{10} + \dots + |1018\rangle_{10}) \otimes |16\rangle_5 \\
 &\quad + (|5\rangle_{10} + |11\rangle_{10} + \dots + |1019\rangle_{10}) \otimes |11\rangle_5 / (\sqrt{2^{10}}) \\
 &= \frac{1}{\sqrt{2^{10}}} \left(\sum_{a=0}^{170} |6a+0\rangle_{10} \otimes |1\rangle_5 + \sum_{a=0}^{170} |6a+1\rangle_{10} \otimes |2\rangle_5 \right. \\
 &\quad + \sum_{a=0}^{170} |6a+2\rangle_{10} \otimes |4\rangle_5 + \sum_{a=0}^{170} |6a+3\rangle_{10} \otimes |8\rangle_5 \\
 &\quad \left. + \sum_{a=0}^{169} |6a+4\rangle_{10} \otimes |16\rangle_5 + \sum_{a=0}^{169} |6a+5\rangle_{10} \otimes |11\rangle_5 \right).
 \end{aligned}$$

Observamos los dos últimos términos tienen menos elementos en la suma. Recordemos que, en el caso en el que r fuese una potencia de 2, todas las sumas tendrían el mismo número de términos.

- ✱ Cálculo de $|\pi_4\rangle$. Observamos que el estado básico asociado al segundo registro puede tomar valores en el conjunto $\{1, 2, 4, 8, 16, 11\}$. Supongamos que al medir el segundo registro obtenemos el estado $|8\rangle_5$. En este caso:

$$\begin{aligned}
 |\pi_4\rangle &= \frac{1}{\sqrt{171}} (|3\rangle_{10} + |9\rangle_{10} + \dots + |1023\rangle_{10}) \otimes |10\rangle_5 \\
 &= \frac{1}{\sqrt{171}} \sum_{a=0}^{170} |6a+3\rangle_{10} \otimes |8\rangle_5.
 \end{aligned}$$

Tal y como comentábamos en la descripción del algoritmo, no tendremos en cuenta el segundo registro por simplicidad en la notación:

$$|\pi_4\rangle = \frac{1}{\sqrt{171}} \sum_{a=0}^{170} |6a+3\rangle_{10}.$$

- ✱ Cálculo de $|\pi_5\rangle$:

$$\begin{aligned}
 |\pi_5\rangle &= \frac{1}{\sqrt{171}} \sum_{a=0}^{170} \left(\frac{1}{\sqrt{2^{10}}} \sum_{k=0}^{2^{10}-1} \exp\left(-2\pi i \frac{(6a+3)k}{2^{10}}\right) |k\rangle_{10} \right) \\
 &= \frac{1}{\sqrt{2^{10}}} \sum_{k=0}^{2^{10}-1} \left(\frac{1}{\sqrt{171}} \sum_{a=0}^{170} \exp\left(-2\pi i \frac{6ak}{2^{10}}\right) \right) \exp\left(-2\pi i \frac{3k}{2^{10}}\right) |k\rangle_{10}.
 \end{aligned}$$

✱ Cálculo de $|\pi_6\rangle$. Dado un elemento $k \in \{0, \dots, 2^{10} - 1\}$, denotemos por α_k a la amplitud del estado básico $|k\rangle_{10}$:

$$\alpha_k = \frac{1}{\sqrt{171 \cdot 2^{10}}} \left(\sum_{a=0}^{170} \exp \left(-2\pi i \frac{6ak}{2^{10}} \right) \right) \exp \left(-2\pi i \frac{3k}{2^{10}} \right).$$

Se tendrá entonces que la probabilidad de obtener el estado $|k\rangle_{10}$ tras la medición es

$$|\alpha_k|^2 = \frac{1}{171 \cdot 2^{10}} \left| \sum_{a=0}^{170} \exp \left(-2\pi i \frac{6ak}{2^{10}} \right) \right|^2.$$

Si representamos gráficamente la distribución de probabilidades obtenemos la Figura 3.9. Supongamos entonces que medimos el estado básico más probable

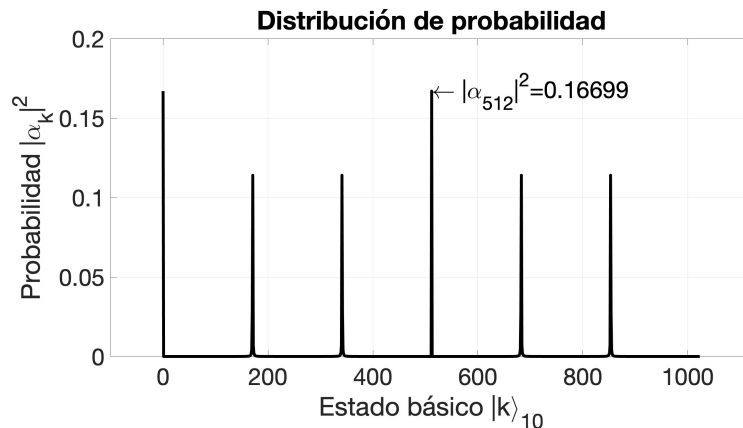


Fig. 3.9. Distribución de probabilidad.

distinto de $|0\rangle_{10}$. En este caso, será el estado $|512\rangle_{10}$. Por lo tanto, $\tilde{w} = 512$.

◇ **Paso 3.**

✱ **Paso 3.1.** Definimos $\xi = 512/1024$ y lo expresamos como una fracción continua:

$$\xi = 0 + \frac{1}{2} = [0; 2].$$

El primer y único convergente es $1/2$, se tiene que $2^2 \bmod 21 = 4$, por lo que debemos repetir la parte cuántica.

Supongamos que volvemos a repetir la parte cuántica y recuperamos el segundo pico $\tilde{w} = 171$. En este caso $\xi = 171/1024$. Si lo expresamos como fracción continua:

$$\xi = 0 + \frac{1}{6 + \frac{1}{-21 + \frac{1}{-2}}}.$$

El primer convergente es $1/6$, además, $2^6 \bmod 21 = 1$. Tenemos entonces que $r = 6$.

- ✳ **Paso 3.2.** Puesto que r es par, lo único que tenemos que comprobar es si $x^{r/2} + 1 \not\equiv 0 \pmod{21}$. Se tendrá que $x^3 + 1 \pmod{21} = 9$, por lo que podemos continuar.
- ✳ **Paso 3.3.** Calculamos:

$$d_1 = \text{mcd}(x^{r/2} + 1, N) = 3,$$

$$d_2 = \text{mcd}(x^{r/2} - 1, N) = 7.$$

Tenemos que $d_1 = 3$ y $d_2 = 7$ son factores no triviales de $N = 21$. De hecho, $N = d_1 \cdot d_2$.



3.5 Algoritmo de Grover

El *algoritmo de Grover* (ver [191–193]) se emplea para encontrar un elemento con una determinada propiedad en una base de datos sin estructura de $N = 2^n$ elementos. Se asienta sobre dos hipótesis fundamentales: la primera es que existe tal elemento y la segunda es que es único. Los algoritmos clásicos de búsqueda, en el peor de los casos, tendrán que comprobar todos los elementos de la base de datos, por lo que el orden de complejidad es $O(2^n)$. En el caso del algoritmo de Grover el orden de complejidad se reduce a $O(\sqrt{2^n})$ lo cual supone una mejora con respecto a los algoritmos clásicos.

Algoritmo 3.17 (Algoritmo de Grover). *Supongamos que tenemos una base de datos de $N = 2^n$ elementos sin estructura cuyos elementos están numerados de 0 a $2^n - 1$. Dentro de la base de datos existe un elemento único identificado con el índice $j_0 \in \{0, \dots, 2^n - 1\}$ tal que:*

$$f : j \in \{0, \dots, 2^n - 1\} \longrightarrow f(j) = \begin{cases} 1, & j = j_0, \\ 0, & j \neq j_0. \end{cases}$$

Se trata de encontrar el índice j_0 que cumple la propiedad anterior. Para ello, se emplea el algoritmo de la Figura 3.10.

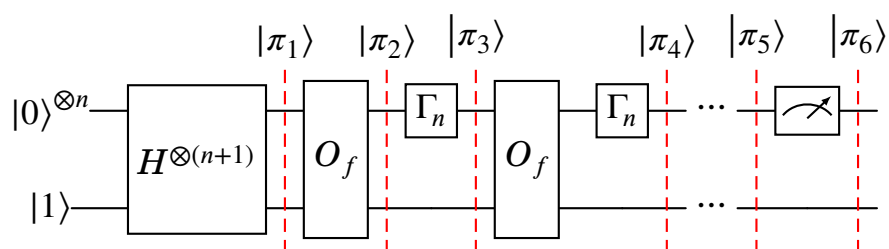


Fig. 3.10. Algoritmo de Grover.

Analizamos cada una de las fases de dicho algoritmo:

◊ Cálculo de $|\pi_1\rangle$.

$$\begin{aligned} |\pi_1\rangle &= H^{\otimes(n+1)} (|0\rangle^{\otimes n} \otimes |1\rangle) = (H^{\otimes n} |0\rangle^{\otimes n}) \otimes (H |1\rangle) \\ &= \left(\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle_n \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = \left(\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle_n \right) \otimes |-\rangle. \end{aligned}$$

◊ Cálculo de $|\pi_2\rangle$. Aplicamos la siguiente transformación unitaria:

$$O_f : |j\rangle_n \otimes |k\rangle \longrightarrow O_f (|j\rangle_n \otimes |k\rangle) = |j\rangle_n \otimes |k \oplus f(j)\rangle.$$

Para ello, introduzcamos los siguientes estados:

$$|\rho\rangle = \frac{1}{\sqrt{2^n-1}} \sum_{j=0, j \neq j_0}^{2^n-1} |j\rangle_n \quad |\gamma\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle_n.$$

Se tendrá que

$$|\gamma\rangle = \frac{\sqrt{2^n-1}}{\sqrt{2^n}} |\rho\rangle + \frac{1}{\sqrt{2^n}} |j_0\rangle_n.$$

En particular,

$$|\pi_1\rangle = |\gamma\rangle \otimes |-\rangle,$$

por lo tanto,

$$\begin{aligned} |\pi_2\rangle &= O_f (|\gamma\rangle \otimes |-\rangle) = O_f \left(\left(\frac{\sqrt{2^n-1}}{\sqrt{2^n}} |\rho\rangle + \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle \right) \\ &= O_f \left(\frac{\sqrt{2^n-1}}{\sqrt{2^n}} |\rho\rangle \otimes |-\rangle \right) + O_f \left(\frac{1}{\sqrt{2^n}} |j_0\rangle_n \otimes |-\rangle \right). \end{aligned}$$

Ahora bien, por un lado,

$$O_f \left(\frac{\sqrt{2^n-1}}{\sqrt{2^n}} |\rho\rangle \otimes |-\rangle \right) = \frac{\sqrt{2^n-1}}{\sqrt{2^n}} |\rho\rangle \otimes |-\rangle,$$

por otro lado,

$$\begin{aligned} O_f \left(\frac{1}{\sqrt{2^n}} |j_0\rangle_n \otimes |-\rangle \right) &= \frac{1}{\sqrt{2^n}} \left(O_f \left(\frac{1}{\sqrt{2}} |j_0\rangle_n \otimes |0\rangle - \frac{1}{\sqrt{2}} |j_0\rangle_n \otimes |1\rangle \right) \right) \\ &= \frac{1}{\sqrt{2^n}} \left(\frac{1}{\sqrt{2}} |j_0\rangle_n \otimes |1\rangle - \frac{1}{\sqrt{2}} |j_0\rangle_n \otimes |0\rangle \right) \\ &= - \frac{1}{\sqrt{2^n}} |j_0\rangle_n \otimes |-\rangle. \end{aligned}$$

Teniendo en cuenta lo anterior,

$$|\pi_2\rangle = \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle \otimes |-\rangle - \frac{1}{\sqrt{2^n}} |j_0\rangle_n \otimes |-\rangle.$$

- ◊ Cálculo de $|\pi_3\rangle$. Aplicamos la transformación unitaria $\Gamma_n \otimes I$, donde $\Gamma_n = 2 |\gamma\rangle \langle \gamma| - I^{\otimes n}$:

$$\begin{aligned} |\pi_3\rangle &= \left((2 |\gamma\rangle \langle \gamma| - I^{\otimes n}) \left(\frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle - \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \right) \otimes |-\rangle \\ &= \left(\frac{2\sqrt{2^n - 1}}{\sqrt{2^n}} |\gamma\rangle \langle \gamma| \rho - \frac{2}{\sqrt{2^n}} |\gamma\rangle \langle \gamma| j_0\rangle_{10} - \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle. \end{aligned}$$

Ahora bien,

$$\begin{aligned} \langle \gamma | \rho \rangle &= \left(\frac{\sqrt{2^n - 1}}{\sqrt{2^n}} \langle \rho | + \frac{1}{\sqrt{2^n}} \langle j_0 | \right) |\rho\rangle = \frac{\sqrt{2^n - 1}}{\sqrt{2^n}}, \\ \langle \gamma | j_0 \rangle_{10} &= \left(\frac{\sqrt{2^n - 1}}{\sqrt{2^n}} \langle \rho | + \frac{1}{\sqrt{2^n}} \langle j_0 | \right) |j_0\rangle_n = \frac{1}{\sqrt{2^n}}, \end{aligned}$$

de donde,

$$\begin{aligned} |\pi_3\rangle &= \left(\frac{2^{n-1} - 1}{2^{n-2}} |\gamma\rangle - \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle \\ &= \left(\frac{\sqrt{2^n - 1}}{\sqrt{2^n}} \left(\frac{2^{n-2} - 1}{2^{n-2}} \right) |\rho\rangle + \frac{1}{\sqrt{2^n}} \left(\frac{3 \cdot 2^{n-2} - 1}{2^{n-2}} \right) |j_0\rangle_n \right) \otimes |-\rangle. \end{aligned}$$

Observamos que la probabilidad de medir el término $|j_0\rangle_n$ en el primer registro,

$$\left(\frac{1}{\sqrt{2^n}} \left(3 - \frac{1}{2^{n-2}} \right) \right)^2 \geq \left(\frac{2}{\sqrt{2^n}} \right)^2 = \frac{4}{2^n},$$

es cuatro veces superior a la probabilidad de medir el término $|j_0\rangle_n$ en el primer registro de $|\pi_1\rangle$ (recordemos que dicha probabilidad es $1/2^n$).

Observación 3.18. Al operador Γ_n se le suele llamar *operador de difusión de Grover* y admite la siguiente representación $\Gamma_n = (H^{\otimes n})(2 |0\rangle_n \langle 0|_n - I^{\otimes n})(H^{\otimes n})$. En las referencias bibliográficas suele denotarse por $G = (\Gamma_n \otimes I)(O_f)$ al operador de Grover.

- ◊ Cálculo de $|\pi_4\rangle$. Con la finalidad de maximizar la probabilidad de medir el estado $|j_0\rangle$ en el primer registro, se aplica la puerta de Grover G de forma reiterada. Se requiere un número $m \simeq O(\sqrt{2^n})$ de iteraciones de G para maximizar la probabilidad de obtener el estado $|j_0\rangle_n$ (ver [91, Theorem 4.6.1]).

Veamos como, efectivamente, aumenta la probabilidad de medir el estado $|j_0\rangle$ en el primer registro si volvemos a aplicar la puerta de Grover a $|\pi_3\rangle$. Para ello, denotemos por:

$$\begin{aligned}\alpha_0 &= 1, \\ \beta_0 &= 1, \\ \alpha_1 &= \left(\frac{2^{n-2} - 1}{2^{n-2}} \right) = \left(1 - \frac{2}{2^{n-1}} \right) = \left(\alpha_0 - \frac{\alpha_0 + \beta_0}{2^{n-1}} \right), \\ \beta_1 &= \left(\frac{3 \cdot 2^{n-2} - 1}{2^{n-2}} \right) = \left(3 - \frac{2}{2^{n-1}} \right) = \left(\alpha_0 + (\alpha_0 + \beta_0) \left(1 - \frac{1}{2^{n-1}} \right) \right),\end{aligned}$$

de esta forma,

$$|\pi_3\rangle = \left(\alpha_1 \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \beta_1 \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle.$$

Si aplicamos el operador O_f :

$$|\pi'_3\rangle = \left(\alpha_1 \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle - \beta_1 \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle.$$

Ahora, aplicamos el operador $\Gamma_n \otimes I$ para obtener $|\pi_4\rangle$:

$$\begin{aligned}|\pi_4\rangle &= \left((2|\gamma\rangle\langle\gamma| - I^{\otimes n}) \left(\alpha_1 \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle - \beta_1 \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \right) \otimes |-\rangle \\ &= \left(\alpha_1 \frac{2\sqrt{2^n - 1}}{\sqrt{2^n}} |\gamma\rangle\langle\gamma|\rho\rangle - \beta_1 \frac{2}{\sqrt{2^n}} |\gamma\rangle\langle\gamma|j_0\rangle_{10} - \alpha_1 \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \beta_1 \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \\ &\quad \otimes |-\rangle \\ &= \left(\left(\frac{\alpha_1 2^n - (\alpha_1 + \beta_1)}{2^{n-1}} \right) |\gamma\rangle - \alpha_1 \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \beta_1 \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle.\end{aligned}$$

Realizando una serie de simplificaciones,

$$\begin{aligned}|\pi_4\rangle &= \left(\left(\alpha_1 - \frac{\alpha_1 + \beta_1}{2^{n-1}} \right) \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle \right. \\ &\quad \left. + \left(\alpha_1 + (\beta_1 + \beta_1) \left(1 - \frac{\alpha_1 + \beta_1}{2^{n-1}} \right) \right) \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle.\end{aligned}$$

Definiendo

$$\alpha_2 = \left(\alpha_1 - \frac{\alpha_1 + \beta_1}{2^{n-1}} \right), \quad \beta_2 = \left(\alpha_1 + (\alpha_1 + \beta_1) \left(1 - \frac{1}{2^{n-1}} \right) \right),$$

tenemos que

$$|\pi_4\rangle = \left(\alpha_2 \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \beta_2 \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle$$

y podemos volver a aplicar la relación de recurrencia para aplicar la puerta de Grover.

- ◊ Cálculo de $|\pi_5\rangle$. Empleando la relación de recurrencia que hemos visto en el punto anterior:

$$|\pi_5\rangle = \left(\alpha_M \frac{\sqrt{2^n - 1}}{\sqrt{2^n}} |\rho\rangle + \beta_M \frac{1}{\sqrt{2^n}} |j_0\rangle_n \right) \otimes |-\rangle,$$

donde $M = O(\sqrt{2^n})$.

- ◊ Cálculo $|\pi_6\rangle$. Después de realizar la medición sobre el primer registro, obtenemos el estado $|j_0\rangle_n \otimes |-\rangle$ con una probabilidad de $\beta_M^2/2^n$.

Ejemplo 3.19. Estudiemos la evolución de la probabilidad de obtener el estado $|j_0\rangle_n \otimes |-\rangle$ para varios valores de n . Para ello, aplicaremos la puerta de Grover $M_n = \lceil \sqrt{2^n} \rceil + 2$ veces.

- ◊ Para $n = 2$, obtenemos la gráfica de la Figura 3.11. Se alcanza el máximo en $n = 2$,

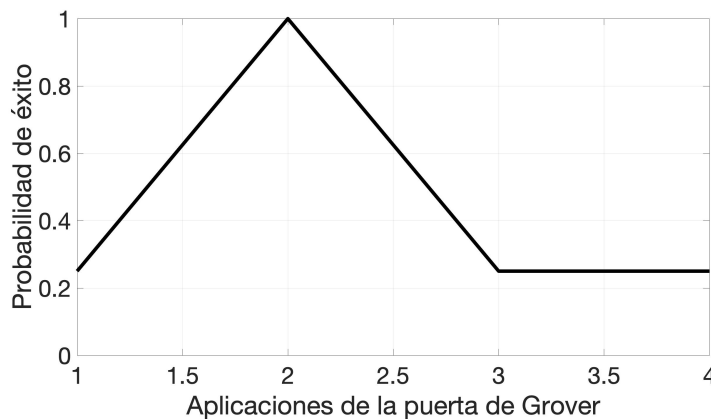


Fig. 3.11. Distribución de probabilidad para $n = 2$.

que se corresponde con $\sqrt{2^2}$.

- ◊ Para $n = 4$, obtenemos la gráfica de la Figura 3.12. Se alcanza el máximo en $n = 4$, que se corresponde con $\sqrt{2^4}$.

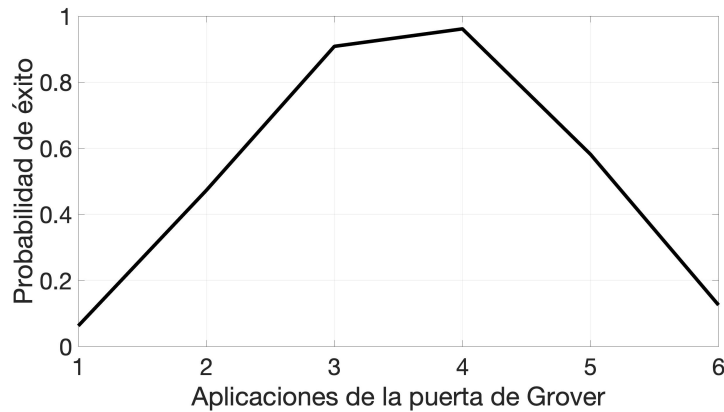


Fig. 3.12. Distribución de probabilidad para $n = 4$.

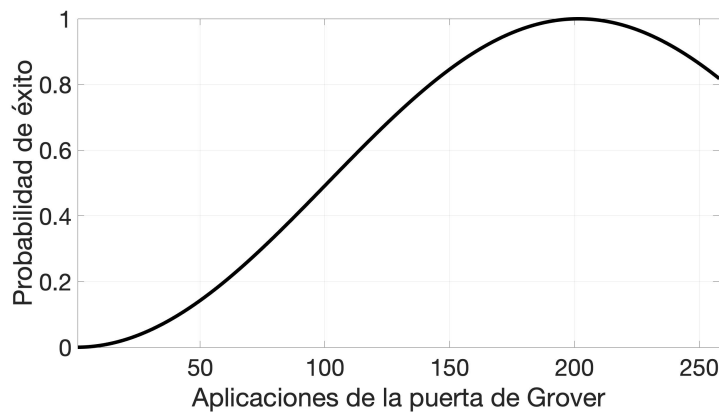



Fig. 3.13. Distribución de probabilidad para $n = 16$.

- ◊ Para $n = 16$, obtenemos la gráfica de la Figura 3.13. En este caso, el máximo se alcanza en $n = 202$ con una probabilidad de $9.999882596461646e - 01$. El valor en donde se alcanza el máximo es inferior a $\sqrt{2^{16}} = 256$.

A la vista del último resultado presentado, puede resultar interesante mostrar gráficamente la evolución de la posición de la probabilidad máxima en función de n (número de cúbits del primer registro). Obtendremos la gráfica de la Figura 3.14. Aunque el número de iteraciones hasta alcanzar el máximo está por debajo de $\sqrt{2^n}$ a partir de un cierto n , el comportamiento de la posición en la que se alcanza el máximo es $O(\sqrt{2^n})$. De hecho, si representamos gráficamente el cociente entre la iteración máxima y $\sqrt{2^n}$, obtenemos la gráfica de la Figura 3.15. A la vista de los resultados numéricos observamos que la posición en la que se alcanza la probabilidad máxima para valores de n superiores a un cierto umbral (pongamos 16 cúbits) es, aproximadamente, $7.853982e - 01 \cdot \sqrt{2^n}$. Por lo tanto, desde un punto de vista práctico, para maximizar la probabilidad de encontrar el elemento buscado, debemos repetir $7.853982e - 01 \cdot \sqrt{2^n}$ veces la puerta de Grover. 

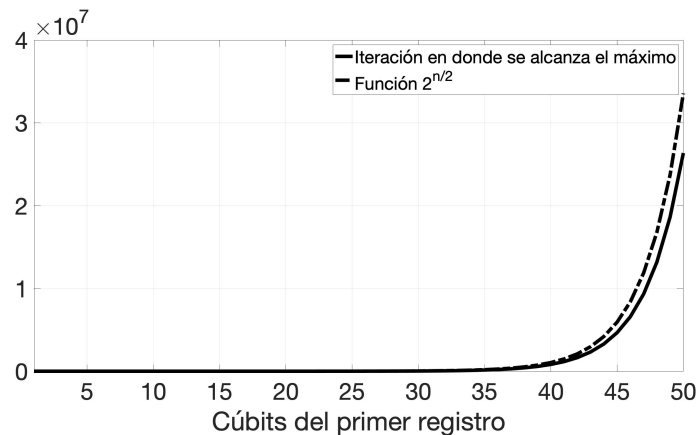


Fig. 3.14. Iteración en la que se alcanza el máximo frente a la función $\sqrt{2^n}$.

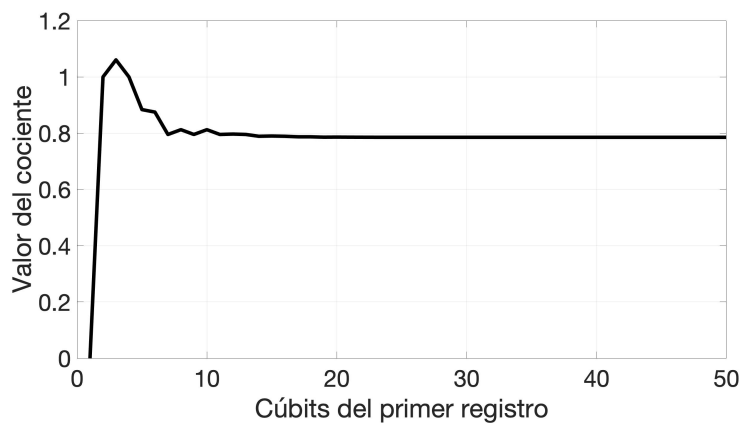


Fig. 3.15. Cociente entre la posición en la que se alcanza la probabilidad máxima y la función $\sqrt{2^n}$.

3.6 El enfoque cuántico para problemas de optimización

Supongamos que queremos resolver un problema de tipo QUBO (*Quadratic Unconstrained Binary Optimization*):

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

Es un problema de optimización combinatoria: en el peor de los casos, podemos obtener la solución comparando el resultado para las 2^p combinaciones binarias posibles de \vec{x} . La solución puede escribirse como un vector (equivalentemente, una cadena) de p bits, ceros y unos. Por ejemplo, imaginemos que la cadena 100 es la solución buscada a un problema QUBO con $p = 3$. Atendiendo a la Notación 1.10, escribiríamos $\vec{j} = 100$ como vector solución.

Esta notación "compacta" es la usada en computación clásica, donde el estado de un registro de p bits es determinista. En este contexto, sólo necesitamos p^2 coeficientes para

definir el problema, esto es, los coeficientes de Q . En una formulación cuántica, el estado de un registro es una combinación compleja unitaria de estados básicos (es decir, de varios vectores \vec{j} como el anterior) y el módulo de los coeficientes de dicha combinación es la probabilidad de que dicho estado sea observado. Por eso, el problema cuántico pasa a estar definido en el espacio $(\mathbb{C}^2)^{\otimes p}$ de dimensión 2^p y debemos trabajar con vectores $|\vec{j}\rangle$, de dicha dimensión.

3.6.1 El hamiltoniano de un sistema cuántico

Para entender cómo el problema compacto de dimensión p se puede describir en el espacio de Hilbert de dimensión 2^p , debemos introducir la ecuación de Schrödinger,

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

donde $|\psi\rangle$ es la función de onda que describe el estado cuántico del sistema, \hbar la constante de Plank reducida, y H es el hamiltoniano, un operador autoadjunto que describe la energía del sistema. Si H es independiente del tiempo, entonces,

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

y, como H es autoadjunto, el operador $\exp\left(-\frac{i}{\hbar}tH\right)$ es unitario. Otra consecuencia de la ecuación de Schrödinger es que, partiendo de un estado $|\psi_0\rangle$ dado, es posible obtener otro estado $|\psi_1\rangle$ evolucionando un sistema con el hamiltoniano adecuado. Esta característica es explotada en la computación cuántica adiabática.

Antes de ver cómo traducir un problema QUBO de p bits a un sistema cuántico con hamiltoniano conocido, debemos remarcar que dicho hamiltoniano tendrá tamaño $2^p \times 2^p$. Por tanto, en la práctica, no tendremos acceso a todas los coeficientes del hamiltoniano (no se almacena H), sino que se realizará el cálculo de la energía del sistema para cualquier estado $|\psi\rangle$. Como veremos, es posible evaluar términos del tipo $\exp(iH) |\psi\rangle$ como una multiplicación de matrices unitarias, expresables en términos de puertas cuánticas.

En resumen, traducir un problema de optimización combinatoria de dimensión p al formalismo cuántico implica obtener un hamiltoniano de tamaño $2^p \times 2^p$. Y no directamente, sino conociendo su evaluación sobre estados $|\psi\rangle$ en términos de una multiplicación de matrices unitarias que puedan describirse como concatenación de puertas cuánticas. Esto abre varias incógnitas que describiremos a continuación.

En principio, el pasar a dimensión 2^p no parece tanto una ventaja (el problema original es de hecho de dimensión p) como una necesidad derivada de la incertidumbre asociada a un sistema cuántico. Además, no hay una forma única de usar el formalismo cuántico:

- ◊ Podemos usar el mundo cuántico sólo para almacenar el problema en sí, permitiendo evaluar el sistema cuántico que luego será usado por un algoritmo clásico de

optimización.

- ◊ A mayores de almacenar el problema, podemos usar algoritmo descrito mediante puertas cuánticas que realice el proceso de optimización.

En el primer caso, el uso de la computación cuántica sólo parece competitiva respecto de la computación clásica si el almacenamiento cuántico se revela más ventajoso que el equivalente clásico. En el segundo, se debe analizar además la ventaja del algoritmo de optimización. Los casos que veremos en esta sección se encuadran en el primer caso (QAOA y VQE). El algoritmo QPE, estudiado previamente, se encuadra en el segundo.

Relacionado con evaluar la ventaja del almacenamiento cuántico, el buscar un método para describir de forma óptima el hamiltoniano en términos de multiplicación de matrices unitarias, es un problema en sí mismo, encuadrado en el problema de la simulación cuántica, tratado en la Sección 9.9.

3.6.2 El modelo Ising

El modelo Ising es un modelo de ferromagnetismo de la mecánica estadística. El modelo se describe en términos de variables discretas que representan el spin atómico de partículas colocadas en una malla, que interaccionan entre sí. El problema consiste en estudiar la evolución del sistema cuántico, lo que requiere definir su hamiltoniano para, por ejemplo, calcular su estado de mínima energía. En concreto, consideremos un conjunto de p partículas colocadas en los vértices V de un grafo, con aristas E . La j -ésima partícula posee un spin, $s_j \in \{-1, 1\}$, siendo $\vec{s} = (s_j)_{j \in V}$ la *configuración de spin*. La energía del sistema es

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

donde $(h_j)_{j \in V}$ es un campo magnético externo actuando sobre el grafo y $(J_{ij})_{(i,j) \in E}$ se relaciona con la interacción entre partículas. Obsérvese que un problema QUBO se puede traducir a Ising con el cambio de variable

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

En el caso de p partículas, dada una configuración de spin, $\vec{s} \in \{-1, 1\}^p$, podemos considerar el estado base de p cúbits asociado, $|\vec{s}\rangle \in (\mathbb{C}^2)^{\otimes p}$. La energía del estado $|\vec{s}\rangle$ se obtiene operando con el hamiltoniano. En el caso del modelo Ising, es posible describir dicho hamiltoniano en función de matrices unitarias (ver [401]), del siguiente modo:

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

donde

$$M_{ij}^k = \begin{cases} \sigma_z & \text{si } k = i \text{ ó } k = j, \\ I & \text{en otro caso} \end{cases} \quad \text{y} \quad M_j^k = \begin{cases} \sigma_z & \text{si } k = j, \\ I & \text{en otro caso.} \end{cases}$$

En la expresión anterior, σ_z es la matriz de Pauli Z e I es la matriz identidad 2×2 .

El efecto del hamiltoniano queda así descrito como una suma de matrices unitarias. De hecho, todo hamiltoniano con interacciones locales puede escribirse de este modo. Por último, la fórmula de Trotter-Suzuki [115] permitirá aproximar la suma anterior por multiplicación de matrices unitarias, abriendo así el camino a su implementación como circuito cuántico:

$$e^{it \sum_j H_j} = \lim_{m \rightarrow \infty} \left(\prod_j e^{iH_j/m} \right)^m .$$

3.6.3 Computación cuántica adiabática

Está basada en el teorema adiabático, de Born y Fock, que establece que si un sistema cuántico se modifica de forma "suficientemente" gradual, entonces el nivel de energía no cambia. Más concretamente, si pretendemos calcular el estado de mínima energía de un hamiltoniano H y conocemos el estado de mínima energía $|\psi_0\rangle$ de otro hamiltoniano H_0 , podemos definir el nuevo hamiltoniano evolutivo en tiempo,

$$H(t) = (1 - t/T)H_0 + t/TH, \quad 0 \leq t \leq T.$$

Si T es suficientemente grande y partimos de $|\psi_0\rangle$, entonces el estado que observaremos para $t = T$ será el buscado. El tamaño de T es inversamente proporcional al espacio (*gap*) existente entre los dos estados de menor energía del hamiltoniano [165]. Este resultado es la base de las máquinas cuánticas adiabáticas. Actualmente disponemos de un subtipo de las anteriores denominado *Quantum Annealer* [286], como las máquinas diseñadas por D-Wave.

3.6.4 Algoritmo QAOA

Este algoritmo parte de la idea del algoritmo cuántico adiabático de dejar evolucionar el hamiltoniano. En este caso, se cambia el tiempo por un parámetro α . Por analogía con la solución de un hamiltoniano estacionario, la solución de $e^{(1-\alpha)H_0 + \alpha H}$ se puede describir de forma análoga a la fórmula de Trotter a través de una multiplicación de exponenciales [272]. En concreto, se parte de un estado inicial $|\psi_0\rangle$, superposición de todos los estados base. Se toma como H_0 un hamiltoniano que aplica a cada dimensión una puerta X de Pauli y , en p pasos, se multiplica por las exponenciales que dependen de los parámetros $\vec{\beta} = (\beta_k)$, $\vec{\gamma} = (\gamma_k)$, para obtener un nuevo estado:

$$|\psi\rangle_{\vec{\beta}\vec{\gamma}} = \left(\prod_{k \in \{p, p-1, \dots, 1\}} e^{-i\beta_k H_0} e^{-i\gamma_k H} \right) |\psi_0\rangle.$$

Estas multiplicaciones permiten transformar la fase en probabilidad, persiguiendo que el estado buscado sea más probable. Para encontrar los valores óptimos de los parámetros:

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

se utiliza un algoritmo de optimización clásico, ejecutado en una máquina clásica. De este modo, la máquina cuántica se utiliza únicamente para almacenar el problema. Los métodos de descenso de gradiente pueden combinarse con pasos de recocido simulado o estrategias que involucren comenzar desde múltiples puntos iniciales [292].

3.6.5 Algoritmo VQE

Este algoritmo permite calcular el autovector asociado al menor autovalor E_0 del hamiltoniano. La idea principal tras el método es el llamado *principio variacional*:

$$\langle \psi | H | \psi \rangle \geq E_0 \langle \psi | \psi \rangle, \text{ para todo estado } |\psi\rangle.$$

Para buscar el estado que minimiza la energía, se propone una representación parametrizada del estado (o *ansatz*) que permita recorrer un subespacio de $(\mathbb{C}^2)^{\otimes n}$. La elección de este *ansatz* es fundamental para la convergencia del método.

El algoritmo VQE admite representaciones parametrizadas que no pueden ser simulados de forma eficiente en un ordenador clásico, lo que podría suponer una ventaja de la computación cuántica. En [325] se mostró un caso con escalado polinómico en el tamaño del registro en cúbits. Además, se debe escoger un optimizador apropiado ya que este tendrá un impacto directo en la convergencia del método, sobre todo porque las mediciones en una máquina cuántica son de facto estocásticas, por lo que para obtener la esperanza de un operador es necesario repetir las mediciones hasta alcanzar el nivel de precisión deseado [389].

4 Computación clásica y computación cuántica

En este apartado hablaremos de la relación que existe entre la computación clásica y la cuántica desde varios puntos de vista de modo que podamos compararlas.

4.1 Clases de complejidad

Empezaremos hablando de la complejidad de los problemas, es decir, del tiempo o espacio (memoria) que requiere su resolución. Hay que destacar que la complejidad está en realidad asociada a los algoritmos de resolución que se utilizan para resolver los problemas, pero se sospecha que existen problemas genuinamente más difíciles, es decir, que todo algoritmo que los resuelva requiere muchos recursos.

4.1.1 Complejidad clásica

La complejidad computacional es un campo de la informática que se ocupa de analizar y clasificar la eficiencia de los algoritmos y problemas en términos de los recursos computacionales que requieren. Su objetivo es comprender cómo crecen los requisitos de tiempo y espacio de los algoritmos a medida que aumenta el tamaño de los datos de entrada.

La clase de *complejidad computacional P* (tiempo polinómico) consiste en problemas de decisión que pueden resolverse en tiempo polinómico en una *máquina de Turing determinista* (el modelo básico de computación). Estos son problemas para los que existe un algoritmo que puede proporcionar una solución en un tiempo que es una función polinómica del tamaño de la entrada.

Una *máquina de Turing no determinista* (NDTM) es un modelo de computación que extiende el concepto de una máquina de Turing determinista al poder estar en varios estados simultáneamente y explorar múltiples rutas de cálculo en paralelo.

Si un problema está en la *clase NP* (tiempo polinómico no determinista), significa que la solución al problema se puede verificar en tiempo polinómico o, equivalentemente, que una máquina de Turing no determinista puede obtener la solución en tiempo polinómico.

La relación entre NP y P se desconoce a día de hoy. Específicamente, no se sabe si los problemas NP-completos, que son un subconjunto de NP, se pueden resolver en tiempo polinómico (es decir, si $P = NP$).

Un problema pertenece a a clase *NP-completo* (tiempo polinómico no determinista completo) si es un problema de NP al cual cualquier otro problema de NP se puede reducir en tiempo polinómico.

La clase *NP-difícil* (tiempo polinómico no determinista difícil) se refiere a aquellos problemas de decisión L tales que cada problema en NP puede reducirse a L en tiempo polinómico. La distinción clave entre los problemas NP-difícil y NP-completos es que mientras que los problemas NP-completos son un subconjunto de los problemas NP-difícil y pertenecen a NP en sí mismos, los problemas NP-difícil no necesariamente pertenecen a NP.

La *clase de complejidad co-NP* contiene problemas de decisión para los cuales se puede verificar en tiempo polinómico que una solución propuesta es incorrecta o no es válida.

La *clase PSPACE* representa aquellos problemas de decisión que se pueden resolver usando una cantidad de memoria polinómica en el tamaño de la entrada en una máquina de Turing determinista. Es la contraparte de la clase de complejidad temporal P pero se centra en el uso del espacio o la memoria en lugar del tiempo. En general suele haber una compensación entre la complejidad temporal y la complejidad espacial. Cuanto más eficiente con relación al espacio es un algoritmo, tanto menos lo es temporalmente y viceversa.

La *clase de complejidad #P* es una clase de problemas de conteo. A diferencia de los problemas de decisión, que buscan una respuesta binaria (sí o no), los problemas en #P requieren determinar el número exacto de soluciones válidas o rutas posibles dentro de una instancia de problema. #P es una subclase de la clase de complejidad PSPACE.

La *clase de complejidad BPP*, que significa "Bounded Error Probabilistic Polynomial time", es una clase que captura problemas que pueden resolverse en tiempo polinómico con cierta probabilidad de error. Para un problema de decisión en BPP, debe haber dos probabilidades asociadas con él: la probabilidad de que el algoritmo genere *sí* cuando la respuesta correcta es de hecho *sí* debe ser mayor que $1/2 + \epsilon$, donde ϵ es alguna constante positiva y la probabilidad de que el algoritmo genere *no* cuando la respuesta correcta es *no* también debe ser mayor que $1/2 + \epsilon$. En otras palabras, a los algoritmos BPP se les permite cometer errores con una probabilidad de como máximo $1/2 + \epsilon$ para cada entrada posible, pero deben ser más propensos a producir la respuesta correcta.

4.1.2 Complejidad cuántica

En el caso de los ordenadores cuánticos, tenemos que lidiar con un nuevo paradigma de computación que requiere nuevas clases de complejidad.

La *clase de complejidad BQP*, que significa "Bounded Error Quantum Polynomial time", es el análogo cuántico de la clase de complejidad clásica BPP. En BQP el algoritmo debe ejecutarse en tiempo polinómico con respecto al tamaño de la entrada y se le permite tener una probabilidad de error acotada, similar a la probabilidad de error permitida en la clase BPP. Esto significa que, para un problema en BQP, el ordenador debe proporcionar la respuesta correcta con alta probabilidad (por ejemplo, mayor de $2/3$ de probabilidad de ser correcta) cuando se le da una entrada específica. Un problema es *BQP-completo* si puede ser resuelto por un ordenador cuántico en tiempo polinómico, y cualquier problema BQP puede reducirse a este problema.

La *clase de complejidad Quantum-Merlin-Arthur*, QMA, captura problemas de decisión para los cuales un ordenador cuántico puede verificar soluciones de un problema de decisión con alta probabilidad. Este proceso de verificación puede implicar la ejecución de un algoritmo cuántico para comprobar si un estado cuántico (que representa una solución) satisface ciertas propiedades. Se requiere que el proceso de verificación se ejecute en tiempo polinómico con respecto al tamaño de la entrada. Además, para que un problema esté en QMA, debe existir un *testigo cuántico*, esto es, un estado cuántico que, cuando se proporciona como entrada al verificador cuántico, convence al verificador de la correc-

ción de la solución con alta probabilidad. En otras palabras, si la respuesta al problema de decisión es *sí*, debería existir un estado cuántico que, cuando sea comprobado por el verificador cuántico, tenga una alta probabilidad de ser aceptado como una solución válida. Al igual que BQP, QMA permite una probabilidad acotada de error. El proceso de verificación debe aceptar soluciones válidas con alta probabilidad, típicamente mayor que $2/3$, y rechazar soluciones no válidas con alta probabilidad.

QMA es un análogo cuántico de la *clase de complejidad clásica MA* (Merlin-Arthur), que implica la verificación probabilística por un probador (Merlin) para convencer a un verificador (Arthur) de que existe una solución.

La *clase de complejidad de un cúbit limpio* (DQC1) consiste en los problemas de decisión que pueden ser resueltos en tiempo polinómico por una máquina de *cúbits limpios* (con estados puros) con una probabilidad de corrección de al menos $2/3$ [371]. En este modelo se presenta un estado cuántico inicial que consiste en un solo cúbit en el estado puro cero y n cúbits en el estado máximo mezclado. Se puede aplicar cualquier circuito cuántico de tamaño polinómico y luego medir el primer cúbit en la base computacional, así como repetir el experimento una cantidad de veces polinómica en la entrada.

4.2 La ventaja cuántica

// There are two kinds of quantum advantages. The theoretical one, i.e. the possibility that in an idealized world a perfect quantum computer could perform parametrically better than a classical one for a given task. And the practical one, i.e. the possibility that an actual device does something useful faster than a classical machine. //

E.M. Stoudenmire and Xavier Waintal
Grover's Algorithm Offers No Quantum Advantage (2023).

La ventaja cuántica, también conocida como *supremacía cuántica*, es posiblemente uno de los temas más contenciosos dentro de la computación cuántica, por razones que enseguida serán evidentes.

La *ventaja cuántica* puede entenderse, de manera informal, como la capacidad de un ordenador cuántico para resolver un problema determinado que un ordenador clásico no puede resolver o para la resolución del cual requeriría un tiempo inasumible. La vaguedad de esta noción intuitiva lleva a que no exista un acuerdo en qué requisitos debe satisfacer un algoritmo u ordenador cuántico para poder afirmar que existe una ventaja cuántica. Elegir aplicar el concepto ventaja cuántica a un algoritmo o a un ordenador cuántico conlleva una distinción importante. Los algoritmos son abstracciones matemáticas, libres de las ataduras del mundo real, mientras que los ordenadores cuánticos son objetos físicos cuya viabilidad depende tanto de la facultad de conceptualizarlos como de la capacidad para construirlos. En esta disyuntiva vamos a optar de forma conservadora por un criterio

estricto: para que haya ventaja cuántica debe existir

1. un ordenador cuántico
2. que resuelva un problema (de entrada a salida)
3. que un ordenador clásico no puede resolver en un tiempo razonable.

Que exista o no un tiempo razonable depende esencialmente de que haya una diferencia entre la complejidad de los algoritmos en cuestión entre el ordenador clásico y el cuántico. De este modo, tomando una entrada suficientemente grande, si la complejidad del algoritmo cuántico es mejor que la del clásico, el ordenador cuántico podrá resolver el problema mientras que el clásico no.

Obtener las complejidades de los algoritmos es, contraintuitivamente, el requisito más sencillo de verificar. El problema no reside tanto en obtener la complejidad del algoritmo cuántico, sino en demostrar que no puede existir algoritmo clásico que la iguale. Existen cotas inferiores para la complejidad de ciertos algoritmos clásicos sencillos (por ejemplo, el ordenamiento de listas), pero en general no se conocen dichas cotas. Con esto, muchas declaraciones de supremacía cuántica se basan en comparar los algoritmos cuánticos con los mejores algoritmos clásicos conocidos. Esto es relevante ya que, a medida que se han descrito algoritmos cuánticos mejores, también han aparecido algoritmos clásicos nuevos que limitan la ventaja de estos [7], fenómeno que se conoce como *descuantización* [128]. En general, determinar si la ventaja que presenta un algoritmo cuántico frente al mejor algoritmo clásico conocido se deriva de la naturaleza cuántica del algoritmo o meramente del ingenio del mismo (y por tanto puede obtenerse una versión clásica de éste) es un problema crucial al que los investigadores deben enfrentarse a cada paso y que pone en competición directa a la computación clásica y la cuántica. El resultado de esta competición es netamente positivo ya que conlleva mejoras en ambos campos.

Indicar que el problema debe ser resuelto de entrada a salida, también es crucial. Muchos algoritmos cuánticos usan *oráculos*, esto es, cajas negras formales que dada una entrada devuelven la salida deseada de forma inmediata y sin limitaciones técnicas. El uso de estos oráculos puede ocultar la verdadera complejidad del problema. De poco sirve un algoritmo cuántico que, para un problema dado, tiene una complejidad mejor que la clásica en una parte del mismo si en otra, la del oráculo, no la tiene. Determinar si el oráculo es clásico o no también tiene ramificaciones. Existen situaciones en las cuales si el oráculo se puede simular de forma clásica de manera sencilla, no es necesario un ordenador cuántico, mientras que si requiere un ordenador cuántico, la implementación cuántica es inviable [380].

Esto nos lleva al último punto: un ordenador cuántico capaz de resolver el problema debe poder construirse. Los ordenadores clásicos dejan de ser competitivos para problemas de alta complejidad cuando las entradas son muy grandes, pero cualquier ordenador cuántico que pretenda resolver el mismo problema debe ser capaz de gestionar dichas entradas. Para muchos algoritmos cuánticos, esto no solo supone la inclusión de un gran

número de cúbits, sino la interconexión de dichos cubits, lo cual, más allá de las limitaciones tecnológicas actuales, no es escalable. A la hora de diseñar algoritmos cuánticos existe el riesgo de convertir la complejidad temporal del problema en complejidad espacial (complejidad del circuito físico, tanto por número de componentes como por conexiones), de modo que se obtiene un algoritmo que *en teoría* es mucho mejor que el clásico, pero que nunca se podría implementar. Esta relación inversa entre la complejidad temporal y espacial es bien conocida [242, 291], pero los problemas de la complejidad espacial no terminan ahí. Los ordenadores cuánticos, más allá de que trabajen con frecuencia con algoritmos probabilísticos (algoritmos que presentan una cierta incertidumbre en los resultados), están sujetos a errores físicos (ruido) y decoherencia (pérdida de las propiedades cuánticas). Este problema es mucho más acuciante que en la computación clásica dada la fragilidad de los estados cuánticos y este tipo de errores crece a medida que lo hace la complejidad física. Un algoritmo cuántico complejo requiere también mantener el estado cuántico durante el tiempo suficiente para hacer los cálculos y este estado puede decaer mucho antes, lo que imposibilita realizar el cálculo. Desde los inicios de la computación cuántica hasta la actualidad se ha dedicado mucho esfuerzo a desarrollar mecanismos de corrección de errores y algoritmos resistentes a los errores [34, 51, 186, 376]. Teniendo en cuenta estas dificultades, es previsible que para que un algoritmo cuántico sea útil en la práctica, el problema a resolver deberá contar con una cantidad reducida de datos y una aceleración exponencial frente a los algoritmos clásicos [211].

El término “supremacía cuántica” ha caído paulatinamente en desuso a favor del más moderado “ventaja cuántica” a medida que las expectativas puestas inicialmente sobre la computación cuántica se han ido demostrando excesivas. Es un término que sin embargo se ha utilizado mucho en el sector industrial de la computación cuántica (e.g. [32]). La implementación real de la computación cuántica supone una inversión extraordinaria por parte de las empresas interesadas, que requiere, por tanto, la obtención de un producto extraordinario. Si bien los hitos conseguidos hasta la fecha son ciertamente pasos de gigante, hay que ser conscientes de los intereses subyacentes a las declaraciones de supremacía cuántica.

Toda esta discusión nos lleva a una última pregunta que se esconde en el corazón de todo aquel que se dedica o quiera dedicarse a investigar en computación cuántica: *¿merece la pena?*

Creemos que la respuesta es sí. Incluso aunque la promesa cuántica no llegase a materializarse, el mero hecho de investigar sobre ella ya ha dado frutos que de sobra compensan el esfuerzo. A nivel tecnológico ha supuesto un impulso a tecnologías cruciales para otros sectores, como los superconductores o la refrigeración a muy bajas temperaturas, a nivel físico a supuesto la constación de los principios de la mecánica cuántica, área que aún a día de hoy no entendemos del todo, y a nivel matemático y algorítmico ha generado una ola de algoritmos clásicos inspirados en algoritmos cuánticos que nos permitirán dar un nuevo empuje a la computación en una época en la que la deceleración de la ley de Moore (los procesadores están llegando a su límite físico de tamaño debido, precisamente, a la mecánica cuántica) ha hecho que la eficiencia en el cálculo cobre más importancia que nunca.

Somos conscientes de que muchas de estas preocupaciones no son relevantes para muchos matemáticos (tenemos el privilegio de poder alejarnos del mundo real) pero también creemos que no se cumplirán los peores pronósticos. En la siguiente sección detallamos como creemos que será la computación cuántica en la práctica en un futuro cercano y su papel en el desarrollo de la ciencia, las matemáticas y la sociedad.

4.3 El futuro de la computación cuántica

La discusión relativa a la ventaja cuántica anterior adolece de un problema de perspectiva. Equivale a preguntar *¿qué es más útil para comer, un tenedor o un cuchillo?* La respuesta obvia es que son dos instrumentos distintos para distintos fines y que los mejores resultados se obtienen al usarlos conjuntamente. Lo mismo puede decirse de la computación clásica y la cuántica.

Creemos que un paradigma realista del futuro a medio plazo incluirá una ventaja cuántica efectiva, esto es, existirán tareas concretas para las cuales los ordenadores cuánticos serán la mejor opción en ese momento dado. Previsiblemente, estas tareas tendrán relación con la optimización de funciones y la resolución de problemas combinatorios ya que la computación cuántica, por su naturaleza, es especialmente propicia para este tipo de tareas.

Del mismo modo que, en la actualidad, muchos centros de investigación cuentan con superordenadores conectados en línea que se utilizan para realizar subrutinas que admiten un cálculo en paralelo eficiente dentro de un algoritmo más complejo, es previsible que los mismos centros cuenten con ordenadores cuánticos accesibles en línea para realizar cálculos concretos. Estos ordenadores cuánticos no sustituirán a los superordenadores clásicos, sino que se convertirán en una herramienta más de la computación.

A nivel industrial, es esperable que se ofrezcan servicios de computación cuántica en línea para la realización de cálculos cuánticos (empresas como por ejemplo IBM, Google, Amazon, Microsoft, D-Wave o Rigetti ya los ofrecen) en centros de computación cuántica y análisis de datos especializados. Estos cálculos seguramente serán "breves" para evitar errores y con varias llamadas a lo largo de un algoritmo clásico que coordinará el trabajo.

También es previsible la creación de QPUs (procesadores cuánticos) "analógicos" que permitan resolver problemas de optimización relativos a la química, a la física y a la biología. Estos procesadores serían creados *ad hoc* para resolver el problema en cuestión usando la naturaleza cuántica del problema como ventaja (esto es, usar ordenadores cuánticos para simular procesos cuánticos).

Menos probable es la distribución de QPUs comerciales para uso doméstico o en pequeñas instalaciones ya que, hasta la fecha, no se ha encontrado una forma de mantener los estados cuánticos sin un delicado y costoso equipamiento no apto para el uso doméstico. Es posible que esa situación cambie a largo plazo, con algún avance que permita dar el salto que los semiconductores ofrecieron a la computación clásica, pero cualquier argumento en esa dirección resultaría puramente especulativo.

4.4 El papel de la investigación matemática en la computación cuántica

Queda entonces por determinar cual es o debe ser el papel de la comunidad matemática en el campo de la computación cuántica. En España los esfuerzos relativos a la computación cuántica están coordinados a través de la red Quantum Spain¹ de la cual el Centro de Supercomputación de Galicia (CESGA) forma parte. Esta red tiene, entre otros objetivos, crear un computador cuántico de altas prestaciones y un servicio de acceso remoto en la nube al procesador con la finalidad de permitir a la industria y al sector público experimentar con los nuevos algoritmos cuánticos y desarrollar librerías de algoritmos cuánticos útiles, aplicables a problemas reales, para usuarios finales tanto de empresas como de entidades públicas.

Es en este último apartado donde la comunidad matemática más puede aportar. Ya existen grupos de investigación trabajando en este ámbito, como por ejemplo, el grupo QUANTIC² en el Centro Nacional de Supercomputación (BSC-CNS) en Barcelona, el grupo de QUANTIA³ de la Universidad de Zaragoza, el proyecto Basque Quantum⁴ de la Fundación Basca para la Ciencia (Ikerbasque) o el EHU Quantum Center⁵ de la Universidad del País Vasco (UPV/EHU), entre otros, además de investigadores de todo tipo de organismos de investigación como pueden ser el ICREA en Cataluña, la Universidad del País Vasco (UPV/EHU), el BCAM en el País Vasco o el CESGA en Galicia, entre otros.

Pese al número creciente de grupos de investigación a nivel estatal dedicados a la computación cuántica, la participación de los matemáticos resulta a veces limitada, más aún en Galicia, donde no hay equipos de investigación de matemáticos dedicados a la computación cuántica o que cuenten con la computación cuántica como una de sus líneas de investigación, aunque hay que destacar, como parte de la Facultad de Informática de A Coruña, el Laboratorio de Investigación y Desarrollo en Inteligencia Artificial (LIDIA) que tiene la computación cuántica entre sus líneas de trabajo.

La investigación matemática resulta clave a la hora de avanzar en la computación cuántica, ya que es la única forma de conocer las limitaciones y posibilidades de la computación cuántica antes de realizar la inversión necesaria en tecnología para implementar los algoritmos y, una vez hecha esta, resulta fundamental a la hora de entender el funcionamiento de los ordenadores cuánticos en relación a su arquitectura y para la elaboración de algoritmos cuánticos adaptados a la máquina en cuestión.

El CESGA contará dentro de poco con un ordenador cuántico dentro de su centro para la computación cuántica como parte del Polo de Tecnologías Cuánticas de Galicia. Esto supone una oportunidad crucial para que los matemáticos podamos acceder a la tecno-

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/>.

⁴<https://www.ikerbasque.net/es/noticias/presentacion-del-proyecto-basque-quantum>.

⁵<https://www.ehu.eus/es/web/quantum-center>.

logía con la que poder comprobar los frutos de nuestra investigación en computación cuántica.

Parte II

Algoritmos y líneas de investigación actuales en computación cuántica

En esta segunda parte comentaremos la bibliografía que se puede consultar (monografías básicas y revisiones bibliográficas especializadas) y los recursos disponibles para informarse, investigar y usar la computación cuántica. También ofreceremos una lista de problemas y algoritmos, descritos brevemente, con abundantes referencias bibliográficas referentes al estado del arte y, en su caso, los problemas abiertos y tendencias. Incluimos también un resumen de las posibles aplicaciones a la industria y casos de uso de la computación cuántica. Finalmente ponemos el foco sobre el caso de España, sus instituciones en materia de computación cuántica, sus recursos y sus proyectos abiertos.

5 Introducción

5.1 Bibliografía y recursos

La investigación en computación cuántica en lo referente a algoritmos y resolución de problemas matemáticos ha crecido exponencialmente en las dos últimas décadas. A pesar de ser un campo incipiente, se cuenta ya con una gran número de monografías y revisiones. Estos documentos sirven la necesidad fundamental de ir estableciendo un camino sólido sobre el cual formar a los nuevos investigadores y reflexionar sobre los retos que quedan por abordar, pero, debido a la enorme velocidad del desarrollo del campo, a menudo se quedan parcialmente anticuadas con el paso un unos pocos años.

En cualquier caso, el lector interesado puede consultar, entre otras, el artículo de iniciación a la computación cuántica [306] y las monografías [117, 144, 210, 266] para acceder a una breve introducción a los algoritmos cuánticos y sus aplicaciones. Con respecto a los estudios técnicos y revisiones bibliográficas, se pueden consultar [170, 183, 196, 297, 304, 313, 319, 345, 375] y, en lo relativo a aquellos centrados en aplicaciones concretas, señalamos las siguientes en las áreas de álgebra [101, 135], búsqueda cuántica [185], comprobación cuántica de propiedades [300], *machine learning* [30, 149, 150, 152, 177, 262, 288, 438], algoritmos variacionales [92], caminatas cuánticas [228, 393], finanzas [15, 75, 155, 188, 209, 305, 320], complejidad [9, 392] e imágenes [87, 402, 424, 425].

Hay que destacar también la cada vez mayor prominencia de los recursos electrónicos y en línea a la hora de investigar en computación cuántica. Contamos, por una parte, con los repositorios tradicionales como puede ser *arXiv*, en particular el *Computing Research Repository*¹ (CoRR) especializado en investigación en computación, donde aparecen publi-

¹<https://info.arxiv.org/help/cs/index.html>.

cadav la mayoría de versiones preliminares de artículos de investigación en computación cuántica. *Quantum Algorithm Zoo*¹ es una página web que ofrece un enorme y exhaustivo catálogo de algoritmos cuánticos así como bibliografía relativa a los mismos y que hemos usado extensamente para este informe. *Quantum Computing Report*² por su parte, ofrece noticias actualizadas, opiniones y otros recursos en línea. *Quantum Computing Stack Exchange*³ por su parte es un foro donde se pueden realizar y responder a preguntas relativas a la computación cuántica a la comunidad. Este puede ser un recurso muy útil para obtener respuestas rápidas a dudas comunes o consultar detalles específicos que no se explican de forma habitual en la bibliografía más tradicional.

Algunas páginas web ofrecen la posibilidad de aprender a programar algoritmos cuánticos (por ejemplo, *Qiskit Textbook*⁴ de IBM) o presentan lenguajes de programación, entornos de desarrollo o recursos implementación de estos. Este es el caso de Qiskit⁵ (IBM), *Microsoft Quantum Development Kit*⁶ (Microsoft), *Cirq*⁷ (Google), *Quantum Computing Playground*⁸ o *Rigetti Forest*⁹.

En la Tabla 5.1 se ofrece una comparativa de diferentes herramientas de software para la computación cuántica.

Finalmente, para aquellos que deseen acceder al uso de un ordenador cuántico desde la nube, *IBM Quantum*¹⁰ ofrece la posibilidad de realizar computación cuántica real usando Qiskit y *Google Quantum AI*¹¹ con Cirq, entre otros.

5.2 Planteamiento de las líneas de investigación y problemas

Presentaremos las diferentes líneas de investigación de la siguiente manera: plantearemos en cada sección un problema o algoritmo clasificado según su área de conocimiento. Esta división es, en última instancia, arbitraria, ya que muchos algoritmos y problemas son relativos a diversas áreas, pero su objetivo es facilitar la localización de las distintas líneas. También hay que destacar que no existe una correspondencia biyectiva entre problemas y algoritmos: a menudo un problema se puede resolver usando diferentes algoritmos y un algoritmo puede ser usado, tal vez con pequeñas modificaciones, para resolver varios problemas, lo que a veces dificulta la clasificación y hace que haya referencias cruzadas. Cada problema o algoritmo lleva asociadas además unas palabras clave que podrán

¹<https://quantumalgorithmzoo.org/>.

²<https://quantumcomputingreport.com/news/>.

³<https://quantumcomputing.stackexchange.com/>.

⁴<https://qiskit.org/learn/>.

⁵<https://qiskit.org/>.

⁶<https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk>.

⁷<https://quantumai.google/cirq>.

⁸<https://www.quantumplayground.net/#/home>.

⁹<https://pyquil-docs.rigetti.com/en/v2.7.2/>.

¹⁰<https://quantum-computing.ibm.com/>.

¹¹<https://quantumai.google/>.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
QuEST	✓	✓	✓	X	X	X	X	X	✓	✓	✓	X	X	X	X	C
Staq	✓	✓	✓	X	X	X	X	X	✓	✓	✓	X	X	X	X	C++
Scaffold / ScaffCC	✓	✓	✓	X	X	X	X	X	✓	X	✓	X	✓	X	X	Scaffold
Qrack	✓	✓	✓	X	X	X	X	X	✓	X	✓	X	X	X	X	C++
QX Simulator	✓	✓	✓	X	X	X	X	X	✓	X	✓	X	X	✓	X	Quantum Code
Quantum++	✓	✓	✓	X	X	X	X	X	✓	X	✓	X	X	X	X	C++
Quantum Programming Studio	X	✓	✓	X	X	X	X	✓	X	✓	✓	X	✓	✓	✓	Javascript
Q++	✓	X	✓	X	X	X	X	X	✓	✓	✓	X	✓	X	✓	C++
Quantum Circuit	✓	X	✓	X	X	X	X	X	✓	✓	✓	X	✓	X	✓	Javascript
Quantum.NET	✓	X	✓	X	X	X	X	X	✓	✓	✓	X	X	X	X	NET
Cirq	✓	✓	✓	X	X	X	X	X	✓	✓	✓	✓	✓	✓	✓	Python
Qiskit	✓	✓	✓	X	X	✓	X	X	✓	✓	✓	✓	✓	✓	✓	Python
Quantum Development Kit (QDK)	✓	✓	✓	X	X	✓	X	X	✓	✓	✓	✓	✓	✓	✓	Python, Q#
Quantum-Walk, j1	✓	✓	✓	X	X	✓	X	X	✓	✓	✓	✓	X	✓	✓	Julia
Bloch Sphere	✓	✓	✓	X	X	✓	✓	✓	X	✓	✓	X	✓	X	✓	Java

Tabla 5.1. Herramientas y tecnologías para software cuántico, adaptada de [375, Table 2].

Leyenda: **1** nombre de la herramienta o técnica, **2** biblioteca, **3** caja de herramientas, **4** código abierto, **5** comercial, **6** software libre, **7** interfaz de usuario, **8** visualización 3D, **9** soporte para "arrastrar y soltar", **10** uso de línea de comandos, **11** soporte para puertas cuánticas, **12** simulación, **13** implementación real, **14** ayuda integrada para algoritmos cuánticos, **15** temporalización de las puertas y paralelismo, **16** soporte para matrices o diagramas, **17** lenguaje de programación usado para la herramienta.

ser buscadas en el índice al final del documento para simplificar su localización. En general, se señalará en cursiva el problema concreto que se pretende estudiar. A veces la línea en cuestión es relativa a una familia de problemas y, en dichos casos, se destacarán a lo largo del texto. Las descripciones son breves y no buscan entrar en los detalles, para los cuales el lector dispondrá de una extensa bibliografía. Se busca simplemente dar a conocer la naturaleza del problema a estudiar, el estado del arte al respecto y los problemas abiertos.

Haremos uso la siguiente tabla de notaciones para la complejidad de los algoritmos:¹

Notación	Definición	Definición con límite
$f(n) = o(g(n))$	$\forall k > 0 \exists n_0 \forall n > n_0 : f(n) < k g(n)$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$
$f(n) = O(g(n))$	$\exists k > 0 \exists n_0 \forall n > n_0 : f(n) \leq k g(n)$	$\limsup_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty$
$f(n) = \Theta(g(n))$	$\exists k_1 > 0 \exists k_2 > 0 \exists n_0 \forall n > n_0 : k_1 g(n) \leq f(n) \leq k_2 g(n)$	$f(n) = O(g(n))$ y $f(n) = \Omega(g(n))$
$f(n) \sim g(n)$	$\forall \varepsilon > 0 \exists n_0 \forall n > n_0 : \left \frac{f(n)}{g(n)} - 1 \right < \varepsilon$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$
$f(n) = \Omega(g(n))$	$\exists k > 0 \exists n_0 \forall n > n_0 : f(n) \geq k g(n)$	$\liminf_{n \rightarrow \infty} \frac{f(n)}{g(n)} > 0$
$f(n) = \omega(g(n))$	$\forall k > 0 \exists n_0 \forall n > n_0 : f(n) > k g(n)$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty$

Cuando las notaciones anteriores aparezcan con el símbolo \sim encima, esto significa que se están omitiendo factores *polilogarítmicos*, esto es, factores de la forma $\log^c n$ con $c > 1$. Existen dos definiciones en uso: algunos autores utilizan $f(n) = \tilde{O}(g(n))$ para indicar $f(n) = O(g(n) \log^c n)$ mientras que otros quieren decir $f(n) = O(g(n) \log^c g(n))$ (algunos autores usan O^* en este caso). Cuando $g(n)$ es de orden polinómico, i.e. $g(n) = O(p(n))$ para algún polinomio p , no hay diferencia, pero sí que la hay cuando se trata de funciones exponenciales. En los algoritmos que plantearemos no será relevante esta diferencia.

También usaremos ciertas notaciones para tipos particulares de complejidad.

Notación	Significado
$\text{poli}(n)$	Tiempo polinómico, $O(n^r)$ para $r \in \mathbb{N}$ suficientemente grande.
$\text{spoli}(n)$	Tiempo superpolinómico, complejidad estrictamente mayor que $O(n^r)$ para cualquier r .
$\text{polilog}(n)$	Tiempo polilogarítmico, $O(\log^c n)$ con $c > 1$.

¹https://en.wikipedia.org/wiki/Big_O_notation#Family_of_Bachmann%E2%80%93Landau_notations.

6 Lógica, conjuntos y funciones

6.1 Búsqueda cuántica

Palabras clave: búsqueda, algoritmo de Grover, estimación de amplitud.

Problema: Dada $f : \{1, \dots, n\} \rightarrow \{0, 1\}$ tal que $f^{-1}(\{1\}) = \{w\}$, encontrar w .

Este problema consiste en buscar un elemento particular de una lista de n elementos. Para ello contamos con la función oráculo f que determina dicho elemento. El problema puede resolverse, en el contexto de la computación clásica, con $\Omega(n)$ consultas (basta comprobar todos los valores de f). Sin embargo, Lov Grover [192] consiguió resolverlo con computación cuántica con una complejidad de $O(\sqrt{n})$ consultas (ver Sección 3.5) que resulta ser óptima [50], lo cual demuestra, además, que los algoritmos cuánticos no tienen por qué poder resolver problemas NP en tiempo polinómico (para ser exactos, $\text{NP} \cap \text{co-NP}$ no se puede resolver con probabilidad uno con una máquina de Turing cuántica en tiempo $o(2n/3)$). Este algoritmo se ha generalizado para la búsqueda de subconjuntos de la lista (caso en que $f^{-1}(\{1\})$ tiene varios elementos) [76], obtener el número de elementos de $f^{-1}(\{1\})$ (conteo) [76, 79], hallar el mínimo global de una función arbitraria [154, 249], obtener la mediana [307], aproximar integrales definidas [315], y calcular puntos fijos [184, 194, 391], entre otros [22, 67, 125, 257, 294, 440]. Existe una generalización del algoritmo de Grover conocida como *estimación de amplitud* [77] que es una parte clave de muchos algoritmos cuánticos modernos, en especial aquellos relacionados con la búsqueda de colisiones y las propiedades de los grafos. Una de las aplicaciones de la amplificación de la amplitud es la mejora en la complejidad de algoritmos para problemas NP-completos de la computación clásica, como por ejemplo el problema 3-SAT clásico [20] para el que se obtiene una aceleración cuadrática. Esto también sucede para otros problemas de satisfacción [93].

Uno de los puntos débiles de la búsqueda de Grover es que requiere una estructura espacial del circuito cuántico que es difícilmente escalable, por lo que resulta interesante estudiar el problema cuando se establecen limitaciones a esta estructura, lo que se conoce como *búsqueda espacial*. Aún así, en grafos suficientemente bien conectados, se puede alcanzar una complejidad de búsqueda $O(\sqrt{n})$ [94, 103, 213, 222, 287, 416, 417].

El algoritmo de Grover (y por extensión la estimación de amplitud) han recibido críticas relativas a su utilidad práctica. Por una parte, la difícil escalabilidad señalada antes, pero por otra, el hecho de que la parte complicada del problema puede estar siendo ocultada en la evaluación del oráculo. Así, en [380] señalan que *"Nuestro hallazgo implica que no hay una aceleración cuántica teórica a priori asociada al algoritmo de Grover. [...] Para un problema dado, si el oráculo es fácil de simular, entonces no se necesita un ordenador cuántico, mientras que si es difícil de simular, la implementación cuántica estará, como veremos, más allá del alcance del hardware previsible"*. Para ello usan un algoritmo clásico inspirado en el algoritmo de Grover (QiGA) que resuelve el problema de búsqueda en un ordenador clásico, asumiendo que el oráculo de evaluación es cuántico para que la comparación sea más justa.

Esta alternativa se suma a otras basadas en paralelización virtual [96] que también ofrecen algoritmos clásicos competitivos así como a las críticas del algoritmo cuántico relativas a la corrección de errores [34].

6.2 Evaluación de fórmulas

Palabras clave: fórmula, lógica booleana.

Problema: *Evaluar una fórmula booleana.*

Una expresión booleana se denomina *fórmula* si cada variable solo se utiliza una vez. Una fórmula corresponde a un circuito sin *fanout*, esto es, el número de entradas de puerta correspondientes a la salida de otra puerta lógica es uno, por lo que tiene la topología de un árbol. La complejidad de consulta de cualquier fórmula con *fanin* (número de entradas de las puertas lógicas) de complejidad $O(1)$ sobre n variables es $\Theta(\sqrt{n})$ [338]. La complejidad cuántica de la evaluación de fórmulas no booleanas también se ha comenzado a estudiar [121], pero aún está en sus primeras fases de desarrollo. La evaluación de fórmulas booleanas se ha generalizado al caso en que las variables de entrada pueden repetirse (*i.e.* la primera capa de el circuito puede incluir fanout) [106], obteniendo una complejidad $O(\min\{n, \sqrt{s}, n^{1/2}g^{1/4}\})$ en consultas, donde n es el número de variables de entrada sin incluir la multiplicidad, s es el número de entradas contando la multiplicidad y g es el número de puertas de la fórmula. Este algoritmo tiene aplicaciones a la verificación del producto de matrices booleanas y a la complejidad de circuitos. Entre los problemas abiertos los autores destacan la búsqueda de mejores cotas inferiores de la complejidad y ponen como ejemplo circuitos basados en planos afines o proyectivos. También indican la necesidad de aumentar la generalidad de los resultados, incluyendo más entradas y salidas para las puertas.

6.3 Reconocimiento de patrones

Palabras clave: patrón, reconocimiento, cadenas, alfabeto, concordancia, coincidencia.

Problema: *Dadas dos cadenas (secuencias de símbolos) T y P de un alfabeto finito de longitudes respectivas n y $m < n$, determinar si P es una subcadena de T .*

Más allá de cadenas, T y P podrían ser *arrays* o tensores d -dimensionales. En tal caso, el problema de reconocimiento de patrones consiste en la localización de P como *array* $m \times m \times \dots \times m$ dentro del *array* T de dimensiones $n \times n \times \dots \times n$ o informar de que no existe tal contenido. La búsqueda no estructurada tiene un límite inferior de complejidad cuántica de consulta $\Omega(\sqrt{n})$ [50], por lo que la complejidad cuántica en el peor de los casos del problema de reconocimiento de patrones es de $\Omega(\sqrt{n} + \sqrt{m})$.

En [331] se describe un algoritmo cuántico que alcanza esta cota. Este algoritmo cuántico funciona mediante el uso del algoritmo de Grover junto con un método de muestreo

determinista. Más recientemente, se demostró [298] que puede lograrse una aceleración cuántica superpolinómica de la complejidad del caso esperado siempre que m crezca más rápidamente que logarítmicamente en n . En concreto, el algoritmo cuántico dado en [298] resuelve el caso esperado con una complejidad $\tilde{O}((n/m)^{d/2} 2^{O(d^{3/2} \sqrt{\log m})})$. Este algoritmo cuántico se construye generalizando el algoritmo de tamiz cuántico de Kuperberg [253] para subgrupos diédrico ocultos (ver Sección 7.6) y problemas de desplazamiento oculto para que pueda operar en d dimensiones y admitir una cierta cantidad de ruido y, finalmente, reducir el problema de forma clásica a una versión ruidosa d -dimensional del problema del desplazamiento oculto. Sin embargo, esta mejora en el caso esperado tiene como contrapartida el hecho de que el algoritmo pueda fallar con alta probabilidad en algunos casos, algo que los autores reconocen que no se puede evitar. También plantean como problema abierto mejorar el término $2^{O(d^{3/2} \sqrt{\log m})}$ de la complejidad, lo cual es de esperar que requiera obtener un algoritmo eficiente para el problema del subgrupo dihédrico oculto. También llaman la atención sobre la necesidad de investigar algoritmos eficientes para el reconocimiento de patrones aproximado.

En [314] se presenta un algoritmo cuántico para reconocimiento de patrones en $\tilde{O}(\sqrt{n})$ con un modelo de entrada diferente, en el que las cadenas se escriben utilizando $n + m$ cúbits en lugar de mediante consultas cuánticas a un oráculo que proporcione los bits individuales.

6.4 Búsqueda en listas ordenadas

Palabras clave: ordenamiento, búsqueda ordenada, lista.

Problema: *Dado un número x y una lista de n números ordenados, encontrar donde se debería insertarse x en la lista para que siga estando ordenada.*

El mejor algoritmo clásico para este problema es la búsqueda binaria que requiere $\log_2 n$ consultas [164]. Sin embargo, se han encontrado algoritmos cuánticos con una complejidad mejor, como por ejemplo el de [109] con una complejidad $0.433 \log_2 n$ en consultas. Este algoritmo hace uso de la relación entre los algoritmos de búsqueda y una representación en términos de polinomios de Laurent y de la programación semidefinida, resaltando así la relación entre la complejidad cuántica de búsqueda y la optimización convexa.

Se sabe además que el menor número de consultas cuánticas posible no puede ser inferior a $\frac{\ln 2}{\pi} \log_2 n$ [110,214] respondiendo así a la pregunta de si un algoritmo de complejidad $o(\log n)$ existe planteada en [109,164]. Se sospecha que esta cota puede ser óptima, así que mejoras en el problema del ordenamiento puntual vendrán de parte de nuevos algoritmos [110]. En [48] se presenta un algoritmo cuántico aleatorio para búsqueda ruidosa con complejidad de consulta esperada inferior a $\frac{1}{3} \log_2 n$. También proporcionan una cota inferior de la complejidad de los algoritmos cuánticos ruidosos de búsqueda.

6.5 Búsqueda de subconjuntos

Palabras clave: subconjuntos, búsqueda, lógica booleana.

Problema: Dada una función $f : D \rightarrow R$ entre conjuntos finitos y una propiedad $P \subset (D \times R)^k$, determinar si existe $((x_1, f(x_1)), \dots, (x_k, f(x_k))) \in P$ y, en tal caso, calcular una instancia.

Existe un algoritmo cuántico [102] basado en [21] que resuelve este problema con una complejidad $O(|D|^{k/(k+1)})$ en consultas cuánticas. En particular, el algoritmo es de utilidad para resolver problema de la suma en subconjuntos ($P = \{(x_1, \dots, x_k), y \in (D \times R)^k : \sum_{j=1}^k x_j = n\}$ para algún n). En [47] se obtuvo un límite inferior para la complejidad de la consulta cuántica.

Hay que destacar que estos algoritmos tienen una complejidad espacial exponencial y utilizan un modelo de memoria cuántica que es actualmente difícil de implementar en *sistemas cuánticos de escala intermedia ruidosos (NISQ)* [443], por lo que es necesario investigar en alternativas que sean más viables en la práctica.

7 Álgebra y teoría de números

7.1 Cálculo de logaritmo discreto

Palabras clave: logaritmo, algoritmo de Shor.

Problema: Dados $a, b, n \in \mathbb{N}$ de n -bits, el objetivo es resolver la ecuación $b \equiv a^s \pmod{n}$ para algún s sabiendo que la ecuación admite una solución $s \in \mathbb{N}$.

Este problema puede resolverse con un ordenador cuántico con complejidad $\text{poli}(n)$ [370] utilizando esencialmente el algoritmo de Shor (ver Sección 3.4), mientras que los algoritmos conocidos para un ordenador clásico requieren $\text{spoli}(n)$. Usando técnicas similares a las de [370], los ordenadores cuánticos pueden resolver el problema del logaritmo discreto sobre curvas elípticas, rompiendo así la criptografía basada en dichas curvas [72,328]. Otras optimizaciones del algoritmo de Shor para el cálculo del logaritmo aparecen en [157,343]. La aceleración cuántica superpolinómica también se ha extendido al problema del logaritmo discreto en semigrupos [37,104].

7.2 Criterios de primalidad

Palabras clave: números primos, primalidad.

Problema: Dado un número de n -bits buscamos decidir si es primo o no.

Los algoritmos clásicos que resuelven este problema son, por una parte, el AKS con una complejidad cuártica [53,97], y el ECPP [302], donde la complejidad heurística tam-

bién es esencialmente cuártica. Por su parte, el algoritmo cuántico más rápido conocido para este problema tiene complejidad $O(n^2(\log n)^3 \log \log n)$ [146]. Este algoritmo está basado en otro de búsqueda cuántica del período que subyace al algoritmo de Shor y que es de complejidad $O(n^3 \log n)$. Un resultado de Harvey y Van Der Hoeven relativo a la complejidad de la multiplicación de enteros [204] podría aplicarse para mejorar complejidad del algoritmo cuántico.

7.3 Verificación del producto de matrices

Palabras clave: matriz, verificación, producto.

Problema: *Dadas tres matrices $n \times n$, A, B, C , decidir si $AB = C$.*

El algoritmo clásico habitual para este problema es de una complejidad $O(n^2)$, mientras que el algoritmo clásico usual para la multiplicación de matrices es de complejidad $O(n^{2.373})$ [19]. En cambio, se conoce un algoritmo cuántico de complejidad $O(n^{1.666})$ [83] para la verificación de productos de matrices. Este algoritmo está basado en los pasos aleatorios cuánticos [385] y siempre devuelve "igual" si $AB = C$. En el caso $AB \neq C$, entonces devuelve "desigual" con probabilidad al menos $2/3$. Tiene una complejidad en el peor caso de $O(n^{5/3})$, mientras que su tiempo de computación esperado es de $O(n^{5/3}/q(W)^{1/3})$ (W es el conjunto de entradas de la matriz para las cuales la identidad no se satisface y $q(W)$ una función que depende de W y de n), con una complejidad espacial de $O(n)$.

Entre los problemas abiertos [83], está determinar si la complejidad temporal del algoritmo aumenta si la complejidad del espacio está acotada. En particular, si se puede probar una compensación espacio-temporal para el problema de verificación similar a la compensación para el cálculo de productos matriciales [245]. En la actualidad no se ha demostrado la existencia de compensaciones espacio-temporales para ningún problema de decisión.

7.4 Problemas de conmutatividad

Palabras clave: matriz, conmutatividad, producto, grupo conmutativo, álgebra conmutativa.

El problema general consisten en determinar *si dados los k generadores de un grupo, éste es conmutativo*. En el caso particular de matrices, podemos plantear el problema como *dadas k matrices $n \times n$, $M_j, j = 1, \dots, k$, comprobar si conmutan dos a dos*. Disponemos además de un oráculo que nos determina el producto del grupo. El algoritmo clásico más utilizado requiere $O(k)$ consultas [322]. Por su parte, en el caso cuántico se ha demostrado que la complejidad de consulta se puede reducir a $\tilde{O}(k^{2/3})$ [283].

En el caso de las matrices, el problema se plantea a través de un oráculo tal que, dados enteros $i, j \in \{1, 2, \dots, n\}$, y $M \in \{M_1, \dots, M_k\}$ el oráculo devuelve la entrada ij

de la matriz M matriz. Con computación clásica, este problema es de una complejidad $\Omega(kn^2)$, pero se ha comprobado que un ordenador cuántico puede resolver este problema en $O(k^{4/5}n^{9/5})$ consultas [217].

En ambos casos los algoritmos desarrollados se basan en recorridos aleatorios cuánticos. Finalmente, en [123] experimentan con un algoritmo de computación cuántica adiabática (Sección 9.10) para determinar si un álgebra es conmutativa o no.

7.5 Rango de una matriz

Palabras clave: matriz, rango.

Problema: *Dada una matriz, determinar su rango.*

El problema se plantea con un oráculo que devuelve las entradas (enteras) de una matriz A de dimensiones $n \times m$. Con un algoritmo clásico el problema se resuelve con una complejidad $O(mn)$. Se conoce un algoritmo cuántico [46] basado en la equivalencia entre los programas de lapso (*span programs*) y los algoritmos de consulta cuántica [337] que puede utilizar menos consultas en el caso en el que se conozca con antelación que el rango de la matriz es menor que r . En concreto, este algoritmo es de complejidad $O(\sqrt{r(n-r+1)}LT)$, donde L es la media cuadrática de los recíprocos de los r mayores valores singulares de A y T es un factor que depende de la dispersión de la matriz. Para una matriz arbitraria A , $T = O(\sqrt{nm})$. Si A tiene a lo sumo k entradas no nulas en cualquier fila o columna, entonces $T = O(k \log(n+m))$.

En particular, se puede usar este algoritmo para determinar si una matriz cuadrada es singular, lo que se conoce como el *problema del determinante*. Para una matriz arbitraria A la complejidad cuántica de consulta del problema del determinante no es inferior a la complejidad de consulta clásica [148]. Sin embargo, es un problema abierto determinar si bajo ciertas hipótesis (matriz dispersa, valores singulares grandes...) pueda haber una ventaja cuántica para este problema [148].

7.6 Subgrupo oculto abeliano

Palabras clave: subgrupo oculto, abeliano, conmutativo.

Problema: *Dado un grupo abeliano finitamente generado G , un subgrupo H de G tal que G/H es finito y una función f definida sobre G tal que $f(g_1) = f(g_2)$ si y sólo si $g_1 - g_2 \in H$ (es decir, f pasa al cociente G/H), encontrar un conjunto de generadores de H a través de consultas a f .*

Este problema se puede solucionar con una complejidad $\Omega(|G|)$ con algoritmos clásicos. Sin embargo, se conoce un algoritmo cuántico que lo resuelve en $O(\log |G|)$ [72]. Este algoritmo, basado en la Transformada de Fourier Cuántica (Sección 3.1), generaliza muchos algoritmos cuánticos como casos especiales [312], como el algoritmo de Simon [374], que fue la inspiración del algoritmo de Shor para encontrar el periodo que a su vez que

forma el núcleo de los algoritmos de factorización y del cálculo del logaritmo discreto. El algoritmo para el cálculo de subgrupos abelianos ocultos también es esencial en el estudio de problemas como el estudio de la ecuación de Pell, el cálculo de ideales principales, el cálculo grupos de unidades (Sección 7.8) o el cálculo de grupos de clase. En ciertos casos, el problema del subgrupo oculto abeliano se puede resolver con una única consulta [45]. En el caso de la búsqueda del período s de un grupo, se suele asumir que $f(x) \neq f(y)$ si $x - y \neq s$, pero existen alternativas sin esta restricción [198]. También se ha generalizado el algoritmo de [198] para el caso en el que sólo se conozcan algunas cifras de los valores de f [372].

Los algoritmos para obtener el subgrupo oculto abeliano tienen además aplicaciones a la compresión cuántica de información [267]. También existen versiones deterministas del algoritmo [428] y otras para grupos continuos [36].

Muchos de los problemas abiertos en esta área consisten en extender los resultados obtenidos al caso de grupos no conmutativos.

7.7 Subgrupo oculto no abeliano

Palabras clave: subgrupo no abeliano, subgrupo no conmutativo.

Problema: *Dado un grupo no abeliano finitamente generado G , un subgrupo H de G tal que G/H es finito y una función f definida sobre G tal que $f(g_1) = f(g_2)$ si y sólo si $g_1 \in g_2 H$ (es decir, f pasa al cociente G/H), encontrar un conjunto de generadores de H a través de consultas a f .*

Este problema, que generaliza al problema del grupo oculto abeliano, es de una dificultad mayor. En el caso de ordenadores clásicos este problema se ha solucionado con algoritmos con una complejidad temporal $\Omega(|G|)$, pero se conoce un algoritmo cuántico que lo resuelve en $O(\log |G|)$ [160,200]. Sin embargo, este algoritmo no es eficiente ya que, en general, la complejidad de consulta necesaria para procesar los estados cuánticos puede ser exponencial [160]. En el caso de ciertos grupos no abelianos (producto semidirecto de ciertos grupos cíclicos, determinados grupos resolubles, etc.) sí que se conocen algunos algoritmos eficientes [35,52,98,100,126,140,176,180,216,218–220,277,301,342,398]. Dos casos particularmente interesantes son los de los grupos de simetrías, cuya solución resolvería el problema del isomorfismo de grafos; y diédricos, que permitirían solucionar ciertos problemas de retículos [334].

Salvo casos concretos, no se conocen algoritmos polinómicos para resolver el problema del grupo oculto no abeliano en el caso de grupos diédricos [341], pero sí que existen algoritmos de complejidad temporal $2^{O(\sqrt{\log n})}$ y complejidad espacial polinómica para D_n [335]. Las principales líneas de investigación relativas a este problema consisten en ampliar la familia de grupos no abelianos para los cuales se dispone de algoritmos eficientes y determinar si es posible, en general, encontrar este tipo de algoritmos.

7.8 Grupos de unidades

Palabras clave: grupo, unidad.

Problema: *Encontrar un conjunto de generadores de un grupo de unidades.*

El cuerpo $\mathbb{Q}(\theta)$ se dice que es de *grado* d si el polinomio de menor grado del que θ es una raíz tiene grado d . El conjunto O de elementos de $\mathbb{Q}(\theta)$ que son raíces de polinomios mónicos en $\mathbb{Z}[x]$ forma un anillo, llamado *anillo de enteros* de $\mathbb{Q}(\theta)$. El conjunto de unidades (elementos invertibles) del anillo O forman un grupo denominado *grupo de unidades* de O y denotado por O^* . Dado $\mathbb{Q}(\theta)$ de grado fijo, un ordenador cuántico puede encontrar en tiempo polinómico un conjunto de generadores para O^* dada una descripción de θ [199, 355]. Estos algoritmos se basan en el problema del subgrupo oculto abeliano tomando por grupo el grupo aditivo de números reales. En la actualidad no se conoce ningún algoritmo clásico de tiempo polinómico para este problema. En estudios recientes se demuestra como lograr una mejora polinómica en el grado [66, 156].

Adicionalmente, se han optimizado este tipo de algoritmos para reducir el número de cúbits físicos necesarios para la implementación en el caso concreto de cuerpos ciclotómicos [39].

7.9 Desplazamiento oculto

Palabras clave: desplazamiento.

Problema: *Dada una función conocida $g : \mathbb{Z}_n \rightarrow \mathbb{C}$ y un oráculo para una función $f : \mathbb{Z}_n \rightarrow \mathbb{C}$ tal que $f(x) = g(x + s)$ para todo $x \in \mathbb{Z}_n$ y cierto $s \in \mathbb{Z}_n$, encontrar s .*

En la actualidad se desconocen algoritmos clásicos de complejidad $\text{polilog}(n)$ para este problema, pero utilizando el algoritmo de Grover podemos llegar a la conclusión de que al menos \sqrt{n} consultas son necesarias. Sin embargo, ciertos casos concretos se pueden resolver con un ordenador cuántico con complejidad $O(1)$, por ejemplo en el caso en que f sea un carácter multiplicativo de un anillo o cuerpo finito [134], como puede ser en el caso del símbolo de Legendre $\left(\frac{x}{p}\right)$, que es un carácter de un cuerpo finito de orden p con p primo [132, 133].

En el caso de funciones booleanas aleatorias $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ se ha comprobado que la complejidad del caso medio es $O(n)$ [181], mientras que la clásica es $\Omega(2^{n/2})$. Más información al respecto a este problema así como su relación con la criptografía puede encontrarse en [147].

7.10 Criptografía

Palabras clave: descodificación, códigos correctores de errores, criptografía, criptoanálisis.

La relación entre la computación cuántica y la criptografía comienza con el algoritmo de Shor para la factorización de enteros [369, 370] que abrió la puerta a poder romper los sistemas criptográficos clásicos, como el RSA y Diffie-Hellman, así como variantes de estos basados en curvas elípticas [72, 328]. Este hecho ha derivado en la fundación de la *criptografía poscuántica*, en la que se busca algoritmos de encriptación clásicos que sean resistentes a los ataques cuánticos. Los algoritmos cuánticos ofrecen una vía para acelerar la descodificación de códigos convolucionales [190] y códigos simplex [40], pero la mayoría de la investigación en algoritmos cuánticos se centra en determinar qué algoritmos clásicos son resistentes y cuales no. Por una parte tenemos el desarrollo de algoritmos que utilizan consultas de superposición cuántica (como el algoritmo de Grover o el de Simon) para obtener la clave de encriptación [231, 232, 254, 255, 346, 348]. Muchos de estos algoritmos explotan la simetría de ciertas claves de encriptación clásicas.

Por otra parte están los algoritmos que consiguen una mejora polinómica sobre ataques clásicos a través de la computación cuántica [26, 54, 78, 173, 189, 230, 257]. También se ha comprobado que usar isogenias entre curvas elípticas como sistema de codificación es un mecanismo potencialmente frágil frente a ataques cuánticos [105].

En la actualidad se sigue intentando entender las capacidades de los algoritmos cuánticos para romper los sistemas de encriptación clásicos de modo que se pueda encontrar sistemas clásicos fiables que puedan sustituir a aquellos actuales que sean frágiles. Algunos sistemas, como el AES, establecido como estándar por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) en 2001, parece resistente a los ataques cuánticos conocidos [73].

Finalmente, también se están desarrollando algoritmos de encriptación cuánticos (distribución de claves cuánticas, ver por ejemplo [282]), pero se espera que su uso sea reducido (limitado a gobiernos y ciertas instituciones) debido a que en la actualidad no es fácil acceder a un ordenador cuántico.

7.11 Obtención de autovalores

Palabras clave: autovalores, espectro, computación híbrida

Problema: Dado un hamiltoniano H , calcular el autovector asociado a su menor autovalor.

El algoritmo Variational Quantum Eigensolver (VQE) permite calcular el autovector asociado al menor autovalor del hamiltoniano, minimizando el valor esperado. Para buscar dicho estado, se propone una representación parametrizada del estado (o *ansatz*) que permita recorrer un subespacio del espacio de Hilbert. La parte de minimización es llevada a cabo con computación clásica, por lo que se trata de un algoritmo de computación híbrida. El algoritmo VQE sufre de algunas dificultades relacionadas con usar métodos de optimización basados en el cálculo de gradientes, como la incapacidad de evadir los numerosos mínimos locales que presenta el espacio de optimización y, por ende, de llegar al estado fundamental, hecho que se ve magnificado por la existencia de "barren pla-

teaus”, zonas donde los gradientes se vuelven nulos [27,161,252]. Como posible solución a este problema, se propone el algoritmo evolutivo Quantum Particle Swarm Optimization (QPSO) [382].

El algoritmo VQE y sus variaciones han sido aplicados al estudio de estructura electrónica de materiales además de a otros problemas de mecánica cuántica con similares problemas de escalado. Entre ellos cabe destacar algunos de física nuclear [143,289] y problemas de estructura nuclear [243,344], física de altas energías [41,42,44], espectroscopía vibracional y vibrónica [221,278,352], predicciones de propiedades de reacciones fotoquímicas [316], sistemas periódicos [431], resolución de ecuaciones de Schrödinger no lineales [281], y cálculo de estados cuánticos de un agujero negro Schwarzschild-de Sitter o cosmología Kantowski-Sachs [227].

8 Geometría y Topología

8.1 Análisis cuántico de datos topológicos

Palabras clave: datos topológicos, invariante.

El *análisis topológico de datos* (ATD) consiste en el análisis de conjuntos de datos utilizando técnicas topológicas. Es particularmente útil para la extracción de información de conjuntos de datos que son de dimensión alta, incompletos o ruidosos. Las técnicas del ATD buscan obtener la *forma* de los mismos. La herramienta principal es la *homología persistente*, una adaptación de la homología a datos de nubes de puntos.

En el caso clásico, obtener la homología (en particular los números de Betti) de un conjunto de n datos presenta una complejidad $O(2^{2n})$. Sin embargo, se conoce un algoritmo cuántico basado en el algoritmo de Grover que calcula los números de Betti y los autovectores de los núcleos del laplaciano combinatorio en $O(n^5)$ [273], lo cual supone una mejora exponencial de la complejidad. Esto es posible gracias a que un ordenador cuántico puede almacenar en n cúbits (asociados a n vértices de un grafo) la información combinatoria de los mismos (que sería del orden de 2^n). Este algoritmo ha sido recientemente generalizado para detectar los cambios en la homología que se producen al variar la resolución (homología persistente) [24,206]. En [70] se describe un algoritmo para el cálculo de los números de Betti que funciona bien para complejos simpliciales dispersos, aunque la complejidad para el cálculo exacto es exponencial en el peor de los casos.

Existen indicios de que la mejora exponencial de estos algoritmos frente a los clásicos es genuina (es decir, no existen algoritmos clásicos exponencialmente mejores que los que se conocen) [197], pero este es todavía un problema abierto y trabajos recientes han mostrado que la mejora es posible en ciertas situaciones [28]. En cualquier caso, se esperan mejoras tanto para los algoritmos cuánticos como clásicos en un futuro próximo.

8.2 Invariantes de nudos

Palabras clave: invariante, nudo, trenza, polinomio de Jones.

El entrelazamiento cuántico puede interpretarse en términos de operadores de trenzas, lo que crea un puente natural entre la computación cuántica y la topología [237]. De hecho, Edward Witten demostró que el polinomio de Jones (un polinomio invariante de nudos) se puede entender usando herramientas de teorías cuánticas de campos topológicas (TQFTs) [414]. Es en este contexto que se demostró que el problema de aproximar (usando una aproximación aditiva [74]) el polinomio de Jones de un determinado grupo de trenzas es un problema BQP-completo [174, 175]. Este resultado fue posteriormente reformulado de manera más sencilla (sin recurrir a las TQFTs) y extendido en [5, 8]. Esta teoría se llevó un paso más allá en [415], donde los autores obtuvieron un algoritmo cuántico para estimar el polinomio HOMFLY, del cual el polinomio de Jones es un caso concreto.

También se ha comprobado que los ordenadores cuánticos pueden estimar en tiempo polinómico una cierta aproximación aditiva del polinomio de Tutte para grafos planos [6] y que el problema de encontrar una cierta aproximación aditiva del polinomio de Jones de la clausura de traza de una trenza es DQC1-completo [371].

En general, hay una idea clara de la existencia de una ventaja cuántica a la hora de calcular este tipo de invariantes, pero precisar en qué consiste y extenderla a otros invariantes es un campo de investigación abierto.

8.3 Invariantes de variedades de dimensión tres

Palabras clave: invariante de Turaev-Viro, variedad.

El *invariante de Turaev-Viro* es una función invariante por homeomorfismos que asigna números reales a variedades topológicas de dimensión tres. Dada una variedad diferencial de dimensión tres, a través de una división de Heegaard, un ordenador cuántico puede encontrar eficientemente una cierta aproximación aditiva de su invariante de Turaev-Viro y esta aproximación es BQP-completa [14]. Por otra parte, el *invariante de Witten-Reshitikhin-Turaev* (WRT) es tal que, al cuadrado, se obtiene el invariante de Turaev-Viro. En [179] se aporta un algoritmo cuántico de complejidad polinómica para aproximar el WRT de una variedad dada a través de una presentación quirúrgica, pero se desconoce si la aproximación lograda es BQP-completa.

Recientemente ha habido algún progreso en este campo. Por ejemplo, en [84], se demuestra que la complejidad del problema de calcular los invariantes de Turaev-Viro depende del número del invariante en cuestión. Por otra parte, en [284] ofrecen un algoritmo de tiempo polinómico para calcular los invariantes de Turaev-Viro $TV_{4,q}$ de variedades de dimensión tres con un primer número de Betti acotado. Los autores también aportan experimentos computacionales que permiten comprobar la capacidad del invariante de distinguir 3-variedades y obtener el tiempo de ejecución y compararlo con el de otros

métodos.

8.4 Determinación de propiedades de grafos

Palabras clave: grafo, ciclo, árbol, matriz de adyacencia, camino.

A la hora de trabajar con grafos en computación cuántica existen varios modelos de algoritmos. Por una parte están aquellos que cuentan con un oráculo que, dados dos vértices, nos dice si existe una arista entre ellos o no, esto es lo que se conoce como *modelo de matriz de adyacencia*. Por otra parte existe el *modelo de lista de adyacencia*, en el que se nos da acceso a un oráculo que, cuando se consulta la etiqueta de un vértice x y un número natural j devuelve como resultado la etiqueta del vecino número j del vértice x , si este existe, y 0 en caso contrario. Estos modelos son propicios para diferentes tipos de algoritmos que detallamos a continuación.

Para el caso del modelo de matriz de adyacencia, se ha demostrado [153] para los problemas de encontrar un árbol de expansión mínimo en grafos ponderados y el de decidir la conectividad para grafos dirigidos y no dirigidos una complejidad cuántica de consulta $\Theta(n^{3/2})$ donde n es el número de vértices del grafo. Por su parte, los problemas de decidir si un grafo es bipartito, detectar ciclos y decidir si se puede llegar a un vértice dado desde otro (problema de *conectividad st*) se puede lograr utilizando una serie de consultas y puertas cuánticas de complejidad $\tilde{O}(n^{3/2})$ en tiempo y $O(\log n)$ en espacio [86]. Estos algoritmos pueden contrastarse con los algoritmos clásicos que, debido a la *conjetura de Aanderaa-Karp-Rosenberg*, se sospecha que tienen una complejidad de consulta clásica $\Omega(n^2)$. Esta conjetura afirma que “*toda propiedad gráfica monótona no trivial para grafos de n vértices es evasiva*”, donde propiedad se dice *evasiva* si determinar si un grafo dado tiene esta propiedad a veces requiere $n(n-1)/2$ consultas (todas las posibles) y una propiedad se dice *monótona* si se mantiene cuando se añaden aristas (e.g. conectividad, existencia de ciclos, etc). Esta conjetura sigue abierta, aunque varias propiedades especiales de grafos han demostrado ser evasivas para todo n . La conjetura ha sido resuelta para el caso en que n es una potencia prima [229] y para grafos bipartitos [427].

Trabajos recientes en la conectividad *st*, la detección de ciclos y otros problemas comunes ponen su enfoque en obtener algoritmos eficientes en espacio. Por ejemplo, en [138] se obtienen algoritmos para estos problemas con una complejidad logarítmica.

Otro problema computacional habitual consiste en encontrar un subgrafo H de un grafo dado G . El caso más sencillo de este encontrar un triángulo, problema para el cual existe un algoritmo cuántico de complejidad $O(n^{5/4})$ [90]. Para el problema general de encontrar subgrafos, un ordenador cuántico puede encontrar un subgrafo arbitrario de k vértices, m aristas y grado mínimo $d \geq 1$ utilizando $O(n^{2-2/k-t})$ consultas donde

$$t = \text{máx} \left\{ \frac{k^2 - 2(m+1)}{k(k+1)(m+1)}, \frac{2k - d - 3}{k(d+1)(m-d+2)} \right\}$$

[259]. En el caso de grafos dispersos se conocen algoritmos que mejoran la complejidad para algunos de los problemas anteriores (e.g. [107]).

El modelo de lista de adyacencia se ha utilizado también para el problema del árbol de expansión mínimo, obteniendo una complejidad de consulta cuántica $\Theta(\sqrt{nm})$ donde n es el número de vértices y m el número de aristas [153]. Por su parte, decidir la conectividad de un grafo con este modelo tiene una complejidad de consulta cuántica $\Theta(n)$ en el caso no dirigido y $O(\sqrt{nm \log n})$ en el caso dirigido y calcular el camino de menor peso desde un vértice determinado a todos los demás vértices de un grafo ponderado tiene una complejidad de consulta cuántica $O(\sqrt{nm} \log^2 n)$. Por otra parte, en [86] se proponen algoritmos cuánticos para estudiar conectividad, decidir la bipartición y decidir si un grafo es un bosque de complejidad temporal $\tilde{O}(n\sqrt{d})$ y $O(\log n)$ en espacio donde d es el grado máximo de cualquier vértice del grafo.

Los algoritmos cuánticos parecen ser especialmente propicios para determinar las propiedades combinatorias de grafos, por lo que es de esperar mejoras en la complejidad de los algoritmos cuánticos para determinarlas. Es importante prestar atención a la complejidad espacial y de consulta de estos algoritmos para que puedan ser implementados en un futuro.

9 Estadística, optimización y simulación numérica

9.1 Diferencia estadística

Palabras clave: distribución, probabilidad, diferencia estadística, norma L^1 .

Problema: *Dados dos oráculos A y B que implementan sendas variables aleatorias de dominio $\{1, \dots, t\}$ y de rango $\{1, \dots, n\}$, aproximar con precisión constante la distancia L^1 entre las distribuciones de probabilidad de A y B .*

Los algoritmos clásicos resuelven este problema con una complejidad que esencialmente es lineal en n . Sin embargo, un ordenador cuántico puede conseguirlo utilizando $O(\sqrt{n})$ consultas [80]. La uniformidad aproximada y la ortogonalidad de las distribuciones también se pueden decidir en un ordenador cuántico con complejidad $O(n^{1/3})$. La herramienta principal de esta solución es el algoritmo de recuento cuántico de [79] que a su vez se basa en los algoritmos de Grover y Shor. En [296] mejoran este algoritmo usando un método de Montecarlo cuántico que además tiene aplicaciones a muchos otros problemas. Recientemente [261], se han logrado nuevas mejoras y simplificaciones en este tipo de algoritmos, incluidos aquellos para la distancia en L^2 .

Entre las líneas abiertas, se espera poder mejorar las cotas de la complejidad de este problema y poder aplicar este tipo de métodos a otros problemas de distribuciones estadísticas, tales como la estimación de diversas medidas de entropía [400].

9.2 Flujos en redes

Palabras clave: red de flujo, optimización.

Problema: Dada una red con una fuente y un sumidero, encontrar un flujo de valor máximo.

Una *red de flujo* es un grafo dirigido cuyas aristas son etiquetadas con números (no negativos) que indican su capacidad de carga y con dos vértices destacados, una fuente y un sumidero de modo que cualquier otro vértice se haya en un camino que empieza en la fuente y termina en el sumidero [124,247]. Un *flujo* en un es una asignación de pesos a las aristas de modo que ningún peso supere la capacidad de esa arista y, para cada vértice que no sea la fuente o el sumidero, el flujo total de entrada es igual al flujo total de salida. El *valor del flujo* es la diferencia entre el flujo de salida y de entrada de la fuente.

Para una red con n vértices, m aristas y capacidades enteras de magnitud máxima U existe un algoritmo cuántico basado en el algoritmo de búsqueda de Grover para calcular el valor del flujo máximo de complejidad $O(\min\{n^{7/6} \sqrt{m} U^{1/3}, \sqrt{nUm}\} \log n)$ [23]. En comparación, el algoritmo clásico más conocido [187] tiene un tiempo de ejecución de $O(\min\{m^{1/2}, n^{2/3}\} m \log \frac{n^2}{m} \log u_{\max})$, donde u_{\max} es un parámetro inherente [434].

Posteriormente se han obtenido algoritmos con una complejidad mejor de $O(n^{5/2})$ [434], pero aún se desconoce cual puede ser la complejidad óptima (aunque existen cotas).

9.3 Temple simulado (Simulated Annealing, SA)

Palabras clave: optimización, temple simulado, simulated annealing.

El temple simulado es una estrategia heurística clásica para aproximar el mínimo global de una función dada. Se utiliza a menudo cuando el espacio de búsqueda es discreto, muy grande o con un gran número de mínimos locales. El proceso se basa en un camino aleatorio a través del espacio de búsqueda para el cual las probabilidades del proceso estocástico varían dependiendo de si el cambio de estado es favorable a los objetivos de la optimización, a menudo reduciendo las probabilidades de cambio a medida que avanza el tiempo (*temple simulado adaptativo*).

Existen varios modelos algorítmicos para implementar esta estrategia. El modelo Monte-Carlo de cadenas de Markov (Markov chain Monte-Carlo, MCMC), habitual en la física estadística, se basa en una cadena de Markov que codifica un recorrido por el espacio de posibles soluciones del problema a través de una serie de "reglas de transición" (matrices) M_1, M_2, \dots, M_n que varían lentamente en el sentido de que sus distribuciones límite $\pi_1, \pi_2, \dots, \pi_n$ satisfacen $|\pi_{t+1} - \pi_t| \leq \epsilon$ para algún ϵ pequeño. Estas distribuciones pueden considerarse como distribuciones térmicas en temperaturas sucesivamente más bajas (de ahí el nombre *temple simulado*).

Sea δ_k es la diferencia entre el mayor y el segundo mayor valor propio de M_k y $\delta = \min\{\delta_k : k = 1, \dots, n\}$. El tiempo de ejecución del algoritmo (clásico) es proporcional a

$1/\delta$ [18], pero con ayuda de la computación cuántica este tiempo se puede reducir a uno proporcional a $1/\sqrt{\delta}$ [379]. Se ha demostrado además que, usando caminos cuánticos se puede aumentar la eficiencia de este algoritmo [296].

9.4 Temple cuántico (Quantum Annealing, QA)

Palabras clave: optimización, QA, temple cuántico, quantum annealing.

El temple cuántico (QA) es un proceso de optimización para encontrar el mínimo global de una función objetivo sobre un conjunto de estados posible a través de un proceso que utiliza fluctuaciones cuánticas [303]. Al igual que el temple simulado, se utiliza principalmente para problemas en los que el espacio de búsqueda es discreto (problemas de optimización combinatoria) con muchos mínimos locales.

El temple cuántico parte de una superposición cuántica de todos los estados posibles (estados candidatos) con pesos iguales. A continuación, el sistema evoluciona siguiendo la ecuación de Schrödinger. Las amplitudes de todos los estados candidatos van cambiando con el paso del tiempo y la naturaleza cuántica de los estados permite que tenga lugar el efecto túnel, por el cual un estado puede convertirse en otro pasando a través de una barrera de potencial. Si la tasa de cambio del campo es lo suficientemente lenta, el sistema permanecerá cerca del estado fundamental (el de menor energía) del hamiltoniano en cada instante, mientras que si es rápida, el sistema puede abandonar el estado fundamental temporalmente, con una mayor probabilidad de acabar en el estado fundamental del hamiltoniano final del problema, como ocurre en el temple simulado.

El temple cuántico puede compararse con el temple simulado, cuyo parámetro de temperatura desempeña un papel similar a la intensidad del campo del efecto túnel en QA. En el temple simulado, la temperatura determina la probabilidad de pasar a un estado de mayor energía a partir de un único estado actual. En el temple cuántico, la intensidad del campo determina la probabilidad de cambiar las amplitudes de todos los estados en paralelo. En pocas palabras, el temple cuántico lleva a cabo de forma física (y por tanto sin necesidad de intervención) un proceso estocástico análogo al que simula el temple simulado. Esto parece ofrecer una ventaja al temple cuántico, lo cual se ha visto confirmado tanto por estudios teóricos como pruebas numéricas [207, 303, 349, 423].

A día de hoy ya se ha implementado este tipo de algoritmos en ordenadores cuánticos, como el ordenador cuántico adiabático D-Wave [17, 248]. Estas pruebas también muestran una mejora frente al temple simulado.

9.5 Algoritmo de Optimización Cuántica Aproximada (QAOA)

Palabras clave: optimización, QAOA.

Muchos problemas de optimización combinatoria son NP-completos. Hay también resultados que demuestran que aproximar la solución de algunos de estos problemas por

debajo de un error dado es NP-complejo. En [162], se desarrolló una técnica llamada Algoritmo de Optimización Cuántica Aproximada (QAOA) (ver Sección 3.6.4) que permite encontrar soluciones aproximadas de problemas de optimización combinatoria. Este algoritmo puede entenderse como una versión discretizada del temple cuántico. Si H denota el hamiltoniano dependiente del tiempo del problema a considerar, se divide el intervalo de integración en segmentos muy pequeños. Su evolución temporal puede aproximarse asumiendo que H es constante en cada uno de dichos intervalos (como en la definición de la integral de Riemann). De este modo, el estado del sistema puede aproximarse por un producto de funciones exponenciales complejas que determinan operadores unitarios y que son los que se implementarán en el ordenador cuántico [162].

Actualmente, la potencia de QAOA en relación con la computación clásica y a estrategias cuánticas alternativas es un área muy activa de investigación [38, 264, 403, 426] (ver el fenómeno de la *descuantización* en la Sección 4.2). Resumimos a continuación el estado del arte.

Para una profundidad $p = 1$ (p indica el número de parámetros a determinar en el algoritmo) se ha demostrado que no existe una forma eficiente de simular QAOA de forma clásica [167], lo cual no quiere decir que no existan algoritmos alternativos que resuelvan de forma eficiente los mismos problemas. De hecho, la eficiencia relativa de QAOA con respecto a otros algoritmos depende en gran medida del problema estudiado [411]. Por ejemplo, el problema de corte máximo de un grafo requiere de cientos de cúbits para que el algoritmo QAOA pueda resolverlo de forma competitiva frente a uno clásico [195]. Esta dificultad ha llevado al estudio de modificaciones en la aplicación del algoritmo para resolver este problema en máquinas con un número bajo de cúbits [444, 445].

9.6 Ajuste de mínimos cuadrados

Palabras clave: optimización, mínimos cuadrados.

Problema: *Dado un conjunto de datos, ajustar los parámetros de una determinada curva en el sentido de mínimos cuadrados.*

La idea fundamental es transformar el problema de mínimos cuadrados en un sistema lineal a través de las ecuaciones y emplear algoritmos QLSA (Quantum Lineal Solver Algorithm) del tipo HHL (véase sección 3.3) para la resolución del sistema lineal resultante. Véase, por ejemplo, [407], y los trabajos posteriores que citan a este trabajo. La ventaja cuántica reside, por lo tanto, en la mejora que los algoritmos QLSA presentan frente los algoritmos clásicos.

9.7 Machine learning y análisis de datos

Palabras clave: aprendizaje automático, clustering, redes neuronales.

El aprendizaje automático, o *machine learning*, abarca una amplia variedad de proble-

mas que pueden ser atacados por un gran conjunto de técnicas algorítmicas. En [238, 239, 273–275, 333, 360, 441, 442] pueden verse algoritmos cuánticos para resolver sistemas lineales [202] que se aplican para acelerar la búsqueda de *clusters*, análisis de componentes principales, clasificación binaria, entrenamiento de redes neuronales y diversas formas de regresión, siempre que los datos cumplan determinadas condiciones (véase también [184] para las mejoras posteriores de análisis cuántico de componentes principales). Sin embargo, una serie de algoritmos de aprendizaje automático basados en sistemas lineales han sido “descuántizados”. En concreto, Tang demostró en [386, 387] que en el caso de problemas de sistemas de recomendación y en el análisis de componentes principales, resueltos por los algoritmos cuánticos en [238, 333], estos problemas se pueden resolver también en tiempo polinómico con algoritmos clásicos aleatorios. Un método de *clustering* no basado en los sistemas lineales de [202] se da en [408]. Los artículos [3, 25, 49, 129, 310, 329] exploran el uso de técnicas de optimización adiabática para acelerar el entrenamiento de clasificadores.

Los principales tipos de algoritmos encontrados son implementaciones cuánticas de algoritmos clásicos de aprendizaje automático, como las máquinas de soporte vectorial o el modelo de los k -vecinos más cercanos, y algoritmos clásicos de aprendizaje profundo, como las redes neuronales cuánticas. Una de las aplicaciones más relevantes en el campo del aprendizaje automático es la clasificación de imágenes. A pesar de que los resultados son prometedores, el aprendizaje automático cuántico está lejos de alcanzar su máximo potencial. En [177] se hace una revisión bastante completa de estos métodos, destacando los relacionados con las redes neuronales. En este contexto, una red neuronal cuántica (QNN), al igual que una red neuronal clásica, puede representar datos etiquetados, clásicos o cuánticos. El conjunto de parámetros se asocia a una serie de matrices unitarias $\exp(i\theta\sigma)$, donde σ es una matriz de Pauli generalizada [169]. Algunos tipos específicos de estos métodos serían los siguientes:

- ◊ *máquinas de Boltzmann cuánticas*: Estas máquinas emulan a una máquina de Boltzmann clásica usando hamiltonianos tipo Ising [446]. En [409] se propone un método para entrenar máquinas de Boltzmann manipulando estados cuánticos coherentes con amplitudes proporcionales a los pesos de Boltzmann. Se puede obtener una aceleración polinómica aplicando la búsqueda de Grover y técnicas afines, como la amplificación de la amplitud, a aquellas subrutinas propicias para los algoritmos clásicos de aprendizaje automático más avanzados. Véase, por ejemplo [12, 13, 145, 233, 323].
- ◊ Utilizando *redes de convolución gráfica híbridas (QGCNN)*, se ha propuesto el diseño y la implementación de algoritmos híbridos de aprendizaje profundo que, en comparación con las redes neuronales convolucionales cuánticas, el perceptrón multicapa clásico (MLP) y las redes de convolución clásicas, pueden lograr un mejor rendimiento [395]. Se trata de un sistema cuántico donde cada nodo del grafo está en un espacio de Hilbert H_v , formando el conjunto un espacio de Hilbert $H_V = \bigotimes_{v \in V} H_v$.
- ◊ *Circuitos cuánticos de profundidad variable (vVQC)*: Los circuitos cuánticos variacionales o parametrizados son algoritmos cuánticos que dependen de parámetros li-

bres. Estos circuitos variacionales se entrenan mediante un algoritmo de optimización clásico que realiza consultas al dispositivo cuántico [215].

- ◇ *Computación cuántica de reservorio (QRC)*: Este método utiliza un sistema dinámico para llevar a cabo tareas de procesamiento de información temporal [383]. El objetivo principal de esta tarea, llamada predicción, es crear una función que transforme una secuencia de entrada (series temporales) en una secuencia de salida objetivo para la predicción de series temporales y la clasificación de patrones.
- ◇ *Clasificador cuántico multiclase (QMCC)*: En [95] se propone un circuito variacional diseñado para clasificar el conjunto de datos con cuatro características.
- ◇ *Máquinas de soporte vectorial con un estimador de núcleo cuántico (QSVM-Kernel)*: El algoritmo SVM localiza eventos de datos en un espacio de características de mayor dimensión, donde mide la similitud entre dos eventos de datos utilizando una "entrada de núcleo" [420]. La máquina de soporte vectorial cuántica QSVM y el estimador de núcleo cuántico (QSVM-Kernel) explotan el espacio de estados cuánticos como un espacio de características para calcular eficientemente las entradas de núcleo. En [271] se utiliza la estimación de núcleo cuántico para implementar un clasificador de vectores de soporte que resuelva un problema de aprendizaje que es tan difícil como el logaritmo discreto (ver Sección 7.1). Varias revisiones recientes se pueden consultar en los artículos [4, 65, 359] y el libro [412].
- ◇ *Modelo híbrido de vecinos cercanos (HKNN)*: En estados cuánticos, la superposición entre dos estados actúa como una medida de similitud análoga a la distancia euclidiana y esta superposición se encuentra a través de un circuito simple conocido como una "prueba de intercambio" (swap-test). Este circuito se puede utilizar para evaluar las distancias entre vectores clásicos en algoritmos de KNN [258].
- ◇ *Otros tipos diferentes de topologías para redes neuronales*: redes neuronales ortogonales, redes neuronales cuánticas completamente auto-supervisadas (QFS-Net), redes neuronales CNOT (CMN), redes neuronales convolucionales profundas cuánticas (QDCNN), redes neuronales cuánticas de retropropagación (QBP), redes neuronales feedforward (ffNN), redes neuronales de memoria a corto y largo plazo (LTSM-QNN), redes neuronales generativas adversarias cuánticas (QGAN), redes neuronales cuánticas recurrentes (RQNN), etc.

Otros algoritmos de aprendizaje automático cuántico que no entran dentro de ninguna de las categorías anteriores incluyen [413, 430]. Algunas limitaciones de los algoritmos de aprendizaje automático cuántico están descritas en [1]. Muchos otros algoritmos de consulta que extraen la estructura oculta de una función tipo "caja negra" podrían considerarse algoritmos de aprendizaje automático. Véanse, por ejemplo [55, 114, 136, 137, 295]. Algunas ventajas de la computación cuántica para aprender de oráculos ruidosos se describen en [130, 203]. Existe un conjunto de trabajos relacionados, no estrictamente de estrictamente dentro del marco estándar de los algoritmos cuánticos, con respecto a aprendizaje cuántico, en el caso de que los propios datos sean coherentes desde el punto de vista cuántico. Véase [11, 30, 31, 69, 82, 151, 293, 350, 351, 366].

9.8 Análisis financiero

Palabras clave: finanzas.

La aplicación de algoritmos cuánticos para el análisis financiero se planteó por primera vez hace más de dos décadas [353] y desde entonces se han propuesto todo tipo de técnicas con este fin. En general, esas técnicas suelen basarse en métodos de Monte Carlo cuánticos, métodos de optimización cuánticos y machine learning cuántico, es decir, técnicas clásicas pero aceleradas a través de la computación cuántica [75, 155]. Sin embargo estas técnicas aún no han conseguido aplicación práctica en tanto que requieren de ordenadores cuánticos con un mayor número de cúbits y una reducción drástica del ruido y la decoherencia. Es por esto que mucha de la investigación actual en este campo se centra en la obtención de algoritmos que puedan ser efectivos incluso con las limitaciones de hardware actuales [158].

9.9 Simulación cuántica y redes de tensores

Palabras clave: simulación, redes de tensores.

Este concepto proviene de de la teoría de la información cuántica y del estudio de sistemas cuánticos de muchos cuerpos [361, 396, 404, 421]. Para representar la función de onda de un sistema cuántico de muchos cuerpos, podemos escribir:

$$\psi = \sum_{i_1, i_2, \dots, i_N} A_{i_1, i_2, \dots, i_N} \vec{m},$$

donde $A \in M_{n \times (\dots \times n)}(\mathbb{C})$. Por motivos prácticos, se considera aquí un *tensor* como una generalización de una matriz a más de dos dimensiones.

El número de elementos del tensor A crece exponencialmente con N (maldición de la dimensionalidad). Una forma de evitarlo sería con una descomposición SVD (también denominada PCA) seguida de una reducción de orden, eliminando los autovalores de menor peso. De este modo, A se escribiría como el producto $U\tilde{S}V^t$, donde \tilde{S} es la matriz diagonal donde se han eliminado algunos autovalores. Las sumas de los productos matriciales se realizarían sobre menos dimensiones que las existentes originalmente. Esta es la idea detrás del método MPS utilizado en este campo [184].

En general, los algoritmos estudiados en las redes de tensores cuánticas (en inglés, *quantum tensor networks* o QTN) aprovechan la estructura local del hamiltoniano que genera dichos tensores. El objetivo es poder describirlo como una multiplicación de matrices unitarias de forma óptima, lo que se conoce como el problema de *simulación cuántica*. A menos que la clase BPP sea igual a la clase BQP (véase sección 4.1), este problema no es resoluble en un ordenador clásico en tiempo polinómico. Se han desarrollado muchas técnicas de simulación cuántica para clases generales de hamiltonianos [10, 56, 58–61, 63, 71, 99, 116, 279, 280, 378, 378, 410, 436], dinámica química [205, 235, 263, 339, 367], física de la materia condensada [2, 318, 419], mecánica cuántica relativista (la ecuaciones de Dirac y

Klein-Gordon) [127, 172, 429], sistemas cuánticos abiertos [89, 111, 122, 246] y teoría cuántica de campos [81, 85, 201, 224–226].

La complejidad exponencial de simular clásicamente sistemas cuánticos llevó a Feynman a proponer por primera vez que los ordenadores cuánticos podrían superar a los ordenadores clásicos en determinadas tareas [171]. El problema de encontrar estados base de hamiltonianos locales es QMA-completa y, por lo tanto, probablemente requiera un tiempo exponencial en un ordenador cuántico en el peor de los casos. En todo caso, se han desarrollado algoritmos cuánticos para aproximar el estado base [29, 33, 64, 168, 234, 326, 363, 390, 399, 405, 406], así como otros estados de mayor energía [118, 236, 327, 340, 388], para algunas clases de hamiltonianos y estados de equilibrio para algunas clases de ecuaciones [332]. También se han obtenido algoritmos cuánticos para preparar ciertas clases de estados de la red tensorial [182, 356, 357, 361, 362, 364].

La técnica de redes de tensores se ha aplicado recientemente para extraer funciones codificadas en amplitudes [290], problemas de combinatoria [269] y se ha estudiado su relación con el aprendizaje automático [365].

9.10 Computación cuántica adiabática

Palabras clave: adiabática, annealer, máquina de temple cuántico.

Este tipo de computación es diferente del de las máquinas de puertas cuánticas. Está basada en el teorema adiabático de Born y Fock, que establece que si un sistema cuántico se modifica de forma “suficientemente” gradual, entonces el nivel de energía no cambia. Aunque el debate sobre si la máquina D-Wave realmente aprovecha los fenómenos cuánticos genera controversia, es indiscutible el hecho de que estos superordenadores están especialmente predispuestos para resolver problemas de optimización cuadrática con variables binarias [88, 384, 394]. Trabajos previos sobre este tema que buscaban resolver problemas de la vida real con la ayuda de una máquina de temple cuántico se incluyen en [88, 394]. Si bien uno se ocupa de la resolución del problema del tiempo de difusión y el otro resuelve el problema de programación de talleres, ambos plantean únicamente variables binarias en sus formulaciones. Un trabajo que aborda la resolución de Problemas Lineales de Enteros Mixtos (MILP) con la ayuda de una máquina de temple cuántico y un ordenador clásico para la parte real, aplicado a la optimización de una refinería, puede verse en [321]. Otros trabajos, como [373], adoptan este esquema híbrido clásico-cuántico inspirado en métodos de generación de columnas desarrollados en el campo de la Investigación Operativa.

A continuación, indicamos algunos de los campos de aplicación indicados en la revisión [196]. Para un estudio sobre la dependencia del tamaño del intervalo mínimo de excitación en el algoritmo adiabático cuántico, véase [432]. Sobre el problema del algoritmo de optimización adiabática cuántica y los mínimos locales, véase [336]. Sobre el problema de muestreo del estado cuántico Gibbs térmico y la evaluación de funciones de partición con un ordenador cuántico, véase [327]. Sobre el problema de la transición de fase de primer orden en el algoritmo adiabático cuántico, véase [433]. Sobre los pro-

blemas de la condición adiabática y el tiempo de colisión cuántica de cadenas de Markov, véase [251]. Puede encontrarse un método de mezcla cuántica secuencial para cadenas de Markov que evolucionan lentamente en [317]. Para la descripción de un algoritmo metrópolis cuántico-cuántico, véase [435]. Sobre las propiedades de un algoritmo de evolución adiabática cuántica aplicado a instancias aleatorias de un problema NP-completo, véase [163]. Acerca del rendimiento del algoritmo adiabático cuántico en instancias aleatorias de dos problemas de optimización en hipergrafos regulares, véase [166]. Para un estudio sobre el entrenamiento de un clasificador binario con el algoritmo adiabático cuántico, véase [310]. Sobre el problema de entrenar un clasificador a gran escala con el algoritmo adiabático cuántico, véase [311]. Para una demostración práctica de la clasificación binaria utilizando la implementación de hardware de recocido cuántico, véase [309]. Acerca del problema de entrenamiento de un clasificador a gran escala con optimización cuántica adiabática, véase [308]. Sobre el tema de la clasificación robusta con optimización cuántica adiabática, véase [139].

Otra revisión de interés en computación cuántica adiabática que explica variantes del teorema adiabático y AQC estocástica es [16] y, para el campo de las finanzas, puede consultarse [208]. Un libro que revisa el trabajo de D-Wave para la construcción de su máquina es [285].

9.11 Ecuaciones diferenciales ordinarias

Palabras clave: Ecuaciones diferenciales ordinarias, métodos numéricos para EDOs.

Problema: *Dado un problema de valores iniciales en \mathbb{R}^n , $d\mathbf{x}/dt = \mathbf{f}(t, \mathbf{x})$, $\mathbf{x}(t_0) = \mathbf{x}_0$, aproximar numéricamente su solución en un determinado tiempo o conjunto finito de tiempos.*

Existe una gran variedad de literatura que aborda el problema para el caso lineal, véase, entre otros, [57, 62, 112, 240, 250, 422]. En esencia, gran parte de estos trabajos parten de esquemas numéricos clásicos para la resolución de EDOs para llegar a un sistema lineal. La principal ventaja cuántica reside en que los sistemas lineales resultantes pueden ser abordados con algoritmos QLSA (Quantum Lineal Solver Algorithm) del tipo HHL (véase Sección 3.3). En general, en los algoritmos presentados, se observa una mejora exponencial en el orden de complejidad con respecto a los algoritmos clásicos.

En lo que respecta a los problemas no lineales se observa una gran variedad de técnicas, desde la aplicación de métodos numéricos clásicos para reducir el problema a un sistema lineal, técnicas de linealización, aproximaciones polinómicas, etc. (véase, entre otros, [250, 256, 260, 270, 437]). En todos los trabajos consultados los autores son optimistas en lo que se refiere a la ventaja de la computación cuántica frente a la clásica.

Como aspecto negativo cabe destacar que los algoritmos QLSA nos proporcionan la solución en forma de estado cuántico, lo cual dificulta el acceso a la información completa sobre la solución. En el caso de que estemos interesados en el valor de la aproximación en un punto en concreto, una posible solución a la limitación comentada anteriormente

es introducir de forma artificial ecuaciones en el sistema lineal de forma que se repita la solución buscada un número lo suficientemente alto de veces para que al medir el estado cuántico la probabilidad de observarla sea elevada (véase, entre otros, [57]).

9.12 Ecuaciones en derivadas parciales

Palabras clave: Ecuaciones en derivadas parciales, métodos numéricos para EDPs.

Problema: *Dada una ecuación en derivadas parciales con condiciones de contorno y, en su caso, condiciones iniciales, aproximar numéricamente su solución.*

Los métodos numéricos de resolución de EDPs clásicos (Diferencias Finitas, Elementos Finitos, Métodos Espectrales, etc.) reducen el problema de aproximar la solución a un sistema lineal. Es en la resolución del sistema lineal donde los algoritmos QLSA (Quantum Linear Solver Algorithm) del tipo HHL (véase Sección 3.3) muestran su ventaja frente a los algoritmos clásicos. Este es el argumento que se emplea en, por ejemplo, [113, 127, 131, 223, 265, 299, 439]. Al igual que en el caso de las ecuaciones diferenciales, uno de los principales inconvenientes a la hora de aplicar estas técnicas a la hora de aproximar la solución de una EDP radica en el hecho de que dicha solución viene dada en forma de estado cuántico. En los trabajos anteriores se proponen diferentes situaciones en las cuales el uso de la solución en forma de estado cuántico se puede emplear para realizar determinados cálculos.

Recientemente, el concepto de *computación variacional cuántica* (VQC) para resolver problemas de optimización se ha comprobado que es viable para resolver ecuaciones en derivadas parciales. Básicamente los algoritmos VQC son algoritmos de optimización híbridos en donde la evaluación del funcional de coste se realiza a través de un ordenador cuántico, mientras que el algoritmo de optimización se lleva a cabo empleando algoritmos clásicos. Destacamos, entre otros, [268].

10 Ordenadores cuánticos, aplicaciones a la industria y casos de uso

En los últimos años se han formulado muchas potenciales aplicaciones de la computación cuántica a sectores productivos como pueden ser las finanzas, la industria farmacéutica, la industria química, la industria del automóvil o la de la energía, entre otras [43, 68, 209, 324, 368, 375], todo ello acompañado de un crecimiento exponencial de la financiación pública dedicada a proyectos de computación cuántica liderado por China (15,3 mil millones de dólares) y, en segundo lugar, la Unión Europea (8,4 millones de dólares) [377].

Sin embargo, los casos de uso en la actualidad son muy limitados debido a la naturaleza incipiente de la tecnología, cuyos errores o falta de capacidad hacen que aún sea

inviabile para muchas aplicaciones. También es importante tener en cuenta la dificultad de conocer estos casos de uso, sobre todo en aplicaciones experimentales, debido a la falta de transparencia de la industria, a menudo fruto del celo por proteger la propiedad intelectual [68,368]. Este hecho, junto con la dificultad de implementar la tecnología, deriva en la carencia de un marco coherente de aplicación y a una falta de impacto probado en la industria, lo cual, a su vez, limita la inversión privada más allá de las principales empresas proveedoras de servicios de computación cuántica (IBM, Google, D-Wave, etc) [375]. A pesar de ello, la inversión privada y las startups relativas a computación cuántica se han disparado entre el 2015 y el 2021 [68], aunque este impulso se ha ralentizado en el 2022 [377].

En el caso de la Unión Europea, esta lanzó en 2018 el *Buque Insignia de Tecnologías Cuánticas* (Quantum Flagship) [330]. Se trata de una iniciativa de investigación a gran escala y a largo plazo con un presupuesto de 1.000 millones de euros financiada por la UE que reúne a instituciones de investigación, la industria y financiadores públicos¹. Además, como parte de la *Empresa Común Europea de Informática de Alto Rendimiento* (EuroHPC JU²), la Comisión Europea ha empezado a construir ordenadores cuánticos piloto. Estos ordenadores actuarán como aceleradores interconectados con los superordenadores de la Empresa Común, formando máquinas híbridas que combinan tecnologías informáticas cuánticas y clásicas. Entre sus objetivos, estarán abordar problemas complejos de simulación y optimización, especialmente en el desarrollo de materiales, descubrimiento de fármacos, pronóstico del tiempo, transporte y otros problemas del mundo real de gran importancia para la industria y la sociedad. En última instancia, se pretende ofrecer el primer ordenador con aceleración cuántica en 2025.

En octubre de 2022, la Empresa Común EuroHPC anunció la selección de seis sitios en toda la UE para albergar los primeros ordenadores cuánticos europeos, que se integrarán en los superordenadores EuroHPC. Estas computadoras cuánticas recién adquiridas a través de un presupuesto de 100 millones de euros se basarán en tecnología europea puramente de vanguardia y se ubicarán en Chequia, Alemania, España, Francia, Italia y Polonia.

Por otra parte, a nivel nacional, es Alemania la que lidera en la Unión Europea la inversión pública en computación cuántica, suponiendo un 42% de la financiación total de la UE [377]. Asimismo, la inversión privada en Alemania se ha catalizado a través del consorcio de empresas QUTAC (Quantum Technology and Application Consortium). Esta agrupación recoge a empresas líderes en sectores como la manufactura de vehículos (BMW, Bosch, Volkswagen), la industria química y farmacéutica (BASF, Boehringer Ingelheim, Merck), los seguros (Munich Re) y la tecnología (Infieon, SAP, Siemens). El consorcio ha señalado una serie de usos con potencial impacto que están investigando (ver Tabla 10.1).

¹<https://digital-strategy.ec.europa.eu/en/policies/quantum>.

²<https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing-joint-undertaking>.

Reto	Ámbito	Empresa	Caso de uso	Impacto
Ingeniería y diseño	Machine Learning	AIRBUS	Computación cuántica para modelización de EDPs	Alto
	Optimización	AIRBUS	Optimización del diseño de la caja del ala	Alto
		Bosch	Comprobación de software y demostración de corrección	Medio
	Simulación	Bosch	Optimizaciones de diseño para motores eléctricos usando simulación numérica y elementos finitos	Medio
		Merck	Identificación y control de parámetros accionables para el control de la propagación de enfermedades	Desconocido
Ciencia de materiales	Optimización	Boehringer Ingelheim	Técnicas de imágenes optimizadas – Técnicas de imágenes inspiradas en algoritmos cuánticos	Medio
	Simulación	BASF	Química cuántica – Predicción de la reactividad química en química cuántica molecular	Alto
		Boehringer Ingelheim	Dinámica molecular – Simulación de la dinámica de moléculas	Alto
		Merck	Desarrollo de materiales y drogas usando simulaciones cuánticas	Medio
		Munich Re	Cobertura de batería - Garantías de rendimiento para baterías de vehículos eléctricos	Medio
		VW	Computación química para investigación en baterías	Alto
Producción y logística	Machine Learning	Siemens	QaRL – Aprendizaje con refuerzo asistido por computación cuántica – Aplicable a muchos casos de uso industriales	Medio
	Optimización	BASF	Gestión de flotas – Despliegue y enrutado de camiones y maquinaria <i>in situ</i>	Medio
		BMW	Planificación de producción robotizada – Optimización de recorridos de robots para robots de producción (e.g. robot de sellado de PVC)	Medio
		BMW	Prueba de componentes de vehículos – Optimización de la configuración de las opciones de vehículos de pruebas	Medio

Reto	Ámbito	Empresa	Caso de uso	Impacto
		BMW	Configuración de turnos – Optimización de la asignación de turnos laborales	Medio
		Infineon	Satisfacción de demanda en cadenas de suministro – Decisión de un plan de producción dada una demanda prevista	Medio
		Infineon	Uso de los actuadores y sensores Infineon para optimizar cadenas de suministros del lado del cliente	Medio
		Munich Re	Cobertura de transporte – Seguros de transportes de material en los que el tiempo es crítico	Medio
		SAP	Logística – Carga de camiones	Medio
		SAP	Planificación de la cadena de suministros – Escalado mejorado y acelerado de órdenes de venta (escalado de lotes)	Alto
		Siemens	QoMP – Producción matricial con optimización cuántica – Optimización en tiempo real del taller de producción	Medio
		VW	Optimización de rutas de vehículos – Optimización de la utilización de vehículos en una red de transporte	Alto
Seguridad poscuántica	Criptografía	Munich Re	IoT Cyber Cover – Seguros de criptografía poscuántica	Medio

Cuadro 10.1. Casos de uso identificados por QUTAC [43, Table 3].

Existen pocos casos de uso en la industria a día de hoy, pero podemos destacar los siguientes ejemplos de investigación en aplicaciones de la computación cuántica por parte de diferentes empresas.

- ◊ *Airbus*: En el año 2020 ofreció una competición, llamada *Airbus Quantum Computing Challenge*¹, para buscar soluciones a una serie de problemas utilizando computación cuántica. Los ganadores resolvieron un problema de optimización de la carga de un avión utilizando un algoritmo cuántico.
- ◊ *Amazon y BMW*: En una colaboración reciente [358] se plantearon problemas de planificación de trayectorias de robots a escalas relevantes para la industria, para lo que desarrollaron un proceso de optimización con algoritmos cuánticos híbridos.

¹<https://www.airbus.com/en/innovation/disruptive-concepts/quantum-technologies/airbus-quantum-computing-challenge>.

- ◇ *BMW*: En el año 2021 ofreció una competición similar a la de Airbus: *BMW Group Quantum Computing Challenge*¹. Se proclamaron ganadores en cuatro áreas: posiciones de los sensores para las funciones de conducción automatizada, simulación de deformaciones de materiales, optimización de la configuración de vehículos preserie y análisis de calidad automatizados.
- ◇ *Volkswagen*: En una publicación reciente [381] muestran como aplicaron un algoritmo cuántico de optimización aproximada (QAOA) al problema del taller de pintura que surge la industria del automóvil [159]. Realizaron simulaciones numéricas junto con datos experimentales obtenidos de un ordenador cuántico de iones atrapados logrando proporcionar una comparación entre el rendimiento de QAOA y la heurística clásica en el límite de tamaño infinito para la computación cuántica sin ruido. Los resultados experimentales de este artículo ponen de manifiesto el empeoramiento del rendimiento del algoritmo cuántico al aumentar el tamaño del problema. Destacan además que este tipo de algoritmos pueden aplicarse a otros problemas, como el problema de optimización de los coches que ensamblan los trabajadores: los coches con techo solar son más difíciles de ensamblar y no deben estar adyacentes en una secuencia para que los trabajadores puedan seguir el ritmo de la velocidad constante de la cinta transportadora. Comentan además que responder a la pregunta de si QAOA es un algoritmo de aproximación de factor constante podría abrir un nuevo espacio para la ventaja cuántica.

Por otra parte, en [397], se presentó un método de elementos finitos para optimizar un objeto tridimensional bajo criterios físicos dados (por ejemplo, diseñar un retrovisor que minimice el ruido que genera en los lugares donde se sientan los pasajeros). Se obtuvo una aproximación de este problema de elementos finitos con optimización cuadrática binaria sin restricciones (QUBO) y se introdujo la matriz correspondiente en una QPU D-Wave. Con esto se calculó la presión sonora sobre una geometría inicial de forma clásica y la QPU resolvió el problema preparado en el ordenador clásico. Esta combinación híbrida generó la solución deseada.

10.1 Computación cuántica en España

Como se mencionó anteriormente, España es fue uno de los países seleccionados dentro del proyecto EuroHPC JU de la Comisión Europea. El ordenador situado en España, en el marco del consorcio EuroQCS-España, será alojado por el Barcelona Supercomputing Center (BSC) e integrado en el superordenador EuroHPC MareNostrum5². El consorcio EuroQCS-España está liderado por el BSC e incluye al Institut de Física d'Altes Energies (IFAE) de España y al International Iberian Nanotechnology Laboratory (INL) de Portugal. El objetivo de EuroQCS-España es desarrollar un ordenador cuántico analógico, comple-

¹<https://www.press.bmwgroup.com/global/article/detail/T0362463EN/bmw-group-quantum-computing-challenge:-the-winners-have-been-decided?language=en>.

²<https://www.bsc.es/news/bsc-news/one-step-closer-european-quantum-computing-the-eurohpc-ju-signs-hosting-agreements-six-quantum>.

mentando al ordenador cuántico digital y al emulador cuántico que el BSC ya hospeda bajo la iniciativa *Quantum Spain* de la que forman parte el Centro Nacional de Supercomputación (BSC-CNS), el Centro de Supercomputación de Galicia (CESGA), el Centro de Supercomputación de Castilla y León (SCAYLE), la Universidad de Zaragoza, la Universidad de Valencia, la Fundación Computación y Tecnologías Avanzadas de Extremadura (Computaex), el Instituto de Astrofísica de Canarias (IAC), el Consorcio de Servicios Universitarios de Cataluña (CSUC), el Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT), Navarra de Servicios y Tecnologías (NASERTIC), la Universidad Autónoma de Madrid, la Universidad de Málaga y la Universidad de Cantabria¹. Ambos sistemas cuánticos serán integrados, lo que creará un sistema de computación heterogéneo compuesto por diferentes unidades de procesamiento cuántico analógico y digital.

Además del consorcio EuroQCS-España dentro del proyecto Quantum Spain, el informe *Spain Quantum Industry Report 2023* [178] recoge la situación actual de la industria de la computación cuántica en España, incluyendo las principales empresas, centros tecnológicos y de investigación, asociaciones y ecosistemas regionales, los proyectos actuales y oportunidades de financiación.

De entre los proyectos destacamos el proyecto CUCO (liderado por GMV, y constituido por las empresas BBVA, DAS Photonics, GMV, Multiverse computing, Qilimanjaro Quantum Tech y Repsol; los centros de investigación BSC, CSIC, DIPC, ICFO y Tecnalia; y la Universitat Politècnica de València), para la investigación de la computación cuántica aplicada a industrias estratégicas (energía, finanzas, espacio, defensa y logística).

En la comunidad gallega se creó en 2022 el Polo de Tecnologías Cuánticas de Galicia con el objetivo de que Galicia sea un referente europeo e internacional en computación y comunicación cuántica de cara al 2030, tanto a nivel académico y de investigación, como empresarial y comercial². Dentro de este proyecto está la financiación otorgada por la Xunta de Galicia para la compra de un ordenador cuántico Fujitsu para el CESGA.

10.2 Riesgos y consideraciones éticas

Al igual que cualquier otra tecnología disruptiva, la computación cuántica presenta una serie de riesgos y retos éticos [212,241,418]. Comparte con otras nuevas tecnologías los problemas relativos al acceso equitativo por parte de todas las partes interesadas, el acceso a educación relativa a la tecnología y el riesgo de oligopolio a través de patentes, entre otros.

El peligro más destacable inherente a la computación cuántica es la posibilidad de usarla para descifrar información cifrada con RSA (es sistema de encriptación más común a día de hoy) que hasta ahora se consideraba segura. Existen ya protocolos de encriptación poscuántica que se prevé sean resistentes a estos ataques, pero eso no elimina el

¹<https://portalayudas.mineco.gob.es/Quantum%20Spain/normativa/Paginas/bases.a.spx>.

²<https://www.cesga.es/polo-de-tecnologias-cuanticas-de-galicia/>.

riesgo de que la información encriptada que se transmite a día de hoy se almacene y sea descodifique cuando la tecnología esté disponible, lo que se conoce como un ataque “*interceptar ahora, desencriptar más tarde*” [241]. Esta situación podría revelar información sensible de estados, empresas y particulares, por lo que urge cambiar los sistemas de encriptación cuanto antes por unos resistentes a estos ataques.

Referencias

- [1] Aaronson, S.: *Quantum Machine Learning Algorithms: Read the Fine Print*. Nat. Phys. **11**(4), 291–293 (2015). URL <http://www.scottaaronson.com/papers/qml.pdf>
- [2] Abrams, D.S., Lloyd, S.: *Simulation of Many-Body Fermi Systems on a Universal Quantum Computer*. Phys. Rev. Lett. **79**, 2586–2589 (1997). DOI 10.1103/PhysRevLett.79.2586. URL <https://link.aps.org/doi/10.1103/PhysRevLett.79.2586>
- [3] Adachi, S.H., Henderson, M.P.: *Application of quantum annealing to training of deep neural networks*. arXiv preprint arXiv:1510.06356 (2015). URL <http://arxiv.org/abs/1510.06356>
- [4] Adcock, J., Allen, E., Day, M., Frick, S., Hinchliff, J., Johnson, M., Morley-Short, S., Pallister, S., Price, A., Stanisic, S.: *Advances in quantum machine learning*. arXiv preprint arXiv:1512.02900 (2015). URL <https://doi.org/10.48550/arXiv.1512.02900>
- [5] Aharonov, D., Arad, I.: *The BQP-hardness of approximating the Jones polynomial*. New J. Phys. **13**(3), 32 (2011). URL https://inis.iaea.org/search/search.aspx?orig_q=RN:43027052
- [6] Aharonov, D., Arad, I., Eban, E., Landau, Z.: *Polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane*. arXiv preprint quant-ph/0702008 (2007). URL <http://arxiv.org/abs/quant-ph/0702008>
- [7] Aharonov, D., Gao, X., Landau, Z., Liu, Y., Vazirani, U.: *A Polynomial-Time Classical Algorithm for Noisy Random Circuit Sampling*. In: Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, pp. 945–957. Association for Computing Machinery, New York, NY, USA (2023). DOI 10.1145/3564246.3585234. URL <https://dl.acm.org/doi/10.1145/3564246.3585234>
- [8] Aharonov, D., Jones, V., Landau, Z.: *A polynomial quantum algorithm for approximating the Jones polynomial*. In: J.M. Kleinberg (ed.) Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21–23, 2006, pp. 427–436. ACM (2006). DOI 10.1145/1132516.1132579. URL <https://doi.org/10.1145/1132516.1132579>
- [9] Aharonov, D., Naveh, T.: *Quantum NP—a survey*. arXiv preprint quant-ph/0210077 (2002). URL <http://arxiv.org/abs/quant-ph/0210077>
- [10] Aharonov, D., Ta-Shma, A.: *Adiabatic quantum state generation and statistical zero knowledge*. In: L.L. Larmore, M.X. Goemans (eds.) Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9–11, 2003, San Diego, CA, USA, pp. 20–29. ACM (2003). DOI 10.1145/780542.780546. URL <https://doi.org/10.1145/780542.780546>
- [11] Aïmeur, E., Brassard, G., Gambs, S.: *Machine Learning in a Quantum World*. In: L. Lamontagne, M. Marchand (eds.) Advances in Artificial Intelligence, 19th Conference of the Canadian Society for Computational Studies of Intelligence, Canadian AI 2006, Québec City, Québec, Canada, June 7–9, 2006, Proceedings, *Lecture Notes in Computer Science*, vol. 4013, pp. 431–442. Springer (2006). DOI 10.1007/11766247_37. URL https://doi.org/10.1007/11766247_37
- [12] Aïmeur, E., Brassard, G., Gambs, S.: *Quantum clustering algorithms*. In: Z. Ghahramani (ed.) Machine Learning, Proceedings of the Twenty-Fourth International Conference (ICML 2007), Corvallis, Oregon, USA, June 20–24, 2007, *ACM International Conference Proceeding Series*, vol. 227, pp. 1–8. ACM (2007). DOI 10.1145/1273496.1273497. URL <https://doi.org/10.1145/1273496.1273497>

- [13] Aïmeur, E., Brassard, G., Gambs, S.: *Quantum speed-up for unsupervised learning*. Mach. Learn. **90**(2), 261–287 (2013). DOI 10.1007/s10994-012-5316-5. URL <https://doi.org/10.1007/s10994-012-5316-5>
- [14] Alagic, G., Jordan, S., Koenig, R., Reichardt, B.: *Estimating Turaev-Viro three-manifold invariants is universal for quantum computation*. Phys. Rev. A **82**, 040,302(R) (2010). URL <https://journals.aps.org/prabstract/10.1103/PhysRevA.82.040302>
- [15] Albareti, F.D., Ankenbrand, T., Bieri, D., Hänggi, E., Lötscher, D., Stettler, S., Schöngens, M.: *A Structured Survey of Quantum Computing for the Financial Industry*. arXiv preprint arXiv:2204.10026 (2022). URL <http://arxiv.org/abs/2204.10026>
- [16] Albash, T., Lidar, D.A.: *Adiabatic quantum computation*. Rev. Mod. Phys. **90**, 015,002 (2018). DOI 10.1103/RevModPhys.90.015002. URL <https://link.aps.org/doi/10.1103/RevModPhys.90.015002>
- [17] Albash, T., Lidar, D.A.: *Demonstration of a Scaling Advantage for a Quantum Annealer over Simulated Annealing*. Phys. Rev. X **8**(3), 031,016 (2018). DOI 10.1103/PhysRevX.8.031016. URL <https://link.aps.org/doi/10.1103/PhysRevX.8.031016>
- [18] Aldous, D.J.: *Some inequalities for reversible Markov chains*. Journal of the London Mathematical Society **2**(3), 564–576 (1982). URL <https://doi.org/10.1112/jlms/s2-25.3.564>
- [19] Alman, J., Williams, V.V.: *A Refined Laser Method and Faster Matrix Multiplication*. In: Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 522–539 (2021). DOI 10.1137/1.9781611976465.32. URL <https://epubs.siam.org/doi/abs/10.1137/1.9781611976465.32>
- [20] Ambainis, A.: *Quantum search algorithms*. SIGACT News **35**(2), 22–35 (2004). DOI 10.1145/992287.992296. URL <https://doi.org/10.1145/992287.992296>
- [21] Ambainis, A.: *Quantum Walk Algorithm for Element Distinctness*. SIAM J. Comput. **37**(1), 210–239 (2007). DOI 10.1137/S0097539705447311. URL <https://doi.org/10.1137/S0097539705447311>
- [22] Ambainis, A.: *Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations*. arXiv preprint arXiv:1010.4458 (2010). URL <http://arxiv.org/abs/1010.4458>
- [23] Ambainis, A., Spalek, R.: *Quantum Algorithms for Matching and Network Flows*. In: B. Durand, W. Thomas (eds.) STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science, Marseille, France, February 23–25, 2006, Proceedings, *Lecture Notes in Computer Science*, vol. 3884, pp. 172–183. Springer (2006). DOI 10.1007/11672142. URL <https://doi.org/10.1007/11672142>
- [24] Amenyro, B., Maroulas, V., Siopsis, G.: *Quantum persistent homology*. arXiv preprint arXiv:2202.12965 (2022). URL <http://arxiv.org/abs/2202.12965>
- [25] Amin, M.H., Andriyash, E., Rolfe, J., Kulchytksyy, B., Melko, R.: *Quantum Boltzmann Machine*. Phys. Rev. X **8**, 021,050 (2018). DOI 10.1103/PhysRevX.8.021050. URL <https://link.aps.org/doi/10.1103/PhysRevX.8.021050>
- [26] Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., Schanck, J.: *Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3*. In: R. Avanzi, H. Heys (eds.) Selected Areas in Cryptography – SAC 2016, Lecture Notes in Computer Science, pp. 317–337. Springer International Publishing, Cham (2017). DOI 10.1007/978-3-319-69453-5_18. URL https://link.springer.com/chapter/10.1007/978-3-319-69453-5_18
- [27] Anschuetz, E.R., Kiani, B.T.: *Quantum variational algorithms are swamped with traps*. Nat. Commun. **13**(1), 7760 (2022). DOI 10.1038/s41467-022-35364-5. URL <https://doi.org/10.1038/s41467-022-35364-5>

- [28] Apers, S., Sen, S., Szabó, D.: *A (simple) classical algorithm for estimating Betti numbers*. arXiv preprint arXiv:2211.09618 (2022). URL <http://arxiv.org/abs/2211.09618>
- [29] Arad, I., Sattath, O.: *A Constructive Quantum Lovász Local Lemma for Commuting Projectors*. arXiv preprint arXiv:1310.7766 (2013). URL <https://doi.org/10.48550/arXiv.1310.7766>
- [30] Arunachalam, S., de Wolf, R.: *A Survey of Quantum Learning Theory*. ACM SIGACT News **48**(2), 41–67 (2017). DOI 10.1145/3106700.3106710. URL <https://dl.acm.org/doi/10.1145/3106700.3106710>
- [31] Arunachalam, S., de Wolf, R.: *Optimal Quantum Sample Complexity of Learning Algorithms*. J. Mach. Learn. Res. **19**, 71:1–71:36 (2018). URL <http://jmlr.org/papers/v19/18-195.html>
- [32] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G.S.L., Buell, D.A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., Fowler, A., Gidney, C., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M.P., Hartmann, M.J., Ho, A., Hoffmann, M., Huang, T., Humble, T.S., Isakov, S.V., Jeffrey, E., Jiang, Z., Kafri, D., Kechedzhi, K., Kelly, J., Klimov, P.V., Knysh, S., Korotkov, A., Kostrița, F., Landhuis, D., Lindmark, M., Lucero, E., Lyakh, D., Mandrà, S., McClean, J.R., McEwen, M., Megrant, A., Mi, X., Michielsen, K., Mohseni, M., Mutus, J., Naaman, O., Neeley, M., Neill, C., Niu, M.Y., Ostby, E., Petukhov, A., Platt, J.C., Quintana, C., Rieffel, E.G., Roushan, P., Rubin, N.C., Sank, D., Satzinger, K.J., Smelyanskiy, V., Sung, K.J., Trevithick, M.D., Vainsencher, A., Villalonga, B., White, T., Yao, Z.J., Yeh, P., Zalcman, A., Neven, H., Martinis, J.M.: *Quantum supremacy using a programmable superconducting processor*. Nature **574**(7779), 505–510 (2019). DOI 10.1038/s41586-019-1666-5. URL <https://www.nature.com/articles/s41586-019-1666-5>
- [33] Aspuru-Guzik, A., Dutoi, A.D., Love, P.J., Head-Gordon, M.: *Simulated quantum computation of molecular energies*. Science **309**(5741), 1704–1707 (2005). URL <https://doi.org/10.1126/science.1113479>
- [34] Babbush, R., McClean, J.R., Newman, M., Gidney, C., Boixo, S., Neven, H.: *Focus beyond Quadratic Speedups for Error-Corrected Quantum Advantage*. PRX Quantum **2**(1), 010,103 (2021). DOI 10.1103/PRXQuantum.2.010103. URL <https://link.aps.org/doi/10.1103/PRXQuantum.2.010103>
- [35] Bacon, D., Childs, A.M., van Dam, W.: *From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*. In: 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23–25 October 2005, Pittsburgh, PA, USA, Proceedings, pp. 469–478. IEEE Computer Society (2005). DOI 10.1109/SFCS.2005.38. URL <https://doi.org/10.1109/SFCS.2005.38>
- [36] Bae, E., Lee, S.: *Quantum Algorithm for Solving the Continuous Hidden Symmetry Subgroup Problem*. IEEE Access **9**, 93,248–93,254 (2021). DOI 10.1109/ACCESS.2021.3092723. URL <https://ieeexplore.ieee.org/document/9466135>
- [37] Banin, M., Tsaban, B.: *A reduction of Semigroup DLP to classic DLP*. Des. Codes Cryptogr. **81**(1), 75–82 (2016). DOI 10.1007/s10623-015-0130-2. URL <https://doi.org/10.1007/s10623-015-0130-2>
- [38] Barak, B., Moitra, A., O’Donnell, R., Raghavendra, P., Regev, O., Steurer, D., Trevisan, L., Vijayaraghavan, A., Witmer, D., Wright, J.: *Beating the Random Assignment on Constraint Satisfaction Problems of Bounded Degree*. In: N. Garg, K. Jansen, A. Rao, J.D.P. Rolim (eds.) Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2015, August 24–26, 2015, Princeton, NJ, USA, LIPIcs, vol. 40, pp. 110–123.

- Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2015). DOI 10.4230/LIPIcs.APPROX-RANDOM.2015.110. URL <https://doi.org/10.4230/LIPIcs.APPROX-RANDOM.2015.110>
- [39] Barbulescu, R., Poulalion, A.: *The Special Case of Cyclotomic Fields in Quantum Algorithms for Unit Groups*. In: N. El Mrabet, L. De Feo, S. Duquesne (eds.) *Progress in Cryptology - AFRI-CACRYPT 2023*, Lecture Notes in Computer Science, pp. 229–251. Springer Nature Switzerland, Cham (2023). DOI 10.1007/978-3-031-37679-5_10. URL https://link.springer.com/chapter/10.1007/978-3-031-37679-5_10
- [40] Barg, A., Zhou, S.: *A quantum decoding algorithm of the simplex code*. In: *Proceedings of the 36th Annual Allerton Conference* (1998). URL <http://www.ece.umd.edu/~abarg/reprints/rm1dq.pdf>
- [41] Bass, S.D., Zohar, E.: *Quantum technologies in particle physics*. *Phil. Trans. R. Soc. A* **380** (2022). DOI doi.org/10.1098/rsta.2021.0072. URL <https://royalsocietypublishing.org/doi/10.1098/rsta.2021.0072>
- [42] Bauer, C.W., Davoudi, Z., Balantekin, A.B., Bhattacharya, T., Carena, M., de Jong, W.A., Draper, P., El-Khadra, A., Gemelke, N., Hanada, M., Kharzeev, D., Lamm, H., Li, Y.Y., Liu, J., Lukin, M., Meurice, Y., Monroe, C., Nachman, B., Pagano, G., Preskill, J., Rinaldi, E., Roggero, A., Santiago, D.I., Savage, M.J., Siddiqi, I., Siopsis, G., Van Zanten, D., Wiebe, N., Yamauchi, Y., Yeter-Aydeniz, K., Zorzetti, S.: *Quantum Simulation for High-Energy Physics*. *PRX Quantum* **4**, 027,001 (2023). DOI 10.1103/PRXQuantum.4.027001. URL <https://link.aps.org/doi/10.1103/PRXQuantum.4.027001>
- [43] Bayerstadler, A., Becquin, G., Binder, J., Botter, T., Ehm, H., Ehmer, T., Erdmann, M., Gaus, N., Harbach, P., Hess, M., et al.: *Industry quantum computing applications*. *EPJ Quantum Technol.* **8**(1), 25 (2021). URL <https://doi.org/10.1140/epjqt/s40507-021-00114-x>
- [44] Bañuls, M., Blatt, R., et al., J.C.: *Simulating lattice gauge theories within quantum technologies*. *Eur. Phys. J. D* **74**(165) (2020). DOI doi.org/10.1140/epjd/e2020-100571-8. URL <https://link.springer.com/article/10.1140/epjd/e2020-100571-8>
- [45] de Beaudrap, J.N., Cleve, R., Watrous, J.: *Sharp Quantum versus Classical Query Complexity Separations*. *Algorithmica* **34**(4), 449–461 (2002). DOI 10.1007/s00453-002-0978-1. URL <https://doi.org/10.1007/s00453-002-0978-1>
- [46] Belovs, A.: *Span-program-based quantum algorithm for the rank problem*. arXiv preprint [arXiv:1103.0842](https://arxiv.org/abs/1103.0842) (2011). URL <http://arxiv.org/abs/1103.0842>
- [47] Belovs, A., Spalek, R.: *Adversary lower bound for the k-sum problem*. In: R.D. Kleinberg (ed.) *Innovations in Theoretical Computer Science, ITCS '13*, Berkeley, CA, USA, January 9–12, 2013, pp. 323–328. ACM (2013). DOI 10.1145/2422436.2422474. URL <https://doi.org/10.1145/2422436.2422474>
- [48] Ben-Or, M., Hassidim, A.: *Quantum search in an ordered list via adaptive learning* (2007). URL <https://arxiv.org/abs/quant-ph/0703231>. ArXiv preprint [arXiv:quant-ph/0703231](https://arxiv.org/abs/quant-ph/0703231)
- [49] Benedetti, M., Realpe-Gómez, J., Biswas, R., Perdomo-Ortiz, A.: *Quantum-Assisted Learning of Hardware-Embedded Probabilistic Graphical Models*. *Phys. Rev. X* **7**, 041,052 (2017). DOI 10.1103/PhysRevX.7.041052. URL <https://link.aps.org/doi/10.1103/PhysRevX.7.041052>
- [50] Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.V.: *Strengths and Weaknesses of Quantum Computing*. *SIAM J. Comput.* **26**(5), 1510–1523 (1997). DOI 10.1137/S0097539796300933. URL <https://doi.org/10.1137/S0097539796300933>
- [51] Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: *Mixed-state entanglement and quantum error correction*. *Phys. Rev. A* **54**(5), 3824–3851 (1996). DOI 10.1103/PhysRevA.54.3824. URL <https://link.aps.org/doi/10.1103/PhysRevA.54.3824>

- [52] Bermejo-Vega, J., Zatloukal, K.C.: *Abelian hypergroups and quantum computation*. arXiv preprint arXiv:1509.05806 (2015). URL <http://arxiv.org/abs/1509.05806>
- [53] Bernstein, D.J.: *Proving primality in essentially quartic random time*. Math. Comput. **76**(257), 389–403 (2007). DOI 10.1090/S0025-5718-06-01786-8. URL <https://doi.org/10.1090/S0025-5718-06-01786-8>
- [54] Bernstein, D.J.: *Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?* In: Proceedings of the 4th Workshop on Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS'09), pp. 105–116 (2009). URL <https://cr.ypt.to/hash/collisioncost-20090517.pdf>
- [55] Bernstein, E., Vazirani, U.V.: *Quantum complexity theory*. In: S.R. Kosaraju, D.S. Johnson, A. Aggarwal (eds.) Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, May 16–18, 1993, San Diego, CA, USA, pp. 11–20. ACM (1993). DOI 10.1145/167088.167097. URL <https://doi.org/10.1145/167088.167097>
- [56] Berry, D., Novo, L.: *Corrected quantum walk for optimal Hamiltonian simulation*. Proc. Spie. **16**(15&16), 1295–1317 (2016). URL <https://doi.org/10.26421/QIC16.15-16>
- [57] Berry, D.W.: *High-order quantum algorithm for solving linear differential equations*. J. Phys. A: Math. Theor. **47** (2014). URL <https://iopscience.iop.org/article/10.1088/1751-8113/47/10/105301/meta>
- [58] Berry, D.W., Ahokas, G., Cleve, R., Sanders, B.C.: *Efficient quantum algorithms for simulating sparse Hamiltonians*. Comm. Math. Phys. **270**(2), 359–371 (2007). URL <https://doi.org/10.1007/s00220-006-0150-x>
- [59] Berry, D.W., Childs, A.M., Cleve, R., Kothari, R., Somma, R.D.: *Exponential improvement in precision for simulating sparse Hamiltonians*. In: D.B. Shmoys (ed.) Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 – June 03, 2014, pp. 283–292. ACM (2014). DOI 10.1145/2591796.2591854. URL <https://doi.org/10.1145/2591796.2591854>
- [60] Berry, D.W., Childs, A.M., Cleve, R., Kothari, R., Somma, R.D.: *Simulating Hamiltonian Dynamics with a Truncated Taylor Series*. Phys. Rev. Lett. **114**, 090,502 (2015). DOI 10.1103/PhysRevLett.114.090502. URL <https://link.aps.org/doi/10.1103/PhysRevLett.114.090502>
- [61] Berry, D.W., Childs, A.M., Kothari, R.: *Hamiltonian Simulation with Nearly Optimal Dependence on all Parameters*. In: V. Guruswami (ed.) IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17–20 October, 2015, pp. 792–809. IEEE Computer Society (2015). DOI 10.1109/FOCS.2015.54. URL <https://doi.org/10.1109/FOCS.2015.54>
- [62] Berry, D.W., Childs, A.M., Ostrander, A., Wang, G.: *Quantum Algorithm for Linear Differential Equations with Exponentially Improved Dependence on Precision*. Comm. Math. Phys. **356**, 1057 – 1081 (2017). URL <https://doi.org/10.1007/s00220-017-3002-y>
- [63] Berry, D.W., Cleve, R., Somma, R.D.: *Exponential improvement in precision for Hamiltonian-evolution simulation*. arXiv preprint arXiv:1308.5424 (2013). URL <http://arxiv.org/abs/1308.5424>
- [64] Berry, D.W., Kieferová, M., Scherer, A., Sanders, Y.R., Low, G.H., Wiebe, N., Gidney, C., Babbush, R.: *Improved techniques for preparing eigenstates of fermionic Hamiltonians*. npj Quantum Inf. **4**(1), 22 (2018). URL <https://doi.org/10.1038/s41534-018-0071-5>
- [65] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., Lloyd, S.: *Quantum machine learning*. Nature **549**(7671), 195–202 (2017). URL <https://doi.org/10.1038/nature23474>
- [66] Biasse, J., Song, F.: *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*. In: R. Krauthgamer (ed.) Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016,

- Arlington, VA, USA, January 10-12, 2016, pp. 893–902. SIAM (2016). DOI 10.1137/1.9781611974331.ch64. URL <https://doi.org/10.1137/1.9781611974331.ch64>
- [67] Biham, E., Biham, O., Biron, D., Grassl, M., Lidar, D.: *Grover’s quantum search algorithm for an arbitrary initial amplitude distribution*. Phys. Rev. A **60**(4), 2742 (1999). URL <https://journals.aps.org/prabstract/10.1103/PhysRevA.60.2742>
- [68] Biondi, M., Heid, A., Henke, N., Mohr, N., Pautasso, L., Ostojic, I., Wester, L., Zemme, R.: *Quantum computing: An emerging ecosystem and industry use cases*. McKinsey & Company (2021)
- [69] Bisio, A., Chiribella, G., D’Ariano, G.M., Facchini, S., Perinotti, P.: *Optimal quantum learning of a unitary transformation*. Phys. Rev. A **81**, 032,324 (2010). DOI 10.1103/PhysRevA.81.032324. URL <https://link.aps.org/doi/10.1103/PhysRevA.81.032324>
- [70] Black, M., Maxwell, W., Nayyeri, A.: *An Incremental Span-Program-Based Algorithm and the Fine Print of Quantum Topological Data Analysis*. arXiv preprint arXiv:2307.07073 (2023). URL <http://arxiv.org/abs/2307.07073>
- [71] Boghosian, B.M., Taylor, W.: *Simulating quantum mechanics on a quantum computer*. Phys. D **120**, 30–42 (1998). URL [https://doi.org/10.1016/S0167-2789\(98\)00042-6](https://doi.org/10.1016/S0167-2789(98)00042-6)
- [72] Boneh, D., Lipton, R.J.: *Quantum cryptanalysis of hidden linear functions*. In: D. Coppersmith (ed.) CRYPTO ’95, Lecture Notes in Computer Science, pp. 424–437. Springer-Verlag (1995). URL https://link.springer.com/chapter/10.1007/3-540-44750-4_34
- [73] Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: *Quantum Security Analysis of AES*. IACR Transactions on Symmetric Cryptology pp. 55–93 (2019). DOI 10.13154/tosc.v2019.i2.55-93. URL <https://tosc.iacr.org/index.php/ToSC/article/view/8314>
- [74] Bordewich, M., Freedman, M., Lovász, L., Welsh, D.: *Approximate Counting and Quantum Computation*. Comb. Probab. Comput. **14**(5-6), 737–754 (2005). DOI 10.1017/S0963548305007005. URL <https://doi.org/10.1017/S0963548305007005>
- [75] Bouland, A., van Dam, W., Joorati, H., Kerenidis, I., Prakash, A.: *Prospects and challenges of quantum finance*. arXiv preprint arXiv:2011.06492 (2020). URL <http://arxiv.org/abs/2011.06492>
- [76] Boyer, M., Brassard, G., Høyer, P., Tapp, A.: *Tight bounds on quantum searching*. Fortschr. Phys. **46**, 493–505 (1998). URL [https://doi.org/10.1002/\(SICI\)1521-3978\(199806\)46:4/5<493::AID-PROP493>3.0.CO;2-P](https://doi.org/10.1002/(SICI)1521-3978(199806)46:4/5<493::AID-PROP493>3.0.CO;2-P)
- [77] Brassard, G., Høyer, P., Mosca, M., Tapp, A.: *Quantum amplitude amplification and estimation*. In: S.J.L. Jr., H.E. Brandt (eds.) Quantum Computation and Quantum Information, *AMS Contemporary Mathematics Series*, vol. 305. American Mathematical Society (2002). URL <https://doi.org/10.1090/conm/305/05215>
- [78] Brassard, G., Høyer, P., Tapp, A.: *Quantum cryptanalysis of hash and claw-free functions*. SI-GACT News **28**(2), 14–19 (1997). DOI 10.1145/261342.261346. URL <https://doi.org/10.1145/261342.261346>
- [79] Brassard, G., Høyer, P., Tapp, A.: *Quantum counting*. In: K.G. Larsen, S. Skyum, G. Winskel (eds.) Automata, Languages and Programming, Lecture Notes in Computer Science, pp. 820–831. Springer, Berlin, Heidelberg (1998). DOI 10.1007/BFb0055105. URL <https://link.springer.com/chapter/10.1007/BFb0055105>
- [80] Bravyi, S., Harrow, A.W., Hassidim, A.: *Quantum Algorithms for Testing Properties of Distributions*. IEEE Trans. Inf. Theory **57**(6), 3971–3981 (2011). DOI 10.1109/TIT.2011.2134250. URL <https://doi.org/10.1109/TIT.2011.2134250>
- [81] Brennen, G.K., Rohde, P., Sanders, B.C., Singh, S.: *Multiscale quantum simulation of quantum field theory using wavelets*. Phys. Rev. A **92**, 032,315 (2015). DOI 10.1103/PhysRevA.92.032315. URL <https://link.aps.org/doi/10.1103/PhysRevA.92.032315>

- [82] Bshouty, N.H., Jackson, J.C.: *Learning DNF over the Uniform Distribution Using a Quantum Example Oracle*. SIAM J. Comput. **28**(3), 1136–1153 (1998). DOI 10.1137/S0097539795293123. URL <https://doi.org/10.1137/S0097539795293123>
- [83] Buhrman, H., Spalek, R.: *Quantum verification of matrix products*. In: Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2006, Miami, Florida, USA, January 22-26, 2006, pp. 880–889. ACM Press (2006). URL <http://dl.acm.org/citation.cfm?id=1109557.1109654>
- [84] Burton, B.A., Maria, C., Spreer, J.: *Algorithms and complexity for Turaev–Viro invariants*. J. Appl. Comput. Topol. **2**(1), 33–53 (2018). DOI 10.1007/s41468-018-0016-2. URL <https://doi.org/10.1007/s41468-018-0016-2>
- [85] Byrnes, T., Yamamoto, Y.: *Simulating lattice gauge theories on a quantum computer*. Phys. Rev. A **73**, 022,328 (2006). DOI 10.1103/PhysRevA.73.022328. URL <https://link.aps.org/doi/10.1103/PhysRevA.73.022328>
- [86] Cade, C., Montanaro, A., Belovs, A.: *Time and space efficient quantum algorithms for detecting cycles and testing bipartiteness*. Quantum Inf. Comput. **18**(1&2), 18–50 (2018). DOI 10.26421/QIC18.1-2-2. URL <https://doi.org/10.26421/QIC18.1-2-2>
- [87] Cai, Y., Lu, X., Jiang, N.: *A Survey on Quantum Image Processing*. Chinese J. Electron. **27**(4), 718–727 (2018). DOI 10.1049/cje.2018.02.012. URL <https://onlinelibrary.wiley.com/doi/abs/10.1049/cje.2018.02.012>
- [88] Calude, C.S., Dinneen, M.J.: *Solving the Broadcast Time Problem Using a D-wave Quantum Computer*, pp. 439–453. Springer International Publishing (2017). DOI 10.1007/978-3-319-33924-5_17. URL https://doi.org/10.1007/978-3-319-33924-5_17
- [89] Candia, R.D., Pedernales, J.S., del Campo, A., Solano, E., Casanova, J.: *Quantum simulation of dissipative processes without reservoir engineering*. Sci. Rep. **5**, 9981 (2015). URL <https://doi.org/10.1038/srep09981>
- [90] Carette, T., Laurière, M., Magniez, F.: *Extended Learning Graphs for Triangle Finding*. In: H. Vollmer, B. Vallée (eds.) 34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany, *LIPICs*, vol. 66, pp. 20:1–20:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2017). DOI 10.4230/LIPICs.STACS.2017.20. URL <https://doi.org/10.4230/LIPICs.STACS.2017.20>
- [91] Castillo, J.O.: *Quantum algorithms for the combinatorial invariants of numerical semigroups*. Ph.D. thesis, Universidad de Sevilla (2019). URL <https://hdl.handle.net/11441/87264>
- [92] Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S.C., Endo, S., Fujii, K., McClean, J.R., Mitarai, K., Yuan, X., Cincio, L., et al.: *Variational quantum algorithms*. Nature Reviews Physics **3**(9), 625–644 (2021). URL <https://doi.org/10.1038/s42254-021-00348-9>
- [93] Cerf, N.J., Grover, L.K., Williams, C.P.: *Nested Quantum Search and NP-Hard Problems*. Appl. Algebra Eng. Commun. Comput. **10**, 311–338 (2000). DOI 10.1007/s002000050134. URL <https://doi.org/10.1007/s002000050134>
- [94] Chakraborty, S., Novo, L., Ambainis, A., Omar, Y.: *Spatial Search by Quantum Walk is Optimal for Almost all Graphs*. Phys. Rev. Lett. **116**(10), 100,501 (2016). DOI 10.1103/PhysRevLett.116.100501. URL <https://link.aps.org/doi/10.1103/PhysRevLett.116.100501>
- [95] Chalumuri, A., Kune, R., Manoj, B.S.: *A hybrid classical-quantum approach for multi-class classification*. Quantum Inf. Process. **20**(3), 119 (2021). DOI 10.1007/s11128-021-03029-9. URL <https://doi.org/10.1007/s11128-021-03029-9>
- [96] Chamon, C., Mucciolo, E.R.: *Virtual Parallel Computing and a Search Algorithm Using Matrix Product States*. Phys. Rev. Lett. **109**(3), 030,503 (2012). DOI 10.1103/PhysRevLett.109.030503. URL <https://link.aps.org/doi/10.1103/PhysRevLett.109.030503>

- [97] Cheng, Q.: *Primality Proving via One Round in ECPP and One Iteration in AKS*. In: D. Boneh (ed.) *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, Lecture Notes in Computer Science*, vol. 2729, pp. 338–348. Springer (2003). DOI 10.1007/978-3-540-45146-4_20. URL https://doi.org/10.1007/978-3-540-45146-4_20
- [98] Chi, D.P., Kim, J.S., Lee, S.: *Notes on the hidden subgroup problem on some semi-direct product groups*. arXiv preprint quant-ph/0604172 (2006). URL <http://arxiv.org/abs/quant-ph/0604172>
- [99] Childs, A.M.: *Quantum information processing in continuous time*. Ph.D. thesis, MIT (2004). URL <http://www.math.uwaterloo.ca/~amchilds/papers/thesis.pdf>
- [100] Childs, A.M., van Dam, W.: *Quantum algorithm for a generalized hidden shift problem*. In: N. Bansal, K. Pruhs, C. Stein (eds.) *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2007, New Orleans, Louisiana, USA, January 7-9, 2007*, pp. 1225–1232. SIAM (2007). URL <http://dl.acm.org/citation.cfm?id=1283383.1283515>
- [101] Childs, A.M., van Dam, W.: *Quantum algorithms for algebraic problems*. *Rev. Mod. Phys.* **82**(1), 1–52 (2010). DOI 10.1103/RevModPhys.82.1. URL <https://link.aps.org/doi/10.1103/RevModPhys.82.1>
- [102] Childs, A.M., Eisenberg, J.M.: *Quantum algorithms for subset finding*. *Quantum Inf. Comput.* **5**(7), 593–604 (2005). DOI 10.26421/QIC5.7-7. URL <https://doi.org/10.26421/QIC5.7-7>
- [103] Childs, A.M., Goldstone, J.: *Spatial search by quantum walk*. *Phys. Rev. A* **70**, 022,314 (2004). URL <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.70.022314>
- [104] Childs, A.M., Ivanyos, G.: *Quantum computation of discrete logarithms in semigroups*. *J. Math. Cryptol.* **8**(4), 405–416 (2014). URL <https://doi.org/10.1515/jmc-2013-0038>
- [105] Childs, A.M., Jao, D., Soukharev, V.: *Constructing elliptic curve isogenies in quantum subexponential time*. *J. Math. Cryptol.* **8**(1), 1–29 (2014). DOI 10.1515/jmc-2012-0016. URL <https://doi.org/10.1515/jmc-2012-0016>
- [106] Childs, A.M., Kimmel, S., Kothari, R.: *The Quantum Query Complexity of Read-Many Formulas*. In: L. Epstein, P. Ferragina (eds.) *Algorithms - ESA 2012 - 20th Annual European Symposium, Ljubljana, Slovenia, September 10-12, 2012. Proceedings, Lecture Notes in Computer Science*, vol. 7501, pp. 337–348. Springer (2012). DOI 10.1007/978-3-642-33090-2_30. URL https://doi.org/10.1007/978-3-642-33090-2_30
- [107] Childs, A.M., Kothari, R.: *Quantum query complexity of minor-closed graph properties*. In: T. Schwentick, C. Dürr (eds.) *28th International Symposium on Theoretical Aspects of Computer Science, STACS 2011, March 10-12, 2011, Dortmund, Germany, LIPIcs*, vol. 9, pp. 661–672. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2011). DOI 10.4230/LIPIcs.STACS.2011.661. URL <https://doi.org/10.4230/LIPIcs.STACS.2011.661>
- [108] Childs, A.M., Kothari, R., Somma, R.D.: *Quantum Algorithm for Systems of Linear Equations with Exponentially Improved Dependence on Precision*. *SIAM J. Comput.* **46**(6), 1920–1950 (2017). DOI 10.1137/16M1087072. URL <https://doi.org/10.1137/16M1087072>
- [109] Childs, A.M., Landahl, A.J., Parrilo, P.A.: *Quantum algorithms for the ordered search problem via semidefinite programming*. *Phys. Rev. A* **75**, 032,335 (2007). DOI 10.1103/PhysRevA.75.032335. URL <https://link.aps.org/doi/10.1103/PhysRevA.75.032335>
- [110] Childs, A.M., Lee, T.: *Optimal Quantum Adversary Lower Bounds for Ordered Search*. In: L. Aceto, I. Damgård, L.A. Goldberg, M.M. Halldórsson, A. Ingólfssdóttir, I. Walukiewicz (eds.) *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part I: Track A: Algorithms, Automata, Complexity, and*

- Games, *Lecture Notes in Computer Science*, vol. 5125, pp. 869–880. Springer (2008). DOI 10.1007/978-3-540-70575-8_71. URL https://doi.org/10.1007/978-3-540-70575-8_71
- [111] Childs, A.M., Li, T.: *Efficient simulation of sparse Markovian quantum dynamics*. *Quantum Inform. Compu.* **17**(11-12), 901–947 (2017). URL <https://doi.org/10.26421/QIC17.11-12>
- [112] Childs, A.M., Liu, J.P.: *Quantum Spectral Methods for Differential Equations*. *Comm. Math. Phys.* **375**, 1427–1457 (2019). URL <https://doi.org/10.1007/s00220-020-03699-z>
- [113] Childs, A.M., Liu, J.P., Ostrander, A.: *High-precision quantum algorithms for partial differential equations*. *Quantum* **5**, 574 (2021). DOI 10.22331/q-2021-11-10-574. URL <https://doi.org/10.22331/q-2021-11-10-574>
- [114] Childs, A.M., Schulman, L.J., Vazirani, U.V.: *Quantum algorithms for hidden nonlinear structures*. In: *Proceedings of the 48th IEEE Symposium on Foundations of Computer Science*, pp. 395–404 (2007). URL <https://doi.org/10.1109/FOCS.2007.18>
- [115] Childs, A.M., Su, Y., Tran, M.C., Wiebe, N., Zhu, S.: *Theory of Trotter Error with Commutator Scaling*. *Phys. Rev. X* **11**, 011,020 (2021). DOI 10.1103/PhysRevX.11.011020. URL <https://link.aps.org/doi/10.1103/PhysRevX.11.011020>
- [116] Childs, A.M., Wiebe, N.: *Hamiltonian simulation using linear combinations of unitary operations*. *Quantum Inf. Comput.* **12**(11-12), 901–924 (2012). DOI 10.26421/QIC12.11-12-1. URL <https://doi.org/10.26421/QIC12.11-12-1>
- [117] Choi, M.S.: *A Quantum Computation Workbook*. Springer (2022). URL <https://link.springer.com/book/10.1007/978-3-030-91214-7>
- [118] Chowdhury, A.N., Somma, R.D.: *Quantum algorithms for Gibbs sampling and hitting-time estimation*. *Quantum Inform. Compu.* **17**(1-2), 41–64 (2017). URL <https://dl.acm.org/doi/abs/10.5555/3179483.3179486>
- [119] Clader, B.D., Jacobs, B.C., Sprouse, C.R.: *Preconditioned Quantum Linear System Algorithm*. *Phys. Rev. Lett.* **110**, 250,504 (2013). DOI 10.1103/PhysRevLett.110.250504. URL <https://link.aps.org/doi/10.1103/PhysRevLett.110.250504>
- [120] Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: *Proposed Experiment to Test Local Hidden-Variable Theories*. *Phys. Rev. Lett.* **23**, 880–884 (1969). DOI 10.1103/PhysRevLett.23.880. URL <https://doi.org/10.1103/PhysRevLett.23.880>
- [121] Cleve, R., Gavinsky, D., Yonge-Mallo, D.L.: *Quantum algorithms for evaluating min-max trees*. In: *Workshop on Quantum Computation, Communication, and Cryptography*, pp. 11–15. Springer (2008). URL https://doi.org/10.1007/978-3-540-89304-2_2
- [122] Cleve, R., Wang, C.: *Efficient Quantum Algorithms for Simulating Lindblad Evolution*. In: I. Chatzigiannakis, P. Indyk, F. Kuhn, A. Muscholl (eds.) *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10–14, 2017, Warsaw, Poland, LIPIcs*, vol. 80, pp. 17:1–17:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2017). DOI 10.4230/LIPIcs.ICALP.2017.17. URL <https://doi.org/10.4230/LIPIcs.ICALP.2017.17>
- [123] Combarro, E.F., Ranilla, J., Rúa, I.F.: *Experiments testing the commutativity of finite-dimensional algebras with a quantum adiabatic algorithm*. *Comput. Math. Methods* **1**(1), e1009 (2019). DOI 10.1002/cmm4.1009. URL <https://onlinelibrary.wiley.com/doi/abs/10.1002/cmm4.1009>
- [124] Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: *Introduction to algorithms*. MIT press (2022). URL <http://mitpress.mit.edu/9780262046305/introduction-to-algorithms/>

- [125] Cornwell, D.J.: *Amplified quantum transforms*. Phd thesis, University of Maryland, Baltimore County (2014). URL <https://www.proquest.com/docview/1553207994?pq-origsite=gscholar&fromopenview=true>
- [126] Cosme, C.M.M., Portugal, R.: *Quantum algorithm for the hidden subgroup problem on a class of semidirect product groups*. arXiv preprint quant-ph/0703223 (2007). URL <http://arxiv.org/abs/quant-ph/0703223>
- [127] Costa, P.C.S., Jordan, S., Ostrander, A.: *Quantum algorithm for simulating the wave equation*. Phys. Rev. A **99**, 012,323 (2019). DOI 10.1103/PhysRevA.99.012323. URL <https://link.aps.org/doi/10.1103/PhysRevA.99.012323>
- [128] Cotler, J., Huang, H.Y., McClean, J.R.: *Revisiting dequantization and quantum advantage in learning tasks*. arXiv preprint arXiv:2112.00811 (2021). URL <http://arxiv.org/abs/2112.00811>
- [129] Crawford, D., Levit, A., Ghadermarzy, N., Oberoi, J.S., Ronagh, P.: *Reinforcement learning using quantum Boltzmann machines*. Quantum Inf. Comput. **18**(1&2), 51–74 (2018). DOI 10.26421/QIC18.1-2-3. URL <https://doi.org/10.26421/QIC18.1-2-3>
- [130] Cross, A.W., Smith, G., Smolin, J.A.: *Quantum learning robust against noise*. Phys. Rev. A **92**, 012,327 (2015). DOI 10.1103/PhysRevA.92.012327. URL <https://link.aps.org/doi/10.1103/PhysRevA.92.012327>
- [131] Cui, L., Wu, Z., Xiang, H.: *Quantum radial basis function method for the Poisson equation*. J. Phys. A: Math. Theor. **56**(22), 225,303 (2023). DOI 10.1088/1751-8121/acce83. URL <https://dx.doi.org/10.1088/1751-8121/acce83>
- [132] van Dam, W.: *Quantum Algorithms for Weighing Matrices and Quadratic Residues*. Algorithmica **34**(4), 413–428 (2002). DOI 10.1007/s00453-002-0975-4. URL <https://doi.org/10.1007/s00453-002-0975-4>
- [133] van Dam, W., Hallgren, S.: *Efficient Quantum Algorithms for Shifted Quadratic Character Problems*. CoRR **quant-ph/0011067** (2000). URL <http://arxiv.org/abs/quant-ph/0011067>
- [134] van Dam, W., Hallgren, S., Ip, L.: *Quantum Algorithms for Some Hidden Shift Problems*. SIAM J. Comput. **36**(3), 763–778 (2006). DOI 10.1137/S009753970343141X. URL <https://doi.org/10.1137/S009753970343141X>
- [135] van Dam, W., Sasaki, Y.: *Quantum algorithms for problems in number theory, algebraic geometry, and group theory*. Diversities in Quantum Computation and Quantum Information pp. 79–105 (2013). URL https://doi.org/10.1142/9789814425988_0003
- [136] Decker, T., Draisma, J., Wocjan, P.: *Efficient quantum algorithm for identifying hidden polynomials*. Quantum Inform. Compu. **9**(3), 215–230 (2009). URL <https://dl.acm.org/doi/abs/10.5555/2011781.2011784>
- [137] Decker, T., Høyer, P., Ivanyos, G., Santha, M.: *Polynomial time quantum algorithms for certain bivariate hidden polynomial problems*. Quantum Inf. Comput. **14**(9-10), 790–806 (2014). DOI 10.26421/QIC14.9-10-6. URL <https://doi.org/10.26421/QIC14.9-10-6>
- [138] DeLorenzo, K., Kimmel, S., Witter, R.T.: *Applications of the Quantum Algorithm for st-Connectivity*. In: 14th Conference on the Theory of Quantum Computation, Communication and Cryptography, p. 33 (2019). URL <https://doi.org/10.4230/LIPIcs.TQC.2019.6>
- [139] Denchev, V.S., Ding, N., Vishwanathan, S.V.N., Neven, H.: *Robust Classification with Adiabatic Quantum Optimization*. In: Proceedings of the 29th International Conference on International Conference on Machine Learning, ICML'12, p. 1003–1010. Omnipress, Madison, WI, USA (2012). URL <https://icml.cc/2012/papers/461.pdf>

- [140] Denney, A., Moore, C., Russell, A.: *Finding conjugate stabilizer subgroups in $PSL(2; q)$ and related groups*. Quantum Inform. Compu. **10**(3), 282–291 (2010). URL <https://dl.acm.org/doi/abs/10.5555/2011350.2011358>
- [141] Deutsch, D.: *Quantum theory, the Church-Turing principle, and the universal quantum computer*. Proc. R. Soc. London, Ser. A **400**, 97–117 (1985). URL <https://doi.org/10.1098/rspa.1985.0070>
- [142] Deutsch, D., Jozsa, R.: *Rapid solution of problems by quantum computation*. Proc. R. Soc. London, Ser. A **493**, 553–558 (1992). URL <https://doi.org/10.1098/rspa.1992.0167>
- [143] Di Matteo, O., McCoy, A., Gysbers, P., Miyagi, T., Woloshyn, R.M., Navrátil, P.: *Improving Hamiltonian encodings with the Gray code*. Phys. Rev. A **103**, 042,405 (2021). DOI 10.1103/PhysRevA.103.042405. URL <https://link.aps.org/doi/10.1103/PhysRevA.103.042405>
- [144] Djordjevic, I.B.: *Quantum information processing, quantum computing, and quantum error correction: an engineering approach*. Academic Press (2021)
- [145] Dong, D., Chen, C., Chen, Z.: *Quantum Reinforcement Learning*. In: L. Wang, K. Chen, Y. Ong (eds.) *Advances in Natural Computation, First International Conference, ICNC 2005, Changsha, China, August 27–29, 2005, Proceedings, Part II, Lecture Notes in Computer Science*, vol. 3611, pp. 686–689. Springer (2005). DOI 10.1007/11539117. URL <https://doi.org/10.1007/11539117>
- [146] Donis-Vela, A., García-Escartín, J.C.: *A quantum primality test with order finding*. Quantum Inf. Comput. **18**(13&14), 1143–1151 (2018). DOI 10.26421/QIC18.13-14-5. URL <https://doi.org/10.26421/QIC18.13-14-5>
- [147] Dooms, A., Emerencia, C., Lemmens, A.: *Shaping Post-Quantum Cryptography: The Hidden Subgroup and Shift Problems*. IEEE BITS the Information Theory Magazine pp. 1–12 (2023). DOI 10.1109/MBITS.2023.3275885. URL <https://ieeexplore.ieee.org/abstract/document/10124284>
- [148] Dörn, S., Thierauf, T.: *The quantum query complexity of the determinant*. Inf. Process. Lett. **109**(6), 325–328 (2009). DOI 10.1016/j.ipl.2008.11.006. URL <https://doi.org/10.1016/j.ipl.2008.11.006>
- [149] Duan, B., Yuan, J., Yu, C.H., Huang, J., Hsieh, C.Y.: *A survey on HHL algorithm: From theory to application in quantum machine learning*. Phys. Lett. A **384**(24), 126,595 (2020). DOI 10.1016/j.physleta.2020.126595. URL <https://www.sciencedirect.com/science/article/pii/S037596012030462X>
- [150] Dunjko, V., Briegel, H.J.: *Machine learning & artificial intelligence in the quantum domain: a review of recent progress*. Rep. Prog. Phys. **81**(7), 074,001 (2018). DOI 10.1088/1361-6633/aab406. URL <https://dx.doi.org/10.1088/1361-6633/aab406>
- [151] Dunjko, V., Taylor, J.M., Briegel, H.J.: *Quantum-Enhanced Machine Learning*. Phys. Rev. Lett. **117**, 130,501 (2016). DOI 10.1103/PhysRevLett.117.130501. URL <https://link.aps.org/doi/10.1103/PhysRevLett.117.130501>
- [152] Dunjko, V., Wittek, P.: *A non-review of Quantum Machine Learning: trends and explorations*. Quantum Views **4**, 32 (2020). DOI 10.22331/qv-2020-03-17-32. URL <https://quantum-journal.org/views/qv-2020-03-17-32/>
- [153] Dürr, C., Heiligman, M., Høyer, P., Mhalla, M.: *Quantum Query Complexity of Some Graph Problems*. SIAM J. Comput. **35**(6), 1310–1328 (2006). DOI 10.1137/050644719. URL <https://doi.org/10.1137/050644719>
- [154] Durr, C., Hoyer, P.: *A quantum algorithm for finding the minimum*. arXiv preprint quant-ph/9607014 (1996). URL <http://arxiv.org/abs/quant-ph/9607014>
- [155] Egger, D.J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., Simonetto, A., Woerner, S., Yndurain, E.: *Quantum Computing for Finance: State-of-the-Art and Future*

- Prospects*. IEEE Trans. Quantum Eng. **1**, 1–24 (2020). DOI 10.1109/TQE.2020.3030314. URL <https://ieeexplore.ieee.org/abstract/document/9222275>
- [156] Eisenträger, K., Hallgren, S., Kitaev, A.Y., Song, F.: *A quantum algorithm for computing the unit group of an arbitrary degree number field*. In: D.B. Shmoys (ed.) Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014, pp. 293–302. ACM (2014). DOI 10.1145/2591796.2591860. URL <https://doi.org/10.1145/2591796.2591860>
- [157] Ekerå, M.: *On post-processing in the quantum algorithm for computing short discrete logarithms*. Des. Codes Cryptogr. **88**(11), 2313–2335 (2020). DOI 10.1007/s10623-020-00783-2. URL <https://eprint.iacr.org/2017/1122>
- [158] Emmanoulopoulos, D., Dimoska, S.: *Quantum machine learning in finance: Time series forecasting*. arXiv preprint arXiv:2202.00599 (2022). URL <http://arxiv.org/abs/2202.00599>
- [159] Epping, T., Hochstättler, W., Oertel, P.: *Complexity results on a paint shop problem*. Discrete Appl. Math. **136**(2), 217–226 (2004). DOI 10.1016/S0166-218X(03)00442-6. URL <https://www.sciencedirect.com/science/article/pii/S0166218X03004426>
- [160] Ettinger, M., Høyer, P., Knill, E.: *The quantum query complexity of the hidden subgroup problem is polynomial*. Inf. Process. Lett. **91**(1), 43–48 (2004). DOI 10.1016/j.ipl.2004.01.024. URL <https://doi.org/10.1016/j.ipl.2004.01.024>
- [161] Failde, D., Viqueira, J.D., Juane, M.M., Gómez, A.: *Using Differential Evolution to Avoid Local Minima in Variational Quantum Algorithms*. arXiv preprint arXiv:2303.12186 (2023). URL <https://doi.org/10.48550/arXiv.2303.12186>
- [162] Farhi, E., Goldstone, J., Gutmann, S.: *A quantum approximate optimization algorithm*. arXiv preprint arXiv:1411.4028 (2014). URL <http://arxiv.org/abs/1411.4028>
- [163] Farhi, E., Goldstone, J., Gutmann, S., Lapan, J., Lundgren, A., Preda, D.: *A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem*. Science **292**(5516), 472–475 (2001). DOI 10.1126/science.1057726. URL <https://www.science.org/doi/abs/10.1126/science.1057726>
- [164] Farhi, E., Goldstone, J., Gutmann, S., Sipser, M.: *Invariant quantum algorithms for insertion into an ordered list*. arXiv preprint quant-ph/9901059 (1999). URL <https://arxiv.org/abs/quant-ph/9901059>
- [165] Farhi, E., Goldstone, J., Gutmann, S., Sipser, M.: *Quantum computation by adiabatic evolution*. arXiv preprint quant-ph/0001106 (2000). URL <https://doi.org/10.48550/arXiv.quant-ph/0001106>
- [166] Farhi, E., Gosset, D., Hen, I., Sandvik, A.W., Shor, P., Young, A.P., Zamponi, F.: *Performance of the quantum adiabatic algorithm on random instances of two optimization problems on regular hypergraphs*. Phys. Rev. A **86**, 052334 (2012). DOI 10.1103/PhysRevA.86.052334. URL <https://link.aps.org/doi/10.1103/PhysRevA.86.052334>
- [167] Farhi, E., Harrow, A.W.: *Quantum supremacy through the quantum approximate optimization algorithm*. arXiv preprint arXiv:1602.07674 (2016). URL <https://arxiv.org/abs/1602.07674>
- [168] Farhi, E., Kimmel, S., Temme, K.: *A quantum version of Schoning’s algorithm applied to quantum 2-SAT*. Quantum Inf. Comput. **16**(13&14), 1212–1227 (2016). DOI 10.26421/QIC16.13-14-7. URL <https://doi.org/10.26421/QIC16.13-14-7>
- [169] Farhi, E., Neven, H.: *Classification with quantum neural networks on near term processors*. arXiv preprint arXiv:1802.06002 (2018). URL <https://doi.org/10.48550/arXiv.1802.06002>
- [170] Fedorov, A., Gisin, N., Belousov, S., Lvovsky, A.: *Quantum computing at the quantum advantage threshold: a down-to-business review*. arXiv preprint arXiv:2203.17181 (2022). URL <http://arxiv.org/abs/2203.17181>

- [171] Feynman, R.P.: *Simulating physics with computers*. Int. J. Theor. Phys. **21**(6/7), 467–488 (1982)
- [172] Fillion-Gourdeau, F.m.c., MacLean, S., Laflamme, R.: *Algorithm for the solution of the Dirac equation on digital quantum computers*. Phys. Rev. A **95**, 042,343 (2017). DOI 10.1103/PhysRevA.95.042343. URL <https://link.aps.org/doi/10.1103/PhysRevA.95.042343>
- [173] Fluhrer, S.: *Quantum Cryptanalysis of NTRU*. Cryptology ePrint Archive **2015/676** (2015). URL <https://eprint.iacr.org/2015/676>
- [174] Freedman, M., Kitaev, A., Wang, Z.: *Simulation of topological field theories by quantum computers*. Comm. Math. Phys. **227**, 587–603 (2002). URL <https://link.springer.com/article/10.1007/s002200200635>
- [175] Freedman, M., Larsen, M., Wang, Z.: *A modular functor which is universal for quantum computation*. Comm. Math. Phys. **227**, 605–622 (2002). URL <https://link.springer.com/article/10.1007/s002200200645>
- [176] Friedl, K., Ivanyos, G., Magniez, F., Santha, M., Sen, P.: *Hidden Translation and Translating Coset in Quantum Computing*. SIAM J. Comput. **43**(1), 1–24 (2014). DOI 10.1137/130907203. URL <https://doi.org/10.1137/130907203>
- [177] García, D.P., Cruz-Benito, J., García-Peñalvo, F.J.: *Systematic literature review: Quantum machine learning and its applications*. arXiv preprint arXiv:2201.04093 (2022). URL <https://doi.org/10.48550/arXiv.2201.04093>
- [178] García, A., Gaspar, V., Jordán, J., Moreno, A., Gil, G.: *Spain Quantum Industry Report 2023*. Ametic (2023). URL <https://www.investinspain.org/content/icex-invest/en/publicaciones/ametic-report.html>
- [179] Garnerone, S., Marzuoli, A., Rasetti, M.: *Efficient quantum processing of 3-manifold topological invariants*. Adv. Theor. Math. Phys. **13**(6), 1601–1652 (2009). URL <https://dx.doi.org/10.4310/ATMP.2009.v13.n6.a1>
- [180] Gavinsky, D.: *Quantum Solution to the Hidden Subgroup Problem for Poly-near-Hamiltonian Groups*. Quantum Info. Comput. **4**(3), 229–235 (2004). URL <https://dl.acm.org/doi/abs/10.5555/2011617.2011625>
- [181] Gavinsky, D., Roetteler, M., Roland, J.: *Quantum Algorithm for the Boolean Hidden Shift Problem*. In: B. Fu, D. Du (eds.) Computing and Combinatorics - 17th Annual International Conference, COCOON 2011, Dallas, TX, USA, August 14-16, 2011. Proceedings, *Lecture Notes in Computer Science*, vol. 6842, pp. 158–167. Springer (2011). DOI 10.1007/978-3-642-22685-4_14. URL https://doi.org/10.1007/978-3-642-22685-4_14
- [182] Ge, Y., Molnár, A., Cirac, J.I.: *Rapid Adiabatic Preparation of Injective Projected Entangled Pair States and Gibbs States*. Phys. Rev. Lett. **116**, 080,503 (2016). DOI 10.1103/PhysRevLett.116.080503. URL <https://link.aps.org/doi/10.1103/PhysRevLett.116.080503>
- [183] Gill, S.S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., Buyya, R.: *Quantum computing: A taxonomy, systematic review and future directions*. Software: Practice and Experience **52**(1), 66–114 (2022). DOI 10.1002/spe.3039. URL <https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.3039>
- [184] Gilyén, A., Su, Y., Low, G.H., Wiebe, N.: *Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics*. In: M. Charikar, E. Cohen (eds.) Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019, pp. 193–204. ACM (2019). DOI 10.1145/3313276.3316366. URL <https://doi.org/10.1145/3313276.3316366>
- [185] Giri, P.R., Korepin, V.E.: *A review on quantum search algorithms*. Quantum Inf. Process. **16**(12), 315 (2017). DOI 10.1007/s11128-017-1768-7. URL <https://doi.org/10.1007/s11128-017-1768-7>

- [186] Girvin, S.M.: *Introduction to quantum error correction and fault tolerance*. SciPost Physics Lecture Notes p. 070 (2023). DOI 10.21468/SciPostPhysLectNotes.70. URL https://www.scipost.org/SciPostPhysLectNotes.70?acad_field_slug=all
- [187] Goldberg, A.V., Rao, S.: *Beyond the flow decomposition barrier*. J. ACM **45**(5), 783–797 (1998). DOI 10.1145/290179.290181. URL <https://dl.acm.org/doi/10.1145/290179.290181>
- [188] Gómez, A., Leitao, Á., Manzano, A., Musso, D., Nogueiras, M.R., Ordóñez, G., Vázquez, C.: *A Survey on Quantum Computational Finance for Derivatives Pricing and VaR*. Arch. Comput. Methods Eng. **29**(6), 4137–4163 (2022). DOI 10.1007/s11831-022-09732-9. URL <https://doi.org/10.1007/s11831-022-09732-9>
- [189] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: *Applying Grover’s Algorithm to AES: Quantum Resource Estimates*. In: T. Takagi (ed.) Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24–26, 2016, Proceedings, *Lecture Notes in Computer Science*, vol. 9606, pp. 29–43. Springer (2016). DOI 10.1007/978-3-319-29360-8_3. URL https://doi.org/10.1007/978-3-319-29360-8_3
- [190] Grice, J.R., Meyer, D.A.: *A quantum algorithm for Viterbi decoding of classical convolutional codes*. Quantum Inf. Process. **14**(7), 2307–2321 (2015). DOI 10.1007/s11128-015-1003-3. URL <https://doi.org/10.1007/s11128-015-1003-3>
- [191] Grover, L.K.: *A fast quantum mechanical algorithm for database search*. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212–219 (1996). URL <https://dl.acm.org/doi/pdf/10.1145/237814.237866>
- [192] Grover, L.K.: *Quantum mechanics helps in searching for a needle in a haystack*. Phys. Rev. Lett. **79**(2), 325–328 (1997). URL <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.79.325>
- [193] Grover, L.K.: *From Schrödinger’s equation to the quantum search algorithm*. Amer. J. Phys. **69**(7), 769–777 (2001). URL <https://doi.org/10.1007/s12043-001-0128-3>
- [194] Grover, L.K.: *Fixed-point quantum search*. Phys. Rev. Lett. **95**, 150501 (2005). URL <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.95.150501>
- [195] Guerreschi, G.G., Matsuura, A.Y.: *QAOA for Max-Cut requires hundreds of qubits for quantum speed-up*. Sci. Rep. **9**(1), 6903 (2019). DOI 10.1038/s41598-019-43176-9. URL <https://www.nature.com/articles/s41598-019-43176-9>
- [196] Gyongyosi, L., Imre, S.: *A Survey on quantum computing technology*. Comput. Sci. Rev. **31**, 51–71 (2019). DOI 10.1016/j.cosrev.2018.11.002. URL <https://www.sciencedirect.com/science/article/pii/S1574013718301709>
- [197] Gyurik, C., Cade, C., Dunjko, V.: *Towards quantum advantage via topological data analysis*. Quantum **6**, 855 (2022). URL <https://doi.org/10.22331/q-2022-11-10-855>
- [198] Hales, L., Hallgren, S.: *An Improved Quantum Fourier Transform Algorithm and Applications*. In: 41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12–14 November 2000, Redondo Beach, California, USA, pp. 515–525. IEEE Computer Society (2000). DOI 10.1109/SFCS.2000.892139. URL <https://doi.org/10.1109/SFCS.2000.892139>
- [199] Hallgren, S.: *Fast quantum algorithms for computing the unit group and class group of a number field*. In: H.N. Gabow, R. Fagin (eds.) Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22–24, 2005, pp. 468–474. ACM (2005). DOI 10.1145/1060590.1060660. URL <https://doi.org/10.1145/1060590.1060660>
- [200] Hallgren, S., Russell, A., Ta-Shma, A.: *Normal subgroup reconstruction and quantum computation using group representations*. In: F.F. Yao, E.M. Luks (eds.) Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21–23, 2000, Portland, OR, USA, pp. 627–635. ACM (2000). DOI 10.1145/335305.335392. URL <https://doi.org/10.1145/335305.335392>

- [201] Hamed Moosavian, A., Jordan, S.: *Faster quantum algorithm to simulate fermionic quantum field theory*. Phys. Rev. A **98**, 012,332 (2018). DOI 10.1103/PhysRevA.98.012332. URL <https://link.aps.org/doi/10.1103/PhysRevA.98.012332>
- [202] Harrow, A.W., Hassidim, A., Lloyd, S.: *Quantum Algorithm for Linear Systems of Equations*. Phys. Rev. Lett. **103**, 150,502 (2009). DOI 10.1103/PhysRevLett.103.150502. URL <https://link.aps.org/doi/10.1103/PhysRevLett.103.150502>
- [203] Harrow, A.W., Rosenbaum, D.J.: *Uselessness for an Oracle model with internal randomness*. Quantum Inf. Comput. **14**(7-8), 608–624 (2014). DOI 10.26421/QIC14.7-8-5. URL <https://doi.org/10.26421/QIC14.7-8-5>
- [204] Harvey, D., Hoeven, J.v.D.: *Integer multiplication in time $O(n \log n)$* . Ann. of Math. (2) (2021). DOI 10.4007/annals.2021.193.2.4. URL <https://hal.science/hal-02070778>
- [205] Hastings, M.B., Wecker, D., Bauer, B., Troyer, M.: *Improving quantum algorithms for quantum chemistry*. Quantum Inf. Comput. **15**(1-2), 1–21 (2015). DOI 10.26421/QIC15.1-2-1. URL <https://doi.org/10.26421/QIC15.1-2-1>
- [206] Hayakawa, R.: *Quantum algorithm for persistent Betti numbers and topological data analysis*. Quantum **6**, 873 (2022). URL <https://quantum-journal.org/papers/q-2022-12-07-873/>
- [207] Heim, B., Rønnow, T.F., Isakov, S.V., Troyer, M.: *Quantum versus classical annealing of Ising spin glasses*. Science **348**(6231), 215–217 (2015). DOI 10.1126/science.aaa4170. URL <https://www.science.org/doi/10.1126/science.aaa4170>
- [208] Herman, D., Googin, C., Liu, X., Galda, A., Safro, I., Sun, Y., Pistoia, M., Alexeev, Y.: *A survey of quantum computing for finance*. arXiv preprint arXiv:2201.02773 (2022). URL <https://doi.org/10.48550/arXiv.2201.02773>
- [209] Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., Pistoia, M., Alexeev, Y.: *Quantum computing for finance*. Nature Reviews Physics pp. 1–16 (2023). DOI 10.1038/s42254-023-00603-1. URL <https://www.nature.com/articles/s42254-023-00603-1>
- [210] Hidary, J.D., Hidary, J.D.: *Quantum computing: an applied approach*. Springer (2019). URL <https://link.springer.com/book/10.1007/978-3-030-23922-0>
- [211] Hoefler, T., Häner, T., Troyer, M.: *Disentangling hype from practicality: on realistically achieving quantum advantage*. Commun. ACM **66**(5), 82–87 (2023). URL <https://doi.org/10.1145/3571725>
- [212] Hoofnagle, C.J., Garfinkel, S.: *Law and Policy for the Quantum Age*. SSRN **4007638** (2022). DOI 10.2139/ssrn.4007638. URL <https://papers.ssrn.com/abstract=4007638>
- [213] Hoyer, P., Komeili, M.: *Efficient Quantum Walk on the Grid with Multiple Marked Elements*. In: H. Vollmer, B. Vallée (eds.) 34th Symposium on Theoretical Aspects of Computer Science (STACS 2017), *Leibniz International Proceedings in Informatics (LIPIcs)*, vol. 66, pp. 42:1–42:14. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany (2017). DOI 10.4230/LIPIcs.STACS.2017.42. URL <http://drops.dagstuhl.de/opus/volltexte/2017/6990>
- [214] Høyer, P., Neerbek, J., Shi, Y.: *Quantum complexities of ordered searching, sorting, and element distinctness*. In: Proceedings of ICALP, pp. 429–448 (2002). URL https://doi.org/10.1007/3-540-48224-5_29
- [215] Huang, Y., Lei, H., Li, X., Zhu, Q., Ren, W., Liu, X.: *Quantum Generative Model with Variable-Depth Circuit*. Computers, Materials & Continua **65**(1), 445–458 (2020). DOI 10.32604/cmc.2020.010390. URL <http://www.techscience.com/cmc/v65n1/39576>
- [216] Inui, Y., Gall, F.L.: *Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups*. Quantum Inform. Compu. **7**(5), 559–570 (2007). URL <https://dl.acm.org/doi/abs/10.5555/2011832.2011841>

- [217] Itakura, Y.K.: *Quantum algorithm for commutativity testing of a matrix set*. arXiv preprint quant-ph/0509206 (2005). URL <http://arxiv.org/abs/quant-ph/0509206>
- [218] Ivanyos, G., Magniez, F., Santha, M.: *Efficient Quantum Algorithms For Some Instances Of The Non-Abelian Hidden Subgroup Problem*. Int. J. Found. Comput. Sci. **14**(5), 723–740 (2003). DOI 10.1142/S0129054103001996. URL <https://doi.org/10.1142/S0129054103001996>
- [219] Ivanyos, G., Sanselme, L., Santha, M.: *An Efficient Quantum Algorithm for the Hidden Subgroup Problem in Extraspecial Groups*. In: W. Thomas, P. Weil (eds.) STACS 2007, 24th Annual Symposium on Theoretical Aspects of Computer Science, Aachen, Germany, February 22–24, 2007, Proceedings, *Lecture Notes in Computer Science*, vol. 4393, pp. 586–597. Springer (2007). DOI 10.1007/978-3-540-70918-3_50. URL https://doi.org/10.1007/978-3-540-70918-3_50
- [220] Ivanyos, G., Sanselme, L., Santha, M.: *An Efficient Quantum Algorithm for the Hidden Subgroup Problem in Nil-2 Groups*. In: E.S. Laber, C.F. Bornstein, L.T. Nogueira, L. Faria (eds.) LATIN 2008: Theoretical Informatics, 8th Latin American Symposium, Búzios, Brazil, April 7–11, 2008, Proceedings, *Lecture Notes in Computer Science*, vol. 4957, pp. 759–771. Springer (2008). DOI 10.1007/978-3-540-78773-0_65. URL https://doi.org/10.1007/978-3-540-78773-0_65
- [221] Jahangiri, S., Arrazola, J.M., Quesada, N., Delgado, A.: *Quantum algorithm for simulating molecular vibrational excitations*. Phys. Chem. Chem. Phys. **22**, 25,528–25,537 (2020). DOI 10.1039/D0CP03593A. URL <http://dx.doi.org/10.1039/D0CP03593A>
- [222] Janmark, J., Meyer, D.A., Wong, T.G.: *Global symmetry is unnecessary for fast quantum search*. Phys. Rev. Lett. **112**(21), 210,502 (2014). URL <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.112.210502>
- [223] Jin, S., Liu, N.: *Quantum algorithms for computing observables of nonlinear partial differential equations*. arXiv preprint arXiv:2202.07834 (2022). URL <https://arxiv.org/abs/2202.07834>
- [224] Jordan, S.P., Lee, K.S., Preskill, J.: *Quantum algorithms for quantum field theories*. Science **336**(6085), 1130–1133 (2012). URL <https://doi.org/10.1126/science.1217069>
- [225] Jordan, S.P., Lee, K.S., Preskill, J.: *Quantum algorithms for fermionic quantum field theories*. arXiv preprint arXiv:1404.7115 (2014). URL <https://doi.org/10.48550/arXiv.1404.7115>
- [226] Jordan, S.P., Lee, K.S.M., Preskill, J.: *Quantum simulation of scattering in scalar quantum field theories*. Proc. Spie. **14**(11/12), 1014–1080 (2014). URL <https://dl.acm.org/doi/abs/10.5555/2685155.2685163>
- [227] Joseph, A., White, T., Chandra, V., McGuigan, M.: *Quantum Computing of Schwarzschild-de Sitter Black Holes and Kantowski-Sachs Cosmology*. arXiv preprint arXiv:2202.09906 (2022). URL <https://doi.org/10.48550/arXiv.2202.09906>
- [228] Kadian, K., Garhwal, S., Kumar, A.: *Quantum walk and its application domains: A systematic review*. Comput. Sci. Rev. **41**, 100,419 (2021). DOI 10.1016/j.cosrev.2021.100419. URL <https://www.sciencedirect.com/science/article/pii/S1574013721000599>
- [229] Kahn, J., Saks, M., Sturtevant, D.: *A topological approach to evasiveness*. Combinatorica **4**(4), 297–306 (1984). DOI 10.1007/BF02579140. URL <https://doi.org/10.1007/BF02579140>
- [230] Kaplan, M.: *Quantum attacks against iterated block ciphers*. Mat. Vopr. Kriptogr. **7**(2), 71–90 (2016). DOI 10.4213/mvk185. URL <http://mi.mathnet.ru/mvk185>
- [231] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: *Breaking Symmetric Cryptosystems Using Quantum Period Finding*. In: M. Robshaw, J. Katz (eds.) Advances in Cryptology – CRYPTO 2016, Lecture Notes in Computer Science, pp. 207–237. Springer, Berlin, Heidelberg

- (2016). DOI 10.1007/978-3-662-53008-5_8. URL https://link.springer.com/chapter/10.1007/978-3-662-53008-5_8
- [232] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: *Quantum Differential and Linear Cryptanalysis*. IACR Trans. Symmetric Cryptol. **2016**(1), 71–94 (2016). DOI 10.13154/tosc.v2016.i1.71-94. URL <https://doi.org/10.13154/tosc.v2016.i1.71-94>
- [233] Kapoor, A., Wiebe, N., Svore, K.M.: *Quantum Perceptron Models*. In: D.D. Lee, M. Sugiyama, U. von Luxburg, I. Guyon, R. Garnett (eds.) *Advances in Neural Information Processing Systems 29: Annual Conference on Neural Information Processing Systems 2016*, December 5–10, 2016, Barcelona, Spain, pp. 3999–4007 (2016). URL <https://proceedings.neurips.cc/paper/2016/hash/d47268e9db2e9aa3827bba3afb7ff94a-Abstract.html>
- [234] Kassal, I., Aspuru-Guzik, A.: *Quantum algorithm for molecular properties and geometry optimization*. J. Chem. Phys. **131**(22) (2009). URL <https://doi.org/10.1063/1.3266959>
- [235] Kassal, I., Jordan, S.P., Love, P.J., Mohseni, M., Aspuru-Guzik, A.: *Quantum algorithms for the simulation of chemical dynamics*. Proc. Natl. Acad. Sci. **105**, 18,681 (2008). URL <https://doi.org/10.1073/pnas.0808245105>
- [236] Kastoryano, M.J., Brandao, F.G.S.L.: *Quantum Gibbs Samplers: the commuting case*. Comm. Math. Phys. **344**(3), 915–957 (2016). URL <https://doi.org/10.1007/s00220-016-2641-8>
- [237] Kauffman, L.H., Mehrotra, E.: *Topological aspects of quantum entanglement*. Quantum Inf. Process. **18**(3), 76 (2019). DOI 10.1007/s11128-019-2191-z. URL <https://doi.org/10.1007/s11128-019-2191-z>
- [238] Kerenidis, I., Prakash, A.: *Quantum Recommendation Systems*. In: C.H. Papadimitriou (ed.) *8th Innovations in Theoretical Computer Science Conference, ITCS 2017, January 9–11, 2017, Berkeley, CA, USA, LIPIcs*, vol. 67, pp. 49:1–49:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2017). DOI 10.4230/LIPIcs.ITCS.2017.49. URL <https://doi.org/10.4230/LIPIcs.ITCS.2017.49>
- [239] Kerenidis, I., Prakash, A.: *Quantum gradient descent for linear systems and least squares*. Phys. Rev. A **101**, 022,316 (2020). DOI 10.1103/PhysRevA.101.022316. URL <https://link.aps.org/doi/10.1103/PhysRevA.101.022316>
- [240] Kiani, B.T., De Palma, G., Englund, D., Kaminsky, W., Marvian, M., Lloyd, S.: *Quantum advantage for differential equation analysis*. Phys. Rev. A **105**, 022,415 (2022). DOI 10.1103/PhysRevA.105.022415. URL <https://link.aps.org/doi/10.1103/PhysRevA.105.022415>
- [241] Kiesow Cortez, E., Bambauer, J.R., Guha, S.: *A Quantum Policy and Ethics Roadmap*. SSRN **4507090** (2023). DOI 10.2139/ssrn.4507090. URL <https://papers.ssrn.com/abstract=4507090>
- [242] Kim, P., Han, D., Jeong, K.C.: *Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2*. Quantum Inf. Process. **17**(12), 339 (2018). DOI 10.1007/s11128-018-2107-3. URL <https://doi.org/10.1007/s11128-018-2107-3>
- [243] Kiss, O., Grossi, M., Lougovski, P., Sanchez, F., Vallecorsa, S., Papenbrock, T.: *Quantum computing of the ⁶Li nucleus via ordered unitary coupled clusters*. Phys. Rev. C **106**, 034,325 (2022). DOI 10.1103/PhysRevC.106.034325. URL <https://link.aps.org/doi/10.1103/PhysRevC.106.034325>
- [244] Kitaev, A.Y.: *Quantum computations: algorithms and error correction*. Russ. Math. Surv. **52**, 1191–1249 (1997). URL <https://doi.org/10.1070/rm1997v052n06abeh002155>
- [245] Klauck, H., Špalek, R., de Wolf, R.: *Quantum and Classical Strong Direct Product Theorems and Optimal Time-Space Tradeoffs*. SIAM J. Comput. **36**(5), 1472–1493 (2007). DOI 10.1137/05063235X. URL <https://doi.org/10.1137/05063235X>

- [246] Kliesch, M., Barthel, T., Gogolin, C., Kastoryano, M., Eisert, J.: *Dissipative quantum Church-Turing theorem*. Phys. Rev. Lett. **107**(12), 120,501 (2011). URL <https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.107.120501>
- [247] Korte, B.H., Vygen, J., Korte, B., Vygen, J.: Combinatorial optimization, vol. 1. Springer (2011). URL <https://link.springer.com/book/10.1007/978-3-662-56039-6>
- [248] Koshka, Y., Novotny, M.A.: *Comparison of D-Wave Quantum Annealing and Classical Simulated Annealing for Local Minima Determination*. IEEE Journal on Selected Areas in Information Theory **1**(2), 515–525 (2020). DOI 10.1109/JSAIT.2020.3014192. URL <https://ieeexplore.ieee.org/abstract/document/9159646>
- [249] Kowada, L.A.B., Lavor, C., Portugal, R., de Figueiredo, C.M.H.: *A new quantum algorithm for solving the minimum searching problem*. Int. J. Quantum Inf. **6**(3), 427–436 (2008). URL <https://www.worldscientific.com/doi/epdf/10.1142/S021974990800361X>
- [250] Krovi, H.: *Improved quantum algorithms for linear and nonlinear differential equations*. Quantum **7**, 913 (2023). DOI 10.22331/q-2023-02-02-913. URL <https://doi.org/10.22331/q-2023-02-02-913>
- [251] Krovi, H., Ozols, M., Roland, J.: *Adiabatic condition and the quantum hitting time of Markov chains*. Phys. Rev. A **82**, 022,333 (2010). DOI 10.1103/PhysRevA.82.022333. URL <https://link.aps.org/doi/10.1103/PhysRevA.82.022333>
- [252] Kulshrestha, A., Safro, I.: *BEINIT: Avoiding Barren Plateaus in Variational Quantum Algorithms*. In: 2022 IEEE International Conference on Quantum Computing and Engineering (QCE), pp. 197–203 (2022). DOI 10.1109/QCE53715.2022.00039. URL <https://doi.org/10.1109/QCE53715.2022.00039>
- [253] Kuperberg, G.: *A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem*. SIAM J. Comput. **35**(1), 170–188 (2005). DOI 10.1137/S0097539703436345. URL <https://doi.org/10.1137/S0097539703436345>
- [254] Kuwakado, H., Morii, M.: *Quantum distinguisher between the 3-round Feistel cipher and the random permutation*. In: 2010 IEEE International Symposium on Information Theory, pp. 2682–2685 (2010). DOI 10.1109/ISIT.2010.5513654. URL <https://ieeexplore.ieee.org/document/5513654>. ISSN: 2157-8117
- [255] Kuwakado, H., Morii, M.: *Security on the quantum-type Even-Mansour cipher*. In: 2012 International Symposium on Information Theory and its Applications, pp. 312–316 (2012). URL <https://ieeexplore.ieee.org/document/6400943>
- [256] Kyriienko, O., Paine, A.E., Elfving, V.E.: *Solving nonlinear differential equations with differentiable quantum circuits*. Phys. Rev. A **103**, 052,416 (2021). DOI 10.1103/PhysRevA.103.052416. URL <https://link.aps.org/doi/10.1103/PhysRevA.103.052416>
- [257] Laarhoven, T., Mosca, M., van de Pol, J.: *Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search*. In: P. Gaborit (ed.) Post-Quantum Cryptography, Lecture Notes in Computer Science, pp. 83–101. Springer, Berlin, Heidelberg (2013). DOI 10.1007/978-3-642-38616-9_6. URL https://link.springer.com/chapter/10.1007/978-3-642-38616-9_6
- [258] LaBorde, M.L., Rogers, A.C., Dowling, J.P.: *Finding broken gates in quantum circuits: exploiting hybrid machine learning*. Quantum Inf. Process. **19**(8), 230 (2020). DOI 10.1007/s11128-020-02729-y. URL <https://doi.org/10.1007/s11128-020-02729-y>
- [259] Lee, T., Magniez, F., Santha, M.: *Learning graph based quantum query algorithms for finding constant-size subgraphs*. Chicago J. Theoret. Comput. Sci. **10**, 1–21 (2012). URL <http://cjtc.cs.uchicago.edu/articles/2012/10/cj12-10.pdf>

- [260] Leyton, S.K., Osborne, T.J.: *A quantum algorithm to solve nonlinear differential equations*. arXiv preprint arXiv:0812.4423 (2008). URL <https://doi.org/10.48550/arXiv.0812.4423>
- [261] Li, L., Luo, J.: *Concise and Efficient Quantum Algorithms for Distribution Closeness Testing*. arXiv preprint arXiv:2302.06084 (2023). URL <http://arxiv.org/abs/2302.06084>
- [262] Li, Y., Tian, M., Liu, G., Peng, C., Jiao, L.: *Quantum Optimization and Quantum Learning: A Survey*. IEEE Access **8**, 23,568–23,593 (2020). DOI 10.1109/ACCESS.2020.2970105. URL <https://ieeexplore.ieee.org/document/8972916>
- [263] Lidar, D.A., Wang, H.: *Calculating the thermal rate constant with exponential speedup on a quantum computer*. Phys. Rev. E **59**(2), 2429–2438 (1999). URL <https://doi.org/10.1103/PhysRevE.59.2429>
- [264] Lin, C.Y.Y., Zhu, Y.: *Performance of QAOA on typical instances of constraint satisfaction problems with bounded degree*. arXiv preprint arXiv:1601.01744 (2016). URL <http://arxiv.org/abs/1601.01744>
- [265] Linden, N., Montanaro, A., Shao, C.: *Quantum vs. Classical Algorithms for Solving the Heat Equation*. Comm. Math. Phys. **395**, 601 – 641 (2020). URL <https://doi.org/10.1007/s00220-022-04442-6>
- [266] Lipton, R.J., Regan, K.W.: *Introduction to quantum algorithms via linear algebra*. MIT Press (2021). URL <https://mitpress.mit.edu/9780262045254/introduction-to-quantum-algorithms-via-linear-algebra/>
- [267] Liu, F., Bian, K., Meng, F., Zhang, W., Dahlsten, O.: *Information compression via hidden subgroup quantum autoencoders*. arXiv preprint arXiv:2306.08047 (2023). URL <http://arxiv.org/abs/2306.08047>
- [268] Liu, H.L., Wu, Y.S., Wan, L.C., Pan, S.J., Qin, S.J., Gao, F., Wen, Q.Y.: *Variational quantum algorithm for the Poisson equation*. Phys. Rev. A **104**, 022,418 (2021). DOI 10.1103/PhysRevA.104.022418. URL <https://link.aps.org/doi/10.1103/PhysRevA.104.022418>
- [269] Liu, J.G., Gao, X., Cain, M., Lukin, M.D., Wang, S.T.: *Computing solution space properties of combinatorial optimization problems via generic tensor networks*. SIAM J. Sci. Comput. **45**(3), A1239–A1270 (2023). DOI 10.1137/22M1501787. URL <https://doi.org/10.1137/22M1501787>
- [270] Liu, J.P., Øie Kolden, H., Krovi, H.K., Loureiro, N.F., Trivisa, K., Childs, A.M.: *Efficient quantum algorithm for dissipative nonlinear differential equations*. Proc. Natl. Acad. Sci. **118**(35), e2026805,118 (2021). DOI 10.1073/pnas.2026805118. URL <https://www.pnas.org/doi/abs/10.1073/pnas.2026805118>
- [271] Liu, Y., Arunachalam, S., Temme, K.: *A rigorous and robust quantum speed-up in supervised machine learning*. Nat. Phys. **17**(9), 1013–1017 (2021). URL <https://doi.org/10.1038/s41567-021-01287-z>
- [272] Lloyd, S.: *Universal Quantum Simulators*. Science **273**(5278), 1073–1078 (1996). DOI 10.1126/science.273.5278.1073. URL <https://www.science.org/doi/abs/10.1126/science.273.5278.1073>
- [273] Lloyd, S., Garnerone, S., Zanardi, P.: *Quantum algorithms for topological and geometric analysis of data*. Nat. Commun. **7**(1), 10,138 (2016). DOI 10.1038/ncomms10138. URL <https://www.nature.com/articles/ncomms10138>
- [274] Lloyd, S., Mohseni, M., Rebentrost, P.: *Quantum algorithms for supervised and unsupervised machine learning*. arXiv preprint arXiv:1307.0411 (2013). URL <https://doi.org/10.48550/arXiv.1307.0411>
- [275] Lloyd, S., Mohseni, M., Rebentrost, P.: *Quantum principal component analysis*. Nat. Phys. **10**(9), 631 (2014). URL <https://doi.org/10.1038/nphys3029>

- [276] Lomonaco, S.J.: *Shor's quantum factoring algorithm*. In: Quantum Computation: A grand Mathematical Challenge for the Twenty-First Century and the Millennium (2002). URL <https://arxiv.org/abs/quant-ph/0010034>
- [277] Lomont, C.: *The hidden subgroup problem-review and open problems*. arXiv preprint [quant-ph/0411037](https://arxiv.org/abs/quant-ph/0411037) (2004). URL <http://arxiv.org/abs/quant-ph/0411037>
- [278] Lötstedt, E., Yamanouchi, K., Tsuchiya, T., Tachikawa, Y.: *Calculation of vibrational eigenenergies on a quantum computer: Application to the Fermi resonance in CO₂*. *Phys. Rev. A* **103**, 062,609 (2021). DOI 10.1103/PhysRevA.103.062609. URL <https://link.aps.org/doi/10.1103/PhysRevA.103.062609>
- [279] Low, G.H., Chuang, I.L.: *Optimal Hamiltonian Simulation by Quantum Signal Processing*. *Phys. Rev. Lett.* **118**, 010,501 (2017). DOI 10.1103/PhysRevLett.118.010501. URL <https://link.aps.org/doi/10.1103/PhysRevLett.118.010501>
- [280] Low, G.H., Chuang, I.L.: *Hamiltonian simulation by qubitization*. *Quantum* **3**, 163 (2019). URL <https://doi.org/10.22331/q-2019-07-12-163>
- [281] Lubasch, M., Joo, J., Moinier, P., Kiffner, M., Jaksch, D.: *Variational quantum algorithms for nonlinear problems*. *Phys. Rev. A* **101**, 010,301 (2020). DOI 10.1103/PhysRevA.101.010301. URL <https://link.aps.org/doi/10.1103/PhysRevA.101.010301>
- [282] Lucamarini, M., Yuan, Z.L., Dynes, J.F., Shields, A.J.: *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters*. *Nature* **557**(7705), 400–403 (2018). DOI 10.1038/s41586-018-0066-6. URL <https://www.nature.com/articles/s41586-018-0066-6>
- [283] Magniez, F., Nayak, A.: *Quantum Complexity of Testing Group Commutativity*. In: L. Caires, G.F. Italiano, L. Monteiro, C. Palamidessi, M. Yung (eds.) Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings, *Lecture Notes in Computer Science*, vol. 3580, pp. 1312–1324. Springer (2005). DOI 10.1007/11523468_106. URL https://doi.org/10.1007/11523468_106
- [284] Maria, C., Spreer, J.: *A Polynomial-Time Algorithm to Compute Turaev–Viro Invariants $TV_{r,q}$ of 3-Manifolds with Bounded First Betti Number*. *Lond. Math. S.* **20**(5), 1013–1034 (2020). DOI 10.1007/s10208-019-09438-8. URL <https://doi.org/10.1007/s10208-019-09438-8>
- [285] McGeoch, C.C.: *Adiabatic Quantum Computation and Quantum Annealing*. Synthesis Lectures on Quantum Computing (SLQC). Springer (2014). URL <https://link.springer.com/book/10.1007/978-3-031-02518-1>
- [286] McGeoch, C.C., Wang, C.: *Experimental Evaluation of an Adiabatic Quantum System for Combinatorial Optimization*. In: Proceedings of the ACM International Conference on Computing Frontiers, CF '13. Association for Computing Machinery, New York, NY, USA (2013). DOI 10.1145/2482767.2482797. URL <https://doi.org/10.1145/2482767.2482797>
- [287] Meyer, D.A., Wong, T.G.: *Connectivity is a poor indicator of fast quantum search*. *Phys. Rev. Lett.* **114**(11), 110,503 (2014). URL <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.114.110503>
- [288] Meyer, N., Ufrecht, C., Periyasamy, M., Scherer, D.D., Plinge, A., Mutschler, C.: *A survey on quantum reinforcement learning*. arXiv preprint [arXiv:2211.03464](https://arxiv.org/abs/2211.03464) (2022). URL <http://arxiv.org/abs/2211.03464>
- [289] Miceli, R., McGuigan, M.: *Effective matrix model for nuclear physics on a quantum computer*. In: 2019 New York Scientific Data Summit (NYSDS), pp. 1–4 (2019). DOI 10.1109/NYSDS.2019.8909693. URL <https://doi.org/10.1109/NYSDS.2019.8909693>
- [290] Miyamoto, K., Ueda, H.: *Extracting a function encoded in amplitudes of a quantum state by tensor network and orthogonal function expansion*. *Quantum Inf. Process.* **22**(6), Paper No.

- 239, 30 (2023). DOI 10.1007/s11128-023-03937-y. URL <https://doi.org/10.1007/s11128-023-03937-y>
- [291] Miyazaki, J., Hajdušek, M., Murao, M.: *Analysis of the trade-off between spatial and temporal resources for measurement-based quantum computation*. Phys. Rev. A **91**(5), 052,302 (2015). DOI 10.1103/PhysRevA.91.052302. URL <https://link.aps.org/doi/10.1103/PhysRevA.91.052302>
- [292] Moll, N., Barkoutsos, P., Bishop, L.S., Chow, J.M., Cross, A., Egger, D.J., Filipp, S., Fuhrer, A., Gambetta, J.M., Ganzhorn, M.: *Quantum optimization using variational algorithms on near-term quantum devices*. Quantum Sci. Technol. **3**(3) (2018). DOI 10.1088/2058-9565/aab822. URL <https://doi.org/10.1088/2058-9565/aab822>
- [293] Monràs, A., Sentís, G., Wittek, P.: *Inductive Supervised Quantum Learning*. Phys. Rev. Lett. **118**, 190,503 (2017). DOI 10.1103/PhysRevLett.118.190503. URL <https://link.aps.org/doi/10.1103/PhysRevLett.118.190503>
- [294] Montanaro, A.: *Quantum Search with Advice*. In: W. van Dam, V.M. Kendon, S. Severini (eds.) Theory of Quantum Computation, Communication, and Cryptography - 5th Conference, TQC 2010, Leeds, UK, April 13-15, 2010, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 6519, pp. 77-93. Springer (2010). DOI 10.1007/978-3-642-18073-6_7. URL https://doi.org/10.1007/978-3-642-18073-6_7
- [295] Montanaro, A.: *The quantum query complexity of learning multilinear polynomials*. Inf. Process. Lett. **112**(11), 438-442 (2012). DOI 10.1016/j.ipl.2012.03.002. URL <https://doi.org/10.1016/j.ipl.2012.03.002>
- [296] Montanaro, A.: *Quantum speedup of Monte Carlo methods*. Proceedings of the Royal Society A **471**(2179), 20150,301 (2015). DOI 10.1098/rspa.2015.0301. URL <http://doi.org/10.1098/rspa.2015.0301>
- [297] Montanaro, A.: *Quantum algorithms: an overview*. npj Quantum Inf. **2**(1), 1-8 (2016). URL <https://doi.org/10.1038/npjqi.2015.23>
- [298] Montanaro, A.: *Quantum Pattern Matching Fast on Average*. Algorithmica **77**(1), 16-39 (2017). DOI 10.1007/s00453-015-0060-4. URL <https://doi.org/10.1007/s00453-015-0060-4>
- [299] Montanaro, A., Pallister, S.: *Quantum algorithms and the finite element method*. Phys. Rev. A **93**, 032,324 (2016). DOI 10.1103/PhysRevA.93.032324. URL <https://link.aps.org/doi/10.1103/PhysRevA.93.032324>
- [300] Montanaro, A., de Wolf, R.: *A Survey of Quantum Property Testing*. Theory of Computing pp. 1-81 (2016). DOI 10.4086/toc.gs.2016.007. URL <https://theoryofcomputing.org/articles/gs007>
- [301] Moore, C., Rockmore, D., Russell, A., Schulman, L.J.: *The power of basis selection in fourier sampling: hidden subgroup problems in affine groups*. In: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms, pp. 1113-1122 (2004). URL <https://dl.acm.org/doi/abs/10.5555/982792.982957>
- [302] Morain, F.: *Implementing the Asymptotically Fast Version of the Elliptic Curve Primality Proving Algorithm*. Math. Comp. **76**(257), 493-505 (2007). URL <https://www.jstor.org/stable/40234389>
- [303] Morita, S., Nishimori, H.: *Mathematical foundation of quantum annealing*. Journal of Mathematical Physics **49**(12), 125,210 (2008). URL <https://doi.org/10.1063/1.2995837>
- [304] Mosca, M.: *Quantum Algorithms*. arXiv preprint arXiv:0808.0369 (2008). URL <https://arxiv.org/abs/0808.0369>

- [305] Naik, A., Yeniaras, E., Hellstern, G., Prasad, G., Vishwakarma, S.K.L.P.: *From Portfolio Optimization to Quantum Blockchain and Security: A Systematic Review of Quantum Computing in Finance*. arXiv preprint arXiv:2307.01155 (2023). URL <http://arxiv.org/abs/2307.01155>
- [306] Nannicini, G.: *An Introduction to Quantum Computing, without the Physics*. SIAM Rev. **62**(4), 936–981 (2020). DOI 10.1137/18M1170650. URL <https://epubs.siam.org/doi/abs/10.1137/18M1170650>
- [307] Nayak, A., Wu, F.: *The Quantum Query Complexity of Approximating the Median and Related Statistics*. In: J.S. Vitter, L.L. Larmore, F.T. Leighton (eds.) Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, May 1-4, 1999, Atlanta, Georgia, USA, pp. 384–393. ACM (1999). DOI 10.1145/301250.301349. URL <https://doi.org/10.1145/301250.301349>
- [308] Neven, H., Denchev, V., Rose, G., Mcready, W.: *Qboost: Large scale classifier training with adiabatic quantum optimization*. In: Proceedings of Machine Learning Research, PMLR, vol. 25, pp. 333–348. Singapore Management University (2012). URL <https://proceedings.mlr.press/v25/neven12.html>
- [309] Neven, H., Denchev, V.S., Drew-Brook, M., Zhang, J., Mcready, W.G., Rose, G.: *Nips 2009 demonstration: Binary classification using hardware implementation of quantum annealing*. Quantum **4**, 1 (2009). URL https://static.googleusercontent.com/media/www.google.com/es//googleblogs/pdfs/nips_demoreport_120709_research.pdf
- [310] Neven, H., Denchev, V.S., Rose, G., Mcready, W.G.: *Training a binary classifier with the quantum adiabatic algorithm*. arXiv preprint arXiv:0811.0416 (2008). URL <https://doi.org/10.48550/arXiv.0811.0416>
- [311] Neven, H., Denchev, V.S., Rose, G., Mcready, W.G.: *Training a large scale classifier with the quantum adiabatic algorithm*. arXiv preprint arXiv:0912.0779 (2009). URL <https://doi.org/10.48550/arXiv.0912.0779>
- [312] Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press (2010). DOI 10.1017/CBO9780511976667. URL <https://doi.org/10.1017/CBO9780511976667>
- [313] Nimbe, P., Weyori, B.A., Adekoya, A.F.: *Models in quantum computing: a systematic review*. Quantum Inf. Process. **20**(2), 80 (2021). DOI 10.1007/s11128-021-03021-3. URL <https://doi.org/10.1007/s11128-021-03021-3>
- [314] Niroula, P., Nam, Y.: *A quantum algorithm for string matching*. NPJ Quantum Information **7**, 37 (2021). URL <https://www.nature.com/articles/s41534-021-00369-3>
- [315] Novak, E.: *Quantum Complexity of Integration*. J. Complex. **17**(1), 2–16 (2001). DOI 10.1006/jcom.2000.0566. URL <https://doi.org/10.1006/jcom.2000.0566>
- [316] Omiya, K., Nakagawa, Y.O., Koh, S., Mizukami, W., Gao, Q., Kobayashi, T.: *Analytical Energy Gradient for State-Averaged Orbital-Optimized Variational Quantum Eigensolvers and Its Application to a Photochemical Reaction*. J. Chem. Theory Comput. **18**(2), 741–748 (2022). DOI 10.1021/acs.jctc.1c00877. URL <https://doi.org/10.1021/acs.jctc.1c00877>. PMID: 35060747
- [317] Orsucci, D., Briegel, H.J., Dunjko, V.: *Faster quantum mixing for slowly evolving sequences of Markov chains*. Quantum **2**, 105 (2018). URL <https://doi.org/10.22331/q-2018-11-09-105>
- [318] Ortiz, G., Gubernatis, J.E., Knill, E., Laflamme, R.: *Quantum algorithms for fermionic simulations*. Phys. Rev. A **64**, 022319 (2001). DOI 10.1103/PhysRevA.64.022319. URL <https://link.aps.org/doi/10.1103/PhysRevA.64.022319>

- [319] Orts, F., Ortega, G., Combarro, E.F., Garzón, E.M.: *A review on reversible quantum adders*. J. Netw. Comput. Appl. **170**, 102,810 (2020). DOI 10.1016/j.jnca.2020.102810. URL <https://www.sciencedirect.com/science/article/pii/S1084804520302812>
- [320] Orús, R., Mugel, S., Lizaso, E.: *Quantum computing for finance: Overview and prospects*. Rev. Phys. **4**, 100,028 (2019). DOI 10.1016/j.revip.2019.100028. URL <https://www.sciencedirect.com/science/article/pii/S2405428318300571>
- [321] Ossorio-Castillo, J., Pena-Brage, F.: *Optimization of a refinery scheduling process with column generation and a quantum annealer*. Optim. Eng. **23**(3), 1471–1488 (2022). DOI 10.1007/s11081-021-09662-8. URL <https://doi.org/10.1007/s11081-021-09662-8>
- [322] Pak, I.: *Testing commutativity of a group and the power of randomization*. LMS J. Comput. Math. **15**, 38–43 (2012). DOI 10.1112/S1461157012000046. URL <https://doi.org/10.1112/S1461157012000046>
- [323] Paparo, G., Dunjko, V., Makmal, A., Martin-Delgado, M., Briegel, H.: *Quantum speedup for active learning agents*. Phys. Rev. X **4**(3), 031,002 (2014). URL <https://doi.org/10.1103/PhysRevX.4.031002>
- [324] Paudel, H.P., Syamlal, M., Crawford, S.E., Lee, Y.L., Shugayev, R.A., Lu, P., Ohodnicki, P.R., Mollot, D., Duan, Y.: *Quantum Computing and Simulations for Energy Applications: Review and Perspective*. ACS Engineering Au **2**(3), 151–196 (2022). DOI 10.1021/acsengineeringau.1c00033. URL <https://doi.org/10.1021/acsengineeringau.1c00033>
- [325] Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.H., Zhou, X.Q., Love, P.J., Aspuru-Guzik, A., O’Brien, J.L.: *A variational eigenvalue solver on a photonic quantum processor*. Nat. Commun. **5**, 4213 (2014). DOI 10.1038/ncomms5213. URL <https://pubmed.ncbi.nlm.nih.gov/25055053>
- [326] Poulin, D., Kitaev, A., Steiger, D.S., Hastings, M.B., Troyer, M.: *Quantum Algorithm for Spectral Measurement with a Lower Gate Count*. Phys. Rev. Lett. **121**, 010,501 (2018). DOI 10.1103/PhysRevLett.121.010501. URL <https://link.aps.org/doi/10.1103/PhysRevLett.121.010501>
- [327] Poulin, D., Wocjan, P.: *Sampling from the Thermal Quantum Gibbs State and Evaluating Partition Functions with a Quantum Computer*. Phys. Rev. Lett. **103**, 220,502 (2009). DOI 10.1103/PhysRevLett.103.220502. URL <https://link.aps.org/doi/10.1103/PhysRevLett.103.220502>
- [328] Proos, J., Zalka, C.: *Shor’s discrete logarithm quantum algorithm for elliptic curves*. Quantum Inf. Comput. **3**(4), 317–344 (2003). DOI 10.26421/QIC3.4-3. URL <https://doi.org/10.26421/QIC3.4-3>
- [329] Pudenz, K.L., Lidar, D.A.: *Quantum adiabatic machine learning*. Quantum Inf. Process. **12**(5), 2027–2070 (2013). DOI 10.1007/s11128-012-0506-4. URL <https://doi.org/10.1007/s11128-012-0506-4>
- [330] Quantum Flagship: *Strategic Research and Industry Agenda* (2022). URL https://qt.eu/media/pdf/Quantum-Flagship_SRIA_2022.pdf?m=1674660050&
- [331] Ramesh, H., Vinay, V.: *String matching in $\tilde{O}(\sqrt{n} + \sqrt{m})$ quantum time*. J. Discrete Algorithms **1**, 103–110 (2003). URL [https://doi.org/10.1016/S1570-8667\(03\)00010-8](https://doi.org/10.1016/S1570-8667(03)00010-8)
- [332] Ramusat, N., Savona, V.: *A quantum algorithm for the direct estimation of the steady state of open quantum systems*. Quantum **5**, 399 (2021). DOI 10.22331/q-2021-02-22-399. URL <https://doi.org/10.22331/q-2021-02-22-399>
- [333] Rebentrost, P., Mohseni, M., Lloyd, S.: *Quantum support vector machine for big data classification*. Phys. Rev. Lett. **113**, 130,503 (2014). URL <https://doi.org/10.1103/PhysRevLett.113.130503>

- [334] Regev, O.: *Quantum Computation and Lattice Problems*. SIAM J. Comput. **33**(3), 738–760 (2004). DOI 10.1137/S0097539703440678. URL <https://doi.org/10.1137/S0097539703440678>
- [335] Regev, O.: *A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space*. arXiv preprint quant-ph/0406151 (2004). URL <https://arxiv.org/abs/quant-ph/0406151>
- [336] Reichardt, B.W.: *The quantum adiabatic optimization algorithm and local minima*. In: Conference Proceedings of the Annual ACM Symposium on Theory of Computing, pp. 502–510 (2004). DOI 10.1145/1007352.1007428. URL <https://doi.org/10.1145/1007352.1007428>
- [337] Reichardt, B.W.: *Span Programs and Quantum Query Complexity: The General Adversary Bound Is Nearly Tight for Every Boolean Function*. In: 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25–27, 2009, Atlanta, Georgia, USA, pp. 544–551. IEEE Computer Society (2009). DOI 10.1109/FOCS.2009.55. URL <https://doi.org/10.1109/FOCS.2009.55>
- [338] Reichardt, B.W.: *Reflections for quantum query algorithms*. In: Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 560–569. SIAM (2011). URL <https://doi.org/10.1137/1.9781611973082.44>
- [339] Reiher, M., Wiebe, N., Svore, K.M., Wecker, D., Troyer, M.: *Elucidating reaction mechanisms on quantum computers*. Proc. Natl. Acad. Sci. **114**(29), 7555–7560 (2017). DOI 10.1073/pnas.1619152114. URL <https://www.pnas.org/doi/abs/10.1073/pnas.1619152114>
- [340] Riera, A., Gogolin, C., Eisert, J.: *Thermalization in Nature and on a Quantum Computer*. Phys. Rev. Lett. **108**, 080402 (2012). DOI 10.1103/PhysRevLett.108.080402. URL <https://link.aps.org/doi/10.1103/PhysRevLett.108.080402>
- [341] Roetteler, M.: *Quantum Algorithms for Abelian Difference Sets and Applications to Dihedral Hidden Subgroups*. In: A. Broadbent (ed.) 11th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2016, September 27–29, 2016, Berlin, Germany, *LIPICs*, vol. 61, pp. 8:1–8:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2016). DOI 10.4230/LIPICs.TQC.2016.8. URL <https://doi.org/10.4230/LIPICs.TQC.2016.8>
- [342] Roetteler, M., Beth, T.: *Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups*. arXiv preprint quant-ph/9812070 (1998). URL <http://arxiv.org/abs/quant-ph/9812070>
- [343] Roetteler, M., Naehrig, M., Svore, K.M., Lauter, K.E.: *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms*. In: T. Takagi, T. Peyrin (eds.) Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part II, *Lecture Notes in Computer Science*, vol. 10625, pp. 241–270. Springer (2017). DOI 10.1007/978-3-319-70697-9_9. URL https://doi.org/10.1007/978-3-319-70697-9_9
- [344] Romero, A.M., Engel, J., Tang, H.L., Economou, S.E.: *Solving nuclear structure problems with the adaptive variational quantum algorithm*. Phys. Rev. C **105**(6) (2022). DOI 10.1103/physrevc.105.064317. URL <https://doi.org/10.1103/physrevc.105.064317>
- [345] Rötteler, M.: *Quantum algorithms: A survey of some recent results*. Informatik - Forschung und Entwicklung **21**(1), 3–20 (2006). DOI 10.1007/s00450-006-0008-7. URL <https://doi.org/10.1007/s00450-006-0008-7>
- [346] Rötteler, M., Steinwandt, R.: *A note on quantum related-key attacks*. Inf. Process. Lett. **115**(1), 40–44 (2015). DOI 10.1016/j.ipl.2014.08.009. URL <https://doi.org/10.1016/j.ipl.2014.08.009>

- [347] Saad, Y.: *Iterative Methods for Sparse Linear Systems: Second Edition*. Other Titles in Applied Mathematics. Society for Industrial and Applied Mathematics (2003). URL <https://doi.org/10.1137/1.9780898718003>
- [348] Santoli, T., Schaffner, C.: *Using Simon's algorithm to attack symmetric-key cryptographic primitives*. *Quantum Inf. Comput.* **17**(1&2), 65–78 (2017). DOI 10.26421/QIC17.1-2-4. URL <https://doi.org/10.26421/QIC17.1-2-4>
- [349] Santoro, G.E., Tosatti, E.: *Optimization using quantum mechanics: quantum annealing through adiabatic evolution*. *J. Phys. A: Math. Gen.* **39**(36), R393 (2006). DOI 10.1088/0305-4470/39/36/R01. URL <https://dx.doi.org/10.1088/0305-4470/39/36/R01>
- [350] Sasaki, M., Carlini, A.: *Quantum learning and universal quantum matching machine*. *Phys. Rev. A* **66**, 022,303 (2002). DOI 10.1103/PhysRevA.66.022303. URL <https://link.aps.org/doi/10.1103/PhysRevA.66.022303>
- [351] Sasaki, M., Carlini, A., Jozsa, R.: *Quantum template matching*. *Phys. Rev. A* **64**, 022,317 (2001). DOI 10.1103/PhysRevA.64.022317. URL <https://link.aps.org/doi/10.1103/PhysRevA.64.022317>
- [352] Sawaya, N.P.D., Paesani, F., Tabor, D.P.: *Near- and long-term quantum algorithmic approaches for vibrational spectroscopy*. *Phys. Rev. A* **104**, 062,419 (2021). DOI 10.1103/PhysRevA.104.062419. URL <https://link.aps.org/doi/10.1103/PhysRevA.104.062419>
- [353] Schaden, M.: *Quantum finance*. *Phys. A* **316**(1), 511–538 (2002). URL <https://ideas.repec.org/a/eee/phsmap/v316y2002i1p511-538.html>
- [354] Scherer, W.: *Mathematics of Quantum Computing: An Introduction*. Springer International Publishing (2019). URL <https://doi.org/10.1007/978-3-030-12358-1>
- [355] Schmidt, A., Vollmer, U.: *Polynomial time quantum algorithm for the computation of the unit group of a number field*. In: H.N. Gabow, R. Fagin (eds.) *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, Baltimore, MD, USA, May 22-24, 2005, pp. 475–480. ACM (2005). DOI 10.1145/1060590.1060661. URL <https://doi.org/10.1145/1060590.1060661>
- [356] Schön, C., Hammerer, K., Wolf, M.M., Cirac, J.I., Solano, E.: *Sequential generation of matrix-product states in cavity QED*. *Phys. Rev. A* **75**, 032,311 (2007). DOI 10.1103/PhysRevA.75.032311. URL <https://link.aps.org/doi/10.1103/PhysRevA.75.032311>
- [357] Schön, C., Solano, E., Verstraete, F., Cirac, J.I., Wolf, M.M.: *Sequential Generation of Entangled Multiqubit States*. *Phys. Rev. Lett.* **95**, 110,503 (2005). DOI 10.1103/PhysRevLett.95.110503. URL <https://link.aps.org/doi/10.1103/PhysRevLett.95.110503>
- [358] Schuetz, M.J., Brubaker, J.K., Montagu, H., van Dijk, Y., Klepsch, J., Ross, P., Luckow, A., Resende, M.G., Katzgraber, H.G.: *Optimization of Robot-Trajectory Planning with Nature-Inspired and Hybrid Quantum Algorithms*. *Phys. Rev. Appl.* **18**(5), 054,045 (2022). DOI 10.1103/PhysRevApplied.18.054045. URL <https://link.aps.org/doi/10.1103/PhysRevApplied.18.054045>
- [359] Schuld, M., Sinayskiy, I., Petruccione, F.: *An introduction to quantum machine learning*. *Contemp. Phys.* **56**(2), 172 (2014). URL <https://doi.org/10.1080/00107514.2014.964942>
- [360] Schuld, M., Sinayskiy, I., Petruccione, F.: *Prediction by linear regression on a quantum computer*. *Phys. Rev. A* **94**, 022,342 (2016). URL <https://doi.org/10.1103/PhysRevA.94.022342>
- [361] Schwarz, M., Buerschaper, O., Eisert, J.: *Approximating local observables on projected entangled pair states*. *Phys. Rev. A* **95**(6) (2017). DOI 10.1103/physreva.95.060102. URL <https://doi.org/10.1103/physreva.95.060102>

- [362] Schwarz, M., Cubitt, T.S., Temme, K., Verstraete, F., Perez-Garcia, D.: *Preparing topological PEPS on a quantum computer*. Phys. Rev. A **88**(3), 032,321 (2013). URL <https://doi.org/10.1103/PhysRevA.88.032321>
- [363] Schwarz, M., Cubitt, T.S., Verstraete, F.: *An Information-Theoretic Proof of the Constructive Commutative Quantum Lovász Local Lemma*. arXiv preprint arXiv:1311.6474 (2013). URL <https://doi.org/10.48550/arXiv.1311.6474>
- [364] Schwarz, M., Temme, K., Verstraete, F.: *Preparing projected entangled pair states on a quantum computer*. Phys. Rev. Lett. **108**(11), 110,502 (2012). URL <https://doi.org/10.1103/PhysRevLett.108.110502>
- [365] Sengupta, R., Adhikary, S., Oseledets, I., Biamonte, J.: *Tensor networks in machine learning*. Eur. Math. Soc. Mag. **126**, 4–12 (2022). DOI 10.4171/mag/101. URL <https://doi.org/10.4171/mag/101>
- [366] Servedio, R.A., Gortler, S.J.: *Equivalences and Separations Between Quantum and Classical Learnability*. SIAM J. Comput. **33**(5), 1067–1092 (2004). DOI 10.1137/S0097539704412910. URL <https://doi.org/10.1137/S0097539704412910>
- [367] Setia, K., Whitfield, J.D.: *Bravyi-Kitaev Superfast simulation of electronic structure on a quantum computer*. J. Chem. Phys. **148**(16), 164,104 (2018). DOI 10.1063/1.5019371. URL <https://doi.org/10.1063/1.5019371>
- [368] Shaya, O.: *When could NISQ algorithms start to create value in discrete manufacturing?* arXiv preprint arXiv:2209.09650 (2022). URL <http://arxiv.org/abs/2209.09650>
- [369] Shor, P.W.: *Algorithms for quantum computation: discrete logarithms and factoring*. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994). DOI 10.1109/SFCS.1994.365700. URL <https://ieeexplore.ieee.org/document/365700>
- [370] Shor, P.W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM J. Comput. **26**(5), 1484–1509 (1997). DOI 10.1137/S0097539795293172. URL <https://doi.org/10.1137/S0097539795293172>
- [371] Shor, P.W., Jordan, S.P.: *Estimating Jones polynomials is a complete problem for one clean qubit*. Quantum Inf. Comput. **8**(8), 681–714 (2008). DOI 10.26421/QIC8.8-9-1. URL <https://doi.org/10.26421/QIC8.8-9-1>
- [372] Shparlinski, I.E., Winterhof, A.: *Quantum period reconstruction of approximate sequences*. Inf. Process. Lett. **103**(6), 211–215 (2007). DOI 10.1016/j.ipl.2007.02.019. URL <https://doi.org/10.1016/j.ipl.2007.02.019>
- [373] da Silva Coelho, W., Henriot, L., Henry, L.P.: *Quantum pricing-based column-generation framework for hard combinatorial problems*. Phys. Rev. A **107**, 032,426 (2023). DOI 10.1103/PhysRevA.107.032426. URL <https://link.aps.org/doi/10.1103/PhysRevA.107.032426>
- [374] Simon, D.: *On the Power of Quantum Computation*. In: Proceedings of the 35th Symposium on Foundations of Computer Science, pp. 116–123 (1994). URL <https://ieeexplore.ieee.org/document/365701>
- [375] Singh, J., Bhangu, K.S.: *Contemporary Quantum Computing Use Cases: Taxonomy, Review and Challenges*. Arch. Comput. Methods Eng. **30**(1), 615–638 (2023). DOI 10.1007/s11831-022-09809-5. URL <https://doi.org/10.1007/s11831-022-09809-5>
- [376] Sivak, V.V., Eickbusch, A., Royer, B., Singh, S., Tsioutsios, I., Ganjam, S., Miano, A., Brock, B.L., Ding, A.Z., Frunzio, L., Girvin, S.M., Schoelkopf, R.J., Devoret, M.H.: *Real-time quantum error correction beyond break-even*. Nature **616**(7955), 50–55 (2023). DOI 10.1038/s41586-023-05782-6. URL <https://www.nature.com/articles/s41586-023-05782-6>
- [377] Soller, H., Bogobowicz, M., Gao, S., Gshwendtner, M.: *Quantum Technology Monitor*. McKinsey & Company (2023). URL <https://www.mckinsey.com/~media/mckinsey/businessf>

- unctions/mckinseydigital/ourinsights/quantumtechnologysseesrecordinvestmentsprogressontalentgap/quantum-technology-monitor-april-2023.pdf
- [378] Somma, R.D.: *A Trotter-Suzuki approximation for Lie groups with applications to Hamiltonian simulation*. J. Math. Phys. **57**(6) (2016). URL <https://doi.org/10.1063/1.4952761>
- [379] Somma, R.D., Boixo, S., Barnum, H., Knill, E.: *Quantum Simulations of Classical Annealing Processes*. Phys. Rev. Lett. **101**, 130,504 (2008). DOI 10.1103/PhysRevLett.101.130504. URL <https://link.aps.org/doi/10.1103/PhysRevLett.101.130504>
- [380] Stoudenmire, E., Waintal, X.: *Grover's Algorithm Offers No Quantum Advantage*. arXiv preprint arXiv:2303.11317 (2023). URL <http://arxiv.org/abs/2303.11317>
- [381] Streif, M., Yarkoni, S., Skolik, A., Neukart, F., Leib, M.: *Beating classical heuristics for the binary paint shop problem with the quantum approximate optimization algorithm*. Phys. Rev. A **104**(1), 012,403 (2021). DOI 10.1103/PhysRevA.104.012403. URL <https://link.aps.org/doi/10.1103/PhysRevA.104.012403>
- [382] Sun, J., Lai, C.H., Wu, X.J.: Particle Swarm Optimisation Classical and Quantum Perspectives. Chapman & Hall/CRC Numerical Analysis and Scientific Computing Series. Routledge, Taylor & Francis (2012). URL <https://doi.org/10.1201/b11579>
- [383] Suzuki, Y., Gao, Q., Pradel, K.C., Yasuoka, K., Yamamoto, N.: *Natural quantum reservoir computing for temporal information processing*. Sci. Rep. **12**(1), 1353 (2022). DOI 10.1038/s41598-022-05061-w. URL <https://doi.org/10.1038/s41598-022-05061-w>
- [384] Syrichas, A., Crispin, A.: *Large-scale vehicle routing problems: Quantum Annealing, tunings and results*. Comput. Oper. Res. (2017). URL <https://doi.org/10.1016/j.cor.2017.05.014>
- [385] Szegedy, M.: *Quantum speed-up of Markov chain based algorithms*. In: Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, p. 32 (2004). URL <https://ieeexplore.ieee.org/document/1366222>
- [386] Tang, E.: *A quantum-inspired classical algorithm for recommendation systems*. In: M. Charikar, E. Cohen (eds.) Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23–26, 2019, pp. 217–228. ACM (2019). DOI 10.1145/3313276.3316310. URL <https://doi.org/10.1145/3313276.3316310>
- [387] Tang, E.: *Quantum Principal Component Analysis Only Achieves an Exponential Speedup Because of Its State Preparation Assumptions*. Phys. Rev. Lett. **127**, 060,503 (2021). DOI 10.1103/PhysRevLett.127.060503. URL <https://link.aps.org/doi/10.1103/PhysRevLett.127.060503>
- [388] Temme, K., Osborne, T.J., Vollbrecht, K.G., Poulin, D., Verstraete, F.: *Quantum metropolis sampling*. Nature **471**(7336), 87–90 (2011). URL <https://doi.org/10.1038/nature09770>
- [389] Tilly, J., Chen, H., Cao, S., Picozzi, D., Setia, K., Li, Y., Grant, E., Wossnig, L., Rungger, I., Booth, G.H., Tennyson, J.: *The Variational Quantum Eigensolver: A review of methods and best practices*. Phys. Rep. **986**, 1–128 (2022). DOI 10.1016/j.physrep.2022.08.003. URL <https://doi.org/10.1016/j.physrep.2022.08.003>
- [390] Toloui, B., Love, P.J.: *Quantum algorithms for quantum chemistry based on the sparsity of the CI-matrix*. arXiv preprint arXiv:1312.2579 (2013). URL <https://doi.org/10.48550/arXiv.1312.2579>
- [391] Tulsi, T., Grover, L.K., Patel, A.D.: *A new algorithm for fixed point quantum search*. Quantum Inf. Comput. **6**(6), 483–494 (2006). DOI 10.26421/QIC6.6-2. URL <https://doi.org/10.26421/QIC6.6-2>

- [392] Vazirani, U.: *A survey of quantum complexity theory*. In: Proceedings of Symposia in Applied Mathematics, vol. 58, pp. 193–220 (2002). URL <https://redirect.cs.umbc.edu/~lomonaco/ams/lecturenotes/Vazirani.pdf>
- [393] Venegas-Andraca, S.E.: *Quantum walks: a comprehensive review*. Quantum Inf. Process. **11**(5), 1015–1106 (2012). DOI 10.1007/s11128-012-0432-5. URL <https://doi.org/10.1007/s11128-012-0432-5>
- [394] Venturelli, D., Marchand, D.J.J., Rojo, G.: *Quantum annealing implementation of job-shop scheduling*. arXiv preprint arXiv:1506.08479 (2015). URL <https://doi.org/10.48550/arXiv.1506.08479>
- [395] Verdon, G., McCourt, T., Luzhnica, E., Singh, V., Leichenauer, S., Hidary, J.: *Quantum graph neural networks*. arXiv preprint arXiv:1909.12264 (2019). URL <https://doi.org/10.48550/arXiv.1909.12264>
- [396] Verstraete, F., Porras, D., Cirac, J.I.: *Density Matrix Renormalization Group and Periodic Boundary Conditions: A Quantum Information Perspective*. Phys. Rev. Lett. **93**(22) (2004). DOI 10.1103/physrevlett.93.227205. URL <https://doi.org/10.1103/physrevlett.93.227205>
- [397] van Vreumingen, D., Neukart, F., Von Dollen, D., Othmer, C., Hartmann, M., Voigt, A.C., Bäck, T.: *Quantum-assisted finite-element design optimization*. arXiv preprint arXiv:1908.03947 (2019). URL <http://arxiv.org/abs/1908.03947>
- [398] Wallach, N.: *A quantum polylog algorithm for non-normal maximal cyclic hidden subgroups in the affine group of a finite field*. arXiv preprint arXiv:1308.1415 (2013). URL <http://arxiv.org/abs/1308.1415>
- [399] Wang, H., Kais, S., Aspuru-Guzik, A., Hoffmann, M.R.: *Quantum algorithm for obtaining the energy spectrum of molecular systems*. Phys. Chem. Chem. Phys. **10**(35), 5388–5393 (2008). URL <https://doi.org/10.1039/b804804e>
- [400] Wang, Q., Guan, J., Liu, J., Zhang, Z., Ying, M.: *New quantum algorithms for computing quantum entropies and distances*. arXiv preprint arXiv:2203.13522 (2022). URL <http://arxiv.org/abs/2203.13522>
- [401] Wang, Z., Hadfield, S., Jiang, Z., Rieffel, E.G.: *Quantum approximate optimization algorithm for MaxCut: A fermionic view*. Phys. Rev. A **97**(2) (2018). DOI 10.1103/physreva.97.022304. URL <https://doi.org/10.1103/physreva.97.022304>
- [402] Wang, Z., Xu, M., Zhang, Y.: *Review of Quantum Image Processing*. Arch. Comput. Methods Eng. **29**(2), 737–761 (2022). DOI 10.1007/s11831-021-09599-2. URL <https://doi.org/10.1007/s11831-021-09599-2>
- [403] Wecker, D., Hastings, M.B., Troyer, M.: *Training a quantum optimizer*. Phys. Rev. A **94**(2), 022,309 (2016). DOI 10.1103/PhysRevA.94.022309. URL <https://link.aps.org/doi/10.1103/PhysRevA.94.022309>
- [404] White, S.R.: *Density matrix renormalization group algorithms with a single center site*. Phys. Rev. B **72**, 180,403 (2005). DOI 10.1103/PhysRevB.72.180403. URL <https://link.aps.org/doi/10.1103/PhysRevB.72.180403>
- [405] Whitfield, J.D.: *Spin-free quantum computational simulations and symmetry adapted states*. J. Chem. Phys. **139**(2), 021,105 (2013). URL <https://doi.org/10.1063/1.4812566>
- [406] Whitfield, J.D., Biamonte, J., Aspuru-Guzik, A.: *Simulation of electronic structure Hamiltonians using quantum computers*. Mol. Phys. **109**(5), 735–750 (2011). URL <https://doi.org/10.1080/00268976.2011.552441>
- [407] Wiebe, N., Braun, D., Lloyd, S.: *Quantum Algorithm for Data Fitting*. Phys. Rev. Lett. **109**, 050,505 (2012). DOI 10.1103/PhysRevLett.109.050505. URL <https://link.aps.org/doi/10.1103/PhysRevLett.109.050505>

- [408] Wiebe, N., Kapoor, A., Svore, K.M.: *Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning*. Quantum Inf. Comput. **15**(3&4), 316–356 (2015). DOI 10.26421/QIC15.3-4-7. URL <https://doi.org/10.26421/QIC15.3-4-7>
- [409] Wiebe, N., Kapoor, A., Svore, K.M.: *Quantum deep learning*. Quantum Inf. Comput. **16**(7&8), 541–587 (2016). DOI 10.26421/QIC16.7-8-1. URL <https://doi.org/10.26421/QIC16.7-8-1>
- [410] Wiesner, S.: *Simulations of many-body quantum systems by a quantum computer*. arXiv preprint quant-ph/9603028 (1996). URL <https://doi.org/10.48550/arXiv.quant-ph/9603028>
- [411] Willsch, M., Willsch, D., Jin, F., De Raedt, H., Michielsen, K.: *Benchmarking the quantum approximate optimization algorithm*. Quantum Inf. Process. **19**(7), 197 (2020). DOI 10.1007/s1128-020-02692-8. URL <https://doi.org/10.1007/s1128-020-02692-8>
- [412] Wittek, P.: *Quantum Machine Learning: what quantum computing means to data mining*. Academic Press (2014). URL <https://doi.org/10.1016/C2013-0-19170-2>
- [413] Wittek, P., Gogolin, C.: *Quantum enhanced inference in Markov logic networks*. Scientific reports **7**(1), 45,672 (2017). URL <https://doi.org/10.1038/srep45672>
- [414] Witten, E.: *Quantum field theory and the Jones polynomial*. Comm. Math. Phys. **121**(3), 351–399 (1989). DOI 10.1007/BF01217730. URL <https://doi.org/10.1007/BF01217730>
- [415] Wocjan, P., Yard, J.: *The Jones polynomial: quantum algorithms and applications in quantum complexity theory*. Quantum Inf. Comput. **8**(1), 147–180 (2008). DOI 10.26421/QIC8.1-2-10. URL <https://doi.org/10.26421/QIC8.1-2-10>
- [416] Wong, T.G.: *Quantum walk search on Johnson graphs*. J. Phys. A: Math. Theor. **49**(19), 195,303 (2016). DOI 10.1088/1751-8113/49/19/195303. URL <https://dx.doi.org/10.1088/1751-8113/49/19/195303>
- [417] Wong, T.G.: *Spatial search by continuous-time quantum walk with multiple marked vertices*. Quantum Inf. Process. **15**(4), 1411–1443 (2016). DOI 10.1007/s1128-015-1239-y. URL <https://doi.org/10.1007/s1128-015-1239-y>
- [418] World Economic Forum: *Quantum Computing Governance Principles* (2022). URL https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf
- [419] Wu, L.A., Byrd, M.S., Lidar, D.A.: *Polynomial-Time Simulation of Pairing Models on a Quantum Computer*. Phys. Rev. Lett. **89**, 057,904 (2002). DOI 10.1103/PhysRevLett.89.057904. URL <https://doi.org/10.1103/PhysRevLett.89.057904>
- [420] Wu, S.L., Sun, S., Guan, W., Zhou, C., Chan, J., Cheng, C.L., Pham, T., Qian, Y., Wang, A.Z., Zhang, R., Livny, M., Glick, J., Barkoutsos, P.K., Woerner, S., Tavernelli, I., Carminati, F., Di Meglio, A., Li, A.C.Y., Lykken, J., Spentzouris, P., Chen, S.Y.C., Yoo, S., Wei, T.C.: *Application of quantum machine learning using the quantum kernel algorithm on high energy physics analysis at the LHC*. Phys. Rev. Res. **3**, 033,221 (2021). DOI 10.1103/PhysRevResearch.3.033221. URL <https://link.aps.org/doi/10.1103/PhysRevResearch.3.033221>
- [421] Xie, Z.Y., Chen, J., Yu, J.F., Kong, X., Normand, B., Xiang, T.: *Tensor Renormalization of Quantum Many-Body Systems Using Projected Entangled Simplex States*. Phys. Rev. X **4**, 011,025 (2014). DOI 10.1103/PhysRevX.4.011025. URL <https://link.aps.org/doi/10.1103/PhysRevX.4.011025>
- [422] Xin, T., Wei, S., Cui, J., Xiao, J., Arrazola, I.n., Lamata, L., Kong, X., Lu, D., Solano, E., Long, G.: *Quantum algorithm for solving linear differential equations: Theory and experiment*. Phys. Rev. A **101**, 032,307 (2020). DOI 10.1103/PhysRevA.101.032307. URL <https://link.aps.org/doi/10.1103/PhysRevA.101.032307>

- [423] Yan, B., Sinitsyn, N.A.: *Analytical solution for nonadiabatic quantum annealing to arbitrary Ising spin Hamiltonian*. Nat. Commun. **13**(1), 2212 (2022). DOI 10.1038/s41467-022-29887-0. URL <https://www.nature.com/articles/s41467-022-29887-0>
- [424] Yan, F., Ilyasu, A.M., Le, P.Q.: *Quantum image processing: A review of advances in its security technologies*. Int. J. Quantum Inf. **15**(03), 1730,001 (2017). DOI 10.1142/S0219749917300017. URL <https://www.worldscientific.com/doi/abs/10.1142/S0219749917300017>
- [425] Yan, F., Ilyasu, A.M., Venegas-Andraca, S.E.: *A survey of quantum image representations*. Quantum Inf. Process. **15**(1), 1–35 (2016). DOI 10.1007/s11128-015-1195-6. URL <https://doi.org/10.1007/s11128-015-1195-6>
- [426] Yang, Z.C., Rahmani, A., Shabani, A., Neven, H., Chamon, C.: *Optimizing Variational Quantum Algorithms Using Pontryagin's Minimum Principle*. Phys. Rev. X **7**(2), 021,027 (2017). DOI 10.1103/PhysRevX.7.021027. URL <https://link.aps.org/doi/10.1103/PhysRevX.7.021027>
- [427] Yao, A.C.C.: *Monotone Bipartite Graph Properties are Evasive*. SIAM J. Comput. **17**(3), 517–520 (1988). DOI 10.1137/0217031. URL <https://epubs.siam.org/doi/10.1137/0217031>
- [428] Ye, Z., Li, L.: *Deterministic algorithms for the hidden subgroup problem*. Inform. and Comput. **289**, 104,975 (2022). DOI 10.1016/j.ic.2022.104975. URL <https://www.sciencedirect.com/science/article/pii/S0890540122001304>
- [429] Yepez, J.: *Highly covariant quantum lattice gas model of the Dirac equation*. arXiv preprint arXiv:1106.0739 (2011). URL <https://arxiv.org/abs/1106.0739>
- [430] Yoo, S., Bang, J., Lee, C., Lee, J.: *A quantum speedup in machine learning: finding a N-bit Boolean function for a classification*. New J. Phys. **6**(10), 103,014 (2014). URL <https://doi.org/10.1088/1367-2630/16/10/103014>
- [431] Yoshioka, N., Sato, T., Nakagawa, Y.O., Ohnishi, Y.y., Mizukami, W.: *Variational quantum simulation for periodic materials*. Phys. Rev. Res. **4**, 013,052 (2022). DOI 10.1103/PhysRevResearch.4.013052. URL <https://link.aps.org/doi/10.1103/PhysRevResearch.4.013052>
- [432] Young, A.P., Knysh, S., Smelyanskiy, V.N.: *Size Dependence of the Minimum Excitation Gap in the Quantum Adiabatic Algorithm*. Phys. Rev. Lett. **101**, 170,503 (2008). DOI 10.1103/PhysRevLett.101.170503. URL <https://link.aps.org/doi/10.1103/PhysRevLett.101.170503>
- [433] Young, A.P., Knysh, S., Smelyanskiy, V.N.: *First-Order Phase Transition in the Quantum Adiabatic Algorithm*. Phys. Rev. Lett. **104**, 020,502 (2010). DOI 10.1103/PhysRevLett.104.020502. URL <https://link.aps.org/doi/10.1103/PhysRevLett.104.020502>
- [434] Yu, C.M., Tsai, I.M., Chou, Y.H., Kuo, S.Y.: *Improving the network flow problem using quantum search*. In: 2007 7th IEEE Conference on Nanotechnology (IEEE NANO), pp. 1126–1129 (2007). DOI 10.1109/NANO.2007.4601381. URL <https://ieeexplore.ieee.org/document/4601381>. ISSN: 1944-9399
- [435] Yung, M.H., Aspuru-Guzik, A.: *A quantum–quantum Metropolis algorithm*. Proc. Natl. Acad. Sci. **109**(3), 754–759 (2012). DOI 10.1073/pnas.1111758109. URL <https://www.pnas.org/doi/abs/10.1073/pnas.1111758109>
- [436] Zalka, C.: *Efficient simulation of quantum systems by quantum computers*. Proc. R. Soc. London, Ser. A **454**, 313 (1996). URL <https://doi.org/10.1098/rspa.1998.0162>
- [437] Zanger, B., Mendl, C.B., Schulz, M., Schreiber, M.: *Quantum Algorithms for Solving Ordinary Differential Equations via Classical Integration Methods*. Quantum **5**, 502 (2020). URL <https://doi.org/10.22331/q-2021-07-13-502>
- [438] Zeguendry, A., Jarir, Z., Quafafou, M.: *Quantum Machine Learning: A Review and Case Studies*. Entropy-switz. **25**(2), 287 (2023). DOI 10.3390/e25020287. URL <https://www.mdpi.com/1099-4300/25/2/287>

- [439] Zhang, J., Feng, F., Zhang, Q.J.: *Quantum Method for Finite Element Simulation of Electromagnetic Problems*. 2021 IEEE MTT-S International Microwave Symposium (IMS) pp. 120–123 (2021). DOI 10.1109/IMS19712.2021.9574852. URL <https://doi.org/10.1109/IMS19712.2021.9574852>
- [440] Zhang, K., Korepin, V.E.: *Depth optimization of quantum search algorithms beyond Grover’s algorithm*. Phys. Rev. A **101**(3), 032,346 (2020). DOI 10.1103/PhysRevA.101.032346. URL <https://link.aps.org/doi/10.1103/PhysRevA.101.032346>
- [441] Zhao, Z., Fitzsimons, J.K., Fitzsimons, J.F.: *Quantum-assisted Gaussian process regression*. Phys. Rev. A **99**, 052,331 (2019). DOI 10.1103/PhysRevA.99.052331. URL <https://link.aps.org/doi/10.1103/PhysRevA.99.052331>
- [442] Zhao, Z., Pozas-Kerstjens, A., Rebentrost, P., Wittek, P.: *Bayesian deep learning on a quantum computer*. Quantum Mach. Intell. **1**(1-2), 41–51 (2019). DOI 10.1007/s42484-019-00004-7. URL <https://doi.org/10.1007/s42484-019-00004-7>
- [443] Zheng, Q., Zhu, P., Xue, S., Wang, Y., Wu, C., Yu, X., Yu, M., Liu, Y., Deng, M., Wu, J., Xu, P.: *Quantum algorithm and experimental demonstration for the subset sum problem*. Science China Information Sciences **65**(8), 182,501 (2022). DOI 10.1007/s11432-021-3334-1. URL <https://doi.org/10.1007/s11432-021-3334-1>
- [444] Zhou, L., Wang, S.T., Choi, S., Pichler, H., Lukin, M.D.: *Quantum Approximate Optimization Algorithm: Performance, Mechanism, and Implementation on Near-Term Devices*. Phys. Rev. X **10**(2), 021,067 (2020). DOI 10.1103/PhysRevX.10.021067. URL <https://link.aps.org/doi/10.1103/PhysRevX.10.021067>
- [445] Zhou, Z., Du, Y., Tian, X., Tao, D.: *QAOA-in-QAOA: Solving Large-Scale MaxCut Problems on Small Quantum Machines*. Phys. Rev. Appl. **19**(2), 024,027 (2023). DOI 10.1103/PhysRevApplied.19.024027. URL <https://link.aps.org/doi/10.1103/PhysRevApplied.19.024027>
- [446] Zoufal, C., Lucchi, A., Woerner, S.: *Variational quantum Boltzmann machines*. Quantum Machine Intelligence **3**(1), 7 (2021). DOI 10.1007/s42484-020-00033-7. URL <https://doi.org/10.1007/s42484-020-00033-7>

Índice alfabético

A

abeliano	95
adiabática	109
AES	98
alfabeto	91
álgebra conmutativa	94
algoritmo	
<i>de consulta cuántica</i>	95
<i>de estimación de fase</i>	46
<i>de Grover</i>	67, 90
<i>de Shor</i>	59, 93
HHL	53
análisis topológico de datos	99
anillo de enteros	97
annealer	109
aprendizaje automático	105
aproximación aditiva	100
árbol	101
<i>de expansión mínimo</i>	101, 102
autovalores	98

B

bra-vector	9
búsqueda	90, 93
<i>espacial</i>	90
<i>ordenada</i>	92

C

cadena	91
camino	101
carácter	97
ciclo	101
circuito cuántico de profundidad variable	
106	
clase de complejidad	
#P	79
BPP	79
BQP	79

BQP-completo	79
co-NP	78
DQC1	80
MA	80
NP	78
NP-completo	78
NP-difícil	78
P	78
PSPACE	79
QMA	79

clasificador cuántico multiclase	107
clausura de traza	100
clustering	105
códigos correctores de errores	97
coincidencia	91
computación	
<i>cuántica de reservorio</i>	107
<i>híbrida</i>	98
<i>variacional cuántica</i>	111
concordancia	91
conectividad	101
<i>st</i>	101
configuración de spin	75
conjetura de Aanderaa-Karp-Rosenberg	
101	
conmutatividad	94
conmutativo	95
convergente <i>k</i> -ésimo	60
criptoanálisis	97
criptografía	97, 98
<i>poscuántica</i>	98
cúbit	10
<i>auxiliar</i>	55
<i>limpio</i>	80
cuerpo	
<i>ciclotómico</i>	97

D

datos topológicos	99
descodificación	97
desplazamiento	97

<i>de fase</i>	22
diferencia estadística	102
Diffie-Hellman	98
distribución	102
división de Heegaard.....	100
DQC1-completo.....	100

E

ecuaciones	
<i>diferenciales ordinarias</i>	110
<i>en derivadas parciales</i>	111
esfera de Bloch	11
espectro	98
estado	
<i>básico</i>	10
<i>entrelazado</i>	19
<i>producto</i>	19
estimación de amplitud.....	90

F

factor de fase	22
finanzas.....	108
flujo.....	103
fórmula.....	91

G

grado de un cuerpo.....	97
grafo	101
grupo.....	94, 97
<i>conmutativo</i>	94
<i>de unidades</i>	97

H

homología persistente	99
-----------------------------	----

I

invariante	99, 100
<i>de Turaev-Viro</i>	100
<i>de Witten-Reshitikhin-Turaev</i>	100
isogenia.....	98

K

ket-vector	9
------------------	---

L

laplaciano	99
lista	92
logaritmo	93
lógica booleana.....	91, 93

M

máquina	
<i>de Boltzmann cuántica</i>	106
<i>de soporte vectorial con un estimador de núcleo cuántico</i>	107
<i>de temple cuántico</i>	109
<i>de Turing</i>	
determinista	78
no determinista.....	78
matriz.....	94, 95
<i>de adyacencia</i>	101
<i>de Pauli</i>	
<i>X</i>	22
<i>Y</i>	23
<i>Z</i>	23
métodos numéricos	
<i>para EDOs</i>	110
<i>para EDPs</i>	111
mínimos cuadrados	105
modelo	
<i>de lista de adyacencia</i>	101
<i>de matriz de adyacencia</i>	101
<i>híbrido de vecinos cercanos</i>	107
<i>Monte-Carlo de cadenas de Markov</i>	103

N

NISQ	93
norma L^1	102
nudo	100
número	
<i>de Betti</i>	99
<i>primo</i>	93

O

optimización 103–105
ordenamiento 92

P

paralelismo cuántico 37
patrón 91
Pauli
 X 22
 Y 23
 Z 23
p-cúbit 13
polilogaritmo 89
polinomio
 de Jones 100
 de Tutte 100
 HOMFLY 100
primalidad 93
primo 93
principio de no clonación 36
probabilidad 102
problema del determinante 95
producto 94
programa de lapso 95
propiedad
 evasiva 101
 monótona 101
puerta
 CNOT 27
 de desplazamiento de fase 22
 de factor de fase 22
 de Hadamard 23
 de medida 30
 lógica 24
 NOT controlada 27
 Pauli-X 22
 Pauli-Y 23
 Pauli-Z 23
 SWAP 28

Q

QA 104
QAOA 104, 105
quantum annealing 104
QUBO 73

R

rango 95
reconocimiento 91
red
 de convolución híbrida 106
 de flujo 103
 de tensores 108
 neuronal 105
RSA 98

S

símbolo de Legendre 97
simulación 108
simulated annealing 103
span program 95
subconjuntos 93
subgrupo
 no abeliano 96
 no conmutativo 96
 oculto 95
superposición 10
supremacía cuántica 80

T

teletransportación cuántica 37
temple
 cuántico 104
 simulado 103
teoría cuántica de campos 100
testigo cuántico 79
transformada de Fourier cuántica . 37, 95
 inversa 45
trenza 100

U

unidad 97

V

valor del flujo 103
variedad 100
ventaja cuántica 80
verificación 94