Computación cuántica

Seminario: Introducción a la física cuántica segundo semestre 2025–2026

Fernando Chamizo https://matematicas.uam.es/~fernando.chamizo/

La idea de que la evolución de sistemas cuánticos podría utilizarse para llevar a cabo cálculos tiene ya unas décadas, casi medio siglo. Desde entonces se han diseñado algoritmos teóricos que tendrían consecuencias espectaculares implementados en un ordenador cuántico ideal. En los últimos años hemos asistido a un esfuerzo económico y humano sin precedentes para hacer realidad ordenadores cuánticos con potenciales aplicaciones prácticas.

4.1. Qubits y circuitos cuánticos

La computación tradicional utiliza el *bit* como unidad de información mientras que la *computación cuántica* está basada en el *qubit* que es solo otro nombre que recibe un vector de $\mathbb{C}^2$ que representa un estado de espín. En este contexto lo común es escribir $|0\rangle$ en lugar de $|+\rangle$ y $|1\rangle$ en lugar de $|-\rangle$. Además, casi siempre se impone la normalización. De esta forma, un qubit es

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{con} \quad \alpha,\beta\in\mathbb{C} \quad \text{tales que} \quad |\alpha|^2+|\beta|^2=1.$$

Para un matemático, $|0\rangle$ y $|1\rangle$ son formas raras de escribir los vectores de la base canónica en dimensión 2 y qubit es un nombre curioso para un punto de la circunferencia unidad de $\mathbb{C}^2$.

Un bit solo puede tomar dos valores: 0 y 1, mientras que un qubit puede tomar toda una circunferencia compleja de valores. En principio contiene infinitamente más información. Sin embargo, por lo que sabemos del Postulado 3, cuando accedemos a un qubit con una medición que decida entre $|0\rangle$ y $|1\rangle$, colapsará en uno de estos dos estados con cierta probabilidad. En este sentido, un qubit medido se transforma en un bit y, además, de manera no determinista, lo que sugiere a primera vista que la computación cuántica no puede superar a la tradicional. La escapatoria a esta paradoja radica en lo que se puede hacer antes de medir. En términos matemáticos, a n qubits se aplican operadores de $\mathbb{C}^2\otimes\overset{n\text{ veces}}{\cdots}\otimes\mathbb{C}^2\cong\mathbb{C}^{2^n}$ que son objetos mucho más complejos que las combinaciones de puertas lógicas que podamos aplicar a n bits, pues, aunque estas estas sean un número inmensamente grande, cada una opera de manera discreta. En [12] se explica de una manera poética:

> [...] *so a quantum state of such a system is specified by* 2^n *amplitudes. For* $n = 500$ *this number is larger than the estimated number of atoms in the Universe! Trying to store all these complex numbers would not be possible on any conceivable classical computer. Hilbert space is indeed a big place. In principle, however, Nature manipulates such enormous quantities of data, even for systems containing only a few hundred atoms. It is as if Nature were keeping* 2^{500} *hidden pieces of scratch paper on the side, on which she performs*

her calculations as the system evolves. This enormous potential computational power is something we would very much like to take advantage of.

La abreviatura para productos tensoriales se aplica también con la nueva notación, así $|010\rangle$ significa $|0\rangle \otimes |1\rangle \otimes |0\rangle$. Denotaremos con B_n las cadenas de longitud formadas por ceros y unos (las listas de n bits). Al ordenarlas por orden creciente como números binarios obtendremos una base de $\mathbb{C}^2 \otimes \overset{n \text{ veces}}{\cdots} \otimes \mathbb{C}^2$, que no es otra que la lexicográfica, que denotaremos $\mathcal{B}_n$. Por ejemplo,

$$B_2 = \{00, 01, 10, 11\} \qquad \text{y} \qquad \mathcal{B}_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

Una vez fijado el número de qubits n, se suele trabajar en esta base del espacio de Hilbert del sistema cuántico correspondiente y por ello se dice que es la *base computacional*. Los elementos del espacio se dice que son *registros cuánticos*. A veces se identifican los elementos de B_n con su valor como números binarios y, de este modo, el n-ésimo elemento de $\mathcal{B}_n$ es $|n-1\rangle$. Por ejemplo, para $n = 2$ se podría escribir $|2\rangle$ en lugar de $|10\rangle$. Obviamente, hay cierto abuso de notación en ello, pero en la práctica es casi imposible que lleve a confusión. Para practicar con estas notaciones, aquí están tres formas de representar un registro $|\varphi\rangle$ (normalizado) de n qubits:

$$|\varphi\rangle = \sum_{b \in B_n} a_b |b\rangle = \sum_{|b\rangle \in \mathcal{B}_n} a_b |b\rangle = \sum_{b=0}^{2^n-1} a_b |b\rangle \qquad \text{con} \qquad \sum_{b \in B_n} |a_b|^2 = 1.$$

Según el Postulado 2, la evolución de un registro de n qubits viene dada por una matriz unitaria $2^n \times 2^n$. Una *computación cuántica* desde el punto de vista matemático no es más que la aplicación de matrices unitarias y proyecciones. Estas últimas corresponden a mediciones y pueden posponerse al final [12, §4.4], siendo la parte más sencilla. De este modo, lo que hace un *ordenador cuántico* es fundamentalmente multiplicar por matrices unitarias. Se conoce que con matrices unitarias aplicadas a elementos de $\mathcal{B}_2$ se pueden simular las puertas lógicas [11, §4.3], por tanto, desde un punto de vista teórico un ordenador cuántico podría hacer todas las tareas que hace un ordenador convencional (aunque esto es radicalmente falso en la práctica con los desarrollos técnicos presentes).

Como 2^n crece exponencialmente, en computación cuántica no se escriben demasiadas matrices completas, más bien se indica cómo construirlas a partir de otras más sencillas. Sin que haya una definición precisa, estas matrices sencillas se llaman *puertas cuánticas* debido a que guardan cierta analogía con las puertas lógicas de los ordenadores convencionales.

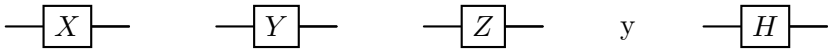
El caso más simple es $n = 1$, el de un solo qubit, con matrices de dimensión $2^1 = 2$. Por ejemplo, se llama *puerta de Hadamard*[1] a la que tiene como matriz en la base $\mathcal{B}_1 = \{ |0\rangle, |1\rangle \}$

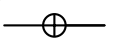
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Para indicar una computación cuántica se emplean representaciones pictóricas de las puertas cuánticas y las mediciones, conformando un *circuito cuántico* que dada una entrada a la izquierda genera una salida a la derecha. En el caso de las puertas cuánticas que actúan sobre

[1] El nombre proviene de que las *matrices de Hadamard* son las matrices unitarias tales que todos sus elementos son de la forma $\pm\alpha$ con $\alpha \in \mathbb{R}$, que fueron estudiadas por J. Hadamard. Se conjetura que si la dimensión es un múltiplo de 4 tales matrices existen. Para potencias de dos es fácil considerando $H \otimes H \otimes \cdots \otimes H$.

un solo qubit la representación es un rectángulo que encierra el nombre de la matriz unitaria con una línea a la izquierda y otra a la derecha que representan los "cables" de entrada y de salida. A las matrices de Pauli en computación cuántica se les cambia el nombre a X, Y y Z. Así, las representaciones pictóricas de las puertas cuánticas asociadas a ellas y a H son:



La primera, la correspondiente a la primera matriz de Pauli σ_1, también se representa con el símbolo  y a veces se dice que es la puerta NOT. El nombre se debe a que σ_1 intercambia $|0\rangle$ y $|1\rangle$ que es la negación de un bit en el sentido tradicional.

Cuando se opera con $n > 1$ qubits se conviene en los circuitos que los cables que están más arriba corresponden a los bits de más significativos. Por ejemplo, si en la entrada (a la izquierda) de un circuito hay tres cables, $n = 3$, e introducimos $|100\rangle$, entonces por el cable superior entrará $|1\rangle$ y por los otros $|0\rangle$.

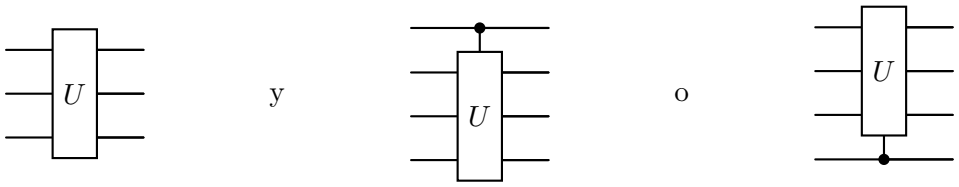
La operación más básica con dos qubits es la puerta CNOT (que abrevia *controlled* NOT). El circuito que la representa es el siguiente:

Su efecto sobre los elementos de la base computacional $\mathcal{B}_2$ es que si el primer qubit, el del cable superior, es $|0\rangle$, entonces se comporta como la identidad y si es $|1\rangle$, entonces preserva el primer qubit y aplica NOT al segundo. Por supuesto, cuando la puerta CNOT se aplica a elementos que no son de la base, se procede por linealidad (recuerda que $\vec{v} \otimes \vec{w}$ es lineal en $\vec{v}$ y $\vec{w}$). Por ejemplo, aplicaría $\frac{3}{5}|10\rangle + \frac{4}{5}|11\rangle$ en $\frac{3}{5}|11\rangle + \frac{4}{5}|10\rangle$ y $\frac{3}{5}|01\rangle + \frac{4}{5}|11\rangle$ en $\frac{3}{5}|01\rangle + \frac{4}{5}|10\rangle$, lo que podríamos representar como:

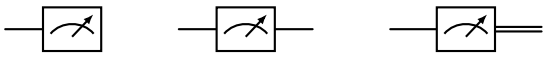
Es importante notar que en el segundo caso hemos partido de un estado producto y hemos llegado a uno entrelazado. Una de las grandes fortalezas de la computación cuántica (y también de las dificultades para llevarla a la práctica) es poder trabajar con estados altamente entrelazados que simulan una computación paralela más allá de lo imaginable con los métodos convencionales (núcleos, *clusters*, etc.). Se puede demostrar que podríamos construir el circuito correspondiente a cualquier matriz unitaria solo con puertas de un bit y puertas CNOT [12, §4.5.2], pero limitarnos a ellas daría lugar a esquemas complicados.

Generalizando lo anterior, la acción de una matriz unitaria que actúa en registros de n qubits, se representa en un circuito mediante una caja que encierra el nombre de la matriz con n cables de entrada y de salida. Un punto relleno en un cable por encima de la caja y conectado a ella significa, en analogía con la puerta CNOT, que el primer qubit controla a los otros n, esto es, que si es $|0\rangle$, el bloque actúa como la identidad y si es $|1\rangle$, conserva ese $|1\rangle$ y al registro correspondiente a los cables que pasan por la caja le aplica la matriz. Se dice que el primer qubit *controla* la puerta cuántica asociada a la matriz. De la misma

forma se podría introducir un control con el último qubit. En breve, $|1\rangle$ activa la acción de la matriz y $|0\rangle$ preserva la entrada sin cambios. Para U unitaria de dimensión $8 = 2^3$, la puerta correspondiente y dicha puerta controlada por un cuarto qubit en primer o en último lugar, se representarían mediante:

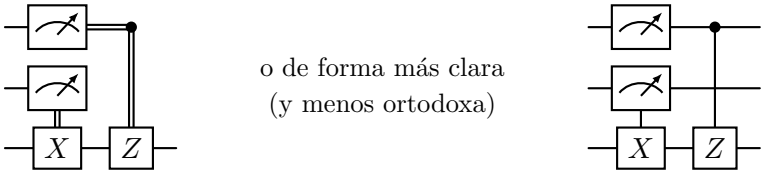


El último elemento básico de los circuitos cuánticos son las mediciones, que corresponden a las proyecciones sobre $|0\rangle$ y sobre $|1\rangle$. Se indican con una especie de dial con una aguja y un cable de entrada, el de salida típicamente se omite o se duplica:



La segunda representación es poco común. Omitir el cable de salida es natural porque las mediciones se posponen habitualmente al final del circuito. Duplicarlo proviene de que los cables dobles indican "bits clásicos". Una vez que el estado ha colapsado a $|0\rangle$ o a $|1\rangle$ tras la medición, ya está totalmente determinado, es un bit clásico que no será afectado por mediciones posteriores. Estos bits no dejan de ser estados especiales de qubits y por consiguiente se pueden seguir usando dentro de una computación cuántica, para controlar una puerta o para servir de entrada a ella.

Para practicar, analicemos el efecto del siguiente circuito sobre $|b\rangle \otimes |\varphi\rangle$ con $b \in B_2$ y $|\varphi\rangle$ un qubit arbitrario:

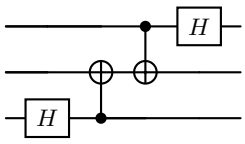


Los dos primeros qubits de $|b\rangle \otimes |\varphi\rangle$ se comportan como bit clásicos porque $|b\rangle \in \mathcal{B}_2$ y al medirlos se obtiene de nuevo $|b\rangle$. Si $b = 00$ entonces no se activan ni X ni Z, sino que ambas se comportan como la identidad y también $|\varphi\rangle$ queda invariante. Por el contrario, si $b = 11$ se activan ambas y el efecto será aplicar primero X y después Z que actuarán sobre $|\varphi\rangle$ para dar $\sigma_3\sigma_1 |\varphi\rangle = i\sigma_2 |\varphi\rangle$ que es el mismo estado que aplicar σ_2, o Y con la notación de la computación cuántica. Los otros dos casos se tratan de forma similar para completar la tabla

Entrada:	$\|00\rangle \otimes \|\varphi\rangle$	$\|01\rangle \otimes \|\varphi\rangle$	$\|10\rangle \otimes \|\varphi\rangle$	$\|11\rangle \otimes \|\varphi\rangle$
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
Salida:	$\|00\rangle \otimes \|\varphi\rangle$	$\|01\rangle \otimes \sigma_1 \|\varphi\rangle$	$\|10\rangle \otimes \sigma_3 \|\varphi\rangle$	$i \|11\rangle \otimes \sigma_2 \|\varphi\rangle$

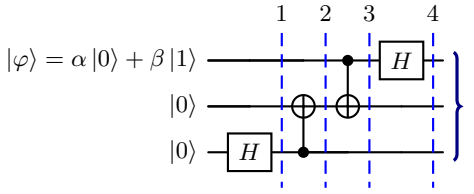
Esto recuerda al tipo de expresiones que aparecían en el teletransporte.

Practiquemos ahora comprobando que



aplica $|\varphi\rangle\otimes|00\rangle \downarrow \frac{1}{2}|00\rangle\otimes|\varphi\rangle+\frac{1}{2}|01\rangle\otimes\sigma_1|\varphi\rangle+\frac{1}{2}|10\rangle\otimes\sigma_3|\varphi\rangle-\frac{i}{2}|11\rangle\otimes\sigma_2|\varphi\rangle$

Hay cuatro pasos en el circuito que analizaremos uno a uno escribiendo $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.



El primer paso aplica H al tercer qubit, que es $|0\rangle$. Es como calcular $H\vec{e}_1$ y resulta

$$\text{Paso 1} \to |\varphi\rangle\otimes|0\rangle\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}} = |\varphi\rangle\otimes\frac{|00\rangle+|01\rangle}{\sqrt{2}}.$$

Después se usa el tercer qubit para controlar una puerta NOT (la aplicación de σ_1) sobre el segundo. Es decir, cuando sea $|1\rangle$ cambia al segundo y no hace nada cuando es $|0\rangle$. Así,

$$\text{Paso 2} \to |\varphi\rangle\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}} = |\varphi\rangle\otimes|\Phi_0\rangle\,.$$

En el tercer paso participa el primer qubit. La parte $\alpha\,|0\rangle$ deja el segundo qubit invariante y la parte $\beta\,|1\rangle$ la cambia con una puerta NOT. Por tanto,

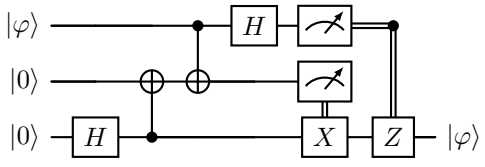
$$\text{Paso 3} \to \alpha\,|0\rangle\otimes|\Phi_0\rangle + \beta\,|1\rangle\otimes(\sigma_1\otimes 1)\,|\Phi_0\rangle = \frac{\alpha}{\sqrt{2}}\,|000\rangle + \frac{\alpha}{\sqrt{2}}\,|011\rangle + \frac{\beta}{\sqrt{2}}\,|110\rangle + \frac{\beta}{\sqrt{2}}\,|101\rangle\,.$$

Finalmente, en el paso 4 debemos aplicar H al primer qubit. El efecto es $|0bc\rangle \mapsto \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|bc\rangle$ y $|1bc\rangle \mapsto \frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes|bc\rangle$. Sustituyendo en el paso anterior, se obtiene

$$\text{Paso 4} \to \frac{\alpha}{2}\,|000\rangle + \frac{\beta}{2}\,|001\rangle + \frac{\beta}{2}\,|010\rangle + \frac{\alpha}{2}\,|011\rangle + \frac{\alpha}{2}\,|100\rangle - \frac{\beta}{2}\,|101\rangle - \frac{\beta}{2}\,|110\rangle + \frac{\alpha}{2}\,|111\rangle$$

que es el resultado esperado.

En definitiva, combinando ambos circuitos en



conseguimos teletransportar $|\varphi\rangle$ del primer qubit al tercero.

Terminemos con un breve sumario histórico. Desde que unos pocos visionarios, como el matemático Y. Manin en 1980 y algo después Feynman, sugirieran la computación cuántica, pasaron años durante los cuales se desarrollaron algunos algoritmos sin que hubiera máquinas cuánticas en las que implementarlos. A mediados de los años 90 la publicación de [2] acercó la posibilidad de que crear qubits y puertas cuánticas básicas, especialmente la CNOT. De hecho, en 1998 se logró construir el primer "ordenador" cuántico que contaba solo con dos qubits. El área permaneció más bien estancada en el plano práctico, no así en el teórico, hasta que desde hace pocos años grandes empresas han realizado inversiones ingentes con el objetivo de desarrollar ordenadores cuánticos con aplicaciones prácticas. Fruto de este esfuerzo ha habido un avance técnico notable y una de estas empresas con un ordenador de 54 qubits anunció en 2019 haber conseguido la *supremacía cuántica*. Este termino se refiere a resolver un problema que un ordenador clásico no sería capaz de abordar en tiempo razonable. El anuncio fue muy discutido con razones poderosas (sobre todo por una empresa de la competencia). En cualquier caso, hay que dejar claro que el problema era artificial, fabricado expresamente para resaltar las ventajas cuánticas. Actualmente la situación de la computación cuántica es incierta. Parece que la opinión de los expertos es que no es tan acuciante incrementar el número de qubits como controlar la *decoherencia* (la pérdida de la naturaleza cuántica por interacción con el ambiente, que fue una preocupación desde el principio [13]). También parece que se ha desechado la posibilidad a medio plazo de un ordenador cuántico de propósito general que pueda sustituir a los que usamos habitualmente, y más bien se cree que podrían ser útiles para ciertos propósitos particulares.

4.2. El algoritmo de Grover

Suponemos una lista de datos distintos que tiene cardinal 2^n (esto no es una restricción significativa porque siempre se podría completar con datos artificiales para conseguir una potencia de dos) y queremos encontrar un dato en la lista determinando la posición que ocupa.

Parece claro que la única posibilidad es recorrer la base de datos y eso requiere en media 2^{n-1} consultas. En 1996 L. Grover diseñó un algoritmo probabilista [5] que permite completar esta tarea haciendo del orden de $2^{n/2}$ "consultas cuánticas" con una probabilidad de fracaso que tiende exponencialmente a cero con n. El truco está en que la computación cuántica permite que estas consultas se realicen de algún modo en paralelo. En palabras de Grover [6]:

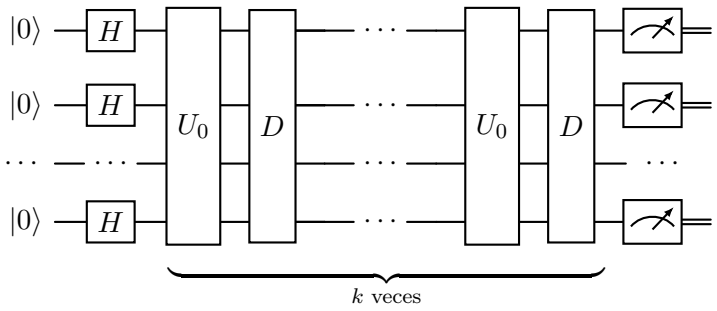
> [...] *imagine a phone directory containing N names arranged in completely random order. To find someone's phone number with a probability of* 50 %, *any classical algorithm (whether deterministic or probabilistic) will need to access the database a minimum of* $0.5N$ *times. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names.*

El circuito que corresponde al algoritmo de Grover está representado más abajo. Se parte de $|0\cdots 0\rangle$, el primer elemento de la base $\mathcal{B}_n$, se aplican sucesivas puertas lógicas, un bloque de dos de ellas k veces, y se procede a una medición final. Tras dicha medición obtendremos $|b\rangle$ con $b \in B_n$ que se identifica con una posición de nuestra base de datos si las numeramos con enteros en $[0, 2^n)$. Digamos que el dato que deseamos buscar está en la posición binaria b_0,

entonces el funcionamiento del algoritmo es:

$$|0\overset{n \text{ veces}}{\cdots\cdots}0\rangle \xrightarrow{\text{circuito}} |b\rangle \quad \text{con } b \in B_n \quad \text{tal que} \quad \text{Prob}(b = b_0) \geq 1 - 2^{-n}.$$

Por ejemplo, si lográsemos trabajar con 64 qubits la probabilidad de que el algoritmo fracasase sería menor que $6 \cdot 10^{-20}$.



Para dar sentido al circuito tenemos que definir los operadores U_0 y D asociados a las puertas y escoger el número k. El primero de los operadores, U_0, es el que aleja este y otros algoritmos cuánticos de la práctica. Es lo que se conoce en la jerga con el eufemismo de un *oráculo*, un operador que funciona como una "caja negra" sin especificar su construcción, que quizá solo podría llevar a cabo alguien que conociera la solución del problema. En nuestro caso es un operador que nos avisa de que hemos encontrado la solución cambiándola de signo:

$$U_0 |b\rangle = |b\rangle \quad \text{si } b \in B_n - \{b_0\} \qquad \text{y} \qquad U_0 |b_0\rangle = -|b_0\rangle$$

Una fórmula compacta alternativa surge si conocemos las *transformaciones de Householder*[2]

$$U_0 = 1 - 2 |b_0\rangle \langle b_0| ,$$

donde, como otras veces, 1 representa el operador identidad. La primera forma de la definición quizá nos dé más esperanzas prácticas sobre el oráculo porque, haciendo honor a su nombre, funciona como una consulta a la base de datos. Sin embargo, esto es engañoso. La segunda forma recuerda que U_0 actúa sobre todo $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, no solo sobre la base computacional. En un estado muy superpuesto, no responde a una consulta clásica sino a muchas. Parece ser que en las demostraciones experimentales hasta la fecha del algoritmo de Grover solo se han usado tres qubits y colecciones predeterminadas de oráculos [4].

El operador D que sigue al oráculo en el circuito es una transformación de Householder salvo un signo:

$$D = 2 |\eta\rangle \langle \eta| - 1 \qquad \text{con} \quad |\eta\rangle = H|0\rangle \overset{n \text{ veces}}{\otimes \cdots \otimes} H|0\rangle = \frac{1}{2^{n/2}} \sum_{b \in B_n} |b\rangle .$$

[2]Son aquellas de la forma $1 - 2|\varphi\rangle\langle\varphi|$ con $|\varphi\rangle$ normalizado. Son unitarias, hermíticas y sencillas de construir. Se utilizan ampliamente en cálculo numérico. A. S. Householder las introdujo originalmente como parte de un algoritmo para diagonalizar.

La segunda igualdad en la definición de $|\eta\rangle$ es prácticamente notación: el producto tensorial de cadenas de bits se representa concatenándolas, por ejemplo, $|1\rangle \otimes |01\rangle = |101\rangle$. Este operador no es un oráculo que dependa de la solución, por tanto, es teóricamente construible de manera universal. Definimos el vector normalizado auxiliar

$$(1) \qquad |\psi\rangle = \frac{1}{\sqrt{2^n-1}} \sum_{b\in B_n-\{b_0\}} |b\rangle \qquad \text{que verifica} \qquad |\eta\rangle = 2^{-n/2}\,|b_0\rangle + \sqrt{1-2^{-n}}\,|\psi\rangle\,.$$

Al sustituir $|\eta\rangle$ en la definición de D, tras unos cálculos tediosos y simplificando con $\langle\psi|b_0\rangle$, se obtiene

$$DU_0 = (1+r)\big(\,|b_0\rangle\,\langle b_0| + |\psi\rangle\,\langle\psi|\,\big) + \sqrt{1-r^2}\big(\,|b_0\rangle\,\langle\psi| - |\psi\rangle\,\langle b_0|\,\big) - 1 \qquad \text{con} \quad r = 1-2^{1-n}.$$

Como $|\eta\rangle$ se obtiene cuando en el circuito $|0\cdots0\rangle$ pasa por las puertas de Hadamard, antes de las mediciones tendremos $(DU_0)^k\,|\eta\rangle$ y la probabilidad de que tras ellas el estado colapse al que representa $|b_0\rangle$ es

$$p = \big|\,\langle b_0|(DU_0)^k|\eta\rangle\,\big|^2.$$

Sea W el subespacio con base (ortonormal) $\{|b_0\rangle\,,|\psi\rangle\}$. Según (1), se cumple $|\eta\rangle \in W$ y tiene coordenadas $2^{-n/2}$ y $\sqrt{1-2^{-n}}$ en dicha base. Por supuesto, las de $|b_0\rangle$ y $|\psi\rangle$ coinciden con los vectores canónicos. Así pues, pasando a coordenadas, la probabilidad anterior se reescribe como

$$p = \left|\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix} r & \sqrt{1-r^2} \\ -\sqrt{1-r^2} & r\end{pmatrix}^k \begin{pmatrix} 2^{-n/2} \\ \sqrt{1-2^{-n}}\end{pmatrix}\right|^2.$$

Introduzcamos un ángulo $-\frac{\pi}{2} < \alpha < 0$ tal que $\operatorname{sen}\frac{\alpha}{2} = -2^{-n/2}$. Se tiene $r = \cos\alpha$ y $\sqrt{1-r^2} = -\operatorname{sen}\alpha$ por las fórmulas del ángulo doble. Por tanto, la matriz anterior es la de un giro de ángulo α y al elevar a k se obtendrá la de otro de ángulo $k\alpha$. En definitiva,

$$p = \left|\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix} \cos(k\alpha) & -\operatorname{sen}(k\alpha) \\ \operatorname{sen}(k\alpha) & \cos(k\alpha)\end{pmatrix}\begin{pmatrix} -\operatorname{sen}\frac{\alpha}{2} \\ \cos\frac{\alpha}{2}\end{pmatrix}\right|^2 = \operatorname{sen}^2\big((k+1/2)\alpha\big).$$

Finalmente, escogemos k como la parte entera de $-\frac{\pi}{2\alpha}$, lo que asegura $0 \le \frac{\pi}{2} + k\alpha < -\alpha$ y permite deducir

$$p = \operatorname{sen}^2\big((k+1/2)\alpha\big) = \cos^2\left(\frac{\pi}{2} + k\alpha + \frac{\alpha}{2}\right) \ge \cos^2\frac{\alpha}{2} = 1-2^{-n}$$

que es la cota anunciada para la probabilidad.

Es importante notar que como $\alpha \sim -2^{1-n/2}$ entonces el número de pasos k es comparable a $2^{n/2}$, lo cual es comparable a la raíz del número de consultas medio a la base de datos en un ordenador convencional. Se conoce [16], [12, §6.6] que un algoritmo de búsqueda no puede mejorar demasiado al de Grover en cuanto a número de pasos.

Una pequeña anécdota es que Grover publicó inicialmente su algoritmo en las actas de un congreso de teoría de la computación [5] y allí aparece revestido de cinco teoremas (sencillos) con sus pruebas y corolarios. Sin embargo, cuando después lo hizo en una revista de física [6] se desprendió de esa estructura tan matemática.

4.3. El algoritmo de Shor

Sin duda el algoritmo más citado de la computación cuántica es el introducido por Shor [14] en 1997 para encontrar factores no triviales de un número impar $N \in \mathbb{Z}_{>2}$. La razón es que uno de los criptosistemas más famosos está basado en la dificultad para completar esta tarea con los algoritmos conocidos si N es enorme [7]. Además, algunas variantes permitirían también ataques a otros criptosistemas y métodos de intercambio de claves. La existencia del algoritmo de Shor ha marcado una tendencia actual a la *criptografía poscuántica*, aquella invulnerable a potenciales ordenadores cuánticos futuros.

A pesar del abultado número de citas, no es tan fácil encontrar descripciones detalladas completas del algoritmo de Shor, incluso en la literatura especializada. Por ejemplo, en [12], seguramente el texto más empleado de computación cuántica, se deja mucha tarea al lector (por el contrario, dado el carácter de [15], sorprende su nivel de detalle). Hay varias razones que contribuyen a ello, la más general es que no es un algoritmo sencillo. Por otro lado, requiere algunos conocimientos de teoría de números elemental que quizá no sean tan familiares para los interesados en computación cuántica. Finalmente, tampoco ayuda que en una parte del algoritmo sea mejor emplear computación tradicional y en otra, cuántica.

Lo que daremos aquí es una descripción más detallada que las habituales, pero no totalmente autocontenida, pues algún punto aritmético se relegará a referencias. Supondremos conocido el lenguaje de las congruencias e indicaremos con $\gcd(a, b)$ el máximo común divisor de dos enteros a y b no simultáneamente nulos.

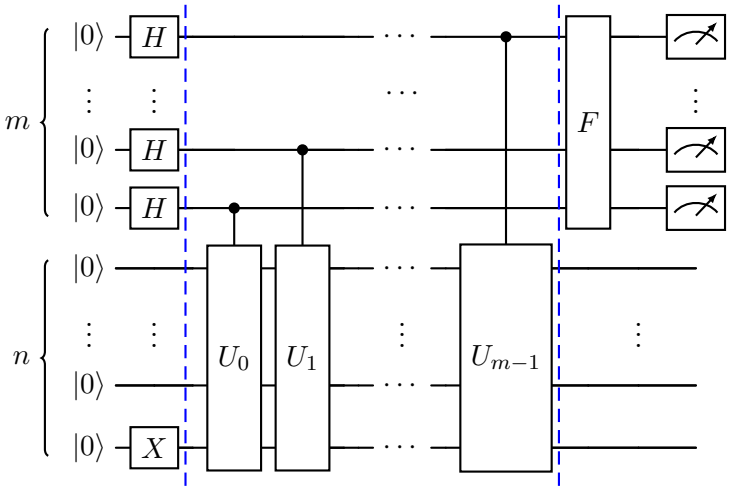
En primer lugar hay que enunciar el esquema teórico del algoritmo de Shor, cuya entrada es el número impar $N \in \mathbb{Z}_{>2}$ del que deseamos hallar un factor no trivial y un entero auxiliar $2 \leq a < N$ elegido al azar. Dependiendo de su elección el algoritmo puede tener éxito o no. Suponemos que N no es primo, porque no tendría sentido problema, y también excluimos las potencias de primos (hay buenos algoritmos [7] para detectar estos casos). El esquema teórico consta de tres pasos:

① Si $\gcd(a, N) \neq 1$, entonces a es un factor no trivial y el algoritmo termina.
② Se calcula el orden multiplicativo r de a, el menor $r \in \mathbb{Z}^+$ tal que $a^r \equiv 1 \pmod{N}$.
③ Si r es par y $a^{r/2} \not\equiv -1 \pmod{N}$, entonces $\gcd\left(N, a^{r/2} + 1\right)$ es un factor no trivial.

Si al llegar al tercer paso r es impar o r es par con $a^{r/2} \equiv -1 \pmod{N}$, el algoritmo no funciona y hay que probar con otro a. Se conoce (esencialmente por el teorema chino del resto y la existencia de raíces primitivas [8, §3.9]), que si N no es potencia de un primo el grupo multiplicativo módulo N es suma directa de al menos dos grupos cíclicos de orden par, por tanto, hay muchos elementos con orden par y hay raíces cuadradas de la unidad distintas de 1 y -1. Con ello, la probabilidad de éxito es mayor que cierta constante y a base de ejecutar estos pasos con muchos valores de a la probabilidad de fracaso tiende exponencialmente a cero. El algoritmo es, por tanto, probabilista.

Los pasos ① y ③ se pueden llevar a cabo eficientemente en un ordenador convencional incluso para números de miles de cifras o más (gracias al algoritmo de Euclides y de exponenciación de congruencias [7, §1.3.2]). Por otro lado, no se conocen algoritmos convencionales que calculen el orden requerido en ② para números enormes. Nótese el parecido con el problema del logaritmo discreto.

Justamente, la parte cuántica del algoritmo de Shor es el cálculo del orden, para lo cual se utiliza un circuito de la forma:



En la entrada, como se indica, hay $m+n$ ceros. Tomando $m = 2n+1$ ya se tiene un algoritmo aceptable y con m mayor se incrementa la posibilidad de éxito, ya que esta parte cuántica del algoritmo también es probabilista: no siempre a partir de la salida del circuito inferiremos el orden correcto. Hay que comprobar el resultado y ejecutar de nuevo el circuito en caso de fracaso. La n hay que escogerla de forma que 2^n sea mayor que N.

Habíamos convenido que cuando tratamos con n qubits, con el obvio abuso de notación, para k un entero no negativo $|k\rangle$ se refiere al elemento $|b\rangle \in \mathcal{B}_n$ tal que b es la representación binaria de k. Por ejemplo, si $n = 4$ entonces $|7\rangle$ significa $|0111\rangle$. ahora extendemos un poco el convenio entendiendo que si k es una potencia que supera a N nos referimos a su residuo módulo N. Por ejemplo, si $n = 5$ y $N = 21$, entonces $|5^{2026}\rangle$ significa $|16\rangle$, que es $|10000\rangle$, porque el resto de 5^{2026} al dividir por 21 es 16. Con este convenio y la notación de ② definimos los vectores normalizados

$$|u_j\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \ell j/r} \, |a^\ell\rangle \,, \qquad \text{con } j = 0, 1, \ldots, r-1.$$

Por supuesto, no sabemos construirlos porque nuestro objetivo es calcular r. Aunque los desconozcamos individualmente, como la suma de raíces k-ésimas de la unidad es nula excepto para $k = 1$, al sumar los $|u_j\rangle$ solo subsistirá la contribución de $\ell = 0$, esto es,

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \ell j/r} \, |u_j\rangle$$

donde, según el convenio, $|1\rangle$ representa $|00\cdots01\rangle \in \mathcal{B}_n$.

En el circuito, este $|1\rangle$ es lo que se obtiene con los n qubits inferiores, los menos significativos, antes de la línea de puntos izquierda debido a la presencia de la puerta X. En los m qubits

superiores, los más significativos, se obtiene $\sum_{b\in B_m}|b\rangle$ normalizado, igual que en el algoritmo de Grover. En definitiva, el vector correspondiente al estado antes de dicha línea de puntos es

$$|\psi_1\rangle = \frac{1}{2^{m/2}}\sum_{b\in B_m}|b\rangle\otimes|1\rangle = \frac{1}{2^{m/2}\sqrt{r}}\sum_{b\in B_m}\sum_{j=0}^{r-1}|b\rangle\otimes|u_j\rangle\,.$$

Para cada $0\le d<m$ consideramos el operador que actúa sobre $|\ell\rangle\in\mathcal{B}_n$ como

$$U_d\,|\ell\rangle = \begin{cases}|a^{2^d}\ell\rangle & \text{si } 0\le\ell<N,\\ |\ell\rangle & \text{en otro caso}\end{cases}$$

donde se aplica a $a^{2^d}\ell$ el mismo convenio que a las potencias, esto es, se identifica con su resto al dividir por N. Por ① sabemos que $\gcd(a^{2^d},N)=1$, entonces la multiplicación por a^{2^d} solo reordena los restos módulo N [8, §2.3]. En particular U_d reordena los elementos de la base computacional $\mathcal{B}_n$ y, por tanto, es un operador unitario que da lugar a una puerta cuántica válida.

Se cumple

$$U_0\,|u_j\rangle = \frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1}e^{-2\pi i\ell j/r}\,|a^{\ell+1}\rangle = \frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1}e^{-2\pi i(\ell-1)j/r}\,|a^{\ell}\rangle = e^{2\pi ij/r}\,|u_j\rangle\,.$$

Es decir, los $|u_j\rangle$ son autovalores del operador unitario U_0 con autovalores distintos, en particular, son ortonormales [10]. En general,

$$U_d = U_0^{2^d} \qquad \text{implica} \qquad U_d\,|u_j\rangle = e^{2\pi ij2^d/r}\,|u_j\rangle\,.$$

Cada $b\in B_m$ corresponde a la expresión en bits, en binario, de un número $0\le k<m$. Esto es,

$$k = b_0 + 2^1b_1 + 2^2b_1 + \cdots + 2^{m-1}b_{m-1} = \sum_{d=0}^{m-1}2^db_d \qquad \text{con} \quad b_d\in\{0,1\}.$$

Al utilizar el bit b_d para controlar la puerta U_d, como indica el circuito, el efecto sobre $|u_j\rangle$ será multiplicar por $e^{2\pi ij2^d/r}$ si $b_d=1$ y no hacer nada (la identidad) si $b_d=0$. Ambas posibilidades se resumen en multiplicar por $e^{2\pi ijb_d2^d/r}$. De esta forma, la acción conjunta de las puertas controladas actúa sobre $|k\rangle\otimes|u_j\rangle$ de la siguiente forma:

$$|k\rangle\otimes|u_j\rangle \longmapsto \Big(\prod_{d=0}^{m-1}e^{2\pi ijb_d2^d/r}\Big)\,|k\rangle\otimes|u_j\rangle = e^{2\pi ijk/r}\,|k\rangle\otimes|u_j\rangle$$

y, recordando la fórmula para el vector $|\psi_1\rangle$ en la primera línea de puntos, se deduce que a la segunda llega

$$|\psi_2\rangle = \frac{1}{2^{m/2}\sqrt{r}}\sum_{k=0}^{2^m-1}\sum_{j=0}^{r-1}e^{2\pi ijk/r}\,|k\rangle\otimes|u_j\rangle\,.$$

La puerta F del circuito es la que actúa sobre registros de m qubits aplicando la *transformada de Fourier cuántica*:

$$F:\ |k\rangle \longmapsto \frac{1}{2^{m/2}} \sum_{\ell=0}^{2^m-1} e^{-2\pi i k\ell/2^m}\,|\ell\rangle\,.$$

Habitualmente se define con los coeficientes conjugados. La analogía con la transformada de Fourier discreta [9, IV], [12, §5.1] es patente. Salvo el factor que normaliza, su matriz es una de Vandermonde formada por raíces de la unidad y, por lo dicho sobre su suma, se tiene que las columnas son ortonormales, lo que prueba que F es un operador unitario que da lugar a una puerta cuántica. Tras pasar por ella, justo antes de la medición, obtendremos

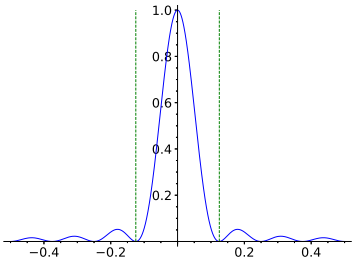
$$(F\otimes 1\otimes\cdots\otimes 1)\,|\psi_2\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{2^m-1}\sum_{j=0}^{r-1} D_m\Big(\frac{j}{r}-\frac{k}{2^m}\Big)\,|k\rangle\otimes|u_j\rangle \qquad \text{con} \quad D_m(x)=\frac{1}{2^m}\sum_{\ell=0}^{2^m-1} e^{2\pi i\ell x}.$$

Este D_m es una sencilla variante del *núcleo de Dirichlet*, el cual admite una fórmula explícita sumando la progresión geométrica [9, §18] y resulta que $|D_m(x)|^2$ es una función 1-periódica que en $[-\frac12,\frac12]$ tiene una parte sustancial de su masa (área limitada por su gráfica) concentrada en la banda $|x|<2^{-m}$ como ilustran las siguientes gráficas:

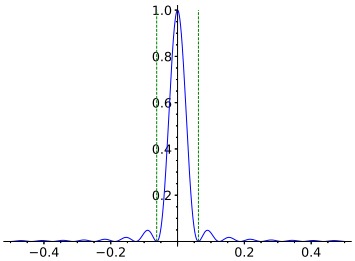
$$\big|D_m(x)\big|^2 = \frac{\operatorname{sen}^2(2^m\pi x)}{2^{2m}\operatorname{sen}^2(\pi x)}$$

$$\int_{-1/2}^{1/2} \big|D_m\big|^2 = \frac{1}{2^m}$$

$$\int_{-2^{-m}}^{2^{-m}} \big|D_m\big|^2 > \frac{0{,}9}{2^m}$$



Gráfica de D_3 y $x=\pm 2^{-3}$



Gráfica de D_4 y $x=\pm 2^{-4}$

De hecho, con un poco de análisis se prueba que la proporción de masa de $|D_m(x)|^2$ en $|x|<2^{-m}$ es siempre mayor que $\pi^{-2}\int_{-1}^{1} x^{-2}\operatorname{sen}^2(\pi x)\,dx = 0{,}9028\ldots$, esto es, más del 90 % de la masa está allí.

Finalmente, llegamos a la medición en el circuito, que se lleva a cabo sobre los primeros m qubits de $(F\otimes 1\otimes\cdots\otimes 1)\,|\psi_2\rangle$. Tal medición colapsará los $|k\rangle$ a un $|k_0\rangle$ y este k_0, como lista de bits, es el que darán los aparatos de medida. Solo puede haber un j tal que $\frac{j}{r}-\frac{k_0}{2^m}$ dista de un entero menos de 2^{-m} porque $1/r > N^{-1} > 2^{-n} > 2^{-m}$. Entonces, según lo dicho sobre la masa de $|D_m|^2$, tras la medición se tendrá con alta probabilidad

$$|k_0\rangle\otimes|u_j\rangle \qquad \text{con} \quad \Big|\frac{j}{r}-\frac{k_0}{2^m}\Big| < \frac{1}{2^m}. \tag{2}$$

En rigor, también podría aparecer dentro del valor absoluto ± 1, pues D_m es 1-periódica, pero estos casos se tratar de manera similar redefiniendo formalmente j como $j\pm r$, que deja

invariante la fórmula para $|u_j\rangle$. Con esto termina la parte cuántica, ahora tomamos el k_0 obtenido en los aparatos de medición y trabajamos con él en un ordenador convencional.

Un resultado de teoría de números [8, §10.7] afirma que dado $\alpha \in \mathbb{R}$ las fracciones irreducibles a/q que verifican $|\alpha - a/q| < \frac{1}{2}q^{-2}$ son *convergentes* de la *fracción continua* de α. En caso de que desconozcas esta terminología, lo único que necesitas saber es que estas convergentes son unas fracciones irreducibles asociadas a α cuyo numerador y denominador tienen crecimiento exponencial que responde a una recurrencia relacionada con el algoritmo de Euclides. Esta recurrencia hace que sea computacionalmente fácil hallar convergentes con denominadores gigantescos si se conoce α con precisión. El caso $\alpha \in \mathbb{Q}$, que es el que nos atañe, es especialmente sencillo. Los detalles se pueden encontrar en [8, §10.1] y una rápida introducción en [12, §A.4.4].

En nuestro caso, aplicamos el resultado con $\alpha = k_0/2^m$ y $a/q = j/r$. Teniendo en cuenta $r < N < 2^n$ y $m \geq 2n + 1$ la condición de (2) asegura $|\alpha - a/q| < \frac{1}{2}q^{-2}$, por tanto, j/r es una convergente. De hecho, entre las convergentes solo hay una compatible con (2), porque si hubiera dos, a_1/q_1 y a_2/q_2 con $q_1, q_2 < N$, la cadena de desigualdades siguiente llevaría a una contradicción:

$$\frac{1}{2^{2n}} < \frac{1}{N^2} < \frac{1}{q_1 q_2} \leq \left|\frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \leq \left|\alpha - \frac{a_1}{q_1}\right| + \left|\alpha - \frac{a_2}{q_2}\right| \leq \frac{2}{2^m}.$$

Recapitulando, con el algoritmo cuántico se obtiene k_0 y a partir de este valor un algoritmo de teoría de números da j/r con alta probabilidad. Este último algoritmo es determinista, la probabilidad proviene de que la desigualdad en (2) no está garantizada. En principio, a partir de j/r obtenemos r como su denominador. Sin embargo, queda un último detalle insidioso en la teoría, aunque raramente afecta a la práctica.

El número racional j/r no determina r si la fracción no es irreducible. En ese caso, el algoritmo podría producir un divisor propio de r en lugar de r, ya que cada convergente a/q es irreducible y $a/q = j/r$ implica $q \mid r$. Ejecutando varias veces el algoritmo se obtendrán divisores de r y cuántos más tengamos más fácil será recuperar r mediante el mínimo común múltiplo. En [3, §4] hay un análisis teórico de la situación. Por otro lado, las simulaciones sugieren que esto no es un gran problema en la práctica. Aquí solo añadiremos como indicio teórico favorable que la mayor parte de las fracciones son irreducibles en el sentido de que la probabilidad de que dos enteros $j, r \in [1, N]$ sean coprimos tiende a $6/\pi^2 = 0{,}6079\ldots$ cuando $N \to \infty$.

El algoritmo de Shor no depende de oráculos y, por tanto, no hay obstáculos teóricos para implementarlo en los ordenadores cuánticos. Al estar buena parte de la criptografía actual sujeta a problemas que se podrían atacar con el algoritmo de Shor o algunas de sus variantes, el reciente desarrollo de tecnologías relativas a la computación cuántica ha propiciado que se hagan algunas previsiones bastante cercanas (a una década) sobre la llegada de lo que se está viniendo en llamar el *Q-day*, el momento en que los algoritmos criptográficos actuales sean vulnerables utilizando ordenadores cuánticos.

Sin embargo, las implementaciones conocidas del algoritmo de Shor tienen un alcance ridículo. Por ejemplo, en [1] se reporta cómo los autores consiguen factorizar $N = 15$ y $N = 21$ pero no $N = 35$. Es justo añadir que desde su publicación las tecnologías cuánticas han mejorado.

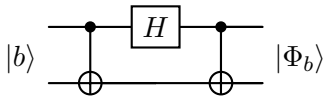
A día de hoy, con superodenadores o con muchas horas de ordenadores convencionales se llega a encontrar factores para N con cientos de bits mientras que miles de bits se considera inabordable. Como el algoritmo de Shor requiere $2^n > N$, el reto de la computación cuántica para ser competitiva en este aspecto es lograr que el circuito funcione con n comparable a 1000, lo cual está utópicamente lejos de la realidad actual. Al igual que en otros problemas, no es solo una cuestión del número de qubits, sino también de la construcción de puertas U_d suficientemente rápidas, pues cuanto más tarden en operar, es más probable que el sistema pierda las propiedades cuánticas por la decoherencia, la principal enemiga de la computación cuántica [12, §7.1].

Ejercicios de la sección 4

Ejercicio 1. Demuestra que CNOT $\neq U \otimes V$ con U y V operadores unitarios actuando sobre un qubit.

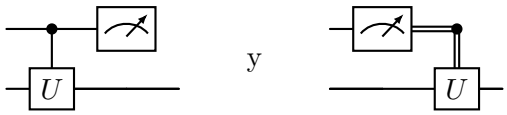
Ejercicio 2. Prueba la igualdad CNOT $= |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes X$ donde X indica la puerta correspondiente a σ_1 y halla la matriz de CNOT en la base computacional $\mathcal{B}_2$.

Ejercicio 3. Muestra que para $b \in B_2$ se cumple lo que se afirma en el siguiente circuito:



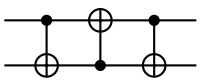
donde $|\Phi_b\rangle$ son los estados de Bell salvo por una constante multiplicativa global en $|\Phi_2\rangle$ y hacemos la identificación de b con su valor en binario.

Ejercicio 4. Comprueba que para cualquier operador unitario U en $\mathbb{C}^2$ los circuitos



son equivalentes. Es decir, que actuando sobre un estado genérico dan los mismos resultados.

Ejercicio 5. Demuestra que el circuito



representa el operador de intercambio en $\mathbb{C}^2 \otimes \mathbb{C}^2$, es decir, el que aplica $|\varphi\rangle \otimes |\psi\rangle$ en $|\psi\rangle \otimes |\varphi\rangle$.

Ejercicio 6. Calcula la matriz de DU_0 del algoritmo de Grover en la base computacional para $n = 2$ cuando $b_0 = 01$.

Ejercicio 7. Con la notación del algoritmo de Grover, demuestra que la probabilidad p admite una fórmula del tipo $p = \left(P(2^{-n/2})\right)^2$ con $P \in \mathbb{Z}[x]$ de grado $2k + 1$.

Ejercicio 8. Considera la función $D_m(x) = 2^{-m} \sum_{\ell=0}^{2^m-1} e^{2\pi i \ell x}$, que aparece en el algoritmo de Shor, y demuestra que verifica $\left|D_m(x)\right|^2 = \frac{\operatorname{sen}^2(2^m \pi x)}{2^{2m} \operatorname{sen}^2(\pi x)}$ y $\int_{-1/2}^{1/2} \left|D_m\right|^2 = 2^{-m}$.

Ejercicio 9. Para $n = a = 3$ y $N = 7$ calcula la matriz de U_1 del algoritmo de Shor en la base computacional $\mathcal{B}_3$ indicando, para mayor brevedad, solo los elementos no nulos. Halla el menor $d > 1$ tal que $U_d = U_1$.

Referencias

[1] M. Amico, Z. H. Saleem, and M. Kumph. Experimental study of Shor's factoring algorithm using the IBM Q experience. *Phys. Rev. A*, 100:012305, Jul 2019.

[2] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74(20):4091–4094, 1995.

[3] M. Ekerå. On the success probability of quantum order finding. *ACM Transactions on Quantum Computing*, 5(2), may 2024.

[4] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe. Complete 3-qubit Grover search on a programmable quantum computer. *Nature Communications*, 8(1):1918, Dec 2017.

[5] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 212–219. ACM, New York, 1996.

[6] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, Jul 1997.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, 2008.

[8] L. K. Hua. *Introduction to number theory*. Springer-Verlag, Berlin-Heidelberg-New York, 1982. Transl. from the Chinese by P. Shiu.

[9] T. W. Körner. *Fourier analysis*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2022. With a foreword by T. Tao.

[10] P. D. Lax. *Linear algebra and its applications*. Pure and Applied Mathematics (Hoboken). Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2007.

[11] M. Nakahara and T. Ohmi. *Quantum computing*. CRC Press, Boca Raton, FL, 2008. From linear algebra to physical realizations.

[12] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[13] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[14] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[15] Wikipedia contributors. Shor's algorithm — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Shor%27s_algorithm&oldid=1348170429`, 2026. [Online; accessed 25-April-2026].

[16] C. Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A*, 60:2746–2751, Oct 1999.