Búsqueda de algoritmos computables cuánticamente no Turing-computables

José Luis Ballesteros del Val

2 de septiembre de 2015

Resumen

La computación cuántica constituye una de las líneas de investigación principales, tanto en física, por su parte experimental, centrada en la implementación, como en informática teórica y ciencias de la computación, por su parte teórica, centrada en el diseño de algoritmos.

Esta realiza aportaciones fundamentales tanto en la reducción de complejidad en la resolución de algoritmos, asunto que se trata en el presente escrito, así como da pie al planteamiento de problemas de índole filosófico, relativos a las nuevas formas de entender la lógica o la causalidad.

Abstract

Quantum computing constitutes one of main research lines, both on physiscs, because of its experimental side, focused on implementation, and on theoretical computer science, because of its theoretical side, focused on algorithm design.

This one makes fundamental contributions both on complexity reduction of algorithm solving, subject matter in these writings, and on approach on phylosophical indol problems, about new ways of understanding causality and logic.

1. Introducción

Desde que se comenzase a conocer el extraño comportamiento de la materia a escalas atómicas y subatómicas, que dio lugar, a la postre, a la mecánica cuántica, no han dejado de predecirse teóricamente, a partir de sus postulados, fenómenos totalmente extraños, inconcebibles para el pensamiento habitual, y sin analogía con la mecánica clásica, que han resultado probados experimentalmente.

En el marco de esta mecánica, ha surgido por ejemplo, la electrodinámica cuántica, que es el modelo teórico que con más precisión ha predicho un resultado, dando asimismo un máximo teórico para la precisión que ella misma produce. Este hecho hace que el modelo de la mecánica cuántica sea estudiado por ámbitos distintos al de la física o la química, trascendiendo a las matemáticas o la lógica.

Es en este mismo contexto en el que se ha formulado teóricamente la computación cuántica, un modelo de cómputo totalmente distinto que pretende aprovechar estas extrañezas en pro de la mejora de procedimientos que, en la computación clásica, ya se han demostrado inmejorables.

En el presente escrito, se pretende abarcar, con la profundidad que permiten las limitaciones de extensión, tanto los conceptos básicos de la mecánica cuántica y de las matemáticas necesarias para llegar a su comprensión, así como la esencia del problema de la complejidad computacional, para acabar con la exposición de algunos algoritmos cuánticos que efectivamente reducen la complejidad de algunos problemas dados.

2. Bit, Q-Bit y P-Bit. Conceptos básicos de la mecánica cuántica.

Una de las principales diferencias entre la computación clásica y la cuántica es la naturaleza de la unidad básica de información. En la computación clásica, la unidad básica de información es el bit -entidad que puede tomar valores de verdad (1 en adelante) o falsedad (0 en adelante), exclusivamente. En cambio, en computación cuántica, una entidad análoga puede tomar una combinación o estado intermedio entre 0 y 1 -en el contexto cuántico, se empleará la notación de Dirac, con lo que se representarán, grosso modo, $0 \equiv |0\rangle$ y $1 \equiv |1\rangle$. Dicha entidad se denomina *quantum bit* o *q-bit*, representándose de la siguiente manera $|\psi\rangle = e^{i\phi}(\alpha|0\rangle + \beta|1\rangle),\ \forall\alpha\forall\beta\forall\phi(\alpha, \beta, \phi \in \mathbb{R} \wedge \alpha^2 + \beta^2 = 1)$. El fenómeno citado se llama *superposición*.

Además, en el caso de trabajar con multitud de bits, la información que representa el conjunto de los bits es el conjunto de las informaciones que representan cada uno de los bits por separado. No obstante, en el caso de los q-bits, la información que representa el conjunto de los q-bits no siempre se puede separar en las informaciones que representan a cada uno de los q-bits por separado. Esto se denomina *entrelazamiento*.

Otra de las peculiaridades de la computación cuántica es el acceso a la información. En la obtención del valor de un bit -lo que en adelante se llamará *observación* o *medida* -la respuesta es determinista, es decir, si hay un valor de 0 en el bit, se medirá 0, y si es de 1, se medirá 1. En cambio, dado el q-bit

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, al efectuar una medida sobre dicho q-bit, se obtendrá el valor $|0\rangle$ con una probabilidad $P(|0\rangle) = \alpha^2$ o el valor , se obtendrá el valor $|1\rangle$ con una probabilidad $P(|1\rangle) = \beta^2$. Es decir, no se sabe lo que se va a obtener, sólo se conoce la probabilidad con la que va a resultar uno u otro valor. Además, el q-bit, después de la medida, se verá alterado, adquiriendo instantáneamente el valor que ha arrojado. Esto se conoce como *colapso*. Si se tienen N q-bits sin entrelazar, todos con la misma información, al repetir N veces la medida, se puede recuperar, con $N \to \infty$, la información. A la entidad que almacenaría la información de la probabilidad de cada q-bit se llamaría *probabilistic bit* o *p-bit*.

Es evidente que por muy exitosa que pueda resultar la formulación de un paradigma de computación, si éste quiere pasar de ser un simple -o complejo -experimento mental a una realidad tangible, ha de ser posible su implementación. Naturalmente, todos estos comportamientos se podrían simular en un computador clásico. No obstante, tanto los tiempos de procesamiento como la complejidad serían iguales, puesto que el sustrato de dicha computación seguiría siendo clásico. Lo interesante de la cuestión es que estas entidades formuladas anteriormente corresponden a realidades físicas, en las que esta computación es natural.

A continuación se introducirán nociones básicas y rudimentos matemáticos para el entendimiento de la mecánica cuántica, y, por consiguiente, de la computación basada en ella.

2.1. Rudimentos matemáticos

2.1.1. Números complejos.

Brevemente, los números complejos son una extensión de los números reales basada en la inexistencia de las raíces de índice par sobre números negativos: $\nexists\ \sqrt[2n]{-1}\ \forall n \in \mathbb{N}$. La solución pasa por definir la unidad imaginaria $i \equiv \sqrt{-1}$, de tal forma que el conjunto de los números complejos, denotado por $\mathbb{C}$, es como sigue:

$$\{z \in \mathbb{C} \leftrightarrow z = a + bi \wedge a, b \in \mathbb{R} \wedge i \equiv \sqrt{-1}\} \tag{2.1.1}$$

Además, conociendo la identidad de Euler, $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, un número complejo se puede expresar de la siguiente manera:

$$z = r\ e^{i\theta} \leftrightarrow (r = \sqrt{a^2 + b^2} \wedge \theta = \arctan(\frac{b}{a})) \tag{2.1.2}$$

Ambas formas son equivalentes, llamándose la primera binómica y la segunda polar, y obedecen a las reglas habituales de operatoria conocidas en los números reales. Únicamente hay que tener en cuenta que $i \cdot i = i^2 = -1$, así como cuatro operaciones simples exclusivas del conjunto:

- Partes real e imaginaria, definidas, respectivamente, por: $Re(a+bi)=a$, y por: $Im(a+bi)=b$
- Conjugado, que cambia la unidad imaginaria por su opuesto: $i \to -i$, y definido así: $z = a+bi = re^{i\theta} \leftrightarrow \bar{z} = a-bi = re^{-i\theta}$.
- Módulo y argumento, r y θ respectivamente, correspondientes a la definición dada para la forma polar. Se puede demostrar que $r^2 = \bar{z}z$.

La importancia del conjunto de los números complejos radica en los siguientes puntos:

- Es un conjunto que para las operaciones usuales: suma, diferencia, producto, división, potenciación, radicación, exponenciación, etcétera, es algebraicamente cerrado. Esto significa, simplificadamente, que cualquier operación efectuada sobre un número complejo arroja siempre un número dentro del conjunto de los complejos. Esto no ocurre con los números reales.
- La mecánica cuántica está construida en el conjunto de los números complejos.

2.1.2. Vectores, funciones, y producto escalar. Notación de Dirac (I).

En el tratamiento de la mecánica cuántica, para describir un estado cuántico, se hace imprescindible tratar con los conceptos de vector y función.

Un vector es un conjunto de números, en el presente caso complejos, tal que se les asigna un orden, dado por números, en principio, naturales. Dado un vector v, este se define como:

$$v = \{v_i \in \mathbb{C}, i \in [1, N] \subseteq \mathbb{N}\} \tag{2.1.3}$$

El número N anterior es la dimensión. Si N es finito, se dice que el vector es de dimensión finita. Si es infinito, se dice de dimensión infinita.

Esta ordenación de números se puede presentar, informalmente, en vertical o en horizontal, llamándose respectivamente vector columna o vector fila. No obstante, se entenderá que v está ordenado en columna, mientras que su *transpuesto*, denotado por v^t, está ordenado en fila, de la siguiente manera:

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \tag{2.1.4a}$$

$$v^t = \begin{pmatrix} v_1, & v_2, & \cdots, & v_n \end{pmatrix} \tag{2.1.4b}$$

Así pues, estando los vectores compuestos de números complejos, se puede definirse el conjugado de un vector:

$$\bar{v} = \begin{pmatrix} \bar{v_1} \\ \bar{v_2} \\ \vdots \\ \bar{v_n} \end{pmatrix} \tag{2.1.5a}$$

$$\bar{v^t} = \begin{pmatrix} \bar{v_1}, & \bar{v_2}, & \cdots & \bar{v_n} \end{pmatrix} \tag{2.1.5b}$$

No obstante, y con vectores construidos sobre números complejos, la operación más habitual es la *transposición conjugada*: $v^* \equiv \bar{v^t} = (\bar{v})^t$. Nótese que la transposición y la conjugación son operaciones conmutables.

Entre dos vectores se puede definir una importante operación, conocida como producto escalar, que resulta en un número del conjunto sobre el que se construyen los vectores, y que se define de la siguiente manera:

$$\langle w, v \rangle \equiv w^* \cdot v = \bar{w_1} \cdot v_1 + \bar{w_2} \cdot v_2 + \cdots \bar{w_n} \cdot v_n \equiv \sum_{i=1}^{n} \bar{w_i} \cdot v_i \tag{2.1.6}$$

Esta operación es bilineal y simétrica, es decir:

$$\begin{aligned} \langle \lambda(v+w), \mu(r+s) \rangle &= \bar{\lambda}\mu\langle (v+w), (r+s) \rangle \\ &= \bar{\lambda}\mu(\langle v, (r+s) \rangle + \langle w, (r+s) \rangle) \\ &= \bar{\lambda}\mu(\langle v, r \rangle + \langle w, r \rangle + \langle v, s \rangle + \langle w, s \rangle). \end{aligned} \tag{2.1.7}$$

Donde $\lambda, \mu \in \mathbb{C}$ son números, y v, w, r, s vectores.

Ahora bien, retomando la definición de vector, se tiene que, si se supone que los indices $i \in \mathbb{N}$ no son pertenecientes a los números naturales, sino a los reales, siendo estos $x \in \mathbb{R}$:

$$f = \{ f_x \equiv f(x) \in \mathbb{C}, x \in [a, b] \subseteq \mathbb{R} \} \tag{2.1.8}$$

(El cambio de notación es por conveniencia, ya que son más típicas las letras v, w, r, s para denotar vectores, y las letras i, j, k para índices discretos. Para funciones, suelen usarse las letras f, g, h, y para variables -equivalentes continuos de los índices -se suelen usar x, y, z, t).

Se tiene una definición equivalente a la de función que aplica un intervalo real en el conjunto de los números complejos, lo que lleva a poder definir el producto escalar de forma análoga, pero sumando a infinitas partes, ya que los índices contenidos en un conjunto finito subconjunto de aquel de los reales son infinitos. Esto es lo que se conoce como suma integral, representándose el producto escalar por:

$$\langle g, f\rangle = \int_a^b (g^*(x)\cdot f(x))dx \tag{2.1.9}$$

Dado el paralelismo existente entre ambas formas algebraicas, Paul Dirac enunció una notación para representarlas de forma única, usada en el formalismo de la mecánica cuántica, y por ende, de la computación cuántica, de la siguiente manera:

- Vectores: $|v\rangle \equiv v$; $\langle w| \equiv w^* \equiv \bar{w}^t$
- Funciones: $|f\rangle \equiv f$; $\langle g| \equiv g^* \equiv \bar{g}$

De tal forma que el producto escalar se denota, en caso de funciones: $\langle g|f\rangle$; y en el caso de vectores $\langle w|v\rangle$. En esta notación, los vectores columna se denominan *ket*, mientras que aquellos fila se denominan *bra*, de tal forma que la regla para haber terminado un producto escalar es llegar a un *bra-ket* -se observa cierta comicidad en el origen de la notación. La notación se llama, así pues, *bra-ket*, o *notación de Dirac*. Es esta notación en la que vienen expresados, por ejemplo, los q-bits.

2.1.3. Matrices, operadores, y producto escalar. Notación de Dirac (II).

Al igual que una ordenación de números puede tener una dirección o dimensión, puede tener dos. En este caso, en lugar de un vector, se tiene una matriz, que se define de la siguiente manera:

$$A = \{a_{i,j} \in \mathbb{C}, i, j \in [1, n] \subseteq \mathbb{N}\}$$

Las matrices que corresponden a esa definición son aquellas cuadradas, es decir, que tienen el mismo número filas que de columnas, y se representan de la siguiente manera:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

De la misma manera se definen las matrices transpuestas, en las que se alteran filas por columnas, denotadas por A^t, las matrices conjugadas, en las que se conjuga cada uno de sus elementos, denotadas por $\bar{A}$, y las transpuestas conjugadas, denotadas por $A^* \equiv \bar{A}^t \equiv \bar{A^t}$, representadas de la siguiente manera:

$$A^t = \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{n,1} \\ a_{1,2} & a_{2,2} & \cdots & a_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,n} & a_{2,n} & \cdots & a_{n,n} \end{pmatrix} \quad A^* = \begin{pmatrix} \bar{a}_{1,1} & \bar{a}_{2,1} & \cdots & \bar{a}_{n,1} \\ \bar{a}_{1,2} & \bar{a}_{2,2} & \cdots & \bar{a}_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{a}_{1,n} & \bar{a}_{2,n} & \cdots & \bar{a}_{n,n} \end{pmatrix}$$

Se puede definir el producto de una matriz y un vector como el producto escalar de cada uno de los vectores fila de la matriz con el vector columna dado, quedando el resultado en la posición que ocupaba la fila, formando un nuevo vector columna:

$$A \cdot v = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ a_{2,1} & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{1,1}v_1 + \cdots + a_{1,n}v_n \\ \vdots \\ a_{n,1}v_1 + \cdots + a_{n,n}v_n \end{pmatrix}$$

De la misma manera, se puede transponer y conjugar $A \cdot v$, lo que por brevedad se hará sólo en una operación. Esto es lo que se llama matriz transpuesta conjugada o matriz adjunta:

$$(A \cdot v)^* = v^* \cdot A^* = \begin{pmatrix} \bar{v}_1, & \cdots, & \bar{v}_n \end{pmatrix} \cdot \begin{pmatrix} \bar{a}_{1,1} & \cdots & \bar{a}_{1,n} \\ \vdots & \ddots & \vdots \\ \bar{a}_{n,1} & \cdots & \bar{a}_{n,n} \end{pmatrix} =$$
$$\begin{pmatrix} \bar{a}_{1,1}\bar{v}_1 + \cdots + \bar{a}_{n,1}\bar{v}_n, & \cdots, & \bar{a}_{1,n}\bar{v}_1 + \cdots + \bar{a}_{n,n}\bar{v}_n \end{pmatrix}$$

Continuando con la analogía establecida entre vectores y funciones, se puede establecer una analogía igual entre matrices y los llamados operadores. Los operadores se podrían entender como una entidad que aplicada a otra función da otra función. La analogía es clara, existiendo también equivalente en notación de Dirac:

- Vectores y matrices: $w = A \cdot v$; En notación bra-ket. $|w\rangle = |A|w\rangle$
- Funciones: $g = \mathcal{L}(f)$; En notación bra-ket. $|g\rangle = |\mathcal{L}|f\rangle$

De todo lo anterior se puede deducir también las siguientes propiedades de los bra y los ket de la notación de Dirac:

- $(|\lambda w\rangle) = \lambda(|w\rangle)$
- $\langle \lambda w| = (|\lambda w\rangle)^* = \bar{\lambda}(|w\rangle)^*$

Ahora bien, y por último, existe una modificación del producto escalar, que consiste en interponer un operador o matriz. En notación de Dirac, esto se expresa del siguiente modo: $\langle v|A|w\rangle$ o $\langle g|\mathcal{L}|f\rangle$.

2.1.4. Espacios vectoriales. Base de un espacio vectorial. Vectores y funciones abstractas. Espacios de Hilbert y duales.

Como colofón a este apéndice, cabe destacar el potencial de la notación de Dirac para tratar con entidades matemáticas abstractas. No obstante, para el entendimiento de este concepto de abstracción, es necesario definir el concepto de espacio vectorial. Asimismo, para definir el concepto de espacio vectorial, hay que tratar el concepto de base.

Dado el siguiente vector, que, sin pérdida de generalidad, ha sido reducido a las tres dimensiones, se puede descomponer en la siguiente suma - que se efectúa entre vectores de las misma dimensión y orientación, componente a componente:

$$\begin{aligned} v &= \begin{pmatrix} a \\ b \\ c \end{pmatrix} \\ &= a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \\ &\equiv ae_1 + be_2 + ce_3 \end{aligned} \tag{2.1.10}$$

Se dice entonces que el vector v se expresa en la base $\mathcal{C}$ con coeficientes $\{a, b, c\}$. Se dice que la base es la envolvente lineal de los vectores anteriores: $\mathcal{C} = \mathbb{L}(e_1, e_2, e_3)$. A esta base se le llama base canónica en la tercera dimensión. Es importante destacar que las bases $\mathbb{L}(e_1, e_2, e_3)$ y $\mathbb{L}(e_2, e_3, e_1)$ no son equivalentes, ya que las representaciones del mismo vector serían $\{a, b, c\}$ y $\{b, c, a\}$, respectivamente. Ahora bien, no todas las envolventes lineales son bases de un espacio vectorial. Para serlo, tienen que poder general cualquier vector de dicho espacio mediante la elección apropiada de los coeficientes que acompañan a los vectores de dicha base. A continuación se enumeran algunas definiciones sobre las bases:

- Se dice que una base b está normalizada si se cumple: $\forall b_i \in b(\langle b_i|b_i\rangle = 1)$.
- Se dice que una base b es ortogonal si se cumple: $\forall b_i, b_j \in b(i \neq j \leftrightarrow \langle b_i|b_i\rangle = 0)$.
- Se dice que una base b es ortonormal si es ortogonal y está normalizada. Las bases ortonormales cumplen que: $|b\rangle\langle b| = \mathbb{I}$, donde $\mathbb{I}$ es la identidad, lo que significa que en cualquier parte de una expresión en notación de Dirac se puede introducir sin efectos, por conveniencia.

En la notación de Dirac, pese a lo dicho anteriormente, un vector columna no es exactamente equivalente a un ket, ya que un ket no tiene base especificada, y un vector columna sí. En la notación de Dirac, si se tienen dos bases ortonormales b_1 y b_2, y un vector w, se tiene lo siguiente:

- Vector sin base o ket: $|w\rangle$
- Vector en la base $b1$: $|b_1\rangle\langle b_1|w\rangle$
- Vector en la base $b2$: $|b_2\rangle\langle b_2|w\rangle$

Se dice entonces que un vector sin base es un vector abstracto. Asimismo, se dice que un conjunto de vectores abstractos constituyen un espacio abstracto. Todo lo anterior es generalizable igualmente al concepto de funciones, y a

dimensiones arbitrariamente grandes, conociéndose este tipo de espacios abstractos como espacios de Hilbert.

Además, se dice que si los kets pertenecen a un espacio de Hilbert $\mathcal{E}$, los bras pertenecen a su espacio de Hilbert dual $\mathcal{E}^*$.

Como cierre del apartado, y del apéndice, son muy reseñables las implicaciones que tiene esta formalización de la abstracción, separando, en definitiva, y como ya se verá, lo posible de su implementación real.

2.2. Postulados de la mecánica cuántica

2.2.1. Primer postulado

Todo estado cuántico está representado por un vector normalizado que pertenece a un espacio de Hilbert complejo separable, $|\psi\rangle \in \mathcal{H}$. Dada una base en un espacio de Hilbert $|u_i\rangle$, que ha de ser ortonormal, se cumple: $|u\rangle\langle u|\psi\rangle = \sum_i c_i|u_i\rangle$, con $c_i = \langle u_i|\psi\rangle$.

2.2.2. Segundo postulado

Llamándose observable a una magnitud que se puede medir, los observables, denotados por $\mathcal{O}$, son operadores lineales hermíticos. Tienen unos determinados estados propios, que son aquellos que hacen el operador diagonal, llamándose estos autoestados, denotados por $\langle o_i|$. Los valores que adquiere el operador para cada uno de estos autoestados se llaman autovalores, y se representan por λ_i. El conjunto de los autovalores se denomina espectro.

2.2.3. Tercer postulado

La medida de un observable $\mathcal{O}$ sobre un estado $|\psi\rangle$, arrojará un valor λ_i con una probabilidad $P_{\mathcal{O}}(\lambda_i) = \langle\lambda_i|\psi\rangle$. Este postulado es el que provee la naturaleza indeterminista a la mecánica cuántica.

2.2.4. Cuarto postulado

La medida de un observable $\mathcal{O}$ sobre un estado $|\psi\rangle$, que arroje un valor λ_i, hará colapsar instantáneamente la función de onda a λ_i normalizado. Este postulado es el que causa la perdida de información en la medida.

2.2.5. Quinto postulado

La evolución temporal de un estado cuántico entre medidas viene dado por el operación evolución temporal $\mathcal{T}$. Este operador cambia radicalmente dependiendo de que variante de la mecánica cuántica se considere, dando lugar a diversas ecuaciones -Schrödinger, Klein-Gordon, Dirac. Aun así, esta elección no es la más importante a la hora de explicar los fenómenos relativos a la computación cuántica.

3. Computación, algoritmos y complejidad

3.1. Introducción

En los apartados anteriores se ha abordado una de las dos partes de la computación cuántica: la mecánica que la gobierna, o lo que es lo mismo, las leyes físicas que aplican en la descripción de la realidad y de las posibilidades que ofrece. La otra gran parte del problema es la computación. Entendiéndose por computación la resolución de problemas mediante algoritmos, la definición se reduce a aquella de algoritmo.

Un algoritmo es, así pues, un conjunto finito de instrucciones bien definidas, con un orden dado, que permiten la resolución de un problema sin intervención externa -como podría ser la intervención humana. No existe una definición consensuada formal de lo que es un algoritmo, pero se requieren, generalmente, tres características: secuenciabilidad, abstracción y la completa determinación del paso de un estado al siguiente. En esencia, el algoritmo ha de ser autónomo para considerarse tal, sin necesidad de suposiciones adicionales. Esta autonomía es de gran interés cuando se quiere que la ejecución de dicho algoritmo sea realizada por un autómata -como puede ser un ordenador, un microprocesador o una calculadora, entre otros.

Ahora bien, la computación no solo abarca el hecho de resolver el problema en sí, sino en analizar la eficiencia de dicha resolución. Dicha eficiencia es independiente del tiempo que tarde en ejecutarse el algoritmo. Para catalogar el conjunto de los algoritmos que resuelven un determinado problema, según eficiencia, es necesario conocer el número de iteraciones que se requieren para la resolución de dicho algoritmo, entendiéndose por iteración la repetición de un determinado ciclo del algoritmo, que se considera satisfecho bajo alguna condición de parada. Formalmente, se reduce a, denotando como $\mathcal{A}(\Pi)$ el conjunto de los algoritmos que resuelven un problema denotado por Π, dotar a este conjunto de una relación de orden, denotada por R, en cuanto a eficiencia se refiere: $(\mathcal{A}(\Pi), R)$.

Como observación, el tiempo en esta clasificación es irrelevante, sólo estando relacionado con el tiempo que se tarda en hacer una iteración. Por ejemplo, la ejecución del algoritmo de la suma con llevadas no es más compleja si se ejecuta en un superordenador que por un humano, ya que el número de iteraciones será el mismo, aunque el tiempo por iteración discrepe estrepitosamente.

Ahora bien, para un algoritmo dado, el número de iteraciones requeridas puede variar con las condiciones iniciales o entradas del algoritmo. Por ejemplo, en ordenar una lista de elementos, que está desordenada, el número de iteraciones depende enormemente de lo desordenada que esté la lista, en comparación con el orden buscado. Los elementos de la lista y sus posiciones iniciales serían las entradas del algoritmo. Además, el análisis de la eficiencia de un algoritmo

cobra sentido en número de entradas, denotado por N, lo suficientemente grande, lo que se puede considerar como $N \to \infty$. Es por esto que se utilizan las llamadas cotas asintóticas inferior Θ, superior O, y ajustada, Ω, para cuantificar estos matices.

$$O(g(x)) = \{f(x) : \exists c(c > 0 \wedge (\forall x(x \geq x_0 \geq 0 \wedge (0 \leq |f(x)| \leq c|g(x)|)))\} \quad (3.1.1)$$

$$\Theta(g(x)) = \{f(x) : \exists c(c > 0 \wedge (\forall x(x \geq x_0 \geq 0 \wedge (0 \leq c|g(x)| \leq |f(x)|)))\} \quad (3.1.2)$$

$$\Omega(g(x)) = \{f(x) : (f(x) \in O(g(x)) \wedge f(x) \in O(g(x)))\} \quad (3.1.3)$$

Donde x correspondería al número de entradas N, $f(x)$ al algoritmo que resuelve un problema dado como función de la entrada, y $g(x)$ corresponde a la cota asintótica de dicha función.

Para mayor formalidad, se consigue establecer una serie de conjuntos al que hacer pertenecer algoritmos, estando dichos conjuntos ordenados, y estableciéndose una relación indirecta de orden para los algoritmos. Al final, el conjunto más utilizado es el primero de todos, que daría cuenta de la cota superior, y que está íntimamente relacionado con la clase de complejidad. Se podría decir, informalmente, que:

$$C.C. = M.C. + C.S.A.I. \quad (3.1.4)$$

Donde $C.C.$ es la clase de complejidad, $M.C.$ es el modelo de cómputo, y $C.S.A.I.$ es la cota superior asíntótica para iteraciones.

Entre los modelos de cómputo se encontrarían, por ejemplo:

- La máquina de Turing clásica determinista.
- La máquina de Turing clásica no-determinista.
- La máquina de Turing cuántica.

Las cotas superiores asintóticas serían, por ejemplo:

- Orden constante: $O(1)$
- Orden sublogarímico: $O(\log(\log(n))$
- Orden logarítmico: $O(\log(n))$
- Orden sublineal: $O(\sqrt(n))$
- Orden lineal: $O(n)$
- Orden lineal logarítmico: $O(n \log(n))$
- Orden potencial: $O(n^c)$
- Orden exponencial: $O(c^n), n > 1$

- Orden factorial: $O(n!)$

Es en este punto donde comienza a cobrar sentido el objetivo del presente texto, que consiste en describir algoritmos que, para un mismo problema, mediante un cambio en el modelo de cómputo -cuántico por clásico -reduzcan su complejidad. A continuación se describen, mediante el formalismo de la mecánica cuántica, algoritmos que, bajo la citado cambio de modelo de cómputo.

3.2. Algoritmo de Grover

Uno de los problemas fundamentales relativos a la algoritmia es la búsqueda en listas, esto es, por ejemplo, una lista de textos en la que se quiere buscar si hay un texto determinado, o de forma más abstracta, una lista de conjuntos en la que se quiere buscar si hay un conjunto subconjunto de alguno de los conjuntos de la lista. La lista, a fin de cuentas, es un conjunto indexado, que se denotará por $C = C_i \forall i \in [1, M] \subset \mathbb{N}$. Si se denota el conjunto objeto de búsqueda por D, se puede definir la siguiente función:

$$f : [0, M] \subseteq \mathbb{N} \to 0, 1 \wedge f(x) = 1 \leftrightarrow D \in C_x \tag{3.2.1}$$

Se entiende que la función adquiere el valor 1 en el caso de que la búsqueda encuentre resultado en ese conjunto, y que en cualquier otro caso el valor adquirido es 0.

La búsqueda de este valor en computación clásica, se haría en N iteraciones, en el peor de los casos. Esto equivale a que sólo se podría asegurar la solución del problema cuando se busque en todos los elementos existentes. Esto parece totalmente lógico.

No obstante, el algoritmo de Grover, basado en computación cuántica, ofrece el mismo resultado en $\sqrt{N}$ iteraciones. Esto constituye un cambio de complejidad mediante un cambio de modelo de cómputo.

En este algoritmo, se necesita representar con un registro de q-bits -o lo que es lo mismo, un conjunto ordenado, un número que oscilará entre 0 y N, y ya que cada q-bit admite dos posiciones, se necesitará un número de q-bits $M = \log_2 N$.

Es por esto que se tendrá un registro $\{|1\rangle_i, |0\rangle_i\}$ $\forall i \in [1, M]$. Se podría representar:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{M} (a_i|0\rangle_i + b_i|1\rangle_i) \tag{3.2.2}$$

Los coeficientes a_i y b_i se asignan en función del estado que se quiera, con la condición de normalización $a_i^2 + b_i^2 = 1$. Esta condición refleja que la probabilidad de encontrar un estado en ese estado es 1. Si se quisiera que todos los

los estados, por ejemplo, fueran $|0\rangle$, se tendría que $a_i = 1, b_i = 0\ \forall i$.

El algoritmo es como sigue:

1. Se inicializa un q-bit ajeno al registro, como $|\psi_{aux}\rangle = |1\rangle$. Su función es simplemente la posibilitación de los observables usados.

2. Se inicializan los estados del registro para que todos sean $|0\rangle$.

3. Se aplica a todos los q-bits una transformada de Hadamard, que es como sigue, para un q-bit:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.2.3}$$

   Para cada q-bit $|u_i\rangle$ actúa sobre el vector formado por a_i, b_i, con lo que está en base de los q-bits $|0\rangle_i$ y $|1\rangle_i$. El resultado de la transformación aplicada sobre un q-bit en $|0\rangle$ es el siguiente:

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \end{aligned} \tag{3.2.4}$$

   Este estado es equidistribuido. Así ocurrirá con todos los q-bits, haciendo la distribución equidistribuida o difundida. Esta transformación n-aria de Hadamard se denomina operador de difusión.

4. Se aplica al q-bit ajeno la transformada de Hadamard, que lo deja en: $|\psi_{aux}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Este q-bit no se volverá a modificar.

5. Se aplica un operador conocido como oráculo cuántico, que se denotará por U_w. Es un máximo ejemplo de abstracción, en el que se implementa matemáticamente, pero sin conocimiento material del dispositivo, un objeto que, cuando el registro coincide con el valor en el que la coincidencia se produce, que se llamará $|w\rangle$, desfasa el estado, mientras que si no coincide, lo deja inalterado. Esto es análogo a la función $f(x)$ definida en (). En un espacio abstracto, el operador se definiría:

$$U_w = \mathbb{I} - 2|w\rangle\langle w| \tag{3.2.5a}$$

$$U_w|w\rangle = \mathbb{I}|w\rangle - 2|w\rangle\langle w|w\rangle = -\mathbb{I}|w\rangle = -|w\rangle \tag{3.2.5b}$$

$$U_w|x\rangle = \mathbb{I}|x\rangle - 2|w\rangle\langle w|x\rangle = \mathbb{I}|x\rangle = |x\rangle, |x\rangle \neq |w\rangle \tag{3.2.5c}$$

6. Se aplica el operador de difusión de Grover, que actúa, sobre un q-bit cualquiera, de la siguiente forma:

$$\begin{aligned} H(a|0\rangle + b|0\rangle) &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}((a+b)|0\rangle + (a-b)|1\rangle) \end{aligned} \tag{3.2.6}$$

7. Se repiten 5. y 6. hasta $\sqrt{N}$ veces.

8. Se mide el registro. Con el autovalor resultante para cada q-bit, se calcula el autovector asociado, y, por ende, el registro donde se encontraba el valor buscado.

La explicación es la siguiente. El operador recursivo, que se puede denotar de forma abstracta por:

$$U_s = 2|s\rangle\langle s| - \mathbb{I} \tag{3.2.7a}$$

$$U_w = \mathbb{I} - 2|w\rangle\langle w| \tag{3.2.7b}$$

$$R = U_s U_w = 2|s\rangle\langle s| - 2|w\rangle\langle w| + 4|s\rangle\langle s|w\rangle\langle w| - \mathbb{I} \tag{3.2.7c}$$

aumenta el coeficiente asociado a $|w\rangle$ en detrimento de $|s\rangle$. En la primera iteración, se acaba con:

$$|\psi\rangle = \frac{N-4}{N}|s\rangle + \frac{2}{\sqrt{N}}|w\rangle \tag{3.2.8}$$

Al repetir la operación recursivamente, el valor esperado acaba siendo el autovalor de $|w\rangle$ con muy alta fidelidad. Esto pone de manifiesto que el algoritmo es probabilístico, y puede fallar, mínimamente. Este problema se puede corregir multiplicando los registros y paralelizando, lo que no afecta a la complejidad, ya que $O(\sqrt{mN}) \equiv O(\sqrt{N}), m << N$.

Cabe destacar que si no hay ningún registro coincidente, la recursividad sería equivalente a aplicar U_s, y como $U_s|s\rangle = |s\rangle$, no habría valor esperado, simplemente, seguiría en el estado equipartito inicial.

Uno de los problemas importantes de los algoritmos cuánticos se pone de manifiesto aquí, ya que, como se puede comprobar, no se puede evaluar el estado del proceso durante su transcurso, simplemente al final. Esto es derivado del colapso del estado producido en las medidas.

3.3. Algoritmo de Shor

Otro de los grandes problemas relacionados con la computación, importante por sus implicaciones en la seguridad de las encriptaciones RSA, es el algoritmo de Shor. Este algoritmo está planteado ciertamente como un híbrido, con una parte clásica y una cuántica.

La idea es descomponer un número entero impar M en dos factores factores coprimos, es decir, que no tengan común divisor mas que 1, y que serán también impares. La razón de no trabajar con números pares es que un factor obvio es 2.

El componente clásico es el siguiente:

1. Se selecciona un número aleatorio -por una función random, que siempre es pseudoaleatoria -denotado por a, tal que: $a \in (1, M) \subseteq \mathbb{N}$.
2. Se calcula el máximo común divisor de a y M, denotado por $mcd(a, M)$, lo que da lugar a las siguientes posibilidades.
   a) $mcd(a, M) \neq 1$, con lo que a es factor no trivial de M, luego se acaba el algoritmo.
   b) $mcd(a, M) = 1$, con lo que se puede buscar el periodo de la siguiente función:

$$f(x) = a^x (mod\ N) \tag{3.3.1}$$

   Donde $(mod\ N)$ denota que se trata de álgebra modular, con módulo N. Es decir, significa que $f(x) + N \equiv f(x)(mod\ N)$. El ejemplo más claro es el de las horas de un reloj, o los grados de un giro. Girar 360°es equivalente a no girar.

   Si este periodo es τ, se tiene que $a^\tau \equiv 1(mod\ N)$. τ es un valor mínimo, ya que si no el periodo sería otro, lo que implica que $a^\tau - 1 \equiv 0(mod\ N)$, lo que equivale a decir que $a^\tau - 1 = N$.

   Como $a^\tau - 1 = (a^{\frac{\tau}{2}} - 1)(a^{\frac{\tau}{2}} + 1)$, se entiende que $(a^{\frac{\tau}{2}} - 1)$ y $(a^{\frac{\tau}{2}} + 1)$ son factores de N, no triviales salvo que $a^{\frac{\tau}{2}} \equiv -1$. Si este fuera el caso, se repetiría el algoritmo.

Ahora bien, encontrar el periodo de una función clásicamente puede ser muy costoso, pero no lo es cuánticamente, ya que existe un operador bastante natural en la mecánica cuántica, conocido como transformada cuántica de Fourier, o QFT -por sus siglas en inglés -cuya definición, dados un registro de q-bits de entrada $|u_x\rangle$, y otro de salida $|w_y\rangle$, equidimensionales, es la siguiente:

$$U_{QFT}|u_x\rangle = \frac{1}{\sqrt{N}} \sum_{y=1}^{N} \left(e^{\frac{2\pi i x y}{N}} |w_y\rangle \right) \tag{3.3.2}$$

Es necesario señalar, en primer lugar, que la transformada de Fourier es una aplicación funcional que lleva una función $\mathcal{F} : f(x) \to \tilde{f}(k)$, donde si x es la variable original, $k \equiv \frac{2\pi}{x}$ es la variable conjugada, que da cuenta de las frecuencias de repetición sobre la variable x.

Además, el análisis de Fourier demuestra que toda función sobre un dominio $x \in [a, b] \subseteq \mathbb{R}$ se puede descomponer en una suma, finita o infinita, discreta o continua, de funciones periódicas de distintas frecuencias. Estas frecuencias vienen determinadas por la transformada de Fourier.

Al poder calcular las frecuencias k_i de una función $f(x)$, se puede calcular los periodos $T_i \equiv \frac{2\pi}{k_i}$. En el caso particular tratado, la función solo tiene un periodo, con lo que el resultado será único.

La parte cuántica del algoritmo consiste, simplemente en los siguientes pasos:

1. Se prepara una implementación cuántica de la función f sobre el registro de N q-bits, de tal forma que se pueda obtener $|f(\psi)\rangle \equiv f|\psi\rangle$.

2. Se aplica el operador U_{QFT} sobre $|f(\psi)\rangle$, lo que lleva al siguiente estado:

$$U_{QFT}|f(\psi)\rangle = \frac{1}{\sqrt{N}} \sum_{z=1}^{N} \sum_{y=1}^{N} \left(\left(\sum_{b\{\frac{x}{r}:(f(x)=z)\}} e^{\frac{2\pi i b y}{N}} \right) |w_{y,z}\rangle \right) \tag{3.3.3}$$

3. Se efectúa una medida. La probabilidad de obtener uno de los estados $|w_{y,z}\rangle$ viene dada por:

$$\langle w_{y,z}|U_{QFT}|f(\psi)\rangle = |\sum_{b} e^{\frac{2\pi i b r y}{N}}|^2 \tag{3.3.4}$$

   Esta probabilidad crece enormemente cuando $bry \to 1$, lo que hace la exponencial real.

4. La obtención del periodo habría finalizado, ya que en función del autovalor medido, se sabe el estado $|w_{y,z}\rangle$ asociado a un periodo determinado. Cabe destacar que la implementación de dicho operador, U_{QFT}, requiere un registro adicional.

Este algoritmo, en su parte cuántica, resulta especialmente interesante, porque no requiere de repeticiones, salvo las requeridas internamente para efectuar la transformada de Fourier. No obstante, la respuesta es directa. Dado que la fiabilidad no es total, repitiendo el procedimiento cuántico para cada número ensayado más de una vez, se puede confirmar que el periodo de la función que arroja la parte cuántica es correcto.

3.4. Algoritmo de Deutsch-Josza

Como contrapunto a los dos algoritmos anteriores, el presente no atiende a ningún problema conocido con anterioridad. Simplemente, es un algoritmo que se implementó para demostrar, por ejemplificación, que existen problemas que en la computación clásica deterministas son más complejos que en la computación cuántica. Esto lo convierte en un candidato idóneo para su mención.

El problema planteado es el siguiente: Se tiene una función definida por $f : \{0,1\}^n \to \{0,1\}, n \in \mathbb{N}$. La función, además, sólo tiene tres opciones: arrojar todo 1, para cualquiera de los valores de entrada, arrojar todo 0, o estar repartida equitativamente -es decir, balanceada. Determinar si la función es constante o balanceada.

Antes de nada, es necesario definir una operación, conocida como suma de módulo 2, de la siguiente manera:

$$0 \oplus 0 = 0 \tag{3.4.1a}$$

$$0 \oplus 1 = 1 \tag{3.4.1b}$$

$$1 \oplus 0 = 1 \tag{3.4.1c}$$

$$1 \oplus 1 = 0 \tag{3.4.1d}$$

Lo que sería equivalente a la puerta lógica XOR.

El algoritmo es como sigue:

1. Se tiene un registro de $N+1$ q-bits, inicializados todos a$|\psi_0\rangle$, que deja todos los q-bits en $|0\rangle$ salvo el último, inicializado a $|1\rangle$. Este registro puede almacenar un número del orden de 2^N.

2. Se aplica una transformación de Hadamard al registro, quedando los N primeros q-bits del siguiente modo:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (|0\rangle - |1\rangle)_i \tag{3.4.2}$$

3. Implementada la función f como un oráculo cuántico, de la forma que sigue:

$$f|u_i\rangle = |u_i \oplus f(i)\rangle \tag{3.4.3}$$

4. La probabilidad de medir el registro inicial $|\psi_0\rangle$ viene dada por:

$$\langle\psi_0|u_i \oplus f(i)\rangle = |\frac{1}{N} \sum_{i=0}^{N-1} (-1)^{f(x)}|^2 \tag{3.4.4}$$

   Dicha probabilidad es 1 si $f(x)$ es constante, y 0 si está la función balanceada.

Para evaluar la probabilidad de una medida, es conveniente, debido a la fidelidad no completa, repetir el proceso varias veces, para tener con certeza la información de probabilidad, lo que sería un $p - bit$. Esta repetición no tiene afectación en la complejidad.

3.5. Situación actual

Como conclusión de lo expuesto en la sección anterior, es interesante, después de tanta abstracción, mencionar sucintamente el estado práctico o experimental de la cuestión.

En primer lugar, al igual que en computación clásica, gobernada por el álgebra de Boole, pueden construirse todas las puertas lógicas a partir de dos: puertas de conjunción negada e inversores; está demostrado que todas las puertas imaginables de la computación cuántica se pueden construir a partir de tres: puerta de Hadamard, inversor controlado, y puerta de salto de fase controlado.

Las computadoras cuánticas son, en general muy complicadas y muy susceptibles a las condiciones ambientales, requiriéndose, para su fiabilidad óptima el perfecto aislamiento en la mayoría de los casos. No obstante, y recientemente, se han implementado dos de estas tres puertas, que formarían base -retomando la nomenclatura anterior -de cualquier puerta cuántica, en sustratos de silicio, utilizando fotones como q-bits, en guías de onda impresas con tecnologías equiparables a las de impresión de circuitos electrónicos. Esto es muy prometedor, ya que con esta tecnología no sólo sería una realidad confinada en los laboratorios, sino que se podría llegar a la producción en serie.

No obstante, los circuitos hechos hasta ahora, para resolver algoritmos cuánticos, están todavía muy poco avanzados. Se consiguió así pues demostrar el algoritmo de Shor, pero únicamente para descomponer 15 en 3 y 5 utilizando siete q-bits.

4. Conclusiones

Desde un punto de vista práctico, es muy fácil extraer una idea importante, y es que la computación cuántica resuelve algunos problemas, al menos teóricamente, que la computación clásica no resuelve. Esto puede ser muy apreciado para personas que tengan como objetivo, por ejemplo, romper una encriptación RSA.

No obstante, hay un punto de interés a nivel del pensamiento, que se ha mencionado técnicamente a lo largo del escrito. En referencia al algoritmo de Grover, no hay nadie en el mundo que, a la hora de enfrentarse a un problema como el de buscar elementos en una colección ordenada pueda prometer una solución que no pase por, en el peor de los casos, mirar todos los elementos y

comparar. En referencia al algoritmo de Shor, nadie en el mundo podría resolver, de forma natural, la factorización mediante la transformación de Fourier y el hallazgo del periodo de forma más sencilla que lo haría, por complejo que fuese, probando aleatoriamente y afinando en sus ensayos.

Esto pone de manifiesto que el modo humano de pensar o, mejor dicho, de computar, es, en resumidas cuentas, con todas las salvedades que se quieran, mucho más similar a la computación clásica que a la cuántica. Ya George Boole llamó al tratado de 1854 acerca de las reglas subyacentes a la lógica Ïnvestigación sobre las leyes del pensamiento". La computación cuántica, sin embargo, posibilita hacer operaciones que son inalcanzables para el modo de computar propio de la mente humana.

Por ende, y más allá de las realizaciones prácticas, o de la mejora de la eficiencia, el hecho de que problemas que en el modelo de cómputo clásico no pueden ser simplificados en cuanto a clase de complejidad se refiere, y que estos mismos problemas puedan ser simplificados en el modelo cuántico, rompe una barrera teórica entre la computación clásica y la cuántica, de gran trascendencia en lo referido a las leyes del pensamiento.

Aun así, la computación cuántica es sólo una de las caras de la mecánica cuántica. A lo largo del escrito, se ha hecho referencia a fenómenos, en lo relativo a su estructura matemática, sin profundizar en el problema filosófico que pueden plantear. Es crucial, para cualquier disciplina de la filosofía que pretenda explicar las inferencias o la interacción del razonamiento con la información, afrontar el problema de la medida, es decir, el hecho de que la información, por el hecho de conocerla, se vea alterada instantáneamente. Esto es una limitación teórica fundamental al acceso a la información.

Asimismo, el hecho de múltiples realidades puedan coexistir hasta que son medidas es, cuanto menos, inquietante. Esto no es simplemente una conclusión matemática absurda, sin aplicación práctica, sino un fenómeno medido y tangible. Tanto es así que gran parte de las rarezas de la computación cuántica están basadas en este fenómeno.

Retomando el problema de la medida, este puede tener otras implicaciones, en el campo de la causalidad. Ninguna teoría en la física clásica o relativista, ni siquiera en la física estadística -que en el fondo no es independiente de la mecánica cuántica, aunque anterior, ya que se construyó bajo una asunción que es propia de la cuantización de los estados posibles -da una explicación a la causalidad convincente. La explicación más extendida de porqué el tiempo transcurre hacia delante, problema a veces llamado *la flecha del tiempo*, es que la entropía, o desorden, siempre aumenta, y el tiempo avanza en el sentido en que aumenta la entropía. Esta explicación resulta, en el mejor de los casos, insatisfactoria. Simplemente se demuestra que la entropía o desorden aumenta con el tiempo, lo que es una información muy interesante, pero no explica por-

qué no se puede ir atrás en el tiempo, en el sentido en que la entropía disminuye.

No obstante, el colapso en la medida de un estado cuántico resultaría una explicación convincente, ya que, en el fondo, no depende de un incremento de tiempo, ya que es instantáneo, y constituye una asimetría fundamental entre el antes y el después, que causa que, una vez en el después, no se pueda recuperar la información del antes. Cabe destacar que el problema de la medida no se refiere únicamente a la medida en un laboratorio, sino a cualquier interacción entre estados cuánticos independientes que cause que estos tengan que determinar sus propiedades para efectuar dicha interacción, que puede entenderse como un intercambio de información. Con esto queda claro que ocurren colapsos en las funciones de onda de los constituyentes del Universo constantemente. Además, esta explicación es compatible con el aumento de la entropía en la dirección en la que el tiempo aumenta, o, según este modelo, en aquella determinada por las medidas y los colapsos de funciones de onda.

Por último, en un sentido más físico, el entrelazamiento cuántico plantea un problema. Si dos estados cuánticos, que se han entrelazado, se separan una distancia arbitrariamente grande, seguirían entrelazados. Esto significa que si se colapsa, en un punto, la función de onda, se colapsa, instantáneamente, en el otro. Esto es una transferencia de información, en principio, que supera la limitación impuesta por la Teoría de la Relatividad de Einstein, en cuanto a que no se puede transmitir información más rápido que la velocidad de la luz, que es constante universal. Esto plantea un problema relativo a que, si no se está transfiriendo información, es que la información ya estaba allí. Si la información estaba allí, cómo es posible que allí estuviera recogido el momento en que la persona en cuestión iba a medir la función de onda para colapsarla. Esto sugiere algo así como la predestinación, y, por lo absurdo que parece, a priori, que esto suceda, se hace merecedor de interés por parte tanto de la física como de la filosofía dar explicación a esta paradoja.

Con todo esto queda de manifiesto que el problema de la computación cuántica, y la mecánica que la gobierna, pueden tener implicaciones de mucho mayor calado que, simplemente, la mejora de algoritmos.

5. Referencias

D. Deutsch (1985) *Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer.*, Londres, Proceedings of the Royal Society Publishing, pp. 97-117.

R. P. Feynman (1982) *"Simulating Physics with Computers."*, Berlín, *International Journal of Theoretical Physics*, Vol. 21, Springer Science + Business Media, pp. 467-488.

M. Nielsen, I. Chuang (2000) *Quantum Computation and Quantum Information.*, Cambridge, Cambridge University Press.

Agustín Rayo (2010) *Çomputación cuántica"*, Barcelona, *Investigación y Ciencia*, 405, pp. 92-93.

Mario Mastriani (4 de septiembre de 2014, consultado el 2 de diciembre de 2014) *Memorias matriciales correlacionadas cuánticas, simples y mejoradas: una propuesta para su estudio y simulación sobre GPGPU.*, Internet, (http://sedici.unlp.edu.ar/handle/10915/39869).

Claude Cohen-Tannoudji, Bernard Diu y Frank Laloë (1973) *Mécanique quantique Vol. I et II*, París, Collection Enseignement des Sciences.

S. Auyang (1995) *How is Quantum Field Theory Possible?*, Oxford, Oxford University Press.

G. Birkhoff y J. von Neumann (1936) *"The Logic of Quantum Mechanics"*, Princeton, *Annals of Mathematics*, Second Series, Vol. 37, No. 4, pp. 823-843.

D. Cohen (1957) *An Introduction to Hilbert Space and Quantum Logic.*, Berlin, Springer-Verlag, pp. 885-893.

D. Finkelstein (1969) *Matter, Space and Logic.*, Boston, Proceedings of the Royal Society Publishing.

A. Gleason (1957) *"Measures on the Closed Subspaces of a Hilbert Space."*, Cambridge, Massachusetts, *Journal of Mathematics and Mechanics*, Vol. 6, No. 6, Harvard University Press, pp. 885-893.

R. Kadison (1985) *Isometries of Operator Algebras.*, Londres, Proceedings of the Royal Society Publishing, pp. 97-117.

G. Ludwig (1983) *Foundations of Quantum Mechanics.*, Berlin, Springer-Verlag.

G. Mackey (1963) *Mathematical Foundations of Quantum Mechanics.*, San Francisco, W. A. Benjamin.

J. von Neumann (1955) *Mathematical Foundations of Quantum Mechanics.*, Princeton, Princeton University Press.

R. Omnès (1999) *Understanding Quantum Mechanics.*, Princeton, Princeton University Press.

N. Papanikolaou (2005) *Reasoning Formally About Quantum Systems: An Overview.*, New York, ACM SIGACT News, 36(3), pp. 51-66.

Piron (1976) *Foundations of Quantum Physics.*, San Francisco, W. A. Benjamin.

H. Putnam (1969) *Is Logic Empirical?*, Boston, Boston Studies in the Philosophy of Science Vol. 5.

H. Weyl (1950) *The Theory of Groups and Quantum Mechanics.*, Mineola, Nueva York, Dover Publications.

Alberto Politi, Martin J. Cryan, John G. Rarity, Siyuan Yu, Jeremy L. O'Brien (2008) *"Silica-on-Silicon Waveguide Quantum Circuits."*, *Science*, Vol. 320. no. 5876, Nueva York, pp. 646-649.