Introducción a los algoritmos cuánticos

Ricardo Peña[1]

[a] *Universidad Complutense de Madrid, Facultad de Informática, Madrid,*

Abstract

La computación cuántica ha pasado a ser un tema de actualidad desde que, en 2019, Google anunció que había ejecutado en un computador cuántico un algoritmo que llevaría miles de años a un computador convencional. Lo que el futuro deparará a esta área es todavía incierto pero, por si acaso, muchos paises están invirtiendo cuantiosas sumas en acelerar la investigación en tecnologías cuánticas.

En este trabajo se presentan los fundamentos de los algoritmos cuánticos y se sugiere que una introducción a los mismos debería formar parte del curriculum académico de todos los ingenieros informáticos.

Keywords: Espacios de Hilbert, cúbits, superposición, entrelazado

1. Introducción

La idea de usar los principios de la mecánica cuántica para realizar cómputos se desarrolló durante la década de 1980, impulsada, entre otros, por el Premio Nobel de física Richard Feynman. En la década siguiente, se idearon los primeros algoritmos, muy notablemente el de factorización de enteros, debido al matemático Peter Shor. Es este algoritmo el que ha promocionado con fuerza la investigación en computadores cuánticos, ya que, de poder ejecutarse, emplearía un tiempo polinómico en un problema en el que los computadores clásicos necesitan un tiempo exponencial. Considerando que el desmesurado coste de factorizar grandes enteros es lo que protege las claves de la mayoría de los sistemas criptográficos actuales, la investigación en computación cuántica, y en general en las tecnologías cuánticas, ha pasado a

[1]Work partially funded by the Spanish Ministry of Economy and Competitiveness, under the grant TIN2017-86217-R, and by the Madrid Regional Government, under the grant S2018/TCS-4339, co-funded by the European Union EIE funds.

ser una prioridad de las grandes potencias, las cuales están dedicando cuantiosos fondos a este fin. En 2017, IBM anunció que disponía de un computador cuántico con 50 cúbits y, un año más tarde, Google anunció que el suyo había alcanzado los 72 cúbits. En octubre de 2019, Google reclamó haber alcanzado la "supremacía cuántica" por haber ejecutado con éxito un algoritmo que habría llevado miles de años a un computador convencional. Se estima que, para poder romper las claves criptográficas con el algoritmo de Shor, harían falta del orden de 1500 cúbits.

Seguramente estamos aún lejos de este escenario debido a los problemas de estabilidad que presentan los computadores cuánticos actuales, ya que no resulta sencillo mantener la coherencia de un número tan elevado de cúbits. Pero, tampoco parece prudente desentenderse de esta tecnología esperando a que otros la hagan madurar. Se pueden dar las siguientes razones para interesarse por la computación cuántica:

- Es un área de importancia estratégica para un país, como lo fue en su día la investigación en cohetes, en energía nuclear o en inteligencia artificial. Si el área fructificase en un futuro, tal vez sería ya demasiado tarde para empezar a interesarse por ella partiendo de cero.

- Los computadores actuales han llegado al límite de la miniaturización que es posible alcanzar. Seguir disminuyendo los dispositivos de almacenamiento y de cálculo hará que los efectos cuánticos pasen a ser relevantes.

- La investigación en computación y algorítmica debe trabajar con todo modelo de cómputo que permita resolver los problemas de forma eficiente. Hasta hoy, la conjetura de Church-Turing afirmaba que todos los modelos conocidos podían computar las mismas funciones y que, además, los algoritmos podían transformarse de unos a otros modelos con un coste polinomial. El modelo cuántico no parece incrementar el número de funciones computables, pero sí romper la equivalencia polinomial.

Por estas razones, en este trabajo proponemos incluir una introducción a la algorítmica cuántica en los cursos convencionales de algoritmos. En algunos grados y másteres existen ya asignaturas opcionales sobre esta materia, pero defendemos que, sin perjuicio de ello, todo estudiante de ingeniería informática debería tener unas mínimas nociones sobre lo que es un algoritmo

cuántico y sobre cuál es la razón de su mayor eficiencia de cómputo. El propósito de estas notas es contribuir a proporcionar dichas nociones.

Los conceptos de física que se necesita conocer para ello no son muchos. Tan solo asumir, como algo que nos viene dado por la naturaleza, que las partículas cuánticas se encuentran normalmente en una superposición de estados y que podemos manipular dicha superposición para realizar cómputos. También, que la superposición persiste mientras la partícula no sea perturbada por una medición. Cualquier intento de observar su estado hace que la superposición desaparezca y colapse a uno de los estados básicos. El ejemplo más característico es el experimento de la doble rendija: un fotón lanzado hacia dos rendijas cercanas hace que este se comporte como una onda que atraviesa ambas, interfiere consigo mismo y produce tras ellas una figura típica de interferencia ondulatoria. En cambio, si colocamos un detector detrás de cada rendija, el fotón se comportará como una partícula y solo será detectado en una de ellas.

En la siguiente sección, se introducen brevemente los conceptos matemáticos en los que se basa la computación cuántica; a continuación, la sección 3 define los cúbits, la superposición de estados y el fenómeno del entrelazado cuántico; la sección 4 presenta los elementos de cómputo, es decir, las puertas cuánticas y la sección 5 explica en detalle uno de los primeros algoritmos cuánticos, históricamente hablando; finalmente, en la sección 6, se dan algunas conclusiones.

Estas notas están basadas en los documentos [1, 2, 3] y [4].

2. Base matemática de la computación cuántica

La matemática necesaria para diseñar algoritmos cuánticos son los espacios de Hilbert de base finita sobre el cuerpo de los números complejos. También se requieren nociones básicas de álgebra lineal.

2.1. Números complejos

El conjunto de los números complejos, denotado $\mathbb{C}$, tiene la estructura algebraica de *cuerpo*, cuya axiomática exige dos operaciones binarias —en este caso, la suma y el producto— conmutativas, asociativas y dotadas de elemento neutro que, además, satisfacen las siguientes propiedades:

- Propiedad distributiva: para todo $v, w, z \in \mathbb{C}$, $v(w + z) = vw + vz$.
- Para todo $z \in \mathbb{C}$, existe su inverso aditivo: $z + (-z) = 0$.

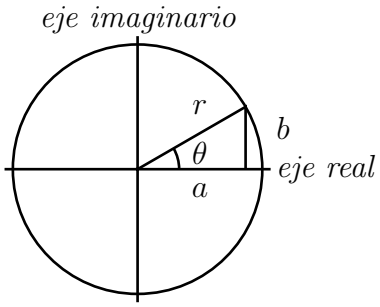


Figura 1: Representaciones binómica y polar de un número complejo

- Para todo $z \in \mathbb{C}, z \neq 0$, existe su inverso multiplicativo $zz^{-1} = 1$.

La representación más habitual de los números complejos es la forma *binómica*, $z = a + bi$, $a, b \in \mathbb{R}$, en la que estos se expresan como la suma de una parte real a y una parte imaginaria bi, múltiplo real de la unidad imaginaria i, que satisface la igualdad $i^2 = -1$. Esta representación hace a los números complejos isomorfos al plano real $\mathbb{R}^2$ y permite considerarlos, junto con su operación de suma, como un espacio vectorial de dimensión 2. Históricamente, los números complejos surgieron para garantizar que las ecuaciones polinómicas de cualquier grado tuvieran raíces.

Si $z = a + bi$, su *conjugado*, denotado z^*, se define como $z^* = a - bi$ y su *módulo*, denotado $|z|$, como $|z| = \sqrt{a^2 + b^2}$. Nótese que:

$$z^* z = a^2 - b^2 i^2 = a^2 + b^2 = |z|^2$$

Una representación alternativa es la llamada forma *polar*, en la que el vector $z = a + bi$ se expresa mediante el par (r, θ) formado por su módulo $r = |z|$ y el ángulo θ que dicho vector forma con el semieje real positivo en sentido antihorario (véase la figura 1). La transformación de esta representación a la binómica consiste, simplemente, en hacer $a = r\cos\theta$ y $b = r\sin\theta$.

En 1748, Euler demostró la siguiente igualdad,

$$e^{i\theta} = \cos\theta + i\sin\theta$$

siendo e la base de los logaritmos neperianos, por lo que también puede escribirse $a + bi = re^{i\theta}$. Nótese que:

$$|e^{i\theta}|^2 = \cos^2\theta + \sin^2\theta = 1$$

y que, si $z = e^{i\theta}$, entonces $z^* = e^{-i\theta}$ y $z^* z = e^0 = 1$.

2.2. Espacios de Hilbert

Un *espacio vectorial* sobre un cuerpo $\mathbb{K}$ es una terna $\langle V, +, \cdot \rangle$, donde V es un conjunto no vacío; $+ : V \times V \to V$ es una operación binaria conmutativa, asociativa, con elemento neutro $\mathbf{0}$, y existencia de inverso: para todo $\mathbf{v} \in V$ existe $-\mathbf{v} \in V$ tal que $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$; y $\cdot : \mathbb{K} \times V \to V$, llamada *producto por un escalar*, es asociativa, distributiva con respecto al $+$ de V y al $+$ de $\mathbb{K}$ y con un elemento neutro por la izquierda, $1 \cdot \mathbf{v} = \mathbf{v}$.

Un vector $\mathbf{v} \in V$ es *linealmente dependiente* de un conjunto de vectores $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$ si puede obtenerse como una combinación lineal —es decir, productos por escalares y sumas— de ellos. Un conjunto de vectores $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ es *linealmente independiente*, si $\mathbf{0}$ no puede obtenerse como combinación lineal suya, excepto cuando todos los coeficientes escalares son nulos. Una *base* de V es un subconjunto de vectores linealmente independientes tal que todo $\mathbf{v} \in V$ puede obtenerse como combinación lineal suya. Todas las bases de un espacio vectorial tienen el mismo cardinal y este recibe el nombre de *dimensión* del espacio. Los productos cartesianos $\mathbb{R}^n$ y $\mathbb{C}^n$, con $+$ definido como la suma de tuplas, componente a componente, son ejemplos de espacios vectoriales n-dimensionales.

Un *espacio de Hilbert* es un espacio vectorial $\mathcal{H}$ sobre un cuerpo $\mathbb{K}$, dotado de un *producto interno* $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{K}$, que satisface las siguientes propiedades:

- El producto interno define una *norma*, $\|x\| = \sqrt{\langle x|x \rangle}$, que genera una métrica en $\mathcal{H}$.
- Toda sucesión de Cauchy —una generalización de sucesión convergente— con respecto a dicha norma tiene límite en $\mathcal{H}$.

Se admiten espacios de Hilbert con dimensión infinita —por ejemplo, espacios de funciones—. Sin embargo, en el uso de ellos que haremos aquí, tendrán siempre dimensión finita.

Una operación que utilizaremos será el *producto tensorial* de dos espacios de Hilbert: si $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ es una base del espacio n-dimensional $\mathcal{H}_\mathcal{A}$ y $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ es una base del espacio m-dimensional $\mathcal{H}_\mathcal{B}$, el espacio nm-dimensional producto tensorial, denotado, $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$, consiste en todos los vectores que son el producto tensorial de un vector de $\mathcal{H}_\mathcal{A}$ y otro de $\mathcal{H}_\mathcal{B}$, los cuales tendrán la forma:

$$(\sum_{i=1}^{n} a_i \mathbf{v_i}) \otimes (\sum_{j=1}^{m} b_j \mathbf{u_j}) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j (\mathbf{v_i} \otimes \mathbf{u_j})$$

constituyendo $\{\mathbf{v_i} \otimes \mathbf{u_j}\}_{i\in\{1..n\},j\in\{..m\}}$ una base en $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. El producto tensorial de espacios de Hilbert es asociativo.

3. Cúbits: superposición, entrelazado y medición

Como se ha dicho, una partícula cuántica —un electrón, un átomo, un ión, un fotón— puede adoptar varios estados básicos. Por ejemplo, el espín de un protón puede tomar los valores básicos *arriba* y *abajo* y el electrón de un átomo de hidrógeno puede estar ubicado en diferentes orbitales, dependiendo del estado de excitación del átomo. Si n es el número de estados básicos de la partícula, modelizaremos dichos estados como una base de vectores en un espacio de Hilbert n-dimensional $\mathcal{H}$ y los denotaremos $|0\rangle, |1\rangle, \ldots, |n-1\rangle$. Cuando se realice una medición, obtendremos uno de estos estados básicos, pero, antes de ella, la partícula se encuentra en un estado $|\varphi\rangle$ que es una *superposición* de dichos estados y que modelizaremos como un vector de $\mathcal{H}$:

$$|\varphi\rangle = \alpha_0|0\rangle + \cdots + \alpha_{n-1}|n-1\rangle$$

Los coeficientes α_i se llaman *amplitudes* y son números complejos. Cuando, tras una medición, el estado $|\varphi\rangle$ colapsa a uno de los estados básicos $|i\rangle$, lo hace con una probabilidad $|\alpha_i|^2$. Exigiremos, por tanto, $\sum_{i=0}^{n-1} |\alpha_i|^2 = 1$.

En dicho espacio, el producto interno de dos vectores, $|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i|i\rangle$, $|\varphi\rangle = \sum_{i=0}^{n-1} \beta_i|i\rangle$, se define del modo siguiente:

$$\langle\psi|\varphi\rangle = \sum_{i=0}^{n-1} \alpha_i^* \beta_i$$

Como consecuencia de esta definición, $\|\psi\| = \langle\psi|\psi\rangle = \sum_{i=0}^{n-1} |\alpha_i|^2 = 1$.

Al igual que un computador clásico, un computador cuántico se compone de una memoria y una o varias unidades de cálculo. La unidad mínima de memoria es el *cúbit* —abreviatura de *bit cuántico*— y sus estados básicos son $|0\rangle$ y $|1\rangle$. Su estado antes de cualquier medición será, en general, una superposición de ambos:

$$|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \qquad\qquad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

La información relevante almacenada en un cúbit es su vector de amplitudes (α_0, α_1). Decimos que el cúbit "vive" en el espacio $\mathbb{C}^2$. Identificamos la base del espacio con los vectores $|0\rangle = (1, 0)$ y $|1\rangle = (0, 1)$.

La realización física de un cúbit es una partícula cuántica que pueda adoptar dos estados básicos y tal que dicho estado pueda ser alterado externamente. En algunas realizaciones, un cúbit es un ión atrapado a temperaturas cercanas al cero absoluto y, en otras, es un fotón confinado dentro de un circuito superconductor.

Los cúbits de un computador cuántico, a diferencia de los bits clásicos, no son independientes, sino que sus estados están *entrelazados*. Esta es una característica exclusiva del mundo cuántico que ha sido evidenciada experimentalmente de forma exhaustiva. El estado de dos cúbit entrelazados se corresponde exactamente con el producto tensorial de los espacios individuales de cada cúbit. Así, un vector en dicho espacio tendría la siguiente forma:

$$|\varphi\rangle = \alpha_{00}(|0\rangle \otimes |0\rangle) + \alpha_{01}(|0\rangle \otimes |1\rangle) + \alpha_{10}(|1\rangle \otimes |0\rangle) + \alpha_{11}(|1\rangle \otimes |1\rangle)$$

que abreviaremos notacionalmente a

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

y que cumple la condición de normalización $\sum_{i,j\in\{0,1\}} |\alpha_{ij}|^2 = 1$.

Una memoria de dos cúbit almacena, pues, cuatro números complejos. Generalizando, una memoria de n cúbits almacena 2^n números complejos. Esta cantidad es enorme: por ejemplo, con 270 cúbits —unos treinta y cuatro octetos— se podrían almacenar tantos valores como protones se estima que existen en el universo. Se aprecia, entonces, una ganancia exponencial con respecto a la memoria de un computador convencional, en la que n bits almacenan tan solo un número entero entre 0 y $2^n - 1$. La dificultad de la memoria cuántica estriba en que la inmensa cantidad de información que almacena tan solo persiste en tanto dure la superposición de estados. Si efectuamos una medición de los n cúbits, solo obtendremos —con cierta probabilidad cada uno de ellos— uno de los estados básicos, es decir, un entero entre 0 y $2^n - 1$.

Algunos estados entrelazados expresan propiedades sorprendentes, pero que también han sido verificadas experimentalmente. Supongamos una memoria de dos cúbits en una superposición $|\varphi\rangle$ expresada en $\mathbb{C}^4$ por el vector $(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}})$, es decir:

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

Si ahora efectúasemos una medición del primer cúbit y su lectura fuera, por ejemplo, $|0\rangle$ —simétricamente para $|1\rangle$—, el valor del segundo cúbit pasaría

a ser también $|0\rangle$ aunque no fuera medido e, incluso, aunque ese cúbit fuese separado físicamente del primero y llevado a mucha distancia. Los cúbits que están en este tipo de superposición se denominan pares EPR (en honor a A. Einstein, B. Podolsky y N. Rosen, que los estudiaron por primera vez[2]) y, como veremos, pueden conseguirse con relativa facilidad.

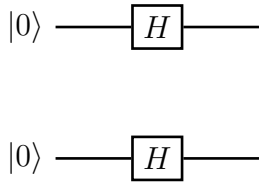
4. Puertas cuánticas

La unidades de cálculo de un computador cuántico son las puertas lógicas cuánticas, cuya finalidad es transformar el estado de los cúbits o/y combinar los estados de varios de ellos. A diferencia de las puertas lógicas clásicas, las cuánticas tienen el mismo número de entradas que de salidas. Si consideramos que los cúbits son átomos o fotones confinados, no tiene mucho sentido que los cúbits se creen y se destruyan dinámicamente. Por eso, ha de entenderse que las "salidas" de una puerta cuántica son los mismos cúbits de la entrada, pero con su superposición de estados modificada.

Si una puerta transforma el estado de n cúbits, deberá convertir un vector de $N = 2^n$ componentes en otro vector con el mismo número de ellas. Las transformaciones de estados cuánticos que suceden en la naturaleza son siempre lineales, por lo que el efecto de la puerta se puede definir mediante una matriz $N \times N$. Más aún, las matrices han de preservar la norma de los vectores de estado. Si A es una de dichas matrices y $\varphi \in \mathbb{C}^N$ es un estado, ha de cumplirse $\|A\varphi\| = \|\varphi\| = 1$. Decimos que A es *unitaria* y se puede demostrar que esta propiedad es equivalente a $A^{-1} = A^*$, donde A^* denota la traspuesta conjugada —también llamada *adjunta*— de A. El hecho de que la matriz que define una puerta cuántica siempre tenga inversa nos conduce a otra propiedad interesante de los cómputos cuánticos y es que son reversibles: basta con aplicar la puerta inversa de una puerta —suponiendo que podamos construir cualquier puerta— para deshacer su efecto.

Las puertas que transforman el estado de un solo cúbit se pueden definir mediante matrices de dimensión 2×2. El físico austriaco Wolfgang Pauli (1900-1958) propuso las cuatro siguientes:

[2]De hecho, esta paradójica acción a distancia predicha por la teoría, pero en ese momento aún no confirmada experimentalmente, llevó a Einstein a desconfiar de la mecánica cuántica.



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

Figura 2: Dos puertas de Hadamard aplicadas cada una a un cúbit

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

Además de su importancia individual, estas cuatro puertas forman una base en el espacio de las matrices complejas unitarias 2×2, es decir, cualquier matriz A de estas características se puede obtener como una combinación lineal de las matrices de Pauli:

$$A = \alpha_0 I + \alpha_1 X + \alpha_2 Y + \alpha_3 Z$$

Por otro lado, las cuatro coinciden con su traspuesta conjugada y, por lo tanto, son su propia inversa.

La puerta X puede asimilarse a una puerta NOT clásica, ya que convierte el estado $|0\rangle$ en el estado $|1\rangle$ y viceversa. Su efecto general es intercambiar las amplitudes de una superposición:

$$X(\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_1|0\rangle + \alpha_0|1\rangle$$

Otra puerta importante, de las que se aplican a un solo cúbit, es la llamada —en honor al matemático francés Jacques Hadamard (1865-1963), que ideó dichas matrices en un contexto diferente— *puerta de Hadamard* o puerta H: si se aplica H a un cúbit en estado $|0\rangle$ o $|1\rangle$, lo sitúa en una superposición equiprobable de ambos estados:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Si se aplicara H a cada uno de dos cúbits entrelazados (véase la figura 2), podemos preguntarnos cúal sería la matriz 4×4 que expresaría la transformación. La respuesta es el *producto tensorial* $H \otimes H$ de dos matrices H,

denotado $H^{\otimes 2}$. En general, si A y B son dos matrices de dimensiones $n \times m$ y $r \times s$, respectivamente, su producto tensorial es una matriz $nr \times ms$ que se define del modo siguiente:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{pmatrix}$$

Es inmediato demostrar que el producto tensorial de matrices es asociativo. El lector puede comprobar que, si los dos cúbits están en el estado inicial $|00\rangle$, la superposición obtenida en la figura 2 es una configuración equiprobable de los cuatro estados básicos posibles:

$$H^{\otimes 2}|00\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

Si se aplicara una puerta a un cúbit y ninguna al otro, aún así la superposición resultante afectaría a los dos. Para ello, cabe imaginar que al segundo cúbit se le aplica una puerta identidad I. Por ejemplo:

$$(H \otimes I)|00\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

Una puerta que afecta a dos cúbits es CNOT (*Controlled NOT*), cuya intuición es que, si el primer cúbit está en estado $|0\rangle$, el segundo queda inalterado, pero, si el primero es $|1\rangle$, entonces el efecto sobre el segundo es el mismo que si se le aplicara una puerta X. Se suele dibujar como una línea vertical que intersecta dos cúbits: la primera intersección —que corresponde al bit de control— se marca con el símbolo $\bullet$ y, la segunda, con el símbolo $\oplus$, que es el que se emplea para una puerta X. Su matriz de transformación es:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

En la figura 3 mostramos un circuito con una puerta CNOT aplicada a dos cúbits en la superposición de estados $|\varphi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle$. El lector puede comprobar el siguiente resultado:

$$CNOT|\varphi\rangle = \alpha|00\rangle + \beta|11\rangle$$

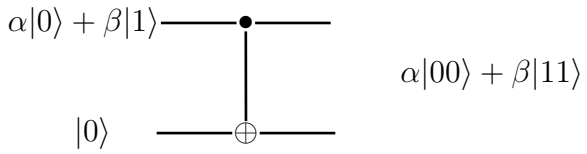


Figura 3: Circuito cuántico con puerta CNOT, que genera un par EPR

que constituye un par EPR.

Una última puerta, que en este caso afecta a tres cúbits, es la llamada *puerta de Toffoli* y también CCNOT (*Controlled-Controlled NOT*). Con respecto a los dos primeros cúbits, se comporta como la identidad. En cuanto al tercero, se comporta como una puerta X, sólo si los dos primeros valen $|1\rangle$; en otro caso, lo deja inalterado. Si a, b y c fueran los estados básicos —$|0\rangle$ o $|1\rangle$— de los tres cúbits, el valor devuelto para el tercero sería $c \oplus ab$, donde $\oplus$ es la operación o-exclusivo de dos bits. Los siguientes dos usos permiten simular con CCNOT una puerta NAND convencional y también duplicar un cúbit, con lo que es posible aumentar el *fanout* de una conexión lógica:

CCNOT $\|a, b, 1\rangle = \|a, b, \neg(ab)\rangle$	Simula una puerta NAND
CCNOT $\|1, a, 0\rangle = \|1, a, a\rangle$	Simula un *fanout* de 2

Con ello, cualquier circuito lógico clásico puede ser simulado en el mundo cuántico, a condición de disponer de algunos cúbits adicionales inicializados a $|0\rangle$ o a $|1\rangle$.

5. Algoritmos

Un algoritmo cuántico es un circuito formado por un conjunto de puertas tal que, aplicado a una superposición inicial de los estados de n cúbits, transforma dicha superposición en otra que contiene la solución buscada. Una dificultad inherente a los algoritmos cuánticos es que la lectura de dicha solución destruye la superposición final y se pierde el vector de amplitudes. Por ello, es necesario cierto ingenio para obtener la información buscada aun contando con dicha destrucción del estado.

Antes de ver un ejemplo de algoritmo, vamos a desvelar de dónde proviene la ventaja en eficiencia de la computación cuántica con respecto a la clásica. Supongamos, para ello, que contamos con el equivalente cuántico de un circuito lógico clásico que calcula una función f de n en m bits, es decir:

$$f : \{0,1\}^n \to \{0,1\}^m \quad \text{, o bien,} \quad f : \{0, \ldots, 2^n - 1\} \to \{0, \ldots, 2^m - 1\}$$

Hemos visto que, contando con las puertas de Toffoli, es posible imitar en el mundo cuántico las puertas lógicas clásicas, a condición de disponer de algunos cúbits adicionales para contener las "salidas" del circuito. Sea Q_f dicho circuito, el cual, aplicado a $n+m$ cúbits, los últimos m inicialmente en estado $|0^m\rangle$, produce la siguiente correspondencia para todo $z \in \{0,1\}^n$:

$$Q_f : |z\rangle|0^m\rangle \to |z\rangle|f(z)\rangle$$

También hemos visto que, aplicando una puerta de Hadamard a los primeros n cúbits, de un conjunto de $n+m$ cúbits cúbits inicialmente en estado $|0\rangle$, se crea la siguiente superposición equiprobable de los 2^n valores posibles:

$$(H^{\otimes n} \otimes I^{\otimes m})|0^{n+m}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle|0^m\rangle$$

Si, tras esta transformación, aplicamos al estado de los $n+m$ cúbits la matriz unitaria U_{Q_f} correspondiente al circuito Q_f, obtenemos:

$$U_{Q_f}\left(\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle|0^m\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} U_{Q_f}|z\rangle|0^m\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle|f(z)\rangle$$

Obsérvese que, en dicha superposición, sólo tienen amplitud no nula los estados básicos en los que el valor z de los primeros n cúbits está emparejado con el valor $f(z)$ de los siguientes m.

En la primera igualdad es donde se produce el "milagro" de la computación cuántica: el circuito Q_f es aplicado *simultáneamente* a todos los valores de 0 a $2^n - 1$, lo cual produce una ganancia exponencial en el tiempo de cálculo con respecto a la computación clásica. El circuito clásico tendría que calcular $f(z)$ secuencialmente para cada entrada z diferente.

La dificultad del "milagro" estriba en que, si realizásemos una medición de los $n+m$ cúbits, tan solo obtendríamos aleatoriamente un valor v de los 2^n calculados, junto con su resultado $f(v)$.

5.1. El algoritmo de Deutsch-Jozsa

Este algoritmo fue planteado por D. Deutsch y R. Jozsa en 1992 con el propósito de mostrar la aceleración exponencial que se puede conseguir con los algoritmos cuánticos, pero no tiene una especial utilidad. El problema que resuelve se puede plantear como el siguiente juego:

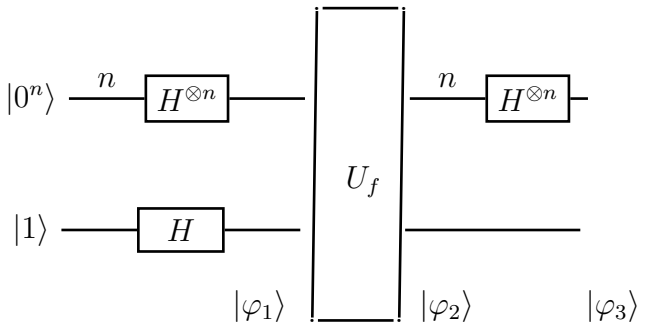


Figura 4: Algoritmo cuántico de Deutsch-Jozsa

Bob ha ideado una función $f : \{0,1\}^n \to \{0,1\}$ y promete a Alice que pertenece a uno de estos dos tipos: o bien es *constante*, en cuyo caso devuelve siempre el mismo valor para todo $x \in \{0,1\}^n$; o bien es *equilibrada*, en cuyo caso la mitad de las veces devuelve un 0 y la otra mitad devuelve un 1. Alice debe adivinar de un modo eficiente a cuál de los dos tipos pertenece f. Nótese que, en un computador clásico, f debería ser invocada al menos $2^{n-1}+1$ veces, en el caso peor en que f devolviera el mismo valor las primeras 2^{n-1} veces. Para ello, le pide a Bob que le proporcione una implementación cuántica U_f que calcule:

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$$

donde $x \in \{0,1\}^n, y \in \{0,1\}$ y $\oplus$ es la operación o-exclusivo sobre dos bits. Con la ayuda de las puertas de Toffoli, dicho circuito es factible si es factible uno para f. Entonces, Alice construye el circuito mostrado en la figura 4, que puede expresarse mediante la fórmula:

$$(H^{\otimes n} \otimes I) \cdot U_f \cdot (H^{\otimes (n+1)})|0^n\rangle|1\rangle$$

A continuación, realiza una medición de los primeros n cúbits: si obtiene el estado básico $|0^n\rangle$, concluye que f es constante; si obtiene cualquier otro estado $|x\rangle$, $x \neq 0^n$, concluye que es equilibrada. Veamos por qué.

Tras la aplicación de las primeras $n+1$ puertas de Hadamard, la superposición de estados resultante es:

$$\varphi_1 = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\right) \otimes (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$$

Tras la aplicación de U_f, se pasa a la superposición:

$$\varphi_2 = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\right) \otimes (\frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle))$$

donde $|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = |f(x)\rangle - |1 - f(x)\rangle$. Si $f(x) = 0$, el estado resultante es $|0\rangle - |1\rangle$ y, en caso contrario, es $|1\rangle - |0\rangle$. Podemos entonces escribir:

$$\varphi_2 = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \right) \otimes ((-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$$

Tras la aplicación de la última columna de puertas, se obtiene:

$$\varphi_3 = \left(\frac{1}{2^n} \sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{x \cdot z + f(x)} |z\rangle \right) \otimes (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) \tag{1}$$

donde $x \cdot z$ denota el producto escalar de x y z, considerados como vectores de n bits. Para entender la razón del exponente $x \cdot z$ de -1, conviene empezar por ver qué sucede cuando $n = 1$ y, por lo tanto, $x \in \{0, 1\}$:

$$H|x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle) = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{x \cdot z} |z\rangle$$

es decir, el exponente de -1 es impar si y solo si ambos, x y z, valen 1. Considerando que, para $n > 1$, $H^{\otimes n} = H^{\otimes n-1} \otimes H$, y procediendo por inducción sobre n, es inmediato probar la siguiente fórmula:

$$H^{\otimes n} |x_1, \ldots, x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{(z_1, \ldots, z_n) \in \{0,1\}^n} (-1)^{x_1 z_1 + \cdots + x_n z_n} |z_1, \ldots, z_n\rangle$$

que, al aplicarla al estado φ_2, conduce a la ecuación 1.

Observemos, en dicha ecuación, que la amplitud del estado básico $z = |0^n\rangle$ es $\frac{1}{2^n}(\sum_{x=0}^{2^n-1}(-1)^{f(x)})$. Si f es una función constante y, para todo x, $f(x) = 0$, dicha amplitud es 1; si $f(x) = 1$ para todo x, la amplitud es -1. Puesto que $\|\varphi_3\| = 1$, las amplitudes del resto de los estados básicos han de ser necesariamente 0. Por otro lado, si f es una función equilibrada, la mitad de los exponentes de -1 serían 0 y, la otra mitad, -1, lo que conduce a una amplitud 0 para el estado $z = |0^n\rangle$.

Resumiendo, si en el estado φ_3 se realiza una medición de los primeros n cúbits y la superposición colapsa al estado básico $|0^n\rangle$, Alicia concluye que f es constante. Si colapsa a cualquier otro estado básico, concluye que f es equilibrada.

El número de puertas cuánticas utilizadas para llegar a esta conclusión está en la clase de complejidad $O(n)$, por lo que el tiempo de cómputo no puede estar en una clase superior. En cambio, un computador clásico necesitaría un tiempo en $O(2^n)$ en el caso peor para llegar a la misma conclusión.

La parte más ingeniosa del algoritmo es la última columna de puertas H. En el estado φ_2, el algoritmo ya ha calculado la función f para todos los posibles valores de x, pero una medición en ese punto de los primeros n cúbits no arrojaría ningún resultado útil, sino tan solo un valor aleatorio x entre 0 y $2^n - 1$. Las puertas H hacen *interferir* todos los resultados de f entre sí a través del término $\sum_{x=0}^{2^n-1}(-1)^{x\cdot z+f(x)}$. Al igual que al lanzar un fotón de luz hacia dos rendijas, este produce una figura de interferencia tras las mismas, con sus picos y valles en los que se refuerza o se anula la señal, la interferencia de todos los valores de $f(x)$ conducen en este caso a una señal nítida: la presencia o ausencia del estado básico $|0^n\rangle$. El fenómeno de la interferencia es otra de las peculiaridades de la mecánica cuántica que los algoritmos cuánticos pueden explotar.

6. Conclusiones

Hemos presentado los fundamentos de los computadores y de los algoritmos cuánticos, la base matemática necesaria para entenderlos y un ejemplo no trivial de algoritmo de coste polinomial cuyo coste sería exponencial en un computador convencional.

Estas notas pretender servir como guion para introducir a los estudiantes de ingeniería informática en esta nueva faceta de la algoritmia que es la computación cuántica.

Referencias

[1] M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[2] R. d. Wolf, Quantum Computing: Lecture Notes, CWI and University of Amsterdam, arXiv:1907.09415 (2021).

[3] M. Allende López, Tecnologías Cuánticas, Banco Interamericano de Desarrollo, 2019.

[4] A. Rayo, y otros, Computación cuántica, Investigación y Ciencia, Especial num. 49 (2020).