

Cuántica y computación: Una aproximación desde los postulados de la mecánica cuántica

Andrés Sicard Ramírez,
asicard@eafit.edu.co

Mario E. Vélez Ruiz
mvelez@eafit.edu.co

Universidad EAFIT; Medellín, Colombia

Mayo 30 de 1999

PACS : 03.65. – *w*, 03.67.*Lx*, 89.70. + *c*

Resumen

Se presenta un resumen de cuatro formulaciones diferentes y equivalentes de la mecánica cuántica. Se elige el formalismo de Dirac, como el más adecuado para presentar una aproximación a la computación cuántica desde los postulados de la mecánica cuántica.

1 Introducción

Los esquemas mentales que exige la nueva física para su comprensión, no son comparables a los de la física clásica, donde cada situación es representable por una imagen mental claramente intuible en el terreno de lo causal-determinista. Dadas las condiciones iniciales de un sistema, es posible saber con toda precisión la evolución del mismo, debido a que su comportamiento es expresable como un sistema de ecuaciones diferenciales lineales y hasta cierto punto, es posible conocer sus múltiples relaciones con otros objetos. Contrariamente a esa imagen del mundo, la física moderna, en particular la mecánica cuántica, no permite esa estructuración; la intuición causal-determinista es remplazada por la intuición probabilística. Los eventos no se desenvuelven en el terreno del determinismo clásico sino más bien, en una suerte de evoluciones probabilísticas.

De esa nueva estructuración, ha sido posible deducir y posteriormente medir, es decir, hacer objetivas, una serie de entidades físicas, las cuales no tienen análogas clásicas. Los sistemas nunca están en un estado, sino en una superposición de una serie dada de estados, representados por un vector de un espacio de Hilbert, cuya evolución es mediada por la ecuación de Schrödinger.

A diferencia de la mecánica clásica, en la cual las variables dinámicas del sistema lo describen completamente sin ninguna restricción sobre dichas variables, las cuales en

principio se determinan con precisión infinita, en la mecánica cuántica la situación no es tan directa, la medida requiere la interacción del sistema con un aparato de medida el cual por definición se considera clásico, en el proceso de medida el estado dinámico del sistema se ve afectado por la medida, esta situación en la mecánica clásica era despreciable, pero en mecánica cuántica es de una relevancia fundamental, puesto que la medida perturba el sistema de una manera imprevisible e incontrolable.

En esa nueva perspectiva, no es posible una medición simultánea de algunas variables, tales como la posición y el momento lineal o la energía y el tiempo, entre otras. Existe un principio de indeterminación inherente a las cosas. Pese a lo anterior es posible formar un conjunto completo de variables dinámicas mutuamente compatibles, es decir, medibles simultáneamente, todas las variables de un conjunto como ese, son compatibles dos a dos, y sobre el sistema no existen otras variables diferentes a las ya involucradas en él, a no ser funciones de esas mismas variables.

La computación cuántica es una aplicación de la mecánica cuántica en un territorio diferente a la física del micromundo, ella hace uso de las propiedades y efectos considerados por la mecánica cuántica. Las compuertas cuánticas por ejemplo, se describen mediante los diferentes acoples de los átomos, acoples que en computación cuántica se realizan entre qubits. Los estados internos del átomo sirven en principio para almacenar información cuántica y la interacción espín-espín o espín-orbita, darían los acoples entre los qubits del computador cuántico [11].

La computación cuántica fué inicialmente sugerida por Feynman en los años 80, formalizada por Deutsch (en la forma de máquinas de Turing cuánticas en 1985 [3] y en la forma de circuitos cuánticos en 1989 [4]) y resaltada su potencialidad por Shor en 1994 [10].

1.1 Formulaciones de la mecánica cuántica

En la actualidad son conocidas por lo menos cuatro formulaciones diferentes de la mecánica cuántica, todas equivalentes ente sí, dos son realizaciones concretas de espacios de Hilbert, mientras que otras dos, hacen referencia a espacios de Hilbert abstractos más generales. La primera de ellas es debida a Schrödinger, fué formulada hacia 1923 y conocida como mecánica ondulatoria. Se basa en la formulación clásica de los modos normales de vibración asociados a estados excitados en objetos materiales, como los modos de vibración de una cuerda atada en los extremos, o los modos de vibración producidos por el sonido en una cavidad resonante, estas cuestiones junto a la idea de una onda piloto asociada a todo objeto en movimiento, inspirada por de Broglie, hizo Schrödinger hacia 1923 la idea de una mecánica cuántica en la cual lo determinante era que los electrones excitaban modos armónicos de vibración en el interior de los átomos.

La primera formulación de la mecánica cuántica es la versión de Schrödinger, se formaliza en el marco de las funciones de cuadrado integrable de \mathbb{R}^3 a \mathbb{C} , definidas en un tiempo t

particular como:

$$L^2(\mathbb{R}^3, d\mathbf{r}) = \{\Psi: \mathbb{R}^3 \rightarrow \mathbb{C} \mid \int_{\mathbb{R}^3} d\mathbf{r} |\Psi(\mathbf{r})|^2 < \infty\},$$

su producto interno está definido en este espacio por:

$$\langle \Psi, \Phi \rangle = \int_{\mathbb{R}^3} d\mathbf{r} \bar{\Psi}(\mathbf{r})\Phi(\mathbf{r}), \quad \text{para todo } \Psi, \Phi \in L^2(\mathbb{R}^3, d\mathbf{r})$$

donde la barra sobre la función Ψ corresponde a su compleja conjugada.

Hay una relación muy estrecha entre el espacio de funciones de cuadrado integrable definido anteriormente y el espacio que resulta al tomar las transformadas de Fourier a esas funciones, ambos están relacionados mediante un operador unitario, el cual es la propia transformada de Fourier [7]. Esto implica que; $L^2(\mathbb{R}^3, d\mathbf{r})$ es isomorfo a $L^2(\mathbb{R}^3, d\mathbf{p})$ y el teorema de Parseval-Plancherel [7],

$$\langle \mathcal{F}\Psi, \mathcal{F}\Phi \rangle = \langle \Psi, \Phi \rangle, \quad \text{para todo } \Psi, \Phi \in L^2(\mathbb{R}^3, d\mathbf{r}),$$

justifica que la transformada de Fourier es quién realiza el isomorfismo. El espacio definido por las transformadas de Fourier de las funciones de cuadrado integrable de \mathbb{R}^3 a \mathbb{C} , también es de cuadrado integrable y se define mediante la siguiente expresión:

$$\begin{aligned} \mathcal{F}: L^2(\mathbb{R}^3, d\mathbf{r}) &\rightarrow L^2(\mathbb{R}^3, d\mathbf{p}), \\ \Psi &\rightarrow \mathcal{F}\Psi, \end{aligned}$$

donde p es el *momentum*. Más específicamente se tiene:

$$(\mathcal{F}\Psi)(\mathbf{p}) = \frac{1}{(2\pi\hbar)^{3/2}} \int_{\mathbb{R}^3} d\mathbf{r} \Psi(\mathbf{r}) \exp\left(-\frac{i}{\hbar}\mathbf{p}\cdot\mathbf{r}\right).$$

La segunda formulación es la matricial de la mecánica cuántica, fué propuesta por Heisenberg hacia 1926 y es denominada mecánica matricial. Históricamente se creyó que no debía existir ninguna afinidad con la formulación ondulatoria de Schrödinger pero posteriormente el mismo Schrödinger, demostró su equivalencia. En esta imagen lo verdaderamente importante es la novedosa idea de saltos cuánticos y de discontinuidades en los espectros de algunos observables de los átomos, con un agravante adicional, la imposibilidad de intuir imágenes de los átomos, sugerido en la formulación de uno de los principios más importantes y controvertidos de la mecánica cuántica, “El principio de incertidumbre de Heisenberg.”

La formulación matricial de la mecánica cuántica, se describe en términos del espacio de secuencias infinitas de cuadrado sumable, el cual está definido como:

$$l_2 = \{\Psi = (\Psi_0, \Psi_2, \dots) \mid \Psi_k \in \mathbb{C}, \text{ donde } \sum_{k=0}^{\infty} |\Psi_k|^2 < \infty\}, \quad (1)$$

en la expresión (1) las componentes del multiplete expresan los pesos del estado, respecto a una base. El producto escalar está definido por:

$$\langle \Psi, \Phi \rangle_{l_2} = \sum_{k=0}^{\infty} \bar{\Psi}_k \Phi_k.$$

Casualmente el espacio de secuencias infinitas de cuadrado integrable, substrato de la formulación de Heisenberg, había sido introducido por Hilbert en 1912, y su axiomática formulada en 1927 por von Newman en un trabajo sobre los fundamentos de la mecánica cuántica, es muy coincidencial que la monografía de Courant y Hilbert sobre la matemática de los espacios de Hilbert fuera publicada en 1924, justo en la época que se construía la mecánica cuántica. En palabras de Hilbert:

“I developed my theory of infinitely many variables from purely mathematical interests and even called it ‘spectral analysis’ without any presentiment that it would later find an application to the actual spectrum of physics [7, p. 1911].”

El isomorfismo entre $L^2(\mathbb{R}^3, d\mathbf{r})$ y l_2 se realiza al tomar una función cualquiera $\Psi \in L^2(\mathbb{R}^3, d\mathbf{r})$ y asignarle una secuencia $(\Psi_0, \Psi_1, \dots) \in l_2$, que consiste de las componentes $\Psi_n = \langle n | \Psi \rangle_{L^2}$ de Ψ , con respecto a una base ortonormal $\{|n\rangle\}_{n \in \mathbb{N}}$ de $L^2(\mathbb{R}^3, d\mathbf{r})$.

La tercera formulación fundamentada por Dirac y Jordan en 1931 llamada formulación invariante, inspirada en la idea de un formalismo invariante general, sugerido en la demostración hecha por Schrödinger, de la equivalencia entre las dos mecánicas rivales, los vectores de la formulación invariante; vectores “bra” y “ket”, fueron inventados por el propio Dirac [5], actualmente este formalismo es el más usado en los textos, permite un cálculo simbólico que de alguna manera es más elegante y fácil de implementar, pero al mismo tiempo genera muchas inconsistencias matemáticas [7]. En la formulación de Dirac se usa un espacio de Hilbert abstracto, infinito y separable (admite bases ortonormales que consisten de una familia numerable de vectores). Se regresa a este punto más adelante, cuando se describan los postulados de la mecánica cuántica, descripción que se hará en términos del formalismo de Dirac.

En la cuarta formulación, Feynman¹ en 1948 introdujo una nueva visión de la mecánica cuántica, Dirac por su parte, motivado en la idea de una formulación invariante, en la cual tanto las variables espaciales como las temporales jugaran un papel similar, fundamentaron una formulación de la mecánica cuántica diferente a las anteriores, basada en una novedosa idea de integral de camino. Dirac no se conformó con la idea de una mecánica cuántica en la cual el tiempo jugara un papel tan preponderante, puesto que esto no es aplicable a un sistema relativista, en las anteriores circunstancias se viola la invariancia de Lorentz de la teoría, insinuó dicha formulación con el propósito de que el espacio y el tiempo esten al pie de igualdad.

¹Feynman, R.: P. Rev. Mod. Phys., 20, 367 (1948)

La formulación de la integral de camino de la mecánica cuántica, fundamentalmente esta basada en la noción de propagador \mathbf{G} . Dada una función de onda Ψ en una posición \mathbf{r}_i y en un tiempo t_i , es posible con la ayuda del propagador dar la función de onda Ψ en una posición \mathbf{r}_f y en un tiempo t_f , mediante la siguiente expresión [9]:

$$\Psi(\mathbf{r}_f, t_f) = \int \mathbf{G}(\mathbf{r}_f t_f; \mathbf{r}_i t_i) \Psi(\mathbf{r}_i, t_i) d\mathbf{r}_i.$$

En la interpretación usual de la mecánica cuántica $\Psi(\mathbf{r}_f, t_f)$, es la amplitud de probabilidad de que la partícula se encuentre en el punto \mathbf{r}_f en el tiempo t_f , así que $\mathbf{G}(\mathbf{r}_f t_f; \mathbf{r}_i t_i)$, es la amplitud de probabilidad para la transición desde \mathbf{r}_i en el tiempo t_i hasta \mathbf{r}_f en el tiempo t_f , la probabilidad correspondiente para esa amplitud es [9]:

$$\mathbf{P}(\mathbf{r}_f t_f; \mathbf{r}_i t_i) = |\mathbf{G}(\mathbf{r}_f t_f; \mathbf{r}_i t_i)|^2$$

El propagador resume todas las propiedades de la mecánica cuántica del sistema, la idea de Feynman fue expresar el propagador en términos de una integral de camino, en la cual estan todas las posibles contribuciones de todos los posibles caminos que conducen de un estado a otro, todos esos caminos son físicamente indistinguibles², contribuyen coherentemente a la amplitud cuántica, con igual peso, pero con fases $\exp(iS/\hbar)$ [6]. La integral de camino puede ser formalmente expresada como:

$$\langle \mathbf{r}_f, t_f | \mathbf{r}_i, t_i \rangle = \int \mathcal{D}\mathbf{r} \exp \left[\frac{i}{\hbar} \int_{t_i}^{t_f} \mathcal{L} dt \right], \quad (2)$$

la expresión del lado izquierdo en la última ecuación es el propagador, mencionado anteriormente:

$$\langle \mathbf{r}_f, t_f | \mathbf{r}_i, t_i \rangle = \mathbf{G}(\mathbf{r}_f t_f; \mathbf{r}_i t_i),$$

en (2), $\mathcal{L} = \mathcal{L}(\mathbf{r}, \dot{\mathbf{r}})$ es la Lagrangiana, la cual se construye como la diferencia entre la energía cinética y la potencial. Feynman pudo deducir de estas consideraciones los resultados fundamentales de la mecánica cuántica.

Los siguientes párrafos estan dedicados a una descripción de los postulados de la mecánica cuántica y de la computación cuántica, tomando como referencia la formulación de Dirac.

2 Postulados

Existen varios intentos por describir de una manera formal y sistemática la mecánica cuántica [2, 6], estos párrafos no pretenden de ninguna manera contribuir en esa dirección, sino hacer una pequeña reflexión sobre la pertinencia de los axiomas de la mecánica cuántica en la computación cuántica.

En lo que sigue se dará una descripción de algunos conceptos y nociones referentes a la axiomática de la mecánica cuántica y su correlación con la computación cuántica.

²El término ‘indistinguibles’ significa que no es posible observarlos con algún experimento.

2.1 Primer postulado

Postulado 1. *A cada sistema físico descrito por la mecánica cuántica se le asocia un espacio de Hilbert, y a cada estado del sistema un vector (ket), de ese espacio.*

2.1.1 Caso de un 1-qubit

La unidad fundamental de información cuántica es el qubit $|x\rangle$, este es un elemento del espacio de Hilbert \mathbb{H}_2 de funciones de onda de cuadrado integrable más simple no trivial de dos dimensiones³, al cual puede asociarse una forma lineal, llamada “bra”, inducida mediante el producto interno definido en el espacio \mathbb{H}_2 , es decir:

$$w_{|x\rangle} \equiv \langle x|: \mathbb{H}_2 \rightarrow \mathbb{C}$$
$$|y\rangle \rightarrow w_{|x\rangle}(|y\rangle) = \langle x|y\rangle.$$

El bra $\langle x|$ resulta ser un elemento del espacio dual, del espacio de Hilbert \mathbb{H}_2 , dado por:

$$\mathbb{H}_2^* = \{w: \mathbb{H}_2 \rightarrow \mathbb{C}\}.$$

Existe una correspondencia uno a uno entre los vectores ket y bra, definidos de esa manera. A cada ket le corresponde un bra y viceversa.

Una base de \mathbb{H}_2 , $\{|n\rangle\}_{n \in \{0,1\}}$ es un conjunto formado por dos vectores linealmente independientes $\{|0\rangle, |1\rangle\}$, los cuales satisfacen la siguiente relación de ortonormalidad:

$$\langle n|m\rangle = \delta_{nm}, \quad \text{para todo } n, m \in \{0, 1\}, \quad (3)$$

en esta última expresión δ_{nm} es la función delta de Kronecker, definida por:

$$\delta_{nm} = \begin{cases} 1 & \text{si } n = m, \\ 0 & \text{si } n \neq m. \end{cases} \quad (4)$$

La base de \mathbb{H}_2 , permite definir una relación de clausura, que garantiza la expansión de cualquier vector de \mathbb{H}_2 en esa base:

$$\sum_{n=0}^1 |n\rangle \langle n| = \mathbf{1}_{\mathbb{H}_2}. \quad (5)$$

Los vectores base pueden ser expresados en una representación particular como:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

³El 2 en el subíndice de \mathbb{H}_2 hace referencia a la dimensión del espacio.

a partir de estos dos vectores es posible construir los transpuestos de los ket, los cuales por definición corresponden a los vectores bra:

$$\begin{aligned}\langle 0| &= (1 \ 0), \\ \langle 1| &= (0 \ 1).\end{aligned}$$

El estado más general, denominado qubit (bit cuántico) que se puede formar en el espacio \mathbb{H}_2 , es la superposición lineal de los dos elementos de la base:

$$|x\rangle = c_0 |0\rangle + c_1 |1\rangle, \quad \text{donde } c_0, c_1 \in \mathbb{C}. \quad (6)$$

Los coeficientes que hacen posible dicha superposición satisfacen:

$$|c_0|^2 + |c_1|^2 = 1.$$

De acuerdo a la relación (5), los coeficientes que permiten la combinación (6), resultan ser:

$$c_0 = \langle 0|x\rangle, \quad c_1 = \langle 1|x\rangle,$$

físicamente c_0 y c_1 representan las amplitudes de probabilidad de que al hacer una medida el sistema salte al estado $|0\rangle$, o al estado $|1\rangle$, respectivamente.

Los registros cuánticos se construyen como secuencias de qubits, una secuencia pueden considerarse como el estado total de un sistema que consiste de n qubits cuánticos, los cuales en general no pueden ser descritos como productos tensoriales de los n qubits individuales. Físicamente, el producto tensorial permite hacer un tratamiento unificado de las propiedades cuánticas de los sistemas, estas propiedades, de un lado pueden ser: correlacionadas, es decir; cada una de esas propiedades no puede ser medida sin que de alguna manera haya que hacer referencia a las demás, y de otro lado, no correlacionadas, es decir, las propiedades físicas pueden ser medidas independientemente, sin necesidad de hacer referencias a las otras. La mecánica cuántica con ayuda del producto tensorial permite describir en el mismo ket, tanto las propiedades intrínsecas como las propiedades extrínsecas, las primeras dependen de la estructura interna, son análogas al momento angular o al espín y las segundas son relaciones espacio-temporales.

En la física clásica el estado de un sistema de n partículas, cuyos estados individuales están descritos por un vector en un espacio de dos dimensiones, forma un espacio vectorial de $2n$ dimensiones, mientras que el estado de un sistema cuántico con esas mismas condiciones está descrito por un espacio vectorial de 2^n dimensiones. El espacio estado en el caso clásico se obtiene como un producto cartesiano, en tanto que para el caso cuántico se obtiene como un producto tensorial.

2.1.2 Caso de un 2-qubit

El estado general de un sistema físico que consiste de n partículas, cuyos estados individuales están simbolizados por un espacio vectorial de dos dimensiones, está representado por

un espacio de Hilbert de 2^n dimensiones. En particular, si el sistema físico que se pretende describir está representado por un espacio de Hilbert de cuatro dimensiones, la base debe poderse expresar como:

$$\{|n\rangle \otimes |m\rangle\}_{n,m \in \{0,1\}}. \quad (7)$$

En la relación (7), el símbolo \otimes , muestra justamente, que la base para el espacio en cuestión, es la misma que se obtiene del producto tensorial de los espacios $\mathbb{H}_2 \otimes \mathbb{H}_2 = \mathbb{H}_4$. Los elementos de este espacio cuatrodimensional son denominados 2-qubits. La ecuación (7), puede expresarse de varias maneras:

$$|n\rangle \otimes |m\rangle = |n, m\rangle = |nm\rangle, \quad (8)$$

en estas últimas expresiones $n, m \in \{0, 1\}$.

La relación (8) permite definir la base del espacio estado cuatrodimensional \mathbb{H}_4 como:

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\};$$

la última ecuación puede ser escrita en una forma completamente equivalente como:

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

De otro lado, el 2-qubit normalizado más general

$$|x_1, x_2\rangle = \underbrace{|x_1\rangle}_{1^{er} \text{ qubit}} \otimes \underbrace{|x_2\rangle}_{2^{do} \text{ qubit}},$$

que se puede formar en este espacio es la superposición lineal de los cuatro elementos de la base, es decir:

$$|x_1, x_2\rangle = c_0 |0, 0\rangle + c_1 |0, 1\rangle + c_2 |1, 0\rangle + c_3 |1, 1\rangle, \quad (9)$$

los coeficientes en la expresión (9) satisfacen las siguientes condiciones:

$$c_0, c_1, c_2, c_3 \in \mathbb{C}; \quad \sum_{i=0}^{2^2-1} |c_i|^2 = 1. \quad (10)$$

Nuevamente c_0 representa, la amplitud de probabilidad de que al hacer una medida sobre el sistema, este se encuentre en el estado $|0, 0\rangle$, de igual forma se interpreta cada uno de los c_i .

2.1.3 Caso de un n -qubit

El caso general de un n -qubit no *entangled*, se obtiene apelando a una convención muy usada en la computación cuántica

$$|x_1, x_2, \dots, x_m\rangle \equiv |x\rangle, \quad (11)$$

donde x_1, x_2, \dots, x_m es denominada la representación binaria del entero x , y $|x\rangle$ es denominada la representación decimal del entero x , es decir:

$$x = x_1 2^{m-1} + x_2 2^{m-2} + \dots + x_{m-1} 2^1 + x_m 2^0. \quad (12)$$

De acuerdo con (11) y (12), la base de un espacio formado por n qubits cuya dimensión es 2^n está formada por:

$$\{|0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle\};$$

entonces el n -qubit normalizado más general:

$$|x_1, \dots, x_n\rangle = \underbrace{|x_1\rangle}_{1^{\text{er}} \text{ qubit}} \otimes \dots \otimes \underbrace{|x_n\rangle}_{n \text{ qubit}},$$

viene dado por la superposición lineal de los 2^n elementos de la base:

$$|x_1, x_2, \dots, x_n\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle \quad (13)$$

y los coeficientes de la combinación satisfacen las siguientes condiciones:

$$c_0, \dots, c_{2^n-1} \in \mathbb{C}; \quad \sum_{i=0}^{2^n-1} |c_i|^2 = 1.$$

Si se considera el caso en el cual, el estado global de un sistema no es un producto tensorial de estados, es decir, no puede ser expresado en la forma

$$|x\rangle \otimes |y\rangle,$$

las medidas no pueden ser hechas sin relación de un estado con otro, esta situación refleja la correlación entre estos dos estados del sistema global, las medidas de las propiedades cuánticas de uno u otro estado, corresponden a variables aleatorias las cuales no son independientes, por tanto son correlacionadas. El estado general del sistema no puede ser expresado como el producto tensorial de los estados que lo conforman, los estados que no pueden ser expresados como producto tensorial de otros estados se denominan estados *entangled*. Esta situación no tiene un análogo clásico.

2.2 Segundo postulado

Postulado 2. *Toda cantidad física medible está descrita por un operador \hat{A} que actúa sobre el espacio de Hilbert, este operador es un observable.*

En la mecánica cuántica, los observables están descritos por operadores autoadjuntos que actúan sobre el espacio de Hilbert.

Un operador es autoadjunto si satisface:

$$\hat{A} = \hat{A}^\dagger, \quad (14)$$

de (14) se deduce que:

$$\hat{A}|x\rangle = \hat{A}^\dagger|x\rangle, \quad (15)$$

esta última condición asegura que el dominio de definición de \hat{A} es el mismo dominio de \hat{A}^\dagger ,

$$\mathcal{D}(\hat{A}) = \mathcal{D}(\hat{A}^\dagger). \quad (16)$$

El dominio de un operador \hat{A}^\dagger , que actúa sobre un espacio de Hilbert \mathbb{H} , puede definirse como:

$$\begin{aligned} \mathcal{D}(\hat{A}^\dagger) &= \{|x\rangle \in \mathbb{H} \mid \exists \tilde{\phi}(A, x) \in \mathbb{H}\} \\ &\text{tal que } \langle x | \hat{A} y \rangle = \langle \tilde{\phi}(A, x) | y \rangle \\ &\text{para todo } |y\rangle \in \mathcal{D}(\hat{A}); \end{aligned}$$

donde, para $|x\rangle \in \mathcal{D}(\hat{A}^\dagger)$ se tiene que $\hat{A}^\dagger|x\rangle = \tilde{\phi}(A, x)$.

La ecuación (15) asegura que el espectro del operador \hat{A} es real, sus autovectores forman una base ortonormal completa de vectores. El espectro de un operador autoadjunto es la unión de una parte discreta, para la cual sus autovectores pertenecen a un espacio de Hilbert, y de una parte continua cuyos autovectores asociados no pertenecen al espacio de Hilbert. Todo operador autoadjunto admite una representación espectral [8].

Un operador autoadjunto con espectro discreto, puede ser representado como:

$$\hat{A} = \sum_n a_n \hat{P}_n, \quad (17)$$

donde cada a_n es un autovalor de \hat{A} , y \hat{P}_n es el proyector ortogonal, definido de modo que pueda operar sobre el espacio de autovectores con autovalor a_n . Para el caso de autovalores no degenerados se tiene:

$$\hat{P}_n = |n\rangle \langle n|. \quad (18)$$

Los proyectores satisfacen el siguiente conjunto de ecuaciones:

$$\begin{aligned} \hat{P}_n \hat{P}_m &= (|n\rangle \langle n|)(|m\rangle \langle m|) \\ &= |n\rangle \delta_{nm} \langle m| \\ &= \delta_{nm} \hat{P}_n. \end{aligned} \quad (19)$$

El operador proyección también es autoadjunto, es decir:

$$\hat{P}_n = \hat{P}_n^\dagger.$$

Si el espectro de un operador no es acotado, el dominio de definición del operador no es todo \mathbb{H} , además si el espectro del operador contiene una parte continua, los autovectores correspondientes no pertenecen a \mathbb{H} sino a un espacio mayor.

De otro lado, uno de los operadores autoadjuntos más representativo en la mecánica cuántica es el Hamiltoniano, el cual contiene toda la información del sistema referente a su energía, a partir del Hamiltoniano del sistema, es posible estudiar la evolución de un sistema cuántico, esto será tratado en el sexto postulado.

2.2.1 Caso de un 1-qubit

De acuerdo a (18), los proyectores \hat{P}_0 y \hat{P}_1 para el observable \hat{A} , definidos de acuerdo a la representación espectral que se deduce de la base $\{|n\rangle\}_{n \in \{0,1\}}$, están dados por:

$$\begin{aligned} \hat{P}_0 &= |0\rangle \langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes (1 \ 0) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \end{aligned} \tag{20}$$

$$\begin{aligned} \hat{P}_1 &= |1\rangle \langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes (0 \ 1) \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}; \end{aligned} \tag{21}$$

entonces, de acuerdo a (17), al conjunto de autovalores $\{a_0, a_1\}$ y a (20) y (21), el observable \hat{A} más general para un qubit en esta base es:

$$\begin{aligned} \hat{A} &= \sum_{n=0}^1 a_n \hat{P}_n \\ &= a_0 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a_0 & 0 \\ 0 & a_1 \end{pmatrix}. \end{aligned} \tag{22}$$

En particular si los autovalores del operador pertenecen al conjunto $\{a_0 = 0, a_1 = 1\}$, el observable \hat{A} , toma la forma:

$$\hat{A} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

observese que si se usa la notación binaria, el término del lado izquierdo de (22), puede expresarse como:

$$\hat{A} = \sum_{n=0}^{2^1-1} a_n \hat{P}_n.$$

2.2.2 Caso de un 2-qubit

La ecuación (17), puede generalizarse para un 2-qubit, de la siguiente manera:

$$\hat{A} = \sum_{n=0}^1 \sum_{m=0}^1 a_{nm} \hat{P}_{nm} \quad (23)$$

De acuerdo a (23), los proyectores \hat{P}_{00} , \hat{P}_{01} , \hat{P}_{10} y \hat{P}_{11} para el observable \hat{A} , definidos de acuerdo a la representación espectral que se deduce de la base canónica $\{|n\rangle \otimes |m\rangle\}_{n,m \in \{0,1\}}$, estan dados por cuatro matrices 4×4 , cada una de las cuales tiene un valor igual a 1 en el elemento diagonal correspondiente, por ejemplo para \hat{P}_{10} se tiene:

$$\hat{P}_{10} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

El observable \hat{A} más general que se tiene en esta representación particular de 2-qubit es:

$$\hat{A} = \begin{pmatrix} a_0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 \end{pmatrix}.$$

En notación decimal, de acuerdo a (11), se puede expresar el observable \hat{A} , en la base anterior como:

$$\hat{A} = \sum_{n=0}^{2^2-1} a_n \hat{P}_n.$$

2.2.3 Caso de un n -qubit

La manera más adecuada de generalizar (17), para un n -qubit, es hacerlo en la notación decimal, en ésta, el observable más general que se puede tener en la base canónica es:

$$\hat{A} = \sum_{n=0}^{2^n-1} a_n \hat{P}_n.$$

En esta base se puede construir el siguiente observable general, que actúa sobre un n -qubit:

$$\hat{A} = \begin{pmatrix} a_0 & 0 & \dots & 0 \\ 0 & a_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix}.$$

2.3 Tercer postulado

Postulado 3. *El único resultado posible de una medida física, es un autovalor del correspondiente observable.*

En mecánica cuántica una medida física da como resultado un valor real, esto es una consecuencia de que los autovalores de un operador hermítico siempre son de esa naturaleza (ecuaciones (15) y (16)). Los autovalores asociados a los autovectores que representan los estados de un sistema de computación cuántica, por su naturaleza deben pertenecer al conjunto $\{0, 1\}$.

2.3.1 Caso de un 1-qubit

Al operar con el observable \hat{A} sobre cada uno de los estados base del 1-qubit expresado en (6), se obtienen los siguientes resultados:

$$\begin{pmatrix} a_0 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = a_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

de igual forma para el otro estado base se tiene:

$$\begin{pmatrix} a_0 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = a_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

lo que puede ser expresado en una forma más compacta como:

$$\begin{aligned} \hat{A} |0\rangle &= a_0 |0\rangle, \\ \hat{A} |1\rangle &= a_1 |1\rangle. \end{aligned}$$

2.3.2 Caso de un 2-qubit

Cada uno de los elementos base de (9) pueden ser expresados como productos tensoriales de elementos base de 1-qubits, de la siguiente forma:

$$|0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad (24)$$

al realizar la misma operación con cada uno de los elementos base del 2-qubit en cuestión, se obtienen las siguientes ecuaciones:

$$|1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |2\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Al operar con el observable \hat{A} el estado base del 2-qubit, expresado en (24), se obtienen los siguientes resultados:

$$\begin{pmatrix} a_0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = a_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad (25)$$

la ecuación (25) puede ser expresada más concretamente como:

$$\hat{A} |00\rangle = a_0 |00\rangle,$$

donde a_0 es el autovalor del observable \hat{A} correspondiente a una medida realizada sobre el estado base $|00\rangle$, de un 2-qubit. De una forma completamente análoga se pueden realizar los cálculos anteriores para los otros estados base del 2-qubit:

$$\begin{aligned} \hat{A} |01\rangle &= a_1 |01\rangle, \\ \hat{A} |10\rangle &= a_2 |10\rangle, \\ \hat{A} |11\rangle &= a_3 |11\rangle. \end{aligned}$$

2.4 Cuarto postulado

Postulado 4. (*caso discreto no degenerado*) Cuando una cantidad física es medida sobre un sistema, el cual está en un estado normalizado $|x\rangle$, la probabilidad de encontrar el autovalor a_n correspondiente a un observable \hat{A} es:

$$P(a_n) = |\langle n|x\rangle|^2,$$

donde $|n\rangle$ es el autovector normalizado de \hat{A} , asociado al autovalor a_n .

2.4.1 Caso de un 1-qubit

Para el caso de un qubit, representado en (6). Los números complejos c_0 y c_1 pueden ser interpretados de la siguiente manera. Al proyectar el estado sobre el ket $|0\rangle$, primer elemento de la base y usar el resultado encontrado en (3) y en (4) se obtiene:

$$\langle 0|c_0|0\rangle + \langle 0|c_1|1\rangle = c_0\langle 0|0\rangle + c_1\langle 0|1\rangle = c_0, \quad (26)$$

y al proyectar el estado $|x\rangle$ sobre el ket $|1\rangle$, segundo elemento de la base, se obtiene:

$$\langle 1|c_0|0\rangle + \langle 1|c_1|1\rangle = c_0\langle 1|0\rangle + c_1\langle 1|1\rangle = c_1. \quad (27)$$

El valor c_0 obtenido en (26) es la amplitud de probabilidad de que el sistema se encuentre en el estado $|0\rangle$, al ser medido con respecto a la base $\{|n\rangle\}_{n\in\{0,1\}}$. De igual forma, el valor c_1 obtenido en (27), da cuenta de la amplitud de probabilidad de que el sistema se encuentre en el estado $|1\rangle$, al ser medido sobre la misma base. La relación entre la amplitud de probabilidad y la probabilidad viene dada por:

$$\begin{aligned} P(c_0) &= P(0) = |c_0|^2, \\ P(c_1) &= P(1) = |c_1|^2. \end{aligned}$$

2.4.2 Caso de un 2-qubit

Considere ahora la medida de un sistema cuántico, el cual se representa por un 2-qubit. El estado ha sido descrito (9) y (10). Los números c_i , en las ecuaciones mencionadas, son al igual que en el caso de un qubit, las amplitudes de probabilidad de que el sistema se encuentre, en el i -ésimo vector de base, con probabilidad $|c_i|^2$.

Cuando el primer qubit, en la expresión (9) es medido con respecto a la base representada por (7), la probabilidad de encontrar un cero en el primer qubit del 2-qubit es:

$$|c_0|^2 + |c_1|^2,$$

de forma similar, cuando el primer qubit en la expresión (9), es medido con respecto a la base descrita en (7), la probabilidad de encontrar un uno en el primer qubit del 2-qubit es:

$$|c_2|^2 + |c_3|^2.$$

Análogamente, cuando el segundo qubit en la expresión (9), es medido con respecto a la base descrita en (7), la probabilidad de encontrar un cero en el segundo qubit del 2-qubit es:

$$|c_0|^2 + |c_2|^2.$$

Al medir el segundo qubit en la expresión (9), respecto a la base descrita en (7), la probabilidad de encontrar un uno en el segundo qubit del 2-qubit es:

$$|c_1|^2 + |c_3|^2.$$

2.4.3 Caso de un n -qubit

Al medir el k -ésimo qubit en el registro cuántico, dado por (13), respecto de la base canónica, la probabilidad de encontrar un cero en esa posición, viene dada por la suma de los módulos cuadrados de los coeficientes en la combinación que involucran un cero en dicha posición, cuando son expresados en su notación binaria. De igual forma se halla la probabilidad, para el caso en el que, el registro cuántico tenga un uno en la k -ésima posición.

2.5 Quinto postulado

Postulado 5. Si la medida de una cantidad física sobre un sistema que está en un estado $|x\rangle$ da un resultado a_n , el estado del sistema está, inmediatamente después de la medida, en la proyección normalizada,

$$\frac{\hat{P}_n |x\rangle}{\sqrt{\langle x|\hat{P}_n|x\rangle}}, \quad (28)$$

de $|x\rangle$ sobre el auto-subespacio asociado a a_n .

2.5.1 Caso de un 1-qubit

De acuerdo al postulado anterior, al medir el observable \hat{A} para el qubit dado en (22), se obtiene el autovalor a_0 . El estado del sistema $|x\rangle$ pasa al autoestado base correspondiente al autovalor medido, el cual está dado por la siguiente proyección normalizada:

$$\frac{\hat{P}_0 |x\rangle}{\sqrt{\langle x|\hat{P}_0|x\rangle}}. \quad (29)$$

En (29):

$$\hat{P}_0 |x\rangle = c_0 |0\rangle, \quad (30)$$

también:

$$\langle x|\hat{P}_0|x\rangle = |c_0|^2, \quad (31)$$

al substituir (30) y (31) en (29), se obtiene:

$$\frac{c_0}{\sqrt{|c_0|^2}} |0\rangle.$$

Una situación análoga se presenta si el valor obtenido es a_1 .

2.5.2 Caso de un 2-qubit

Al medir el observable \hat{A} sobre un 2-qubit, se puede obtener cualquiera de los autovalores ubicados en las posiciones diagonales del observable mencionado, el proceso de medida sobre cualquiera de los estados base del 2-qubit en cuestión, implica que el sistema salta al estado inducido en la proyección. Como ejemplo para el caso de un 2-qubit, se supone una medida, la cual arroja el autovalor a_2 , inmediatamente el sistema salta al estado dado por la proyección normalizada inducida sobre el autovector correspondiente a ese autovalor, es decir:

$$\frac{\hat{P}_2 |x\rangle}{\sqrt{\langle x|\hat{P}_2|x\rangle}} \quad (32)$$

Obsérvese que en la última ecuación se ha usado la notación decimal, el ket $|x\rangle$ está dado en (13) con $n = 2$. En la notación decimal, la ecuación (18) es igualmente válida.

En (32):

$$\hat{P}_2 |x\rangle = c_2 |2\rangle, \quad (33)$$

también:

$$\langle x | \hat{P}_2 |x\rangle = |c_2|^2, \quad (34)$$

al substituir (33) y (34) en (32), se obtiene:

$$\frac{c_2}{\sqrt{|c_2|^2}} |2\rangle. \quad (35)$$

Un resultado completamente equivalente se obtiene para cada uno de los autovalores del observable \hat{A} , el cual actúa sobre un 2-qubit.

2.5.3 Caso de un n -qubit

La generalización al caso de un n -qubit es directa si se observa que en notación decimal, al tomar una medida que arroja un resultado a_n , el sistema después de la medida salta al estado normalizado representado por:

$$\frac{\hat{P}_n |x\rangle}{\sqrt{\langle x | \hat{P}_n |x\rangle}} \quad (36)$$

En (36):

$$\hat{P}_n |x\rangle = c_n |n\rangle, \quad (37)$$

también:

$$\langle x | \hat{P}_n |x\rangle = |c_n|^2, \quad (38)$$

al substituir (37) y (38) en la (36), se obtiene:

$$\frac{c_n}{\sqrt{|c_n|^2}} |n\rangle. \quad (39)$$

Si la medida es repetida, entonces de acuerdo a esta regla, se obtiene el mismo estado de salida con probabilidad uno.

2.6 Sexto postulado

Postulado 6. *La evolución en el tiempo del vector de estado $|x(t)\rangle$ es gobernada por la ecuación de Schrödinger:*

$$i\hbar \frac{d}{dt} |x(t)\rangle = H(t) |x(t)\rangle, \quad (40)$$

donde $H(t)$ es el Hamiltoniano del sistema, observable asociado con la energía.

La ecuación de Schrödinger es lineal y homogénea, sus soluciones pueden superponerse linealmente. Sean $|x_1(t)\rangle$, $|x_2(t)\rangle$ dos soluciones linealmente independientes. El estado inicial del sistema en el tiempo t_0 es:

$$|x(t_0)\rangle = \lambda_1 |x_1(t_0)\rangle + \lambda_2 |x_2(t_0)\rangle,$$

el estado del sistema evoluciona hasta una instancia en el tiempo t , la cual está descrita por:

$$|x(t)\rangle = \lambda_1 |x_1(t)\rangle + \lambda_2 |x_2(t)\rangle,$$

de este modo la correspondencia entre $|x(t_0)\rangle$ y $|x(t)\rangle$ es lineal, de lo cual puede deducirse que existe un operador lineal tal que:

$$|x(t)\rangle = U(t, t_0) |x(t_0)\rangle, \quad (41)$$

al substituir (41) en (40), se obtiene:

$$i\hbar \frac{\partial}{\partial t} U(t, t_0) |x(t_0)\rangle = H(t) U(t, t_0) |x(t_0)\rangle,$$

la derivada parcial indica en la anterior expresión que se toma con respecto a t y a t_0 .

De la comparación de los dos miembros de la ecuación anterior, se obtiene:

$$i\hbar \frac{\partial}{\partial t} U(t, t_0) = H(t) U(t, t_0),$$

para un Hamiltoniano independiente del tiempo, la expresión anterior puede ser integrada, si se tiene en cuenta de (41) que $U(t_0, t_0) = \mathbb{I}$, se obtiene:

$$U(t, t_0) = \exp\{(-iH(t - t_0)/\hbar)\},$$

si se define $A = H(t - t_0)/\hbar$, puesto que H es hermítico, A también lo es y el operador:

$$U = \exp(-iA)$$

es unitario puesto que

$$U^\dagger = \exp(-iA^\dagger) = \exp(-iA).$$

El operador U es llamado *operador de evolución temporal*, este operador es unitario⁴.

Las transformaciones que involucran operadores unitarios preservan el producto escalar y por tanto la norma de los estados transformados.

Se considera a continuación algunos ejemplos de operadores de evolución, los cuales son en última instancia las compuertas lógico-cuánticas, encargadas de realizar los cómputos.

⁴Un operador es unitario si su adjunto es igual a su inverso, lo que es expresado como:

$$U^\dagger U = \mathbb{I}.$$

La computación cuántica ha sufrido un desarrollo paralelo desde los años 80 cuando Feynman la sugirió, pasando por los enunciados de Peter Shor sobre la factorización de números en 1994, hasta nuestros días donde se reclama su formalización. Este trabajo de alguna manera contribuye a la búsqueda de los elementos necesarios para esclarecer, tomando como referente la axiomática de la mecánica cuántica, los elementos para una posible formalización axiomática de la computación cuántica.

4 Agradecimientos

Este artículo fue realizado como parte del proyecto de investigación N₀. 817407 financiado por la Universidad EAFIT.

Referencias

- [1] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52(5):3457–3467, 1995.
- [2] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum Mechanics*, volume 1. Hermann and John Wiley and Sons, 1997.
- [3] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97–117, 1985.
- [4] David Deutsch. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425:73–90, 1989.
- [5] P. A. M. Dirac. *Principios de Mecánica Cuántica*. Ediciones Ariel, 1967.
- [6] A. Galindo and P. Pascual. *Mecánica Cuántica*. Editorial Alhambra, S.A., 1978.
- [7] François Gieres. Mathematical surprises and Dirac’s formalism in quantum mechanics. *Reports on Progress in Physics*, 63(12):1893–1931, 2000.
- [8] Erwin Kreyszig. *Introductory Functional Analysis with Applications*. Jhon Wiley & Sons, 1978.
- [9] Lewis H. Rydes. *Quantum Field Theory*. Cambridge University Press, 1985.
- [10] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
- [11] I. V. Volovich. Atomic quantum computer. Eprint: [arXiv.org/abs/quant-ph/9911062](https://arxiv.org/abs/quant-ph/9911062), 1999.