1

Computación cuántica

El incremento de la integración de componentes en los microprocesadores está llegando a un punto en el que fenómenos cuánticos tienen lugar haciendo que sea imposible seguir en esta línea de avance.

La computación cuántica se presenta como la alternativa para un futuro no muy lejano en el que se trata directamente con las propiedades cuánticas de las partículas para realizar el procesamiento de la información.

En la sección 1 se hace una pequeña introducción y se comenta el fenómeno que impide se siga aumentando el grado de integración. En la sección 2 se tratan los fundamentos teóricos de la computación cuántica. En la sección 3 se habla sobre distintos aspectos de la computación cuántica como las posibles arquitecturas o los algoritmos y su potencia en comparación con el paradigma de computación clásica.

Alejandro Avilés del Moral

cc BY NC SA

1.1 Introducción

Hasta ahora, el principal avance en la capacidad de computación se ha derivado de una mayor integración de transistores en los microchips, pero el nivel de miniaturización está aproximándose a los límites físicos que mantienen la coherencia de la información del sistema.

Esta limitación es consecuencia directa de las propiedades cuánticas que presentan los electrones, los cuales se comportan como ondas y pueden escapar de sus confinamientos físicos a escala de nanómetros. Este efecto es conocido como efecto túnel.

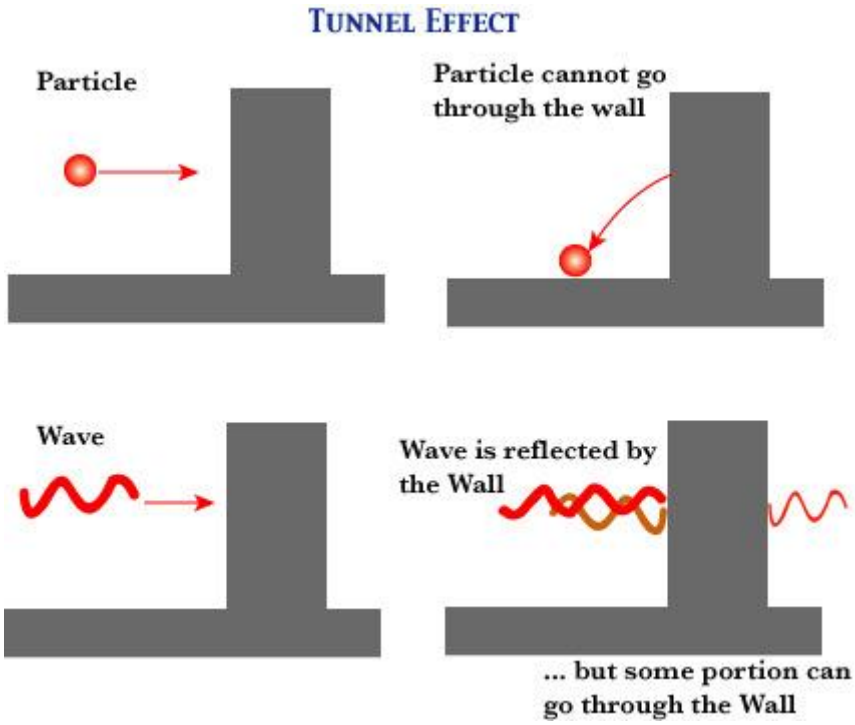


Figura 1.1: Representación gráfica del efecto túnel. En la parte superior ilustra el comportamiento en la mecánica clásica y en la inferior el de la cuántica.

El efecto túnel explica el comportamiento anómalo que presentan las partículas a escalas cuánticas, violando las leyes de la mecánica clásica. A dicha escala las partículas tienen un comportamiento ondular que, en el ámbito de la computación, implica que un electrón al chocarse con una barrera de potencial (la pared de la imagen) puede llegar a atravesarla, perdiendo su significando y

provocando un comportamiento arbitrario en los microchips, imposible de controlar.

Parece obvio que el avance tecnológico debe tomar un nuevo rumbo que sortee estos problemas y para ello es necesario adoptar un paradigma capaz de enfrentarse a limitaciones cuánticas. Es así como surge la idea de la computación cuántica, aplicando las leyes de la mecánica cuántica en la teoría de la información y computación.

1.2 Fundamentos teóricos

Antes de embarcarse en las explicaciones más cercanas al ámbito computacional se explicarán de forma superficial los fundamentos que hacen posible la computación cuántica.

1.2.1 Mecánica Cuántica

Para hablar sobre cuestiones más cercanas a la computación cuántica considero necesario comentar algunos hitos teóricos e interpretaciones que se hacen de la mecánica cuántica, las cuales dieron lugar a su posterior aplicación en las ciencias de la información.

Los hitos teóricos que dieron lugar a la mecánica cuántica:

- 1900: Max Planck propone el cuanto de energía.
- 1905: Albert Einstein propone el fotón.
- 1913 – 1915: Niels Bohr y Arnold Sommerfeld proponen la Teoría cuántica antigua.
- 1924: Louis de Broglie propone la dualidad onda-partícula.
- 1925: Erwin Schrödinger propone la Mecánica ondulatoria y Werner Heisenberg la Mecánica matricial.
- 1926 – 1930: Max Born, Pascual Jordan, Wolfang Pauli, John Von Neumann, etc. demuestran que la mecánica ondulatoria y la matricial son equivalentes. Se unifica y formaliza la teoría cuántica poniendo gran énfasis en la medición y la naturaleza estadística de la percepción de la realidad.
- 1930 – actualidad: Se unifica Desarrollo de aplicaciones de la Teoría Cuántica.

La mecánica cuántica ha conseguido dar resultados más exactos que la física clásica en cuanto a la descripción del comportamiento de partículas individuales y, aunque se apoya en un formalismo matemático bien establecido consistente en espacios vectoriales del álgebra lineal, su interpretación física

todavía es controvertida y abierta a debate ya que describe fenómenos ajenos a nuestra intuición ordinaria y nuestro cerebro es incapaz de concebirlos por naturaleza.

La mecánica clásica es determinista, lo que implica que el conocimiento del estado del sistema y su dinámica permite predecir con certeza absoluta el valor de cualquier variable. La naturaleza probabilística de la mecánica cuántica rompe con este determinismo, planteando una serie de debates de índole filosófica. El estado de un sistema y su medición, equivalentes en la mecánica clásica, no son así en la mecánica cuántica, llegando a sugerir cuestionarse la propia realidad percibida. Incluso Einstein, uno de los fundadores de la teoría, se mostró disgustado con esta pérdida de realismo en la medición quedando patente en su famosa afirmación "Dios no juega a los dados con el universo".

¿Qué ha conseguido explicar entonces la mecánica cuántica?

- La estructuras de átomos y moléculas.
- Las reacciones químicas.
- La estructura electrónica de los sólidos.
- La física nuclear y de partículas.
- La física a bajas temperaturas.

La estructura formal de una mecánica se compone por tres elementos: el estado mecánico del sistema, los observables, relación entre el estado y los resultados de las medidas, y la dinámica, evolución del estado en el tiempo. En la mecánica clásica no existe diferenciación entre el estado y los observables, exhibiendo una filosofía positivista, pero en la cuántica no se puede obviar su separación.

Finalmente, y concretando esta estructura formal en la mecánica cuántica tenemos:

- Estado mecánico: vector en espacio de Hilbert.
- Observables: operador lineales autoadjuntos.
- Dinámica unitaria.

Dicho esto, sin entrar en definiciones matemáticas o explicaciones físicas más detalladas, posteriormente se deduce de aquí el qubit y las distintas posibilidades de operación que se presentan con respecto al bit.

1.2.2 Información cuántica: el qubit

En cuanto a la teoría de la información, ésta trata del estudio del procesamiento de información, es decir, su almacenamiento, transformación y transmisión. Desde un punto de vista físico, el computador es pues un sistema en que a los estados se les da un significado y la computación consta de una

preparación del sistema en un estado específico (entrada), una evolución del estado en el tiempo (procesamiento) y una medición del estado final (salida).

El computador clásico es un sistema físico que evoluciona de forma clásica y cuyo ingrediente básico es el bit y su espacio de estados es 0 ó 1. El estado se puede representar como una cadena de bits y estos se ven modificados según la dinámica especificada (algoritmo).

En cuanto al computador cuántico, su unidad mínima de información es el qubit (quantum bit), análogo al bit en el sentido en que puede tener dos valores (0 ó 1), pero muy distinto en cuanto a que su estado puede ser combinación de ambos, un efecto conocido como superposición cuántica que pone de manifiesto su naturaleza continua. A pesar de esto, sólo es posible obtener un resultado discreto de una medición sobre un qubit con una probabilidad dada.

Es muy conocido el experimento del gato de Schrödinger para explicar la superposición cuántica y por extensión la naturaleza del qubit. En él se propone una caja cerrada con un gato en su interior, una botella de gas venenoso, un átomo radiactivo con un 50% de probabilidades de desintegrarse y un dispositivo detector, que de ocurrir dicha desintegración hará que la botella se rompa y el gato muera. El estado del gato (nuestro qubit), supongamos que es 1 de estar vivo y 0 de estar muerto, depende directamente de una partícula sujeta a las leyes de la mecánica cuántica, encontrándose pues simultáneamente en ambos estados potenciales mientras la caja se encuentre cerrada, ya que el estado de las partículas subatómicas no puede ser descrito más que probabilísticamente. Al abrir la caja, con el simple hecho de realizar una medición sobre el sistema se producen modificaciones en él, observándose entonces solamente o un gato vivo o uno muerto.

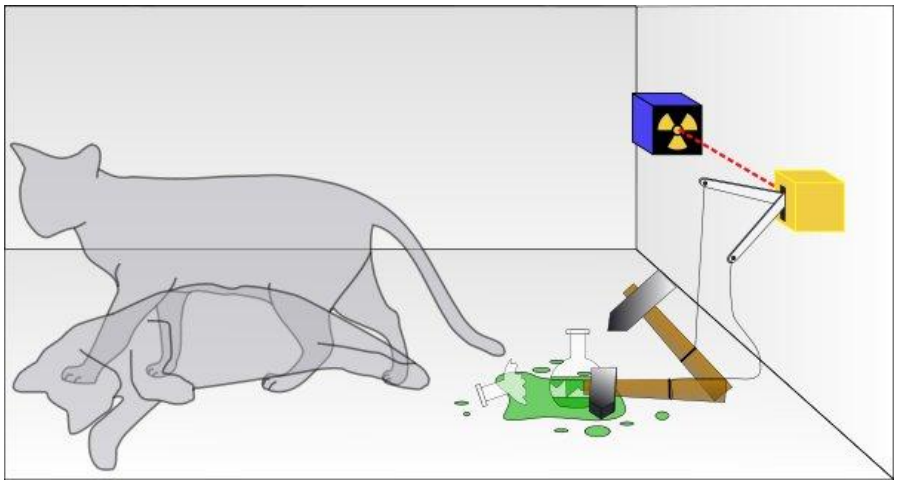


Figura 1.2: El experimento del Gato de Schröndinger.

El qubit, definido matemáticamente, es un espacio vectorial complejo bidimensional de módulo 1 que puede ser entendido con la siguiente representación geométrica: la Esfera de Bloch. Los estados básicos se expresan con la notación bra-ket, $|0\rangle$ (ket cero) y $|1\rangle$ (ket uno), y los estados puros como una combinación lineal de estos: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ siendo α y β números complejos que representan probabilidades de amplitud y que deben cumplir la siguiente ecuación: $|\alpha|^2 + |\beta|^2 = 1$. Dicho esto, la probabilidad de obtener el estado $|0\rangle$ es $|\alpha|^2$ y la de obtener $|1\rangle$ es $|\beta|^2$.

Analizando la Figura 1.3, la superficie es un espacio bidimensional que representa los estados puros del qubit, expresados mediante vectores de un espacio de Hilbert, y, finalmente, el interior es el conjunto de estados entrelazados, combinación de varios estados puros, necesarios para expresar sistemas de varios qubits.

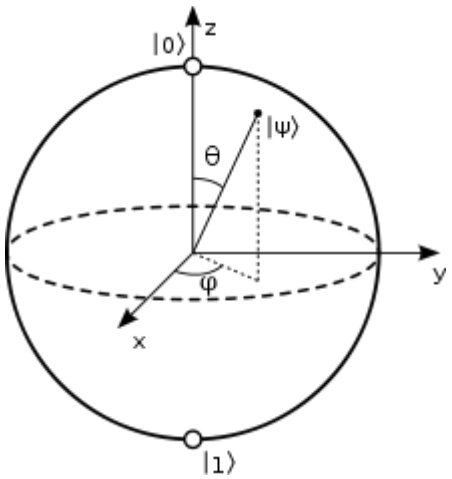


Figura 1.3: Esfera de Bloch representando los dos estados básicos $|0\rangle$ (ket cero) y $|1\rangle$ (ket uno) y todos los estados puros en superposición.

Algunas propiedades resultantes de esta perspectiva de la información cuántica sin equivalencia en la computación clásica son el paralelismo cuántico y el entrelazamiento cuántico, y de ellas se deriva en gran medida la potencia de la computación cuántica.

Una rápida comparativa de las posibilidades que aportan estas cualidades: un computador cuántico de tan sólo 30 qubits tiene una capacidad de cómputo de 10 teraflops, mientras que, por poner un ejemplo ilustrativo, la videoconsola más potente en la actualidad, la PlayStation 3, tiene una capacidad de 2.5 teraflops.

1.2.2.1 Paralelismo cuántico

Como se ha podido ver, el qubit representa ambos estados superpuesto $|0\rangle$ y $|1\rangle$, y las puertas lógicas y, por extensión, algoritmos cuánticos operarán sobre todas las combinaciones de la entrada a la vez.

1.2.2.2 Entrelazamiento cuántico

Se dice que varios qubits pueden representarse mediante un estado de entrelazamiento cuántico, expresando una correlación mayor de lo que es posible en sistemas clásicos.

Es similar al eje de coordenadas cartesiano, en que el $x \in \mathbb{R}$ e $y \in \mathbb{R}$, su combinación, resultado del producto cartesiano, se describe como $(x, y) \in \mathbb{R}^2$.

Un sistema de dos qubits entrelazados, recordemos son representados como vectores en un espacio de Hilbert, forman un nuevo espacio H^2, fruto de su producto tensorial, en el que se pueden expresar nuevos estados, imposibles de describir con qubits por separado. Al medir el sistema se dice que colapsa y se produce una proyección del estado entrelazado en cada qubit. En la Esfera de Bloch, si entendemos los estados entrelazados como puntos del interior, la proyección se realiza sobre la superficie.

La adición de qubits al sistema incrementa la dimensión del espacio de estados posibles, dotando a la computación cuántica de una capacidad de procesamiento muy superior a la clásica.

Gracias al entrelazamiento cuántico, además de la capacidad de cómputo, emerge un fenómeno conocido como teleportación cuántica.

1.2.2.3 Teleportación cuántica

La teleportación cuántica, descrita teóricamente en 1993 y demostrada experimentalmente en 1997, es un fenómeno que se sustenta en el entrelazado cuántico para transmitir un qubit desde una localización a otra sin que atraviese el espacio que separa ambos puntos. En la teleportación cuántica no se transmite materia, energía, ni permite la comunicación de información clásica, por lo que tampoco es útil para la comunicación a velocidades mayores a la de la luz.

Suponiendo un estado entrelazado formado a partir de dos qubits: $\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, las probabilidades de obtener $|00\rangle$ o $|11\rangle$ son idénticas ya que $\left|\frac{1}{\sqrt{2}}\right|^2 = 0.5$. Ahora, los qubits son separados y se realiza la medida en ellos de forma individual. Si uno de ellos devuelve el valor 0, debido al entrelazamiento

cuántico, y puesto que no existen los estados $|01\rangle$ o $|10\rangle$, el otro también devolverá el mismo valor, aunque se encuentre a años luz de distancia. Esta característica se utiliza para la implementación práctica de la teleportación cuántica.

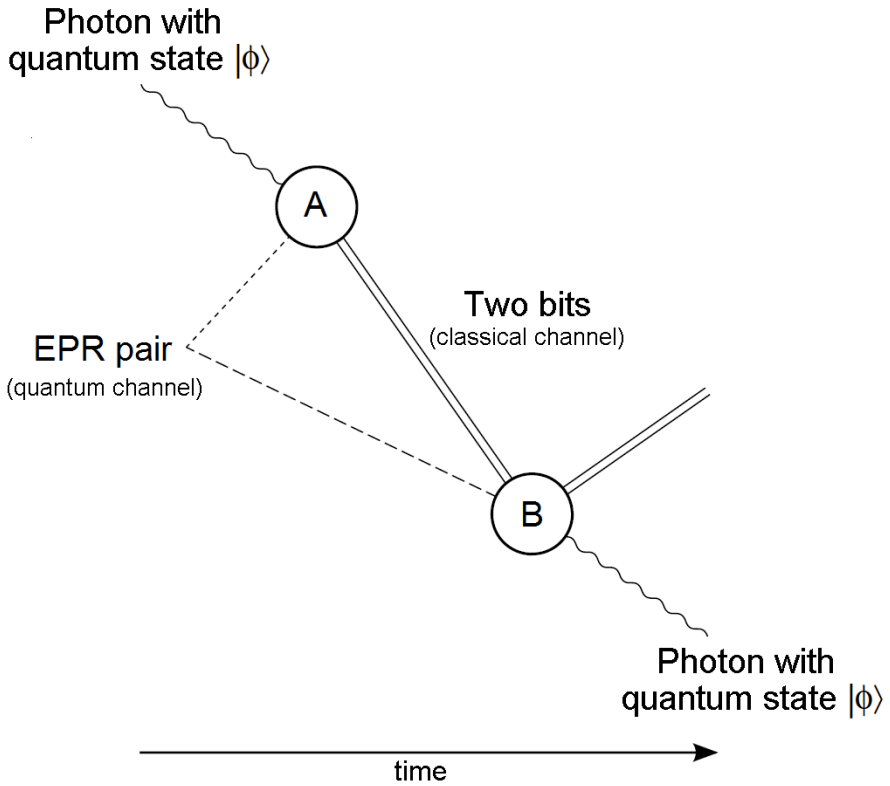


Figura 1.4: Protocolo de teleportación cuántica de un qubit a través de un par de qubits entrelazados.

Los prerrequisitos necesarios para llevara a cabo una teleportación cuántica son los siguientes:

- Un qubit para teleportar.
- Un canal de comunicación convencional capaz de transmitir dos bits.
- Una forma de generar un estado entrelazado a partir de dos qubits (EPR pair). Esto se considera un canal cuántico.

Tal y como se ilustra en la figura 1.4, el protocolo de una teleportación cuántica se define de forma resumida en:

1. Se genera un estado entrelazado a partir de un par de qubits posteriormente distribuidos en dos localizaciones A y B.

2. Se realiza una medición del qubit entrelazado y el qubit a transmitir, generando dos bits clásicos y destruyéndose ambos qubits.
3. Usando el canal convencional, los dos bits se transmiten desde A hasta B.
4. En la localización B el qubit entrelazado se modifica, usando los dos bits clásicos para seleccionar cuál de los cuatro es el estado cuántico correcto. Esto genera un qubit idéntico al que se deseaba transmitir.

Los resultados experimentales de esta técnica alcanzaron una distancia de 600 metros en 2004 utilizando fibra óptica, incrementados a 16 kilómetros en 2010 con una precisión del 89%. En este mismo año se ha conseguido realizar teleportaciones con un 100% de precisión.

1.3 Computación cuántica

Una vez comentados los fundamentos teóricos físicos y matemáticos que sustentan y da sentido a la computación cuántica se analizará la trayectoria seguida por este paradigma computacional desde los comienzos, los problemas de construcción que aún existen en la actualidad, las puertas lógicas que implementarán las arquitecturas cuánticas, algunos de los algoritmos cuánticos ya existentes, y demás detalles relacionados con su potencia frente a la computación clásica y las utilidades esperadas.

1.3.1 Historia

La computación cuántica aún se encuentra en los albores de su vida. Desde 1981 que se propusieran los fundamentos teóricos ya ha superado la desconfianza que generaba con las primeras etapas de experimentación y actualmente se avanza en dirección a su aplicación práctica.

Hitos de la computación cuántica:

- 1981: Paul Benioff propone teóricamente un computador que opera con algunos principios de la mecánica cuántica.
- 1981-1982: Richard Feynman defiende la utilidad de la computación cuántica afirmando que algunas operaciones complejas se podrían ejecutar mucho más rápidas utilizando fundamentos cuánticos.
- 1985: David Deutsch describe el primer computador cuántico universal.

- 1993: Dan Simon demuestra la ventaja práctica de un computador cuántico con respecto a uno clásico.
- 1993: Charles Benett descubre el teletransporte cuántico.
- 1994: Peter Shor define un algoritmo capaz de calcular números primos muchísimo más rápido que los tradicionales, capaz de romper la mayoría de sistemas criptográficos.
- 1995: Peter Shor propone un sistema de corrección de errores para cálculos cuánticos.
- 1996: Lov Grover define un algoritmo cuántico de búsqueda.
- 1997: Se realizan con éxito algunos experimentos como la comunicación cuántica segura o el teletransporte cuántico de un fotón.
- 1998-1999: Se consigue transmitir un qubit, se construyen los primeros computadores cuánticos de 2 y 3 qubits y se ejecuta el algoritmo de Grover.
- 2001: Se consigue ejecutar el algoritmo Shor en un computador de 7-qubits.
- 2005: Se crea el primer qubyte, 8 qubits unidos mediante trampas de iones
- 2007: Se diseña el primer bus cuántico con componentes superconductores.
- 2008: Se consigue por primera vez almacenar un qubit por 1.75 segundos en el interior de un núcleo de un átomo de fósforo.
- 2009: Se construye el primer procesador cuántico de estado sólido, similar a los convencionales.

1.3.2 Hardware

Existen múltiples dificultades en cuanto a la construcción de computadores cuánticos, y por ahora sólo se han resuelto algunos problemas triviales. Es por ello que aún no existe un hardware ideal si no una lista de requisitos a cumplir, establecidos por David DiVicenzo:

- El sistema debe ser físicamente escalable para incrementar el número de qubits.
- Los qubits del sistema deben poder ser inicializados a valores arbitrarios.
- Las puertas cuánticas deben ser más rápidas que el tiempo de decoherencia cuántica para mantener la coherencia a través de las operaciones.
- Poseer un conjunto universal de puertas lógicas para manipular los qubits de forma controlada.
- Los qubits resultado de un cálculo deben poderse leer fácilmente.

1.3.2.1 Decoherencia cuántica

Para que se mantenga la coherencia de la información, se comenta en uno de los puntos que las operaciones deben realizarse a una velocidad mayor a la de decoherencia cuántica. Esto quiere decir, que debido a que las partículas usadas para representar los qubits se encuentran en constante interacción con el entorno, tienden a formar cuerpos mayores que dejan de comportarse según las leyes de la mecánica cuántica y por ello se deshacen los estados de superposición en los qubits y los resultados obtenidos son incorrectos.

Para mantener el estado de coherencia se dice es necesario obtener una tasa de errores inferior a 10^{-4} y así aplicar mecanismos de corrección de errores.

1.3.2.2 Implementaciones

A lo largo de los años se han propuesto gran cantidad de distintos sistemas físicos, demostrando el estado de infancia en que se encuentra la computación cuántica. Algunos de ellos, distinguidos según el método físico en que se basan para implementar el qubit y sin entrar en detalles, son:

- Superconductores. Implementan el qubit como el estado de pequeños circuitos superconductores.
- Trampas de iones. El qubit es implementado por los estados internos de los iones suspendidos.
- Entramados ópticos. Qubit implementado por el estado interno de átomos neutrales atrapados en un entramado óptico.
- Eléctricamente definidos o de puntos cuánticos auto-ensamblados. El qubit se implementa por el spin de un electrón en un punto cuántico.
- Resonancia nuclear magnética (NMR) de moléculas en disolución. Qubit entendido como el spin nuclear de la molécula disuelta.
- Resonancia nuclear magnética (NMR) en estado sólido. Qubit entendido como el spin nuclear de átomos donantes de fósforo en silicio.
- Electrones en helio. El qubit viene definido por el spin del electrón.
- Moléculas imán.
- Fullereno. Qubit basado en el spin electrónico de átomos o moléculas encerradas en estructuras de fullereno.

- Óptica cuántica. Qubits distinguidos según los estados de los distintos modos del campo electromagnético.
- Transistores utilizando trampas electroestáticas.
- Etc…

1.3.3 Puertas lógicas cuánticas

O simplemente puertas cuánticas, son los elementos básicos que componen los circuitos cuánticos y, a diferencia de muchas puertas lógicas usadas en computación clásica, son reversibles.

A pesar de esta particularidad, los computadores cuánticos pueden ejecutar todas las operaciones booleanas posibles en computación clásica. Esto se debe a que en computación clásica, aunque no se haga, todas las operaciones se pueden implementar con puertas lógicas reversibles, como por ejemplo puertas Toffoli, que tienen su equivalente exacto en computadores cuánticos.

Las puertas cuánticas se describen normalmente mediante matrices unitarias de $2^k x 2^k$, siendo k el número de qubits de entrada/salida, los cuales son iguales para permitir la reversibilidad. La puerta lógica se aplica multiplicando la matriz por el vector que define el estado cuántico de los qubits.

1.3.3.1 Hadamard

Input	H
$\|0\rangle$	$\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$
$\|1\rangle$	$\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$
Matriz:	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

1.3.3.2 Pauli-X

Equivalente a la puerta NOT. Realiza una rotación de π radianes en el eje X de la Esfera de Bloch que representa al qubit.

Input	X
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
Matriz:	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

1.3.3.3 Pauli-Y

De igual forma que la puerta Pauli-X, aplica una rotación de π radianes en el eje Y de la Esfera de Bloch.

Input	Y
$\|0\rangle$	$-i\|1\rangle$
$\|1\rangle$	$i\|0\rangle$
Matriz:	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$

1.3.3.4 Pauli-Z

Aplica en este caso la rotación sobre el eje Z. Ésta es un caso especial de puerta de cambio de fase cuyo $\theta = \pi$.

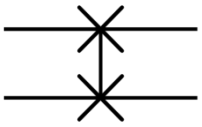
Input	Z
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$
Matriz:	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$

1.3.3.5 Puertas de cambio de fase

La probabilidad de medir $|0\rangle$ o $|1\rangle$ no cambia después de aplicarlas, sin embargo modifican la fase del estado cuántico. Esto es equivalente a trazar un círculo horizontal de θ radianes sobre la Esfera de Bloch.

Input	R_θ
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{i\theta}\|1\rangle$
Matriz:	$\begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix}$

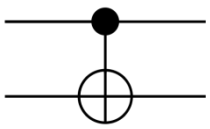
1.3.3.6 Swap (intercambio)



Intercambia los dos qubits de entrada y su matriz viene representada por:

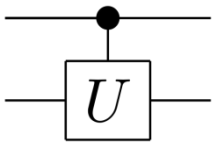
$$SWAP = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$$

1.3.3.7 Controladas



Son puertas que actúan sobre 2 o más qubits, donde uno o varios sirven de control. Por ejemplo, la puerta CNOT realiza una operación NOT sobre el segundo qubit sólo cuando el primero es |1>.

$$CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$



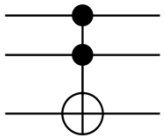
De forma más general, se puede definir la puerta controlada-U, en el que el primer qubit es de control y sobre el segundo se aplica la operación definida por la matriz U.

$$U = \begin{bmatrix}x_{00} & x_{01}\\ x_{10} & x_{11}\end{bmatrix}$$

Input	R_0
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|1\rangle(x_{00}\|0\rangle + x_{10}\|1\rangle)$
$\|11\rangle$	$\|1\rangle(x_{01}\|0\rangle + x_{11}\|1\rangle)$
Matriz:	$C(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{bmatrix}$

Cuando la matriz U es alguna de las matrices de Pauli, a las puertas se les llama controlada-X, controlada-Y o controlada-Z.

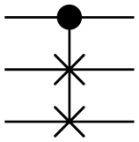
1.3.3.8 Toffoli



También llamada CCNOT, es una puerta universal de 3-bits en la computación clásica. En cuántica es análoga y trabaja con 3 qubits, realizando una operación Pauli-X sobre el tercero si los dos primeros se encuentran en el estado $|1\rangle$.

Input	Toffoli
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|101\rangle$
$\|110\rangle$	$\|111\rangle$
$\|111\rangle$	$\|110\rangle$

1.3.3.9 Fredkin



También llamada CSWAP Al igual que la puerta Toffoli, es universal en computación clásica. Tiene la propiedad de conservar el mismo número de 1s y 0s en la salida.

Input	Fredkin
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|110\rangle$
$\|110\rangle$	$\|101\rangle$
$\|111\rangle$	$\|111\rangle$

1.3.4 Algoritmos cuánticos

Los algoritmos cuánticos son aquellos que se ejecutan sobre circuitos cuánticos, que, por extensión de las leyes de la mecánica cuántica, son probabilísticos. Así como las puertas cuánticas son capaces de implementar todas las funciones booleanas de la computación clásica, los algoritmos cuánticos son capaces de realizar las mismas operaciones clásicas además de las propias.

Una apreciación sobre la potencia de los algoritmos cuánticos es que todos los problemas que pueden resolver también pueden ser resueltos por un algoritmo clásico en un equipo con suficientes recursos (tiempo y memoria). De igual forma, aquellos imposibles de resolver con algoritmos clásicos, como los problemas de decisión indecidible, siguen siendo irresolubles con los cuánticos.

Esto no quiere decir que no aporten una ventaja significativa. Los problemas que pueden ser eficientemente resueltos por un algoritmo cuántico son denominados BQP (BoundedError-Quantum-Polynomial) y se definen como aquellos problemas que pueden ser resueltos por un algoritmo en tiempo polinomial cuya probabilidad de error está acotada por debajo de 0.5. Dicho de otra forma, se dice que un algoritmo resuelve un problema BQP si, para cada instancia, su respuesta será correcta con una alta probabilidad en tiempo polinomial.

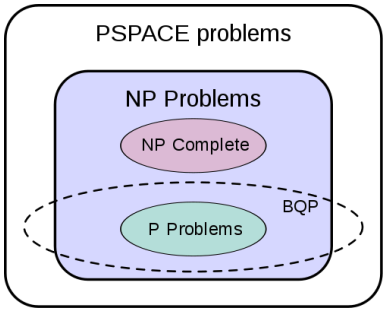


Figura 1.5: Representación gráfica de los subconjuntos de problemas según su complejidad computacional abarcados por BQP.

La clasificación de la complejidad computacional de los problemas BQP se sabe que está contenida en la clase tipo #P, subclase de los PSPACE. Se cree también que abarca todos los problemas P, resolubles en tiempo polinomial por una máquina de Turing determinista, y un subconjunto de los NP, como la factorización de enteros o el cálculo de logaritmos discretos, excluyendo los NP-Completos.

Algunos de los algoritmos cuánticos más conocidos y utilizados para la experimentación son el algoritmo de Shor, el de Grover y el de Deutsch-Jozsa.

1.3.4.1 Algoritmo de Shor

El algoritmo de Shor resuelve el problema del logaritmo discreto y el problema de la factorización de enteros en tiempo polinomial mientras que el mejor algoritmo clásico los resuelve en tiempo superpolinomial, concretamente con una eficiencia de $O((\log N)^3)$.

Su eficiencia descansa en el uso de la transformada cuántica de Fourier y la exponenciación modular binaria.

Cabe destacar, que dado un computador cuántico con suficiente número de qubits, este algoritmo es capaz de romper el esquema criptográfico basado en clave pública, RSA. Éste se basa en el supuesto de que los números extremadamente grandes son imposibles de factorizar en un tiempo razonable, cosa que ya ha sido demostrada falsa en la computación cuántica.

1.3.4.2 Algoritmo de Grover

El algoritmo de Grover busca en una base de datos desestructurada con N entradas usando sólo $\sqrt{\mathrm{N}}$ consultas.

Este algoritmo sirve para ilustrar que en computación cuántica existe un modelo de búsqueda más rápido que la simple comprobación secuencial de todos los elementos, la mejor opción en computación clásica.

También puede ser utilizado para el cálculo de la media y la mediana en grandes conjuntos de datos o el cálculo de problemas de colisión.

1.3.4.3 Algoritmo de Deutsch-Jozsa

El algoritmo de Deutsch-Jozsa resuelve un problema de caja negra que requeriría un número exponencial de consultas a la caja negra para una máquina de Turing determinista con una única consulta en un computador cuántico.

Aunque su uso práctico es nulo, es uno de los primeros ejemplos de algoritmo cuántico capaz de incrementar la eficiencia de forma exponencial cualquier algoritmo clásico determinista.

1.3.5 Arquitecturas cuánticas

Dada la falta de madurez práctica de la computación cuántica y de su falta de interés comercial actualmente, las especificaciones de arquitecturas estándar son inexistentes, como ya se comentaba en el apartado relativo al hardware, y las particulares están detalladas a un nivel que se escapa del alcance de este trabajo.

No obstante, de entre las distintas implementaciones vistas previamente las únicas que tienen posibilidad de llegar realmente de ser de uso general son aquellas basadas en estado sólido.

Uno de los problemas más importantes a los que se enfrentan las arquitecturas cuánticas de cara a su generalización es la escalabilidad física. La interacción entre los qubits está restringida entre aquellos próximo y su solución radica en la existencia de cables cuánticos que utilicen la teleportación cuántica y así se pueda operar con qubits que se encuentren almacenados en una posición arbitraria del computador cuántico.

La teleportación cuántica se propone según el siguiente esquema usando las puertas cuánticas explicadas.

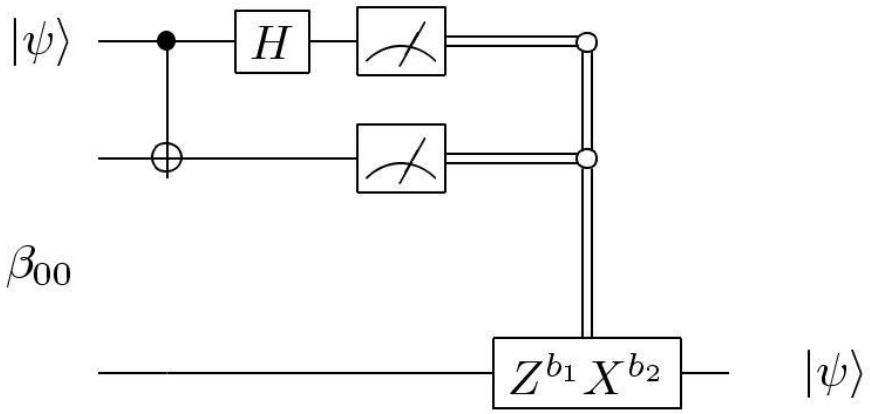


Figura 1.6: Esquema de teleportación cuántica usando un estado entrelazado β_{00}, un qubit $|\psi\rangle$, dos bits b_1 y b_2, y las puertas CNOT, H, Z y X.

Recientemente, en una conferencia de la American Physical Society ha sido presentada una arquitectura de estado sólido llamada RezQu y enfocada en la construcción de computadores cuánticos escalables. En ella se presentó un microprocesador cuántico de 4-qubits y se espera que para finales de años se pueda ampliar a 10.

1.4 Conclusiones

Es un hecho innegable que la computación clásica está comenzando a encontrar limitaciones insalvables de seguir en la dirección de una mayor integración. A pesar de las múltiples técnicas que se vienen observando en los últimos años como el aumento del número de núcleos de los procesadores de cara una mayor paralelización de los procesos, la computación cuántica avanza imparable camino a cambiar drásticamente el campo de la computación, encontrar una forma de aplicación práctica, y hacerse extensible al uso específico o general en un futuro no muy lejano.

La evolución de la computación cuántica aún se encuentra en una fase muy inicial, resolviendo problemas fundamentales necesarios para encontrar formas eficaces de implementación física. También es destacable el cambio que supone este nuevo paradigma de computación en cuanto a su escalabilidad software de cara a los futuros programadores que deberán diseñar programas cuyo funcionamiento interno, vistas las puertas cuánticas, dista enormemente del que estamos acostumbrados.

En cuanto a las consecuencias de la proliferación de computadores cuánticos, ya se ha comentado supone un gran problema de seguridad para muchos

de los esquemas criptográficos. Se habla pues de un campo de la criptográfia denominada post-cuántica, en la que se buscan primitivas irrompibles por computadores cuánticos.

Por último y comentando la aplicabilidad de los computadores cuánticos más allá de la capacidad de cómputo. Áreas de investigación como la nanotecnología así como las del propio estudio de partículas subatómicas son imposibles de simular de forma completamente fidedigna mediante la computación cuántica, es por ello que se cree que algunas de las utilidades más comunes de la computación cuántica serán aquellas relacionadas con la simulación cuántica.

1.5 Bibliografía

Gómez-Esteban, P. (marzo de 2009). *Gato de Schrödinger* [imagen]. Obtenido el 20 de abril de 2011 desde: http://eltamiz.com/images/2009/March/gato-schrodinger-cerrada.jpg

Oskin, M. (2003). *Building quantum wires*. Obtenido el 22 de abril de 2011 desde: http://qarc.cs.berkeley.edu/publications/papers/pdf/isca2003-qwires.pdf

Rubia, D. (22 de marzo de 2011). *Paso adelante en la computación cuántica* [blog]. Obtenido el 22 de abril de 2011 desde: http://alt1040.com/2011/03/paso-adelante-en-la-computacion-cuantica

Uchii, S. (28 de julio de 2004). *Efecto túnel* [imagen]. Obtenido el 20 de abril de 2011 desde: http://www.bun.kyoto-u.ac.jp/~suchii/Bohr/tunnel.jpg

Wikipedia. (13 de abril de 2011). *Computación cuántica* [wiki]. Obtenido el 15 de abril de 2011 desde: http://es.wikipedia.org/wiki/Computación cuántica

Wikipedia. (17 de abril de 2011). *Computational complexity theory* [wiki]. Obtenido el 22 de abril de 2011 desde: http://en.wikipedia.org/wiki/Computational complexity theory

Wikipedia. (25 de junio de 2010). *Decoherencia cuántica* [wiki]. Obtenido el 22 de abril de 2011 desde: http://es.wikipedia.org/wiki/Decoherencia_cuántica

Wikipedia. (7 de marzo de 2011). *Efecto túnel* [wiki]. Obtenido el 20 de abril de 2011 desde: http://es.wikipedia.org/wiki/Efecto_túnel

Wikipedia. (6 de febrero de 2011). *Esfera de Bloch* [wiki]. Obtenido el 20 de abril de 2011 desde: http://es.wikipedia.org/wiki/Esfera_de_Bloch

Wikipedia. (31 de marzo de 2011). *Gato de Schrödinger* [wiki]. Obtenido el 20 de abril de 2011 desde: http://es.wikipedia.org/wiki/Gato_de_Schrödinger

Wikipedia. (5 de agosto de 2010). *Observable* [wiki]. Obtenido el 18 de abril de 2011 desde: http://en.wikipedia.org/wiki/Quantum_mechanics

Wikipedia. (12 de abril de 2011). *Positivismo* [wiki]. Obtenido el 18 de abril de 2011 desde: http://es.wikipedia.org/wiki/Positivismo

Wikipedia. (25 de marzo de 2011). *Post-quantum criptography* [wiki]. Obtenido el 22 de abril de 2011 desde: http://en.wikipedia.org/wiki/Post-quantum_cryptography

Wikipedia. (25 de marzo de 2011). *Quantum algorithm* [wiki]. Obtenido el 22 de abril de 2011 desde: http://en.wikipedia.org/wiki/Quantum_algorithm

Wikipedia. (13 de abril de 2011). *Quantum computer* [wiki]. Obtenido el 15 de abril de 2011 desde: http://en.wikipedia.org/wiki/Quantum_computer

Wikipedia. (10 de abril de 2011). *Quantum gate* [wiki]. Obtenido el 21 de abril de 2011 desde: http://en.wikipedia.org/wiki/Quantum_gate

Wikipedia. (15 de abril de 2011). *Quantum mechanics* [wiki]. Obtenido el 16 de abril de 2011 desde: http://en.wikipedia.org/wiki/Quantum_mechanics

Wikipedia. (17 de abril de 2011). *Quantum teleportation* [wiki]. Obtenido el 22 de abril de 2011 desde: http://en.wikipedia.org/wiki/Quantum_teleportation

Wikipedia. (2 de noviembre de 2009). *Talk: PS3/Archive 1* [wiki]. Obtenido el 22 de abril de 2011 desde: http://en.wikipedia.org/wiki/Talk:PlayStation_3/Archive1#2.18_Teraflops

Wikipedia. (20 de abril de 2011). *Teleportación cuántica* [wiki]. Obtenido el 22 de abril de 2011 desde: http://es.wikipedia.org/wiki/Teleportación_cuántica

Wikipedia. (17 de julio de 2010). *Undecidable problem* [wiki]. Obtenido el 22 de abril de 2011 desde: http://en.wikipedia.org/wiki/Undecidable_problem