Algoritmia para Computadores Cuánticos

Samira Abdel Masih[1], Enrique Cingolani[1], Hugo Colombo[1], Pedro Hecht[2], Jorge Kamlofsky[1], Daniel Veiga[1].

[1]CAETI - Universidad Abierta Interamericana
Av. Montes de Oca 725, Buenos Aires, Argentina
abdel.masih@hotmail.com,{enrique.cingolani, hugo.colombo, jorge.kamlofsky, daniel.veiga}@uai.edu.ar

[2]Universidad de Buenos Aires, Facultades de Ciencias Económicas, de Ciencias Exactas y Naturales y de Ingeniería. Maestría en Seguridad Informática, Buenos Aires, Argentina.
phecht@dc.uba.ar

Resumen

Las computadoras cuánticas fueron creadas por primera vez en el año 1998 y actualmente empresas como Google, IBM y la NASA las están utilizando de modo experimental.

Su importancia radica en la velocidad con que procesan los datos, y lo hacen en un tiempo considerablemente menor que el llevado a cabo por una computadora convencional.

Por ejemplo, a un ordenador clásico le tomaría cientos de años poder encontrar los factores primos de un número natural de 600 dígitos, mientras que a una computadora cuántica sólo le tomaría unos minutos.

En este proyecto se estudian los fundamentos matemáticos de la Computación Cuántica.

Asimismo, se desarrollan algoritmos para ser implementados en un ordenador cuántico.

Si bien este nuevo paradigma de programación está en sus inicios, en un futuro no muy lejano las computadoras cuánticas reemplazarán a las convencionales en entornos de cálculos intensivos, y se tornará cada vez más necesario diseñar algoritmos acordes a esta nueva tecnología.

Palabras clave:
Computación Cuántica, Algoritmos Cuánticos, Quantum Computing, Compuertas Cuánticas, Qubits, Quantum Gates.

Contexto

Los proyectos desarrollados en el CAETI (Centro de Altos estudios en Tecnología Informática, dependiente de la Facultad de Tecnología Informática de la UAI) se clasifican en cinco líneas de investigación. Este proyecto se enmarca dentro la línea de investigación de "*Ingeniería de Software*". Se pretende brindar los fundamentos matemáticos y desarrollar algoritmos para ser utilizados en una computadora cuántica.

Introducción

Una computadora cuántica es un dispositivo que utiliza el modelo de los estados de ciertos elementos del átomo para realizar sus procesos.

Los ordenadores convencionales resumen toda la información que

procesan a lenguaje binario, es decir, sólo utilizan dos estados para almacenar y operar con datos: **0** ó **1**.

La unidad mínima de información utilizada por estos ordenadores es el ***bit***.

Pero en una computadora cuántica la unidad mínima de información es el ***bit cuántico*** o ***qubit***, el cual representa el estado físico de ciertos sistemas cuánticos, por ejemplo partículas subatómicas (que pueden ser electrones, protones, neutrones, fotones, etc.).

Dichos sistemas tienen una curiosa cualidad que hace fascinante a la Computación Cuántica: la ***superposición de estados***.

La ***superposición de estados*** en un sistema cuántico consiste en que éste no sólo puede adoptar el estado **0** ó **1**, sino que puede estar en ambos estados al mismo tiempo.

Gracias a este fenómeno surge el ***paralelismo cuántico***, que es la propiedad que tienen los algoritmos cuánticos de efectuar varias operaciones a la vez.

Así, los ordenadores cuánticos son capaces de probar, al mismo tiempo, todas las posibilidades que existen para la solución concreta de un problema, en lugar de probarlas una tras otra, como lo realizan actualmente las computadoras convencionales.

En definitiva, las computadoras cuánticas procesan los datos en forma paralela, a diferencia de las computadoras actuales, que lo hacen en forma secuencial [1].

Este cambio en el paradigma de la Computación supone un enorme salto hacia adelante, ya que permitirán realizar cálculos complejos que actualmente resultan inalcanzables en la computación clásica.

De este modo, podrán resolverse problemas clásicamente considerados "intratables" por su alto nivel de complejidad.

Gracias a la propiedad del paralelismo, las computadoras cuánticas pueden valuar, en forma simultánea, una función $f(x)$ para múltiples valores de la variable independiente x.

El Algoritmo de Deutsch- Josza [3], uno de los primeros algoritmos cuánticos, es un claro ejemplo que permite apreciar el funcionamiento y la potencia de los programas cuánticos mediante el uso del paralelismo cuántico.

Propuesto por David Deutsch y Richard Josza en 1992, su finalidad es determinar si una función booleana $f(x_1, x_2, \ldots, x_n)$ de n variables es constante (vale 0 o bien 1 en todas las entradas) o está balanceada (es decir, si toma el valor 1 para la mitad de las entradas y 0 para la otra mitad) [2].

Otro algoritmo cuántico muy importante en Ciencias de la Computación es el presentado por Lov Grover en 1997 [4] quien mostró cómo mediante una computadora cuántica se puede hallar un elemento dentro de una lista desordenada en $O(\sqrt{n})$ pasos, mientras que una computadora clásica lo logra en $O(n)$ iteraciones [5]. Es decir, el algoritmo de Grover permite hallar rápidamente resultados dentro de gigantescas bases de datos mediante una consulta simple. Esto es actualmente de gran importancia con el crecimiento de los sistemas de Big Data, alimentados por las nuevas tecnologías IOT (Internet de las Cosas) [6].

En los últimos años se han desarrollado otros algoritmos cuánticos con aplicaciones en múltiples áreas: Física, Química y Genética [7 – 10].

Sin embargo, el área donde la Computación Cuántica causó una revolución paradigmática es en la Criptografía.

Los algoritmos criptográficos asimétricos más usados del mundo [11 - 14] se basan en la dificultad para la

resolución de ciertos problemas numéricos conocidos como: IFP (Integer Factorization Problem) y DLP (Discrete Logarithm Problem). El paralelismo cuántico resulta ser una herramienta adecuada para afrontar estos problemas.

En 1997 Peter Shor presentó un algoritmo que reduce drásticamente la complejidad computacional del problema IFP mediante una computadora cuántica [15]. Los trabajos de Kitaev [16] y Proos-Zalka [17] presentaron ataques eficaces a los problemas DLP y DLP para curvas elípticas también mediante una computadora cuántica.

Hoy la existencia de la computadora cuántica es un hecho: la empresa D-Wave Systems ya vendió computadoras cuánticas a Lockheed Martin, al laboratorio Los Alamos, a Google y a la NASA, entre otros [19]. Además, IBM por su lado, ofrece servicios en la nube con su computadora cuántica [20].

En caso que los algoritmos [15 – 17] logren implementarse en computadoras cuánticas, hecho que la NIST (National Institute of Standards ando Technology) ve posible para un futuro cercano [21], arrasaría con la casi totalidad de los algoritmos empleados en la criptografía actual [18].

Líneas de Investigación, Desarrollo e Innovación

Se trabaja en dos ramas: Matemática y Algoritmos Cuánticos.

La Matemática es utilizada para modelar el comportamiento de los qubits, de las compuertas y de los circuitos cuánticos.

En la rama de los Algoritmos Cuánticos se pretende generar algoritmos para ser implementados en un ordenador cuántico. Estos son probados empíricamente mediante los servicios de computación cuántica ofrecidos por IBM en la nube [9].

Resultados y Objetivos

Como objetivo general, se pretende adquirir conocimientos teóricos y prácticos básicos acerca de la programación en computadoras cuánticas.

Los objetivos específicos son los siguientes:

■ Conocer acerca de las ventajas de la programación en computadoras cuánticas.
■ Investigar, analizar y diseñar circuitos lógicos basados en compuertas cuánticas.
■ Investigar, analizar y diseñar algoritmos diversos para computadores cuánticos.

Por otro lado, en el marco del proyecto se lograron los siguientes resultados a partir del año 2017:

Tesinas: En 2017 Pablo Oviedo presentó en la UAI su tesis para obtener el título de Licenciado en Matemática. La misma se titula: *Fundamentos matemáticos de computación cuántica en el algoritmo de Shor, para la factorización prima de números enteros*.

Dictado de Cursos: *Taller de Computación Cuántica*, en la XI Jornada de Matemática llevada a cabo en la UAI, el 9 de Mayo de 2018.

Premios obtenidos: Primer Premio en el Certamen de Trabajos Estudiantiles del CIITI 2017, que tuvo lugar en Buenos Aires, el 19 de septiembre de 2017. Título del Trabajo: *Algoritmo para la Factorización Prima de Números Enteros en una Computadora Cuántica*.

Diseño de algoritmos: Debido a que el proyecto está en sus inicios, se lograron probar solamente algunos algoritmos cuánticos básicos, con algunas modificaciones, en la computadora cuántica virtual de la empresa IBM. La misma constituye una herramienta de

suma utilidad, ya que es el único medio vigente que permite chequear los resultados de un algoritmo.

Formación de Recursos Humanos

El proyecto está dirigido por la Dra. Samira Abdel Masih y codirigido por el Lic. Jorge Kamlofsky. Integran el proyecto el Lic. Enrique Cingolani, el Ing. Hugo Colombo, el Dr. Pedro Hecht y el Lic. Daniel Veiga.

En el transcurso del año 2019 los estudiantes Yésica Valente y Ariel Savarese presentarán sus Tesis de la carrera de Licenciatura en Matemática, desarrollando temas referentes a algoritmos cuánticos.

Referencias

[1] Hecht, Juan Pedro. *Fundamentos de Computación Cuántica*. Editorial Académica Española. ISBN 978-3-8484-7529-2 (2005).

[2] Oviedo, Pablo. *Fundamentos Matemáticos de Computación Cuántica en el Algoritmo de Shor, para la factorización prima de números enteros* (Tesis de Grado). Universidad Abierta Interamericana, Buenos Aires, (2017).

[3] D. Deutch and R. Jozsa. *Rapid solution of problems by quantum computation.* Proc. Roy Soc. London Ser. pp 553-558. (1992)

[4] Grover, L. K. *Quantum computers can search arbitrarily large databases by a single query*. Phys. Rev. Lett. 79, pp 4709–4712 (1997).

[5] Spector, Lee. *Quantum Computing Applications of Genetic Programming.* Advances in Genetic Programming (1999).

[6] Gustafson S, and Sheth A. *Web of Things.* Computing Now 7.3 (2014).

[7] Holt, Katherine. *Diamond at the nanoscale: applications of diamond nanoparticles from cellular biomarkers to quantum computing*. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 365.1861 (2007): 2845-2861.

[8] Leuenberger, Michael N., and Daniel Loss. *Quantum computing in molecular magnets.* Nature 410.6830 (2001): 789.

[9] Cory, David G., Amr F. Fahmy, and Timothy F. Havel. *Ensemble quantum computing by NMR spectroscopy.* Proceedings of the National Academy of Sciences 94.5 (1997): 1634-1639.

[10] Steane, Andrew. *Quantum computing.* Reports on Progress in Physics 61.2 (1998): 117.

[11] Rivest, Ronald L., Adi Shamir, and Len Adleman: *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM 21.2, pp 120-126. (1978).

[12] Diffie W., Hellman M.E. *New directions in cryptography*. IEEE Transactions on information theory, 22, pp 644-654, (1976).

[13] El Gamal, Taher. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. En Advances in cryptology.* Springer Berlin Heidelberg, pp. 10–18 (1984).

[14] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press (1996).

[15] Shor P. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM J. Comput., 5, pp 1484-1509 (1997).

[16] Kitaev A. *Quantum measurements and the abelian stabilizer problem*. Preprintar Xiv/quant-ph., 9511026 (1995).

[17] Proos J., Zalka C. *Shor's discrete logarithm quantum algorithm for elliptic curves*. Quantum information and computation, 3, pp 317-344 (2003).

[18] Kamlofsky J, Hecht JP. *Post-Quantum Cryptography Using Hiper-complex Numbers*. XXIII Congreso Argentino de Ciencias de la Computación (2017).

[19] D-Wave-Systems Press Releases [en línea], (2018). Disponible en: <http://www.dwavesys.com/news/press-releases>. Fecha de consulta: 28/02/2018.

[20] IBM: IBM Makes Quantum Computing Available on IBM Cloud to Acceletare Innovation [En Linea], (2016). Disponible en: <https://www-03.ibm.com/press/us/en/pressrelease/49661.wss>. Fecha de consulta: 28/02/2018.

[21] National Institute of Standards and Technology, Information Technology Laboratory– Computer Security Division. *Post-Quantum Crypto Proyect* [En línea], (2018) Disponible en: <http: // csrc.nist.gov / groups / ST / post-quantum-crypto/>. Fecha de consulta: 28/02/2018.