2019

CONAIISI

VII Congreso Nacional de Ingeniería Informática - Sistemas de Información

14 y 15 de Noviembre de 2019

RIIIC

DIIT

confedi

Universidad Nacional de La Matanza

Registro del presente Libro de Actas - 7mo CONAIISI 2019

Donadello, Bettina
2019 CONAIISI : VII Congreso Nacional de Ingeniería Informática : Sistemas de Información / Bettina Donadello. - 1a ed . - San Justo : Universidad Nacional de La Matanza, 2020.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-987-4417-73-2

1. Ingeniería Informática. 2. Sistemas de Información. I. Título.
CDD 004.071

El futuro de la Computación Cuántica

Durán, Matías; Seijas, Lucas Gabriel; Peña, Diego Axel; Galio, Juan Cruz; Mombelli, Martín.

Universidad Tecnológica Nacional, Facultad Regional Buenos Aires

Abstract

La Computación Cuántica es un nuevo modelo tecnológico basado en principios de la física cuántica, propone un esquema donde las computadoras pueden ser infinitamente superiores en cuanto a velocidad. El objetivo del presente trabajo, es analizar la Computación Cuántica en relación a su funcionamiento y potencial, y el impacto que puede tener a futuro en la sociedad. En base a la investigación realizada, se observa que la Computación Cuántica no vino a reemplazar a la binaria (la actual), sino más bien, a complementarla debido a que existen acciones que una puede realizar y la otra no, y viceversa.

Palabras Clave

Computación Cuántica, Qubits, decoherencia, superposición, costo

Introducción

La computación tal y como se la conoce, basada en el uso de los dígitos binarios 1 y 0, y que presenta la información en serie o en paralelo, fue creada en 1936 [7]. Sin embargo, en los últimos años se dio un cambio total de paradigma en cuanto al funcionamiento de las computadoras y el potencial que las mismas poseen [4]. La Computación Cuántica es un paradigma de computación que se basa en el uso de qubits en vez de bits y pueden procesar la información en simultáneo [1]. Un qubit puede estar definido como 0, 1 o, como una superposición de los dos. Esto permite que se puedan realizar cómputos sobre ambos valores a la vez [2]. Se puede deducir que este nuevo sistema, tiene más potencial que el actual, ya que por ejemplo un ordenador cuántico con longitud de palabra de 32 qubits tendría una potencia de cálculo equivalente a la de unos 4.300 millones de ordenadores personales de 32 bits, de los que hoy se utilizan, y puede dar paso a sistemas más competentes y tecnologías más avanzadas como por ejemplo la implementación de criptografía cuántica como nuevo método de seguridad informática [3].

En este contexto, el objetivo del presente trabajo (realizado en el marco de la cátedra de "Sistemas y Organizaciones", primer año de cursada), es analizar la Computación Cuántica en cuanto a su funcionamiento y potencial, y el impacto que puede tener a futuro en nuestra sociedad. Para cumplir el objetivo propuesto, el trabajo se estructura de la siguiente manera: en la sección 1, se presenta la Computación Cuántica y sus características; en la sección 2, se examina el potencial que tiene la Computación Cuántica. En la sección 3, se desarrollan los problemas de la Computación Cuántica. En la sección 4, se detalla un análisis de costo/beneficios de esta tecnología. Finalmente, en la sección 5 se desarrollan las conclusiones y futuras líneas de trabajo.

1. Conceptos básicos

La Computación Cuántica abarca todo un paradigma de la computación basado en el uso de qubits en lugar del convencional bit [4]. El qubit es la unidad básica de información, éste puede hallarse en distintos estados, tales como 1 o 0, o como una superposición de ambos [5]. Eso permite que se puedan realizar varias operaciones simultáneas, según el número de qubits.

Según [1] "Con los bits convencionales si teníamos un registro de tres bits había ocho valores posibles, y el registro sólo podía tomar uno de esos valores. En cambio, si tenemos un vector de tres qubits, la partícula puede tomar ocho valores distintos a la vez gracias a la superposición cuántica. Así, un vector de tres qubits permitiría un total de ocho operaciones paralelas." El inconveniente que se puede encontrar al utilizar este tipo de mecánicas, es la medición del valor de uno de estos qubits, ya que las mediciones en la mecánica cuántica no son deterministas, es decir que si se mide el valor de un qubit 100 veces por ejemplo, se encuentra que el valor siempre va a cambiar, ya que el proceso de medida es, por tanto, un experimento aleatorio en el que la probabilidad de cada resultado está determinada por el estado del sistema. A esta situación se la conoce como paralelismo cuántico (a mayor cantidad de qubits que haya en el proceso, la cantidad de pasos aumenta "elevado" por cada qubit disminuyendo el tiempo que tomaría en una computadora clásica de forma exponencial). Según [14], la información se codificará en átomos hacia 2030: "Parecerá demasiado optimista, pero es una indicación razonable de que la técnica alcanzará pronto el mundo microscópico, donde las leyes cuánticas gobiernan el comportamiento de los dispositivos físicos". Cuanto más relevante sea uno de los estados en la superposición, más probabilidad hay de que al medir el valor del qubit, ese sea el valor expresado. Más precisamente, la posibilidad de medir cada estado se calcula como el módulo cuadrado del coeficiente que le acompaña, así por ejemplo, si se encuentra con un qubit cuyos valores de la superposición son 0.81 para el 0, y 0.57 para el 1, la probabilidad de que cada valor se vea expresado al realizar la medición, estará dado por el cálculo $|0.81|^2$ Para el 0 y $|0.57|^2$ para el 1 [6]. De acuerdo a [13], "es la física la ciencia adecuada para estudiar el comportamiento de la información. Después de todo, vivimos en un mundo sensorial y creamos el castillo de conocimientos que tenemos sobre él en base a nuestras sensaciones". La Computación Cuántica usa la superposición de estados para ejecutar más de un cómputo a la vez. Como los electrones del qubit pueden ser 0 y 1 al mismo tiempo, gracias a esto podemos comprobar ambos estados a la par, lo cual nos permite tener ordenadores muchísimo más rápidos. Por supuesto, no garantiza más rapidez en cualquier situación, pero sí en las que se pueda aprovechar éste paralelismo.

2. Potencial de la Computación Cuántica

Un computador cuántico de 30 qubits tiene la misma capacidad de cómputo que el de un procesador convencional de 10 teraflops (millones de millones de operaciones en coma flotante por segundo), cuando actualmente las computadoras trabajan en el orden de gigaflops (miles de millones de

operaciones en coma flotante por segundo), implicando una mejora de rendimiento, teniendo en cuenta que el teraflop es una medida de mayor escala que el gigaflop (sería como comparar metros con centímetros). Hoy en día el computador cuántico más potente se encuentra en manos de Google, y cuenta con una capacidad de procesamiento y almacenamiento de 72 qubits [4]. Uno de los principales usos para los que se plantea esta tecnología, es la criptografía, ya que sistemas que antes tardaban años en romperse, es decir, descifrar un determinado código de seguridad criptográfico, con el uso de un computador cuántico, sólo se tardarían minutos. Uno de los principales usos del computador cuántico, se basaría en derribar la mayoría de las medidas de seguridad existentes. En una entrevista dada por James Clarke (Director de Hardware Cuántico de Intel Corporation), declaró [15]: "Para algunas aplicaciones, la Computación Cuántica es exponencialmente mejor que la computación clásica. Por ejemplo, para algunas aplicaciones, como criptografía, un ordenador clásico puede tardar 1.000 millones de años en romper una clave criptográfica RSA mientras un ordenador cuántico podría hacerlo en minutos."

3. Problemas en el desarrollo la Computación Cuántica

Los tres problemas más importantes en el desarrollo de esta nueva tecnología fueron el hardware, el uso que le corresponde y la decoherencia. El primer problema es el hecho de encontrar hardware adecuado para la implementación de la Computación Cuántica que pueda aprovechar por completo todas sus capacidades. La Computación Cuántica en teoría es prometedora pero, al llevarla a la práctica cuesta mucho trabajo [9]. Esto sucede debido a que es tecnología en la que no se tiene tanta experiencia como para poder manejarla de manera sencilla, los qubits son muy susceptibles a pequeños cambios. Además el costo de producción puede llegar a ser muy elevado para mantener esta tecnología, teniendo en cuenta que hablamos de millones de dólares en una tecnología que promete, pero que a su vez, es incierta [10].

Más adelante, el uso dado es importante ya que al ser solo utilizado en el campo científico-académico, evitaría que una gran cantidad de inversionistas quieran fundar el avance de esta tecnología, es decir, el uso actual de esta tecnología limita los fondos que podría reunir. En los últimos años, los avances en la computación han sido debido a la gran cantidad de dinero que deja el mercado de la tecnología para uso diario o empresarial. Si la tecnología se estanca en estas zonas significaba una gran pérdida de dinero y por lo tanto, menos avances [11].

El último problema a analizar es la decoherencia. Según [12] "la decoherencia cuántica es el proceso que produce la pérdida de coherencia de un estado cuántico". Es el término usado en el estudio de la mecánica cuántica para explicar porque un estado cuántico entrelazado, bajo ciertas condiciones específicas, puede dar lugar a un estado físico clásico (no entrelazado). De acuerdo a [12] "Se puede entender como la destrucción de la interferencia cuántica; la interferencia es el resultado de una de las características más peculiares de la mecánica cuántica, el

principio de superposición". Teniendo esta definición en cuenta, podemos tomar como ejemplo, el caso del experimento imaginario del gato de Schrodinger [8], el hecho de que las partículas del gato en cuestión entren en contacto con el ambiente podrían llevar a cabo una decoherencia que tenga como consecuencia que la combinación de "gato vivo" + "gato muerto" perdiera coherencia y se transformara en un estado normal y por tanto tras un lapso de tiempo, el gato definitivamente estuviera dentro de la caja vivo o muerto, pero no en una superposición de ambos [8]. Esto significa que los qubits se pierden y se transforman en simples unidades de información. Si se pierde el qubit, la computadora simplemente no funcionaría y se podría considerar inservible [1].

4. Análisis del costo y beneficios de la Computación Cuántica

A pesar del principal problema de la tasa de error por qubit, Google pudo avanzar en la construcción de su primer procesador cuántico de 72 qubit reduciendo la tasa de error a 1% [16]. Sin embargo, es una tasa de error que no se puede permitir en un escenario realista, debido a la alta cantidad de error que podrían ocurrir y teniendo en cuenta que los procesadores convencionales tienen una tasa de error inexistente [16]. Por ende, el objetivo que se busca es el de tener una tasa de error del 0,1% en miles de millones de qubits, objetivo para el que queda todavía un largo camino.

Lo mismo realizó Intel por su lado, al crear finalmente un procesador de 49 qubits, dando a conocer las bases que deberán seguir los nuevos procesadores cuánticos. Por ejemplo, se sabe que para que el sistema cuántico de las computadoras funcione, éste debe operar a unos 0° Kelvin, o mejor dicho -273° C, temperatura que roza el Cero Absoluto. Dejando en claro que no habrá un procesador cuántico doméstico en muchos años, el avance es lento y las condiciones de funcionamiento son bastante exigentes.

Sin embargo, existen claros avances cada día que (aunque sean lentos y poco concisos) definirían algún día el estándar de la Computación Cuántica.

Por ejemplo, D-Wave (empresa pionera en Computación Cuántica) descubrió que un procesador de 4000 qubits podría rendir exactamente igual a uno de 2000 qubits debido a la temperatura[17]. Si se quisiese notar una mejora en el rendimiento, se debería bajar aún más la temperatura (teniendo en cuenta que se trabaja normalmente en 0,015°K), algo que parece casi imposible.

Para que la Computación Cuántica tenga un peso relevante frente a la computación convencional, faltan aproximadamente 10 o 15 años, si se tiene en cuenta que el procesador con mayor cantidad de qubits actualmente tiene 128 y se estima que para que sea capaz de rivalizar necesita de al menos 1000 qubits que puedan trabajar de forma estable y con una tasa de error ínfima[18].

5. Conclusiones

El qubit todavía no presenta su máximo potencial, pero se están realizando avances bastante significativos con respecto a su desenvolvimiento y compatibilidad en un entorno de trabajo. Las mejoras con respecto a la cantidad de qubits utilizados en el procesador cuántico fue aumentando, dejando de ser únicamente teoría. Se puede apreciar su funcionamiento estable bajo condiciones que, si bien no son normales, son las necesarias para que funcione esta nueva tecnología y así evitar la decoherencia, que es la capacidad del qubit de perderse y asignar información inútil a la computadora.

También existen nuevos inconvenientes, como el hecho de que la cantidad de núcleos qubit no importaban si la temperatura no era la adecuada debido a que esta falta de frío iba a mermar el rendimiento del procesador, comparable a uno de menos qubits, la temperatura limita el máximo potencial de la computadora cuántica.

Vale recordar que la Computación Cuántica no vino a reemplazar a la binaria (la actual), sino más bien, vino a complementarla debido a que hay acciones que una puede realizar y la otra no, y viceversa. Más que nada debido a que el sistema operativo o programas cargados a la computadora cuántica, distan de ser iguales de una forma inimaginable, haciendo que la Computación Cuántica y la binaria no sean más que incompatibles pero complementarios entre sí. Como futuras líneas de trabajo, se prevé profundizar en las cuestiones económicas que llevan a la Computación Cuántica a ser aún muy restrictiva. Resulta prometedor investigar cómo pueden reducirse los costos de fabricación para así lograr que esta tecnología pueda llegar a lugares al menos más tangibles para el común de la gente como universidades o pequeños laboratorios.

Referencias:

[1] A. Sicard, “Computación cuántica: una perspectiva desde lo continuo” Revista Universidad EAFIT, vol. 36, no. 118, Jun, 2012. [Online]. Available: https://bit.ly/2Sw4vGQ**.** Último ingreso: 29/08/2019

[2] Pastor, Jesús. (2002). Quantum mechanics and brain: A critical review. Revista de neurología. 35. 87-94. [Online]. Available: https://bit.ly/2ULl6HI. Último ingreso: 29/08/2019

[3] F. Montoya, “La criptografía cuántica, ¿realidad o ficción?”, Instituto de Física Aplicada, Departamento del Tratamiento de la Información y Codificación, Consejo Superior de Investigaciones Científicas, Madrid, España, 2004. [Online]. Available: https://bit.ly/2CARPDB. Último ingreso: 29/08/2019

[4] Grupo de Computación Cuántica, “Introducción al modelo cuántico de computación”, Dep. Matemática Aplicada. E.U. Informática Ctra. de Valencia Km. 7, 28031, Madrid, España, 2003. [Online]. Available: https://bit.ly/32QwFNy. Último ingreso: 29/08/2019

[5] V. Moret Bonillo, “Principios fundamentales de la Computación Cuántica”, Departamento de Computación. Facultad de Informática Universidad de A Coruña. , España, 2013. [Online].Available: https://bit.ly/2uwHdzK. Último ingreso: 29/08/2019

[6] O. Organista, V. Gómez, D. Jaimes y J. Rodríguez, “Una idea profunda en la comprensión del mundo físico: el principio de superposición de estados”, Grupo de Física Matemática, Departamento de Física, Universidad Pedagógica Nacional de Colombia, Bogotá D. C., Colombia. 2007 [online] available: https://bit.ly/2HXWMcn. Último ingreso: 29/08/2019

[7] Prieto, A., Lloris, A., & Torres, J. C.. Introducción a la Informatica 3ra edición, 1989 [online] available: https://bit.ly/1RA4bfv. Último

ingreso: 29/08/2019
[8] L. De la Peña, “Decoherencia en mecánica cuántica” in Introducción a la mecánica cuántica, xth ed. 2014, cap. 15, sec. 5.4,
[9] James N. Eckstein, Jeremy Levy, “Materials issues for quantum computation”, MRS Bulletin, 2013, [online] available: https://bit.ly/2JgGXzi. Último ingreso: 29/08/2019
[10] Herve-Victor Formen, “Quantum Computing: a review of investments in 2018”, 2018, [online] available: https://bit.ly/2XrKMWo. Último ingreso: 29/08/2019
[11] Esther Villa Rodriguez, Eneko Osaba Icedo, Javier Del Ser Lorente, “QUANTUM COMPUTING: six key factors to understand the future of computation”, 2012, UNESCO, [online] available: https://bit.ly/2YKxHJ2. Último ingreso: 29/08/2019
[12] Sebastian Fortin, “Decoherencia Cuántica”, 2016, Diccionario Interdisciplinar Austral, [online] available: https://bit.ly/2WVJ002. Último ingreso: 29/08/2019
[13] Nasser Darwish Miranda, “Computación cuántica”, Universidad de La Laguna, España, 2007. [Online]. Available: https://bit.ly/2PbUjAs. Último ingreso: 29/08/2019
[14] Antonio Acín, “Procesamiento cuántico de la información”, Investigación y ciencia, 2006. [Online]. Available: https://bit.ly/2tv72Ta. Último ingreso: 29/08/2019
[15] J. S. Clark, “Quantum computing within the framework of advanced semiconductor manufacturing”, 2016. [Online]. Available: https://bit.ly/2JsiffA. Último ingreso: 29/08/2019
[16] Susana Angulo, “Google lidera nuevamente la computación cuántica”, 2018. [Online]. Available: https://bit.ly/2JA3LJk. Último ingreso: 29/08/2019
[17] Francisco R. Villatoro. El duro camino de D-Wave hacia la supremacía. https://bit.ly/2LgLBxa. Último ingreso: 29/08/2019
[18]Manuel Arenas. El procesador de 49 qubits de Intel por dentro. https://bit.ly/2LH6qk5. Último ingreso: 29/08/2019

2019 CONAIISI
VII Congreso Nacional de Ingeniería Informática - Sistemas de Información

Trabajo de alumno
14 y 15 de NOVIEMBRE

UTN - FRBA

Escanear para contactar a los autores

El Futuro de la Computación Cuántica

Objetivos: analizar la Computación Cuántica en cuanto a su funcionamiento y potencial, definiendo el posible impacto que podría llegar a tener en nuestra sociedad.

Introducción

La ***Computación Cuántica*** se basa en los qubits, que operan de acuerdo con dos principios clave de la física cuántica: la superposición y el enredo. Gracias a estos, una computadora cuántica puede procesar una gran cantidad de cálculos simultáneamente.

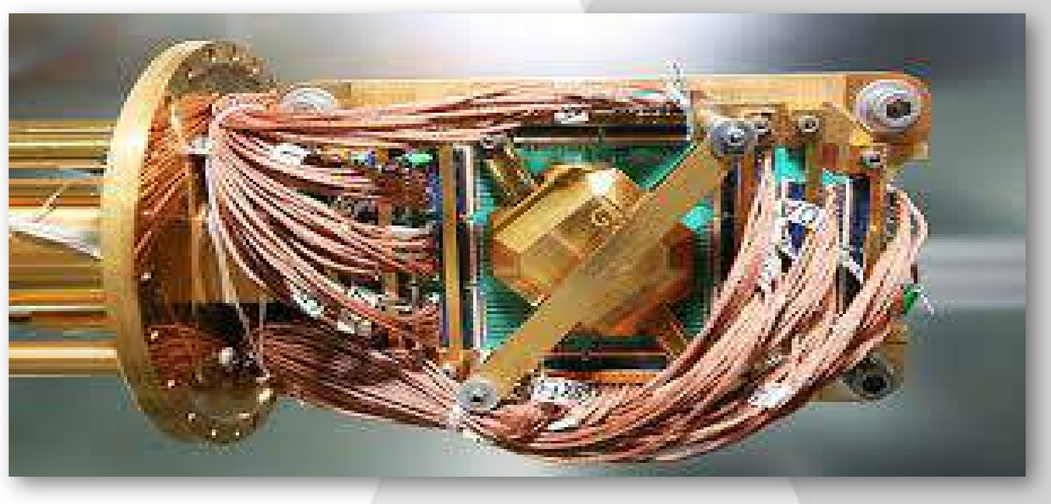
-**No Convencional:** se maneja con el uso de Qubits, a diferencia del Bit convencional.
-**Qubit:** el Bit puede determinar dos posibles estados, 0 y 1. El Qubit puede tomar cualquiera de los dos valores **al mismo tiempo**, permitiendo así operaciones paralelas.
-**Poca Compatibilidad:** diseñar software para los procesadores basados en **Qubits** puede ser muy complicado, anulando de por si, cualquier compatibilidad con un software que no sea especializado en qubits, es decir, la mayoría del software existente.

Potencial de la computación cuántica

A nivel académico, pueden factorizar números muy grandes con facilidad. Pueden desentrañar la complejidad de las interacciones moleculares y químicas que conducen al descubrimiento de nuevos medicamentos y materiales. Resolver problemas financieros o de logística más eficientemente y más rápido.

Problemas que presenta la Computación Cuántica:

- Temperatura
- Decoherencia
- Hardware difícil de manipular
- Financiamiento a largo plazo



Conclusiones

- La Computación Cuántica es una tecnología muy prometedora y muy poco desarrollada.
- Está lejos de poder llegar a tener un propósito general, y muy lejos de poder comercializarse de forma doméstica.
- Sin embargo, podrá hacer lo que a la computadora común le podría llegar a tardar miles de años.

Futuras líneas de trabajo

- ✔ Se prevé profundizar en las cuestiones económicas que llevan a la Computación Cuántica a ser aún muy restrictiva.

Agradecimientos

Este trabajo fue promovido y guiado por el equipo a cargo de Ma. Florencia Pollo-Cattaneo, con la ayuda de Cinthia Vegega, pertenecientes a la cátedra de Sistemas y Organizaciones de la UTN-FRBA.

Autor/es:

Matias Duran
Axel Peña
Lucas Seijas
Juan Cruz Gaglio
Martín Mombelli