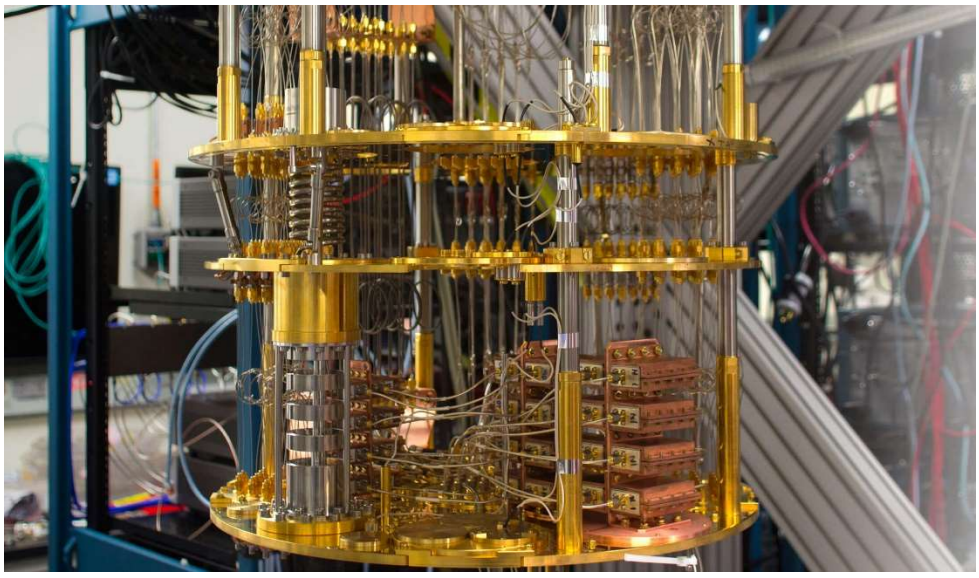
UNIVERSIDAD
DE BURGOS

COMPUTADORES CUÁNTICOS

Arquitectura Avanzada de Computadores



Autores:

David Álvarez Castro

Eduardo Mora González

Contenido

1. INTRODUCCIÓN

A principios del siglo XX, Planck y Einstein proponen que la luz no es una onda continua (como las ondas de un estanque) sino que está dividida en pequeños paquetes o cuantos.

A lo largo de los años otros físicos fueron desarrollando la proposición anterior y llegando a conclusiones sorprendentes, de las cuales al tema que tratamos nos interesarán dos: la superposición de estados y el entrelazamiento.

En ordenadores clásicos la unidad básica de información es el bit, que puede tener dos estados posibles (1/0) y con los que podemos realizar varias operaciones lógicas (AND, NOT, OR). Juntando n bits podemos representar números y operar sobre esos números, pero con limitaciones: sólo podemos representar hasta 2^n estados distintos, y si queremos cambiar x bits tenemos que realizar al menos x operaciones sobre ellos.

Pues bien, la superposición y el entrelazamiento nos permiten reducir esas limitaciones:

- Con la superposición podemos almacenar muchos más que sólo 2^n estados con n bits cuánticos (qubits).
- Con el entrelazamiento se mantiene fijas ciertas relaciones entre qubits de tal forma que las operaciones en un qubit afectan forzosamente al resto.

No obstante, la superposición también es un problema, ya que, aunque tengamos muchos más estados solo podremos leer 2^n distintos (tal y como demostraba Alexander Holevo en 1973).

Esto se debe a que un qubit no vale sólo 1 o 0 como un bit normal, sino que puede ser un 1 en un 80% y un 0 en un 20%. El problema es que cuando lo leemos sólo podemos obtener o 1 o 0, y las probabilidades que tenía cada valor de salir se pierden porque al medirlo lo hemos modificado **[1]**.

2. FUNDAMENTOS FÍSICOS DE LA TECNOLOGÍA CUÁNTICA

En este punto trataremos sobre los distintos fundamentos físicos en los que se basa la tecnología cuántica.

2.1. QUIBT

Benjamín Schumacher –un físico teórico interesado en la teoría cuántica de la información- descubrió, a finales del siglo XX, la forma de interpretar los estados cuánticos como información, y acuñó el término qubit. También descubrió una manera de comprimir la información en un estado y de almacenar la información en el número más pequeño de estados.

Un qubit (del inglés quantum bit o bit cuántico) es un sistema cuántico con dos estados propios y que puede ser manipulado arbitrariamente. También se entiende por qubit la información que contiene ese sistema cuántico de dos estados posibles.

En esta última acepción, el qubit es la unidad mínima y por lo tanto constitutiva de la teoría de la información cuántica. Es un concepto fundamental para la computación cuántica y para la criptografía cuántica, el análogo cuántico del bit en informática. Su importancia radica en que la cantidad de información contenida en un qubit, y, en particular, la forma en que esta información puede ser manipulada, es fundamental y cualitativamente diferente a la de un bit clásico. Hay operaciones lógicas, por ejemplo, que son posibles en un qubit y no en un bit.

Matemáticamente, un qubit puede describirse como un vector de módulo unidad en un espacio vectorial complejo bidimensional. Los dos estados básicos de un qubit son |0> y |1>, que corresponden al 0 y 1 del bit clásico. Pero, además, el qubit puede encontrarse en un estado de superposición cuántica, que es combinación de esos dos estados **[2].**

2.2. REGISTRO CUÁNTICO

Un registro cuántico es un sistema que comprende múltiples qubits. Es el análogo cuántico del registro de procesador clásico. Las computadoras cuánticas realizan cálculos manipulando qubits dentro de un registro cuántico. Registro cuántico Hay una diferencia conceptual entre el registro cuántico y clásico. Un registro clásico de tamaño se refiere a una serie de circuitos que tiene dos estados estables y se puede usar para almacenar información de estado. Un registro cuántico de tamaño es simplemente una colección de qubits.

Además, mientras que un registro clásico de tamaño es capaz de almacenar un valor único de las posibilidades abarcadas por bits puros clásicos, un registro cuántico es capaz de almacenar todas las posibilidades abarcadas por qubits cuánticos puros al mismo tiempo **[3].**

2.3. PARALELISMO CUÁNTICO

La superposición cuántica permite un paralelismo exponencial o paralelismo cuántico en el cálculo, mediante el uso de las compuertas lógicas de qubits. Con una compuerta lógica de un qubit, cuando el qubit de entrada tiene en el estado una superposición igual de ½0> y ½1>, el estado resultante es la superposición de los 2 valores de salida.

Esto quiere decir que para una compuerta lógica de 2 qubits, que tienen dos qubits de entrada en superposición de ½0> y ½1>, tendríamos una superposición de 4 estados y para una compuerta lógica de 3 qubits, que tiene 3 qubits de entrada en superposición de ½0> y ½1>, juntos hacen una superposición de 8 estados, que son evaluados en paralelo. Por cada qubits adicional la cantidad de estados se duplica.

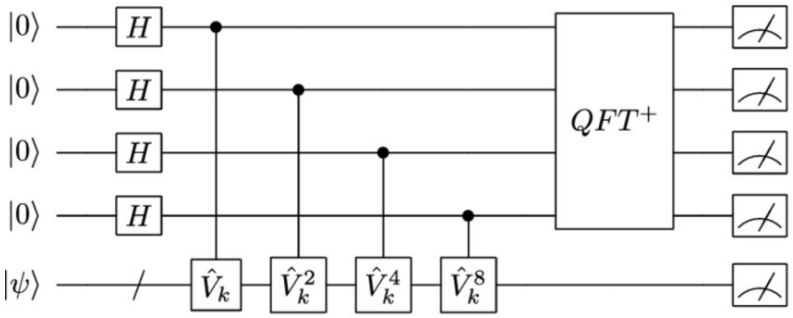
Esto hace que los ordenadores cuánticos sí sean eficaces en el cálculo de periodos, hasta el punto de que se reduce a un tiempo polinómico lo que requeriría un número exponencial de pasos en una máquina clásica **[4].**

2.4. ESTADO DE ENTRELAZAMIENTO CUÁNTICO.

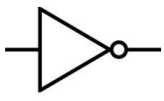
El entrelazamiento es una característica no local que permite que un sistema de qubits se exprese con una correlación más alta que la posible en sistemas clásicos. Un sistema de dos qubits entrelazados no puede descomponerse en factores independientes para cada uno de los qubits **[2].**

2.5. PUERTAS LÓGICAS CUÁNTICAS

Las puertas lógicas cuánticas son conceptualmente análogas a las clásicas: reciben un registro de qubits en un determinado estado, y aplican una operación sobre el mismo, para transformarlo.

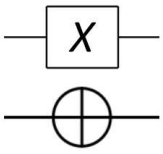


Se representan por matrices cuadradas y unitarias. Además, a diferencia de la mayoría de las puertas lógicas clásicas, son reversibles.

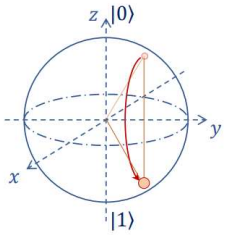


Y	NOT(Y)
0	1
1	0

Puerta NOT clásica



Y	NOT(Y)
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|\psi\rangle$	$X(\|\psi\rangle)$



$Pauli - X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Puerta NOT cuántica

Las puertas cuánticas pueden aplicarse condicionadas al estado de otros qubits, que actúan como controles **[5].**

2.6. LA COMPUTADORA CUÁNTICA DE FEYNMAN

El modelo de Feynman es una versión cuántica de un circuito lógico combinacional.

Se describe la computación a realizar a nivel de circuito, construyéndolo con puertas cuánticas reversibles. En general, podemos entender el circuito como k puertas lógicas actuando sobre m qubits. La transformación conseguida por el circuito puede ser escrita como Ak·Ak-1·...·Ai, donde Ai es un operador que describe la acción de la puerta i-ésima.

Para realizar la composición de matrices Ai hacemos lo siguiente: Sean los |n| átomos del registro. Añadimos un conjunto nuevo de |k+1| átomos que configuran lo que vamos a llamar el contador de posiciones del programa. Denotamos como <qi> al operador de aniquilación de la posición |i| y como <q*i> al operador de creación de la posición |i|, de tal forma que ambos operan desde |i = 0| hasta |i = k|. Necesitamos ahora un electrón cambiando continuamente de una posición a otra. Así, si en un instante dado una posición está vacía el estado de esa posición es |0>, y si en un estado dado una posición está ocupada el estado de esa posición es |1>. Con este planteamiento Feynman propone como Hamiltoniano:

H = SUMA (i=0 -> k-1) <q*i+1> <qi> Ai+1 + Complejo Conjugado

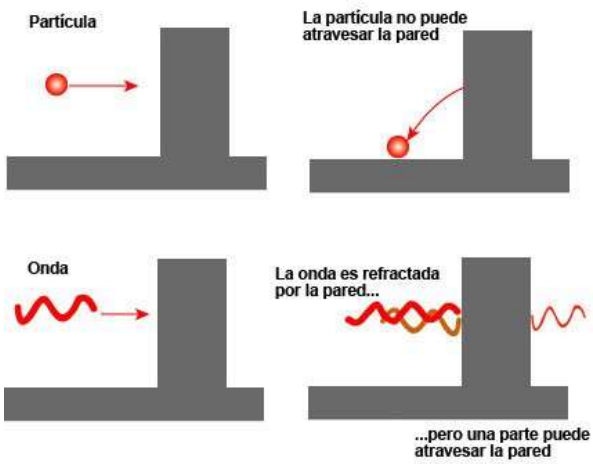
Si todas las posiciones del programa están libres, entonces todos los átomos del programa están en el estado |0>, por lo tanto, no hay cambios ya que cada término del Hamiltoniano comienza con un operador de aniquilación.

Esto significa que la expresión para H sólo es cierta cuando una y sólo una de las posiciones del programa está ocupada. Como consecuencia de lo anterior el número de posiciones del programa en estado |1> es siempre el mismo.

Además, durante el proceso de cómputo sólo puede ocurrir que no haya posiciones ocupadas –en cuyo caso no pasa nada, o que sólo haya una posición ocupada en cuyo caso se realiza una computación elemental. Por otra parte, durante un proceso normal de cómputo, dos o más posiciones de programa no pueden estar ocupadas simultáneamente **[6].**

3. SOLUCIONES TECNOLÓGICAS PARA SU IMPLEMENTACIÓN

Hasta este apartado hemos visto de forma básica los fundamentos físicos de la mecánica cuántica utilizada y se han presentado los bits cuánticos (qubits) y su capacidad de superposición. Si los qubits se encuentran en superposición y entrelazados entre sí, la computación puede funcionar de una manera mucho más rápida que la clásica.



Actualmente, la tecnología utilizada en la construcción de computadores cuánticos es muy complicada de fabricar ya que requieren de unas ciertas características muy complicadas y/o complejas en una situación normal:

- Temperaturas cercanas al cero absoluto (-273 ºC),
- Mecanismos muy frágiles.
- Aislamiento total o casi total del entorno.
- Protección contra la radiación para que los estados de los qubits no varíen.

Todos estos factores son esenciales a la hora de construir un supercomputador debido a la gran sensibilidad e inestabilidad que suelen ser los qubits. Debido a esto es necesario ese aislamiento del exterior y esa protección contra la radiación que se encuentra en el ambiente. Pero es importante recordar que es la propia inestabilidad de los qubits lo que genera esa potencia de cómputo en este tipo de computadores.

Otro aspecto crucial para mantener los qubits estables es la propia temperatura a la que se encuentran. Como se ha indicado anteriormente, los computadores cuánticos operan a temperaturas cercanas al 0 absoluto debido, otra vez, a la propia inestabilidad de los propios qubits. Este aspecto es primordial para su correcto funcionamiento, un método bastante revolucionario llevado a cabo por IBM **[7]** consiste en la refrigeración por efecto túnel **[8]** atravesando un electrón una barreara gracias a que éste puede funcionar tanto como una partícula como una onda.

Si al otro lado de la barrera hay más energía, un electrón con poca energía traspasará la barrera formada por un aislador de 2 nanómetros de espesor. Lo curioso de este efecto es lo siguiente, al entrar en contacto con los diferentes qubits que formen el procesador cuántico, los electrones rebotarán llevándose todo el calor generado por lo qubits y enfriándolos en su defecto. Existen otras investigaciones muy interesantes y con resultados bastante esperanzadores como puede ser la refrigeración láser **[9]** o el desagüe de partículas calientes.

De todas formas, conforme pase el tiempo se espera que la temperatura de funcionamiento de los qubits aumente de forma considerable permitiendo ahorrar miles de euros en equipos de refrigeración **[10]**.

Por lo tanto, la fabricación de estos dispositivos es generalmente un proceso muy difícil y, especialmente, costoso; además de que cuantos más qubits se quieran añadir a la potencia de cómputo, mayor el desafía la hora de comprobar que se cumple el entrelazamiento entre qubits (actualmente sigue siendo muy complicado de probar que existe en un computador cuántico **[11]**) y la superposición de estados (características fundamentales para que se considere computación cuántica). Por lo tanto, si las perturbaciones del medio (ruido, radiación, calor, …) modifican qubits en superposición y los lleva al típico estado de los bits clásicos, o si se rompe el entrelazamiento entre un clúster de qubits, el computador no será clasificado como cuántico si no de un computador no cuántico muy caro que puede solo ejecutar un limitado número de algoritmos (con unos resultados no muy fiables).

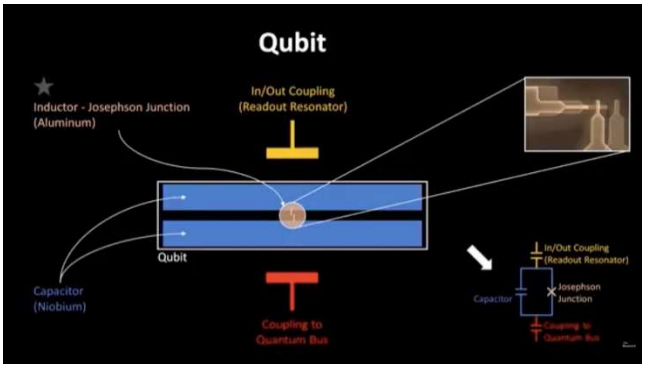
Los qubits son elemento central de la computación cuántica debido a sus características tan diferenciadas. Conseguir estos aspectos no es posible utilizando la misma tecnología que la utilizada en la computación clásica. Hoy en día no existe una única tecnología a la hora de abordar la construcción de un ordenador cuántico debido a que nos encontramos en una etapa muy temprana y de pleno desarrollo de nuevas formas y alternativas a la hora de afrontar este problema; cada una con sus ventajas e inconvenientes. Se presentarán a continuación una lista formada por las tecnologías más usuales en los actuales ordenadores cuánticos.

3.1 SUPERCONDUCTORES

Grandes empresas como IBM (en sus modelos D-Waves **[12]**) o Google (en sus procesadores cuántico Sycamore **[13]**) están utilizando tecnologías en microelectrónica basadas en superconductores como núcleo para sus computadores cuánticos.

Es importante destacar que el ordenador de Google recientemente ha confirmado haber alcanzado la supremacía cuántica **[14]**, lo que hace referencia a que un dispositivo de computación basado en computación cuántica ha conseguido superar, en términos de computación, al mejor de los supercomputadores actuales del Top500 y consigue resolver problemas imposibles para la computación clásica.

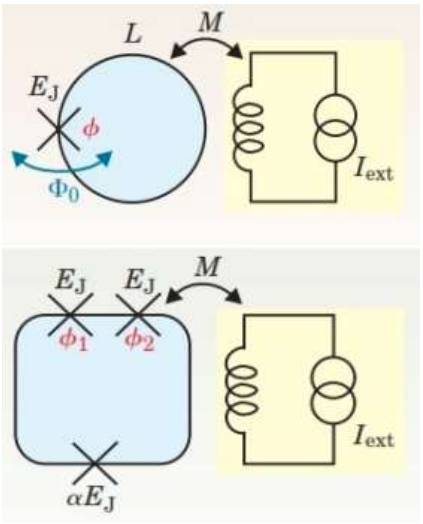
En este tipo de tecnología, los circuitos eléctricos utilizan materiales con poca resistencia como el aluminio. Las temperaturas están próximas al cero absoluto, gracias al uso de helio líquido, consiguiendo disipar todo el calor generado por los qubits durante el cómputo de algoritmos para no influir y degradar la información de los estados. Cada qubit es un circuito formado por un condensador eléctrico y una bobina, para obtener la superposición de |0> y |1> se manipula el estado de energía. Las uniones de Josephson **[15]** son muy importantes en esta tecnología para crear lazos cerrados interrumpidos por una o más secciones muy finas de aislante (referencia a figura uniones Josephson) a través del que se establece un corriente túnel evitando estados superiores.



Este circuito se comporta como un átomo con dos niveles de energía, es decir, funciona perfectamente como un qubit cuántico con superposición de estados. Dentro de esta tecnología existen variantes.

3.1.1. QUBITS DE FASE

Estos qubits están formados por una unión Josephson a través de la cuál pasa una corriente continua que produce una caída de potencial reduciendo el número de estados enlazados en el pozo de energía, como ya se había comentado antes.

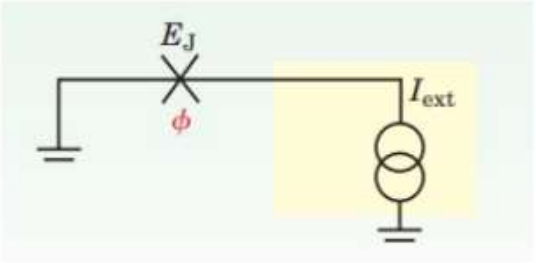


Para medir las probabilidades de ocupar cada estado es necesario estimular el qubit con un pulso de microondas a una frecuencia determinada dando lugar una transición:

- Si estimulamos el estado |1> se dará una transición (excitación) de ese estado al |2> dando lugar al efecto túnel, lo que hará que la unión se comporte como un circuito abierto pasando por ella un cierto voltaje (estado de voltaje no nulo),
- Si estimulamos el estado |0>, no se produce una excitación y por lo tanto no se produce ninguna transición de estado.

3.1.2. QUBITS DE FLUJO MAGNÉTICO

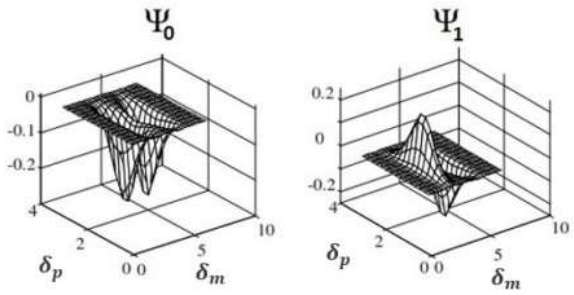
Estos qubits se pueden definir como un lazo superconductor interrumpido por una o tres uniones Josephson (figura de qubit de flujo) al que se le aplica un pequeño campo magnético induciendo una corriente persistente de doble sentido (horario o antihorario) dependiendo del flujo magnético aplicado. La superposición de estados en este tipo de qubits es gracias al acoplamiento débil de las uniones.



Los qubits de flujo de una unión necesitan una inductancia relativamente grande, lo que provoca mayor sensibilidad al ruido producido por el campo magnético; por ello los qubit de flujo de tres uniones son más eficientes en términos de energía y sensibilidad a cambios de estados.

Cuando se aplica un campo magnético a través del lazo se induce una corriente eléctrica en sentido horario (disminuye el flujo) o antihorario (aumenta el flujo) lo que

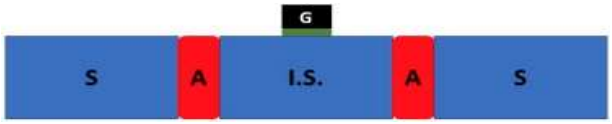
provoca dos estados: flujo magnético apuntando hacia arriba y hacia abajo. En la Imagen (referencia a imagen funciones de ondas de los estados fundamentales) se puede apreciar la representación de los estados:



Se puede medir de forma muy sencilla el estado en el que se encuentra un qubit de flujo mediante un SQUID DC **[16]**.

3.1.3. QUBITS DE CARGA

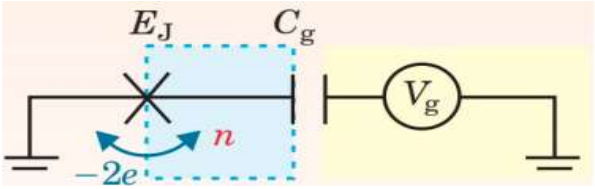
El concepto de isla superconductora se define como un electrodo de material superconductor separado del resto gracias a materiales aislantes y al que se le acopla otro electrodo que será el que controle la entrada y salida de electrones superconductores al aplicar cierto voltaje. La imagen muestra materiales conductores (S) separados por dos materiales aislantes (A), que de forma conjunta envuelven a la ista superconductora (IS)



En este tipo de qubits los estados |0> y |1> se corresponden con N pares de Cooper **[17]**. Al cambiar el voltaje aplicado a la puerta se consigue que un par de Cooper entre o salga de la isla modificando el número de electrones contenidos (*n*) a *n* + *2* o *n* – *2*.

A este sistema se le conoce como una caja de pares de Cooper (CPB) donde los estados difieren en dos electrones acoplados mediante el efecto túnel provocado por las pares a través de la unión. Esto sistema es un qubit de carga, y la siguiente imagen muestra de forma esquemática su circuito donde la caja azul representa una

CPB controlada por un voltaje de puerta, y una unión Josephson que conecta la caja con el exterior:



La CPB funciona de forma análoga a una instalación de fontanería. La caja CPB representa un tanque de agua (un tanque de electrones) que entra y sale mediante una bomba (fuente de voltaje) que mueve el agua a través de una válvula (unión Josephson) y por el interior de un cable superconductor. En ciertas ocasiones se suele cambiar la unión por dos uniones unidas a un segmento de anillo superconductor.

En cuanto a los estados, si el desplazamiento de las cargas de la caja (inducido por el voltaje de la puerta) es parecido a la carga de un electrón, solo existen dos estados de carga (|0> y |1>):

- |0> representan la ausencia de pares de Cooper extra en la CPB
- |1> representa que hay un par de Cooper extra.

En conclusión, tenemos que la unión Josephson permite a los pares de Cooper hacer un efecto túnel hacia la isla de uno en uno. El acoplamiento resultante entre los estados de carga vecinos |n> y |n+1> crea una similitud con los estados cuánticos que se introdujo en el qubit de flujo:

- |n> es equivalente al flujo apuntando hacia abajo
- |n + 1> es equivalente al flujo apuntando hacia arriba

Se presentaron algunos de los subtipos de qubits superconductores de forma muy simple sin entrar en muchos aspectos matemáticos y físicos **[18].**

3.2 TRAMPA DE IONES

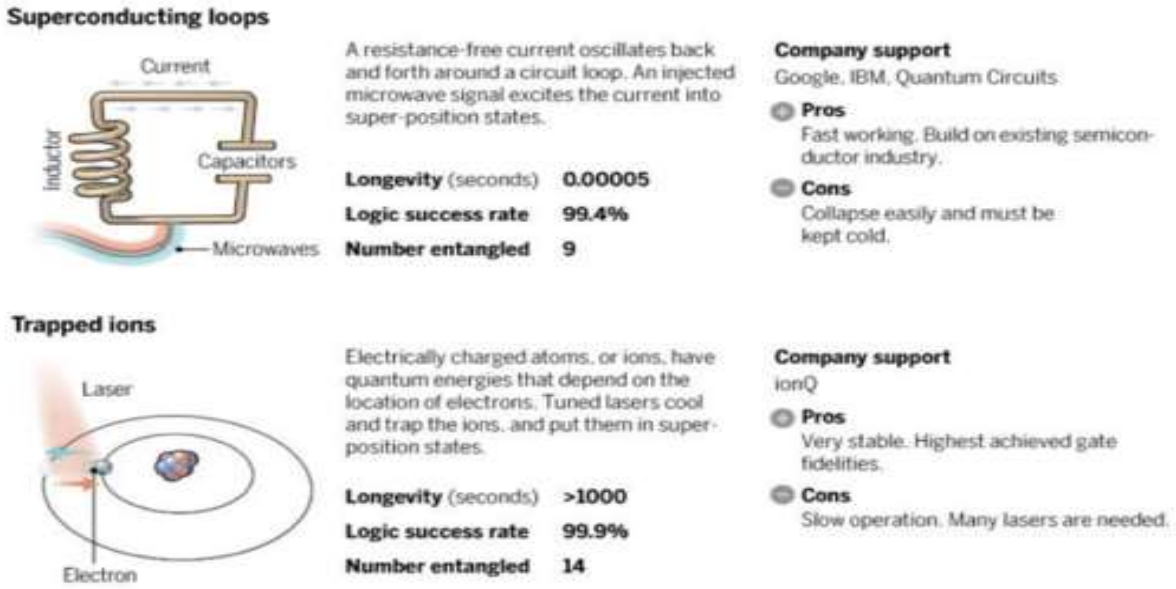
Esta tecnología consiste, en como su nombre indica, en atrapar iones utilizando campos magnéticos o eléctricos para conseguir que se comporten como qubits. Con el fin de aislarse del exterior reduciendo el ruido ambiental se introducen en una cámara de vacío.

Los iones son átomos que tienen una carga eléctrica (se suelen utilizar iones de calcio o de iterbo cargados positivamente), para lograr el estado de superposición es necesario enfriarlos para inducir que los estados del qubit se acoplen entre sí. En esta técnica, a diferencia que, en los superconductores, no se utiliza helio líquido para conseguir temperaturas tan bajas, se aplica un láser (lo que resulta a largo plazo más económico).

Los láseres utilizados en estos dispositivos permiten reducir el ruido y provoca que los qubits se queden en un estado casi estacionario, consiguiendo que sean fáciles de manipular. A diferencia de los modelos de IBM (basados en qubits superconductores), estos equipos no necesitan de grandes equipos criogénicos para refrigerar el computador porque solo es necesario refrigerar el procesador.

No solo se utiliza un láser para enfriar los procesadores, es necesario también para poder realizar las lecturas de estado. Después de la ejecución de un cálculo es necesario utiliza un láser en todos los iones al mismo tiempo para medir el estado de los qubits.

La Imagen (referencia comparativa) **[19]** muestra una comparativa en términos de eficiencia y durabilidad entre los supercomputadores y los de iones atrapados. La principal ventaja de utilizar qubits basados en esta tecnología es amplia vida útil, así como el gran control que se tienen de los iones gracias al láser (permitiendo mantener los qubits estables y controlables durante mucho tiempo).



Otras de las ventajas de la trampa de iones es que todos los átomos son iguales, mientras que los fabricados con materiales superconductores tienen pequeñas diferencias que pueden aumentar el error y empeorar la estabilidad.

El principal problema de esta tecnología es la velocidad de las operaciones; para llegar a velocidades parecidas a los de materiales superconductores se necesitarían muchos láseres. Todo esto lo convierte en una tecnología bastante cara, al igual que la tecnología competidora de superconductores.

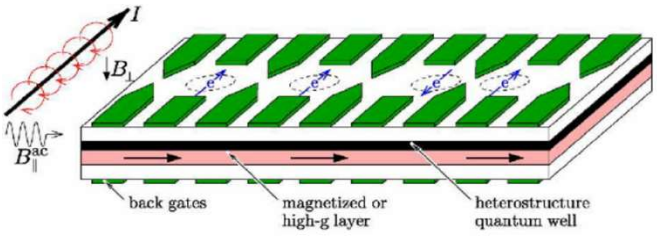
3.3 PUNTOS CUÁNTICOS

También conocidos como los qubits de espín, es una tecnología que permite confinar electrones de manera individual **[20]**. Cada uno de estos electrones se utiliza como un qubit, y se utiliza luz polarizada o campos magnéticos o eléctricos para permitir su manipulación.

Esta teoría ya se postulaba a finales de los 90 **[21]** con una propuesta que consistía en utilizar los giros del electrón (el espín) como bits cuánticos. Al confinar los electrones, cada uno de ellos se encuentran orbitando un punto cuántico de forma similar a como lo hacen los átomos; lo que supone que ocupa una serie de posiciones en el punto, trazando una órbita siguiendo los postulados de la mecánica cuántica (Esfera de Bloch). Los posibles resultados son:

- Si el electrón gira hacia arriba (*spin-up*), el estado será |1>, y
- Si el electrón gira hacia abajo (*spin-down*), el estado será |0>.

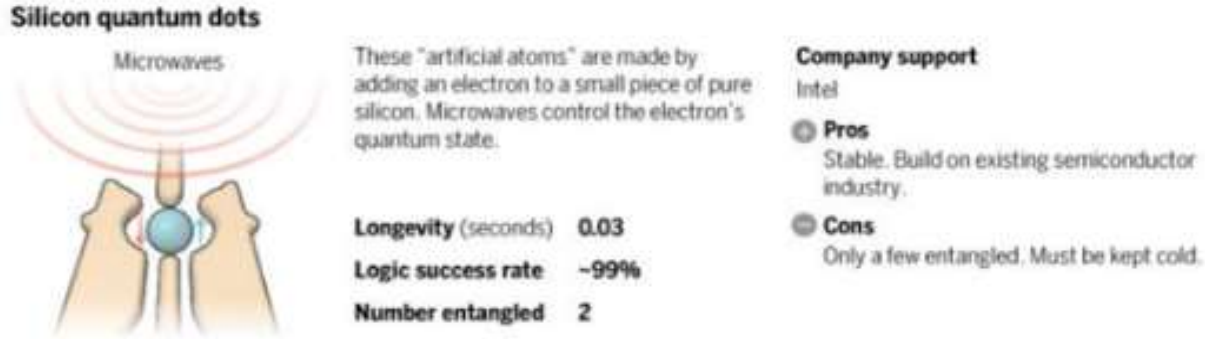
En la Figura **[22]** se muestra un esquema muy básico basado en la propuesta de Loss-DiVicenzo. Las compuertas superiores se utilizan para acercar o alejar electrones (variando el voltaje) y controlar la interacción entre ellos.



Gracias a estas compuertas se pueden aislar, de forma sencilla e individual, los electrones para formar los puntos cuánticos. El giro del electrón será el qubit, y al moverse de forma individual la medición de la corriente que produce es bastante sencilla.

Para manipular los estados de los qubits (giro de los electrones en el plano y), es necesario aplicar un campo magnético perpendicular a las compuestas (representado por B_0 en la figura).

Un aspecto para tener en cuenta cuando se utiliza esta tecnología para disponer de varios qubits es que los puntos cuánticos tienen que ser lo más idénticos y uniformes posibles. La siguiente Figura **[23]** muestra las principales ventajas y desventajas de esta tecnología:



Aunque consiguieron aumentar la temperatura de funcionamiento en comparación con los materiales superconductores, todavía se necesitan temperaturas criogénicas para su funcionamiento; por lo que ambas tecnologías siguen siendo bastante caras.

Los principales desafíos a la hora de utilizar esta tecnología son la inicialización de los estados de movimiento del ion y la vida relativamente breve. Así mismo pueden darse casos de decoherencia cuando, por cualquier razón, los iones interactúan con el exterior.

Por lo tanto, un punto cuántico se puede definir de forma simple como una estructura semiconductora que es capaz de contener un electrón es estados discretos. Por este motivo también se les llama *átomos artificiales*.

Si en el caso de IBM y Google optaban por la tecnología cuántica basada en materiales superconductores, Intel destaca en investigaciones en qubits de espín. Por ejemplo, se conoce que Intel está utilizando tecnología basada en matrices bidimensionales de puntos cuánticos en piezas de silicio para obtener procesadores de 1024 qubits.

3.3.1. ESPINES NUCLEARES (NMR)

También denominados qubits por resonancia magnética nuclear, utiliza los estados de espín de los núcleos dentro de las moléculas. Los estados de la molécula se comprueban a través de una resonancia magnética nuclear, lo que permite que el sistema se comporte como una variación de la espectroscopia de RMN. Existen dos tipos diferenciados: lo NMR de estado líquido (LSNMR) y los de estado sólido (SSNMR); siendo la principal diferencia el estado elemental en la que se encuentra la molécula, además de las ventajas que presentan los qubits SSNMR sobre los LSNMR (mayor precisión en la localización, mediciones de qubits individuales, supresión de la decoherencia, …). Desde los primeros días, se reconoció que los computadores cuánticos de NMR nunca serían muy útiles debido a la escasa escala de la relación señal-ruido.

3.3.2. FOTONES+CAVIDADES

Los fotones son un transporte ideal para los qubits **[24]**, pero es imposible controlar y realizar operaciones sobre ellos. Para ello se hace uso de cavidades ópticas para la interacción fotón-átomo, lo que nos va a permitir implementar las puertas lógicas y el almacenamiento de los estados del qubit. Los principales problemas que tiene son que se necesitaba controlar la interacción del fotón dentro de la cavidad y que para evitar la decoherencia este acople tiene que ser muy fuerte, lo que solo se consigue con cavidades ópticas muy pequeñas y reflexivas.

4. ALGORITMOS CUÁNTICOS RELEVANTES

Un algoritmo en computación cuántica se puede definir como una sucesión ordenada de puertas cuánticas (comentadas en le Sección de Fundamentos físicos) y mediciones aplicadas a un registro de n qubits. Por lo tanto, cada etapa de un algoritmo está definido por una puerta lógica que es en esencia una transformación unitaria en el espacio de Hilbert.

Para simular un algoritmo cuántico, después de haber inicializado la máquina de estados y sus qubits, es necesario aplicar las diferentes transformaciones unitarias indicadas.

Debido a que la medición de resultados es meramente probabilística, es necesario disponer de un generador de números aleatorios. Por ello se afirma que los algoritmos cuánticos son probabilísticos y con facilidad de aplicación del paralelismo cuántico; lo que realmente resulta complicado es conseguir que la probabilidad del resultado objetivo sea elevada.

Los siguientes apartados tratarán de introducir y explicar tres algoritmos con gran relevancia histórica en la computación cuántica.

4.1 ALGORITMO DE DEUTSH-JOZSA

El propósito de este algoritmo es determinar si una función de tipo caja negra (por ejemplo, f: {0, 1} ^n → {0, 1}) es constante o balanceada. Dicho de una forma más sencilla, dada una función de entrada de n bits con una salida representada en un bit, determinar si esta salida obtenida es independiente totalmente de la entrada o si el posible resultado es la mitad ceros y la otra mitad unos; utilizando un solo paso de cómputo.

Los pasos seguidos para la resolución son muy parecidos a los aplicados para resolver en el algoritmo de Deutsch, pero con fórmulas matemáticas un tanto más complejas.

4.1.1. ALGORITMO DEUTSCH

El objetivo de este algoritmo es "*determinar si se puede saber si una función de caja negra del tipo f: {0, 1} → {0, 1} es constante o no, lo que equivale a decir que la salida pertenece a {0,1} (función constante) o a {0} (no constante)".*

4.2 ALGORITMO DE GROVER

Es el primer algoritmo que muestra una clara superioridad en la búsqueda de estructuras no estructuras (no se puede realizar ninguna hipótesis relativa a la estructura del espacio de soluciones) de tamaño *N,* utilizando computación cuántica sobre la clásica **[25]**: "*hallar un número x en un conjunto posible* $C=\{x_1,x_2,x_3,x_4, \ldots, x_n\}$ *tal que la sentencia f(x)=1 sea cierta*".

La diferencia con la búsqueda estructurada clásica es que no se puede utilizar la estructura ordenada del conjunto para aplicar algoritmos eficientes, es necesario comprobar aleatoriamente la veracidad de la sentencia.

4.3 ALGORITMO DE SHOR

La factorización de números enteros es un problema actual, especialmente en el ámbito de los sistemas criptográficos de clave pública (RSA), muy complejo de ejecutar mediante ordenadores clásicos (debido a los elevados tiempos de cómputo). La seguridad de RSA radica en la imposibilidad práctica de factorizar números muy grandes. Gracias al algoritmo cuántico propuesto por Shor **[26]** se ha conseguido resolver tanto el problema de la factorización de un número entero muy grande, así como el problema del logaritmo discreto. El algoritmo se compone de dos partes **[27]**:

- Una primera parte convierte el problema de encontrar un factor propio en un problema de encontrar el periodo de una función (computación clásica).
- Una segunda parte que encuentra el periodo utilizando QFT (transformada cuántica de Fourier) acelerando el proceso (computación cuántica).

5. VENTAJAS DE LA TECNOLOGÍA

La computación cuántica presenta una serie de ventajas en distintos campos, algunas de estas ventajas son **[36]**:

- Tiene muchas aplicaciones en situaciones de la vida diaria. Por ejemplo, la medicina es el campo que puede tener muchos avances.
- La computación cuántica puede permitir avanzar en la investigación en química.
- Es beneficiosa para la búsqueda y desarrollo de fuentes alternativas de energía.
- La computación cuántica puede ser beneficiosa para frenar el cambio climático.
- Es clave para el desarrollo del aprendizaje automático y la inteligencia artificial.

6. EJEMPLOS DE APLICACIÓN

Lo cierto es que no hay muchos algoritmos (y mucho menos aplicaciones "reales") cuánticos que exploten toda la capacidad computacional que se espera que tengan estos ordenadores.

Aunque recientemente se haya confirmado la supremacía cuántica **[28]** gracias a las investigaciones realizadas por el departamento de Quantum Computing de Google, quedan muchas mejoras a nivel de procesamiento, así como de soluciones reales y visibles en nuestro día a día (grandes problemas financieros, problemas farmacéuticos, físicos y un gran número de problemas más).

Aunque mucha gente (tanto relacionados con el mundo de la informática, como los ajenos a ella) piense que la computación cuántica se centra solo y exclusivamente en un área muy específica como puede ser la optimización de problemas **[29]** o la resolución exclusiva de problemas imposibles de resolver [nota pie de página: áreas donde la computación clásica necesitaría de miles de millones de años en resolver estos problemas y que ejecutándolos en un computador cuántico se podrían resolver en cuestión de horas y/o minutos], existen una multitud de ámbitos de la computación donde aplicarlos.

5.1. CIBERSEGURIDAD

Tanto los datos personales como su seguridad seguirán siendo activos importantes para empresas y consumidores (y por lo tanto una excelente fuente de ingresos para crackers), y más actualmente donde muchos de estos datos están almacenados en la nube.

A medida que la dependencia de los datos por parte de los usuarios vaya aumentando, la necesidad de privacidad será proporcional a esa dependencia. La computación cuántica permitirá la implementación de algoritmos de cifrado muchísimo más potentes que los actuales; así como conseguir romper gran parte de la criptografía usada ahora mismo **[30]**.

5.2. MACHINE LEARNING

Gracias a la combinación de machine learning y computación podemos optimizar y mejorar bastante los modelos que, debido a la falta de potencia actual, estaban limitados **[31].**

Gracias a esta mejora, se podrán obtener resultados imposibles hasta ahora en áreas como la genética, reconocimiento de patrones o conducción autónoma **[32]**.

5.3. MEDICINA

Tareas como el diseño y desarrollo de medicamentos a medida o la propia manipulación molecular pueden ser tareas bastante complejas con la tecnología actual que pueden ser una realidad con la explotación de los computadores cuánticos. Gracias a técnicas como la óptica cuántica se podría conseguir aislar y controlar moléculas de forma individual **[34]**.

5.4. SERVICIOS FINANCIEROS

Con el paso de los años, la complejidad en la actividad comercial de los mercados financieros se está disparando: miles de millones de datos y transacciones por segundo.

Problemas como las simulaciones financieras llevadas a cabo por el algoritmo Monte Carlo podrían reducirse en varios órdenes de magnitud el grado de gestión y optimización de los niveles de riesgo en inversiones llevadas a cabo por clientes de entidades financieras (*Risk profiling*) que suele ser crítico en las entidades hoy en día (gestión de la liquidez, precios de los derivados y la medición de riesgo son procesos complejos con cálculos difíciles de realizar) **[34]**.

5.5. INDUSTRIA QUÍMICA

Existen muchos problemas que actualmente no pueden ser resueltos por un ordenador normal o un supercomputador, como puede ser la identificación de un catalizador para fertilizantes que permita reducir los gases de efecto invernadero ayudando a la producción mundial de alimentos **[35]**.

Otros casos de uso podrían ser la expansión en la producción de nuevos yacimientos o la simulación de reacciones químicas complejas.

7. CONCLUSION

Se espera que los computadores cuánticos se apliquen en una multitud de ramas para optimizar y mejorar los tiempos de procesamiento y poder obtener resultados imposibles actualmente.

Además, la realización de este trabajo nos ha ayudado a conocer mas en profundidad un tema bastante actual y que puede ser un futuro inmediato.

REFERENCIAS Y BIBLIOGRAFÍA

1. https://www.xataka.com/ordenadores/computacion-cuantica-que-es-de-donde-viene-y-que-ha-conseguido
2. https://enginyeriainformatica.cat/wp-content/uploads/2016/05/PRINCIPIOS-FUNDAMENTALES-DE-COMPUTACI%C3%93N-CU%C3%81NTICA.pdf
3. https://es.qaz.wiki/wiki/Quantum_register
4. https://501computocuantico.weebly.com/paralelismo-cuaacutentico.html
5. https://www.etsisi.upm.es/sites/default/files/curso_2017_18/MASTER/61AD/material7_rafaelmartin_seminv_2017-18.pdf
6. https://es.wikipedia.org/wiki/Computadora_cu%C3%A1ntica_de_Feynman
7. https://www.adslzone.net/2017/05/10/asi-consiguen-refrigerar-los-ordenadores-cuanticos-sin-ventiladores/
8. http://www.astronoo.com/es/articulos/efecto-tunel.html
9. https://cordis.europa.eu/article/id/34238-laser-cooling-of-semiconductor-membranes-opens-doors-for-quantum-computing/es
10. https://www.investigacionyciencia.es/noticias/lgica-cuntica-caliente-la-computacin-cuntica-encara-el-obstculo-de-la-temperatura-18532
11. https://arxiv.org/abs/1401.3500
12. https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware
13. https://www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html
14. https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html
15. https://www.scientificamerican.com/article/what-are-josephson-juncti/
16. C. H. van der Wal, A. C. J. ter Haar, F. K. Wilhelm, R. N. Schouten, C. J. P. M. Harmans, T. P. Orlando, S. Lloyd y J. E. Mooij, Quantum superposition of macroscopic persistentcurrent states, Science, 290 773 − 777, (2000)
17. http://hyperphysics.phy-astr.gsu.edu/hbasees/Solids/coop.html
18. https://digital.csic.es/bitstream/10261/223815/1/dispocuanti.pdf
19. https://sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one
20. Björn Trauzettel, Denis V. Bulaev, Daniel Loss & Guido Burkard, Spin qubits in graphene quantum dots, Nature Physics volume 3, pages192–196(2007)
21. Daniel Loss and David P. DiVincenzo, Quantum computation with quantum dots, Phys. Rev. A 57, 120, 1998

22. https://www.researchgate.net/publication/45858177_Quantum_Computing_with_Electron_Spins_in_Quantum_Dots
23. https://conventional one. sciencemag.org sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one
24. https://tendencias21.levante-emv.com/controlan-la-forma-de-los-fotones-y-abren-la-via-para-una-internet-cuantica_a39205.html
25. Grover, L.K. A fast quantum mechanical algorithm for database search. Proceedings of the 28th ACM Symposium on the Theory of Computing (1996), pp. 212--219 (arXiv:quant-ph/9605043)
26. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26 (1994) pp.1484--1509 (arXiv:quant-ph/9508027)
27. García López, J. Factorización polinomial de números enteros, La Gaceta de la RSME, 7 (2004), pp. 517--537
28. https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html
29. https://www.youtube.com/watch?v=S52rxZG-zi0&ab_channel=IBMResearch
30. https://www.computing.es/seguridad/noticias/1122304002501/ibm-se-apunta-ciberseguridad-cuantica.1.html
31. https://www.elespanol.com/invertia/disruptores-innovadores/innovadores/tecnologicas/20200309/google-eleva-machine-learning-cuantico-codigo-abierto/473454296_0.html][https://venturebeat.com/2020/03/09/google-launches-tensorflow-quantum-a-machine-learning-framework-for-training-quantum-models/
32. https://www.futurebridge.com/industry/perspectives-mobility/quantum-computing-a-key-to-autonomous-vehicle-industry-success/
33. Shapiro, M. and Brumer, P., *Principles of the Quantum Control of Molecular Processes*. 2003, p. 250.
34. https://www.bbva.com/es/computacion-cuantica-que-puede-aportar-al-sector-financiero/
35. https://youtu.be/qarc7AA4-wM
36. https://futuroelectrico.com/computacioncuantica/#Ventajas_de_la_computacion_cuantica