Arquitectura de la computación cuántica: La información es transmitida más rápido que la velocidad de la luz.

Natalia Gómez*, Angel Gómez*, Andrés Gómez*,David Villabona*

* Facultad de Fisicomecánicas, Ingeniería de Sistemas, Universidad Industrial de Sandander Bucaramanga, Colombia

Resumen

La computación clásica es super poderosa logrando múltiples aplicaciones. Desde los comienzos se ha buscado conseguir computadoras más poderosas y potentes logrando tecnología cada vez más pequeña con mejor rendimiento, obteniendo actualmente transistores entre 5 y 7 nm, pero este es el límite, ya que no se ha logrado reducir más su tamaño porque se estaría alcanzando los efectos de la mecánica cuántica obteniendo como consecuencia limitaciones en las frecuencias de las operaciones, el simple término 'cuántico' demoniza y ahuyenta a un gran número de entusiastas quienes creen no poder entender lo que da vida a estas computadoras. En este artículo trataremos dar una vista general a este nuevo tipo de computación que, aunque tiene diferentes tipos de arquitecturas, tienen una misma composición en la física cuántica.

Abstract

Classic computing is super powerful, achieving multiple applications. Since the beginning, we have sought to achieve more powerful and potent computers, achieving ever smaller technology with better performance, currently obtaining transistors between 5 and 7nm, but this is the limit, since it has not been possible to reduce its size any more because it would be reaching the effects of quantum mechanics obtaining as a consequence limitations in the frequencies of the operations, the simple term "quantum" demonizes and scares off a large number of enthusiasts who believe they can not understand what gives life to these computers. In this article we will try to give a general view to this new type of computation that, although it has different types of architectures, have the same composition in quantum physics.

I. Introduction

La mecánica cuántica clausura las grandes ramas de la física, es la encargada de estudiar las partículas subatómicas, su aplicación ha hecho posible el descubrimiento, desarrollo e innovaciones en la tecnología computacional [1]. Los avances tecnológicos son cada vez más exigentes, desde el principio de los tiempos se ha buscado obtener mayor cantidad de datos a mayor velocidad con menor consumo energético y siendo la medida de innovación su fuente primordial de competitividad.

En la actualidad discurrir en la arquitectura de computación cuántica comprende un nivel de complejidad, así como en los inicios de la computación clásica que los ordenadores alcanzaban tamaños de una habitación de igual forma estamos en un estado muy primario con esta computación, esta tecnología opera a muy bajas temperaturas (-273C) más fría que la temperatura espacial, esta es una de las razones porque esta arquitectura no es una tecnología estándar.

En la computación cuántica el número de configuraciones simultaneas posibles crece de manera exponencial, comparada con la capacidad de computadoras clásicas la computadora más poderosa de todo el mundo no puede simular una computadora de más de 60 qubits, la cantiad de qubits en una computadora cuántica se ha predicho que serán emulares. Las computadoras cuánticas tienen un estado de superposición $c_0|0 + c_1|1 >$ [2]. Esta notación científica en términos técnicos se le llama amplitud, que representa la probabilidad de poder ser un cero o puede ser un uno así, la computacin cuántica se puede ver como una superposición coherente de computaciones digitales que se desarrollan en paralelo [3].

Sin duda esta competencia y los avances presentados tiene a la expectativa a personas que van desde científicos e ingenieros a simples apasionados por la tecnología, disfrutando y especulando con lo que el futuro trae junto con esta nueva herramienta qué puede significar un cambio grande en la forma que se hace computación hoy en día.

Se propone afianzar los conceptos abstractos de la computación cuántica y por medio de algunas analogías con la computación convencional introducirlos en este campo y exponer la arquitectura de ella.

II. ESTADO DEL ARTE

La escalada de los ordenadores cuánticos ha sido pronunciada, desde que en la década de los 80 los físicos Richard Feynman y Paul A. Benioff presentaran de forma independiente teorías relacionada con el aprovechamiento de la física cuántica en la computación, grandes hitos de ingeniería han llevado sus postulados teóricos a la práctica. En los 90 aparecieron los primeros algoritmos cuánticos, algunos de los más famosos son el algoritmo de Shor, basado en la transformada de Fourier, y el algoritmo de búsqueda de Grove el cuál no requiere ordenación de sus elementos. La universidad de Berkeley, en California, tuvo el honor de ser la pionera al crear un ordenador cuántico que contaba con 2 qubits (el qubit es la unidad básica de información en computación cuántica), sin embargo, tan solo un año después, uno de los gigantes tecnológicos del mundo, IBM, fabricó el primer ordenador de 3 qubits, en años posteriores vinieron los 5 qubit y luego el primer qubyte (8 qubits).

Actualmente casi todas las empresas pioneras en tecnología se encuentran involucradas con el desarrollo de ordenadores cuánticos (Google, IBM, Microsoft, NTT, Intel, etc). Google e Intel apuestan por los 49 qubits, afirmando que el pasar a los 50 provocaría una inestabilidad cuántica creando fallas en la coherencia de los datos (decoherencia de datos), mientras que IBM, con su IBM:Q de 50 qubits, presenta todo un entorno interactivo para su ordenador, por medio de su iniciativa Quantum Experience, la cual es una apuesta por parte de la empresa para fomentar el desarrollo de lenguajes de programación orientados a algoritmos cuánticos.

Los desafíos proclamados ante esta tecnología demandan grandes retos especialmente en el área de la arquitectura computacional, ya que en la apuesta por la eminencia cuántica y la

estandarización de estos ordenadores se viene siguiendo una serie de investigaciones en orden ascendente mostradas en la Figura 1 [4].

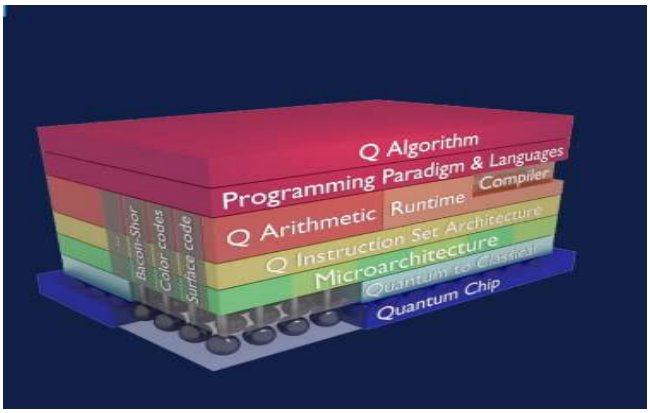

Figure 1: Representación gráfica de los estandares cuánticos en la computación.

El procesador cuántico ya se encuentra en un estado medio de desarrollo, sin embargo, para lograr la cima, ”Q Algorith”, el problema actual se centra en los dos siguientes peldaños, ”De cuántica a clásica” y ”Microarquitectura”; ya que los dos problemas que han frenado el desarrollo de la computación cuántica han sido la refrigeración y la decoherencia de datos, término usado para explicar cómo un estado cuántico da lugar a un estado físico clásico, pues bajo ciertas condiciones deja de exhibir efectos cuánticos y se comporta típicamente, esto está relacionado fuertemente con la forma en que los datos son tratados.

III. Contenido

A. *¿De qué se trata la física cuántica?*

Antes de entrar en materia conozcamos de qué se trata la física cuántica.

La física cuántica es una de las ramas más alucinantes de la física, que estudia los comportamientos de la materia cuando las dimensiones de ésta son muy pequeñas, tanto que empiezan a notarse extraños efectos, como por ejemplo la imposibilidad de conocer con exactitud la posición de una partícula.

Tiene dos principios fundamentales. El primero es que las partículas intercambian energía en múltiplos enteros de una cantidad mínima posible, llamados quantum de energía. El segundo es que la posición teórica de las partículas está dada por una función probabilística, esto quiere decir que es más una probabilidad y no una certeza [5].

La física cuántica predice comportamientos paradójicos increíbles. Por ejemplo, una partícula cuántica no posee solo un valor de una cantidad física, sino todos al mismo tiempo, algo que se llama superposición; dos partículas cuánticas pueden permanecer entrelazadas, aun a distancias ilimitadas y sin ninguna conexión física de por medio; y se pueden teletransportar a través del espacio vacío [6].

B. Computación cuántica

La computación cuántica es un nuevo paradigma de computación el cual se basa en el uso de qubits como unidad básica de información, la diferencia más importante entre computación cuántica y clásica es la complejidad, dando cabida a problemas que se consideraban intratables, pues esta tiene como pilares fundamentales dos términos referentes a la física cuántica, la superposición de estados con la cual un qubit puede estar en uno o dos estados simultáneamente, y el entrelazamiento cuántico con el cual la transferencia de información superaría la velocidad de la luz ya que esta sería instantantánea [3].

En la computación digital se usan bits como unidad básica de información, el cual puede tomar uno de 2 valores, 1 o 0; por el contrario, en la computación cuántica, suceden fenómenos cuánticos como la superposición coherente, por la cual, un qubit, puede ser 1, 0 o los dos a la vez, esto aumenta considerablemente el número de operaciones que se pueden realizar a la vez, dando posibilidades increíbles a disciplinas como la computación paralela, esto es resultado de una interacción de un conjunto de partículas entrelazadas que ocurre durante algunas millonésimas de segundo, este fenómeno es conocido como 'entanglement' [7].

Esta ciencia aplicada surgió como alternativa a la tecnología basada en transistores la cual ya está alcanzando su límite físico, el atómico, pues a una escala nanométrica los electrones se escapan de los canales por donde circulan (efecto túnel) y genera perdida de datos [8].

Imaginar un programa determinado que toma dos números y un bit adicional y hace lo siguiente: si el bit adicional está en el estado 0 entonces el programa suma los dos números y te da el resultado, y si el bit está en el estado 1 el programa resta los números y te da el resultado. Si quisieras obtener la suma y la resta de dos números, tendrías que correr el programa dos veces: uno con el bit adicional en 0 y otro con el bit en 1. En un ordenador cuántico, dado que el qubit puede estar en una superposición de 0 y 1, el programa corre las dos instrucciones en paralelo, así con una sola ejecución se podrá obtener el resultado que sea la superposición de la suma y la resta de los números.

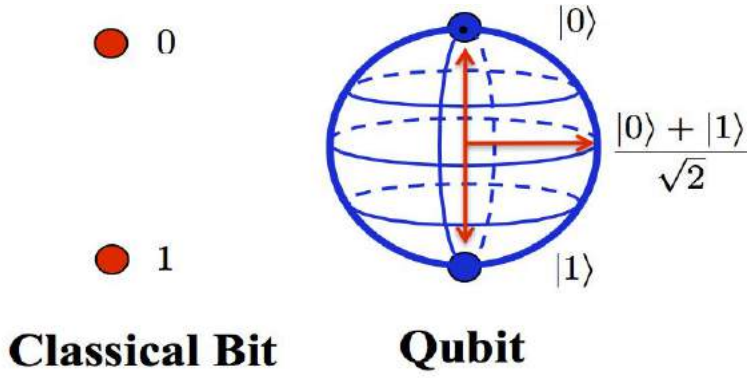

Figure 2: El bit cuántico (qubit) puede dar una superposición de 0 y 1.

C. Arquitectura de una computadora cuántica

1) Procesador: Los inicios de un procesador cuántico se dieron con la idea de computador cuántico del físico Richard Feynman, el cual se basa en átomos, uniéndolos unos a otros de forma concreta, cada uno de estos está en uno cualquiera de dos estados posibles. Dejando que este sistema evolucione con base en leyes de la mecánica cuántica:

- sistema interacciona consigo mismo.
- átomos cambian de estado.
- $< 1 >$ y los $< 0 >$ se cambian.

Feynman propone en su modelo dos matrices denominadas matrices de aniquilación, asegura un estado $|0>$, y de creación, asegura un estado $|1>$. Estas son matrices unitarias, similares a las que se usan para el desarrollo de puertas cuánticas, lo que en cuántica vendrían siendo lo que para la computación convencional son las puertas lógicas [9] [8].

Estas puertas lógicas cuánticas son circuitos cuánticos que operan sobre un pequeo número de qubits, Las puertas cuánticas se suelen representar como matrices. Una puerta que opera sobre k qubits queda representada por una matriz unitaria de $2^k x 2^k$. El número de qubits en la entrada y a la salida tienen que ser iguales. El resultado de la puerta cuántica se halla multiplicando la matriz que representa la puerta con el vector que representa el estado cuántico [10]. Algunas de las puertas cuánticas más conocidas son la puerta de Hadamar, que no es más que la representacin de un qubit de la transformada cuántica de Fourier, la puerta de SWAP la cual intercambia dos qubits y las puertas controladas como la CNOT (puerta NOT controlada) opera sobre dos qubits, y realiza la operación NOT en el segundo qubit solo cuando el primer qubit es $|1>$.

La implementación de estas compuertas para la posterior construcción de un procesador cuántico depende de la arquitectura que se haya decidido adoptar, existen varias, por ejemplo, exista una implementación basada en óptica lineal, en este caso se usan fotones o iones para portar la información, se usan elementos ópticos lineales (como pueden ser divisores de haces de luz y espejos) para procesar la información cuántica y detectores de fotones para su respectiva detección, una de estas implementaciones es el sistema de trampa de iones con 5 qubits que consta de cinco iones $171Yb+$ que se confinan en una trampa Paul lineal y se enfrían con láser cerca de su estado fundamental de movimiento. Los qubits son pares de estados insensibles al campo magnético en el nivel del suelo $2S1/2$ con división hiperfina de cada átomo, lo que da una frecuencia de qubit de $12.642821GHz$. Todos los controles y medidas se realizan de forma óptica. La preparación del estado y la lectura se realizan mediante bombeo óptico y detección de fluorescencia dependiente del estado [11].

El otro tipo de implementación es el usado por IBM, que sus circuitos superconductores en su computadora cuántica se pueden considerar como átomos artificiales. Son qubits transmon o islas superconductoras conectadas mediante uniones de Josephson y condensadores de derivación que proporcionan superposiciones de estados de carga que son insensibles a las fluctuaciones de carga. El dispositivo desarrollado por IBM de 5 qubits tiene un rango de frecuencias qubit entre 5 GHz y 5.4 GHz [12] [11]. Los qubits están conectados entre sí y se tiene un sistema de control clásico por resonadores de microondas.

Un computador cuántico de 30 qubits equivaldría a un procesador convencional de 10 Teraflops (Flotant Point Operations Per Second) y actualmente la meta para la Supremacía cuántica se encuentra en los 122.3 Petaflops que ostenta el Summit-IBM, una supercomputadora usada por el Departamento de Energía y Laboratorio Nacional de Oak Ridge en Estados Unidos. La Figura.3 [13] y la Figura.4[8] muestran una representación esquemática de un eventual ordenador cuántico y una arquitectura cuántica.

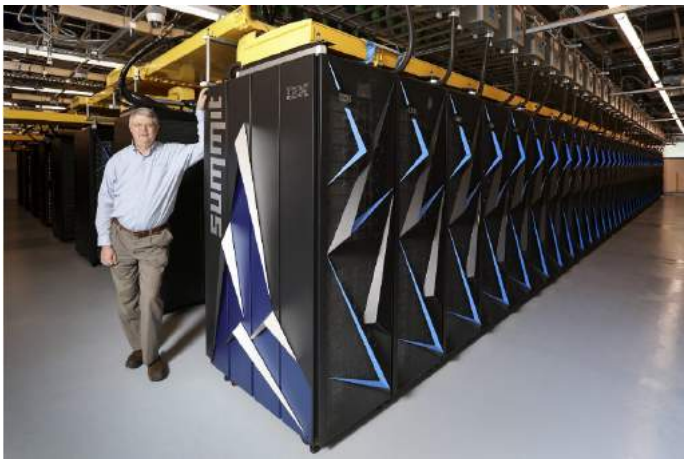

Figure 3

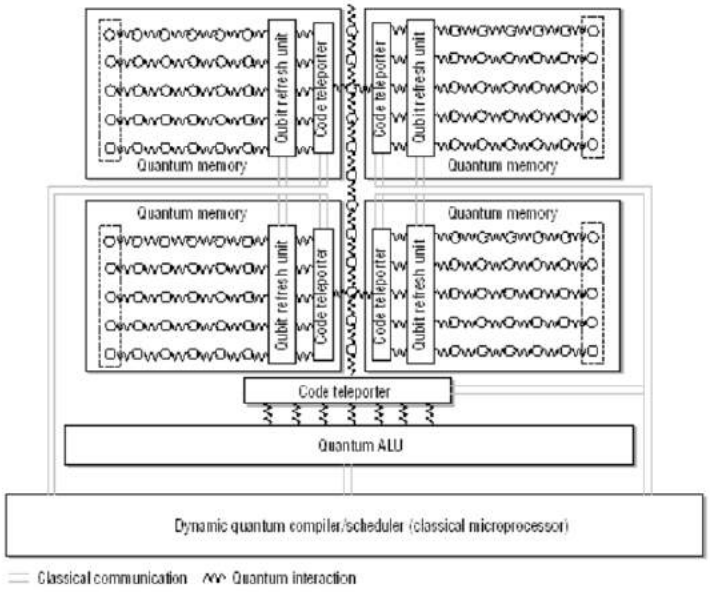

Figure 4

2) ALU Cuántica: La unidad aritmético-lógica en la computación cuántica tiene como funciones fundamentales la corrección de errores y la ejecución de operaciones cuánticas. Se tiene una serie de transformaciones cuánticas para predisponer los datos antes de ejecutar cualquier compuerta estas secuencias son:

- Hadamard (raíz cuadrada, transformada de Fourier de 1 qubit).
- I, Identidad (I, NOP cuántico).
- X, NOT cuántico.
- Z, cambia los signos de las amplitudes.
- Y = XZ.
- rotación por p /4 (S).
- rotación por p /8 (T).
- NOT controlado (CNOT).

Este procedimiento tiene como fin la verificación de paridad. La ALU ejerce el hardware especializado estándar, que provee estados elementales estándares, para producir los estados auxiliares adicionales.

3) Memoria cuántica: En septiembre de 2007, aparece el primer bus cuántico, que puede ser dispuesto como memoria cuántica, antes de lograr enviar la información se produce un periodo de tiempo en el que los datos son retenidos por un lapso corto de tiempo antes de lograr la transferencia a un nuevo dispositivo. Este lapso de tiempo puede ser ampliable mediante métodos de corrección de errores.

4) Tele transportadora de código: La tele transportadora de código es un elemento cuántico que hace parte de la arquitectura computacional cuántica y junto con la transportación cuántica convencional consiguen ejecutar operaciones mientras se transporta los datos cuánticos.

Este mecanismo se usa para la corrección de errores en el codificador de código origen y en el codificador de código destino, como puede observarse en la figura 5. El emisor y el receptor entonces ejecutan qubits lógicos equivalentes en la operación de tele transportación en cada terminal del par ”enredado” (entangled) [7].

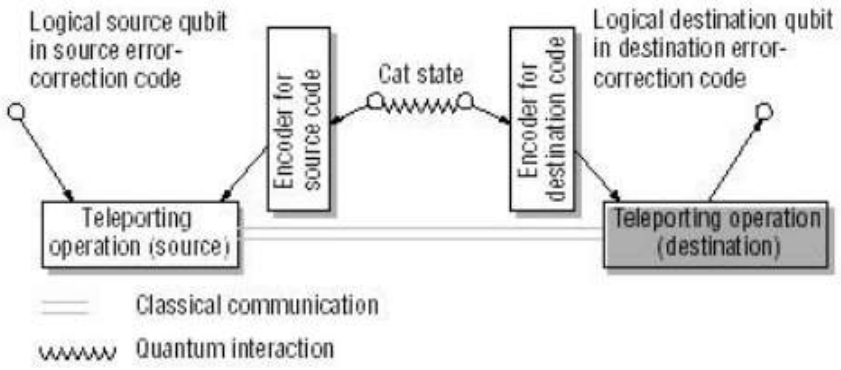

Figure 5: Teletransportadora de código.

5) Planificador dinámico: Oskin et, propone un procesador clásico de alto desempeo como parte principal del planificador dinámico. Este procesador ejecuta un algoritmo de planificación dinámico que toma operaciones cuánticas lógicas, intercaladas con construcciones clásicas de control de flujo, y dinámicamente las traduce en operaciones individuales de qubits físicos [14].

D. Aplicaciones

Sabiendo que las computadoras cuánticas pueden resolver operaciones muy complejas en segundos, esta tecnología se podría emplear para dar respuestas inmediatas como por ejemplo en comunicaciones, prototipos de laboratorio en las ciencias como la química, medicina, entre otras. Así como también en trabajos de investigación y seguridad ya que con estas computadoras se puede trabajar con un mayor número de datos.

A escala empresarial las aplicaciones en este tema son muy importantes, se es capaz de hacer análisis predictivos y estudios analíticos de la información de manera más precisa.

E. Algoritmos

Unos de los algoritmos más conocidos aplicados a la computación cuántica son los algoritmos de Shor y de Grover.

- Algoritmo de Shor: Basado en el método de factorización propuesto por el matemático Peter Shor. Este algoritmo tiene la capacidad de encontrar la descomposición en factores primos de un número en un tiempo que crece linealmente con el tamaño del número a factorizar. [9] Esto es muy útil pues esta misma tarea, descomponer números grandes en factores primos, realizada con computación convencional es ineficiente.

- Algoritmo de Grover: Quizás sea el más conocido por las implicaciones que tiene con respecto a la vulnerabilidad de la criptología tal y como la conocemos. Este es un algoritmo de búsqueda de elementos en listas desordenadas enfocado especialmente en búsquedas pesadas. Es una variante de la bsqueda del periodo de una función. Un ejemplo relativo a la seguridad informática, se tiene una lista de contraseñas almacenadas con encriptación,

por ejemplo, RSA, en algún archivo del sistema. Las personas que pretenden acceder a un sistema protegido de esta manera sin permiso optan por hacer un ataque por fuerza bruta, donde como mínimo, con computación clásica, requeriría un promedio de $N/2$ comparaciones. Con el método de Grove las comparaciones se reducirían a $\sqrt{N}$, sumando los beneficios de la superposición cuántica, el tiempo necesario para encontrar la contraseña correcta sería considerable.

F. Lenguajes de programación

Nuevos lenguajes de programación son necesarios para sustituir a los que están en los ordenadores actuales, puesto que las computadoras clásicas codifican la información en forma binaria con unos y ceros, y las cuánticas con qubits que pueden codificar uno y cero al mismo tiempo.

El más reciente lenguaje de programación proviene de Microsoft, llamado Q#, que junto a una serie de herramientas ayuda a los desarrolladores a crear software. Junto a este se encuentran también QCL, Quipper, entre otros.

Cuando se habla de programación cuántica, existen tres tipos de tecnologías que se han desarrollado. Por un lado, los ordenadores cuánticos analógicos, ordenadores universales, y modelos de ordenamiento cuánticos que comercializa la empresa D-Wave. Estas diferencias de tecnologías hacen que la palabra programar defina diferentes métodos de solución de problemas, ya que un ordenador cuántico es capaz de manejar al mismo tiempo varias soluciones para un mismo problema, gracias a la superposición.

Ante la necesidad de que cada vez más investigadores y programadores se acerquen a esta tecnología, algunas compañías están comenzando a ofrecer herramientas para que las personas comiencen a familiarizarse con estos lenguajes y sus posibilidades [15].

Para poder explotar completamente el poder de una computadora cuántica, los desarrolladores necesitarán estos lenguajes de programación para crear software que aproveche al máximo las capacidades de las computadoras [16].

IV. Conclusiones

- A medida que avanza la tecnología, y en este caso, la computación cuántica, trae muchas ventajas y comodidades como lo son elementos arquitecturales que faciliten la corrección de errores, leer gran cantidad de información sin que se desestabilice el sistema, trabajar en un entorno más veloz.

- El gran salto y desarrollo que nos ha dado la tecnología nos facilita la manera de resolver nuestros problemas en ella. A pesar de su complejidad en todos sus ámbitos, está claro que la computación cuántica a pesar de todas las dudas e interrogantes que ha venido dando con el paso del tiempo, es una promesa para revolucionar la tecnología y resolver problemas millones de veces más rápido que los dispositivos actuales.

REFERENCES

1 contributors, E., "Mecnica cuntica."
2 Vélez, M. and Sicard, A., "Computación cuántica: una perspectiva desde lo continuo," *Revista Universidad EAFIT*, vol. 25, pp. 41–46, 2000.
3 Loss, D. and DiVincenzo, D. P., "Quantum computation with quantum dots," *Physical Review A*, vol. 57, no. 1, p. 120, 1998.
4 S.L., W., "As es el ordenador cuntico de 49 qubits de intel por dentro."
5 Arzabal, M., "Qué es la física cuántica."
6 Perkowitz, S., "La fsica cuntica, para entenderla por fin."
7 Caituiro-Monge, H. and Caituiro, H., "Arquitectura cuántica."
8 Bonillo, V. M., "Principios fundamentales de computación cuántica," *Universidad de La Coruña*, 2013.
9 Miranda, N. D., "Computación cuántica." *Universidad de La Laguna*, vol. 1, pp. 1–89, 2007.
10 Wikipedia, "Puerta cuántica."
11 Linke, N. M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K. A., Wright, K., and Monroe, C., "Experimental comparison of two quantum computing architectures," *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3305–3310, 2017.
12 IBM, "Ibm."
13 HINES, J., "Oak ridge national laboratory."
14 Victoria, P., "Cómo funciona la computacin cuántica, explicado de manera sencilla," 09 2017.
15 Martha, R., "Programador de ordenadores cuánticos: el oficio futurista que nadie quiere aprender," 05 2017.
16 Martin, G., "Computación cuántica busca los nuevos lenguajes que la programarán en un futuror," 01 2018.