Tesla cantaba Kumbaya alrededor de su bobina

Arias E., Sagasti A.

26 de junio de 2014

Parte I
Conceptos Fundamentales

En este capítulo vamos a desarrollar las bases necesarias para poder llegar a un pleno entendimiento de la investigación. Es una especie de marco teórico donde se abarcará la terminología básica de ciertos conceptos matemáticos y computacionales tratados en los siguientes capítulos. No debe entenderse como un glosario o un capítulo de definiciones sino que, este es el comienzo de la investigación en su etapa más básica.

Conceptos matemáticos

Para poder comprender mejor los postulados de la Teoría Cuántica es necesario tener un conocimiento básico de álgebra lineal, específicamente sobre espacios vectoriales. Asumimos que el lector posee conocimientos sobre este tema, sin embargo vamos a hacer un pequeño repaso en conceptos fundamentales. Shankar (1994) define los espacios vectoriales como:

> *Un espacio vectorial lineal* $\mathbb{V}$ *es una colección de objetos* $|1\rangle, |2\rangle, ..., |V\rangle, ..., |W\rangle, ...,$ llamados vectores, para los cuales existe
>
> 1. Una regla definida para realizar la suma de vectores, denotada $|V\rangle + |W\rangle$
> 2. Una regla definida para la multiplicación por escalares *a,b,...,* denotada $a|V\rangle$ con las siguientes características:
>
> - El resultado de estas operaciones resulta en otro elemento del espacio, una característica llamada *cerrado*: $|V\rangle + |W\rangle \in \mathbb{V}$.
> - La multiplicación por escalares es *distributiva en los vectores*: $a(|V\rangle + |W\rangle) = a|V\rangle + a|W\rangle$.
> - La multiplicación por escalares es *distributiva en los escalares*: $(a + b)|V\rangle = a|V\rangle + b|V\rangle$.
> - La multiplicación por escalares es *asociativa*: $a(b|V\rangle) = ab|V\rangle$.
> - La suma es *conmutativa*: $|V\rangle + |W\rangle = |W\rangle + |V\rangle$.
> - La suma es *asociativa*: $|V\rangle + (|W\rangle + |Z\rangle) = (|V\rangle + |W\rangle) + |Z\rangle$.
> - Existe un *vector nulo* $|0\rangle$ que obedece $|V\rangle + |0\rangle = |V\rangle$.
> - Para cada vector $|V\rangle$ existe un *inverso respecto a la suma*, $|-V\rangle$, tal que $|V\rangle + |-V\rangle = |0\rangle$. (p. 2)

Esta notación de vectores $|V\rangle$ llamada *notación Dirac* será muy utilizada más adelante cuando veamos los qubits, los cuales se rigen por las mismas reglas de espacios vectoriales mencionadas anteriormente. Además de estas reglas es necesario que consideremos los conceptos de *campo*, *combinaciones lineales* y *bases ortonormales*.

Es importante que definamos el *campo* de un espacio vectorial. El campo se refiere al espacio donde están definidos los escalares que multiplican al espacio vectorial. Como los vectores no son número en sí, estos no se pueden multiplicar. Entonces, para poder multiplicar vectores necesitamos usar escalar inscritos a un campo. Por ejemplo, un *espacio vectorial real* es un espacio definido por escalares reales. De igual manera tenemos los *espacios vectoriales complejos*, entre otros.

Debemos tener una noción básica de las combinaciones lineales en los espacios vectoriales. Como definición básica encontramos que Arce, Castillo y González (2003) explican que:

> *Sea E un espacio vectorial y* $\{v_1, v_2, ..., v_p\}$*, un conjunto de vectores de E. Se llama combinación lineal de los vectores* $v_1, v_2, ..., v_p$ *al vector*
>
> $$v = a_1v_1 + a_2v_2 + \cdots + a_pv_p$$
>
> *cualquiera sea la elección de los escalares* $a_1, a_2, ..., a_p$*. Y al conjunto*
>
> $$\mathcal{C}\ell = \{v_1, ..., v_p\} = \{a_1v_1, a_2v_2, ..., a_pv_p \mid a_1, a_2, ..., a_p \in \mathbb{R}\}$$
>
> *se le denomina conjunto de combinaciones lineales de* $v_1, v_2, ..., v_p$*.(p. 221)*

Este concepto nos sirve además para comprender qué es una base. Se dice que:

> *Un conjunto de vectores* $\{v_1, v_2, .., v_k\}$ *de un espacio vectorial E, es una base de este espacio si y solo si todo vector* $v \in E$ *se puede expresar como combinación lineal* ***única*** *de los vectores* $v_1, v_2, .., v_k$*. (Arce et al., 2003, p. 226)*

Finalmente, para comprender el concepto de bases ortonormales necesitamos aclarar una operación de vectores y una característica de los mismos. Estas son el producto punto y la norma. El producto punto se define como:

> *Sean* $\vec{a} = (a_1, a_2, ..., a_n)^t$ *y* $\vec{b} = (b_1, b_2, ..., b_n)^t$*. El producto escalar, o producto punto de* $\vec{a}$ *y* $\vec{b}$ *es un número real denotado y expresado en la siguiente forma:*

$$\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \text{ (Arce et al., 2003, p. 158)}$$

Es decir, si tenemos dos vectores podemos multiplicar las entradas de estos en orden y la suma de estos dará un número real, o complejo dependiendo del campo. Debemos anotar que esta es la notación ordinaria de vectores. En la notación Dirac si tenemos los vectores V y W el producto punto está denotado como $\langle V|W\rangle$. Dos vectores son *ortogonales o perpendiculares* si y solo si $\langle V|W\rangle = 0$. Por otro lado, la norma de un vector, también conocida como magnitud, de una forma generalizada se define por: "$\sqrt{\langle V|V\rangle} \equiv |V|$ (...). Un *vector normal* tiene una norma igual a uno."(Shankar, 1994, p. 9)

Ahora bien, aclarados esto términos podemos definir una *base ortonormal* como: "Un conjunto de vectores base normales, los cuales son ortogonales dos a dos."(Shankar, 1994, p. 9).

Introducción a la Mecánica Cuántica

En cuanto al concepto de Mecánica cuántica no discutiremos a profundidad los postulados que este propone, puesto que eso sería un enorme discusión. Sin embargo, vamos a comparar el primer postulado de la mecánica cuánticacon el primer postulado de la mecánica clásica. El primero afirma que: "El estado de una partícula en algún momento dado está especificado por las variables *x(t)* y *p(t)*, i.e., como un punto en un espacio de dos dimensiones." (Shankar, 1994, p. 115). Mientras que el segundo dice que: "El estado de una partícula está representado por el vector $|\psi(t)\rangle$ en un espacio Hilbert." (Shankar, 1994, p.115)

Con este postulado, podríamos decir que tenemos la base para comprender el concepto de los qubits. Pero en general, qué es la mecánica cuántica. Nielsen y Chuang (2010) la definen como: "(...)un marco matemático o un conjunto de reglas para la construcción de teorías de la física." (p. 2). Nos parece contextualmente comprensible la analogía que plantean estos autores. En esta, comparan la relación que tiene la mecánica cuántica y las teorías que derivan de ella con un sistema operativo y sus aplicaciones de software (p. 2). Como vemos entre ambas relaciones hay una conexión de base, donde el primer concepto sirve de fundamento para que se creen los elementos con los cuales se relacionan.

Incluso yendo más allá de una simple definición y contexto histórico Nielsen y Chuang (2010) se atreven, luego de hacer una línea de tiempo en el desarrollo de la mecánica cuántica a proponerla como un reto para la computación. Ellos exponen los inicios de esta nueva forma de ver la física, que se remontan a las años 20 hasta los hallazgos más destacables que datan desde los años 70 hasta la actualidad. Luego, hace una reflexión acerca de que los intentos por desarrollar nuevos hallazgos científicados, aunque sea por mera corazonada, han dado nacimiento a importantes descubrimientos en la

historia de la humanidad. Es aquí donde ellos recalcan que la computación e informática cuántica caben a la perfección en este esquema de resolver retos propuestos por nuevos esquemas de conocimiento. (pp. 2-3)

Entonces, el desarrollo de la mecánica cuántica en las ciencias de la computación puede representar un inmenso avance en el desarrollo de soluciones para los problemas propios de este ciencia.

Para poner un ejemplo, vamos a retroceder un momento en historia y remontemos sobre los inicios de la computación. Si nos colocamos en los antecedentes de las primeras computadoras electrónicas tenemos el gran aporte de Alan Turing. Turing (1936) propone el concepto de una máquina que es capaz de interpretar un número finito de instrucciones llamadas "m-configurations". Esta máquina será alimentada por una cinta seccionada que va a contener el conjunto de instrucciones que se desean que la máquina interprete y como resultado imprimirá en otra cinta los resultados de las instrucciones que la máquina va a interpretar. (p. 232). Solo para recalcar la importancia del trabajo de Turing, Herken (1998) afirma que: "Es bastante sorprendente ver cómo, en tan sólo diez años después de "Computable Numbers", había traducido sus ideas en una poderosa visión profética del potencial de la tecnología informática" (p. 8)

Pero volviendo a la línea histórica, tenemos el trabajo de Turing que mencionamos que data de 1936, luego tenemos a John Von Neumann. Los aportes que Von Neumann hizo al conocimiento científico en general son muchos y en diversas áreas (incluyendo en la mecánica cuántica) pero ahora nos limitaremos a su trabajo *First Draft of a Report on the EDVAC*. Incluso siendo una borrador incompleto, muestra la arquitectura de la computadora EDVAC. Esta se convirtió en la arquitectura más usada en la creación de nuevas computadoras y como base se ha mantenido hasta la actualidad. Con la invención del transistor en 1947 el desarrollo de nuevo hardware se vió impulsado y esta arquitectura obtuvo mucha más fuerza.

Gracias a los transistores, se comenzó el desarrollo de circuitos integrados. El experto en fisicoquímica Gordon Moore (1965) habla sobre las ventajas y los posibles usos de los circuitos integrados. Inclusive afirma que:

> el futuro de la electrónica integrada es el futuro de la electrónica misma.(...)
>
> La electrónica integrada hará las técnicas electrónicas más accesibles al resto de la sociedad, realizando muchas funciones que en el presente se hacen inadecuadamente o no se hacen del todo. La principal ventaja serán bajos costos y diseños grandemente simplificados—recompensa de un suministro de paquetes funcionales de bajo costo. (pp. 1-2)

Sin embargo, él propone en este artículo una cierta preocupación. Moore (1965) espera que para la siguiente década se duplique el número de compo-

nentes en un circuito integrado. Esta aproximación resulto ser casi apegada a la realidad del futuro tanto que se le dió el nombre de *Ley de Moore*.

Con esto ya expuesto podemos tener una aproximación del futuro en la construcción de computadores a nivel de hardware. El crecimiento acelerado de componentes va a llegar a un punto donde va a ser necesario buscar una solución. Es aquí donde Nielsen y Chuang (2010) proponen como solución buscar nuevos paradigmas computacionales, y uno de estos puede ser fruto de la teoría de la computación cuántica. Los autores hablan sobre computadoras que procesen información usando métodos de mecánica cuántica a velocidad increíblemente rápidas en comparación con los métodos actuales con mecánica clásica. (pp. 4-5) Por tanto, decidimos investigar acerca de estos métodos de computación mediante mecánica cuántica. Como primera instancia, expondremos las unidades básicas y características fundamentales de la computación cuántica.

Parte II
Computación Cuántica (considerar otro nombre menos extenso

Qubits

Los quantum bits, o qubits, son objetos matemáticos que tiene dos posibles estados, $|0\rangle$ y $|1\rangle$. La diferencia entre un qubit y un bit normal es que un qubit puede tener estados adicionales formados por combinaciones lineales de sus estados originales. (Nielsen, 2010, p.13)

Asumiendo que tenemos un espacio vectorial $\mathbb{C}$, podemos afirmar que los vectores $|0\rangle$ y $|1\rangle$ pertenecen a este espacio. En general, si queremos representar un qubit usamos la siguiente fórmula donde $|\psi\rangle$ es un vector que pertenece a $\mathbb{C}$:

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

Los números α y β son números complejos, aunque estos se pueden asumir como números reales. De otra manera, el estado de un qubit es un espacio vectorial complejo de dos dimensiones. Los estados $|0\rangle$ y $|1\rangle$ se conocen como "estados base computacionales" y forman una base ortonormal para este espacio vectorial. (Nielsen, 2010, p.13)

Podemos examinar un bit clásico para ver el valor que éste tiene. Por ejemplo, las computadoras revisan valores de bits constantemente al extraer contenidos de memoria. Sin embargo, no podemos examinar un qubit para determinar el estado en el que está. La mecánica cuántica nos dice que tenemos acceso solamente a información restringida sobre el estado cuántico de un qubit. Cuando medimos un qubit podemos tener dos posibles resultados: 0 con probabilidad α^2 o 1 con probabilidad de β^2. La suma de ambas probabilidades debe dar 1. Geométricamente, podemos interpretar esto como la condición en la cual el estado del qubit se normaliza a 1. En general, el estado de un qubit es un vector unitario en un espacio vectorial complejo de dos dimensiones. (Nielsen, 2010, p.13)

La habilidad de un qubit de estar en un estado superpuesto va en contra del entendimiento clásico del mundo que nos rodea. Un qubit puede existir en un continuo de estados entre $|0\rangle$ y $|1\rangle$ hasta que es observado. Cuando se observa un qubit, su medición es '0' o '1'. (Nielsen, 2010, p.14)

Los qubits son reales, y varios sistemas físicos se pueden utilizar para hacer qubits. Por ejemplo, se pueden realizar con las dos distintas polarizaciones de un fotón, con el alineamiento del espín nuclear en un campo magnético uniforme, como dos estados de un electrón orbitando un átomo. (Nielsen, 2010, p.14)

La representación geométrica de un qubit se puede apreciar en la figura 1.1 Me falta meter la foto hu3hu3hu3. Hay que ponerle el full file path o algo, y prefiero hacerlo al final.

Parte III
Computación Cuántica

Los cambios que le suceden a un estado cuántico se pueden describir usando la computación cuántica. De la misma manera que una computadora clásica está construida con base en circuitos lógicos, una computadora cuántica se basa en circuitos cuánticos con compuertas cuánticas elementales.

Compuertas con un qubit

Consideremos la operación lógica NOT que modifica un bit clásico. Es una operación que no pierde información y es reversible con otro NOT. (Feynman,) Su tabla de verdad está descrita en el Cuadro 1.

Cuadro 1: Tabla de verdad de NOT

x	NOT x
0	1
1	0

Al usar qubits, tener un NOT que cambie de $|0\rangle$ a $|1\rangle$ y viceversa no establece qué sucede en los estados de superposición. El NOT funciona de una manera lineal porque toma el estado $\alpha|0\rangle + \beta|1\rangle$ y lo modifica hasta que los papeles del $|0\rangle$ y $|1\rangle$ estén completamente intercambiados. $\alpha|1\rangle + \beta|0\rangle$. Las compuertas cuánticas NOT se pueden describir en matrices de 2x2 (surge directamente de la linealidad). Supongamos que la X representa una compuerta NOT. $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ Si escribimos el estado cuántico $\alpha|0\rangle + \beta|1\rangle$ en notación vectorial $\begin{bmatrix} \alpha & \beta \end{bmatrix}$ la salida del NOT cuántico es $X \begin{bmatrix} \alpha & \beta \end{bmatrix} = \begin{bmatrix} \beta & \alpha \end{bmatrix}$.

La acción de un NOT es tomar el estado 0 y reemplazarlo por el estado correspondiente a la primera columna de la matriz X. De igual manera el estado 1 es reemplazado por el estado correspondiente a la segunda columna de la matriz X.

Hay dos otras compuertas de un qubit importantes. La primera es la compuerta Z. $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Esta compuerta deja el 0 sin modificar y cambia el signo de 1 a -1.

La segunda es la compuerta Hadamard. $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.

Compuertas con múltiples qubits

CONTROLLED NOT En un CONTROLLED NOT entran dos datos, *a* y *b*, y salen dos datos *a'* y *b'*. *a* es la línea de control: si se activa y *a*=1, entonces *b'* es la negación de *b*. Si *a*=0, entonces *b*=*b'*. La acción de un CONTROLLED NOT es revertida al aplicar un CNOT de nuevo. La salida *b'* es en realidad una función simétrica de *a* y *b* conocida como XOR. Es a la vez la suma módulo dos de *a* y *b*. Se puede utilizar para comparar los valores de *a* y *b* y dar como resultado 1 cuando son diferentes. (Feynman, 1985, p.12)

CONTROLLED CONTROLLED NOT En este caso hay dos líneas de control a y b que modifican a la tercera línea c y le aplican un NOT sólo cuando ambas líneas de control están activadas (a=1 y b=1). Si no, la salida c' se mantiene inmutada. (Feynman, 1985, p.12)

El CNOT y las compuertas de un qubit son los prototipos necesarios para hacer cualquier otro tipo de compuerta (son el NAND de los bits clásicos). (Nielsen, 2010, p.22)

Circuitos cuánticos

¿Podemos simular circuitos con compuertas clásicas usando circuitos cuánticos? La respuesta es sí. Sin embargo, la mayoría de las compuertas cuánticas son reversibles, mientras las compuertas clásicas son irreversibles. (Nielsen, 2010, p.29) Cualquier circuito clásico puede ser reemplazado por uno equivalente construido únicamente con elementos reversibles, utilizando la *compuerta Toffoli*. La compuerta Toffoli tiene tres bits de entrada y tres de salida. Dos de esos bits son de control y no los afecta la acción de la compuerta en sí. El tercero es un bit que es "flippeado", si las dos líneas de control están activadas. Aplicar dos veces la compuerta Toffoli a un bit hace que se revierta al estado original porque su inversa es sí misma. (Nielsen, 2010, p.29) La compuerta Toffoli se puede utilizar para simular compuertas NAND. (Nielsen, 2010, p.29)

Superposición y Entrelazamiento cuántico

El entrelazamiento cuántico es uno de los fenómenos más extraños y sorprendentes de la mecánica cuántica. No es un concepto nuevo, la propuesta del entrelazamiento se remonta hacia los años 30 donde la teoría cuántica comenzaba por desarrollarse. Como es natural esta teoría tenía quiénes la refutaran, entre ellos Einstein.

Pero dejemos un momento a Einstein y definamos básicamente el concepto de entrelazamiento. Para hacerlo de una forma comprendible vamos a referirnos a la analogía propuesta por Aczel (2001). Esta nos propone que

imaginemos que Alice y Bob están casados. Cuando Alice se va de viaje Bob conoce a Carol. Carol está casada con Dave, quién también está fuera de la ciudad. Entonces Bob y Carol se olvidan de sus esposos y se entrelazan profundamente. Por una extraña razón Alice y Dave se encuentran y ellos también se entrelazan sin siquiera saber por qué. Entonces si cambiamos las personas por partículas: A, B, C, D y si sabemos que A y B están entrelazadas al igual que C con D entonces podemos entrelazar A con D por medio de entrelazar a B con C. (p. 2)

Entonces, si dos partículas están entrelazas, no importa cuán lejos estén siempre van a estar unidas. Hay una relación intrínseca entre las dos que no las deja separarse. Evidentemente esto suena absurdo bajo nuestra física clásica. Es en este contexto donde Albert Einstein, Boris Podolski y Nathan Rosen proponen en 1935 una paradoja (llamada paradoja EPR) que viene a criticar a la mecánica cuántica.

Esta paradoja, a grandes rasgos, supone dos partículas P y Q que están entrelazadas. Además propone que si dos individuos observan esa partícula van a tener dos medidas distintas, esto por la naturaleza de una partícula cuántica. Por tanto, concluyen que esta medición no describe la realidad física de la partícula y por consiguiente la teoría cuántica es una teoría incompleta. A(Abala, 2007, pp. 7-11)

Luego de esto, en 1964 John Bell desarrolla una forma con la cual comprobar la paradoja anteriormente descrita. Bell se basa en los principios del determinismo y la localidad para crear unas desigualdades. Si estan son validadas entonces la paradoja se cumple. Gracias a este trabajo varios grupos de investigadores continuaron el análisis del entrelazamiento y en 1972 dos físicos americanos dieron pruebas de la existencia del entrelazamiento. (Aczel, 2001, p. xvi)

Entonces, el entrelazamiento viene a ser una aplicación de un concepto desarrollado en el pasado llamado el *principio de superposición de estados.* Aczel (2001) lo presenta como:

> El principio de superposición dice que un nuevo estado de un sistema puede estar compuesto por dos o más estados, de manera tal que el nuevo estado comparta algunas de las propiedades de los estados combinados. Si A y B atribuyen dos propiedades diferentes a una partícula, como la de estar en dos distintos lados, entonces la *superposición* de estados, escrita como $A + B$, tiene algo en común con el estado A y el estado B. En particular, la partícula tendrá probabilidades distintas de cero de estar en cada uno de los dos estados, pero no en otra parte, si la posición de la partícula es observada. (p. 25)
>
> El entrelazamiento consiste en un sistema formado por dos o más subsistemas. En este caso el subsistema corresponde a una partícula. Veamos entonces qué significa decir que dos partícu-

las están entrelazadas. Supongamos una partícula 1. Esta puede estar en dos estados: A y C. Estos estados manifiestan dos propiedades contradictorias como lo es el estar en dos lugares a la vez. Por otro lado, la partícula 2 puede estar en dos estados: B y D. De igual forma estos dos estados presentar la propiedad contradictoria de estar en dos lugares distintos. El estado AB es un producto de estados. Cuando el sistema completo esta en AB sabemos que la partícula 1 esta en A y la partícula 2 está en B. Analógicamente, con el estado CD. Observemos entonces el estado $AB + CD$. Este estado representa la aplicación del principio de superposición en todo el sistema de dos partículas. Como el principio permite este comportamiento de combinación de estados, el estado $AB+CD$ es llamado un *estado entrelazado*. (Aczel, 2001, p. 26)

Referencias

[1] Autor, A. (año). *Título del libro.* Lugar: Editorial

[2] Abal, G. (2007). *Paradoja EPR y desigualdades de Bell: pruebas experimentales, estado acual del conocimiento.* Montevideo.Recuperado de http://www.fing.edu.uy/ abal/trabajos/tdet.pdf

[3] Aczel, A. (año). *ENTANGLEMENT The Greatest Mystery in Physics.* (E. Arias, Trad.) New York: Four Wall Eight Windows

[4] Arce, C., Castillo, W., González, J. (2003). *Álgebra Lineal.* Lugar: Editorial

[5] Herken, R. (Ed.) (1988). *The Universal Turing Machine. A Half-Century Survey.* (E. Arias, Trad.) Oxford University Press

[6] Moore, G. (1965). Cramming more components onto integrated circuits. *Electronics.* Vol 3., No. 8.

[7] Nielsen, M., Chuang, I. (2010). *Quantum Computation and Quantum Information.* (E. Arias, Trad.) New York: Cambridge University Press

[8] Shankar, R. (1994). *Principles of Quantum Mechanics.* (E. Arias, Trad.) New York: Plenum Press

[9] Turing, A. (1936). *ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM.* (E. Arias, Trad.) Recuperado de http://classes.soe.ucsc.edu/cmps210/Winter11/Papers/turing-1936.pdf

[10] Von Neumann, J. (1945). *First Draft of a Report on the EDVAC* University of Pennsylvania. Recuperado de http://www.virtualtravelog.net/wp/wp-content/media/2003-08-TheFirstDraft.pdf