Universidad de Huelva

Tema 9

Computación cuántica

- La Mecánica Clásica se basa en que el estado de un sistema físico viene determinado por la posición y velocidad de las partículas que lo forman.
- Si consideramos una única partícula, el estado del sistema viene dado por su posición, $r(t)$, y su velocidad, $v(t)$.
- Conocido el estado en un determinado instante es posible determinarlo en cualquier instante mediante las leyes de la Mecánica de Newton. Estas leyes describen el efecto sobre el estado del sistema de las fuerzas o campos presentes en el espacio.

- Para la Mecánica Cuántica, el estado de un sistema viene dado por su **función de onda**, $\psi(r,t)$, que define un valor complejo en cada punto del espacio y en cada instante.
- La evolución del estado del sistema está determinada por la ecuación de Schrödinger para la función de onda:

$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = \left[\frac{-\hbar^2}{2\mu}\nabla^2 + V(\mathbf{r},t)\right]\Psi(\mathbf{r},t)$$

- La función de onda se puede interpretar como una densidad de probabilidad (Max Born), de manera que la probabilidad de encontrar una partícula en un volumen $d^3r = dx\ dy\ dz$ es

$$|\psi(r,t)|^2 d^3r$$

- Las funciones de onda son funciones acotadas, definidas sobre todo el espacio, continuas e infinitamente diferenciables. Este tipo de funciones forman un espacio de Hilbert, es decir, un espacio vectorial con un producto escalar, denominado $\mathcal{F}$.
- El producto escalar de dos funciones, $\boldsymbol{\psi(r)}$ y $\boldsymbol{\varphi(r)}$, se define como

$$(\psi, \varphi) = \int \psi^*(r)\varphi(r)\mathrm{d}^3 r$$

- El operador * se refiere al conjugado complejo ($i \rightarrow -i$)

- Sobre las funciones de onda pueden actuar operadores lineales. Un operador lineal es una entidad matemática que transforma funciones.

$$\psi'(r) = A\psi(r)$$

- El carácter lineal implica que

$$A(a \cdot \psi(r) + b \cdot \varphi(r)) = a \cdot A\psi(r) + b \cdot A\varphi(r)$$

- El producto de dos operadores lineales es la composición de los dos operadores. En general es una operación no conmutativa.

$$AB\psi(r) = A(B\psi(r))$$

- El producto escalar de funciones permite definir una norma. Una función está normalizada si su norma es la unidad.

$$\|\psi(r)\|^2 = (\psi, \psi) = \int \psi^*(r)\psi(r)\mathrm{d}^3 r$$

- Dos funciones son ortogonales si su producto escalar es cero.

$$\psi \perp \varphi \Leftrightarrow \int \psi^*(r)\varphi(r)\mathrm{d}^3 r = 0$$

- Un conjunto de funciones ortonormales es una colección de funciones $u_i(r)$ que cumplen

$$(u_i, u_j) = \int u_i^*(r)u_j(r)\mathrm{d}^3 r = \delta_{ij}$$

- Un conjunto de funciones ortonormales forman una base de $\mathcal{F}$ si cualquier función de onda puede expresarse de forma unívoca como una combinación lineal de las funciones que constituyen el conjunto.

$$\psi(r) = \sum_i c_i \cdot u_i(r)$$

- Los espacios de Hilbert son una generalización de los espacios vectoriales en los que la dimensión puede ser infinita. En estos casos se pueden enumerar las funciones mediante un parámetro real α.
- Un conjunto ortonormal parametrizado es un conjunto de funciones ω_α que cumplen

$$\int \omega_\alpha{}^*(r)\omega_{\alpha'}(r)\mathrm{d}^3r = \delta(\alpha - \alpha')$$

- Un conjunto ortonormal parametrizado forma una base parametrizada si toda función puede descibirse como

$$\psi(r) = \int c_\alpha \cdot \omega_\alpha(r) d\alpha$$

- Dadas dos funciones de onda, $\psi(\mathbf{r})$ y $\varphi(\mathbf{r})$, cuyos componentes en una base concreta paramétrica son conocidos, se puede calcular su producto escalar como

$$\psi(r) = \int a_\alpha \cdot \omega_\alpha(r) d\alpha$$
$$\varphi(r) = \int b_{\alpha'} \cdot \omega_{\alpha'}(r) d\alpha'$$
$$(\psi, \varphi) = \int a^*{}_\alpha b_\alpha d\alpha$$

- Si consideramos una cierta base, discreta o continua, el estado de una partícula en un instante determinado viene dado por el vector de los coeficientes de la función de onda en esa base.
- Dada la función de ondas, $\psi(\mathbf{r})$, se denota como $|\psi\rangle$ el vector formado por estos coeficientes. Esta representación, propuesta por Paul Dirac, se denomina "ket".
- Dado un espacio vectorial se puede definir un espacio dual formado por todas las aplicaciones lineales del espacio original que a cada vector le asocia un número complejo. Se denominan "bras" a estas aplicaciones.

- Dado un "ket" $|\psi\rangle$ se puede definir un "bra" $\langle\psi|$, es decir, un elemento del espacio dual, que representa a la aplicación que a cada vector $|\varphi\rangle$ le asigna el producto escalar $(|\psi\rangle, |\varphi\rangle)$.
- Utilizando esta notación, el producto escalar entre vectores se puede expresar como

$$\langle\psi|\varphi\rangle = (|\psi\rangle, |\varphi\rangle)$$

- Dada una base discreta o continua del espacio de estados, un ket cualquiera se puede representar como un vector columna formado por sus componentes en dicha base:

$$|\psi\rangle = \begin{pmatrix} \langle u_1|\psi\rangle \\ \langle u_2|\psi\rangle \\ \dots \\ \langle u_i|\psi\rangle \\ \dots \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} \dots \\ \dots \\ \langle \omega_\alpha|\psi\rangle \\ \dots \\ \dots \end{pmatrix}$$

- Por su parte, un bra se puede representar como un vector fila:

$$\langle\psi| = (\langle\psi|u_1\rangle, \dots, \langle\psi|u_i\rangle, \dots) = (\langle u_1|\psi\rangle^*, \dots, \langle u_i|\psi\rangle^*, \dots)$$

- Siguiendo esta representación, los operadores lineales se pueden representar mediante una matriz:

$$A|\psi\rangle = \begin{pmatrix} \langle u_1|A|u_1\rangle & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \langle u_i|A|u_j\rangle & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} \langle u_1|\psi\rangle \\ \dots \\ \langle u_i|\psi\rangle \\ \dots \end{pmatrix}$$

- Dado un operador lineal, A, se puede definir su operador dual, $A^\dagger$, tal que:

$$A^\dagger|\psi\rangle = |\varphi\rangle \Leftrightarrow \langle\varphi|A = \langle\psi|$$

- Este operador se conoce como el hermítico conjugado de A y cumple que

$$\langle\alpha|A^\dagger|\psi\rangle = \langle\psi|A|\alpha\rangle^*$$

- Es decir, la matriz del operador hermítico conjugado es la matriz conjugada traspuesta.

- Dado un operador lineal, A, se definen sus autovalores, a, y sus autovectores ψ a aquellos valores que cumplen

$$A|\psi\rangle = a|\psi\rangle$$

- Se define la traza de un operador como el valor

$$tr\{A\} = \sum_i \langle u_i|A|u_i\rangle$$

- Un operador lineal, *H*, es hermítico si es su propio conjugado.

$$H = H^{\dagger}$$

- Un operador lineal *I* es antihermítico si es el opuesto de su conjugado.

$$I = -I^{\dagger}$$

- Cualquier operador lineal se puede escribir de forma única como la suma de un operador hermítico y otro antihermítico

$$A = H_A + I_A \qquad H_A = (A + A^{\dagger})/2 \qquad I_A = (A - A^{\dagger})/2$$

- Se llama inverso de un operador A al operador A^{-1} que verifica

$$AA^{-1} = A^{-1}A = 1$$

- Un operador es unitario si su conjugado es su inverso.

$$UU^{\dagger} = U^{\dagger}U = 1$$

- Un proyector sobre el vector ψ es un operador P_ψ definido como

$$P_\psi|\varphi\rangle = |\psi\rangle(\langle\psi|\varphi\rangle) = (|\psi\rangle\langle\psi|)|\varphi\rangle$$

- Dado un conjunto de vectores ortonormales se puede definir el operador de proyección sobre el subespacio vectorial definido por dicho conjunto.

$$P_q = \sum_{i=1}^{q} |u_i\rangle\langle u_i|$$

- Los autovalores de un operador hermítico son valores reales.
- Los autovectores de un operador hermítico asociados a diferentes autovalores son ortogonales.
- Se dice que un operador es observable si es hermítico y sus autovectores forman una base.

- El formalismo anterior se aplica al estado de un sistema formado por una partícula elemental de masa m. Vamos a plantear ahora la representación de un sistema formado por dos partículas lo suficientemente separadas como para despreciar su interacción.
- Para este caso, la partícula 1 tendrá un estado $|\psi_1>$ definido sobre el espacio $\mathcal{E}_1$ y la partícula 2 tendrá un estado $|\psi_2>$ definido sobre el espacio $\mathcal{E}_2$.
- Vamos a desarrollar un formalismo para describir el conjunto de las dos partículas. Es lo que llamamos el producto tensorial $\otimes$

- Dados dos espacios de Hilbert, $\mathcal{E}_1$ y $\mathcal{E}_2$, se define el espacio producto tensorial $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2$ como el espacio formado por los vectores $|\psi_1,\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ con las siguientes propiedades:
- Linealidad con respecto al producto por escalares

$$(\lambda|\psi_1\rangle) \otimes |\psi_2\rangle = \lambda(|\psi_1\rangle \otimes |\psi_2\rangle)$$
$$|\psi_1\rangle \otimes (\lambda|\psi_2\rangle) = \lambda(|\psi_1\rangle \otimes |\psi_2\rangle)$$

- Distributividad frente a la suma

$$|\psi_1\rangle \otimes (|\psi_2\rangle + |\varphi_2\rangle) = (|\psi_1\rangle \otimes |\psi_2\rangle) + (|\psi_1\rangle \otimes |\varphi_2\rangle)$$
$$(|\psi_1\rangle + |\varphi_1\rangle) \otimes |\psi_2\rangle = (|\psi_1\rangle \otimes |\psi_2\rangle) + (|\varphi_1\rangle \otimes |\psi_2\rangle)$$

- Producto escalar

$$\langle\varphi_1, \varphi_2|\psi_1, \psi_2\rangle = \langle\varphi_1|\psi_1\rangle\langle\varphi_2|\psi_2\rangle$$

- Base del espacio producto tensorial: Si el conjunto $\{|u_i\rangle\}$ es una base del espacio $\mathcal{E}_1$ y el conjunto $\{|v_j\rangle\}$ es una base del espacio $\mathcal{E}_2$, el conjunto $\{|u_i\rangle \otimes |v_j\rangle\}$ forma una base del espacio $\mathcal{E}$.

$$|\psi\rangle = \sum_{i,j} c_{ij}(|u_i\rangle \otimes |v_j\rangle)$$

- Operadores: Dados los operadores A_1 y A_2 pertenecientes a los espacios $\mathcal{E}_1$ y $\mathcal{E}_2$, se define el operador $A_1 \otimes A_2$ como

$$(A_1 \otimes A_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A_1|\psi_1\rangle) \otimes (A_2|\psi_2\rangle)$$

- Operadores extendidos: Dado un operador A_1 definido en $\mathcal{E}_1$ se puede definir el operador extendido sobre $\mathcal{E}$ como

$$\tilde{A}_1(|\psi_1\rangle \otimes |\psi_2\rangle) = (A_1|\psi_1\rangle) \otimes |\psi_2\rangle$$

- La formulación matemática de la Mecánica Cuántica fue desarrollada durante las décadas de 1920 y 1930.
- La forma final de esta descripción se basa en un conjunto de postulados que fueron propuestos por Paul Dirac y John von Neumann en 1932.

- Primer postulado de la Mecánica Cuántica

  Hasta ahora hemos considerado el estado cuántico de una partícula, que viene descrito por su función de onda perteneciente al espacio $\mathcal{F}$. Hemos visto que se puede representar mediante un ket en un espacio $\mathcal{E}$. El primer postulado es una generalización para cualquier sistema físico, independientemente del número de partículas.

  – *Para un instante cualquiera t_0, el estado cuántico de un sistema físico está perfectamente determinado por un ket $|\psi(t_0)>$ perteneciente a $\mathcal{E}$.*

- Segundo postulado de la Mecánica Cuántica

  – *A toda magnitud física A medible sobre un sistema físico se le puede asociar un operador observable $\hat{A}$ que actua sobre el espacio de estados $\mathcal{E}$.*

- Tercer postulado de la Mecánica Cuántica

  - *Los únicos resultados posibles de la medida de la magnitud física A sobre el sistema físico son los autovalores del observable $\hat{A}$ asociado a la magnitud.*
  - *Como los observables son operadores hermíticos los resultados de las medidas serán siempre números reales.*

- Cuarto postulado de la Mecánica Cuántica
  - *Cuando la magnitud A se mide sobre un sistema físico caracterizado por el estado $|\psi>$, la probabilidad de obtener como resultado de la medida el valor a_n es*

$$Pr(a_n) = \sum_{m=1}^{g_n} \left|\langle \psi_n^m | \psi \rangle\right|^2$$

donde g_n es el índice de degeneración del autovalor a_n y $|\psi_n{}^m>$ son autovectores que forman una base en el subespacio del autovalor.

  - *Una vez realizada la medida, si el resultado corresponde al autovalor a_n el estado del sistema se transforma en la proyección sobre ese subespacio*

$$|\psi_n\rangle = \frac{\hat{P}_n|\psi\rangle}{\langle\psi|\hat{P}_n|\psi\rangle^{1/2}} \qquad \hat{P}_n = \sum_{m=1}^{g_n} |\psi_n^m\rangle\langle\psi_n^m|$$

- Quinto postulado de la Mecánica Cuántica
  - *La evolución temporal del estado del sistema, $|\psi>$, viene dada por la ecuación de Schrödinger, que en notación de Dirac se escribe*

$$\frac{ih}{2\pi}\frac{\mathrm{d}}{\mathrm{d}t}|\psi\rangle = \hat{H}|\psi\rangle$$

  - *Donde H es el observable asociado a la energía total del sistema, denominado Hamiltoniano. Puesto que el operador H es hermítico y la ecuación es lineal, se puede reescribir en forma de operador de evolución $\hat{U}(t,t_0)$*

$$|\psi(t)\rangle = \hat{U}(t, t_0)|\psi(t_0)\rangle$$

  - *Si el sistema es conservativo, H es independiente del tiempo y*

$$U(t, t_0) = \exp\left(-i\frac{2\pi}{h}H(t, t_0)\right)$$

- Principio de incertidumbre de Heisenberg
  - *Sean dos observables A y B, tales que su conmutador [A,B] = iC donde C es un operador arbitrario. Para cualquier estado $|\psi\rangle$ del sistema físico sobre el que se realice una medida simultánea de ambos observables se verifica que*

$$(\Delta\hat{A})^2(\Delta\hat{B})^2 \geq \frac{1}{4}\left|\langle\hat{C}\rangle\right|^2$$

  - donde ΔA y Δ B se refieren a las desviaciones estándar de las mediciones de los observables A y B y se pueden interpretar como una evaluación de la incertidumbre en estas mediciones.
  - Aplicados a la posición *x* y a la cantidad de movimiento *p* de una partícula, este principio (que es consecuencia de los postulados anteriores) implica que

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

- La Teoría de la Información Clásica fue propuesta por Claude Shannon en 1940.
- Esta teoría describe los procesos de comunicación de información de forma abstracta, independientemente de los soportes físicos sobre los que se desarrolle esta comunicación. De esta forma la Información se trata como una entidad cuantificable que puede estudiarse mediante modelos matemáticos.
- La unidad básica de información utilizada en esta teoría es una magnitud que pueda tener únicamente dos valores (que solemos denotar como 0 y 1).
- Esta unidad básica de información se denomina ***bit***.

- La Mecánica Cuántica ofrece la oportunidad de desarrollar una nueva Teoría Cuántica de la Información en la que las magnitudes o los canales de información estén representados mediante estados cuánticos.
- De forma análoga a la Teoría de la Información Clásica, la cantidad mínima de información que utilizada en la Teoría Cuántica de la Información es el ***quantum bit*** o ***qubit***.

- Definición de **Qubit**
  - Se denomina ***qubit*** a un estado cuántico asociado a un espacio de Hilbert bidimensional.
  - Un espacio de Hilbert bidimensional se puede generar a partir de una base ortonormal formada por dos kets: |0 > y |1 >.
  - La forma general de un *qubit* es

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

Donde $\mathbf{a_0}$ y $\mathbf{a_1}$ son números complejos.

  - Puesto que los estados cuánticos deben estar normalizados, los valores $\mathbf{a_0}$ y $\mathbf{a_1}$ deben cumplir que

$$|a_0|^2 + |a_1|^2 = 1$$

- Sistemas *multiqubit*
  - Supongamos un sistema formado por dos *qubits*. El espacio de estados del sistema se puede describir como el producto tensorial de los espacios de los *qubits*.

$$\mathcal{E}_{\text{Total}} = \mathcal{E}_1 \otimes \mathcal{E}_2$$

  - La base natural de este espacio estará formada por los estados

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

  - Un estado genérico estaría formado por una combinación lineal de los estados de la base

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

- Sistemas *multiqubit*
  - En general un sistema de N *qubits* estará representado por un espacio de Hilbert de dimensión 2^N.
  - Si consideramos un estado global formado por N estados independientes:

$$|\psi\rangle = (a_{10}|0\rangle + a_{11}|1\rangle) \otimes \ldots \otimes (a_{N0}|0\rangle + a_{N1}|1\rangle)$$

  - Este tipo de estados solo tienen 2N grados de libertad. Esto quiere decir que hay estados del espacio que no pueden descomponerse de esta forma, es decir, que no están formados por estados independientes.

- Entrelazamiento cuántico
  - La no separabilidad de un estado del espacio tensorial en estados de los espacios individuales fue estudiada por primera vez por Einstein, Podolsky y Rosen por lo que se conoce como paradoja EPR.
  - Esta propiedad de los estados cuánticos se conoce como **entrelazamiento** (*entanglement*) y supone que un estado entrelazado no puede describirse como partículas individuales sino como un estado global.
  - Este efecto es puramente cuántico y no tiene equivalencia en la formulación clásica.
  - El premio Nobel de Física de 2022 ha recaído en Alain Aspect, John F. Clauser y Anton Zeilinger por sus trabajos sobre entrelazamiento cuántico y sus aplicaciones.

- Puertas cuánticas
  - Una puerta cuántica es un dispositivo que permite transformar el estado de un conjunto de qubits.
  - Matemáticamente una puerta cuántica se puede describir como un operador de trasformación del estado cuántico.

$$|\psi'\rangle = A|\psi\rangle$$

- Puertas cuánticas
  - Puesto que los operadores son lineales, se pueden describir en forma matricial.
  - Por ejemplo, para un sistema formado por dos qubits los estados se pueden definir con combinación de la base |00>, |01>, |10>, |11>

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

  - El comportamiento de la puerta cuántica se puede describir como

$$\begin{bmatrix} a'_{00} \\ a'_{01} \\ a'_{10} \\ a'_{11} \end{bmatrix} = \begin{bmatrix} \langle 00|A|00\rangle & \langle 00|A|01\rangle & \langle 00|A|10\rangle & \langle 00|A|11\rangle \\ \langle 01|A|00\rangle & \langle 01|A|01\rangle & \langle 01|A|10\rangle & \langle 01|A|11\rangle \\ \langle 10|A|00\rangle & \langle 10|A|01\rangle & \langle 10|A|10\rangle & \langle 10|A|11\rangle \\ \langle 11|A|00\rangle & \langle 11|A|01\rangle & \langle 11|A|10\rangle & \langle 11|A|11\rangle \end{bmatrix} \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

- Teorema de no-clonación
  - Una de las propiedades que diferencian profundamente la Teoría de la Información Clásica y la Teoría de la Información Cuántica es la imposibilidad de copiar un estado cuántico desconocido.
  - Se puede entender esta imposibilidad como un corolario del principio de incertidumbre. Si se pudiera copiar un estado cuántico sería posible, por ejemplo, medir con exactitud la posición sobre el estado y la cantidad de movimiento sobre la copia, vulnerando de esa forma el principio de incertidumbre.
  - Matemáticamente podemos demostrar fácilmente este teorema considerando un sistema de dos qubits donde queremos generar una copia del primer qubit sobre el segundo.

- Teorema de no-clonación
  - Si suponemos que el segundo qubit comienza con el valor |0> la transformación debería corresponder a un operador que provocara el siguiente resultado:

$$C(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$$
$$C(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$$
$$C((a|0\rangle + b|1\rangle) \otimes |0\rangle) = (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle)$$

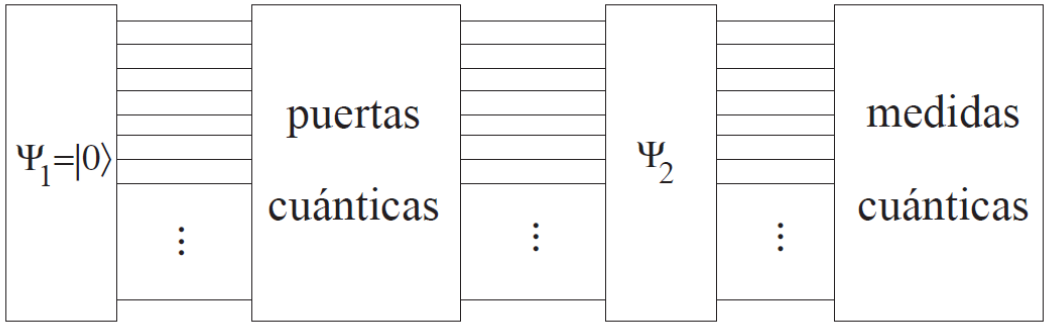
  - Los dos primeros resultados se refieren a la clonación de los estados de la base. Aplicando la linealidad de los operadores cuánticos el resultado en el caso general sería

$$C((a|0\rangle + b|1\rangle) \otimes |0\rangle) = a(|0\rangle \otimes |0\rangle) + b(|1\rangle \otimes |1\rangle)$$

  - Por tanto es imposible que el operador C genere el resultado deseado para el caso general

- Definición
  - El concepto de computación cuántica fue desarrollado a principios de la década de 1980, de manera independiente, por Paul Benioff y Richard Feynman.
  - La idea fundamental es trabajar con sistemas de N qubits entrelazados. De esta forma el estado del sistema es una combinación de los 2^N vectores de la base.

- Definición
  - Una computación cuántica consiste en aplicar una determinada transformación al sistema de N qubits mediante una aplicación sucesiva de puertas cuánticas y finalizar con un proceso de medida que obtiene un autovalor del operador asociado a la magnitud a medir.



- Propiedades
  - El creciente interés en la computación cuántica se debe a que potencialmente abre un camino para afrontar problemas que se consideraban intratables.
  - Es importante entender que la computación cuántica no permite resolver problemas indecidibles. No permite computar nada que no se pueda computar de forma tradicional.
  - Sin embargo, al trabajar de forma paralela sobre 2^N estados, la computación cuántica permitiría resolver en tiempo lineal los problemas que en computación clásica se resuelven en tiempo exponencial.
  - Es decir, la computación cuántica es un camino para resolver problemas NP de forma tratable.

- Puertas cuánticas
  - Una puerta cuántica es un dispositivo que permite realizar una transformación unitaria sobre un conjunto de qubits.
  - Por ejemplo, los operadores de Pauli son puertas cuánticas aplicables a 1 qubit.

$$\hat{I} = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$\hat{X} = |0\rangle\langle 1| + |1\rangle\langle 0|$$
$$\hat{Y} = |1\rangle\langle 0| - |0\rangle\langle 1|$$
$$\hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

- Puertas cuánticas
  - La puerta de Hadamard opera también sobre un único qubit y realiza una transformación de los estados |0> y |1> en una nueva base conocida como |+> |->.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Puertas cuánticas
  - La puerta de SWAP permite intercambiar los estados de dos qubits.

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

- Puertas cuánticas
  - Las puertas controladas operan sobre dos qubits donde el valor del primer qubit controla la aplicación de un operador al segundo qubit. Es decir, si el primer qubit es |0> el segundo qubit no cambia pero si el primer qubit es |1> el segundo qubit sufre la transformación Û.

$$P = |0\rangle\langle 0|\hat{I} + |1\rangle\langle 1|\hat{U}$$

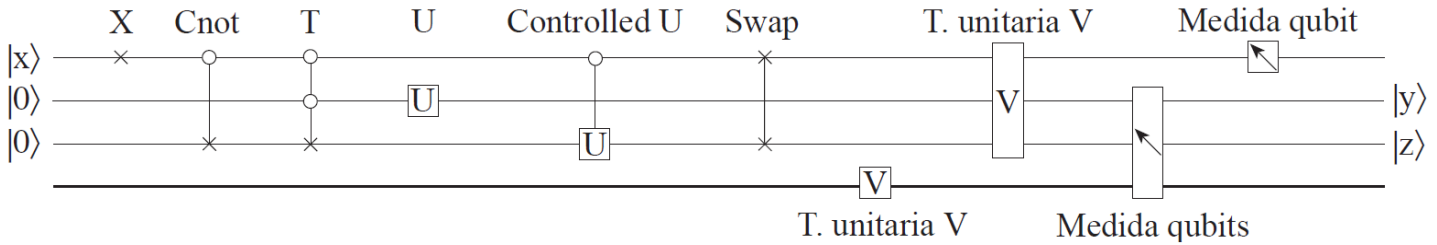
$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

- Puertas cuánticas
  - Los operadores de rotación o divisor de haz son puertas lógicas basadas en dos parámetros angulares θ y ϕ.

$$B(\theta,\phi) = \begin{bmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{i\phi}\sin\theta & \cos\phi \end{bmatrix}$$

- Puertas cuánticas
  - Cualquier circuito lógico se puede generar por medio de un conjunto finito de puertas lógicas. Por ejemplo, el conjunto {AND, OR y NOT} permite generar cualquier circuito lógico. La puerta NAND es capaz por si sola de generar cualquier circuito lógico.
  - Las transformaciones cuánticas, sin embargo, pueden ser infinitas ya que dependen de parámetros continuos (números complejos).
  - Sin embargo, cualquier puerta cuántica puede ser generada mediante la aplicación sucesiva de operadores de rotación y puertas NOT controladas.
  - En este sentido, las puertas NOT controladas y las rotaciones constituyen un conjunto de puertas cuánticas universales.

- Circuitos cuánticos
  - Dado que no es posible clonar los estado cuánticos, cualquier circuito cuántico se traduce en la aplicación sucesiva de puertas cuánticas a un grupo de qubits.
  - Estos circuitos se representan esquemáticamente como un conjunto de líneas (qubits) sobre las que se aplican las puertas cuánticas.



- Evaluación de funciones booleanas
  - Sea f una función booleana genérica que relaciona n bits de entrada con m bits de salida:

$$f: \quad \{0,1\}^n \rightarrow \{0,1\}^m$$

  - Para evaluar la función mediante computación cuántica se considera un espacio de n+m qubits de tal forma que se asocia a la función f el operador U_f con el siguiente comportamiento.

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

  - Donde $\oplus$ es el operador lógico XOR. Para cualquier función booleana es posible construir el operador U_f mediante puertas cuánticas.

- Algoritmo de Deutsch-Jozsa
  - Consideremos las funciones booleanas de un solo bit: {0,1}→{0,1}. Existen 4 funciones diferentes:

$$f_0: \begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 0 \end{matrix}, \quad f_1: \begin{matrix} 0 \mapsto 0 \\ 1 \mapsto 1 \end{matrix}, \quad f_2: \begin{matrix} 0 \mapsto 1 \\ 1 \mapsto 0 \end{matrix}, \quad f_3: \begin{matrix} 0 \mapsto 1 \\ 1 \mapsto 1 \end{matrix}$$

  - De estas 4 funciones, dos son funciones constantes (f_0 y f_3) y dos son funciones equilibradas (f_1 y f_2).
  - Supongamos que tenemos una función desconocida f y queremos saber si es constante o equilibrada. En un sistema clásico la única forma sería evaluar $f(0)$ y $f(1)$ para comprobar si f es constante o equilibrada.
  - El algoritmo de Deutsch resuelve este problema con una única evaluación por medio de computación cuántica.

- Algoritmo de Deutsch-Jozsa
  - Supongamos que disponemos del operador U_f asociado a la función desconocida *f*.
  - Partiendo del estado |0>|0> se van a aplicar tres puertas cuánticas. En primer lugar la negación del segundo qubit, a continuación el operador de Hadamard sobre el primer qubit y por último el operador de Hadamard sobre el segundo qubit.

$$|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |1\rangle \rightarrow \frac{1}{\sqrt{2}}((|0\rangle + |1\rangle) \otimes |1\rangle)$$

$$\rightarrow \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}((|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle))$$

- Algoritmo de Deutsch-Jozsa
  - Expresando los valores binarios de forma compacta

$$|00\rangle \rightarrow \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

  - Si aplicamos el operador U_f sobre este estado

$$\frac{1}{2}U_f(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|0f(0)\rangle - |0\overline{f(0)}\rangle + |1f(1)\rangle - |1\overline{f(1)}\rangle)$$

$$= \begin{cases} \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) & si \quad f = f_0 \\ \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) & si \quad f = f_1 \\ -\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) & si \quad f = f_2 \\ -\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) & si \quad f = f_3 \end{cases}$$

- Algoritmo de Deutsch-Jozsa
  - Si sobre el resultado anterior vuelven a aplicarse los operadores de Hadamard sobre el primer y el segundo qubit,

$$H_2 U_f H_2 |01\rangle = \begin{cases} |01\rangle & si \quad f = f_0 \\ |11\rangle & si \quad f = f_1 \\ -|11\rangle & si \quad f = f_2 \\ -|01\rangle & si \quad f = f_3 \end{cases}$$

  - Es decir, haciendo una medida directa sobre el primer qubit sabríamos si su valor es paralelo a |0> o a |1> y sabríamos con una sola evaluación de U_f si la función es constante (f_0 y f_3) o equilibrada (f_1 y f_2).

- Algoritmo de Deutsch-Jozsa
  - El algoritmo básico de Deutsch se refiere a funciones de un único bit.
  - Una generalización de este resultado fue propuesta por Jozsa y se refiere a funciones de n bits. La idea es distinguir entre funciones de n bits constantes (solo 0 o 1) o balanceadas (el mismo número de 0s que de 1s).
  - Para n bits hay 2^n posibles valores de entrada. La única forma clásica de verificar que la función es constante y no balanceada es realizar $2^{(n-1)}+1$ pruebas.
  - Para resolverlo mediante computación cuántica el esquema es exactamente igual que para funciones de 1 bit. En este caso se consideran n+1 bits y se aplican los operadores de Hadamard sobre todos ellos.
  - De esta forma se resuelve en una única iteración cuántica un problema que requiere un tiempo exponencial en computación clásica.

- Algoritmo de búsqueda de Grover
  - Consideremos el problema de encontrar un cierto elemento en una lista desordenada de tamaño N. Desde un punto de vista clásico la única forma de encontrar el elemento es mediante ensayo y error y el número medio de búsquedas a realizar será N/2.
  - El algoritmo propuesto por Grover utiliza computación cuántica para lograr un número medio de búsquedas de orden $N^{1/2}$.
  - Sea $P(x)$ la función booleana que verifica si el elemento x es el buscado. Es decir, $P(x)$=1 si el elemento buscado está en la posición x de la lista y $P(x) = 0$ en otro caso.
  - Sea U_P la descripción de la función P mediante puertas cuánticas de forma que

$$U_P|x, b\rangle \rightarrow |x, b \oplus P(x)\rangle$$

- Algoritmo de búsqueda de Grover
  - Uno de los ejemplos de uso del algoritmo de Grover es la búsqueda de una clave. Generalmente los valores de las claves no se almacenan directamente sino que se almacena su valor encriptado. La función de encriptado debe ser fácil de ejecutar y su inversa debe ser computacionalmente intratable. Para verificar si una clave es correcta se ejecuta la función de encriptado y se compara con el valor almacenado. La función $P(x)$ consiste entonces en ejecutar la función de encriptado y comparar el resultado.

- Algoritmo de búsqueda de Grover
  - El primer paso del algoritmo consiste en generar un estado cuántico que sea la superposición de todos los posibles valores. Para ello no hay más que aplicar el operador de Hadamard sobre los qubits.

$$|0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x\rangle$$

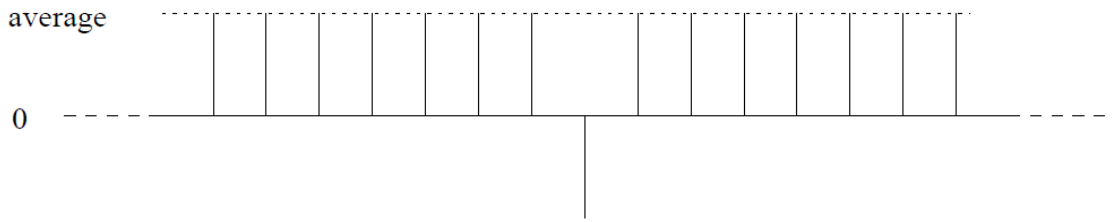
  - El estado cuántico inicial del último qubit se genera con el siguiente valor:

$$|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

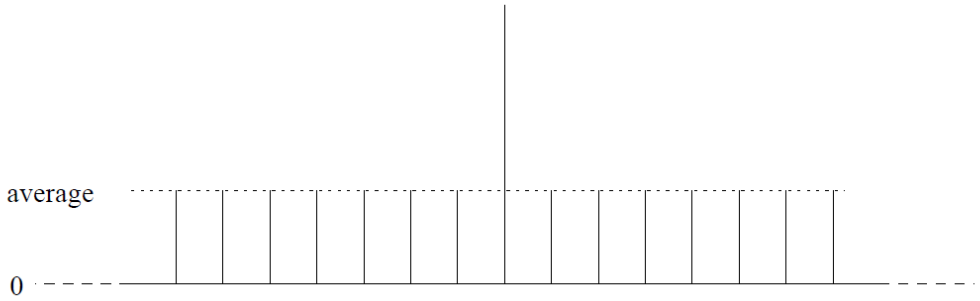
- Algoritmo de búsqueda de Grover
  - El segundo paso es aplicar el operador U_P a este estado generando

$$U_P\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{n-1}|x\rangle\otimes|b\rangle\right)\rightarrow\frac{(-1)^{P(x)}}{\sqrt{2^n}}\sum_{x=0}^{n-1}|x,b\rangle$$

  - Es decir, el efecto del operador es un estado en el que todos los valores tienen la misma amplitud excepto el que corresponde al valor buscado, que tiene la amplitud negativa.



- Algoritmo de búsqueda de Grover
  - Realizar una inversión respecto a la media para incrementar la amplitud del estado que estamos buscando



  - Para realizar este proceso se utiliza la siguiente transformación (donde A es el valor medio de a_i)

$$\sum_{i=0}^{N-1} a_i |x_i\rangle \rightarrow \sum_{i=0}^{N-1} (2A - a_i)|x_i\rangle$$

- Algoritmo de búsqueda de Grover
  - El proceso de inversión respecto a la media se puede generar mediante la siguiente matriz, que puede ser generada por medio de puertas cuánticas

$$D = \begin{pmatrix} \left(\frac{2}{N} - 1\right) & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \left(\frac{2}{N} - 1\right) & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \left(\frac{2}{N} - 1\right) \end{pmatrix}$$

- Algoritmo de búsqueda de Grover
  - Si se repite la acción de cambiar el signo e invertir la amplitud respecto a la media se puede ir aumentando la amplitud del estado buscado hasta acercarlo a la unidad.
  - La amplitud máxima se obtiene después de $\pi/4\ N^{1/2}$ iteraciones. Por encima de este número la amplitud del estado buscado comienza a reducirse.
  - El algoritmo consiste, por tanto, en repetir el procedimiento $\pi/4\ N^{1/2}$ veces y a continuación leer el estado de los qubits que, con gran probabilidad, responderán al estado buscado.

- Algoritmo de búsqueda de Grover
  - Si pretendemos encontrar una clave de 70 bits (por ejemplo, una clave de 10 caracteres en ASCII) realizando una búsqueda por fuerza bruta necesitaríamos probar como término medio 2^{69} claves. Si nuestro sistema informático consigue realizar un millón de pruebas por segundo la búsqueda tardaría unos 18 millones de años.
  - El algoritmo de Grover tiene una complejidad de orden $O(n^{1/2})$ por lo que el número de ejecuciones sería de 2^{35}. Si se pudieran hacer también un millón de pruebas por segundo la búsqueda tardaría unas 9,5 horas.

- Algoritmo de factorización de Shor
  - Se denomina factorizar un número natural N a encontrar dos números n y m tales que $N=n \cdot m$. Si el número N es primo los únicos factores son 1 y N. El problema de búsqueda de los factores de un número natural es de orden exponencial respecto al número de dígitos de N, $\log_2(N)$.
  - El algoritmo de criptografía RSA se basa en utilizar como clave pública un número natural que es producto de dos números primos. Para un número de dígitos lo suficientemente grande se asume que el cálculo de los factores de N es un problema intratable y que es imposible obtener la clave privada (los factores de N) a partir de la clave pública (N).
  - El algoritmo de Shor es un algoritmo de computación cuántica que permite factorizar un número natural en un tiempo polinómico.

- Algoritmo de factorización de Shor
  - Periodo de una función sobre números naturales $f(x)$ es el valor p tal que $\forall x,\ f(x+p)=f(x)$. Por ejemplo, para la función resto de la división por n ($mod\ n$) el periodo es n.
  - Dado el número natural N que pretendemos factorizar, se elige un número aleatorio $y<N$. Si el máximo común divisor $mcd(y,N)$ es distinto de 1, entonces se habrá encontrado un factor de N. En general el número y será tal que $mcd(y,N)=1$.
  - Se puede obtener la factorización de N a partir del periodo p de la función $f_N(x)=y^x \bmod N$.
  - Sea $c = y^{p/2} \bmod N$. Si $c\neq 1$, los factores de N son $mcd(c+1,N)$ y $mcd(c-1,N)$. Si c=1 o p es impar hay que intentarlo de nuevo con un nuevo y aleatorio.
  - El algoritmo de Shor permite calcular el periodo en un tiempo $O(\log N)^3$

- Algoritmo de factorización de Shor
  - Para calcular el periodo de una función $P(x)$ de n bits se utiliza un sistema con $2n$ qubits y se construye el operador U_P tal que

$$U_P|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$$

  - El algoritmo comienza utilizando el operador de Walsh-Hadamard para convertir el estado |0> en una combinación de todos los estados base.

$$H_n|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

  - A continuación se utiliza el operador U_P para obtener en paralelo el resultado de la función sobre todas las entradas.

$$U_P H_n|0\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

- Algoritmo de factorización de Shor
  - El siguiente paso es realizar una medida sobre los n qubits del resultado. Si se mide un valor *t* el resultado de la medida es que el estado cuántico colapsa en un estado en el que los n qubits del resultado representan el valor *t* y los *n* primeros qubits corresponden a los valores de *x* tal que $P(x) = t$.
  - Puesto que la función *P* es periódica los valores de los primeros *n* qubits cumplen que $x = d + c \cdot p$, donde *d* es un desplazamiento, *p* es el periodo de la función *P* y c=0,1,2,3 … M-1. El valor de *M* es aproximadamente $2^n/p$.

$$\frac{1}{\sqrt{M}} \sum_{c=1}^{M-1} |d + c \cdot p\rangle |t\rangle$$

- Algoritmo de factorización de Shor

  – Una vez obtenido un estado formado por *M* valores de *x* separados por una cantidad *p* el siguiente paso es aplicar una *Transformada Discreta de Fourier*. El operador U_{FTT} tiene el siguiente comportamiento

$$U_{FTT}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{i2\pi kx/2^n}|k\rangle$$

- Algoritmo de factorización de Shor

  - Aplicando el operador U_{FTT} al resultado anterior

$$U_{FTT}\ \frac{1}{\sqrt{2^n/p}}\sum_{c=1}^{2^n/p-1}|d+c\cdot p\rangle\ =\ \frac{1}{\sqrt{p}}\sum_k \tilde{f}(k)|k\rangle$$

  - Donde

$$|\tilde{f}(k)|\ =\ \begin{cases}1 & \text{si } k \text{ es múltiplo de } \left(\frac{2^n}{p}\right)\\ 0 & \text{en otro caso}\end{cases}$$

  - Es decir, tomando una medida del registro el resultado es un múltiplo de $2^n/p$, lo que nos permite calcular el periodo p.

- David J. Santos, "*Una breve introducción al procesado cuántico de la información*", Departamento de Teoría de la Señal y Comunicaciones, Universidad de Vigo, 2003.
- Grupo de Computación Cuántica del Departamento de Matemática Aplicada, "*Introducción al modelo cuántico de computación*", Technical report 19, Universidad Politécnica de Madrid, 2003.