MECANICA CUANTICA PARA GENTE MATEMATICAMENTE ILUSTRADA SIN ENTRENAMIENTO EN FISICA

Alberto Mejías[1]

0. Introducción

La Mecánica Cuántica se ocupa del comportamiento de la materia y la radiación en las escalas atómica y subatómica. Procura describir y explicar las propiedades de las moléculas, los átomos y sus constituyentes: electrones, protones, neutrones, y otras partículas más esotéricas como los quarks y los gluones. Esas propiedades incluyen las interacciones de las partículas entre sí y con la radiación electromagnética.

El comportamiento de la materia y la radiación en la escala atómica presenta aspectos peculiares; de acuerdo con ello las consecuencias de la Mecánica Cuántica no siempre son intuitivas ni fáciles de entender. Sus conceptos chocan con las nociones que nos resultan familiares porque derivan de las observaciones cotidianas de la naturaleza en la escala macroscópica. Sin embargo, no hay razones en virtud de las cuales el comportamiento del mundo atómico y subatómico deba seguir las mismas pautas que los objetos de nuestra experiencia diaria.

[1] Alberto R. Mejías E., es Licenciado en Matemática, egresado de la Facultad de Ciencias de la Universidad de los Andes, ULA (Mérida – Venezuela). Profesor de Análisis y Topología. Actualmente es jubilado de la Universidad de los Andes.
alrame59@cantv.net, alrame59@gmail.com, alrame59@hotmail.com.

Mecánica cuántica para gente matemáticamente ilustrada sin entrenamiento en física

El desarrollo de las ideas básicas de la Mecánica Cuántica comenzó a principios del siglo XX, como consecuencia de una serie de descubrimientos y observaciones que pusieron en evidencia las graves dificultades de la Física Clásica para interpretar las propiedades del átomo y sus partes constituyentes así como las propiedades de la radiación electromagnética y su interacción con la materia. Esos descubrimientos revolucionaron las nociones hasta entonces sustentadas por los físicos y plantearon una asombrosa cantidad de enigmas, cuya solución obligó a realizar un profundo replanteo de los fundamentos y conceptos básicos de la Física.

El estudio de la Mecánica Cuántica es importante por varias razones. En primer lugar porque pone de manifiesto la metodología esencial de la Física. En segundo lugar porque tuvo un éxito formidable ya que permitió dar respuestas válidas a casi todos los problemas en los cuales se la ha aplicado. En tercer lugar porque es la herramienta teórica básica para numerosas disciplinas de gran importancia, como la Química Física, la Física Molecular, Atómica y Nuclear, la Física de la Materia Condensada y la Física de Partículas.

Subsiste, sin embargo, una curiosa paradoja alrededor de la Mecánica Cuántica. A pesar de su notable éxito en todas las cuestiones de interés práctico en las que se la ha aplicado, sus fundamentos contienen aspectos aún no aclarados en forma completamente satisfactoria. En particular, cuestiones relacionadas con el proceso de medición.

Una característica esencial de la Mecánica Cuántica, que la diferencia de la Mecánica Clásica, es que en general es imposible por razones de principio, efectuar una medición sobre un sistema sin perturbarlo. Pero los detalles de la naturaleza de esta perturbación, y el punto exacto en que ella ocurre son asuntos aún oscuros y

controvertidos. Por estos motivos la Mecánica Cuántica atrajo algunos de los más brillantes científicos del siglo XX, que han erigido con ella un majestuoso y elegante edificio intelectual.

En su escrito ***From Cbits to Qbits: Teaching Computer Scientists Quantum Mechanics*** (arXiv: quant-ph/0207118v1 19 Jul 2002), N. David Mermin propone una estrategia para la enseñanza a estudiantes matemáticamente ilustrados, sin entrenamiento en Física, de suficiente Mecánica Cuántica como para que puedan entender y desarrollar algoritmos en Computación y Teoría de la Información Cuánticas.

Aunque el artículo está dedicado, en su integridad, a docentes en Física, bien versados en Mecánica Cuántica, el desarrollo didáctico central está directamente dirigido a Informáticos y Matemáticos, con sólo ocasionales referencias a sus docentes. A los físicos no interesados en didáctica cuántica pueden parecerles divertidos (o irritantes) algunos de los puntos de vista de la Mecánica Cuántica típica que se logran desde esta perspectiva heterodoxa; sin embargo, por su simplicidad y originalidad este planteamiento merece una cuidadosa consideración.

1. Informática y Mecánica Cuántica

Comparados con los estudiosos típicos de un curso introductorio a la Mecánica Cuántica, los estudiosos de Informática son matemáticamente ilustrados; pero, a menudo, ignorantes o desinteresados en Física. En general, su interés se reduciría a las aplicaciones de la Mecánica Cuántica durante las últimas décadas, al procesamiento de información y su enfoque hacia el desarrollo de algoritmos (software: programatura) y no hacia la ingeniería (hardware: realización física de las computadoras, panoplia).

Mecánica cuántica para gente matemáticamente ilustrada sin entrenamiento en física

Aunque los obstáculos para que la Computación Cuántica sea una tecnología viable, son formidables, las profundas consecuencias de la Mecánica Cuántica para la teoría de computación descubierta durante las últimas décadas del Siglo XX, deben ser parte del equipaje intelectual de todo estudioso de Informática. Aunque sea sólo porque provee una dramática prueba de que el análisis abstracto de computación no puede estar divorciado de los medios físicos disponibles para su ejecución, los estudiosos de Informática deben aprender Mecánica Cuántica.

Ahora, el problema es ¿cuánta Mecánica Cuántica?

Cuenta David Mermin que cuando, en una conversación, le hizo notar al director del Institute for Theoretical Physics en Santa Bárbara, que había necesitado sólo las primeras cuatro a cinco clases de su curso sobre Computación Cuántica[2] para enseñarle la Mecánica Cuántica necesaria a los informáticos asistentes a su clase, el director le respondió que cualquier aplicación de la Mecánica Cuántica considerada después de una introducción de sólo cuatro horas a la materia, no podría tener un contenido intelectual serio. Además, insistió, a un físico le toma años desarrollar un sentido apreciativo de la Mecánica Cuántica.

Sin dejar de considerar que ese es un buen punto, DM señala que sin embargo, es un hecho que informáticos y matemáticos sin entrenamiento en Física, han sido capaces de aprender rápidamente, suficiente Mecánica Cuántica para comprender y contribuir significativamente a la Teoría de Computación Cuántica, aunque la Computación Cuántica explota, repetidamente, los más notablemente paradójicos aspectos de la materia. Hay tres razones principales para esto:

[2] www.ccmr.cornell.edu/~mermin/qcompCS483.html es una dirección donde se pueden hallar los apuntes y ejercicios correspondientes a este curso.

Primera, una computadora cuántica o, más precisamente, la computadora cuántica abstracta que esperamos que algún día se pueda construir, es un extremadamente simple ejemplo de sistema físico. Es discreto, no continuo. Está constituido por una cantidad finita de unidades, cada una de las cuales es del más simple posible tipo de sistema mecánico cuántico, un sistema de dos estados, cuyo posible comportamiento es altamente restringido y fácilmente analizado. Gran parte de la complejidad analítica en el aprendizaje de la Mecánica Cuántica está relacionada con la pericia para la descripción de sistema continuos (de infinitos estados) en el espacio-tiempo 3+1 dimensional. Restringiendo la atención a las transformaciones discretas que actúan sobre colecciones de 2-estados (estados bidimensionales), se pueden evitar muchos sufrimientos (y perder muchos conocimientos, ningunos de los cuales, al menos en la etapa actual del desarrollo, es relevante para la Teoría de Computación Cuántica).

Segunda, la parte más ardua en el aprendizaje de la Mecánica Cuántica es lograr un sentido de apreciación para la aplicación de los formalismos abstractos a los problemas prácticos en el laboratorio. Esto, casi invariablemente, involucra la formulación de modelos sobresimplificados de los fenómenos reales a los cuales se pueda aplicar el formalismo cuántico efectivamente. Los mejores físicos tienen una intuición extraordinaria con respecto a cuáles aspectos del fenómeno real son esenciales y se deben representar en el modelo abstracto y cuáles son inesenciales y pueden ser ignorados. Toma años de entrenamiento desarrollar esta intuición. Algunos nunca la logran. Sin embargo, la Teoría de Computación Cuántica sólo está interesada en el modelo abstracto, la parte fácil del problema.

Tercera, para comprender como realizar una computadora cuántica o para estudiar cuáles sistemas físicos son candidatos promisorios para realizar tal

dispositivo, hay que tener varios años de experiencia en Mecánica Cuántica y sus aplicaciones en el instrumental. Pero, si, en principio, sólo se quiere saber qué es capaz de hacer un tal dispositivo, entonces no hay razón para involucrarse con la, realmente ardua, Física de la materia. Lo mismo pasa con las computadoras ordinarias ("clásicas"): uno puede ser un informático magistral sin tener la mínima noción de lo que es un transistor, por no decir cómo trabaja.

Así que mientras que el enfoque diseñado por DM, de la Mecánica Cuántica para informáticos, es restringido, no es sobresimplificado ni incompleto para el cometido especial que lo motiva.

2. Bits Clásicos

La primera etapa en la enseñanza de la Mecánica Cuántica para informáticos, es la reformulación del lenguaje de computación convencional (*clásica*) de manera heterodoxa, tal que se presente buena parte del formalismo cuántico mediante un ajuste completamente familiar.

Para comenzar se necesita un término que designe a un sistema físico que puede existir en dos estados distinguibles sin ambigüedades, que se usan para representar 0 y 1. Usualmente, un tal sistema se llama un *bit*; pero, esto puede obscurecer la importante distinción entre el bit abstracto (0 ó 1) y el sistema físico usado para representarlo. Para resolver esta cuestión, llamaremos *Cbit* al sistema físico clásico usado para representar a un bit y *Qbit* a su generalización cuántica.

Puede ser útil, incluso en el nivel estrictamente clásico, representar los dos estados de un Cbit por un par de 2-vectores (vectores de dos dimensiones) ortonormales, denotados por los símbolos[3]

$$|0\rangle, \quad |1\rangle. \tag{1}$$

Para hacer cómputos no triviales se necesita más de un Cbit. Es conveniente (y, como veremos, incluso natural) representar los cuatro estados de dos Cbits, como cuatro vectores ortogonales tetradimensionales, formados por los productos tensoriales de dos de tales pares:

$$|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle. \tag{2}$$

Se puede omitir el signo de multiplicación tensorial $\otimes$ y escribir (2) de la forma más compacta, pero equivalente,

$$|0\rangle\,|0\rangle, \quad |0\rangle\,|1\rangle, \quad |1\rangle\,|0\rangle, \quad |1\rangle\,|1\rangle \tag{3}$$

o, más legiblemente,

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle \tag{4}$$

o, aun más compactamente, usando la representación decimal del número binario representado por el par de Cbits

$$|0\rangle_2, \quad |1\rangle_2, \quad |2\rangle_2, \quad |3\rangle_2. \tag{5}$$

El subíndice 2 es necesario en la última forma (5), porque al cambiar de binario a decimal se pierde la información de cuántos Cbits describe el vector,

[3] Esta notación para vectores se atribuye a Dirac, quien los llamó *kets* y traduciremos como *chetes*.

haciendo necesario indicar de alguna otra manera si $|3\rangle$ significa $|11\rangle = |3\rangle_2$ ó $|011\rangle = |3\rangle_3$ ó $|0011\rangle = |3\rangle_4$, etc.

Como se puede apreciar de esta última observación, los estados de *n* Cbits se representan como 2^n vectores en 2^n dimensiones,

$$|v\rangle_n, \quad 0 \le v < 2^n, \tag{6}$$

dados por los *n*-uples productos tensoriales de *n* pares de 2-vectores mutuamente ortogonales.

Así, por ejemplo,

$$|19\rangle_6 = |010011\rangle = |0\rangle\,|1\rangle\,|0\rangle\,|0\rangle\,|1\rangle\,|1\rangle = |0\rangle\otimes|1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|1\rangle\otimes|1\rangle \tag{7}$$

El hecho de que el producto tensorial es una forma conveniente y muy apropiada para representar los estados de multi-Cbits, se hace más claro si expandimos a los vectores que representan a cada Cbit, como vectores columnas:

$$|0\rangle \;\leftrightarrow\; \begin{pmatrix}1\\0\end{pmatrix}, \qquad |1\rangle \;\leftrightarrow\; \begin{pmatrix}0\\1\end{pmatrix} \quad . \tag{8}$$

Los vectores columnas correspondientes a los productos tensoriales son

$$\begin{pmatrix}y_0\\y_1\end{pmatrix}\begin{pmatrix}z_0\\z_1\end{pmatrix} \;\leftrightarrow\; \begin{pmatrix}y_0z_0\\y_0z_1\\y_1z_0\\y_1z_1\end{pmatrix}, \tag{9}$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}\begin{pmatrix} y_0 \\ y_1 \end{pmatrix}\begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \leftrightarrow \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}, \tag{10}$$

etc.

Así, por ejemplo, el vector columna 8-dimensional que representa a $|5\rangle_3$, viene dado por

$$|5\rangle_3 = |101\rangle = |1\rangle|0\rangle|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 2 \\ 0 & 3 \\ 0 & 4 \\ 1 & 5 \\ 0 & 6 \\ 0 & 7 \end{pmatrix} \tag{11}$$

el cual tiene 0 en cada entrada, excepto 1 en la entrada marcada con el número 5 representado por los tres Cbits[4].Esta regla general para el vector columna que representa a $|v\rangle_n$: 1 en la *posición v* y 0 *en las demás*, *es la obvia generalización* a

[4] Se marcan las entradas contando desde arriba hacia abajo contando a partir de 0: 0,1,2,… Los numerales en el extremo derecho en (11), hacen explícita esta marcación.

n Cbits, de la forma de vector columna para un 1-Cbit. Es una consecuencia automática de la notación típica del producto tensorial.

3. Operaciones sobre los Cbits

En Computación Cuántica todas las operaciones sobre los Qbits son reversibles[5], con excepción del proceso llamado "medición" descrito en la sección 6. La medición no juega ningún rol en Computación Clásica (o, tal vez, más precisamente, juega un rol tan trivial que no se reconoce explícitamente como parte del proceso computacional). Puesto que los estados de los Cbits constituyen un subconjunto (minúsculo) de los estados de los Qbits, la reformulación de los bits clásicos y lo que se puede hacer con ellos, sólo necesita considerar las operaciones reversibles sobre los Cbits.

Sólo hay dos operaciones reversibles sobre los Cbits:

(1) No hacer nada (operador identidad **1**):

$$\mathbf{1}|0\rangle = |0\rangle, \quad \mathbf{1}|1\rangle = |1\rangle. \tag{12}$$

(2) Trocar (operador conmutador **X**)

$$\mathbf{X}|0\rangle = |1\rangle, \quad \mathbf{X}|1\rangle = |0\rangle \qquad (\sigma_x). \tag{13}$$

(Se ha indicado entre paréntesis la notación típica de los físicos; los científicos en Computación Cuántica prefieren **X** a σ_v).

[5] Un ejemplo de operación irreversible es Borrar: $|0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow |0\rangle$. Es irreversible porque no podemos reconstruir la entrada a partir de la salida: no tiene inversa.

Se pueden efectuar operaciones reversibles menos triviales, sobre dos Cbits. Por ejemplo, se pueden intercambiar los valores de los bits que ellos representan (operador de intercambio **S**):

$$\mathbf{S}\left|vw\right\rangle = \left|wv\right\rangle . \tag{14}$$

Al manipular tales operaciones con multi-Cbits es conveniente tener una noción compacta de la acción sobre un estado de operaciones de varios Cbits, que actúa sobre uno solo de los Cbits. Se marcan los Cbits con los enteros 0,1,2,… (comenzando con el cero a la derecha) asociado con la potencia de 2 que representa cada Cbit. Así, si v tiene la expansión binaria $v = 8v_3 + 4v_2 + 2v_2 + v_0$, entonces

$$\left|v\right\rangle_4 = \left|v_3 v_2 v_1 v_0\right\rangle = \left|v_3\right\rangle\left|v_2\right\rangle\left|v_1\right\rangle\left|v_0\right\rangle = \left|v_3\right\rangle \otimes \left|v_2\right\rangle \otimes \left|v_1\right\rangle \otimes \left|v_0\right\rangle . \tag{15}$$

Una operación que actúa sólo sobre el Cbit #2 es

$$\mathbf{X}_2 = \mathbf{1} \otimes \mathbf{X} \otimes \mathbf{1} \otimes \mathbf{1}. \tag{16}$$

Obviamente, el subíndice indica cuál de los cuatro Cbits está sujeto a la operación trocar **X**; es más claro que la forma explícita del operador producto tensorial a la derecha de la igualdad. La notación con subíndices es inevitable cuando hay una numerosa cantidad de Cbits involucrados. En consecuencia, de la definición del producto tensorial, según lo deseado,

$$\mathbf{X}_2\left[\left|v_3\right\rangle \otimes \left|v_2\right\rangle \otimes \left|v_1\right\rangle \otimes \left|v_0\right\rangle\right] = \left|v_3\right\rangle \otimes \left[\mathrm{X}\left|v_2\right\rangle\right] \otimes \left|v_1\right\rangle \otimes \left|v_0\right\rangle . \tag{17}$$

Es posible construir operaciones multi-Cbit significativas a partir de operaciones con Cbits simples, aunque formalmente bien definidas, actúan sobre un Cbit individual de una forma que no tiene interpretación clásica significativa. Aquí

hay, por ejemplo, una operación sobre un Cbit, que no tiene significado y que puede utilizarse para construir operaciones multi-Cbits significativas:

$$\mathbf{Z}|0\rangle = |0\rangle, \qquad \mathbf{Z}|1\rangle = -|1\rangle \qquad (\sigma_z). \quad (18)$$

La acción de **Z** sobre el estado $|1\rangle$, multiplicándolo por –1, mientras que, matemáticamente, bien definida en el espacio vectorial 2-dimensional de los 1-Cbits, produce un vector que no tiene significado dentro del contexto de los Cbits. Sólo los dos vectores $|0\rangle$ y $|1\rangle$ tienen significado como los dos estados distinguibles del Cbit usado para representar 0 y 1. Todo el espacio vectorial de los dos estados clásicos está sumamente subutilizado y, de hecho, el uso de todo un espacio 2^n-dimensional, cuando sólo estamos interesados en un simple conjunto de 2^n vectores básicos ortonormales, podría parecer una extravagante exageración conceptual, a excepción hecha de la afable estructura introducida por la representación como vector columna, del producto tensorial. Las únicas operaciones reversibles sobre *n* Cbits, clásicamente significativas, son las $(2^n)!$ diferentes permutaciones de los 2^n vectores básicos.

Sin embargo, una operación no significativa sobre 1-Cbits, como **Z**, puede adquirir significado clásico cuando se usa en conjunción con otras operaciones no significativas en un contexto multi-Cbit. Como ejemplo importante, nótese que la operación sobre 2-Cbits $\frac{1}{2}(\mathbf{1} + \mathbf{Z}_1\mathbf{Z}_0)$ actúa como la identidad sobre los estados de 2-Cbits $|0\rangle|0\rangle$ y $|1\rangle|1\rangle$, mientras que da 0 (otro resultado sin significado clásico) al actuar sobre $|0\rangle|1\rangle$ ó $|1\rangle|0\rangle$. Por otra parte, la operación $\frac{1}{2}(\mathbf{1} - \mathbf{Z}_1\mathbf{Z}_0)$ actúa como la

identidad sobre $|0\rangle|1\rangle$ y $|1\rangle|0\rangle$, mientras que da 0 sobre $|0\rangle|0\rangle$ y $|1\rangle|1\rangle$. Evidentemente, ambos son operadores proyección en todo el espacio vectorial generado por todos los estados básicos de los 2-Cbits.[6] Puesto que la operación $\mathbf{S}_{10}$, que intercambia los valores de Cbits 1 y 0, actúa como la identidad si su estado es $|00\rangle$ ó $|11\rangle$ y como el operador doble-conmutador $\mathbf{X}_1\mathbf{X}_0$ si su estado es $|01\rangle$ ó $|10\rangle$, se tiene la siguiente representación del operador $\mathbf{S}_{10}$:

$$\mathbf{S}_{10} = \frac{1}{2}(\mathbf{1} + \mathbf{Z}_1\mathbf{Z}_0) + \mathbf{X}_1\mathbf{X}_0\frac{1}{2}(\mathbf{1} - \mathbf{Z}_1\mathbf{Z}_0) \tag{19}$$

ó[7]

$$\mathbf{S}_{10} = \frac{1}{2}(\mathbf{1} + \mathbf{Z}_1\mathbf{Z}_0 + \mathbf{X}_1\mathbf{X}_0 - \mathbf{Y}_1\mathbf{Y}_0) \tag{20}$$

donde

$$\mathbf{Y} \quad = \mathbf{XZ} \qquad\qquad (-i\sigma_y) \tag{21}$$

Aquí vale hacer una digresión para hacer notar a los Físicos que esta derivación "clásica" del operador de intercambio es mucho más simple y clara que la derivación mecánico-cuántica típica que apela a la teoría del momento angular en toda su extensión.

---

[6] Más precisamente, los operadores proyección son las extensiones lineales a todo el espacio, a partir de la base sobre la cual están definidos. Muy generalmente, cualquier operación cuya acción está definida sólo sobre los estados básicos clásicos, se puede identificar con su extensión lineal a todo el espacio vectorial.

[7] Nótese que los operadores de 1-Qbits que actúan sobre diferentes Qbits (como $\mathbf{X}_1$ y $\mathbf{Z}_0$) conmutan aunque los operadores de 1-Qbits ($\mathbf{X}$ y $\mathbf{Z}$) no conmuten cuando actúan sobre el mismo Qbit.

Otro importante ejemplo de operación sobre 2-Cbits es la negación controlada (controlled-NOT) u opción exclusiva reversible (reversible XOR):

$$\mathbf{C}_{10}|v\rangle\,|w\rangle = (\mathbf{X}_0)^v|v\rangle\,|w\rangle = |v\rangle\,|v\oplus w\rangle \tag{22}$$

(donde $\oplus$ denota la adición módulo 2) la cual troca al Cbit 0 (el Cbit *destino*) si y sólo si el Cbit 1 (el Cbit *control*) tiene el valor 1. Podemos construir esta operación a partir de proyecciones de 1-Qbits:

$$\mathbf{C}_{10} = \tfrac{1}{2}(\mathbf{1} + \mathbf{Z}_1) + \mathbf{X}_0\tfrac{1}{2}(\mathbf{1} - \mathbf{Z}_1) = \tfrac{1}{2}(\mathbf{1} + \mathbf{Z}_1 - \mathbf{X}_0\,\mathbf{Z}_1). \tag{23}$$

De esta manera se puede apreciar una curiosa simetría: el intercambio de las operaciones **X** y **Z** tiene el efecto de intercambiar los roles de los Cbits destino y control, convirtiendo $\mathbf{C}_{10}$ en $\mathbf{C}_{01}$.

Una operación clásicamente sin significado, que se puede usar para realizar este intercambio es la transformación *Hadamard*

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{24}$$

Esta lleva los estados de Cbits $|0\rangle$ y $|1\rangle$ a las dos, clásicamente sin significado, combinaciones lineales $\frac{1}{2}(|0\rangle \pm |1\rangle)$. Puesto que

$$\mathbf{X}^2 = \mathbf{Z}^2 = \mathbf{1}, \quad \mathbf{X}\,\mathbf{Z} = -\,\mathbf{Z}\,\mathbf{X}, \tag{25}$$

se tiene que

$$\mathbf{H}^2 = \tfrac{1}{2}(\mathbf{X} + \mathbf{Z})^2 = \mathbf{1}, \quad \mathbf{H}\,\mathbf{X} = (\mathbf{X} + \mathbf{Z})\,\mathbf{X} = \mathbf{Z}\,(\mathbf{X} + \mathbf{Z}) = \mathbf{Z}\,\mathbf{H}, \tag{26}$$

y, por tanto,

$$\mathbf{H}\,\mathbf{X}\,\mathbf{H} = \mathbf{Z}, \quad \mathbf{H}\,\mathbf{Z}\,\mathbf{H} = \mathbf{X} \tag{27}$$

Consecuentemente, se pueden usar cuatro operaciones **H**, clásicamente sin significado, para realizar una operación clásicamente significativa: intercambiar los roles de los Cbits control y destino:

$$\mathbf{C}_{01} = (\mathbf{H}_1\ \mathbf{H}_0)\ \mathbf{C}_{10}\ (\mathbf{H}_1\ \mathbf{H}_0).$$

4. Bits Cuánticos

Hemos representado los estados de *n* Cbits como una base de 2^n vectores ortonormales en un espacio vectorial 2^n–dimensional, construido como el *n*–uple producto tensorial de *n* espacios vectoriales 2–dimensionales. Mientras que las únicas operaciones clásicamente significativas, sobre estos espacios vectoriales consisten de las permutaciones de estos vectores básicos clásicos, hemos podido construir tales operaciones o descubrir relaciones entre ellas, mediante operaciones clásicamente no significativas que multiplican vectores básicos por escalares (en particular, 0 ó –1) ó (como la transformación Hadamard (24)) los operan en combinaciones lineales no triviales.[8]

Uno tiene en mente a la aritmética antes de la introducción de $\sqrt{-1}$. Al introducir el número no significativo *i* se pueden lograr grandes simplificaciones entre ciertas relaciones referidas solamente, a "significativos" números reales. El siguiente paso notable es declarar la insignificancia como significativa, aprovechar completamente, las ventajas del sistema de numeración ampliado.

Una gran parte de la Mecánica Cuántica consiste de una expansión análoga, de la noción de estado de un Cbit, llamada en este marco expandido un *bit cuántico* ó

Qbit. Participativamente, extendemos el conjunto de los estados significativos desde el conjunto de los 2^n estados ortonormales especiales, conocidos en este más amplio sentido como la *base clásica* (ó, en la prevaleciente, pero menos informativa terminología: *base computacional*), hasta los vectores unitarios arbitrarios de todo el espacio consistente de las combinaciones lineales (llamadas *superposiciones*) de los estados básicos clásicos, con coeficientes complejos (llamados *amplitudes*).

Así, el estado general de un simple Qbit es una superposición de los dos estados básicos clásicos

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{28}$$

donde las amplitudes α y β son números complejos restringidos sólo por la condición de normalización

$$|\alpha|^2 + |\beta|^2 = 1. \tag{29}$$

El estado general de *n* Qbits tiene la forma

$$|\Psi\rangle = \left| \sum_{0 \le v < 2^n} \alpha_v |v\rangle_n \right\rangle \tag{30}$$

con amplitudes complejas restringidas sólo por la condición de normalización

---

[8] Una de tales construcciones, la forma (20) del operador de intercambio, que alcanzaría una forma aun más agradable sería introducir $\sqrt{-1}$, reemplazando **Y** con i**Y**. Esto también restauraría otra simetría ya que $\mathbf{X} = \sigma_x$, $i\mathbf{Y} = \sigma_y$ y $\mathbf{Z} = \sigma_z$, son hermitianos.

$$\sum_{0\le v<2^n} \left|\alpha_v\right|^2 = 1. \tag{31}$$

La física ofrece muchos ejemplos de sistemas físicos, Qbits, cuya descripción natural se da en términos de estados que son, precisamente, estas peculiares generalizaciones de los estados de los bits clásicos que expanden el restringido conjunto de los vectores básicos clásicos a todo el espacio vectorial complejo que ellos generan.[9]

En un momento volveremos a las consecuencias de que un conjunto de Qbits tenga estados no clásicos; pero, lo primero que se debe notar es que al expandir el conjunto de los estados de los vectores básicos clásicos al de vectores unitarios arbitrarios en todo el espacio generado por la base clásica, ya hemos introducido una de las más profundas diferencias entre los Cbits y los Qbits:

El estado más general posible de dos Cbits tiene la forma

$$\left|\Psi\right\rangle = \left|v_1\right\rangle\left|w_0\right\rangle. \tag{32}$$

Éste se puede describir como un estado en el cual el Cbit #1 tiene el estado $\left|v_1\right\rangle$ y el Cbit #0, el estado $\left|w_0\right\rangle$: *cada Cbit individual tiene su propio estado*. Por otra parte, el más general estado posible de dos Qbits tiene la forma

$$\left|\Psi\right\rangle = \alpha_3\left|3\right\rangle_2 + \alpha_2\left|2\right\rangle_2 + \alpha_1\left|1\right\rangle_2 + \alpha_0\left|0\right\rangle_2$$

[9] Los más elementales ejemplos físicos son los estados de polarización de un fotón o los estados de espín de una partícula de espín ½. Para comprender los algoritmos cuanto-computacionales no es más importante conocer la física detallada de tales sistemas, que lo que lo es conocer la física detallada de los transistores para comprender los algoritmos de computación clásica.

$$= \alpha_3 |1\rangle |1\rangle + \alpha_2 |1\rangle |0\rangle + \alpha_1 |0\rangle |1\rangle + \alpha_0 |0\rangle |0\rangle . \qquad (33)$$

Si cada Qbit tiene un estado propio, este estado de un 2–Qbit sería, bajo la obvia generalización de la regla para los estados de multi–Cbits, el producto tensorial de esos dos estados de 1–Qbits. Así, el estado del 2–Qbit tendría la forma general

$$|\psi\rangle |\phi\rangle = (\alpha|1\rangle + \beta|0\rangle)(\gamma|1\rangle + \delta|0\rangle)$$

$$= \alpha\gamma|1\rangle|1\rangle + \alpha\delta|1\rangle|0\rangle + \beta\gamma|0\rangle|1\rangle + \beta\delta|0\rangle|0\rangle . \qquad (34)$$

Pero, el estado $|\Psi\rangle$ en (33) no puede tener esta forma, a menos que sea $\alpha_3 \alpha_0 = \alpha_2 \alpha_1$.

Así, en un estado de multi–Qbit general ningún Qbit tiene un estado propio. Ésta es la principal diferencia de los Qbits con los Cbits.

Los estados de *n* Qbits en los cuales ningún subconjunto de menos que *n*, tiene estados propios, se llaman *enmarañados*. Los estados genéricos de los n-Qbits son enmarañados. Las amplitudes en la expansión (30) deben satisfacer restricciones especiales para que el estado sea un producto tensorial de estados asociado con menos de *n* Qbits.

5. Operaciones sobre los Qbits

Los algoritmos cuánticos se constituyen de operaciones que actúan linealmente sobre el estado de los *n*–Qbits, preservando la condición de normalización (31). Los operadores lineales que preservan la norma, sobre un espacio vectorial complejo, son los operadores *unitarios*. Así que los ingredientes básicos de un algoritmo cuántico son los operadores unitarios sobre el espacio complejo 2^n–dimensional:

$$|\Psi\rangle \rightarrow \mathbf{U}|\Psi\rangle, \quad \mathbf{U} \text{ unitario.} \tag{35}$$

Las operaciones clásicas,[10] permutaciones de los 2^n vectores básicos clásicos, son casos especiales de tales operadores.

El problema de la realización física de tales transformaciones unitarias es una cuestión que atañe a la ingeniería computacional cuántica así como la cuestión de cómo producir permutaciones de los valores de una colección de Cbits es un asunto que atañe a la ingeniería computacional clásica. Sin embargo, todo lo que necesita saber el diseñador de programatura computacional cuántica, es que las transformaciones unitarias constituyen todo el cuerpo de operaciones disponibles (salvo las mediciones, descritas en la Sección 6). Por razones prácticas — los diseñadores de programatura deben estar dispuestos a considerar los apremios sugeridos por sentidos prácticos de la ingeniería — el conjunto disponible de transformaciones unitarias, usualmente, está restringido a aquellas que se pueden obtener a partir de productos de transformaciones unitarias cada una de las cuales actúa sólo sobre Qbits individuales o sólo sobre pares de Qbits y una parte importante de la heurística en la programación cuántica está dedicada a mejorar la obtención de más interesantes transformaciones como productos de estas unidades básicas. Así que, si consideramos a los 2^n estados de n bits clásicos como los 2^n vectores básicos ortonormales $|v\rangle_n$ en un espacio vectorial 2^n–dimensional y a las operaciones reversibles que podemos realizar sobre los Cbits, simplemente, como las permutaciones de estos vectores básicos, entonces la generalización a n bits cuánticos es extremadamente simple: *los estados de los Qbits consisten en todas*

[10] Más precisamente, sus extensiones lineales desde la base sobre la cual están definidas, a todo el espacio.

las combinaciones lineales complejas, normalizadas de los vectores básicos clásicos y las operaciones reversibles que podemos realizar sobre los Qbits consisten en las transformaciones unitarias. Los estados clásicos y las operaciones clásicas son muy pequeños subconjuntos de los estados y de las operaciones cuánticas.

Pareciera como que si la extensión de los Cbits a los Qbits abriera un, enormemente, más rico panorama de posibilidades computacionales. Mientras que el estado de un Cbit queda especificado por un solo bit de información, la especificación del estado de un Qbit requiere una cantidad infinita de información: dos números complejos restringidos sólo por la condición de normalización (29) y, en vez de estar limitado a barajar una colección finita de estados de Cbits mediante la permutación, uno puede actuar sobre los Qbits con una colección continua de transformaciones unitarias. Puesto que no es una cuestión más compleja preparar un estado dado para los Qbits que para los Cbits y puesto que no es una cuestión más compleja implantar una amplia gama de transformaciones unitarias sobre los Qbits que implantar permutaciones sobre los Cbits, la extensión de Cbits a Qbits parecería traernos a un nuevo nivel de potencia computacional.

¡Pero hay una reserva! Los Qbits adolecen de una limitación importante que no afecta a los Cbits. Aunque sus estados contienen grandes cantidades de información, dados *n* Qbits

en un cierto estado $|\Psi\rangle$, no hay nada que se pueda hacer a los Qbits que nos permita saber lo que es $|\Psi\rangle$. Por tanto, no hay cómo extraer algo parecido a la enorme cantidad de información contenida en las amplitudes α_v.

¿Para que sirven entonces, los Qbits? ¿Cómo podemos explotar su mayor flexibilidad, para hacer algo útil?

6. Mediciones: cómo extraer información de los Qbits.

A. La Regla Born

Las muy limitadas posibilidades de extraer información es la segunda más importante diferencia entre los Qbits y los Cbits. Si tenemos *n* Cbits en el estado clásico general $|v\rangle_n$, no es problemático saber, conociendo el número *v*, lo que significa el estado. De hecho, es tan directo que el acto de conocer el estado, incluso, no se considera generalmente como parte formal de la computación. Uno mira simplemente lo observa (en una pantalla o un impreso). El estado de los Cbits permanece inalterado por esta adquisición de la información. Una vez que la computadora deja de operar sobre los Cbits, su estado sigue siendo $|v\rangle_n$ aunque nadie se ocupe de comprobar el valor particular de *v*.

Las cosas no podían ser diferentes para los Qbits. Si uno tiene *n* Qbits en el estado

$$|\Psi\rangle_n = \sum_v \alpha_v |v\rangle_n , \tag{36}$$

no hay que nada uno puede hacerles para conocer los valores de las amplitudes α_v. Hay solamente una forma de extraer información de los Qbits: *medirlos*. Medir n-qubits consiste en acoplarlos a un dispositivo que produzca (en una pantalla o un impreso) un número entero v en la gama $0 \leq v < 2^n$. El único acoplamiento entre el estado $|\Psi\rangle$ que uno puede haber impuesto a los Qbits y el valor de *x* revelado por la medición es este: *la probabilidad de conseguir el resultado x es* $p_v = |\alpha_v|^2$,

donde α_v *es la amplitud de* $|v\rangle_n$ *en la expansión (*36) *de* $|\Psi\rangle_n$.[11] Esto se conoce como la *regla Born* en conmemoración del físico Max Born.

Se podría pensar que repitiendo las mediciones, se podrían lograr unas buenas estadísticas de la distribución de las magnitudes $|\alpha_v|$; pero, esta posibilidad de obtener adicional información acerca de $|\Psi\rangle$, queda eliminada por una segunda cláusula fundamental de la regla Born: _una vez que la medición ha indicado el valor *v*, el estado de los n Qbits ya no es $|\Psi\rangle_n$, sino $|v\rangle_n$. El estado de postmedición no contiene trazas de la información presente en el estado de premedición $|\Psi\rangle$ y no es nada más que el estado clásico asociado con el valor de *x* indicado por el dispositivo de medición.

A los físicos, en una nomenclatura que se presta a mala interpretación, les gusta decir que el estado $|\Psi\rangle_n$ se contrae o reduce por la medición, al estado $|v\rangle_n$.

La manera conservadora de ponerlo es, simplemente, indicar la relación entre los estados inmediatamente antes e inmediatamente después de la medición, de una manera que no sugiere ningún mecanismo para el cambio del estado, no confiere ningún estado objetivo a ello, y no hace ninguna referencia a lo que (si acaso) implica un cambio en estado sobre lo que (si acaso) ha sucedido a los Qbits mismos.

Cabría preguntarse cómo puede uno percibir algo de interés computacional bajo estas infortunadas condiciones. El truco general consiste en producir mediante

[11] La condición de que los estados sean vectores unitarios es, por tanto, la condición de que la suma de las probabilidades de todos los resultados de las mediciones, sea 1.

una, astutamente, elaborada transformación unitaria, una superposición (36) en la cual la mayoría de las amplitudes α_v sean cero o muy cerca de cero, con la información útil portada por cualesquiera de los valores de *v* que tienen una probabilidad significativa de ser indicado por la medición. También es importante buscar información que, una vez obtenida, puede ser confirmada fácilmente (e. g. los factores de un número grande) de modo que uno no se confunda por el ocasionalmente irrelevante, resultado de baja probabilidad.

Obviamente, la acción de una medición, sobre el estado de *n* Qbits, es irreversible: todo estado Ψ_n con amplitud distinta de cero se convierte estado $|v\rangle_n$ después de una medición. No hay forma de reconstruir la entrada a partir de la salida. Sin embargo, la medición es la única operación irreversible sobre los Qbits. Todas las otras operaciones son unitarias.

La regla Born tiene, como caso especial, el carácter no problemático de extraer información de los Cbits. Si el estado $|\Psi\rangle$ de *n* Qbits, resulta ser uno de los 2^n estados $\left|v_0\right\rangle_n$ de la base clásica, entonces $\alpha_v = 0$, $v \neq v_0$ y $\alpha_{v_0} = 1$. Así, el resultado de la medición de los Qbits es v_0 con probabilidad 1. La segunda cláusula de la regla Born requiere, entonces, que después de la medición el estado de los Qbits es $\left|v_0\right\rangle_n$, i. e. el estado post-medición sigue siendo lo que era antes de la medición. El carácter estadístico, perturbador del estado, del resultado de una medición de *n* Qbits en un estado general, se convierte en la determinística, conservadora del estado y no problemática, clásica extracción de información, cuando el estado es uno de los 2^n estados clásicos.

Una acotación técnica para los físicos: en esta aproximación a la Mecánica Cuántica, conviene restringir el término "medición" a lo que un más amplio y convencional uso del término caracterizaría como "medición en la base clásica". Puesto que la medición en cualquier otra base se puede lograr aplicando una transformación unitaria apropiada, una que ponga la base en cuestión en términos de la base clásica, seguida por la medición en la base clásica, esta restricción no impide ninguna de las posibilidades más generales.

B. GENERALIZACIÓN DE LA REGLA BORN, PARA MEDICIONES PARCIALES

Hay una generalización de la regla Born, no, a menudo, explícitamente reconocida en los textos de Mecánica Cuántica, que se presenta frecuentemente en Computación Cuántica. Esto sucede sólo cuando se miden algunos de los Qbits. Supóngase que se tienen $m + n$ Qbits y decidimos medir sólo m de ellos. Representando al número z de $m + n$ bits, como v,w, la concatenación de las cadenas binarias de m y n bits, que representan a v y w, podemos escribir el estado de los Qbits $m + n$, como

$$|\Psi\rangle_{m+n} = \sum_{v,w} \alpha_{v,w} |v,w\rangle_{m+n}. \tag{37}$$

Supóngase que decidimos medir sólo los m Qbits de la izquierda.[12] La regla Born generalizada establece que la medición indicará v, $0 \le v < 2^m$, con probabilidad

$$p_v = \sum_{0 \le w < 2^m} |\alpha_{v,w}|^2 \tag{38}$$

[12] Aunque sólo consideramos los m Qbits de la izquierda para ser medidos, la regla para el caso más general es la obvia generalización de la enunciada abajo.

y que después de que se ha indicado el valor de v, el estado de los $m + n$ Qbits cambia de $|\Psi\rangle_{m+n}$ a $|v\rangle_m |\Phi_v\rangle_n$, donde

$$|\Phi_v\rangle_n = p_v^{-1/2} \sum_w \alpha_{v,w} |w\rangle_n . \tag{39}$$

Si se efectúa una medición de los m Qbits a la izquierda, seguida inmediatamente de una medición de los restantes n Qbits a la derecha, esto debería ser equivalente a efectuar directamente, una medición de los $m + n$ Qbits. Y, en efecto, si se aplica la regla Born generalizada dos veces: primero a la medición de los m Qbits a la izquierda y luego a la medición de los restantes n a la derecha. Así se recupera la regla Born ordinaria.

Aunque la regla Born generalizada no es consecuencia directa de la regla Born, es equivalente a la regla Born ordinaria si se le añaden dos condiciones muy razonables:

(1) Supóngase que entre los tiempos t y t' ninguna transformación unitaria actúa sobre los m Qbits de la izquierda, pero sobre los n Qbits de la derecha sí pueden actuar transformaciones unitarias arbitrarias; i. e. que las únicas transformaciones unitarias que actúan sobre los $m + n$ Qbits, entre t y t', son de la forma $\mathbf{U} = \mathbf{1}_m \otimes \mathbf{V}_n$. Entonces la distribución estadística de los resultados, si todos los $m + n$ Qbits se miden al tiempo t', permanece igual que si se hubieran medido los m Qbits de la izquierda, en un tiempo previo, entre t y t'. Informalmente, una vez que la computadora cese la acción adicional sobre cualquier conjunto de Qbits, no hay que esperar hasta el final de la computación para de medir esos Qbits.

(2) Para un conjunto de n Qbits, estar en el estado $|\Phi\rangle$ significa, nada más (o menos) que si los Qbits se miden después de la aplicación de una

transformación unitaria arbitraria **V**, entonces la distribución de los resultados de la medición, será la especificada por la regla Born para *n* Qbits en el estado $\mathbf{V}\left|\Phi\right\rangle$.

En la tabla siguiente se destacan los más importantes principios formulados en las secciones 2 – 6, resumiendo las características relevantes de los Qbits en contraste con características análogas de los Cbits. En la tabla se ha introducido el término "Bit" (con B mayúscula) para significar "Qbit o Cbit" (en contraste con "bit", con b minúscula, que significa "0 ó 1").

BITS CLÁSICOS vs. BITS CUÁNTICOS		
	Cbits	**Qbits**
Estados de *n* Bits	$\left\|v\right\rangle_n$, $0 \le v < 2^n$	$\sum \alpha_v \left\|v\right\rangle_n$, $\sum \|\alpha_v\|^2 = 1$
Subconjuntos de *n* Bits	Siempre con estados definidos	Generalmente, sin estados definidos
Operaciones reversibles sobre los estados	Permutaciones	Transformaciones unitarias
¿Se puede conocer el estado a partir de los Bits?	Si	No
Para obtener información a partir de los Bits	Sólo ver	Hacer mediciones
Información adquirida	*v*	*v* con probabilidad $\|\alpha_v\|^2$
Estado después de adquirida la información	El mismo: sigue siendo $\left\|v\right\rangle$	Diferente: ahora $\left\|v\right\rangle$

7. Observaciones cautelares y reflexiones casi filosóficas

A. ADVERTENCIA IMPORTANTE

Es extremadamente importante evitar una muy tentadora malinterpretación, una grosera sobresimplificación, de la superposición cuántica de los estados clásicos, según se ilustra en el siguiente ejemplo:

Un Qbit en el estado $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|\psi\rangle$, no es lo mismo que un Qbit está en el estado $|0\rangle$ ó en el estado $|1\rangle$ con igual probabilidad, aunque en cualquier caso una medición indicará 0 ó 1 con la misma probabilidad. Para ver que los dos casos son intrínsecamente diferentes, supóngase que se aplica una transformación Hadamard $\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z})$ al Qbit justo antes de hacer la medición. Puesto que

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{40}$$

En el segundo caso, si el estado inicial es $|0\rangle$ ó es $|v\rangle$, la medición después de la aplicación de **H**, seguirá indicando 0 ó 1 con la misma probabilidad. Pero, en el primer caso, en el que el estado inicial es $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, se tiene $\mathbf{H}|\psi\rangle = |0\rangle$; por tanto, la medición después de la aplicación de **H**, debe ser necesariamente, 0.

Un Qbit en una superposición de estados de la base clásica es completamente diferente de un Qbit que está en uno de esos estados clásicos con una probabilidad dada por el cuadrado del módulo de la amplitud correspondiente. Las superposiciones no tienen interpretación clásica. Ellas son *sui generis*, una construcción intrínsecamente mecánico-cuántica, cuyo significado se deriva sólo de las reglas que caracterizan a las operaciones reversibles (unitarias) que se puedan

realizar sobre ellos y de los medios disponibles (mediciones) para extraer información de ellos.

B. SIGNIFICADO DEL ESTADO CUÁNTICO

Se ha estado discutiendo sobre el significado del estado cuántico desde que el concepto apareció por primera vez, sin que haya indicios de un acercamiento a un consenso. Estas cuestiones conceptuales son poco importantes para una comprensión de la Computación Cuántica, que sólo requiere que se conozca como se elaboran los estados a partir de otros estados (mediante apropiadas transformaciones unitarias) y cómo se puede extraer información de los Qbits en un estado dado (mediante mediciones, de acuerdo con las reglas Born).

El estado inicial sobre el cual operan las transformaciones unitarias es generalmente, un estado $|v\rangle_n$ de la base clásica. Tal estado se puede identificar inequívocamente como el estado post-medición de n Qbits después de una medición que indicó el valor v. Desde este punto de vista, el proceso computacional comienza y termina con una medición y todo el papel del estado de los Qbits en cualquier etapa de una secuencia de transformaciones unitarias, es encapsular la probabilidad de los resultados si la medición final se hace en esa etapa del proceso o permitir calcular las probabilidades del resultado si unitario las transformaciones se apliquen antes de la medición.

La noción que el estado de n Qbits es simplemente un instrumento matemático compacto conveniente para calcular las correlaciones entre los resultados de dos mediciones sobre esos Qbits, entre las cuales se pudo haber aplicado una transformación unitaria arbitraria, se asocia a menudo con la constelación de ideas sobre los Mecánica Cuántica llamada la interpretación

Copenhague. Debe contrastarse con la noción que el estado de n Qbits es una característica física objetiva de esos Qbits, en el mismo sentido fuerte que podemos considerar el estado de n Cbits, el valor único v que representan, como característica objetiva de esos Cbits. Quienes consideran al estado cuántico como objetivo en este sentido, tienden a quejarse acerca del hecho de que hay dos maneras absolutamente diferentes, de las cuales pueden cambiar los Qbits: determinística y continuamente vía transformaciones unitarias (si se elabora cada transformación unitaria a partir de muchas infinitesimales) y estadística y discontinuamente vía mediciones. Esta dicotomía pierde su contenido si se substituye "Qbits" por "el estado de los Qbits" y se reconoce que el estado no es nada más que un catálogo de cómo diferentes transformaciones unitarias darán lugar a diferentes distribuciones de los resultados de las mediciones; estados básicos clásicos que solamente se pueden ver como objetivos.

Otra trampa de considerar su estado como una propiedad objetiva de los Qbits, es que se puede sucumbir a la tentación de creer que la aplicación de un conjunto de transformaciones unitarias a los Qbits instrumenta una computación física de todas las amplitudes resultantes α_v. La pista de que esto no se ha logrado se apoya en el hecho, antes señalado, de que, dados los Qbits, no hay nada que se pueda hacer con ellos para revelar los valores de esas amplitudes.

Hay sin embargo, quienes creen que todas las amplitudes α_v han adquirido el estado de cantidades físicas objetivas, con todo lo inaccesible que esas cantidades puedan ser. Tal gente entonces, se pregunta cómo habría podido ser físicamente instrumentado ese número extenso de cálculos de alta precisión (10^{30} amplitudes diferentes si se tienen 100 Qbits). A los que hacen tales preguntas, les gusta proporcionar sensacionales, pero fundamentalmente tontas respuestas que implican

números extensos de universos paralelos, invocando un punto de vista conocido como la interpretación de los *múltiples mundos* de la Mecánica Cuántica. Se podría decir que, con lo imaginativa que esta visión pueda parecer, es sintomática de una carencia de una clase mucho más sutil de imaginación, que puede captar la exquisita distinción entre los estados cuánticos y las propiedades físicas objetivas que la Física Cuántica nos ha impuesto.

C. ¿QUÉ SE HIZO LA CONSTANTE PLANK?

Algunos físicos pueden estar perturbados al ver terminar que lo que pretende ser una exposición de Mecánica Cuántica — de hecho, de Mecánica Cuántica aplicada (bien, *sesudamente* aplicada) — sin recurrir, para nada a la constante de Planck. ¿Cómo puede ser esto?

La respuesta se remonta a la razón dada al principio, por la que la Mecánica Cuántica suficiente para comprender Computación Cuántica, se puede enseñar en sólo cuatro a cinco horas. Estamos interesados en sistemas discretos (2-estados) y transformaciones discretas (unitarias). Pero la constante de Planck aparece solamente en el contexto de los sistemas continuamente infinitos (estados propios de posición) y de las familias continuas de transformaciones (desarrollo en el tiempo) que actúan sobre ellos. Su papel es relacionar las unidades convencionales en las cuales medimos el espacio y el tiempo, con las unidades en las cuales es mecánico–cuánticamente natural considerar los generadores de las transformaciones unitarias que producen translaciones en el espacio o el tiempo.

Si no estamos interesados en la localización en espacio continuo y sólo estamos interesados en transformaciones unitarias globales en vez de

infinitesimales, entonces $\hbar$ no tiene por qué entrar en el cuento. El ingeniero, que debe calcular cómo instrumentar transformaciones unitarias que actúen en un cierto plazo sobre los Qbits localizados en diferentes regiones del espacio físico, debe ocuparse de hecho, de $\hbar$ y de los Hamiltonianos que generan las transformaciones unitarias a partir de las cuales se elabora la computación. Pero, el diseñador de algoritmos para la máquina terminada sólo necesita tratar con las transformaciones unitarias resultantes, de las cuales $\hbar$ ha desaparecido como consecuencia, por ejemplo, de opciones juiciosas de los ingenieros, de los plazos sobre los cuales actúan las interacciones que producen las transformaciones unitarias.

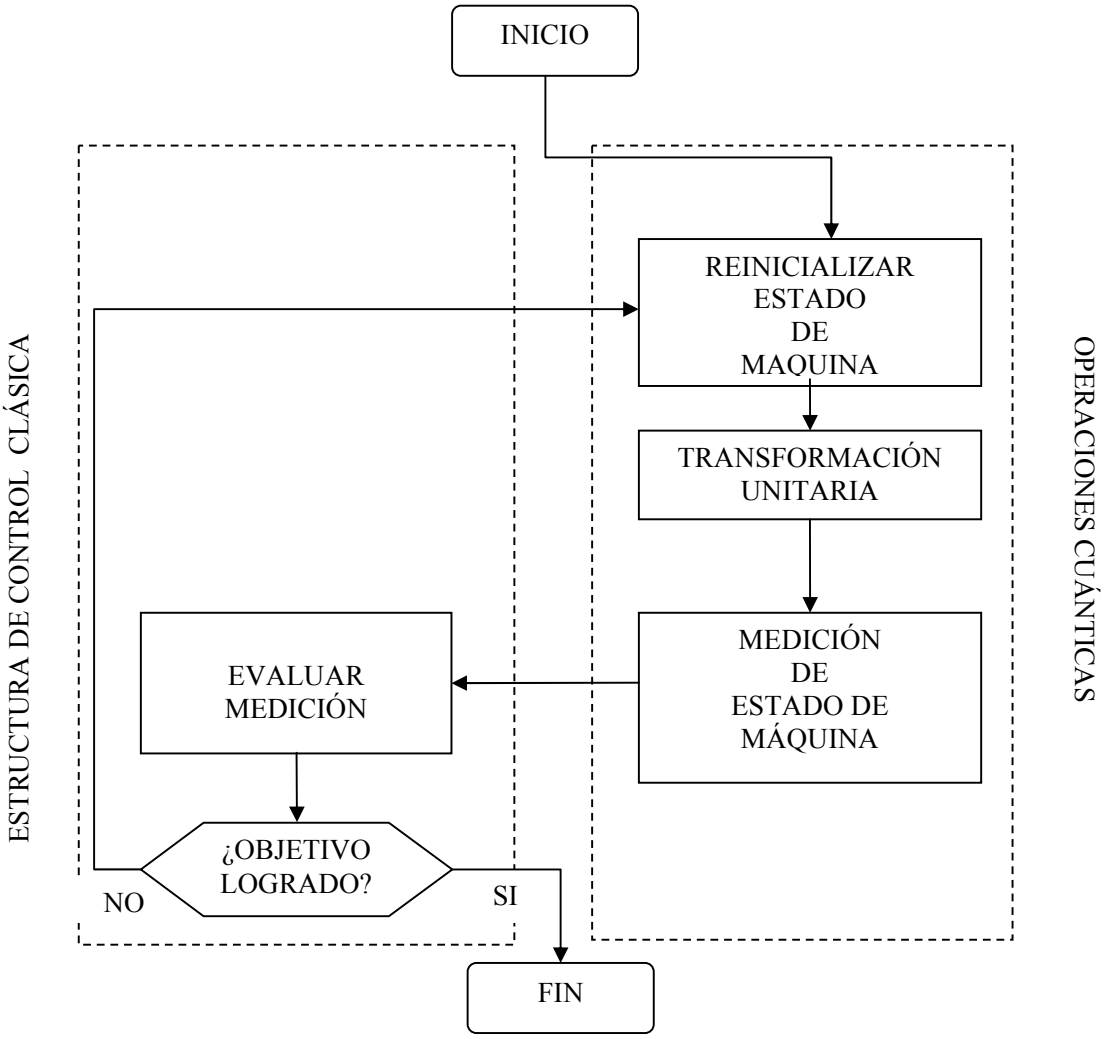
Deplorar la ausencia de $\hbar$ de exposiciones de la informática cuántica es algo como quejarse de que la curva *I*-*V* para una ensambladura *p* - *n* no aparece en las exposiciones de la informática clásica. Es confundir la *informática* con la *ingeniería* de computadoras.

8. Eso es todo lo que se necesita saber

Armado con los contenidos de las secciones ***2 – 6***, ya se está listo para embarcarse en la exposición de la Informática Cuántica. Para estar seguro, habrá oportunidades en las que será conveniente expandir el formalismo mínimo anteriormente desarrollado. Pero, tales expansiones, por ejemplo la introducción de los *cors* — traducción de *bras* — (como funcionales lineales sobre los chetes), la introducción de las matrices de densidad o la útil conexión entre **X**, **Y** y **Z** y el grupo de rotaciones 3–dimensionales, son todas refinamientos matemáticos técnicos dentro de la estructura básica del espacio vectorial complejo de los Qbits. No requieren ningún nuevo principio físico para su desarrollo. Las secciones ***2 – 6***, proporcionan toda la Mecánica Cuántica que se necesita para desarrollar

completamente, el algoritmo de factorización de Peter Shor, el algoritmo de búsqueda de Lov Grover y sus posteriores generalizaciones. Solamente, para desarrollar el tema muy importante de la corrección del error cuántico, se hace necesario introducir una nueva hipótesis física: que el formalismo desarrollado para describir a los Qbits, estados cuánticos, transformaciones unitarias, reglas Born, describe, no sólo a los Qbits, sino a cualquier cosa en el mundo con la que ellos puedan interactuar.

Una exposición detallada de cómo erigir el edificio de la Computación Cuántica sobre esta fundamentación se puede hallar los en capítulos 2-5 de Ref. 1. El capítulo 6 describe algunos otros asuntos en un área más amplia de la informática Cuántica que se pueden elaborar con esta misma fundamentación.



ALGORITMO SIMPLE NO CLASICO