Introducción a la Computación Cuántica

Aridane Rodríguez Moreno

12 de octubre de 2022

El propósito de este escrito es dar los suficientes conocimientos técnicos-matemáticos para poder entender conceptos más avanzados en el sector de la computación cuántica. Aquí no trataremos los conceptos físicos más allá de la naturaleza cuántica de la materia que nos permite realizar todo este desarrollo matemático. Estos apuntes son principalmente obtenidos a través de las clases públicas de computación cuántica por el Instituto de Matemáticas de la UNAM con las correcciones oportunas. Los requisitos mínimos para seguir estos apuntes es tener conocimiento de álgebra lineal. Gracias a este podemos ver todo el potencial que nos daría los ordenadores cuánticos, la computación cuántica es otra demostración de la creatividad e ingenio del ser humano al avanzar en el entendimiento de la naturaleza.

Este escrito puede ser actualizado en un futuro, por los posibles errores que pueda tener y/o para mejorar el entendimiento del mismo. Por favor, cualquier posible error que vea puede contactar conmigo a través de mi página personal https://aridanerodriguez.com.

1. Modelización matemática de los qubits

En esta sección introduciremos los conceptos y definiciones más importantes para la modelización de los qubits. Esta modelización la podemos realizar a través de álgebra lineal y nos permitirá empezar a comprender los algoritmos cuánticos, que introduciremos más adelante, y a través de los mismos entender porque los ordenadores cuánticos son tan interesantes.

Empezaremos introduciendo las propiedades físicas del qubits, sin entrar en detalles, para relacionar estas con los conceptos tan bien conocidas del álgebra lineal.

En la computación clásica la unidad básica de información es el bit, que tiene dos estados 0 y 1. Es decir, puedo modelizar dos posibles estados de un objeto a través de un bit. Por ejemplo, podemos modelizar si una lámpara está encendida con el bit igual a 1 y si está apagada con el bit igual a 0.

Mientras que en la computación cuántica la unidad básica de información es el qubit cuyos estados pueden ser $|0\rangle$, $|1\rangle$ (donde $|\cdot\rangle$ es la notación de Dirac) o un estado de superposición, una combinación de estos dos estados. Esto es gracias al principio de superposición, y el ejemplo más conocido es el gato de Schrödinger.

A diferencia de la computación clásica, en la computación cuántica no podemos saber el estado de los qubits, en el momento que observemos el qubit, el estado de superposición colapsará a uno de los estados $|0\rangle$ o $|1\rangle$. Pero estos estados de superposición podemos manipularlos sin observarlos. Esto es lo que hace interesante la computación cuántica.

Introduciremos los estados de un qubit, $|0\rangle$ y $|1\rangle$ como los vectores $\binom{1}{0}$ y $\binom{0}{1}$, respectivamente, que forman una base del espacio vectorial $\mathbb{C}^2$, usamos el cuerpo de los números complejos porque representan mejor los estados de un qubit en la realidad. Además, sabemos que los qubits pueden estar en una combinación de estos dos estados y al observarlos se transformará a uno de ellos con una cierta probabilidad, a esto lo modelizaremos a través de una combinación lineal de estos estados.

Definición 1.1 *A los estados* $|0\rangle$ *y* $|1\rangle$ *se les denominan* ***estados básicos****. Un* ***estado de superposición*** *de un qubit es una combinación lineal*

$$\alpha_0\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) + \alpha_1\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) \equiv \alpha_0|0\rangle + \alpha_1|1\rangle\,, \quad \alpha_0, \alpha_1 \in \mathbb{C}$$

tal que $|\alpha_0|^2 + |\alpha_1|^2 = 1$*. A* α_0 *y* α_1 *los llamamos* ***amplitud*** *de* $|0\rangle$ *y* $|1\rangle$*, respectivamente.*

Al observar un qubit en un estado de superposición colapsará al estado $|0\rangle$ con probabilidad $|\alpha_0|^2$ y al estado $|1\rangle$ con probabilidad $|\alpha_1|^2$.

La notación de un qubit podemos extenderlos a varios qubits de manera que forman un subconjunto del espacio vectorial $\mathbb{C}^{2^n}$.

Definición 1.2 *Para* n *qubits cada estado básico representa un vector básico de* $\mathbb{C}^{2^n}$ *y se denotan por* $\underbrace{|0\cdots0\rangle}_{n}$, $\underbrace{|0\cdots1\rangle}_{n}$, $\cdots$, $\underbrace{|1\cdots1\rangle}_{n}$ *los* 2^n *estados básicos de* n *qubits.*

Cada dígito en la notación de Dirac $|\cdot\rangle$ representa un qubit. Es decir, el número de dígitos de un estado básico es el número total de qubits de un sistema.

Definición 1.3 *Sean* n *qubits , a cada estado básico le corresponde a un número natural* $0 \leq a \leq 2^n - 1$ *en expresión binaria de* n *dígitos,* $a_{2,n}$*. Por tanto, cada estado básico representa un vector de la base de* $\mathbb{C}^{2^n}$*,*

$$|a_{2,n}\rangle = \left.\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix}\right\} 2^n, \qquad \textit{estando el } 1 \textit{ en la posición } a+1\textit{, siendo la primera posición el } 1.$$

Ejemplo 1.1 *Si tomamos* $a = 1$ *y* $n = 2$ *tenemos que*

$$|0\ 1\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

que es un estado básico para el caso de 2 *qubits.*

Si ahora tomamos $a = 3$ *y* $n = 3$ *tenemos*

$$|0\ 1\ 1\rangle = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}$$

$|a_{2,n}\rangle = |00011\rangle = (00010000)$ *que es un estado básico para el caso de 3 qubits.*

Definición 1.4 *Los estados en superposición de n qubits son combinaciones lineales de la forma*

$$\alpha_0 \underbrace{|0\cdots 0\rangle}_{n} + \cdots + \alpha_{2^n-1} \underbrace{|1\cdots 1\rangle}_{n} \quad \text{con } \alpha_i \in \mathbb{C}$$

tal que $|\alpha_0|^2 + \cdots + |\alpha_{2^n-1}|^2 = 1$.

Ejemplo 1.2 *Sean* 2 *qubits, tomando* $n = 2$ *en la definición anterior, tenemos que los estados básicos son*

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Y los estados de superposición $\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$.

Definiremos ahora la operación que nos permitirá relacionar los estados básicos de un sistema de varios qubits con los de un solo qubits y poder trabajar con ellos de manera más eficaz.

Definición 1.5 *El* ***producto de Kronecker*** *entre* $\mathbb{C}^n$ *y* $\mathbb{C}^m$ *es*

$$\begin{aligned} \otimes : \mathbb{C}^n \times \mathbb{C}^n &\longrightarrow \mathbb{C}^{n+m} \\ (u, v) &\longmapsto (u_1 \cdot v, \cdots, u_n \cdot v) \end{aligned}$$

donde $(u_1, \cdots, u_n)$ *son las componentes del vector* u.

Ejemplo 1.3 *Para* $n = 2$.

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1 \cdot \begin{pmatrix}1\\0\end{pmatrix}\\ 0 \cdot \begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

Proposición 1.1 *Para todo número natural* n *y* a *tal que* $0 \leq a \leq 2^n - 1$. *Se tiene que un estado básico de un sistema de* n *qubits,* $|a_{2,n}\rangle$, *es igual al producto de los estados básicos de los qubits individuales.*

Definición 1.6 *Decimos que un conjunto de qubits están en estado* ***producto*** *si su estado se puede poner como producto de los estados de sus componentes. En el caso contrario decimos que están en estado de* ***entrelazamiento***.

Ejemplo 1.4 *Por la proposición 1.1 tenemos que los estados básicos son estados productos. Y un ejemplo de estado no básico que es un estado producto es el siguiente:*

$$\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

Estos últimos estados de superposición son muy importantes y se suelen denotar de la siguiente manera,

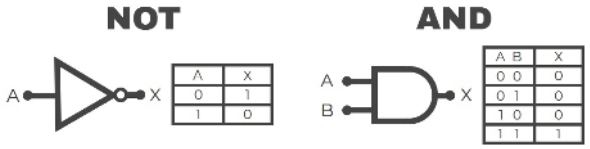
$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \\ |-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \end{aligned} \tag{1}$$

Otro estado importante de un sistema de dos qubits es

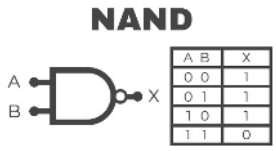
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad \text{llamado par EPR o Estado de Bell.}$$

2. Puertas cuánticas

En computación clásica se manipula la información almacenada en un conjunto de bits usando **puertas lógicas** como la puerta unitaria NOT o la puerta binaria AND.



Una puerta particularmente importante en computación clásica es la puerta NAND, que surge al aplicar una puerta NOT al resultado de una puerta AND, representado de la forma



Esta puerta es importante por su propiedad de **universalidad**, que indica que cualquier circuito lógico clásico se puede obtener como concatenación de puertas NAND.

En computación cuántica, se manipula la información almacenada en un conjunto de qubits usando **puertas cuánticas**. Estas puertas son una generalización de las puertas lógicas clásicas. En el caso de la computación clásica definimos el resultado a través de los estados 0 y 1, los únicos que existen. En el caso cuántico hace falta definir los estados de superposición.

Para lidiar con estos estados, se le exige a las puertas cuánticas que sean lineales, de forma que solo hay que definir el valor de los estados básicos. Es decir, serán funciones lineales de la forma $p : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$. Y por lo tanto, las puertas cuánticas quedarán caracterizadas por una matriz A de la forma

$$\begin{aligned} p : \mathbb{C}^{2^n} &\longrightarrow \mathbb{C}^{2^n} \\ x &\longmapsto Ax \end{aligned}$$

Además, si tenemos un estado de un conjunto de qubits y le aplicamos una puerta p, el resultado tiene que ser un estado válido, es decir, la suma de los cuadrados de los módulos de las amplitudes tiene que seguir siendo 1, lo que implica que la matriz A sea **unitaria**. Esto implica que todas las puertas cuánticas son reversibles, en oposición a las puertas clásicas. Esto tiene consecuencias muy interesantes que no veremos aquí.

A continuación definiremos algunas de las puertas cuánticas más importantes.

Definición 2.1 *El "equivalente" cuántico a la puerta NOT para un qubit, se llama puerta* X *y está definida por*

$$\begin{aligned} |0\rangle &\longrightarrow |1\rangle \\ |1\rangle &\longrightarrow |0\rangle \end{aligned}$$

caracterizada por la matriz $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Definición 2.2 *La puerta Z está definida de forma matricial como*

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Esta puerta cambia el signo de la amplitud del estado $|1\rangle$.

Definición 2.3 *La puerta* ***Hadamard*** H *está definida de forma matricial como*

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

Esta última tiene el efecto de transformar el estado $|0\rangle$ al estado $|+\rangle$ y el estado $|1\rangle$ al estado $|-\rangle$ definidos en (1). Esta puerta se utiliza en muchos algoritmos cuánticos, ya que nos permite poner los qubits en un estado de superposición.

También existen puertas cuánticas de varios qubits. Una de los más importantes es CNOT ("controlled NOT"), cuyo efecto es transformar los estados $|x\ y\rangle$ a $|x\ (y+x)_2\rangle$ donde $x, y \in \{0, 1\}$.

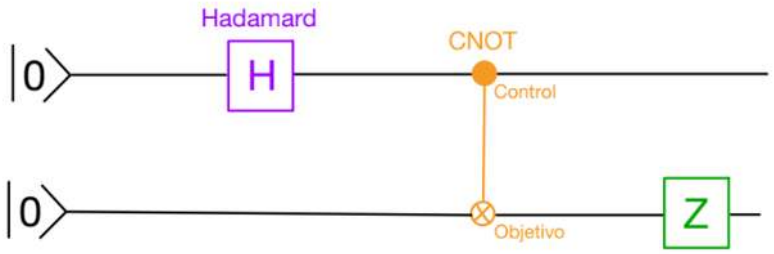
Podemos describir su funcionamiento del siguiente modo. El primer qubit se llama control y el segundo objetivo. Si el control vale 0 el objetivo no cambia y si el control vale 1, negamos el objetivo. En notación matricial:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

3. Circuitos cuánticos

Los circuitos cuánticos son concatenaciones de puertas cuánticas. Consta de cables horizontales (uno por qubit) y se lee de izquierda a derecha. Sobre esos cables colocamos las puertas cuánticas.

Figura 1: Ejemplo de circuito cuántico



En el ejemplo anterior tenemos un sistema formado por dos qubits con un estado inicial $|00\rangle$ donde se le aplica puertas cuánticas.

El circuito empieza realizando una puerta Hadamard al primer qubit, lo que resulta en

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle,$$

después se aplica la puerta binaria, CNOT, que nos da como resultado

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

y finalmente se aplica la puerta unitaria Z al segundo qubit,

$$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle.$$

En resumen, este circuito transforma el estado básico $|00\rangle$ al estado de entrelazamiento

$$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle.$$

3.1. Algunas puertas destacadas que aparecen en circuitos cuánticos

Definición 3.1 *La puerta* ***Controlled-****U donde U es una operación en n qubits. Es una puerta de* $n+1$ *qubits donde el primero qubit se llama* ***control****. Si el control es* 0 *no hace nada y si es* 1 *aplica U al resto de qubits. Como ejemplo tenemos la puerta CNOT.*

Definición 3.2 *La puerta* ***Medida*** *convierte un qubits en estado* $\alpha_0|0\rangle + \alpha_1|1\rangle$ *en un bit clásico que valdrá* 0 *con probabilidad* $|\alpha_0|^2$ *y* 1 *con probabilidad* $|\alpha_1|^2$*. El bit clásico se representa en el circuito con un cable doble.*

Figura 2: Representación de la puerta medida

3.2. Teleportación cuántica

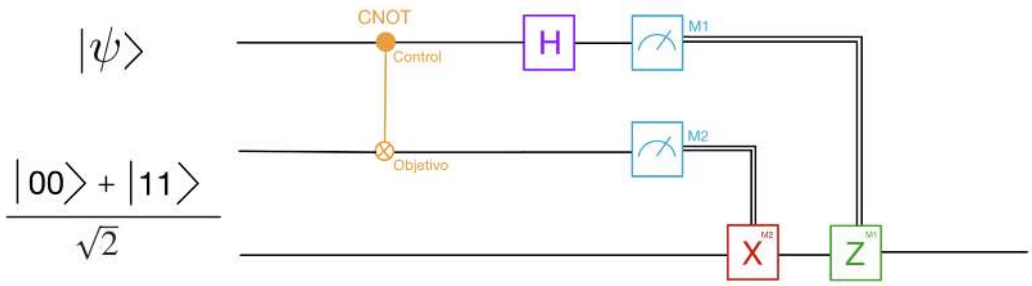
Veamos un caso práctico de un circuito cuántico. Supongamos que Alice y Bob comparten un par EPR, es decir dos qubits en estado $(\sqrt{2})^{-1}(|00\rangle + |11\rangle)$, y Alice necesita enviarle un qubit a Bob, sea $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. Bob no sabe el que estado del qubit que le quiere enviar Alice, y si Bob lo observa colapsará en un estado básico $|0\rangle$ o $|1\rangle$.

Una solución a este problema sería utilizar **teleportación cuántica**, el proceso para enviar información cuántica a través de un canal clásico. En nuestro caso, esta información cuántica no es nada más que las amplitudes α_0 y α_1 del qubit que quiere mandar Alice $|\psi\rangle$.

3.2.1. Proceso de teleportación cuántica

Partimos de un estado inicial donde tenemos 3 qubits, el qubit que quiere enviarle Alice a Bob $|\psi\rangle$ y el par EPR que comparte Alice y Bob.

Figura 3: Circuito de la teleportación cuántica



Con este circuito cuántico, Bob podrá recibir el qubit de Alice a través de 2 bits clásicos. Veamos paso a paso lo que sucede en el circuito.

Como el qubit de Alice $|\psi\rangle$ y el par EPR no están entrelazados, el estado inicial del sistema será:

$$|\psi\rangle \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left(\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|100\rangle + \alpha_1|111\rangle\right).$$

Se aplica la puerta CNOT con control el primer qubit y objetivo el segundo qubit,

$$\frac{1}{\sqrt{2}}\left(\alpha_0|000\rangle + \alpha_0|011\rangle + \alpha_1|110\rangle + \alpha_1|101\rangle\right) = \frac{1}{\sqrt{2}}\left(\alpha_0|0\rangle\left(|00\rangle + |11\rangle\right) + \alpha_1|1\rangle\left(|10\rangle + |01\rangle\right)\right)$$

A continuación se aplica una Hadamard al primer qubit,

$$\frac{1}{\sqrt{2}}\big(\alpha_0|+\rangle\left(|00\rangle + |11\rangle\right) + \alpha_1|-\rangle\left(|10\rangle + |01\rangle\right)\big) =$$
$$\frac{1}{\sqrt{2}}\big(\alpha_0\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(|00\rangle + |11\rangle\right) + \alpha_1\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(|10\rangle + |01\rangle\right)\big).$$

Operando se puede llegar a al siguiente expresión, donde se agrupa los dos primeros qubits que son los qubits de Alice.

$$\frac{1}{2}\Big[|00\rangle\left(\alpha_0|0\rangle + \alpha_1|1\rangle\right) + |01\rangle\left(\alpha_0|1\rangle + \alpha_1|0\rangle\right) + |10\rangle\left(\alpha_0|0\rangle - \alpha_1|1\rangle\right) + |11\rangle\left(\alpha_0|1\rangle - \alpha_1|0\rangle\right)\Big].$$

A continuación se mide los dos primeros qubits, los de Alice. Al hacer esto, Alice obtendrá dos bits clásicos que enviará a Bob y además colapsará el tercer qubit a uno de los estados de arriba. Si el

primer bit es 1 se aplica una puerta Z al qubit de Bob que cambiará el signo de la amplitud de $|1\rangle$, en caso contrario no se aplica la puerta cuántica. Si el segundo bit es 1 se aplica una puerta X que intercambia las amplitudes. Y en caso de que ambos bits sean 1 se aplica primero la puerta X y luego Z.

Así, el qubit EPR inicial de Bob está en el mismo estado que el qubit que quería mandar Alice a Bob $|\psi\rangle$. Hemos teletransportado el qubit de Alice.

4. Algoritmos cuánticos

4.1. Introducción a algoritmos cuánticos

En esta sección vamos a introducir el paralelismo cuántico y algunos algoritmos cuánticos más sencillos como el algoritmo de Deutsh y finalizaremos, nombrando y sin detallar, con el que es posiblemente el algoritmo cuántico más famoso, el algoritmo de Schor.

Definición 4.1 *Se define el* ***paralelismo cuántico*** *como la capacidad de un ordenador cuántico para evaluar una función $f(x)$ para los valores de x de forma simultánea. Donde $f(x) : \{0,1\}^n \to \{0,1\}$.*

Proposición 4.1 *Dado un par de qubits en estado $|x\ y\rangle$ podemos construir una cadena de puertas cuánticas que realice la transformación $|x\ y\rangle \to |x\ y + f(x)\rangle$. El primer qubit se llama control y el segundo objetivo. Esta transformación se denota $\bigcup_f$ y es unitaria. Si el objetivo es cero, el estado final será $|x\ f(x)\rangle$.*

Demostración. Vamos a demostrar que $\bigcup_f$ es unitaria. Tenemos cuatro posibles funciones f:

$$f_1(x) = \begin{cases} 0 & \text{si } x = 1 \\ 1 & \text{si } x = 0 \end{cases} \qquad f_2(x) = \begin{cases} 1 & \text{si } x = 1 \\ 0 & \text{si } x = 0 \end{cases}$$

$$f_3(x) = 0 \qquad\qquad f_4(x) = 1$$

Y las matrices asociadas a la transformación $\bigcup_f$ a cada una de ellas son

$$\bigcup_{f_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \bigcup_{f_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\bigcup_{f_3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \bigcup_{f_4} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Y se puede comprobar fácilmente que todas las matrices son unitarias.

□

Dado un circuito clásico para calcular f existe un circuito cuántico de eficiencia comparable que calcula $\bigcup_f$.

Proposición 4.2 *Tenemos la siguiente transformación*

$$|x\ 0\rangle \to |x\ f(x)\rangle$$
$$|x\ 1\rangle \to |x\ 1 + f(x)\rangle$$

se tiene que $|x\rangle|-\rangle \to (-1)^{f(x)}|x\rangle|-\rangle$ donde $|x\rangle$ es un estado básico.

Demostración.

$$|x\rangle|-\rangle = |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|x\ 0\rangle - |x\ 1\rangle}{\sqrt{2}}\right) \xrightarrow{\bigcup_f} \left(\frac{|x\ f(x)\rangle - |x\ 1 + f(x)\rangle}{\sqrt{2}}\right)$$

Si $f(x) = 0$,

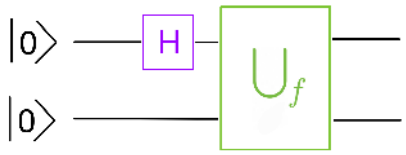
$$\left(\frac{|x\ 0\rangle - |x\ 1\rangle}{\sqrt{2}}\right) = (-1)^0|x\rangle|-\rangle$$

Si $f(x) = 1$,

$$\left(\frac{|x\ 1\rangle - |x\ 0\rangle}{\sqrt{2}}\right) = (-1)^1|x\rangle|-\rangle$$

□

Ejemplo 4.1 *En este circuito cuántico,*



es fácil comprobar que obtenemos el estado final

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

En general podemos preparar $n+1$ qubits en estado $|0\rangle$ y aplicar a los n primeros qubits $H^{\times n}$, esto es aplicar una puerta Hadamard a cada qubit siendo n el número de qubits. Y finalmente aplicando $\bigcup_f$ a los $n+1$ qubits se obtiene el estado

$$\frac{1}{\sqrt{2^n}}\sum_x |x\ f(x)\rangle.$$

Realizando este procedimiento conseguimos una evaluación simultánea de todos los posibles estados. El problema es que al medir colapsará a un estado básico. Para que esto no sea un inconveniente tenemos que ser capaces de obtener información de los valores de $f(x)$ a partir del estado de superposición.

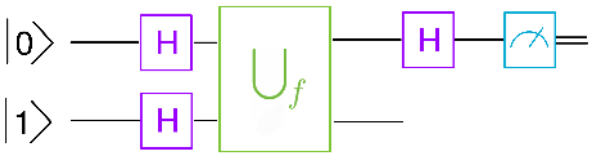
4.2. Algunos algoritmos cuánticos

A continuación veremos algunos algoritmos cuánticos, empezando por el algoritmo de Deutsh, uno de los más sencillos que trataremos con detalle, seguiremos con su generalización Deutsh-Jorza, y finalizaremos viendo la transformación cuántica de Fourier y el algoritmo de Shor.

4.2.1. Algoritmo de Deutsh

El problema que resuelve el algoritmo de Deutsh es cuando estamos en un sistema de dos qubits y queremos saber si $f(0) = f(1)$ o $f(0) \neq f(1)$. En computación clásica el algoritmo sería parecido a esto: return$(f(0) == f(1))$. Es decir que estamos evaluando la función f dos veces. Mientras que el algoritmo de Deutsh solo necesita de una evaluación de $\bigcup_f$ para obtener la solución. El circuito es el siguiente,

Figura 4: Circuito del algoritmo de Deutsh



Veamos paso a paso el circuito. Primero se aplica $H^{\times 2} = H \times H$ a $|0\ 1\rangle$ y obtenemos

$$\frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle.$$

A continuación se aplica $\bigcup_f$, utilizando la proposición 4.2 obtenemos

$$\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle|-\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)|-\rangle.$$

Luego se aplica una puerta Hadamard al primer qubit,

$$\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|+\rangle + (-1)^{f(1)}|-\rangle\right)|-\rangle =$$
$$\frac{1}{\sqrt{2}}\left(\frac{(-1)^{f(0)}\left(|0\rangle + |1\rangle\right)}{\sqrt{2}} + \frac{(-1)^{f(1)}\left(|0\rangle - |1\rangle\right)}{\sqrt{2}}\right)|-\rangle =$$
$$\frac{1}{2}\left(\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle,\right)|-\rangle$$

esta expresión se puede escribir:

$$f_1(x) = \begin{cases} \pm|0\rangle|-\rangle & \text{si } f(0) = f(1) \\ \pm|1\rangle|-\rangle & \text{si } f(0) \neq f(1) \end{cases}$$

Y puesto que si $f(0) = f(1)$ entonces $f(0) + f(1) = 0$ y si $f(0) \neq f(1)$ entonces $f(0) + f(1) = 1$, obtenemos

$$\pm|f(0) + f(1)\rangle|-\rangle$$

Por tanto, midiendo el primer qubit obtenemos $f(0)+f(1)$. Si resulta el valor 0 entonces $f(0) = f(1)$ y si el valor es 1 entonces $f(0) \neq f(1)$.

El siguiente algoritmo es una generalización del algoritmo de Deutsh.

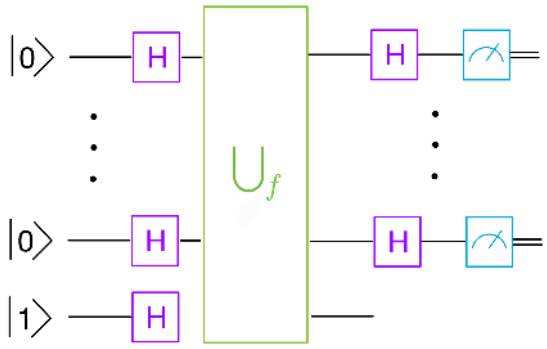
4.2.2. Algoritmo de Deutsch-Jozsa

Si tenemos una función $f : \{0,1\}^n \to \{0,1\}$ y queremos saber si f es constante o f es equilibrada, es decir si tiene el mismo número de 0 y de 1 en sus evaluaciones. Con un algoritmo clásico, para obtener la solución de forma determinista necesitaremos $2^{n-1} + 1$ evaluaciones. Mientras que con el algoritmo de Deutsch-Jozsa solo necesitaremos 1 evaluación de $\bigcup_f$ y n medidas.

Este algoritmo es un ejemplo de un algoritmo cuántico que resuelve un problema de complejidad exponencial a uno polinomial.

El circuito es el siguiente,

Figura 5: Circuito del algoritmo de Deutsh-Jozsa



4.3. Algoritmo de Shor

4.3.1. Transformada Cuántica de Fourier

La Transformada Cuántica de Fourier o TCF forma parte de muchos algoritmos cuánticos, destacando el algoritmo de Shor.

La TCF es la clásica transformada discreta de Fourier aplicado a un vector de amplitudes de un estado cuántico, donde consideremos los vectores de longitud $N = 2^n$ y $n \in \mathbb{N}$. La clásica transformada

de Fourier actúa sobre un vector $(x_1, \cdots, x_{N-1} \in \mathbb{C}^N)$ y lo evalúa a otro vector $(y_1, \cdots, y_{N-1} \in \mathbb{C}^N)$ según la siguiente fórmula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \; w_N^{-jk}, k = 0, 1, ..., N-1,$$

donde $w_N = e^{(2\pi i)/N}$ y $w_N^j = e^{(2\pi ij)/N}$.

De la misma manera, la TCF actúa sobre un estado cuántico

$$|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$$

y lo evalúa a otro estado cuántico

$$|y\rangle = \sum_{j=0}^{N-1} y_j |j\rangle$$

según la fórmula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \; w_N^{jk}, k = 0, 1, ..., N-1.$$

Destacar que por convención la TCF tiene el mismo efecto que la inversa de la transformada discreta de Fourier y viceversa.

Sea $|x\rangle$ un estado básico, la TCF puede también ser expresada por

$$\text{TCF} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w_N^{xj} |j\rangle.$$

La Transformada Cuántica de Fourier también se puede expresar de forma matricial o lo que es lo mismo como puerta cuántica:

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & w_N & \cdots & w_N^{N-1} \\ 1 & w_N^2 & \cdots & w_N^{2(N-1)} \\ 1 & w_N^3 & \cdots & w_N^{3(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w_N^{N-1} & \cdots & w_N^{(N-1)(N-1)} \end{pmatrix}$$

Ejemplo 4.2 *Sea $N = 4 = 2^2$ y $w = e^{(\pi i)/2} = i$ la matriz de la TCF sería*

$$F_4 = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

4.3.2. La importancia del Algoritmo de Shor

El algoritmo de Shor es un algoritmo cuántico para encontrar factores primos de un número entero. En computación clásica el problema de factorizar en números primos un número entero grande es muy costosa computacionalmente, pero el algoritmo de Shor consigue ser casi exponencialmente más rápido que el más eficiente algoritmo clásico en descomposición en números primos. Esto se debe principalmente por la eficiencia en calcular la Transformada Cuántica de Fourier.

Esto tiene principal relevancia porque muchos de los sistemas de encriptación modernos están basada en esto. El ejemplo más conocido de encritación es el criptosistema RSA. El RSA se utiliza en banca, servicios telefónicos, y en varios protocolos de transmisión y red. Y el algoritmo de Shor puede romper este sistema.

Recomiendo al lector, ahora con conocimientos básicos, a estudiar el artículo *Shor's Algorithm and the Quantum Fourier Transform* de **Fang Xi Lin** donde trata con más detalle la transformación de Fourier y el algoritmo de Shor. Y para mayor afianza de los temas tratados en estos apuntes se recomienda la siguiente bibliografía: *Quantum Computation and Quantum Information* de **Isaac Chuang y Michael Nielsen** y *Quantum Computing Explained* de **David McMahon**.