ALGORITMOS FUNDAMENTALES EN COMPUTACIÓN CUÁNTICA

Pastor Díaz, Ulises

Memoria presentada como parte de los requisitos para la obtención del título de Máster Universitario en Matemáticas por la Universidad de Sevilla.

Realizada por

Ulises Pastor Díaz

Tutorizada por

Prof. José María Tornero Sánchez

Índice general

Abstract

"Use your little grey cells mon ami."
-Agatha Christie.

At any point in history, we can find examples of problems solved mechanically, but it was in the 20th century with the arrival of computers that the paradigm shifted and the concept of problem-solving changed forever. It is at that moment when we start a race to not only solve problems but to solve them efficiently. A race against time itself.

Many advances were made from that point on, but already in the childhood of computer science, a question clouded the horizon: how fast can we go? Are there problems which we cannot solve efficiently?

In 1982 American physicist Richard Feynman pointed out that quantum systems could not be efficiently simulated with classical computers, proposing the idea of constructing a new model of computation. Computers fueled not by classical physics, but by quantum physics instead.

This idea, which had already been introduced by American physicist Paul Benioff and Russian mathematician Yuri Manin in 1980, served as inspiration for British physicist David Deutsch to introduce in 1985 a quantum analog to the already well known Turing machines: a quantum Turing machine.

And thus quantum computing was born. This new tool, which opened a new universe of possibilities, has been developed ever since, and many peaks have been reached in its short life.

In 1994 American mathematician Peter W. Shor reached a milestone when he developed a quantum algorithm that solved the factoring problem in polynomial time. This achievement was soon followed by Indian-American Lov K. Grover, who in 1996 described a quantum algorithm that solved the search problem qua-

dratically faster than a classical computer.

In this memory our goal will be to present some of the main algorithms in quantum computing, but to do so we will have to start by introducing the postulates of quantum mechanics and the phenomenon of quantum entanglement.

Next, we will propose a quantum computing model based on those ideas, which will allow us to finally construct some of the most important quantum algorithms so far.

Capítulo 1

Postulados y conceptos básicos

"Very few of us are what we seem."
-**Agatha Christie**.

Antes de sumergirnos en la construcción de algoritmos basados en un modelo cuántico de computación, antes incluso de atrevernos a desarrollar dicho modelo debemos asentar los cimientos. ¿Qué es un sistema cuántico? ¿Cómo evolucionan? ¿Cuáles son las particularidades que los hacen tan interesantes?

Responder a estas preguntas será nuestra primera tarea.

1.1. Postulados de la Mecánica Cuántica

El primer enigma que resolveremos será el de definir qué es un sistema cuántico. En concreto, y dado que nuestros intereses son computacionales, nos centraremos en los sistemas cuánticos discretos.

1.1.1. Primer postulado

Nuestra formalización del concepto de sistema cuántico deberá respetar tanto la naturaleza lineal de las funciones de onda como su comportamiento probabilístico, lo es que motivación suficiente para justificar el primer postulado.

Definición 1.1. *Postulado I: Sistema cuántico.*
El espacio de estados *de un sistema cuántico,* $\mathcal{H}$*, será un espacio de Hilbert complejo.*
Un estado *o* vector de estado *de dicho sistema será un vector unitario de* $\mathcal{H}$*.*

Para más información sobre la inspiración de este y los otros postulados se puede consultar [5].

Nuestro interés, por supuesto, será buscar un sistema cuántico análogo al bit, por lo que nos centraremos en sistemas discretos. Más concretamente en el que llamaremos *bit cuántico* o *qubit*.

Definición 1.2. *Qubit.*
Un qubit *es un sistema cuántico bidimensional.*

Antes de proseguir hagamos un inciso sobre la *notación de Dirac*, que será la convención que emplearemos a lo largo de la memoria. Según esta notación, los vectores se escribirán como *kets*: $|\psi\rangle$, sus duales como *bras*: $\langle\psi|$, los productos escalares como *brackets*: $\langle\psi|\varphi\rangle$ y los productos tensoriales como $|\psi\rangle|\varphi\rangle$ o incluso $|\psi\varphi\rangle$. Todo esto y algunas cosas más se pueden consultar en el anexo.

Acabado el inciso, si tomamos ahora una base $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ y $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ del qubit, que llamaremos *base computacional*, podemos escribir cualquier estado como:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C},$$

con la condición $|\alpha|^2 + |\beta|^2 = 1$, conocida como *condición de normalización*.

Podemos interpretar estas ecuaciones estableciendo una analogía con el modelo probabilístico clásico de computación. Los estados $|0\rangle$ y $|1\rangle$ jugarán los papeles de los bits 0 y 1, y la combinación lineal de ambos nos dirá que nos encontramos en el estado $|0\rangle$ con probabilidad $|\alpha|^2$ y en el estado $|1\rangle$ con probabilidad $|\beta|^2$.

Observación 1.1. Dado que lo importante de los coeficientes que acompañan la base (denotados *amplitudes*) es su módulo, podemos considerar que multiplicar un estado por un coeficiente unitario no cambia su naturaleza (lo que veremos más formalmente al estudiar las mediciones). Siguiendo esta lógica, deberíamos definir vector de estado como un elemento del espacio cociente $\mathbb{P}(\mathcal{H})$ de los vectores unitarios con la relación de equivalencia:

$$|\psi\rangle \sim e^{i\theta}|\psi\rangle, \quad \forall\theta \in \mathbb{R}.$$

A efectos prácticos esto resulta muy costoso y aporta pocos beneficios, por lo que simplemente mantendremos en mente que dos vectores equivalentes representan el mismo estado.

Aunque no usemos la equivalencia a nivel formal, esta observación nos permite visualizar el qubit como la superficie de una esfera, llamada *esfera de Bloch*, usando la *fibración de Hopf* [9].

Lema 1.1. Sea $|\psi\rangle = a|0\rangle + b|1\rangle$ un estado cualquiera del qubit, existen $\theta, \varphi, \gamma \in \mathbb{R}$ tales que

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\,\mathrm{sen}\,\frac{\theta}{2}|1\rangle\right).$$

La demostración de este resultado es inmediata y nos permite definir la esfera de Bloch mediante los parámetros θ y φ tras eliminar el factor $e^{i\gamma}$.

Definición 1.3. *Esfera de Bloch.*
Definimos la esfera de Bloch *como la esfera dada por las coordenadas* $(x, y, z) = (\mathrm{sen}\,\theta\cos\varphi, \mathrm{sen}\,\theta\,\mathrm{sen}\,\varphi, \cos\theta)$ *en* $\mathbb{R}^3$.

Por último, y antes de continuar con el siguiente postulado, podríamos preguntarnos por nuestra capacidad para construir qubits en la práctica. Existen distintas formas de realizar un qubit físicamente, aunque la problemática se aleja del objetivo de este texto. Para los interesados en las realizaciones físicas del qubit, se puede consultar [10].

1.1.2. Segundo postulado

Una vez hemos definido qué es un sistema cuántico podemos pasar a estudiar cómo evoluciona.

En un manual de física cuántica nos encontraríamos la versión continua del segundo postulado, conocida como *ecuación de Schödinger*.

Definición 1.4. *Postulado II: Ecuación de Schrödinger.*
Sea $\mathcal{H}$ *un sistema cuántico aislado dado por* $|\psi(t)\rangle$*, este evoluciona siguiendo la* ecuación de Schrödinger*:*

$$i\hbar\frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle.$$

Donde $\hbar$ es una constante llamada la constante de Planck *y H es un operador hermítico (que puede depender de t pero nosotros consideraremos constante) llamado* Hamiltoniano *del sistema.*

Como nuevamente nuestro interés es la variación discreta del sistema, podemos reformular este segundo postulado a una versión mucho más adaptada a nuestros objetivos.

Definición 1.5. *Postulado II: Evolución discreta.*
Sea $\mathcal{H}$ un sistema cuántico aislado cuyos estados en dos instantes t_1 y t_2 vienen dados por $|\psi_1\rangle$ y $|\psi_2\rangle$ respectivamente, entonces existe un operador unitario U dependiente de t_1 y t_2 tal que:

$$|\psi_2\rangle = U|\psi_1\rangle.$$

¿Cómo están relacionados estos dos postulados aparentemente tan dispares? Veamos la equivalencia. En primer lugar, resolviendo la ecuación de Schrödinger entre dos instantes t_1 y t_2 obtenemos:

$$|\psi(t_2)\rangle = exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]|\psi(t_1)\rangle.$$

Sea ahora

$$U(t_2, t_1) = exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]$$

el operador que relaciona los estados entre ambos instantes podemos comprobar el siguiente resultado.

Lema 1.2. La matriz $U(t_2, t_1)$ es unitaria, y para toda matriz unitaria U existe una matrix hermítica H tal que:

$$U = exp(-ciH),$$

siendo c una constante determinada por U.

La prueba de este resultado puede encontrarse en [12].

Cabe observar que este resultado es coherente con nuestras definiciones, ya que una matriz unitaria llevará vectores unitarios (estados) en vectores unitarios.

Además, nos dice que la única limitación que tenemos a la hora de implementar un cierto operador unitario U es la de construir un sistema cuántico regido por un hamiltoniano particular H, por lo que podemos considerar que cualquier operador unitario es susceptible de determinar la evolución de un determinado sistema.

En particular, la evolución de un qubit vendrá dada por matrices unitarias 2×2, que jugarán el papel de nuestras puertas lógicas a nivel computacional. Sin más dilación, pasemos a ver como podemos construir sistemas más complejos a partir de nuestro ya conocido qubit.

1.1.3. Tercer postulado

¿Qué ocurrirá cuando consideremos sistemas complejos compuestos por varios qubits? Consideremos dos qubits:

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle, \quad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle.$$

Como ya hemos visto, las amplitudes que acompañan a $|0\rangle$ y $|1\rangle$ tienen un significado físico, ya que se pueden identificar con las probabilidades de que nuestro qubit colapse en los respectivos estados de la base. La probabilidad de que ambos qubits estén en el estado $|0\rangle$ será $\alpha_1\alpha_2$, la de que el primero esté en el estado $|0\rangle$ y el segundo en el estado $|1\rangle$ será $\alpha_1\beta_2$, y en general podríamos decir que el estado compuesto es:

$$|\psi_1\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle.$$

Esto justifica el tercer postulado:

Definición 1.6. *Postulado III: Composición de sistemas.*
Sean $\mathcal{H}_1$ y $\mathcal{H}_2$ dos sistemas cuánticos, el sistema cuántico compuesto $\mathcal{H}$ vendrá dado por el producto tensorial de los sistemas simples:

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2.$$

Observación 1.2. Si en general tenemos varios estados, $\{\mathcal{H}_1, \ldots, \mathcal{H}_k\}$, entonces en estado compuesto vendrá dado por el producto tensorial:

$$\mathcal{H} = \bigotimes_{i=1}^{k} \mathcal{H}_i.$$

Dado que podemos ver un qubit como el espacio vectorial complejo bidimiensional $\mathbb{C}^2$, el sistema compuesto por dos qubits podrá identificarse con $\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4$. Si consideramos ahora la situación anterior, $|\psi_1\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}$ y $|\psi_2\rangle = \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}$, tenemos que:

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\psi_2\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix}.$$

Lo que se corresponde con el *producto de Kronecker*.

Observación 1.3. Dados dos sistemas cuánticos $\mathcal{H}_1 \simeq \mathbb{C}^{n_1}$ y $\mathcal{H}_2 \simeq \mathbb{C}^{n_2}$, entonces podemos identificar:

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \simeq \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \simeq \mathbb{C}^{n_1 n_2}.$$

De esta forma, el sistema compuesto por n qubits se podrá identificar con $\mathbb{C}^{2^n}$, los correspondientes productos tensoriales de la base computacional de cada qubit:

$$\bigotimes_{i=1}^{2^n} |i\rangle = |i_1 i_2 \dots i_{2^n-1} i_{2^n}\rangle,$$

formarán la base computacional del sistema compuesto y por tanto un estado arbitrario del sistema se podrá escribir como:

$$|\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |k\rangle.$$

De forma análoga, dados dos operadores U_1 y U_2 de los respectivos qubits, podemos considerar el operador producto $U_1 \otimes U_2$ que actúa linealmente sobre la regla:

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1|\psi_1\rangle) \otimes (U_2|\psi_2\rangle),$$

por lo que siguiendo un razonamiento análogo al anterior observamos que, tomando las identificaciones canónicas, la composición de operadores vendrá dada por el mismo *producto de Kornecker*.

De este postulado surge también un concepto fundamental en la computación cuántica, el llamado *entrelazamiento*. Este fenómeno se deriva del hecho que no todo estado $|\psi\rangle_{\mathcal{H}}$ de un sistema compuesto $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ se puede descomponer como

$$|\psi\rangle_{\mathcal{H}} = |\psi_1\rangle_{\mathcal{H}_1} \otimes |\psi_2\rangle_{\mathcal{H}_2}.$$

De igual manera, no todo operador del sistema compuesto puede descomponerse como producto de operadores de los sistemas simples. Las repercusiones de esto las veremos en el capítulo 2.

1.1.4. Cuarto postulado

El cuarto postulado es quizás el menos intuitivo y más interesante de los cuatro, ya que nos aporta una nueva herramienta con la que no contábamos en el caso clásico: la *medición cuántica*.

Este fenómeno se producirá cuando nuestro sistema aislado pasa a interaccionar con el exterior, produciéndose en este caso una transformación no unitaria. Existe una cierta controversia sobre la posibilidad de considerar la medición como una transformación unitaria de un sistema mayor, pero esto escapa de nuestro interés, por lo que nosotros consideraremos la medición como un fenómeno independiente.

Como ya introdujimos anteriormente, si tenemos un sistema cuántico en un estado arbitrario:

$$|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle,$$

entonces los valores $|\alpha_i|^2$ se correspondían con la probabilidad de que nuestro estado colapsase en el estado $|i\rangle$ respectivamente. Si consideramos ahora los proyectores ortogonales $P_i = |i\rangle\langle i|$, se puede comprobar que:

- Podemos asociar cada probabilidad con:

  $$|\alpha_i|^2 = \langle\psi|P_i|\psi\rangle,$$

  para cada $i = 0, \ldots, N-1$.
- El estado tras el colapso puede identificarse con:

  $$\frac{P_i|\psi\rangle}{|\alpha_i|} = \frac{\alpha_i}{|\alpha_i|}|i\rangle,$$

  que es proporcional a $|i\rangle$, y por tanto el mismo estado.

Usando estas ideas, podemos generalizar el concepto de medición de la siguiente forma.

Definición 1.7. *Postulado IV: Medición cuántica.*
Una medición cuántica *de un sistema cuántico $\mathcal{H}$ será un conjunto de operadores $\{M_i\}$ de $\mathcal{H}$, llamados* operadores de medición, *que satisfacen la* ecuación de completitud*:*

$$\sum_i M_i^* M_i = I,$$

siendo I el operador identidad.

Los índices i de dichos operadores se corresponderán con los posibles resultados de la medición, cada uno de los cuáles ocurrirá con probabilidad:

$$p(i) = \langle\psi|M_i^* M_i|\psi\rangle.$$

Suponiendo que el sistema se encontraba en el estado $|\psi\rangle$ en el momento previo a la medición, el estado del sistema tras suceder el resultado i será:

$$|\psi_i\rangle = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^* M_i|\psi\rangle}}.$$

Observación 1.4. Los operadores $\{P_i\}$ del ejemplo anterior son una medición, ya que cumplen la ecuación de completitud.

Esta ecuación encierra la idea buscada de que la suma de las probabilidades es 1.

Proposición 1.1. Un conjunto de operadores $\{M_i\}$ cumplen la ecuación de completitud si y solo si para todo estado $|\psi\rangle$ se cumple $\sum_i p(i) = 1$.

Demostración. Basta comprobar la siguiente secuencia:

$$\sum_i M_i^* M_i = I \iff \forall|\psi\rangle,\ \langle\psi|\left(\sum_i M_i^* M_i\right)|\psi\rangle = \langle\psi|I|\psi\rangle \iff$$

$$\forall|\psi\rangle,\ \sum_i \langle\psi|M_i^* M_i|\psi\rangle = \langle\psi|\psi\rangle \iff \forall|\psi\rangle,\ \sum_i p(i) = 1.$$

Sin embargo, el caso del ejemplo anterior es algo más concreto, ya que los operadores de medición son proyecciones ortogonales.

Definición 1.8. *Observable.*
Sea $\mathcal{H}$ un sistema, un observable *es un operador hermítico de $\mathcal{H}$.*

Observación 1.5. Usando el teorema de descomposición espectral para matrices hermíticas, sabemos que cualquier observable es diagonalizable en una base ortonormal. Tomando los proyectores ortogonales asociados a los espacios de autovectores (que son ortogonales entre sí), podemos concluir que, dado M un observable con autovalores m_i, entonces:

$$M = \sum_i m_i P_i,$$

donde los P_i son los proyectores ortogonales ya mencionados.

Definición 1.9. *Medición proyectiva.*
Una medición proyectiva *es un observable* $M = \sum_i m_i P_i$*, según el cual, dado un estado* $|\psi\rangle$*, la probabilidad de obtener el resultado* m_i *es:*

$$p(i) = \langle\psi|P_i|\psi\rangle,$$

y el estado tras la medición es:

$$|\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{p(i)}}.$$

Comprobemos que de hecho se trata de un caso concreto de medición cuántica.

Proposición 1.2. La medición proyectiva es un caso concreto de medición cuántica en el cual los operadores se corresponden con proyectores ortogonales.

Demostración. Los proyectores cumplen la ecuación de completitud trivialmente y además, sea un i dado $P_i^* P_i = P_i$ porque son operadores hermíticos y proyectores. ∎

Las mediciones que nosotros llevaremos a cabo, sin embargo, serán un tipo más general de medición proyectiva. Serán las llamadas *mediciones de Von Neumann.*

Definición 1.10. *Medición de Von Neumann.*
Sea $\mathcal{H} = \bigotimes_i \mathcal{H}_i$ *un sistema formado por composición de los* k *qubits* $\mathcal{H}_i$*, llamaremos* medición de Von Neumann *en la base computacional sobre el qubit etiquetado por* i *a la medición cuántica dada por los operadores:*

$$M_0 = (|0\rangle\langle 0|)_i = \underbrace{I \otimes \cdots \otimes I}_{i-1 \text{ veces}} \otimes (|0\rangle\langle 0|) \otimes \underbrace{I \otimes \cdots \otimes I}_{k-i \text{ veces}},$$
$$M_1 = (|1\rangle\langle 1|)_i = \underbrace{I \otimes \cdots \otimes I}_{i-1 \text{ veces}} \otimes (|1\rangle\langle 1|) \otimes \underbrace{I \otimes \cdots \otimes I}_{k-i \text{ veces}}.$$

Lema 1.3. Los operadores de la medición de Von Neumann constituyen una medición cuántica, y en concreto una medición proyectiva.

Demostración. Dado que $|0\rangle\langle 0| + |1\rangle\langle 1| = I$ es inmediato que $M_0 + M_1 = I$ y por tanto se trada de una medición.

Como además $M_j^2 = M_j$ para $j = 0, 1$ es una medición proyectiva.

Además, el siguiente resultado nos permite medir en más de un qubit de forma simultánea.

Proposición 1.3. Mediciones en cascada.
Sean $M = \{M_i\}$ y $N = \{N_j\}$ dos mediciones cuánticas, aplicar primero M y luego N equivale a aplicar una única medición $L = \{L_{ij} = M_i N_j\}$.

Demostración. L es una medición cuántica, ya que:

$$\sum_{ij} L_{ij} = \sum_i M_i \left(\sum_j N_j \right) = I.$$

Sea $|\psi\rangle$ un estado arbitrario del sistema, pasemos a calcular la probabilidad de que ocurra en primer lugar el resultado i en la medición M y luego el j en la medición N:

$$p(i)p(j) = \langle\psi|M_i^* M_i|\psi\rangle\langle\psi_i|N_j^* N_j|\psi_i\rangle = \langle\psi|N_j^* M_i^* M_i N_j|\psi\rangle.$$

Y el estado resultante tras dichas mediciones será:

$$|\psi_{ij}\rangle = \frac{N_j\psi_i}{\sqrt{p(j)}} = \frac{N_j M_i|\psi\rangle}{\sqrt{p(ij)}}.$$

Este tipo de medición nos permitirán medir un qubit de forma aislada sobre la base computacional.

Existe una formulación equivalente a la de los cuatro postulados anteriores muy usada en teoría de la información cuántica, en la que en lugar de trabajar con vectores unitarios trabajamos con *operadores de densidad*. Esta formulación es muy útil cuando se trabaja con ruido, y se puede encontrar en [12] y [7].

Una vez ya hemos visto los cuatro postulados que servirán de cimientos a la hora de construir nuestro sistema de computación pasemos a estudiar el fenómeno fundamental que usaremos como herramienta: el *entrelazamiento cuántico*.

1.2. Entrelazamiento cuántico

Comencemos por considerar el estado *EPR* en un sistema con dos qubits:

$$|\text{EPR}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

Y veamos que no somos capaces de escribir este estado como producto tensorial de estados simples. Sean

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle, \quad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle.$$

Sabemos que

$$|\psi_1\rangle|\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle.$$

Y por tanto tenemos las ecuaciones:

$$\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}, \quad \alpha_1\beta_2 = 0, \quad \beta_1\alpha_2 = 0, \quad \beta_1\beta_2 = \frac{1}{\sqrt{2}},$$

lo que es una contradicción y por tanto no podemos escribir el estado compuesto como composición de estados de los qubits individuales. Este fenómeno lo conocemos como *entrelazamiento cuántico*, y diremos que el estado EPR está entrelazado.

Definición 1.11. *Entrelazamiento cuántico.*
Un estado $|\psi\rangle \in \bigotimes_{i=1}^{n} \mathcal{H}_i$ *se dice* entrelazado *si no existen* $|\psi_i\rangle \in \mathcal{H}_i$ *tales que* $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$. *En caso contrario se dice que el estado es* separable.

El interés de la existencia este fenómeno, que es consecuencia de una conocida propiedad del producto tensorial, es que cuando un sistema compuesto se encuentra en un estado entrelazado lo que ocurre a uno de los sistemas simples altera

necesariamente al resto. Veámoslo llevando a cabo una medición sobre el primer qubit en el ejemplo anterior.

Los operadores de la medición serán:

$$M_0 = |0\rangle\langle 0| \otimes I, \quad M_1 = |1\rangle\langle 1| \otimes I.$$

Y por tanto, si obtenemos el resultado i, el estado resultante será:

$$\frac{M_i|\text{EPR}\rangle}{\sqrt{p(i)}} = |ii\rangle.$$

Por lo que el hecho de que el primer qubit colapse al estado $|i\rangle$ fuerza al segundo a hacer lo mismo. Veamos algunas aplicaciones de este fenómeno.

1.2.1. Superdense coding

Obviando la grandilocuencia del nombre, el *superdense coding* es una técnica que, mediante el entrelazamiento cuántico, nos permite transferir dos bits clásicos de información enviando únicamente un qubit.

Consideremos dos agentes *Alice* y *Bob* que quieren transmitirse dicha información. Cada uno de ellos tendrá un qubit ($\mathcal{H}_A$ y $\mathcal{H}_B$ respectivamente) que previamente habrán entrelazado obteniendo el estado $|\text{EPR}\rangle$ del sistema formado por la composición de ambos qubits $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Una vez se han separado, Bob simplemente tendrá que alterar su qubit de forma que el estado conjunto se transforme en el estado de la base EPR (consultar anexo) que le interese siguiendo la siguiente tabla.

Mensaje a transmitir	Transformación	Estado obtenido
00	Id	$\|\text{EPR}\rangle$
01	$\mathbf{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
10	$\mathbf{X} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\frac{\|10\rangle + \|01\rangle}{\sqrt{2}}$
11	$-i\mathbf{Y} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

Tras esto, Bob enviará su qubit a Alice que llevará a cabo una medición proyectiva en la base EPR para discernir en que estado se encuentra el sistema conjunto, recibiendo 2 bits de información habiendo sido enviado únicamente un qubit.

1.2.2. Teleportación cuántica

Este fenómeno de nombre también exagerado puede verse como el recíproco del anterior, ya que nos permite transmitir un qubit enviando únicamente dos bits de información.

Para ello usaremos los siguientes operadores que introduciremos en el capítulo 2:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathbf{C}_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Supongamos que nos encontramos en la situación anterior, en la cual Alice y Bob comparten un sistema de dos qubits en el estado $|\text{EPR}\rangle$. Supongamos que Alice quiere transmitir a Bob el qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Para ello, hará interaccionar dicho qubit con el sistema que ya compartían, obteniendo un nuevo sistema de tres qubits $\mathcal{H}_{A'} \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ en el estado:

$$\frac{1}{\sqrt{2}}\Big[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\Big].$$

Tras esto, Alice, que puede alterar únicamente los dos primeros qubits, aplicará sobre estos el operador unitario $\mathbf{C}_{NOT} \otimes I$, manteniendo el tercer qubit inalterado y obteniendo el estado:

$$\frac{1}{\sqrt{2}}\Big[\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\Big].$$

Y posteriormente aplicará el operador $\mathbf{H} \otimes I \otimes I$, obteniendo el estado:

$$\frac{1}{2}\Big[\alpha\left(|000\rangle + |100\rangle + |011\rangle + |111\rangle\right) + \beta\left(|010\rangle - |110\rangle + |001\rangle - |101\rangle\right)\Big] =$$

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

Finalmente, Alice llevará a cabo una medición de sus dos qubits en la base computacional y enviará el resultado a Bob. Una vez recibido el mensaje, Bob simplemente tendrá que aplicar la transformación dada por la tabla para obtener el qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Mensaje recibido	Transformación necesaria	Estado de $\mathcal{H}_B$
00	Id	$\alpha\|0\rangle + \beta\|1\rangle$
01	$\mathbf{X} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\beta\|0\rangle + \alpha\|1\rangle$
10	$\mathbf{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\alpha\|0\rangle - \beta\|1\rangle$
11	$-i\mathbf{Y} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\beta\|0\rangle - \alpha\|1\rangle$

Obteniendo Bob el estado buscado habiendo sido enviados únicamente dos bits de información clásica.

1.2.3. En computación

La consecuencia más interesante del entrelazamiento para nosotros será que, sin este fenómeno, la computación cuántica no aporta ninguna ventaja sobre la clásica, lo que podemos ver gracias al siguiente resultado.

Teorema 1.1. *Gottesman-Knill.*
Un algoritmo cuántico que comienza en la base computacional y no hace uso del entrelazamiento cuántico puede ser simulado en tiempo polinomial por un ordenador clásico probabilístico. [6]

Capítulo 2

Modelos de computación cuánticos

> *"I know there's a proverb which that says 'To err is human,' but a human error is nothing to what a computer can do if it tries."*
> -**Agatha Christie**.

Una vez ya hemos consolidado los postulados y fenómenos de la mecánica cuántica podemos por fin plantearnos la construcción de modelos de computación cuánticos. Estos modelos se fundamentan necesariamente sobre dichos cimientos, pero al igual que ocurre con los modelos de computación clásicos, existen diferentes versiones análogas cada una de las cuales presenta sus logros y desventajas.

2.1. Maquinas de Turing cuánticas

Fue David Deutsch quien basándose en los trabajos de Feynman, Manin y Benioff puso los primeros ladrillos y formalizó el concepto de *máquina de Turing cuántica* y el de *ordenador cuántico universal* en [3].

El concepto de máquina de Turing cuántica es análogo al clásico, pero presenta algunos cambios que lo hacen demasiado complejo de definir y trabajar con él, por lo que trabajaremos con el posteriormente introducido *modelo cuántico de circuitos*, que es completamente equivalente.

Como idea sobre el funcionamiento de estas máquinas de Turing cuánticas, el conjunto de estados usual se sustituye por el correspondiente espacio de estados mientras que el lugar de la función de transición lo ocupan transformaciones unitarias de dicho espacio de estados, lo que justifica el modelo de circuitos.

2.2. Modelo de circuitos cuántico

El modelo de circuitos cuántico fue introducido por David Deutsch en [4] y es análogo a su correspondiente versión clásica con algunas diferencias.

La primera salvedad es que por nuestros cables circulará información cuántica. En concreto, por cada cable circulará un qubit.

La segunda diferencia será referente a las puertas lógicas, que serán sustituidas por *puertas cuánticas*.

Definición 2.1. *Puerta cuántica.*
Sea $\mathcal{H}$ un sistema cuántico formado por composición de qubits. Una puerta cuántica es una transformación unitaria de $\mathcal{H}$.

De esta forma, en el contexto del modelo de circuitos, llamaremos puertas cuánticas a las transformaciones unitarias descritas en el postulado 2.

Esto nos aporta además una diferencia adicional con el modelo clásico: las puertas cuánticas tienen necesariamente la misma cantidad de entradas que de salida, ya que todas las transformaciones son reversibles.

Finalmente, la tercera diferencia es que en cualquier punto de un algoritmo cuántico podremos llevar a cabo una medición en uno o más qubits, obteniendo un resultado aleatorio en función del estado en el que se encontraba el cable medido.

Siguiendo la analogía con el modelo clásico, podremos representar un algoritmo en el modelo de circuitos como un diagrama en el cual los cables son líneas horizontales que se leen de izquierda a derecha. A la izquierda de cada cable aparecerá el estado inicial y las puertas cuánticas estarán representadas por rectángulos en las que entrarán y saldrán algunos cables. Las mediciones aparecerán en forma de triángulos al final del cable.

A continuación se presenta un ejemplo.

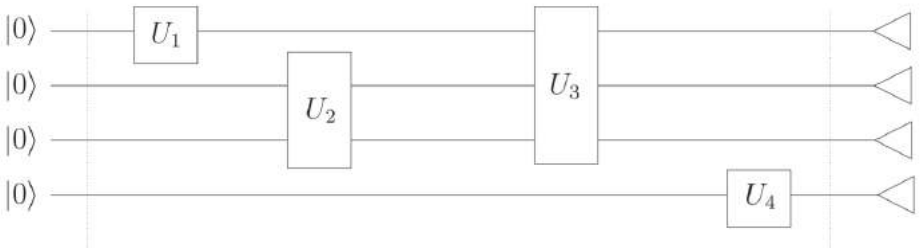

Figura 2.1: Ejemplo de un circuito

2.3. Puertas cuánticas

Llegados a este punto merece la pena estudiar algunas de las puertas cuánticas más usadas y sus resultados más importantes.

2.3.1. Puertas de un qubit

Veamos en primer lugar algunas de las puertas que actúan sobre un solo qubit, comenzando por la que quizás sea la más empleada de todas: la *puerta de Hadamard*.

Definición 2.2. *Puerta de Hadamard.*
Definimos la puerta de Hadamard como la siguiente puerta cuántica de un qubit.

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

Quizás entendamos mejor esta puerta si consideramos su efecto sobre la base computacional.

Lema 2.1. El efecto de la puerta de Hadamard sobre la base computacional del qubit es:

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

para $j = 0, 1$.

Como podemos comprobar, la puerta de Hadamard transforma estados de la base computacional en estados en el que todos los estados de la base computacional aparecen combinados con la misma probabilidad.

En particular, si consideramos su efecto sobre el estado $|0\rangle$ podemos comprobar que no solo aparecen los estados de la base computacional combinados con la misma probabilidad, si no que lo hacen con la misma amplitud.

Este resultado se puede generalizar al caso en el que aplicamos simultáneamente la puerta de Hadamard a múltiples qubits, obteniendo un resultado incluso más interesante.

Proposición 2.1. Sea $\mathcal{H}$ un sistema cuántico formado por composición de n qubits, entonces el efecto de $\mathbf{H}^{\otimes n}$ sobre un elemento de la base computacional $|x\rangle$ con $x \in \{0,1\}^n$ es:

$$\mathbf{H}^{\otimes n}|x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle_n,$$

donde $\cdot$ es el producto escalar bit a bit de las cadenas de $\{0,1\}^n$.

Demostración. Usando el lema anterior es sencillo comprobar que sean $x_i \in \{0,1\}$ tales que $|x\rangle_n = \otimes_{i=1}^n |x_i\rangle$, entonces:

$$\mathbf{H}^{\otimes n}|x\rangle_n = \bigotimes_{i=1}^{n} \left(\frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}} \right).$$

Y se puede comprobar por inducción en i que:

$$\bigotimes_{i=1}^{n} \left(\frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}} \right) = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x_1z_1+\ldots+x_nz_n}|z\rangle_n,$$

donde $|z\rangle_n = \otimes_{i=1}^n |z_i\rangle$ con $z_i \in \{0,1\}$.

De esta forma, la mayor parte de nuestros algoritmos comenzarán aplicando $\mathbf{H}^{\otimes n}$ al estado $|0\rangle_n$ para obtener una combinación de todos los estados de la base computacional con la misma amplitud.

Las siguientes puertas cuánticas ya las hemos introducido para tratar con los fenómenos del entrelazamiento cuántico. Son las *matrices de Pauli*.

Definición 2.3. *Matrices de Pauli.*
Las matrices de Pauli son las siguientes puertas cuánticas de un qubit.

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

La importancia de estas puertas reside en que forman junto con la identidad una base del conjunto de matrices hermíticas 2×2, además de que su aplicación se corresponde con una reflexión en los respectivos ejes de la esfera de Bloch. Veamos su efecto sobre la base computacional.

Lema 2.2. Los efectos de las matrices de Pauli en la base computacional son:

$$\mathbf{X}|j\rangle = |1 \oplus j\rangle, \quad \mathbf{Y}|i\rangle = (-i)^j |1 \oplus j\rangle, \quad \mathbf{Z}|j\rangle = (-1)^j |j\rangle,$$

para $j = 0, 1$.

En general, para describir cualquier puerta de un qubit presentamos el siguiente resultado.

Proposición 2.2. Sea U una puerta cuántica del qubit, entonces existen $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ tales que:

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\beta} & 0 \\ 0 & e^{i\beta} \end{pmatrix} \begin{pmatrix} \cos(\gamma/2) & -\operatorname{sen}(\gamma/2) \\ \operatorname{sen}(\gamma/2) & \cos(\gamma/2) \end{pmatrix} \begin{pmatrix} e^{-i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix}.$$

La demostración de este resultado es directa a partir de la definición de matriz unitaria, y lo que nos dice es que podemos construir cualquier puerta de un qubit mediante las siguientes puertas.

Definición 2.4. *Puertas de rotación.*
Llamamos puertas de rotación con respecto a los ejes X, Y y Z de la esfera de Bloch respectivamente a las puertas de la forma:

$$\boldsymbol{R}_x(\theta) = \begin{pmatrix} \cos(\theta/2) & -i\operatorname{sen}(\theta/2) \\ -i\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix},$$
$$\boldsymbol{R}_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\operatorname{sen}(\theta/2) \\ \operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix},$$
$$\boldsymbol{R}_z(\theta) = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix},$$

con $\theta \in [0, 2\pi)$.

Llegados a este punto podríamos preguntarnos si en un sistema cuántico compuesto podemos construir cualquier puerta cuántica a partir de las puertas de los respectivos qubits, a lo cual obtenemos una respuesta negativa: el producto tensorial de puertas del qubit no produce entrelazamiento.

2.3.2. Conjuntos de puertas universales

La puerta más simple que no se puede construir como producto de puertas cuánticas del qubit es quizás la puerta *NOT controlado* o $\mathbf{C}_{NOT}$.

Definición 2.5. *Puerta $\boldsymbol{C}_{NOT}$.*
La puerta NOT controlado que actúa sobre un sistema de dos qubits es

$$\mathbf{C}_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Esta puerta tiene el efecto de aplicar sobre el segundo qubit (llamado qubit objetivo) una puerta

$$\mathbf{U}_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

si el primer qubit se encuentra en el estado $|1\rangle$ y no hacer nada si el primer qubit se encuentra en el estado $|0\rangle$.

Lema 2.3. El efecto de la puerta $\mathbf{C}_{NOT}$ sobre la base computacional del sistema de dos qubits es:

$$\mathbf{C}_{NOT}|ij\rangle = |i\rangle|i \oplus j\rangle,$$

con $i, j = \{0, 1\}$.

Además, $\mathbf{C}_{NOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \mathbf{U}_{NOT}$ y no puede escribirse como producto tensorial de puertas de un qubit.

Demostración. La primera parte es simplemente una comprobación. Para demostrar la segunda parte bastará con comprobar que el efecto de ambas puertas sobre la base computacional es el mismo. Para la tercera parte basta comprobar que si llevamos a cabo el producto de Kronecker de dos matrices 2×2 arbitrarias y lo igualamos a la puerta $\mathbf{C}_{NOT}$ llegamos a contradicción igual que con el estado EPR.

Esta puerta es fundamental no solo porque es la puerta más simple que nos da entrelazamiento, si no porque además nos permite construir un conjunto de puertas cuánticas muy interesantes: las puertas ***U** controlado*.

Definición 2.6. *Puertas **U** controlado.*
*Sea **U** una puerta cuántica de un qubit, definimos la puerta **U** controlado sobre el sistema de dos qubits como:*

$$\boldsymbol{C}_U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \boldsymbol{U}.$$

Y siguiendo la misma idea podemos comprobar su efecto.

Lema 2.4. El efecto de la puerta **U** controlado sobre la base computacional es:

$$\mathbf{C}_U|0j\rangle = |0j\rangle, \quad \mathbf{C}_U|1j\rangle = |1\rangle\mathbf{U}|j\rangle,$$

con $j = \{0, 1\}$.

Sin embargo, quizás lo más significativo de la puerta $\mathbf{C}_{NOT}$ es el siguiente resultado.

Teorema 2.1. *Conjunto de puertas universales.*
Cualquier puerta cuántica de un sistema de n qubits se puede expresar como una cantidad finita de productos tensoriales de puertas de un solo qubit y la puerta $\boldsymbol{C}_{NOT}$ de dos qubits. [1]

Una vez presentado el nuevo modelo de computación, la cuestión que queda preguntarse es si este nos otorga alguna ventaja sobre los modelos de computación clásicos, ya sean deterministas o probabilísticos.

A nivel de computabilidad es sencillo convencerse de que un ordenador cuántico puede simular cualquier ordenador clásico. Lo que quizás resulte más sorprendente es que los ordenadores cuánticos pueden a su vez ser simulados por modelos clásicos de computación, aunque no de forma eficiente.

De esta forma no podemos resolver ningún problema que no pudiésemos ya resolver; la diferencia fundamental y la principal ventaja de este nuevo modelo de computación será la eficiencia con la que resolvemos dichos problemas.

2.4. Complejidad computacional cuántica

En primer lugar vamos a proceder a definir la clase de los problemas que consideramos son resolubles de forma eficiente en computación cuántica. Por supuesto, esta clase se aplicará únicamente a problemas de decisión, y para definirla nos vamos a inspirar en la clase **BPP**, *Bounded Error Probabilistic Polynomial time*, de los problemas que una maquina de Turing probabilística puede resolver en tiempo polinomial con un error menor o igual a 1/3.

Definición 2.7. *Clase **BQP**.*
*La clase **BQP** o Bounded-error Quantum Polynomial time es la clase de todos los problemas de decisión resolubles por una máquina de Turing cuántica en tiempo polinomial con un error inferior a* 1/3.

A continuación se muestra un gráfico que nos muestra la relación de **BQP** con respecto a otras conocidas clases de complejidad.

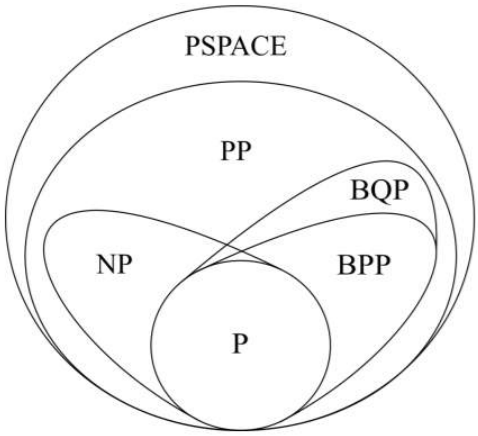

Figura 2.2: Diagrama de las clases de complejidad.

En particular, cabe señalar que **P** $\subset$ **BQP** $\subset$ **PSPACE**, es decir, que todo problema resoluble de forma eficiente por una máquina de Turing determinista tambiés se puede resolver en tiempo polinomial con un máquina de Turing cuántica, y que por otro lado **BPP** $\subset$ **BQP** pero no se sabe si **NP** $\subset$ **BQP** o no.

Para una introducción algo más formal a la teoría de la complejidad cuántica se puede consultar [13].

Capítulo 3

Algoritmos cuánticos

> *"The impossible could not have happened, therefore the impossible must be possible in spite of appearances."*
> **-Agatha Christie**.

Construido ya el modelo cuántico de circuitos podemos manejar al fin una noción de algoritmo: un algoritmo en este modelo será una sucesión de puertas cuánticas y mediciones aplicadas a un registro de n qubits.

Nuestro objetivo ahora será estudiar algunos de los algoritmos cuánticos más relevantes hasta la fecha y las técnicas generales en las que se basan. La primera y quizás más importante de ella será la que presentemos a continuación.

3.1. Phase Kick-Back

En numerosas ocasiones vamos a encontrarnos con la necesidad de implementar una puerta cuántica que codifique una aplicación $f : \{0,1\}^n \to \{0,1\}^m$ dada. Para ello, usaremos las *puertas oráculo*, que podemos construir a partir de la aplicación dada como una caja negra [10].

Definición 3.1. *Puerta oráculo.*
Sea $f : \{0,1\}^n \to \{0,1\}^m$ una aplicación, llamaremos puerta oráculo de f a la puerta cuántica cuyo efecto sobre la base computacional del sistema de $n+m$ qubits es el siguiente.

$$\boldsymbol{O}_f : |x\rangle_n|y\rangle_m \mapsto |x\rangle_n|y \oplus f(x)\rangle_m,$$

para $x \in \{0,1\}^n$ *e* $y \in \{0,1\}^m$.

Por ejemplo, la puerta $\mathbf{C}_{NOT}$ ya estudiada es la puerta oráculo de la aplicación constante $i : \{0,1\} \to \{0,1\}$.

Aplicando la puerta oráculo al estado $|x\rangle_n|0\rangle_m$ obtenemos $|x\rangle_n|f(x)\rangle_m$, en el cual el último registro, llamado qubit objetivo, recoge el valor de $f(x)$.

A primera vista estas puertas no alteran el estado de los primeros n qubits, ya que actúan sobre los m últimos. Sin embargo, tras algo de observación descubrimos que podemos usarlas para diferenciar los valores de f según su imagen gracias al siguiente resultado, previo al cual introduciremos la *base de Hadamard* del qubit:

$$\left\{|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}.$$

Lema 3.1. Sea $f : \{0,1\}^n \to \{0,1\}$ una aplicación, cualquier estado de la forma $|x\rangle_n \otimes |-\rangle$ es un autovalor de la puerta $\mathbf{O}_f$ con autovector $(-1)^{f(x)}$.

Demostración. Podemos descomponer el estado $|x\rangle_n|-\rangle$ (sobrentenderemos el subíndice n a partir de ahora) como:

$$\frac{1}{\sqrt{2}}\Big(|x\rangle|0\rangle - |x\rangle|1\rangle\Big).$$

Y por tanto, al aplicar $\mathbf{O}_f$ obtenemos:

$$\mathbf{O}_f \frac{1}{\sqrt{2}}\Big(|x\rangle|0\rangle - |x\rangle|1\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\Big)$$

$$= \begin{cases} \frac{1}{\sqrt{2}}\Big(|x\rangle|0\rangle - |x\rangle|1\rangle\Big) & \text{si } f(x) = 0 \\ \frac{1}{\sqrt{2}}\Big(|x\rangle|1\rangle - |x\rangle|0\rangle\Big) & \text{si } f(x) = 1, \end{cases}$$

lo que se corresponde con $(-1)^{f(x)}|x\rangle|-\rangle$. ∎

De esta forma, sea $X \subset \{0,1\}^n$ un subconjunto de estados de la base computacional de n qubits y $|\varphi\rangle_n$ un estado combinación de los mismos

$$|\varphi\rangle_n = \frac{1}{\sqrt{|X|}} \sum_{x \in X} |x\rangle_n.$$

Entonces, al aplicar $\mathbf{O}_f$ sobre $|\varphi\rangle_n|-\rangle$ obtendremos el estado:

$$\left(\frac{1}{\sqrt{|X|}} \sum_{x \in X} (-1)^{f(x)} |x\rangle_n \right) \otimes |-\rangle.$$

Codificando aquellos elementos cuya imagen es 1 invirtiendo su signo. A esta técnica es a lo que llamamos *Phase Kick-Back*, y la usaremos de forma frecuente.

3.2. Problema del subgrupo oculto

A continuación vamos a construir nuestros primeros algoritmos usando la técnica descrita anteriormente. Estos primeros algoritmos tendrán en común que pretenderán resolver *el problema del subgrupo oculto* en alguna de sus versiones.

Definición 3.2. *Problema del subgrupo oculto.*
Sea G un grupo finitamente generado, $K \subset G$ un subgrupo y X un conjunto finito con una aplicación $f : G \to X$ tal que

$$f(x) = f(y) \iff xK = yK \text{ (resp. a derecha)},$$

entonces denominamos problema del subgrupo oculto o HSP (del inglés "hidden subgroup problem") al problema de determinar un conjunto generador de K usando f como una caja negra.

Los problemas que plantearemos a continuación serán versiones del HSP para cuya resolución vamos a construir algoritmos que trabajen en tiempo polinomial. Comenzaremos por problemas sencillos para acabar llegando finalmente al *algortimo de factorización de Shor*, el que quizás sea el más conocido de los algoritmos cuánticos hasta la fecha.

3.2.1. Algoritmo de Deutsch

El primer problema que vamos a lanzar a la arena de combate será una versión de HSP para la cual $G = (\{0,1\}, \oplus)$ y $X = \{0,1\}$. Es decir, sea $f : \{0,1\} \to \{0,1\}$ dada como una caja negra, el objetivo es determinar si f es constante o no, lo que se corresponde con averiguar si $K = \{0,1\}$ (f constante) o $K = \{0\}$ (f no constante).

Veamos como podemos llevarlo a cabo con una sola aplicación de la puerta $\mathbf{O}_f$.

Algoritmo de Deutsch:

INICIO

$|\varphi_0\rangle_2 \leftarrow |0\rangle \otimes |1\rangle$

Como queremos obtener el estado $|+\rangle\otimes|-\rangle$ para poder aplicar el Phase Kick-Back, lo más sencillo será comenzar en este estado y aplicar la puerta de Hadamard a ambos qubits.

PASO 1

$|\varphi_1\rangle_2 \leftarrow \mathbf{H}^{\otimes 2}(|\varphi_0\rangle_2)$

Como ya esperábamos

$$|\varphi_1\rangle_2 = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |+\rangle|-\rangle,$$

por lo que ahora podemos aplicar la puerta oráculo.

PASO 2

$|\varphi_2\rangle_2 \leftarrow \mathbf{O}_f|\varphi_1\rangle_2$

Usando el Phase Kick-Back podemos convencernos de que tras aplicar la puerta

oráculo hemos obtenido el estado

$$|\varphi_2\rangle_2 = \mathbf{O}_f \left(\frac{|0\rangle|-\rangle + |1\rangle|-\rangle}{\sqrt{2}} \right) = \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \otimes |-\rangle.$$

Por lo que hemos codificado en el signo de las amplitudes del primer qubit si la aplicación f es constante o no. Si aplicamos ahora la puerta de Hadamard en el primer registro para obtener un estado de la base computacional estaremos listos para medir y obtener el resultado.

PASO 3

$\|\varphi_3\rangle_2 \leftarrow (\mathbf{H} \otimes I)\,\|\varphi_1\rangle_2$

Para entender bien el resultado de este paso consideremos las dos posibles situaciones.

Si $f(0) = f(1)$, entonces $|\varphi_2\rangle_2 = (-1)^{f(0)}|+\rangle|-\rangle$, por lo que al aplicar $\mathbf{H} \otimes I$ obtenemos $|\varphi_3\rangle_2 = (-1)^{f(0)}|0\rangle|-\rangle$.

Si $f(0) \neq f(1)$, entonces $|\varphi_2\rangle_2 = (-1)^{f(0)}|-\rangle|-\rangle$, y al aplicar $\mathbf{H} \otimes I$ obtenemos $|\varphi_3\rangle_2 = (-1)^{f(0)}|1\rangle|-\rangle$.

En general, el resultado tras el paso 3 será:

$$|\varphi_2\rangle_2 = (-1)^{f(0)}|f(0) \oplus f(1)\rangle|-\rangle.$$

PASO 4

$\delta \leftarrow$ medimos el primer qubit.

Como era previsible, tras medir el primer registro obtendremos $\delta \in \{0, 1\}$. Si $\delta = 0$, entonces $f(0) = f(1)$ y por tanto $K = \{0, 1\}$. Si por otro lado $\delta = 1$ entonces $f(0) \neq f(1)$ y por tanto $K = \{0\}$. Gracias a este análisis podemos enunciar el siguiente teorema de corrección.

Teorema 3.1. *Corrección del algoritmo de Deutsch.*
El algoritmo de Deutsch resuelve el HSP para $G = \{0, 1\}$ *y* $X = \{0, 1\}$ *con una única aplicación de la puerta oráculo.*

Con este simple problema ya podemos observar la ventaja de los algoritmos cuánticos frente a los clásicos. Un algoritmo clásico determinista necesita dos comprobaciones de f para resolver este problema, mientras que nuestro algoritmo puede aplicar f a ambos estados a la vez y por tanto resolverlo con una única aplicación.

3.2.2. Algoritmo de Deutsch-Jozsa

La pregunta que nos surge ahora es, ¿podremos generalizar este resultado para el caso en el que tenemos una aplicación $f : \{0, 1\}^n \to \{0, 1\}$? Este será el objetivo de nuestro próximo algoritmo.

El problema que nos plantearemos ahora será el de, dado el grupo $G = (\{0, 1\}^n, \oplus)$ y $X = \{0, 1\}$ determinar si la aplicación f es constante o no. Dado que se trata de un problema de subgrupo oculto, en caso de no ser constante será *equilibrada*, es decir, habrá tantos valores $x \in \{0, 1\}^n$ con $f(x) = 0$ como valores con $f(x) = 1$. Este problema se conoce como *el problema de Deutsch.*

Definición 3.3. *Problema de Deutsch.*
Se llama problema de Deutsch al problema del subgrupo oculto en el cual $G = (\{0, 1\}^n, \oplus)$ *y* $X = \{0, 1\}$.

Veamos el algoritmo que lo resuelve.

Algoritmo de Deutsch-Jozsa:

INICIO

$|\varphi_0\rangle_{n+1} \leftarrow |0\rangle_n \otimes |1\rangle$

Nuevamente queremos obtener un estado de la forma $|x\rangle_n|-\rangle$ siendo $|x\rangle_n$ una combinación de todos los estados de la base computacional con la misma amplitud.

PASO 1

$$|\varphi_1\rangle_{n+1} \leftarrow \mathbf{H}^{\otimes n+1}(|\varphi_0\rangle_{n+1})$$

Como ya esperábamos

$$|\varphi_1\rangle_{n+1} = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n\right) \otimes |-\rangle.$$

PASO 2

$$|\varphi_2\rangle_{n+1} \leftarrow \mathbf{O}_f|\varphi_1\rangle_{n+1}$$

Usando el Phase Kick-Back no es complicado comprobar que

$$|\varphi_2\rangle_{n+1} = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle_n\right) \otimes |-\rangle,$$

donde nuevamente hemos codificado el valor de los estados de base en sus amplitudes.

PASO 3

$$|\varphi_3\rangle_{n+1} \leftarrow \left(\mathbf{H}^{\otimes n} \otimes I\right)|\varphi_1\rangle_{n+1}$$

Usando ahora la proposición 2.1 podemos comprobar que el estado antes de la medición es

$$|\varphi_3\rangle_{n+1} = \left[\frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)+x\cdot y}\right)|y\rangle_n\right] \otimes |-\rangle.$$

PASO 4

$\bar{\delta} \leftarrow$ medimos los n primeros qubits de $|\varphi_3\rangle_{n+1}$

Y aunque parezca un estado muy complicado, basta comprobar que la amplitud de $|0\rangle_n$ cumple que:

$$|a_0|^2 = \left| \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2 = \begin{cases} 1 & \text{si } f \text{ es constante} \\ 0 & \text{si } f \text{ es equilibrada.} \end{cases}$$

Este análisis nos permite enunciar el teorema de corrección.

Teorema 3.2. *Corrección del algoritmo de Deutsch-Jozsa.*
El algoritmo de Deutsch-Jozsa resuelve el problema de Deutsch con una única aplicación de la puerta oráculo.

Esto tiene unas implicaciones mucho más profundas que en el caso anterior, ya que para resolver este problema un algoritmo clásico determinista necesitaría $2^{n-1}+1$ comprobaciones del oráculo de f.

Como consecuencia, la versión de decisión del problema de Deutsch se encuentra en la clase **EQP** de aquellos problemas que se pueden resolver de forma exacta mediante un algoritmo cuántico en tiempo polinomial, pero no pertenece a su análogo determinista **P**.

3.2.3. Algoritmo de Simon

Veamos otro problema de subgrupo oculto antes de proceder con el algoritmo de Shor. Se tratará del *problema de Simon.*

Definición 3.4. *Problema de Simon.*
Sea $f : \{0,1\}^n \to \{0,1\}^n$ una aplicación y $s \in \{0,1\}^n$ tal que $f(x) = f(y)$ si y solo si o bien $x = y \oplus s$ o bien $y = x \oplus s$.
El problema de Simon trata de encontrar s usando f como una caja negra.

Observación 3.1. El problema de Simon es un problema de subgrupo oculto con $G = (\{0,1\}^n, \oplus)$, $X = \{0,1\}^n$ y K es de la forma $K = \{0, s\}$ para algún $s \in \{0,1\}^n$.

Además, a s se la suele llamar la *máscara xor* de f.

Veamos el algoritmo para resolver este problema.

Algoritmo de Simon:

INICIO

$$|\varphi_0\rangle_{2n} \leftarrow |0\rangle_n \otimes |0\rangle_n$$

En este caso queremos obtener $f(x)$ para cada $x \in \{0,1\}^n$ en los n últimos qubits.

PASO 1

$$|\varphi_1\rangle_{2n} \leftarrow \left(\mathbf{H}^{\otimes n} \otimes I^{\otimes n}\right)(|\varphi_0\rangle_{2n})$$

Nuevamente por la proposición 1.2 obtenemos

$$|\varphi_1\rangle_{2n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n |0\rangle_n.$$

PASO 2

$$|\varphi_2\rangle_{2n} \leftarrow \mathbf{O}_f |\varphi_1\rangle_{2n}$$

Según era nuestro objetivo, tras aplicar la puerta oráculo el estado será

$$|\varphi_2\rangle_{2n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_n.$$

PASO 3

$\bar{\delta} \leftarrow$ medimos los n qubits finales de $|\varphi_2\rangle_{2n}$
$|\varphi_3\rangle_n \leftarrow |\varphi_2\rangle_{2n}$ tras la medición

Aquí usamos una nueva herramienta no empleada hasta ahora, llevar a cabo una medición previamente al final del algoritmo. El objetivo es que si obtenemos un determinado $\bar{\delta} \in \{0,1\}^n$, gracias al entrelazamiento el estado que quedará en los n primeros qubits será

$$|\varphi_3\rangle_n = \frac{1}{\sqrt{2}}\Big(|x_0\rangle_n + |x_0 \oplus s\rangle_n\Big),$$

siendo $\{x_0, x_0 \oplus s\} = f^{-1}(\bar{\delta})$.

PASO 4

$|\varphi_4\rangle_n \leftarrow \mathbf{H}^{\otimes n}\left(|\varphi_3\rangle_n\right)$

Si calculamos el resultado de este paso obtenemos:

$$|\varphi_4\rangle_n = \mathbf{H}^{\otimes n}|\varphi_3\rangle_n = \frac{1}{\sqrt{2}}\left(\mathbf{H}^{\otimes n}|x_0\rangle_n + \mathbf{H}^{\otimes n}|x_0 \oplus s\rangle_n\right)$$

$$= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{y\cdot x_0}|y\rangle_n + \frac{1}{\sqrt{2^n}}\sum_{z=0}^{2^n-1}(-1)^{z\cdot(x_0\oplus s)}|y\rangle_n\right]$$

$$= \frac{1}{\sqrt{2^{n+1}}}\sum_{y=0}^{2^{n-1}}(-1)^{y\cdot x_0}\left[(-1)^{y\cdot s}\,|y\rangle_n\right],$$

donde lo realmente importante es que los estados $|y\rangle_n$ de la base computacional cuya amplitud no es cero cumplen que $y \cdot s = 0$ y tras medir los obtenemos con probabilidad $1/2^{n-1}$.

PASO 5

$\bar{\omega} \leftarrow$ medimos $\lvert\varphi_4\rangle_n$

Si obtenemos al menos $n-1$ resultados $\bar{\omega_i}$ linealmente independientes tales que $\bar{\omega} \cdot s = 0$ podemos obtener s resolviendo un sistema de ecuaciones, por lo que la pregunta es cuántas veces tenemos que iterar el algoritmo para obtener suficientes ecuaciones.

Teorema 3.3. *Corrección del algoritmo de Simon.*
El algoritmo de Simon resuelve el problema de Simon con probabilidad al menos $2/3$ *con una* $\mathcal{O}(n)$ *aplicaciones de la puerta oráculo y* $\mathcal{O}(n^3)$ *aplicaciones de otras puertas elementales si llevamos a cabo* $n+3$ *repeticiones del algoritmo. [7]*

La importancia de este problema reside en que un algoritmo probabilístico necesita $\Omega(2^{n/3})$ evaluaciones de f para obtener la solución con probabilidad al menos $2/3$, por lo que estamos frente a una mejora exponencial frente al caso clásico no determinista.

3.3. Algoritmo de Shor

Por último veamos el más importante de los algoritmos cuánticos a razón de sus múltiples aplicaciones: *el algoritmo de Shor*.

Este algoritmo resuelve el problema de la factorización, que dado un entero $N \in \mathbb{Z}_{\geq 0}$ pretende encontrar la única descomposición en factores primos que garantiza el *Teorema Fundamental de la Aritmética*.

Antes de comenzar veamos una importante técnica que introduce este algoritmo y que se puede extender a otros algoritmos cuánticos.

3.3.1. Transformada de Fourier cuántica

Hasta ahora hemos usado la puerta de Hadamard seguida de una puerta oráculo para codificar información el las amplitudes de la combinación de todos los estados

de la base computacional en forma de signo, lo que nos servía para diferenciar entre dos posibles valores de la función.

La nueva puerta cuántica que vamos a introducir, llamada *transformada de Fourier cuántica* por su similitud con la transformada de Fourier discreta, nos permitirá codificar información en una combinación de los elementos de la base computacional con probabilidad homogénea usando que tenemos toda una colección de complejos de la forma $e^{2i\pi\theta}$ de módulo 1.

Definición 3.5. *Transformada cuántica de Fourier.*
Llamamos transformada cuántica de Fourier o $\boldsymbol{QFT}_m$ *con* $m \leq 2^n$ *a la puerta cuántica del sistema de* n *qubits cuyo efecto sobre la base computacional es el siguiente.*

$$\boldsymbol{QTF}_m : |x\rangle_n \mapsto \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} e^{2\pi i y x/m} |y\rangle_n,$$

para $x \in \{0,1\}^n$.

Esta puerta cuántica puede implementarse de forma eficiente, y tendrá especial interés a la hora de encontrar el periodo de un *estado periódico.*

Definición 3.6. *Estado periódico.*
Un estado se dice periódico si es de la forma

$$|\phi_{r,b}\rangle_n = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr+b\rangle_n,$$

donde r *es el periodo y* m *el número de repeticiones.*

El problema que nos permite resolver la **QFT** es el siguiente.

Definición 3.7. *Problema del periodo.*
Dado un estado periódico $|\phi_{r,b}\rangle_n$ *con* m *repeticiones y conocido el valor* rm *hallar* r.

Para resolver este problema nos apoyaremos en el siguiente resultado.

Lema 3.2. Sea $|\phi_{r,b}\rangle$ un estado periódico, entonces:

$$\mathbf{QFT}_{mr} |\phi_{r,b}\rangle_n = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{2\pi i x b/r} |mx\rangle_n.$$

Demostración. Sabiendo que la inversa de $\mathbf{QFT}_{mr}$ es la puerta cuántica cuyo efecto sobre la baso computacional es:

$$\mathbf{QFT}_{mr}^{-1} : |x\rangle_n \mapsto \frac{1}{\sqrt{mr}} \sum_{y=0}^{mr-1} e^{-2\pi i yx/mr} |y\rangle_n,$$

para $x \in \{0,1\}^n$. Vamos a comprobar que aplicando $\mathbf{QFT}_{mr}^{-1}$ en ambos lados de la igualdad obtenemos el mismo resultado. Para ello:

$$\begin{aligned}\mathbf{QFT}_{mr}^{-1}\left(\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1} e^{2\pi i xb/r}|mx\rangle_n\right) &= \frac{1}{\sqrt{r}}\sum_{x=0}^{r-1} e^{2\pi i xb/r}\mathbf{QFT}_{mr}^{-1}|mx\rangle_n \\ &= \frac{1}{\sqrt{r}}\sum_{x=0}^{r-1} e^{2\pi i xb/r}\left(\frac{1}{\sqrt{mr}}\sum_{y=0}^{mr-1} e^{-2\pi i yx/mr}|y\rangle_n\right).\end{aligned}$$

Reordenando los términos obtenemos

$$\frac{1}{\sqrt{m}}\sum_{y=0}^{mr-1}\left[\sum_{x=0}^{r-1}\frac{1}{r}e^{2\pi i x(y-b)/r}\right]|y\rangle_n.$$

Y usando ahora que

$$\sum_{x=0}^{r-1}\frac{1}{r}e^{2\pi i x(y-b)/r} = \begin{cases} r & \text{si } r \mid y-b \\ 0 & \text{en caso contrario}\end{cases}$$

como $y = rz + b$ con $z \in \{0,\ldots,m-1\}$ obtenemos el estado:

$$\frac{1}{\sqrt{m}}\sum_{z=0}^{m-1}|zr+b\rangle_n.$$

Usando este resultado, si medimos ahora el estado

$$\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1} e^{2\pi i xb/r}|mx\rangle_n$$

obtendremos un cierto mx_0, y dado que conocemos mr podemos calcular

$$\frac{mx_0}{mr} = \frac{x_0}{r}.$$

Para poder obtener r a partir de estos datos necesitamos que la última fracción sea irreducible, lo que ocurre con probabilidad $\Omega(\frac{1}{\log\log(r)})$, por lo que bastará repetir el procedimiento un número esperado de veces $\mathcal{O}(\log\log(r))$. [7]

Veamos cómo podemos usar esta herramienta para construir el algoritmo de Shor.

3.3.2. El problema del orden

El algoritmo de Shor (o al menos su parte cuántica) ataca *el problema del orden*, por lo que nos centraremos en el algoritmo que resuelve dicho problema. Para consultar la reducibilidad clásica que existe entre este problema y el de la factorización se puede consultar [14].

Definición 3.8. *Problema del orden.*
Sea $N \in \mathbb{Z}_{\geq 0}$ y s entero con $1 < s < N$, el problema del orden consiste en hallar el orden multiplicativo de s en $\mathbb{Z}/N\mathbb{Z}$.

Observación 3.2. Este problema también se corresponde con un problema de subgrupo oculto en el que $G = \mathbb{Z}$ con la suma módulo N y $f(x) = s^x = s^{x+r}$ donde r es el orden multiplicativo de s.

Algoritmo de Shor:

INICIO

$$|\varphi_0\rangle_{t,n} \leftarrow |0\rangle_t \otimes |0\rangle_n$$

Aquí $n = \lceil \log_2 N \rceil$ y $t = 2n$.

PASO 1

$$|\varphi_1\rangle_{t,n} \leftarrow \left(\mathbf{H}^{\otimes t} \otimes I^n\right)(|\varphi_0\rangle_{t,n})$$

Nuevamente por la proposición 1.2 obtenemos

$$|\varphi_1\rangle_{t,n} = \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle_t |0\rangle_n.$$

PASO 2

$\|\varphi_2\rangle_{t,n} \leftarrow \mathbf{M}_{s,N} \|\varphi_1\rangle_{t,n}$

Donde $\mathbf{M}_{x,N}$ es la puerta cuántica cuyo efecto es

$$\mathbf{M}_{s,N} : |i\rangle_t \otimes |j\rangle_n \mapsto |i\rangle_t \otimes |j + s^i \bmod N\rangle_n,$$

y que podemos construir de forma eficiente como aparece en [14]. Como esperábamos, el estado obtenido es:

$$|\varphi_2\rangle_{t,n} = \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^n-1} |x\rangle_t |s^x \bmod N\rangle_n.$$

PASO 3

$\bar{\delta} \leftarrow$ medimos los t primeros qubits de $\|\varphi_2\rangle_{t,n}$ $\|\varphi_3\rangle_t \leftarrow \|\varphi_2\rangle_{t,n}$ tras la medición

Sea $\bar{\delta} = s^{b_0}$ y r el valor buscado, en el caso en el que r es una potencia de dos obtenemos el estado periódico

$$|\varphi_3\rangle_t = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr + b_0\rangle_t,$$

donde $m = 2^t/r$, por lo que tendremos que aplicar $\mathbf{QTF}_{mr}$ y obtener el periodo r. El caso general es más complejo pero sigue el mismo comportamiento.

PASO 4

$|\varphi_4\rangle_t \leftarrow \mathbf{QFT}_{2^t}\left(|\varphi_3\rangle_t\right)$

PASO 5

$\bar{\omega} \leftarrow$ medimos $|\varphi_4\rangle_t$

Y procedemos como en el problema del periodo, por lo que el algoritmo lleva a cabo la tarea que queremos realizar.

Teorema 3.4. *Corrección del algoritmo de Shor.*
El algoritmo de Shor soluciona el problema del orden en tiempo polinomial con error acotado por $1/3$. *[14]*

La importancia de este algoritmo radica en la hipótesis de que el problema de la factorización no es resoluble de forma eficiente por un ordenador clásico, pieza fundamental en la que se basa la criptografía moderna.

De ser esta hipótesis cierta, estaríamos frente a un problema para el cual existe una mejora exponencial de eficiencia del modelo cuántico frente a los modelos clásicos.

Capítulo 4

Algoritmos de búsqueda y amplificación de amplitudes

"Unless you are good at guessing, it is not much use being a detective."
-**Agatha Christie**.

En este capítulo vamos a centrarnos en la resolución de un problema concreto conocido como el *Problema de Búsqueda* para posteriormente generalizar la técnica de amplificación de amplitudes que usaremos para resolverlo.

4.1. Problema de Búsqueda

Comencemos por tomar un acercamiento intuitivo a nuestro problema. Se nos proporcionará una colección de objetos y se nos pedirá de entre ellos obtener al menos uno que cumpla una cierta propiedad.

Por ejemplo, dado un entero positivo N y el conjunto $\{1, 2, \ldots, \left\lfloor \sqrt{N} \right\rfloor\}$ hallar un factor de dicho N.

Para nuestro interés, los elementos del conjunto podrán ser codificados por cadenas de n ceros y unos y la propiedad por una aplicación $f : \{0,1\}^n \to \{0,1\}$ que devolverá uno si el estado verifica la propiedad y cero en caso contrario.

Veamos la formalización de esta idea.

Definición 4.1. *Problema de Búsqueda.*
Sea n un entero positivo y $\mathbf{O}_f$ un oráculo para computar la función $f : \{0,1\}^n \to \{0,1\}$, el Problema de Búsqueda asociado a estos datos será encontrar un $x \in \{0,1\}^n$ tal que $f(x) = 1$.

En concreto vamos a suponer que existe un único valor válido, aunque posteriormente eliminaremos esta condición.

Una vez tenemos formalizado el problema, podemos plantearnos la siguiente pregunta: ¿cuántas llamadas a $\mathbf{O}_f$ necesitamos para resolver este problema con probabilidad al menos $2/3$?

En el caso clásico necesitamos $\Omega(2^n)$ llamadas, ya que tendremos que hacer una búsqueda exhaustiva. De forma intuitiva, podemos comprobar fácilmente que si tomamos secuencialmente k elementos de forma aleatoria entre los $\{0,1\}^n$, la probabilidad de que uno de ellos sea el x tal que $f(x) = 1$ es $k/2^n$.

Sin embargo, en el caso cuántico existe un algoritmo, llamado *Algoritmo de Grover*, que es capaz de hallar la solución con alta probabilidad realizando $O(\sqrt{2^n})$ llamadas a $\mathbf{O}_f$, lo que supone una mejora cuadrática del caso clásico.

Procedamos a describir este algoritmo.

4.1.1. Algoritmo de Grover

Nuevamente vamos a suponer que se nos provee una puerta oráculo del sistema de $n+1$ qubits $\mathbf{O}_f : \mathcal{H}_{n+1} \to \mathcal{H}_{n+1}$ cuyo efecto, recordamos, es:

$$\mathbf{O}_f : |x\rangle_n \otimes |b\rangle \mapsto |x\rangle_n \otimes |b \oplus f(x)\rangle,$$

lo que nos permite computar la aplicación f preparando el último qubit (qubit objetivo) en el estado $|0\rangle$.

Como era de esperar, vamos a apoyarnos en la idea del Phase Kick-Back para señalar el único estado que verifica la propiedad, con el aliciente de que ahora aplicaremos técnicas para aumentar la amplitud de dicho estado.

Para ello veamos una nueva puerta cuántica, llamada *puerta de cambio de fase*, cuyo efecto será alterar la amplitud de todos los estados ortogonales a $|0\rangle_n$ en un sistema de n qubits, dejando el estado $|0\rangle_n$ invariante.

Definición 4.2. *Cambio de fase.*
Sea $\mathcal{H}$ un sistema de n qubits, llamaremos puerta de cambio de fase del sistema a la puerta cuántica $U_{0^\perp} : \mathcal{H} \to \mathcal{H}$ cuyo efecto en la base computacional es:

$$\begin{cases} \boldsymbol{U}_{0^\perp} : |0\rangle_n \mapsto |0\rangle_n \\ \boldsymbol{U}_{0^\perp} : |x\rangle_n \mapsto -|x\rangle_n \quad si\ x \neq 0. \end{cases}$$

Consideremos además la siguiente puerta cuántica que construiremos a partir del cambio de fase y que llamaremos *puerta de difusión de Grover.*

Definición 4.3. *Puerta de difusión de Grover.*
Llamaremos peurta de difusión de Grover a la siguiente puerta cuántica.

$$\boldsymbol{\Gamma}_n = \boldsymbol{H}^{\otimes n} \boldsymbol{U}_{0^\perp} \boldsymbol{H}^{\otimes n}.$$

Para entender el efecto de esta puerta tomemos la base ortonormal del sistema de n qubits dada por:

$$\left\{ |\psi_i\rangle_n = \mathbf{H}^{\otimes n}|i\rangle_n \mid i = 0, \ldots, 2^n - 1 \right\},$$

y veamos el siguiente resultado.

Lema 4.1. Sea $\boldsymbol{\Gamma}_n$ la puerta cuántica definido anteriormente, su efecto en la base de los $|\psi_i\rangle$ es el siguiente:

$$\boldsymbol{\Gamma}_n|\psi_i\rangle = \begin{cases} |\psi_i\rangle_n & \text{si } i = 0 \\ -|\psi_i\rangle_n & \text{es caso contrario.} \end{cases}$$

Demostración. Basta hacer la comprobación, en la que $\mathbf{H}^{\otimes n} = \mathbf{H}$ por simplicidad:

$$\boldsymbol{\Gamma}_n|\psi_i\rangle = \mathbf{H}\mathbf{U}_{0^\perp}\mathbf{H}\mathbf{H}|i\rangle = \mathbf{H}\mathbf{U}_{0^\perp}|i\rangle = \begin{cases} \mathbf{H}|i\rangle & \text{si } i = 0 \\ -\mathbf{H}|i\rangle & \text{en caso contrario.} \end{cases}$$

Y tenemos el resultado. ∎

Veamos ahora algunas propiedades importantes de esta puerta cuántica.

Proposición 4.1. Sea $\mathbf{\Gamma}_n$ la puerta de difusión, $\{|\psi_i\rangle\}$ la base ortogonal dada y $N = 2^n$, entonces:

i. $\mathbf{\Gamma}_n = 2|\psi_0\rangle\langle\psi_0| - I$.

ii. El estado $|\varphi\rangle = \sum_{x=0}^{N-1} \alpha_x|x\rangle$ es ortogonal a $|\psi_0\rangle$ si y solo si:

$$\sum_{x=0}^{N-1} \alpha_x = 0.$$

iii. Sea $|\varphi\rangle = \sum_{x=0}^{N-1} \alpha_x|x\rangle$ un estado cualquiera, y sea μ la media de sus amplitudes:

$$\mu = \frac{1}{N}\sum_{x=0}^{N-1} \alpha_x.$$

Entonces:

$$\mathbf{\Gamma}_n|\varphi\rangle = \sum_{x=0}^{N-1} (2\mu - \alpha_x)\,|x\rangle.$$

Demostración. i. Para esto veamos que ambas puertas tienen el mismo efecto sobre la base $\{|\psi_i\rangle\}$. Es decir:

$$\Big(2|\psi_0\rangle\langle\psi_0| - I\Big)|\psi_0\rangle = 2|\psi_0\rangle\langle\psi_0|\psi_0\rangle - |\psi_0\rangle = |\psi_0\rangle.$$

Y para $i \neq 0$:

$$\Big(2|\psi_0\rangle\langle\psi_0| - I\Big)|\psi_i\rangle = 2|\psi_0\rangle\langle\psi_0|\psi_i\rangle - |\psi_i\rangle = -|\psi_i\rangle.$$

ii. Calculemos:

$$\langle\varphi|\psi_0\rangle = \left(\sum_{x=0}^{N-1} \alpha_x\langle x|\right)\left(\sum_{x=0}^{N-1} |x\rangle\right) = \sum_{x=0}^{N-1} \alpha_x = 0.$$

iii. En primer lugar, escribamos $|\varphi\rangle$ como $\alpha|\psi_0\rangle + \beta|\bar{\psi}_0\rangle$ donde $|\bar{\psi}_0\rangle$ es un estado ortogonal a $|\psi_0\rangle$. Para ello, tomemos:

$$|\varphi\rangle = \mu|\psi_0\rangle + \beta\left(\sum_{x=0}^{N-1} \frac{\alpha_x - \mu}{\beta}|x\rangle\right).$$

El estado $|\bar{\psi}_0\rangle = \sum_{x=0}^{N-1} \frac{\alpha_x - \mu}{\beta}|x\rangle$, donde

$$\beta = \sqrt{\sum_{x=0}^{N-1} |\alpha_x - \mu|^2}$$

es ortogonal a $|\psi_0\rangle$, ya que si sumamos sus amplitudes:

$$\sum_{x=0}^{N-1} \frac{\alpha_x - \mu}{\beta} = \frac{\left(\sum_{x=0}^{N-1} \alpha_x\right) - N\mu}{\beta} = 0.$$

Estudiando el efecto de $\mathbf{\Gamma}_n$ y usando i tenemos que:

$$\mathbf{\Gamma}_n|\varphi\rangle = \mu|\psi_0\rangle - \beta\left(\sum_{x=0}^{N-1} \frac{\alpha_x - \mu}{\beta}|x\rangle\right) =$$

$$\mu\left(\sum_{x=0}^{N-1}|x\rangle\right) + \beta\left(\sum_{x=0}^{N-1} \frac{\alpha_x - \mu}{\beta}|x\rangle\right) = \sum_{x=0}^{N-1}(2\mu - \alpha_x)|x\rangle.$$

Y obtenemos el resultado buscado.

A la puerta cuántica resultante de aplicar primero $\mathbf{O}_f$ y posteriormente $\mathbf{\Gamma}_n$ la denotaremos *puerta de Grover*.

Definición 4.4. *Puerta de Grover.*
Llamaremos puerta de Grover a la puerta cuántica del sistema de $n+1$ qubits:

$$\boldsymbol{G} = (\mathbf{\Gamma}_n \otimes I)\boldsymbol{O}_f.$$

Veamos cómo podemos usar esta puerta para aumentar la amplitud del estado que nos interesa.

Lema 4.2. En las condiciones del problema de búsqueda, sea $x_0 \in \{0,1\}^n$ tal que $f(x_0) = 1$, y sea

$$|\psi(\alpha,\beta)\rangle = \alpha|x_0\rangle + \beta\left(\sum_{\substack{x=0 \\ x\neq x_0}}^{N-1}|x\rangle\right).$$

Tal que $|\alpha|^2 + (N-1)|\beta|^2 = 1$.
Sea $|\psi(\alpha',\beta')\rangle_n \otimes |-\rangle = \mathbf{G}(|\psi(\alpha,\beta)\rangle_n \otimes |-\rangle)$, entonces:

$$\alpha' = \frac{2N-2}{N}\beta + \frac{N-2}{N}\alpha, \quad \beta' = \frac{N-2}{N}\beta - \frac{2}{N}\alpha.$$

Demostración. En primer lugar calculamos

$$\mathbf{O}_f\Big(|\psi(\alpha,\beta)\rangle \otimes |-\rangle\Big) = -\alpha|x_0\rangle|-\rangle + \beta\left(\sum_{\substack{x=0\\x\neq x_0}}^{N-1}|x\rangle|-\rangle\right).$$

Y aplicando $\mathbf{\Gamma}_n \otimes I$, por el resultado anterior que $\mu = \frac{(N-1)\beta-\alpha}{N}$ y por tanto:

$$\alpha' = (2\mu+\alpha) = \frac{2N-2}{N}\beta - \frac{2}{N}\beta + \alpha = \frac{2N-2}{N}\beta + \frac{N-2}{N}\alpha.$$

$$\beta' = (2\mu-\beta) = \frac{2N-2}{N}\beta - \frac{2}{N}\alpha - \beta = \frac{N-2}{N}\beta - \frac{2}{N}\alpha.$$

Corolario 4.1. Aplicar $\mathbf{G}$ al estado $|\psi(\alpha,\beta)\rangle_n \otimes |-\rangle$ aumenta la amplitud de $|x_0\rangle$ en $|\psi(\alpha',\beta')\rangle_n$ si y solo si $(N-1)\beta > \alpha$.

Estamos ahora preparados para presentar el *algoritmo de Grover*.

Algoritmo de Grover:

INICIO

$\|\varphi_0\rangle_{n+1} \leftarrow \|0\rangle_n \otimes \|1\rangle$

PASO 1

$\|\varphi_1\rangle_{n+1} \leftarrow \mathbf{H}^{\otimes n+1}(\|\varphi_0\rangle_{n+1})$

PASO 2

$\|\varphi_2\rangle_{n+1} \leftarrow \mathbf{G}\|\varphi_1\rangle_{n+1}$

PASO 3

Se repite el paso 2 hasta alcanzar amplitud máxima en el registro que nos interesa, lo que debemos de llevar a cabo $\mathcal{O}(\sqrt{2^n})$ veces. Tras esto, medimos los primeros n qubits.

Antes de analizar el algoritmo veamos un ejemplo.

Ejemplo:

Consideremos el caso $n = 4$ y $x_0 = 7$.

El algoritmo comenzará en el estado: $|0\rangle_4|1\rangle$, y tras el paso 1 tendremos el estado:

$$H^{\otimes 5}|0\rangle_4|1\rangle = \left(\frac{1}{4}\sum_{x=0}^{15}|x\rangle_4\right) \otimes |-\rangle,$$

en el que todos los elementos de base tienen la misma amplitud. Al aplicar $\mathbf{O}_f$ obtenemos el estado:

$$\left(-\frac{1}{4}|7\rangle_4 + \frac{1}{4}\sum_{\substack{x=0\\x\neq 7}}^{15}|x\rangle_4\right) \otimes |-\rangle,$$

en el que el $|7\rangle$ aparece señalado con el cambio de signo de la amplitud. Si aplicamos ahora $\mathbf{\Gamma}_4 \otimes I$ obtenemos:

$$\left(\frac{11}{16}|7\rangle_4 + \frac{5}{16}\sum_{\substack{x=0\\x\neq 7}}^{15}|x\rangle_4\right) \otimes |-\rangle.$$

Y hemos aumentado la amplitud de $|7\rangle$ de $\alpha_0 = 0.25$ a $\alpha_1 \approx 0.4726$. Si volvemos a aplicar $\mathbf{G}$ podemos comprobar que obtenemos $\alpha_2 \approx 0.9084$ y si la volvemos a aplicar otra vez obtenemos $\alpha_3 \approx 0.9613$ y podríamos plantearnos hasta cuando podemos aplicar $\mathbf{G}$ y seguir aumentando la amplitud. Por desgracia, si volvemos a aplicar $\mathbf{G}$ obtenemos $\alpha_4 \approx 0.5817$, por lo que es necesario estudiar más rigurosamente como evoluciona la iteración de esta puerta.

Para ello, consideremos el siguiente resultado.

Teorema 4.1. *Corrección del algoritmo.*
El algoritmo de Grover necesita $\mathcal{O}(2^n)$ iteraciones de $\mathbf{G}$ para maximizar la amplitud del estado deseado $|x_0\rangle$.

Demostración. Para facilitar la prueba consideremos los siguientes estados. Sea $|x_0\rangle_n$ el estado buscado y $N = 2^n$, definiremos:

$$|\gamma\rangle_n = \frac{1}{\sqrt{N-1}} \sum_{\substack{x=0 \\ x \neq x_0}}^{N-1} |x\rangle_n.$$

Sea ahora θ tal que $\operatorname{sen}(\theta) = 1/\sqrt{N}$, consideramos los estados ortogonales:

$$|\psi_0\rangle = \operatorname{sen}(\theta)\,|x_0\rangle + \cos(\theta)\,|\gamma\rangle, \quad |\bar{\psi}_0\rangle = \cos(\theta)\,|x_0\rangle + \operatorname{sen}(\theta)\,|\gamma\rangle.$$

El estado del algoritmo tras el paso 1 será:

$$|\psi_0\rangle \otimes |-\rangle = (\operatorname{sen}(\theta)\,|x_0\rangle + \cos(\theta)\,|\gamma\rangle) \otimes |-\rangle.$$

Y tras aplicar $\mathbf{O}_f$, usando las relaciones $|x_0\rangle = \operatorname{sen}(\theta)\,|\psi_0\rangle + \cos(\theta)\,|\bar{\psi}_0\rangle$ y $|\gamma\rangle = \cos(\theta)\,|\psi_0\rangle - \operatorname{sen}(\theta)\,|\bar{\psi}_0\rangle$ tenemos el estado:

$$\Big(-\operatorname{sen}(\theta)\,|x_0\rangle + \cos\Big(\theta\Big)|\gamma\rangle\Big) \otimes |-\rangle = \Big(\cos(2\theta)\,|\psi_0\rangle - \operatorname{sen}\Big(2\theta\Big)\,|\bar{\psi}_0\rangle\Big) \otimes |-\rangle.$$

Y tras aplicar $\mathbf{\Gamma}_n \otimes I = \Big(2|\psi_0\rangle\langle\psi_0| - I\Big) \otimes I$ obtenemos:

$$\Big(\cos(2\theta)\,|\psi_0\rangle + \operatorname{sen}(2\theta)\,|\bar{\psi}_0\rangle\Big) \otimes |-\rangle = \Big(\operatorname{sen}(3\theta)\,|x_0\rangle + \cos(3\theta)\,|\gamma\rangle\Big) \otimes |-\rangle.$$

Siguiendo este razonamiento podemos probar por inducción que tras aplicar m veces la puerta de Grover $\mathbf{G}$ obtendremos el estado:

$$\Big(\operatorname{sen}((2m+1)\,\theta)\,|x_0\rangle + \cos((2m+1)\,\theta)\,|\gamma\rangle\Big) \otimes |-\rangle.$$

Por tanto, nuestro problema será encontrar el mayor m tal que $\theta(2m+1) \leq \pi/2$, lo que se traduce en $m \leq (\pi - 2\theta)/4\theta$ y por tanto $m = \lfloor(\pi - 2\theta)/4\theta\rfloor$. Dado que si n es grande $\theta \approx \frac{1}{\sqrt{2^n}}$ tenemos que $m \sim \mathcal{O}(\sqrt{2^n})$.

El interés del algoritmo de Grover reside en que la mejora cuadrática que plantea, a pesar de ser inferior a la que dan otros algoritmos, es estricta frente al caso clásico. En otros algoritmos (el algoritmo de Shor por ejemplo) la mejora se basa en la hipótesis de que no se pueden mejorar las versiones clásicas de los algoritmos que resuelven el problema dado.

4.1.2. Soluciones múltiples

Supongamos ahora que nos encontramos de nuevo en la situación del problema de búsqueda, pero en este caso existirá todo un conjunto de elementos $A = \{x \in \{0,1\}^n \mid f(x) = 1\}$ que verifican nuestra condición con $|A| = t$. Para facilitarnos el trabajo denotaremos como $B = \bar{A}$ con $|B| = 2^n - t$.

Veamos cómo podemos generalizar la amplificación de amplitudes a este problema.

En primer lugar, podemos definir los estados:

$$|\psi_A\rangle = \frac{1}{\sqrt{t}} \sum_{x \in A} |x\rangle_n, \quad |\psi_B\rangle = \frac{1}{\sqrt{2^n - t}} \sum_{x \in B} |x\rangle_n.$$

Entonces, si aplicamos las puertas de Hadamard obtendremos el estado

$$|\psi_0\rangle_{n+1} = \sqrt{\frac{t}{2^n}} |\psi_A\rangle_n + \sqrt{\frac{2^n - 1}{2^n}} |\psi_B\rangle_n.$$

Sea ahora θ tal que $\operatorname{sen}(\theta) = \sqrt{t/2^n}$ podemos escribir nuestro estado como:

$$|\bar{\psi_0}\rangle_n = \cos(\theta)|\psi_A\rangle_n - \operatorname{sen}(\theta)|\psi_B\rangle_n.$$

Definiendo su estado ortogonal

$$|\psi_0\rangle_n = \operatorname{sen}(\theta)|\psi_A\rangle_n + \cos(\theta)|\psi_B\rangle_n,$$

podemos llevar a cabo el mismo análisis que en el caso anterior y llegar al siguiente resultado.

Lema 4.3. Tras aplicar m veces la puerta de Grover $\mathbf{G}$ a $|\bar{\psi}_0\rangle_n \otimes |-\rangle$ el estado:

$$\Big(\operatorname{sen}\left((2m+1)\,\theta\right)|\psi_A\rangle + \cos\left((2m+1)\,\theta\right)|\psi_B\rangle\Big) \otimes |-\rangle.$$

El problema ahora reside en calcular cuantas veces hemos de aplicar la puerta de Grover para aumentar la probabilidad de obtener uno de los estados que nos interesan, lo que se complica ya que el valor de θ depende de t que es en principio desconocido.

La cantidad de iteraciones que debemos aplicar es del orden $\mathcal{O}(\sqrt{2^n/t})$ pero no probaremos dicho resultado. [2]

4.2. Quantum counting

El problema que se presentaba en el caso anterior va a inspirar esta sección.

Definición 4.5. *Counting problem.*
Sea n un entero positivo y $\boldsymbol{O}_f$ una puerta oráculo para computar la función $f : \{0,1\}^n \to \{0,1\}$, el counting problem es el problema de determinar el número de valores $x \in \{0,1\}^n$ que verifican $f(x) = 1$.

Para resolver este problema haremos uso no solo de la amplificación de amplitudes si no también de la transformada de Fourier cuántica.

En términos de lo visto en la sección anterior, nuestro objetivo a partir de ahora no será hallar un valor que satisfaga la función; nuestro objetivo será hallar cuántos valores satisfacen dicha condición.

Recordando la notación anterior, tendremos que $A = \{x \in \{0,1\}^n \mid f(x) = 1\}$ con $|A| = t$ y $B = \bar{A}$ con $|B| = 2^n - t$ y nuestro objetivo será hallar t.

De esta forma, volveremos a tener los estados:

$$|\psi_A\rangle = \frac{1}{\sqrt{t}} \sum_{x \in A} |x\rangle_n, \quad |\psi_B\rangle = \frac{1}{\sqrt{2^n - t}} \sum_{x \in B} |x\rangle_n.$$

Antes de ver el algoritmo estudiemos una de las puertas que usa y sus efectos: *la puerta de conteo.*

Definición 4.6. *Puerta de conteo.*
Definimos la puerta de conteo $\boldsymbol{C}_{p,n}$ del sistema de $p+n$ qubits como aquella cuyo efecto en la base computacional es el siguiente:

$$\boldsymbol{C}_{p,n} : |x\rangle_p \otimes |y\rangle_n \mapsto |x\rangle_p \otimes (\boldsymbol{G}_n^x)|y\rangle_n,$$

para $x \in \{0,1\}^p$, $y \in \{0,1\}^n$ y $\boldsymbol{G}_n$ es la puerta de Grover tras aplicarla al sistema de $n+1$ qubits con el qubit objetivo en el estado $|-\rangle$ y descartar dicho qubit.

Para ver sus efectos veamos un resultado previo.

Lema 4.4. Sea $\mathbf{G}_n$ como hemos definido anteriormente y ω tal que $\operatorname{sen}^2(\pi\omega) = t/2^n$, entonces:

1. Los estados

$$|\mu^+\rangle_n = \frac{1}{\sqrt{2}}\Big(|\psi_B\rangle_n - i|\psi_A\rangle_n\Big), \quad |\mu^-\rangle_n = \frac{1}{\sqrt{2}}\Big(|\psi_B\rangle_n + i|\psi_A\rangle_n\Big),$$

   con autovectores de $\mathbf{G}_n$ con autovalores $e^{2i\omega}$ y $e^{-2i\omega}$ respectivamente.
2. Sea

$$|\gamma\rangle_n = \frac{1}{\sqrt{2^n - 1}} \sum_{\substack{x=0 \\ x\neq x_0}}^{2^n-1} |x\rangle_n.$$

   Entonces

$$|\gamma\rangle_n = \operatorname{sen}(\pi\omega)|\psi_A\rangle_n + \cos(\pi\omega)|\psi_B\rangle_n = \frac{e^{i\pi\omega}}{\sqrt{2}}|\mu^+\rangle_n + \frac{e^{-i\pi\omega}}{\sqrt{2}}|\mu^-\rangle_n.$$

Demostración. En primer lugar es sencillo comprobar que

$$|\gamma\rangle_n = \operatorname{sen}(\pi\omega)|\psi_A\rangle_n + \cos(\pi\omega)|\psi_B\rangle_n.$$

Y tras ello podemos ver que

$$\mathbf{G}_n|\psi_A\rangle_n = \left(2|\gamma\rangle\langle\gamma|_n - I^{\otimes n}\right)(-|\psi_A\rangle_n) = 2|\gamma\rangle\langle\gamma|_n + |\psi_A\rangle_n$$
$$= -2\operatorname{sen}(\pi\omega)|\gamma\rangle_n + |\psi_A\rangle_n = -2\operatorname{sen}(\pi\omega)\cos(\pi\omega)|\psi_B\rangle_n + \left(1 - 2\operatorname{sen}^2(\pi\omega)\right)|\psi_A\rangle_n$$
$$= -\operatorname{sen}(2\pi\omega)|\psi_B\rangle_n + \cos(2\pi\omega)|\psi_A\rangle_n.$$

Y de forma análoga

$$\mathbf{G}_n|\psi_B\rangle_n = \cos(2\pi\omega)|\psi_B\rangle_n + \operatorname{sen}(2\pi\omega)|\psi_A\rangle_n.$$

1. El primer apartado es una simple comprobación:

$$\mathbf{G}_n|\mu^+\rangle_n = \frac{1}{\sqrt{2}}\Big(\cos(2\pi\omega)|\psi_B\rangle_n + \operatorname{sen}(2\pi\omega)|\psi_A\rangle_n + i\operatorname{sen}(2\pi\omega)|\psi_B\rangle_n$$
$$-i\cos(2\pi\omega)|\psi_A\rangle_n\Big) = e^{2i\pi\omega}|\mu^+\rangle_n.$$

$$\mathbf{G}_n|\mu^-\rangle_n = \frac{1}{\sqrt{2}}\Big(\cos(2\pi\omega)|\psi_B\rangle_n + \operatorname{sen}(2\pi\omega)|\psi_A\rangle_n - i\operatorname{sen}(2\pi\omega)|\psi_B\rangle_n$$
$$+i\cos(2\pi\omega)|\psi_A\rangle_n\Big) = e^{-2i\pi\omega}|\mu^-\rangle_n.$$

2. Basta llevar a cabo las comprobaciones para obtener el segundo apartado.

Y ahora sí podemos comprobar el efecto de la puerta de conteo.

Lema 4.5. El estado resultante tras aplicar $\mathbf{C}_{p,n}$ al estado $|\gamma\rangle_p \otimes |\gamma\rangle_n$ es:

$$\frac{e^{i\pi\omega}}{\sqrt{2^{p+1}}}\left(\sum_{x=0}^{2^p-1} e^{2i\pi\omega x}|x\rangle_p\right)\otimes|\mu^+\rangle_n + \frac{e^{-i\pi\omega}}{\sqrt{2^{p+1}}}\left(\sum_{x=0}^{2^p-1} e^{2i\pi(1-\omega)x}|x\rangle_p\right)\otimes|\mu^-\rangle_n.$$

Demostración. Desarrollemos los cálculos:

$$\mathbf{C}_{p,n}\left(|\gamma\rangle_p\otimes|\gamma\rangle_n\right) = \frac{1}{\sqrt{2^p}}\sum_{x=0}^{2^p-1}\left[|x\rangle_p\otimes\mathbf{G}_n^x|\gamma\rangle_n\right]$$
$$= \frac{1}{\sqrt{2^p}}\sum_{x=0}^{2^p-1}\left[|x\rangle_p\otimes\mathbf{G}_n^x\left(\frac{e^{i\pi\omega}}{\sqrt{2}}|\mu^+\rangle_n + \frac{e^{-i\pi\omega}}{\sqrt{2}}|\mu^-\rangle_n\right)\right]$$
$$= \frac{1}{\sqrt{2^{p+1}}}\sum_{x=0}^{2^p-1}\left[|x\rangle_p\otimes\left(e^{i\pi\omega}\mathbf{G}_n^x|\mu^+\rangle_n + e^{-i\pi\omega}\mathbf{G}_n^x|\mu^-\rangle_n\right)\right]$$
$$= \frac{1}{\sqrt{2^{p+1}}}\sum_{x=0}^{2^p-1}\left[|x\rangle_p\otimes\left(e^{i\pi\omega(2x+1)}|\mu^+\rangle_n + e^{-i\pi\omega(2x+1)}|\mu^-\rangle_n\right)\right]$$

$$= \frac{e^{i\pi\omega}}{\sqrt{2^{p+1}}} \left(\sum_{x=0}^{2^p-1} e^{2i\pi\omega x} |x\rangle_p \right) \otimes |\mu^+\rangle_n + \frac{e^{-i\pi\omega}}{\sqrt{2^{p+1}}} \left(\sum_{x=0}^{2^p-1} e^{2i\pi(1-\omega)x} |x\rangle_p \right) \otimes |\mu^-\rangle_n.$$

Para entender la importancia de este resultado tomemos el estado de los primeros p qubits en alguno de los sumandos, por ejemplo:

$$\sum_{x=0}^{2^p-1} e^{2i\pi\omega x} |x\rangle_p.$$

Si $\omega = y/2^p$ para algún y entonces este estado se corresponde con aplicar la transformada cuántica de Fourier a $|y\rangle$. De esta forma, si aplicamos $\mathbf{QTF}_{2^p}^{-1}$ a dicho estado obtendremos $y = 2^p\omega$ y podremos por tanto calcular $t = 2^n \operatorname{sen}^2(\pi\omega)$.

Por supuesto en general no nos encontraremos en este caso, pero haciendo p lo suficientemente grande podremos obtener una estimación lo suficientemente buena. El problema que subyace aquí y que no hemos tratado, pero que da lugar a la transformada cuántica de Fourier, es el de la *estimación de fase*. [7]

Quantum counting:

INICIO

$\|\varphi_0\rangle_{p,n} \leftarrow \|0\rangle_p \otimes \|0\rangle_n$

Como ya hemos avanzado, el p será un valor lo suficientemente grande como para garantizar una buena estimación de ω.

PASO 1

$\|\varphi_1\rangle_{p,n} \leftarrow \mathbf{H}^{\otimes p+n}(\|\varphi_0\rangle_{p,n})$

Obtenemos el estado $|\gamma\rangle_p \otimes |\gamma\rangle_n$.

PASO 2

$|\varphi_2\rangle_{p,n} \leftarrow \mathbf{C}_{p,n}|\varphi_1\rangle_{p,n}$

Obtenemos el resultado del lema 4.5.

PASO 3

$|\varphi_3\rangle_{p,n} \leftarrow \left(\mathbf{QFT}_{2^p}^{-1} \otimes I^{\otimes n}\right)|\varphi_2\rangle_{p,n}$

Ya hemos explicado el por qué de este paso, pero vamos a ver en más detalle el resultado.

$$|\varphi_3\rangle_{p,n} = \frac{e^{i\pi\omega}}{\sqrt{2^{p+1}}}\left(\sum_{x=0}^{2^p-1} e^{2i\pi\omega x}\mathbf{QFT}_{2^p}^{-1}|x\rangle_p\right)\otimes|\mu^+\rangle_n + \frac{e^{-i\pi\omega}}{\sqrt{2^{p+1}}}\left(\sum_{x=0}^{2^p-1} e^{2i\pi(1-\omega)x}\mathbf{QFT}_{2^p}^{-1}|x\rangle_p\right)\otimes|\mu^-\rangle_n$$

$$= \frac{e^{i\pi\omega}}{\sqrt{2^{p+1}}}\left(\sum_{y=0}^{2^p-1}\sum_{x=0}^{2^p-1} e^{2i\pi(\omega-\frac{y}{2^p})x}|y\rangle_p\right)\otimes|\mu^+\rangle_n + \frac{e^{-i\pi\omega}}{\sqrt{2^{p+1}}}\left(\sum_{y=0}^{2^p-1}\sum_{x=0}^{2^p-1} e^{2i\pi(1-\omega-\frac{y}{2^p})x}|y\rangle_p\right)\otimes|\mu^-\rangle_n.$$

Y si $y \approx 2^p\omega$ tenemos probabilidad casi 1 de obtener y en el primer sumando, mientras que en el segundo sumando ocurre lo mismo si $\omega = 1 - y/2^p$.

PASO 4

$\bar{l} \leftarrow$ medimos los p primeros qubits de $|\varphi_3\rangle_{p,n}$
if $\bar{l} > 2^{p-1}$ **then**

$\bar{l} \leftarrow 2^p - \bar{l}$
end if
$\bar{t} \leftarrow 2^n \operatorname{sen}^2(\frac{\pi \bar{l}}{2^p})$
return $\bar{t}$

Una vez concluido este paso obtenemos un estimador de t. Gracias al siguiente teorema podemos garantizar que $\bar{t}$ es un buen estimador.

Teorema 4.2. *Corrección del algoritmo de conteo.*
En las circunstancias del algoritmo de conteo se cumple que con probabilidad al menos $\frac{8}{\pi^2}$*:*

$$|t - \bar{t}| \leq \frac{2\pi}{2^p}\sqrt{t(2^n - t)} + \frac{\pi^2}{2^{2p}}|2^n - 2t|.$$

La prueba de este resultado, que no llevaremos a cabo aquí, se puede encontrar en [2].

Al igual que con el problema de búsqueda, para buscar una solución clásica del problema de conteo será necesario llevar a cabo una búsqueda exhaustiva, por que la complejidad de un algoritmo clásico estará en $\Omega(2^n)$.

En el caso cuántico, sin embargo, la complejidad del algoritmo dependerá del estimador p que hemos seleccionado, pero si queremos obtener la solucción exacta la complejidad del algoritmo es $\mathcal{O}\left(\sqrt{(t+1)\,(2^n - t + 1)}\right)$ [7].

Capítulo 5

Conclusión

> *"Everything must be taken into account. If the fact will not fit the theory—let the theory go."*
> **-Agatha Christie**.

Recordemos en primer lugar el camino que hemos recorrido. Dimos el banderazo de salida hablando de los fundamentos de la mecánica cuántica y haciendo especial hincapié en el fenómeno del entrelazamiento por su interés en la construcción de algoritmos cuánticos.

Esto nos permitió construir un nuevo modelo de computación basado en las leyes de la física cuántica y en concreto nos aportó la noción de algoritmo cuántico.

Finalmente, hemos presentado cronológicamente algunos de los algoritmos cuánticos más importantes y las técnicas que se esconden tras ellos, analizando más en detalle el algoritmo de búsqueda de Grover y la amplificación de amplitudes.

Aunque estos algoritmos son importantes en sí mismos y merecen un estudio pormenorizado, nos hemos centrado en la extracción de una serie de técnicas cuya generalización puede permitir la resolución de nuevos problemas en el modelo de computación cuántico.

De hecho, existen numerosos problemas en áreas diversas para los cuales ni siquiera existen algoritmos en este nuevo modelo. Y aunque pueda parecer que la relevancia de los avances en esta dirección se limita a los titulares sensacionalistas de los periódicos en la eterna promesa de construir una realización física de los modelos de computación cuánticos, su importancia trasciende las aplicaciones prácticas. El interés principal que se esconde tras el desarrollo del modelo cuántico

es teórico.

La inclusión de este modelo teórico en el plano de las ciencias de la computación permite establecer nuevas relaciones entre las ya bien conocidas clases de complejidad computacional de los modelos clásicos, por lo que el desarrollo de algoritmos cuánticos puede aportar nuevas vías para resolver problemas de complejidad ya conocidos.

Anexo: Notación

> *"Good advice is always certain to be ignored, but that's no reason not to give it."*
> **-Agatha Christie**.

Durante el desarrollo de toda la memoria usaremos la notación particular llamada *notación de Dirac*. Para sentar las bases de dicha notación y evitar confusiones es conveniente resumirla en este anexo.

- Los vectores se notarán como *kets*: $|\psi\rangle$.
- Los vectores duales se notarán como *bras*: $\langle\psi|$.
- El producto escalar de dos vectores se notará como un *braket*: $\langle\psi|\varphi\rangle$.
- El producto tensorial de dos vectores se notará como producto de bras o de kets respectivamente: $\langle\psi|\otimes\langle\varphi| = \langle\psi|\langle\varphi| = \langle\psi\varphi|$ y $|\psi\rangle\otimes|\varphi\rangle = |\psi\rangle|\varphi\rangle = |\psi\varphi\rangle$.

A lo largo del texto introduciremos el concepto de qubit como un espacio de Hilbert bidimensional. Este sistema cuántico tiene ciertas bases con notaciones estandarizadas.

- La *base computacional* del qubit es la dada por:

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

- La *base de Hadamard* del qubit es la dada por:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \text{ y } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}.$$

Algunos de los operadores cuánticos (o matrices o puertas cuánticas) de un qubit más importantes son:

- La *puerta de Hadamard*, usualmente notada:

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

Cuyo efecto en la base computacional es:

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

para $j = 0, 1$.

- Las *matrices de Pauli* con respecto a los ejes X, Y y Z respectivamente:

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Cuyos efectos en la base computacional son:

$$\mathbf{X}|j\rangle = |1 \oplus j\rangle, \quad \mathbf{Y}|i\rangle = (-i)^j|1 \oplus j\rangle, \quad \mathbf{Z}|j\rangle = (-1)^j|j\rangle,$$

para $j = 0, 1$.

Y podemos comprobar fácilmente que:

Lema 5.1. Todos los operadores anteriores son unitarios, y además, las matrices de Pauli son hermíticas.

Sea ahora $\mathcal{H}$ un sistema cuántico formado por composición de n qubits, un estado cualquiera de $\mathcal{H}$ se notará $|\psi\rangle_n$. Sabemos que los productos tensoriales de las bases computacionales de los respectivos qubits formarán una base de $\mathcal{H}$, que llamaremos base computacional, y que estará formada por los elementos de la forma $\{|i_0 \dots i_{n-1}\rangle\}$ con $i_0, \dots, i_{n-1} = 0, 1$.

Sea un dicho elemento notaremos:

$$|i_0 \dots i_{n-1}\rangle = |j\rangle, \text{ siendo } j = \sum_{k=0}^{n-1} i_k 2^{n-k-1}.$$

De esta forma, un elemento arbitrario de $\mathcal{H}$ se escribirá:

$$|\psi\rangle_n = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle.$$

Además, identificando $\mathcal{H}$ con $\mathbb{C}^{2^n}$ tenemos el siguiente resultado.

Lema 5.2. El elemento de la base $|i\rangle$ se corresponde con el elemento de la base canónica de $\mathbb{C}^{2^n}$ que tiene un 1 en la posición $i + 1$.

La prueba es elemental por inducción.

Otra importante base del sistema formado por 2 qubits es la base *EPR*, llamada así en honor a Albert Einstein, Boris Podolsky y Nathan Rosen. Es la dada por los siguientes estados:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

De ellos, solo el primero se conoce como estado *EPR*.

$$|\text{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

La importancia de esta base es que se trata de una base ortonormal de estados entrelazados, por lo que tiene numerosas aplicaciones.

De igual manera que podemos considerar productos tensoriales de estados para construir sistemas compuestos, dados unos operadores en los sistemas originales, podemos considerar el producto tensorial de dichos operadores que actuará sobre el sistema compuesto. Sean $\{X_i\}$ operadores de un qubit, notaremos:

$$X_1 \otimes X_2 \otimes \cdots \otimes X_n = X_1 X_2 \dots X_n.$$

En casos en el que muchos de estos operadores sean la identidad, podremos acortar esta notación escribiendo como subíndice el sistema sobre el que actúa cada operador y obviando las identidades. Por ejemplo:

$$\mathbf{X}_3\mathbf{Y}_5 = I I \mathbf{X} I \mathbf{Y} I.$$

Siendo $\mathbf{X}$ e $\mathbf{Y}$ las correspondientes matrices de Pauli.

Algunas de las puertas cuánticas en un sistema de múltiples qubits y sus efectos sobre la base computacional son:

- El *NOT controlado* en un sistema de dos qubits:

$$\mathbf{C}_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Cuyo efecto sobre la base computacional es:

$$\mathbf{C}_{NOT}|ij\rangle = |i\rangle|i \oplus j\rangle,$$

con $i, j = \{0, 1\}$.

- El ***U*** *controlado* en un sistema de dos qubits:

$$\mathbf{C}_U|0j\rangle = |0j\rangle, \quad \mathbf{C}_U|1j\rangle = |1\rangle\mathbf{U}|j\rangle,$$

con $j = \{0, 1\}$.
Cuyo efecto sobre la base computacional es:

$$\mathbf{C}_U|0j\rangle = |0j\rangle, \quad \mathbf{C}_U|1j\rangle = |1\rangle\mathbf{U}|j\rangle,$$

con $j = \{0, 1\}$.

- La *puerta oráculo* asociada a una aplicación $f : \{0, 1\}^n \to \{0, 1\}^m$ en un sistema de $n + m$ qubits, cuyo efecto es:

$$\mathbf{O}_f : |x\rangle_n|y\rangle_m \mapsto |x\rangle_n|y \oplus f(x)\rangle_m,$$

para $x \in \{0, 1\}^n$ e $y \in \{0, 1\}^m$.

- La *transformada de Fourier cuántica* en un sistema de n qubits con $m \leq 2^n$, cuyo efecto es:

$$\mathbf{QTF}_m : |x\rangle_n \mapsto \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} e^{2\pi i y x/m}|y\rangle_n,$$

para $x \in \{0, 1\}^n$.

- La *puerta de cambio de fase* en un sistema de n qubits, cuyo efecto sobre la base computacional es:

$$\begin{cases} \mathbf{U}_{0^\perp} : |0\rangle_n \mapsto |0\rangle_n \\ \mathbf{U}_{0^\perp} : |x\rangle_n \mapsto -|x\rangle_n \quad \text{si } x \neq 0. \end{cases}$$

- La *puerta de difusión de Grover* en un sistema de n qubits:

$$\mathbf{\Gamma}_n = \mathbf{H}^{\otimes n}\mathbf{U}_{0^\perp}\mathbf{H}^{\otimes n}.$$

- La *puerta de Grover* asociada a un problema de búsqueda con función característica f en un sistema de $n + 1$ qubits:

$$\mathbf{G} = (\mathbf{\Gamma}_n \otimes I)\mathbf{O}_f.$$

- La *puerta de conteo* en un sistema de $n + p$ qubits, cuyo efecto en la base computacional es el siguiente:

$$\mathbf{C}_{p,n} : |x\rangle_p \otimes |y\rangle_n \mapsto |x\rangle_p \otimes (\mathbf{G}_n^x)|y\rangle_n,$$

para $x \in \{0, 1\}^p$, $y \in \{0, 1\}^n$.

Bibliografía

[1] Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., ... & Weinfurter, H. (1995). *Elementary gates for quantum computation.* Physical review A, 52(5), 3457.

[2] Boyer, M., Brassard, G., Høyer, P. & Tapp, A. (1998). *Tight bounds on quantum searching.* Fortschritte der Physik: Progress of Physics, 46(4-5), 493-505.

[3] Deutsch, D. (1985). *Quantum theory, the Church–Turing principle and the universal quantum computer.* Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818), 97-117.

[4] Deutsch, D. (1989). *Quantum computational networks.* Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 425(1868), 73-90.

[5] Gómez Serván, C. (2017) *Introducción a la mecánica cuántica.* http://hdl.handle.net/11441/66967

[6] Gottesman, D. (1998) *The Heisenberg representation of quantum computers.*
arXiv preprint quant-ph/9807006.

[7] Kaye, P., Laflamme, R. & Mosca, M. (2007). *An introduction to quantum computing.*
Oxford University Press.

[8] Landsberg, J. M. (2018) *A very brief introduction to quantum computing and quantum information theory for mathematicians.*
https://arxiv.org/abs/1801.05893

[9] Lyons, D. W. (2003). *An elementary introduction to the Hopf fibration.* Mathematics magazine, 76(2), 87-98.

[10] Nielsen, M. A. & Chuang I. L. (2010). *Quantum Computation and Quantum Information.* New York: Cambridge University Press.

[11] Ossorio-Castillo, J. & Tornero, J. M. (2018) *Quantum computing from a mathematical perspective: a description of the quantum circuit model.*
arXiv:1810.08277

[12] Pastor Díaz, U. (2018) *Códigos correctores de errores cuánticos.*
https://hdl.handle.net/11441/77568

[13] Pérez-Jiménez, M., & Riscos-Núnez, A. (2004) *Modelos de computación celular, molecular y cuántica.*
Fénix Editorial. Sevilla.

[14] Shor, P. W. (1994) *Algorithms for quantum computation: Discrete logarithms and factoring.*
In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.