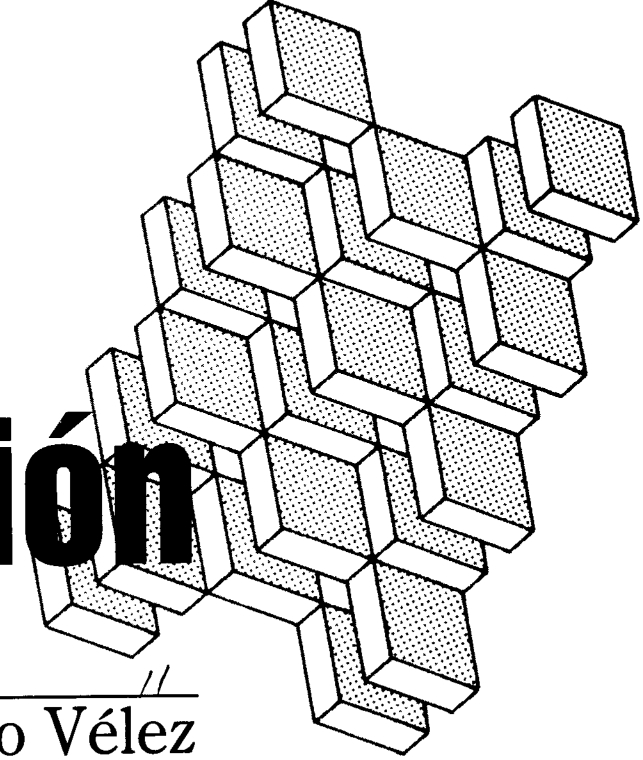

Computación cuántica: una perspectiva desde lo continuo

Mario Vélez
Andrés Sicard

RESUMEN

El artículo espera satisfacer los siguientes objetivos: (i) Conceptualizar parcialmente la teoría de la mecánica cuántica para sistemas descritos por operadores dinámicos con espectro continuo; (ii) Señalar a grandes rasgos la relación que existe, entre los formalismos físico-matemáticos, de dos modelos de computación cuánticos, un modelo discreto y otro modelo continuo; (iii) Resaltar de un lado, el hecho de que la computación cuántica discreta, se formaliza en torno a la noción de "qubit", el qubit es un vector que pertenece a un espacio de Hilbert, del otro lado, la computación cuántica continua se formaliza en torno a la noción de "qunat", el qunat no es un elemento de un espacio de Hilbert e (iv) Indicar muy rapidamente como se puede pensar la computación cuántica continua, fundamentada en teorías de campos cuánticos topológicos.

1. INTRODUCCIÓN

Una de las áreas de mayor investigación en la actualidad es la computación cuántica, que correlaciona elementos de la informática teórica y de la mecánica cuántica, para producir modelos de computación que exploten las propiedades y efectos cuánticos inherentes a las partículas atómicas. El trabajo de Peter Shor (Shor, 1997) señaló el aspecto fundamental en el cual se diferencian la computación clásica y la computación cuántica: la complejidad algorítmica. Esta diferencia consiste en que es posible construir algoritmos cuánticos cuya complejidad temporal sea menor a la de los algoritmos clásicos (conocidos hasta el momento). En particular Shor realizó la descripción de un algoritmo cuántico de complejidad temporal de tipo polinomial para la factorización de números enteros.

2. QUBITS: COMPUTACIÓN CUÁNTICA DISCRETA

Los primeros modelos de computación cuántica se han desarrollado sobre estructuras algebráicas y analíticas basadas en sistemas discretos, similares a sistemas como el espín en la física de partículas elementales. Una noción muy importante en la computación cuántica discreta es la de qubit (Aharonov, 1998, Barenco et al., 1995). Un qubit es el equivalente cuántico del bit clásico:

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

en esta expresión los coeficientes que hacen posible la superposición satisfacen la relación:

$$\sum_{i=0}^{1} |c_i|^2 = 1 \,. \quad \textbf{(2)}$$

En la ecuación **(2),** los números complejos c_0 y c_1 determinan las amplitudes de probabilidad de que al hacer una medida el sistema salte al estado $|0\rangle$ o

MARIO VÉLEZ. Físico, Universidad de Antioquia: Magister en Física, Universidad de Antioquia. Profesor del departamento de Ciencias Básicas, Universidad EAFIT.
E-mail: mvelez@eafit.edu.co

ANDRÉS SICARD. Ingeniero de Sistemas, Universidad EAFIT; Magister en Ingeniería Informática, Universidad EAFIT. Profesor del departamento de Ciencias Básicas, Universidad EAFIT.
E-mail: asicard@eafit.edu.co

REVISTA Universidad EAFIT | abril.mayo.junio | 2000

salte al estado $|1\rangle$, respectivamente. La probabilidad de esos mismos eventos se obtiene elevando al cuadrado las amplitudes de probabilidad. Esa misma relación restringe los valores de las probabilidades a números menores o iguales a uno.

Una de las áreas de mayor investigación en la actualidad es la computación cuántica, que correlaciona elementos de la informática teórica y de la mecánica cuántica, para producir modelos de computación que exploten las propiedades y efectos cuánticos inherentes a las partículas atómicas.

Matemáticamente, el qubit es un elemento de un espacio de Hilbert bidimensional. Con el qubit es posible construir espacios muy generales al efectuar productos tensoriales sobre ellos (Aharonov, 1998):

$$|x_1, \ldots, x_n\rangle = \underbrace{|x_1\rangle}_{1\ qubit} \otimes \ldots \otimes \underbrace{|x_n\rangle}_{n\ qubit}. \quad \textbf{(3)}$$

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.

3. QUNATS: COMPUTACIÓN CUÁNTICA CONTINUA

En la teoría clásica de la información, la unidad fundamental discreta de información es el "bit", y la unidad de información continua es el "nat", el cual se define en términos del bit como:

$$1\text{nat} = \log_2 e \text{ bits.} \quad \textbf{(4)}$$

La unidad de información cuántica continua se ha convenido en llamarla "qunat" (Lloyd y Braunstein, 1999), en completa afinidad con el "qubit". La computación cuántica sobre variables continuas podría pensarse como la capacidad de hacer operaciones sobre los "qunats". En mecánica cuántica, las variables dinámicas se llaman "observables", un operador hermítico es un observable sí posee un sistema ortonormal completo de funciones propias, es decir, los vectores de longitud finita generados por combinaciones lineales a partir de autovectores del operador, forman un espacio de Hilbert. La cuestión de saber si un operador hermítico es un observable o no, es un problema matemático difícil, sin embargo el problema es resuelto para una amplia gama de operadores, aquellos que puedan ser expresados como combinaciones de operadores de proyección. Los operadores hermíticos también son llamados autoadjuntos, ellos satisfacen:

$$\hat{A}=\hat{A}^{\dagger} \quad \textbf{(5)}$$

El hamiltoniano H es quizá el operador hermítico más importante, él representa la energía total del sistema, con él se determina la evolución del sistema, la cual es mediada por la ecuación de Schrödinger:

$$i\hbar \frac{d}{dt}|x(t)\rangle = H(t)\,|x(t)\rangle. \quad \textbf{(6)}$$

La unitariedad de los operadores de evolución en mecánica cuántica es una consecuencia de la ecuación de Schrödinger y de la hermiticidad del hamiltoniano. Un operador es unitario si satisface:

$$U^{\dagger}U=\mathbf{1}. \quad \textbf{(7)}$$

La computación cuántica es realizada por operadores de evolución unitarios los cuales representan las compuertas lógicas, puede decirse entonces que la computación cuántica es la aplicación repetida de operaciones locales, es decir, la funcionalidad de compuertas lógicas cuánticas que operan sobre un número finito de variables (Lloyd y Braunstein, 1999).

Desde el punto de vista de la computación continua, la mecánica cuántica se constituye en una teoría plausible, dado que ésta opera adecuadamente con variables discretas o con variables continuas. Sin embargo, es necesario realizar algunas consideraciones especiales, para la conceptualización de variables continuas al interior de la mecánica cuántica, tal como es indicado (parcialmente) a continuación. Algunos desarrollos en torno a la computación cuántica continua, se pueden encontrar en (Lloyd y Braunstein, 1999, Lloyd y Slotine, 1998, Braunstein, 1998a, Braunstein, 1998b, Patiet al., 2000).

En la axiomática de la mecánica cuántica subyace la noción de estado. Para un instante de tiempo, el estado es representado por una función de onda $|x\rangle$. La interpretación probabilística que da la mecánica cuántica, al respecto de una función de onda, la cual es expresable en una base finita o infinita enumerable de vectores, requiere que esta función sea de cuadrado integrable, es decir, que pertenezca al espacio de funciones cuyo cuadrado es integrable L^2, el cual es un espacio de Hilbert. Para algunos sistemas mecánico-cuánticos de carácter continuo, los cuales han de describirse mediante autovectores de observables como la posición, el momento, la amplitud de campo eléctrico o magnético, o funciones de ellos, la función de onda $|x\rangle$, debe poder expresarse en términos de una base, con un número infinito no enumerable de vectores, esta base no genera un espacio de Hilbert puesto que la norma de los vectores (su longitud) no es finita.

La unidad de información cuántica continua se ha convenido en llamarla "qunat", en completa afinidad con el "qubit". La computación cuántica sobre variables continuas podría pensarse como la capacidad de hacer operaciones sobre los "qunats".

La representación más general posible para $|x\rangle$, es aquella en la cual, la base en la que se representa, puede darse en términos de una combinación en la que una parte sea discreta y la otra parte sea continua. Para todas las posibilidades mencionadas anteriormente, debe estar garantizada la convergencia de los estados que representen el sistema físico. La convergencia se garantiza por una relación de clausura la cual debe poderse expresar en términos de operadores de proyeccción (Cohen-Tannoudji, et al.,1997, Galindo y Pascual, 1978, Landau y Lifshitz, 1972). En particular, la relación de clausura para el caso general, en el que una base pueda expresarse como suma de autovectores ortogonales, tal que, una parte este asociada a un conjunto de autovectores discretos y la otra a un conjunto de autovectores continuos es:

$$\sum_n |n\rangle\langle n| + \int_{\gamma_1}^{\gamma_2} |x_\gamma\rangle\, d\gamma\, \langle x_\gamma| = \mathbf{1}. \quad \textbf{(8)}$$

donde n es un índice discreto y γ es un índice continuo.

Al considerar un operador hermítico con espectro continuo, como la posición, el momentum o las amplitudes de los campos electromagnéticos, que satisfaga la ecuación de valores propios y vectores propios de la mecánica cuántica:

$$\hat{X}\,|x_\gamma\rangle = x(\gamma)\,|x_\gamma\rangle, \quad \textbf{(9)}$$

su espectro recorre una sucesión continua de valores. Los vectores propios pueden ser elegidos de manera que formen una base ortonormal completa, similar a como se forma una base de este tipo para un sistema descrito por magnitudes de espectro discreto, pero esta vez como una integral, tomada con base en un sistema completo de funciones propias de una magnitud con espectro continuo:

$$|x\rangle = \int d\gamma\, c(\gamma)\,|x_\gamma\rangle. \quad \textbf{(10)}$$

Una función de onda en una base de espectro continuo, puede representarse como una combinación infinita no enumerable de vectores propios de un operador que satisface la ecuación de valores y vectores propios en cuestión, los coeficientes de la combinación dependen de un parámetro continuo, dicha combinación, es decir, la integral, se extiende sobre el dominio de valores del parámetro continuo.

La normalización de las funciones de onda en una base de espectro continuo, es diferente al caso de la normalización de las funciones de onda en una base de espectro discreto, la condición de que la integral del cuadrado del módulo de la función de onda sea igual a uno, no se cumple aquí.

Para el caso continuo, la normalización de las funciones de onda se hace teniendo en cuenta que la integral del módulo al cuadrado del coeficiente que permite la combinación infinita no enumerable de vectores, es igual a uno, a diferencia del caso discreto donde, es la integral del cuadrado del módulo de la función de onda, la que es igual a uno, dicha expresión también significa que la suma de las probabilidades de todos los valores del parámetro continuo es igual a uno

$$\int |c(\gamma)|^2\, d\gamma = 1. \quad \textbf{(11)}$$

La condición para la integral del cuadrado del módulo de la función de onda, se da en términos de una distrubución llamada, delta de Dirac. Esta distribución debida a P.A.M. Dirac (Dirac, 1967), se da en términos de la diferencia de dos parámetros continuos, la cual se anula cuando esa diferencia es distinta de cero, y es indeterminada cuando dicho argumento es igual a cero

$$\langle x_{\gamma_1} | x_{\gamma_2} \rangle = \delta(\gamma_1 - \gamma_2). \quad \textbf{(12)}$$

Esta condición también da cuenta de una relación similar a la de ortonormalidad para un sistema de vectores de base discreta. Lo nuevo es que las integrales de los módulos cuadrados de las funciones de onda de espectro continuo son divergentes, es decir, la longitud de los vectores no es finita.

La computación cuántica es realizada por operadores de evolución unitarios los cuales representan las compuertas lógicas, puede decirse entonces que la computación cuántica es la aplicación repetida de operaciones locales, es decir, la funcionalidad de compuertas lógicas cuánticas que operan sobre un número finito de variables.

Aunque la mecánica cuántica opera naturalmente sobre objetos continuos, los modelos actuales de computación cuántica, tales como los circuitos cuánticos [Barencoet al., 1995, Deutsch, 1989, Rieffel y Polak, 1998, Sicard y Vélez , 1999a), y las diferentes versiones de máquinas de Turing cuánticas (Deutsch, 1985, Bernstein y Vazarini, 1997, Ozawa, 1998, Sicard y Vélez, 1999b), entre otros; son considerados modelos de computación discretos (Bernstein y Vazarini, 1997). La computación cuántica universal discreta, la realizan un conjunto de operadores que actúan en un instante de tiempo, sobre un conjunto de variables representadas como estados en un espacio de Hilbert adecuado. Con la aplicación repetida de tales operaciones locales, se puede generar cualquier transformación unitaria sobre un número finito de esas variables, hasta el grado de precisión que se requiera (Lloyd y Braunstein, 1999).

Contrariamente a lo que se pudiera pensar, la computación cuántica sobre variables continuas es un concepto bien definido. En la actualidad existen algunas propuestas de computación cuántica continua; Seth Lloyd y Samuel Braunstein (Lloyd y Braunstein, 1999), han propuesto un modelo de computación cuántica continua bajo ciertas limitaciones de las transformaciones que operan sobre las variables continuas.

De acuerdo a Lloyd y a Braunstein, es posible realizar computación cuántica universal continua, para una amplia subclase de transformaciones unitarias, aquellas para las cuales los hamiltonianos que definen dichas transformaciones, son funciones polinómicas de los operadores correspondientes a variables continuas. La computación cuántica universal continua, la realizan un conjunto restringido de transformaciones continuas, que permiten por medio de un número finito de operaciones, acercarse arbitrariamente a cualquier transformación en el conjunto.

Teóricamente es posible hacer operaciones aritméticas con variables continuas en un computador cuántico continuo. Samuel Braunstein (Braunstein, 1998a) por su parte, presenta para algunas transformaciones cuánticas discretas, sus correspondientes transformaciones cuánticas continuas.

4. COMPUTACIÓN HOLONÓMICA

Una propuesta de carácter muy diferente a las anteriores, la constituye la computación holonómica, Paolo Zanardi y Mario Rasetti (Zanardi y Rasetti, 1999) muestran como es posible realizar computación cuántica continua usando la teoría de la holonomía. En su artículo, se muestra como al codificar información cuántica en el espacio generado por los autovectores de un hamiltoniano degenerado, se puede alcanzar toda la potencia computacional usando solo holonomías. La computación holonómica se realiza al hacer ciclos en una variedad d-dimensional de parámetros de control que rotulan la familia de hamiltonianos. En cada punto de la variedad hay un código cuántico, el conjunto de éstos, describe un haz de códigos, el cual tiene una topología no trivial, la cual puede ser descrita por un potencial, es decir, por un campo *gauge* no abeliano. La holonomía asociada a un campo A genérico, describe computación cuántica universal.

Estos autores afirman que por todas estas razones los campos *gauge*, podrían jugar un papel muy importante en los procesos de información. Dado que algunos modelos de áreas de estudio tales como las interacciónes fundamentales, la relatividad general y la física del estado sólido, entre otras; están basados en las teorías *gauge* de los grupos no abelianos U(N); la computación cuántica continua podría ser otro modelo adicional, basado en estos elementos.

Lo nuevo es que las integrales de los módulos cuadrados de las funciones de onda de espectro continuo son divergentes, es decir, la longitud de los vectores no es finita.

CONCLUSIONES

Es posible desarrollar dos formalismos físico-matemáticos paralelos, uno para la computación cuántica discreta, y el otro, para la computación cuántica continua, similares, pero formalmente diferentes.

La integral del módulo cuadrado de los vectores de estado "qubits", que representa la probabilidad, en el caso de la computación cuántica discreta es finita, ello implica que los vectores de estado, autovectores de los observables, forman un espacio de Hilbert, en tanto que esa misma expresión para los vectores de estado "qunats", no representan la probabilidad, puesto que esta expresión no es finita, los vectores de estado no generan un espacio de Hilbert.

Es posible hacer computación cuántica continua, basada en teorías cuánticas topológicas de campos *gauge,* donde la noción más importante es la holonomía.

Aunque en la actualidad existen algunos trabajos en el área, tal como lo afirman algunos autores anteriores (Lloyd, Braunstein, Zanardi, Rasetti) el área de la computación cuántica continua, está en proceso de gestación.

REFERENCIAS

Aharonov, Dorit. (1998). Quantum Computation (1998). Eprint: quantph /9812037.

Barenco, Adriano, et al. (1995). Elementary gates for quantum computation Eprint: quant-ph/9503016.

Bersntein, Ethan y Vazarini, Umesh. (1997). Quantum Complexity Theory. En, *Siam Journal on Computing,* tomo 26(5): páginas 1411-1473

Braunstein, Samuel L. (1998a). Error Correction for Continuos Quantum Variables. En , Physical Review Letters, tomo 80(18): páginas p. 4084-4087 (1998a). Eprint: quant-ph/9711049.

Braunstein, Samuel L. (1998b). Teleportation of Continuos Quantum Variables. En: *Physical Review Letters,* tomo 80(4): páginas p. 869-872 (1998b).

Cohen-Tannoudji, et al. (1997). *Quantum Mechanics,* tomo 1. Hermann and John Wiley and Sons. Inc. (1997).

Deutsch, David. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. En: *Proc. R. Soc. Lond.,* tomo A400: páginas pp. 97-117 (1985).

Deutsch. (1989). Quantum computational networks. En: *Proc. R. Soc. Lond.,* tomo A425: páginas pp. 73-90 (1989).

Dirac, P.A.M. (1967). Principios de mecánica cuántica. Ediciones Arial Traducción: Antonio Montes.

Galindo, A. y Pascual, P. (1978). Mecánica Cuántica. Editorial Alhambra, S.A.

Landau, L.D. y Lifshitz, E.M. (1972). Mecánica Cuántica no Relativista, tomo III. Editorial Reverté, S.A., 2a. edición Traducción Prof. Dr. Ramón Ortiz Fornaguera.

Lloyd, Seth y Braunstein, Samuel L. (1999). Quantum computation over continuos variables. En: *Physical Review Letters,* tomo 82(8): páginas p. 1784-1787 Eprint: quant-ph/9810082.

Lloyd, Seth y Slotine, Jean Jacques E. (1998). Analog Quantum Error Correction. En: *Physical Review Letters,* tomo 80(18):páginas p. 4088-4091

Ozawa, Masanao. (1998). Quantum Turing Machines: Local Transition, Preparation, Measurement, and Halting. Eprint: quant-ph/9809038.

Pati, Arun K., et al. (2000). Quantum searching with continuos variables (2000). Eprint: quant-ph/0002082.

Rieffel, Eleanor y Polak, Wolfgang. (1998). An Introduction to Quantum Computing for Non-Physicists Eprint: quant-ph/9809016.

Shor, Peter W. (1997). Polinomial-Time Algorithms for Prime Factorizacion and Discrete Logarithms on a Quantum Computer. En: *Siam Journal on Computing,* tomo 26(5):páginas 1484-15090 (1997).

Sicard, Andrés y Vélez, Mario. (1999a). Algunos elementos introductorios acerca de la computación cuántica. En: *Memorias VII Encuentro de la ERM, Realizado en la Universidad de Antioquia.* Escuela Regional de

Matemáticas. En: Informe de Investigación: ¿Máquina de Turing Cuántica Autorrefencial: Una posibilidad?, Universidad EAFIT, 1999.

Sicard, Andrés y Vélez, Mario. (1999b). Some relations between quantum Turing machines and Turing machines (1999b). En: Informe de Investigación: ¿Máquina de Turing Cuántica Autorrefencial: Una posibilidad?, Universidad EAFIT. Eprint: quant-ph/9912012. Sometido a publicación a la Revista Mexicana de Fí sica.

Zanardi, Paolo y Rassetti, Mario. (1999). Holonomic Quantum Computation. Eprint: quant-ph/9904011.