UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRADO DE MATEMÁTICAS

Trabajo de fin de grado

El algoritmo de Shor

Autora: Beatriz Benavente de Lucas

Director: Dr. Xavier Guitart Morales
Realizado en: Departamento de Matemáticas e Informática

Barcelona, 9 de junio de 2024

Abstract

This paper examines the development and relevance of Shor's algorithm for factoring integers $N = pq$. Its potential impact on classical cryptography is highlighted, particularly as an emerging threat to the RSA public-key cryptosystem. To fully grasp the algorithm and its mathematical significance, we introduce the fundamentals of quantum mechanics and number theory upon which it is based. The study explores the algorithm in depth, highlighting its improved complexity of $O((\log N)^3)$ compared to the best-known classical alternative, which has a complexity of $O(e^{(\log N)^{1/3}})$.

Resumen

En este trabajo, se analiza el desarrollo y la relevancia del algoritmo de Shor de factorización de enteros $N = pq$. Se destaca su potencial impacto en la criptografía clásica, particularmente como una amenaza emergente al criptosistema de clave pública RSA. Para una comprensión completa del algoritmo y su importancia desde una perspectiva matemática, se introducen los fundamentos de mecánica cuántica y teoría de números sobre los cuales se fundamenta. El estudio profundiza en el algoritmo, destacando su complejidad mejorada de $O((\log N)^3)$ en comparación con la mejor alternativa clásica conocida, cuya complejidad es de $O(e^{(\log N)^{1/3}})$.

2020 Mathematics Subject Classification. 11Y16, 68Q12, 68Q25, 65Y20.

Agradecimientos

Este trabajo, y en general esta carrera, ha progresado gracias al apoyo de mi familia y amigos. Gracias a mi familia por inculcarme la pasión por el aprendizaje y la perseverancia para seguir adelante. A mis amigos, les doy las gracias por acompañarme en esta aventura, con su escucha y su paciencia. En especial, a mis compañeros de carrera, quienes han compartido conmigo años de descubrimientos, animándome a abordar la vida, las matemáticas y la física con entusiasmo y diversión. Por último, deseo expresar mi gratitud a mi tutor, Xevi Guitart, cuyo apoyo desde el inicio ha sido fundamental. Gracias por introducirme en este fascinante campo de las matemáticas y por guiarme en la creación de este trabajo.

Índice

1. Introducción **1**

2. Criptografía clásica **3**

2.1. RSA 3

3. Introducción a la mecánica cuántica **6**

3.1. Espacios cuánticos 6

3.2. Operadores cuánticos 9

3.3. Puertas cuánticas 11

3.4. Transformada cuántica de Fourier 14

4. Algoritmo de Deutsch **19**

4.1. Desarrollo 19

5. Algoritmo de Shor **22**

5.1. Bases de teoría de números para el algoritmo de Shor 22

5.2. Exponenciación binaria 23

5.3. Fracciones continuas 23

5.4. Parte clásica 25

5.5. Parte cuántica 27

5.5.1. Parte cuántica generalizada 29

6. Distribución cuántica de claves **36**

7. Conclusiones **38**

1. Introducción

La criptografía, del griego *Escritura secreta*, es el conjunto de métodos de cifrado de la información con el objetivo de que sólo sus destinatarios consigan entenderlo. En el contexto de la criptografía, dos personas, típicamente referidas como Alice y Bob desean intercambiar una información sin que un tercero, Eve, la intercepte. Para ello, crean una clave y codifican su mensaje de acuerdo a ella. La criptografía ha estado presente en todas las grandes civilizaciones. Sin embargo, a pesar de existir desde hace miles de años, su mayor desarrollo ha sido en los últimos 100 años, potenciado por el desarrollo tecnológico.

Desde la antigüedad han existido diversas manera de cifrado que han ido evolucionando con la sociedad, desde el simple cifrado del César hasta las sofisticadas máquinas de encriptación como la Enigma utilizada durante la Segunda Guerra Mundial. No obstante, toda la historia antigua de la criptografía viene marcada por un riesgo: el intercambio de claves era manual, en secreto. Con el desarrollo de los ordenadores e internet, la necesidad de intercambiar claves a distancia, y así poder establecer un entorno digital seguro sin necesidad de encontrarse en persona, se hizo imperativa.

En 1976, Whitfield Diffie y Martin Hellman presentaron el innovador método de intercambio de claves Diffie-Hellman, permitiendo a dos partes generar una clave secreta compartida a través de un canal público. Con el avance de internet y la vida digital, la criptografía se ha convertido en un pilar imprescindible en la ciberseguridad. Actualmente, llevamos una vida digital que deseamos sea segura, desde la privacidad de nuestros mensajes, las firmas digitales o la protección de nuestros datos bancarios en las compras online, todo ello pasa por trabajar en una criptografía robusta.

En particular, actualmente se utiliza el criptosistema RSA, introducido por Ron Rivest, Adi Shamir y Leonard Adleman en 1977, para la seguridad de internet, firmas digitales, autentificación de usuarios y otras aplicaciones clave. Este criptosistema se basa en la dificultad del antiguo problema matemático de factorizar un entero de gran magnitud N en sus factores primos. La *dificultad* o complejidad de este problema, depende, al fin y al cabo del algoritmo conocido capaz de la factorización. A su vez, este algoritmo, depende de la rapidez de computación del sistema que lo aplique. Por tanto, en el contexto actual tecnológico, podemos decir que el RSA depende, en realidad, de la complejidad de aplicar el algoritmo clásico conocido, en los ordenadores clásicos para factorizar N. Actualmente la complejidad de este algoritmo es subexponencial en $\log(N)$. Así pues, si encontrásemos un mejor algoritmo o un mejor ordenador, quizás el factorizar N no sería tan complejo.

Los avances de computación y mejoras de algoritmos a finales del siglo XX, se vieron acompañados por un avance en el campo de la física y la informática. En concreto, la incorporación de la teoría cuántica en la informática supuso un nuevo campo conocido como computación cuántica. La diferencia entre la computación clásica y la cuántica comienza en la unidad mínima de información utilizada, y con ella, la manera de manipularla. En la computación clásica, se utilizan los bits, que pueden estar en estado 0 o 1. Por otro lado, en la computación cuántica se introduce una nueva unidad de información, el qubit. El qubit sigue las leyes de la cuántica, que es no determinista, permitiendo que en una unidad de información convivan el estado 0 y el 1, en un estado de superposición. Con esto, a lo que nos referimos es a lo siguiente: supongamos que tenemos numerosas copias idénticas de un qubit que está en un estado, $|\psi\rangle$, de superposición de 0 y 1, lo cual se escribe en notación cuántica como:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

con $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2+|\beta|^2 = 1$. Si midiésemos estas copias idénticas, obtendríamos un 0, con probabilidad $|\alpha|^2$, y un 1, con probabilidad $|\beta|^2$. Esta propiedad que deriva de la cuántica, cambia radicalmente el modo de funcionamiento de los algoritmos y los ordenadores cuánticos. La eficiencia de estos algoritmos cuánticos para abordar problemas clásicos se ha demostrado en múltiples ocasiones. Entre estos algoritmos, destaca el algoritmo de factorización de Shor.

En 1994, Peter Shor, desarrolló un algoritmo cuántico que aprovecha la naturaleza cuántica de los qubits para factorizar de manera eficiente números enteros grandes, N, en factores primos. Este algoritmo tiene una complejidad polinómica de $O((\log N)^3)$, lo que lo hace significativamente más eficiente que el algoritmo clásico, cuya complejidad crece subexponencialmente con N y es del orden de $O(e^{(\log N)^{1/3}})$. Este algoritmo fue implementado experimentalmente por primera vez en 2001, por el grupo IBM, que consiguió factorizar 15 en 3 y 5 utilizando un ordenador cuántico de resonancia magnética nuclear. A pesar de estos avances, aún existe un desafío significativo en la construcción de ordenadores cuánticos debido a la complejidad de su arquitectura y la corrección de errores. En cuanto a la seguridad del RSA utilizado actualmente, se estima que se necesitaría un ordenador cuántico con miles de qubits para romper el RSA con claves de 2048 bits. El mayor ordenador cuántico hoy en día cuenta con 433 qubits, así que el riesgo inmediato es limitado. No obstante, se están explorando alternativas no vulnerables frente a los ordenadores cuánticos, como sistemas de computación clásica basados en problemas aún no resueltos por algoritmos cuánticos o el uso de la criptografía cuántica para la distribución segura de claves.

En este trabajo, trataremos de entender el algoritmo de Shor y su impacto desde una perspectiva matemática. Para ello, comenzaremos por introducir las nociones básicas de criptografía y el sistema RSA. Más adelante, presentaremos los fundamentos de la mecánica cuántica necesarios para entender el desarrollo de los algoritmos cuánticos. Haremos especial atención a la Transformada Cuántica de Fourier, que es un paso clave imprescindible del algoritmo de Shor. Estudiaremos el algoritmo de Deutsch, que es un algoritmo cuántico aplicable a un sistema de 2 qubits, como ejemplo de algoritmo cuántico básico. A continuación, abordaremos el algoritmo de Shor, empezando con las bases de teoría de números para plantear el problema de factorización de N; así como otras herramientas que son necesarias para la completa comprensión del proceso, como son las fracciones continuas. El desarrollo del algoritmo, se hará en dos partes, la parte clásica y la parte cuántica. En todo este desarrollo, estudiaremos la complejidad de los pasos a seguir en el algoritmo, que es la clave de la eficiencia del mismo. Por último, veremos en la última sección una introducción a la criptografía cuántica; en particular, la distribución cuántica de claves.

2. Criptografía clásica

La criptografía es el estudio de los métodos de envío de mensajes codificados de tal manera que solo los destinatarios del mensaje consigan leer el mensaje [1, 3]. En este estudio, mandamos un mensaje, texto en claro, de manera codificada, texto cifrado. Para pasar de un texto en claro a un texto cifrado, utilizamos una transformación de cifrado, $f : \mathcal{P} \to \mathcal{C}$, donde $\mathcal{P}$ es el conjunto de todas las unidades de mensaje de textos simples posibles y $\mathcal{C}$ similarmente de textos cifrados. Para descifrar un mensaje y obtener el texto simple utilizamos la transformación de descifrado, f^{-1}. Un criptosistema es entonces el conjunto de protocolos, transformaciones de cifrado y descifrado y claves que describen dicho intercambio de información. Podemos representar dicho intercambio esquemáticamente tal que:

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

El cifrado puedes describirse con un algoritmo y los valores de los parámetros utilizados en este, que llamamos clave de cifrado K_E. De la misma manera, una transformación de descifrado puede describirse refiriéndose a los valores de los parámetros como clave de descifrado K_D. En general, suponemos que los algoritmos de cifrado y descifrado son conocidos y son las claves K_E y K_D las que pueden ser ocultas. Podemos hacer, entonces, una diferenciación entre los criptosistemas de clave privada y los de clave pública. Típicamente, nos referimos a las personas que desean compartir una información como Alice y Bob.

Criptosistemas de clave privada

Los criptosistemas de clave privada son aquellos en los que, una vez sabida la clave de cifrado, la transformación de descifrado puede implementarse en un tiempo similar al de la transformación de cifrado. En estos sistemas, la misma clave es utilizada tanto para cifrar como para descifrar el mensaje.

En este contexto, Alice y Bob deben intercambiar la clave secreta K de manera segura antes de iniciar la comunicación. Este intercambio de claves supone un riesgo de seguridad, ya que un tercero podría interceptar la clave durante el intercambio.

Criptosistemas de clave pública

Los criptosistemas de clave pública se definen como aquellos criptosistemas en los que el conocimiento de la clave de cifrado no permite conocer la clave de descifrado sin un tiempo de computación prohibitivamente largo. Es decir, una vez sabida la clave de cifrado K_E, la función de cifrado $f : \mathcal{P} \to \mathcal{C}$ es fácil de calcular. Sin embargo, la función inversa, de descifrado, $f^{-1} : \mathcal{C} \to \mathcal{P}$, es muy difícil de calcular en la práctica para alguien que no tenga conocimiento de K_D. Por tanto, la clave K_E puede hacerse pública sin permitir que los mensajes sean descifrados por terceros.

2.1. RSA

El RSA es un sistema de cifrado de clave pública. En este caso, la función cuya inversa es difícil de calcular se basa en el problema de factorización de números enteros

compuestos. Es decir, sea $N = pq$, donde p y q son números primos, la dificultad reside en determinar p y q sabiendo solo N.

El proceso de cifrado se basa en los siguientes pasos:

1. Escoger dos números primos grandes p y q, y calcular $N = pq$.
2. Calcular $\phi(N) = (p-1)(q-1)$.
3. Escoger un número entero e tal que $1 < e < \phi(N)$ y $\gcd(e, \phi(N)) = 1$.
4. Calcular $d = e^{-1} \bmod \phi(N)$.

Por tanto, la clave de cifrado que se hace pública es $K_E = (N, e)$, mientras que la clave de descifrado permanece oculta como $K_D = (N, d)$. La transformación de cifrado es la función sobre $(\mathbb{Z}/N\mathbb{Z})^*$ definida como $f(P) \equiv P^e \bmod N$. La función de descifrado es $f^{-1}(C) \equiv C^d \bmod N$. Para el descifrado del mensaje, utilizamos el Teorema de Euler-Fermat, que recordamos a continuación.

Teorema 2.1. (Euler-Fermat). *Sean a, N dos enteros tales que $N > 0$ y gcd(a, N)=1. Entonces $a^{\phi(N)} \equiv 1 \bmod N$.*

Para el descifrado del mensaje P tenemos

$$\begin{aligned} f^{-1}(f(P)) &= C^d \bmod N \\ &= (P^e \bmod N)^d \bmod N \\ &= P^{ed} \bmod N, \end{aligned}$$

donde $ed \equiv 1 \bmod \phi(N)$ y por tanto podemos expresar este producto como $ed = k\phi(N)+1$. Así pues, aplicando esta propiedad y el teorema de Euler-Fermat:

$$\begin{aligned} P^{ed} \bmod N &= P^{k\phi(N)+1} \bmod N \\ &= (P^{\phi(N)})^k P \bmod N \\ &= 1^k P \bmod N = P. \end{aligned}$$

Por tanto, poder descifrar los mensajes depende del cálculo o conocimiento de $d = e^{-1} \bmod \phi(N)$. Entonces, para obtener d, tenemos que calcular $\phi(N) = (p-1)(q-1)$, y para ello, necesitamos saber p y q. Es decir, calcular d a partir de $\phi(N)$ es equivalente al problema de factorizar N en sus factores primos, un problema computacionalmente difícil para enteros grandes N cuando se eligen adecuadamente los primos p y q.

Para el intercambio efectivo de información, Alice crearía una clave pública como hemos explicado anteriormente y la distribuiría: $K_E = (N, e)$. De esta manera, Bob puede utilizar esta clave pública para cifrar un mensaje M y publicarla como $f(M)$. Como solo Alice tiene la clave de descifrado K_D, solo ella podrá descifrar el mensaje publicado por Bob, obteniendo así : $f^{-1}(f(M)) = M$. Así, Alice y Bob han intercambiado un mensaje de manera segura y pública. Además, en este intercambio puede compartirse una clave $M = K_B$, para una comunicación posterior privada y segura.

Así pues, el RSA permite la comunicación segura en un criptosistema de clave pública. Este método depende de la dificultad de factorización de $N = pq$ utilizando ordenadores clásicos. Actualmente, el algoritmo mejor clásico conocido es el de criba general del cuerpo

de números, [2], que es de una complejidad de $O(e^{(\log N)^{1/3}})$. Sin embargo, existen nuevos algoritmos cuánticos para esta tarea, lo cual supone un riesgo potencial para el RSA. En particular, el algoritmo de Shor ha demostrado su eficacia en la factorización eficiente de números enteros grandes.

3. Introducción a la mecánica cuántica

Los bits cuánticos, o qubits, son la unidad básica de información en la computación cuántica. En la computación clásica, la unidad básica de información son los bits. Éstos pueden estar en un momento dado en un estado 0 o 1. A diferencia de los bits, los qubits pueden estar en una superposición de ambos estados simultáneamente, gracias a los principios de la superposición cuántica. Esta característica del qubit esencialmente permite que los ordenadores cuánticos realicen cálculos de manera paralela, ofreciendo una capacidad de procesamiento exponencialmente mayor que los sistemas clásicos, para algunos procesos.

En esta sección, abordaremos los fundamentos de la mecánica cuántica. La singularidad de los ordenadores cuánticos radica en la aplicación en los principios de la mecánica cuántica y la manipulación de los qubits. Para ello, introduciremos los postulados cuánticos, que son los principios fundamentales que describen un sistema cuántico.

3.1. Espacios cuánticos

Definición 3.1. *Un espacio vectorial E sobre $\mathbb{C}$ es prehilbertiano si está dotado de un producto hermitiano; esto es, una aplicación:*

$$\begin{aligned}\langle , \rangle : & E \times E \longrightarrow \mathbb{C} \\ & (u, v) \longmapsto \langle u, v \rangle,\end{aligned}$$

satisfaciendo:

1. $\langle u, v \rangle = \langle v, u \rangle^*, \forall u, v \in E$. *De hecho,* $\langle u, u \rangle \in \mathbb{R}$.
2. $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle, \forall u, v, w \in E$.
3. $\langle u, \lambda v \rangle = \lambda \langle u, v \rangle \forall u, v \in E, \forall \lambda \in \mathbb{C}$.
4. $\langle u, u \rangle > 0, \forall u \in E - \{0\}$. *Es más,* $\langle u, u \rangle = 0$ *si y sólo si* $u = 0$.

Definición 3.2. *Un espacio de Hilbert, $\mathcal{H}$, es un espacio prehilbertiano sobre $\mathbb{C}$, tal que la norma que induce el producto hermitiano define una métrica completa.*

Postulado 1. La máxima información posible sobre un sistema físico es su estado cuántico, que se representa por un vector unitario con fase arbitraria en un espacio de Hilbert separable, $\mathcal{H}$.

Trabajaremos en un espacio de Hilbert $\mathbb{C}^2$, con el producto escalar usual.

Definición 3.3. *Los vectores*

$$|0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \ y \ |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

se llaman base de estados de un bit cuántico.

En este caso, utilizamos una notación similar a la del bit clásico. Sin embargo, un estado general de un bit cuántico no es necesariamente $|\psi\rangle = |0\rangle$ o $|\psi\rangle = |1\rangle$, si no una combinación lineal de éstos.

Definición 3.4. *Un estado cuántico puro de qubit $|\psi\rangle$ es un vector unitario, combinación lineal de la base de estados,*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

donde $\alpha, \beta \in \mathbb{C}$ son las amplitudes del estado.

Por definición de vector unitario, tenemos que $|\alpha|^2 + |\beta|^2 = 1$ En este trabajo estamos utilizando la notación 'bra-ket' introducida por el físico Paul Dirac. En ella utilizamos los ket, $|\psi\rangle$ para describir un estado cuántico. El complejo conjugado o conjugado Hermítico de $|\psi\rangle$, es descrito por el bra $\langle\psi|$. El producto escalar entre dos estados cuánticos $|\psi\rangle$ y $|\phi\rangle$ se describe por un braket $\langle\psi|\phi\rangle$.

Por lo tanto, $|0\rangle$ y $|1\rangle$ forman una base del espacio de Hilbert $\mathbb{C}^2$. Nos referiremos a esta base como base computacional del qubit. Existen otras bases utilizadas en los sistemas cuánticos como es por ejemplo la base $|+\rangle, |-\rangle$

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

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}.$$

Podemos escribir cualquier estado puro normalizado como

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

donde $\phi \in [0, 2\pi)$ describe la fase relativa y $\theta \in [0, \pi]$ determina la probabilidad de medir $|0\rangle$ o $|1\rangle$.

$$p(0) = \cos^2\frac{\theta}{2} \qquad p(1) = \sin^2\frac{\theta}{2}.$$

Todos los estados puros normalizados pueden ser representados sobre una esfera de radio unidad llamada la esfera de Bloch. Las coordenados del estado sobre la esfera vienen dadas por el vector de Bloch:

$$\vec{r} = \begin{pmatrix}\sin\theta\cos\phi\\ \sin\theta\sin\phi\\ \cos\theta\end{pmatrix}$$

Ejemplos 3.5.

- $|0\rangle : \theta = 0$, ϕ es arbitrario $\rightarrow \vec{r} = \begin{pmatrix}0\\0\\1\end{pmatrix}$
- $|1\rangle : \theta = \pi$, ϕ es arbitrario $\rightarrow \vec{r} = \begin{pmatrix}0\\0\\-1\end{pmatrix}$
- $|+\rangle : \theta = \frac{\pi}{2}$, $\phi = 0 \rightarrow \vec{r} = \begin{pmatrix}1\\0\\0\end{pmatrix}$
- $|-\rangle : \theta = \frac{\pi}{2}$, $\phi = \pi \rightarrow \vec{r} = \begin{pmatrix}-1\\0\\0\end{pmatrix}$

- $|+i\rangle : \theta = \frac{\pi}{2},\ \phi = \frac{\pi}{2} \rightarrow \vec{r} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$
- $|-i\rangle : \theta = \frac{\pi}{2},\ \phi = 3\frac{\pi}{2} \rightarrow \vec{r} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$

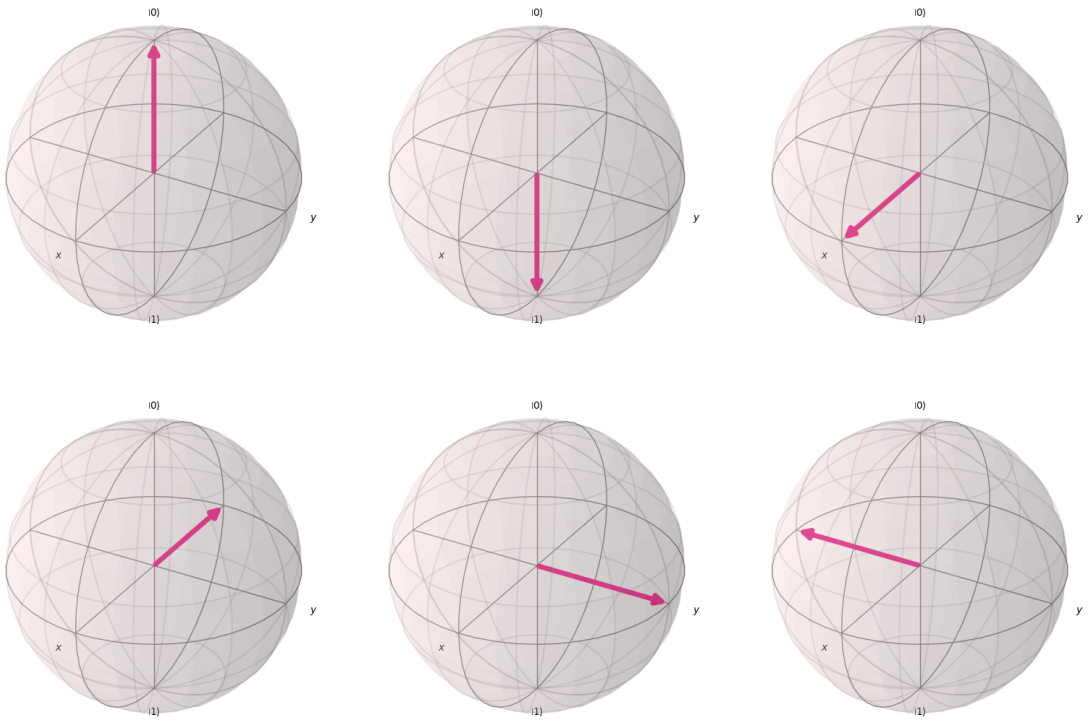

Figura 1: Representaciones de los estados cuánticos $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}$ (de izquierda a derecha empezando por la fila superior) sobre la esfera de Bloch.

Definición 3.6. *Sean E y F espacios vectoriales sobre $\mathbb{C}$ de dimensiones n y m respectivamente. El producto vectorial entre E y F, $E \otimes F$, es un espacio vectorial nm-dimensional generado por los elementos de la forma $v \otimes w$, donde $v \in E$ y $W \in F$ cumpliendo las siguientes propiedades:*

- $\alpha(v \otimes w) = (\alpha v) \otimes w = v \otimes (\alpha w)$
- $(v_1 + v_2) \otimes w = (v_1 \otimes w) + (v_2 \otimes w)$
- $v \otimes (w_1 + w_2) = (v \otimes w_1) + (v \otimes w_2)$

donde $\alpha \in \mathbb{C}, v, v_1, v_2 \in E$ y $w, w_1 w_2 \in F$.

Sean E y F espacios vectoriales de dimensiones n y m respectivamente. Sean $e_1, ..., e_n$ base de E y $f_1, ..., f_m$ base de F. Entonces podemos construir una base del espacio producto tensorial $E \otimes F$ como:

$$e_i \otimes f_j \qquad \begin{matrix} i = 1, \ldots, n \\ j = 1, \ldots, m. \end{matrix}$$

Sean E y F espacios vectoriales. La dimensión del producto tensorial entre E y F es

$$dim(E \otimes F) = dimE \cdot dimF.$$

Sean E y F espacios vectoriales de dimensiones n y m respectivamente. Sean $e_1, ..., e_n$ base de E y $f_1, ..., f_m$ base de F. Un elemento general de $E \otimes F$ viene dado por

$$w = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} e_i \otimes f_j.$$

Debemos tener en cuenta que en general, no se cumple necesariamente $w = u \otimes v$ donde $u \in E$ y $v \in F$. Es decir, el espacio tensorial contiene elementos que no pueden expresarse de manera simple.

Ejemplo 3.7. El siguiente estado $|\psi\rangle$ no puede expresarse de manera simple como producto tensorial de dos estados de los espacios vectoriales, sino como combinación lineal de varios.

$$|\psi\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$$

Observación 3.8. En un ordenador clásico podemos representar un entero $a \in \mathbb{Z}_{\geq 0}$ tal que $a < 2^n$ con un sistema numérico en base 2:

$$a = \sum_{l=0}^{n-1} a_l 2^l$$

donde $a_l \in \{0, 1\}$ son los dígitos binarios de a. En un computador cuántico también representaremos un entero $a \in \mathbb{Z}_{\geq 0}$ tal que $a < 2^n$ con n qubits:

$$|a\rangle_n = |a_{n-1} \dots a_1 a_0\rangle = \bigotimes_{l=0}^{n-1} |a_l\rangle = |a_{n-1}\rangle \otimes \dots \otimes |a_1\rangle |a_0\rangle.$$

Ejemplo 3.9. El número $39 < 2^6$ puede ser representado con 6 qubits de manera que:

$$|39\rangle_6 = |100111\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |1\rangle.$$

Notación 3.10. *A partir de ahora, cuando escribamos el subíndice n a un ket, $|\psi\rangle_n$, nos referiremos a estar trabajando en un sistema de n qubits. Cuando no hagamos uso de ningún subíndice nos referiremos a un sistema de un solo qubit. Además, omitiremos el símbolo de producto tensorial de manera que $|vw\rangle = |v\rangle \otimes |w\rangle$.*

3.2. Operadores cuánticos

Definición 3.11. *Sean $\mathcal{H}_1$, $\mathcal{H}_2$ espacios de Hilbert, un operador cuántico lineal,* O, *es una aplicación lineal*

$$\begin{array}{rcl} \mathrm{O} : \mathcal{H}_1 & \longrightarrow & \mathcal{H}_2 \\ u & \rightarrow & O(x) = v. \end{array}$$

En notación cuántica, $\mathrm{O}\,|u\rangle = |v\rangle$.

Eligiendo bases de $\mathcal{H}_1$, $\mathcal{H}_2$ podemos asociar una matriz al operador cuántico. Típicamente en mecánica cuántica, $\mathcal{H}_1 = \mathcal{H}_2$ por lo que la matriz asociada es cuadrada.

Definición 3.12. *Sean* A *un operador cuántico, diremos que* $\mathrm{A}^\dagger$ *es adjunto de* A *si* $\langle\psi_2|\,\mathrm{A}^\dagger\,|\psi_1\rangle = \langle\psi_1|\,\mathrm{A}\,|\psi_2\rangle^*$.

Definición 3.13. *Diremos que un operador* A *es hermítico si* $\mathrm{A}^\dagger = \mathrm{A}$.

Cuando el dominio de un operador y su adjunto es el mismo, los términos autoadjunto y hermítico son equivalentes. Por tanto, en dimensión finita todo operador hermítico es también autoadjunto.

Postulado 2. Cualquier magnitud observable del sistema físico tiene asociado un operador autoadjunto, definido sobre $\mathcal{H}$. Los valores propios de este operador constituyen una base ortonormal de $\mathcal{H}$.

Definición 3.14. *Un operador unitario es aquel que tiene asociada una matriz unitaria; y preserva la norma de los vectores de estado.*

Definición 3.15. *En el contexto de la computación cuántica, un operador unitario sobre* n *qubits se llama una puerta cuántica sobre* n *qubits.*

Definición 3.16. *Sea* A *una matriz de dimensión* $m \times n$ *y* B *una matriz de dimensión* $k \times l$. *Definimos el producto de Kronecker entre* A *y* B, *denotado* $A \otimes B$, *como la matriz de dimensión* $mk \times nl$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nn}B \end{bmatrix}$$

De manera detallada,

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1l} & \cdots & \cdots & a_{1n}b_{11} & a_{1n}b_{12} & \cdots & a_{1n}b_{1l} \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{11}b_{2l} & \dots & \cdots & a_{1n}b_{21} & a_{1n}b_{22} & \dots & a_{1n}b_{2l} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \dots & \vdots \\ a_{11}b_{k1} & a_{11}b_{k2} & \cdots & a_{11}b_{kl} & \cdots & \cdots & a_{1n}b_{k1} & a_{1n}b_{k2} & \cdots & a_{1n}b_{kl} \\ \vdots & \vdots & & \vdots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & & \ddots & \vdots & \vdots & & \vdots \\ a_{m1}b_{11} & a_{m1}b_{12} & \cdots & a_{m1}b_{1l} & \cdots & \cdots & a_{mn}b_{11} & a_{mn}b_{12} & \cdots & a_{mn}b_{1l} \\ a_{m1}b_{21} & a_{m1}b_{22} & \cdots & a_{m1}b_{2l} & \cdots & \cdots & a_{mn}b_{21} & a_{mn}b_{22} & \cdots & a_{mn}b_{2l} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{k1} & a_{m1}b_{k2} & \cdots & a_{m1}b_{kl} & \cdots & \cdots & a_{mn}b_{k1} & a_{mn}b_{k2} & \cdots & a_{mn}b_{kl} \end{pmatrix}.$$

En particular, el producto de Kronecker se corresponde con la matriz producto tensorial de operadores respecto las bases naturales.

Definición 3.17. *Sean* A *y* B *operadores lineales definidos en* E *y* F *respectivamente, entonces el operador lineal* $\mathrm{A} \otimes \mathrm{B}$ *operando en* $E \otimes F$ *es*

$$(\mathrm{A} \otimes \mathrm{B})(v \otimes w) = (\mathrm{A}\,v) \otimes (\mathrm{B}\,w)$$

donde $v \in E$ *y* $w \in F$. *Además, esta definición se extiende por linealidad.*

Ejemplos 3.18. Veamos los siguientes ejemplos de productos tensoriales entre matrices de diferentes dimensiones.

- $\begin{bmatrix}5\\2\end{bmatrix} \otimes \begin{bmatrix}3\\6\end{bmatrix} = \begin{bmatrix}15\\30\\6\\12\end{bmatrix}$.
- $\begin{bmatrix}2\\1\\2\end{bmatrix} \otimes \begin{bmatrix}1 & 4 & 3\end{bmatrix} = \begin{bmatrix}2 & 8 & 6\\1 & 4 & 3\\2 & 8 & 6\end{bmatrix}$.
- $\begin{bmatrix}1 & 3\\1 & 2\end{bmatrix} \otimes \begin{bmatrix}2 & 4\\2 & 3\end{bmatrix} = \begin{bmatrix}1\begin{bmatrix}2 & 4\\2 & 3\end{bmatrix} & 3\begin{bmatrix}2 & 4\\2 & 3\end{bmatrix}\\1\begin{bmatrix}2 & 4\\2 & 3\end{bmatrix} & 2\begin{bmatrix}2 & 4\\2 & 3\end{bmatrix}\end{bmatrix} = \begin{bmatrix}2 & 4 & 6 & 12\\2 & 3 & 6 & 9\\2 & 4 & 4 & 8\\2 & 3 & 4 & 6\end{bmatrix}$.

Postulado 3. El resultado de la medida del observable A sobre el estado $|\psi\rangle$, sólo puede ser uno de sus autovalores. Además, si $|\psi\rangle$ es unitario y $A = \sum_i \lambda_i \pi_i$, la probabilidad de medir λ_i es

$$\mathcal{P}_{|\psi\rangle}(A : \lambda_i) = ||\pi_i|\psi\rangle||^2 = \langle\psi|\pi_i|\psi\rangle.$$

Postulado 4. Si se hace una medida sobre estado ψ del observable A filtrando respecto del autovalor λ_i, pasa a encontrarse inmediatamente después de la medida en el estado

$$\frac{\pi_i|\psi\rangle}{||\pi_i|\psi\rangle||},$$

con una probabilidad de $||\pi_i|\psi\rangle||^2$, o es destruido durante el proceso de medida.

Este último postulado es el que se conoce como colapso de la función de onda. En otras palabras, se proyecta el estado inicial al subespacio propio de A asociado al valor de la medida.

3.3. Puertas cuánticas

Definición 3.19. *El grupo unitario de grado n, denotado por* $\mathrm{U}_{\mathbb{C}}(n)$*, es el grupo de matrices unitarias* $n \times n$ *, con la multiplicación de matrices como operación del grupo.*

Observación 3.20. Una puerta cuántica actuando sobre un sistema de n qubits se puede representar con una matriz unitaria $A \in \mathrm{U}_{\mathbb{C}}(2^n)$.

Definición 3.21. *La puerta de Hadamard es una puerta que opera sobre un único qubit representada por la matriz unitaria*

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

Observación 3.22. La puerta de Hadamard tiene el siguiente efecto sobre los estados de la base:

$$\mathrm{H} : |j\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j|1\rangle).$$

De hecho, la puerta de Hadamard es una matriz de cambio de base para un sistema de un único qubit.

$$\mathrm{H}\,|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle,$$

$$\mathrm{H}\,|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} - \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

Además, esta transformación genera una combinación lineal de todos los estados de la base con la misma amplitud, dentro de un registro cuántico; lo cual será de gran importancia en los algoritmos cuánticos.

Al aplicar la puerta de Hadamard a un sistema cuántico de n qubits obtenemos lo siguiente:

$$\mathrm{H}^{\otimes n}\,|0\rangle_n = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}^{\otimes n}\begin{bmatrix}1\\0\end{bmatrix}^{\otimes n} = \frac{1}{\sqrt{2^n}}\begin{bmatrix}1\\1\end{bmatrix}^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle_n.$$

Comprobamos que obtenemos una superposición de todos los estados de la base del sistema con igual probabilidad, gracias al entrelazamiento cuántico. Este es un paso importante a la hora de inicializar qubits.

Ejemplo 3.23. Consideremos un sistema de 2 qubits. Los estados que forman la base son:

$$|0\rangle_2 = |00\rangle = \begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \qquad |1\rangle_2 = |01\rangle = \begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}.$$

$$|2\rangle_2 = |10\rangle = \begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \qquad |3\rangle_2 = |11\rangle = \begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

La matriz de Hadamard de sobre un sistema de 2 qubits:

$$\mathrm{H}^{\otimes 2} = \mathrm{H}\otimes\mathrm{H} = \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\otimes\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}.$$

Por lo tanto,

$$\mathrm{H}^{\otimes 2}\,|0\rangle_2 = \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \frac{1}{2}\sum_{j=0}^{2^2-1}|j\rangle_2.$$

Definición 3.24. *La puertas de Pauli son puertas actuando sobre un único qubit con las matrices*

$$\mathrm{X} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \qquad \mathrm{Y} = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}, \qquad \mathrm{Z} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.$$

Las matrices de Pauli afectan a los estados de la base de la siguiente manera

$$\begin{aligned} \mathrm{X} &: |j\rangle \longmapsto |1 \oplus j\rangle \\ \mathrm{Y} &: |j\rangle \longmapsto (-i)^j |1 \oplus j\rangle \\ \mathrm{Z} &: |j\rangle \longmapsto (-1)^j |j\rangle \end{aligned}$$

Las matrices de Pauli junto con la matriz identidad I forman una base del espacio vectorial de las matrices 2×2 hermíticas.

Proposición 3.25. *Sea $A \in U_{\mathbb{C}}(2)$. Entonces existen números reales α, β, γ y δ tales que*

$$A = e^{i\alpha} \begin{pmatrix} e^{-i\beta/2} & \\ & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & \\ & e^{-i\delta/2} \end{pmatrix}.$$

Definición 3.26. *Se dice que dos qubits están entrelazados cuando su estado conjunto no puede expresarse como el producto de los estados de los qubits individuales*

$$|\phi\rangle \neq |\varphi\rangle \otimes |\psi\rangle,$$

donde $|\phi\rangle$ describe el estado del sistema de dos qubits y $|\phi\rangle$, $|\psi\rangle$ describirían el estado de los qubits individualmente.

Ejemplo 3.27.

1. El estado $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ puede escribirse como producto tensorial de los estados de sus qubits individualmente:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) = 1 \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = 1 \otimes |+\rangle.$$

2. El estado $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ no puede escribirse como producto tensorial de los estados de sus qubits individualmente:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Diremos que estos dos qubits, que están en un estado $|\psi_2\rangle$, están entrelazados. Al medir uno de los qubits, el estado del otro quedará determinado. Si medimos, por ejemplo, el primer qubit obteniendo $|0\rangle$, sabemos que el segundo qubit estará en estado $|0\rangle$ también. Formalmente, si $|\psi_2\rangle$ estuviese entrelazado podría escribirse como producto $|\varphi\rangle \otimes |\psi\rangle$ tal que:

$$|\varphi\rangle \otimes |\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}.$$

En nuestro caso, $ad = bc = 0$ y $ac = bd = 1$. Si $a = 0$, entonces tendríamos $ac \neq 1$; si $d = 0$, pasaría para $bd \neq 1$, y llegaríamos a una contradicción. Por tanto, podemos afirmar que no existen $|\varphi\rangle, |\psi\rangle$ tales que $|\psi_2\rangle = |\varphi\rangle \otimes |\psi\rangle$.

Definición 3.28. *La puerta* $\mathrm{C_{NOT}}$ *es una puerta actuando sobre 2 qubits con la representación matricial:*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Esta puerta cuántica tiene el siguiente efecto sobre los estados de la base:

$$\mathrm{C_{NOT}} : |i\rangle \otimes |j\rangle \longmapsto |i\rangle \otimes |i \oplus j\rangle.$$

Esta puerta cuántica es la puerta más simple que produce entrelazamiento cuántico.

Ejemplo 3.29. Sea $|\phi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |3\rangle)$ vemos que podemos escribirlo como producto tensorial de dos estados individuales.

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |3\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$$

Aplicamos $\mathrm{C_{NOT}}$ a $|\psi\rangle$ y obtenemos

$$\mathrm{C_{NOT}}\,|\psi\rangle = \frac{1}{\sqrt{2}} C_{NOT}(|1\rangle + |3\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}((|1\rangle + |2\rangle) = \frac{1}{\sqrt{2}}((|01\rangle + |10\rangle)$$

Podemos comprobar, de la misma manera que en el ejemplo anterior, que este estado no puede expresarse como producto tensorial de estados. Al aplicar la puerta $\mathrm{C_{NOT}}$ se ha producido entrelazamiento.

Teorema 3.30. *Sea* $A \in \mathrm{U}_{\mathbb{C}}(2^n)$ *una puerta cuántica sobre n qubits. Entonces, A puede ser expresada como un número finito de productos tensoriales de puertas cuánticas que actúan sobre un único qubit* $M_i \in \mathrm{U}_{\mathbb{C}}(2)$ *y la puerta* $\mathrm{C_{NOT}}$ *sobre 2 qubits* [4, 5].

3.4. Transformada cuántica de Fourier

La Transformada de Fourier Cuánticam del inglés Quantum Fourier Transform (QFT), es esencial en la computación cuántica y fundamental para el algoritmo de Shor, [6]. Similar a la transformada de Fourier discreta, la QFT permite manipular estados cuánticos en superposición, habilitando la factorización rápida de números grandes.

Definición 3.31. *En un sistema de n qubits, definimos la transformada cuántica de Fourier,* QFT*, como el operador que tiene el siguiente efecto sobre los elementos de la base de estados,* $|j\rangle_n$*:*

$$|\tilde{j}\rangle_n = \mathrm{QFT}\,|j\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle_n$$

Observación 3.32. Cuando escribimos $\sum_{k=0}^{2^n-1}$ debemos recordar que $|k\rangle = |k_1 k_2 \dots k_n\rangle$, donde $[k_1 k_2 \dots k_n]$ es la representación binaria de k. Por tanto,

$$\sum_{k=0}^{2^n-1} \to \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1}.$$

Ejemplo 3.33. Para un sistema de un único qubit tenemos

$$\text{Base computacional} : \{|0\rangle, |1\rangle\}$$
$$\text{Base transformada de Fourier} : \{|+\rangle, |-\rangle\}.$$

Veamos como se deriva esto a partir de la definición anterior. Para un sistema de 1 qubit, $n = 1$ y $|j\rangle = \{|0\rangle, |1\rangle\}$

$$\begin{aligned} |\tilde{j}\rangle = \text{QFT}\,|j\rangle &= \frac{1}{\sqrt{2}}(e^{2\pi i j 0/2}|0\rangle + e^{2\pi i j 1/2}|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i j}|1\rangle) \end{aligned}$$

$$\begin{aligned} j = 0 : |\tilde{0}\rangle = \text{QFT}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^0|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \\ j = 1 : |\tilde{1}\rangle = \text{QFT}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \end{aligned}$$

Como hemos visto anteriormente, este operador es la puerta de Hadamard. Por tanto, la transformada de Fourier sobre un único qubit es la puerta de Hadamard.

Si ahora desarrollamos la Ec.(3.1) teniendo en cuenta que $k = \sum_{x=1}^{n} y_x 2^{n-x}$, tenemos

$$\begin{aligned} |\tilde{j}\rangle_n &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j \sum_{x=1}^{n} \frac{y_x}{2^x}} |k_1 \dots k_n\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \prod_{x=1}^{n} e^{2\pi i j \frac{y_x}{2^x}} |k_1 \dots k_n\rangle_n \\ &= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{\frac{2\pi i j}{2^1}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^2}}|1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^n}}|1\rangle\right). \end{aligned}$$

Podemos ver cómo los qubits de $|j\rangle_n = |j_1 j_2 \dots j_n\rangle_n$ en los qubits de $|k\rangle_n = |k_1 k_2 \dots k_n\rangle_n$:

$$\begin{aligned} |j_1\rangle &\to \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{\frac{2\pi i j}{2^1}}|1\rangle\right) \\ |j_2\rangle &\to \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{\frac{2\pi i j}{2^2}}|1\rangle\right) \\ &\vdots \\ |j_n\rangle &\to \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{\frac{2\pi i j}{2^n}}|1\rangle\right) \end{aligned}$$

Vemos que la transformada de Fourier depende del qubit al que está aplicándose, radicando la diferencia en la fase aplicada a $|1\rangle$.

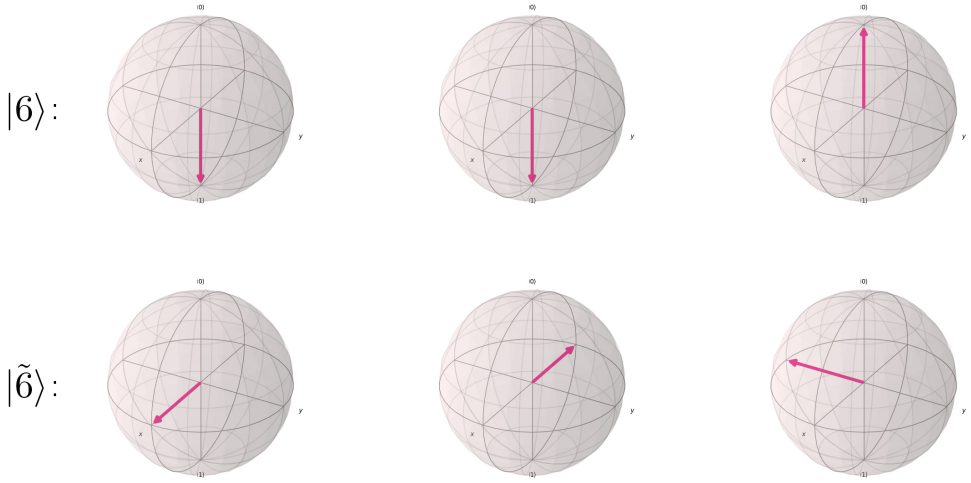

Figura 2: Representación sobre la esfera de Bloch del estado cuántico $|6\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle$, en la parte superior; y su transformada de Fourier $|\tilde{6}\rangle = |+\rangle \otimes |-\rangle \otimes |-i\rangle$, en la parte inferior.

Ejemplo 3.34. Tenemos un sistema de $n = 3$ qubits, $N = 2^3 = 8$. Calculemos la transformada de Fourier cuántica del estado $|6\rangle_3$.

$$\begin{aligned}
|\tilde{6}\rangle_3 &= \mathrm{QFT}\,|6\rangle_3 = \mathrm{QFT}\,|110\rangle_3 \\
&= \frac{1}{\sqrt{8}}\left(|0\rangle + e^{\frac{2\pi i 6}{2}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i 6}{4}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i 6}{8}}|1\rangle\right) \\
&= \frac{1}{\sqrt{8}}\left(|+\rangle \otimes |-\rangle \otimes |-i\rangle\right)
\end{aligned}$$

Definición 3.35. *Un circuito cuántico es un modelo matemático que describe la computación cuántica de un proceso, se basa en una secuencia de puertas y medidas cuánticas aplicadas a n qubits.*

La transformada de Fourier es uno de los pasos clave del algoritmo de Shor. Es importante demostrar que podemos calcularla de manera eficiente, ya que la importancia del algoritmo radica en la mejorada complejidad de implementación. Así pues, veamos como construir un circuito cuántico que aplique la transformada de Fourier. Como decíamos, cada qubit j_x pasa a estar en un estado $|0\rangle + e^{2\pi i j/2^x}|1\rangle$. Para describir este circuito, necesitaremos dos operadores:

- Hadamard gate, H. Como hemos visto en uno de los ejemplos, con esta puerta cuántica conseguimos una fase tal que $|j_x\rangle \leftarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i j_x/2}|1\rangle)$.
- Puerta de rotación, $\mathrm{CROT_x}$. Se trata de una puerta cuántica definida sobre dos qubits representada por la siguiente matriz:

$$CROT_x = \begin{bmatrix} I & 0 \\ 0 & UROT_x \end{bmatrix},$$

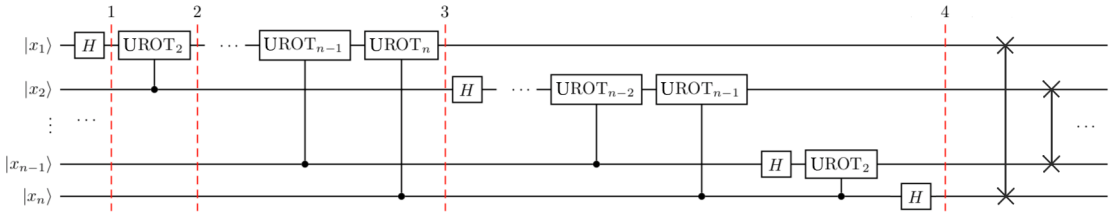

Figura 3: Representación del circuito de implementación de la QFT sobre un registro de n qubits. Fuente: [7].

donde

$$UROT_x = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^x} \end{bmatrix}.$$

Al aplicar esta puerta cuántica sobre dos qubits $|j_l j_k\rangle$, el primero actúa como el de control y sobre el segundo se aplica la fase $e^{2\pi i/2^x}$. Pongamos que $|j_k\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$

$$CROT_x|0j_k\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^x} \end{bmatrix} \begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix} = |0j_k\rangle$$

$$CROT_x|1j_k\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^x} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ a \\ be^{2\pi i/2^x} \end{bmatrix} = e^{2\pi i j_k/2^x}|1j_k\rangle$$

Entonces la implementación del circuito sería la siguiente. Comencemos con un registro de n qubits $|j_1 j_2 \dots j_n\rangle$

1. Aplicamos la puerta de Hadamard al primer qubit, obteniendo:

$$|\phi_1\rangle = H_1|j_1 j_2 \dots j_n\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2} j_1\right)|1\rangle\right] \otimes |j_2 j_3 \dots j_n\rangle$$

2. Aplicamos la puerta $UROT_2$ sobre el qubit 1 controlada por el qubit 2

$$|\phi_2\rangle = UROT_2|\phi_1\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^2} j_2 + \frac{2\pi i}{2} j_1\right)|1\rangle\right] \otimes |j_2 j_3 \dots j_n\rangle$$

3. Aplicamos sucesivamente $UROT_3, UROT_4, \dots, UROT_{n-1}, UROT_n$ sobre el primer qubit obteniendo en el último paso:

$$\begin{aligned} UROT_n|\phi_{n-1}\rangle &= \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^n} j_n + \ldots + \frac{2\pi i}{2^2} j_2 + \frac{2\pi i}{2} j_1\right)|1\rangle\right] \otimes |j_2 j_3 \dots j_n\rangle \\ &= \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^n} j\right)|1\rangle\right] \otimes |j_2 j_3 \dots j_n\rangle, \end{aligned}$$

donde hemos utilizado que $j = \sum_{y=1}^{n} 2^{n-y} j_y$.

4. Aplicamos una secuencia similar para el resto de qubits, como se muestra en la Fig.(3).

5. Por último, nótese que obtenemos el output inverso al input.

   Definición 3.36. *Sea* $|c\rangle_n$ *un registro de* n *qubits*

   $$|c\rangle_n = |c_1 c_2 \dots c_n\rangle,$$

   diremos que $|b\rangle_n$ *es el inverso de* $|c\rangle_n$

   $$|b\rangle_n = |c_n \dots c_2 c_1\rangle.$$

   Para obtener, pues, la QFT, debemoos calcular el inverso. Este último paso se representa en la Fig.(3) con las líneas verticales que comienzan y acaban en aspas, X.

Por tanto, hemos que visto podemos implementar la QFT, de manera eficiente en un número $n(n-1)/2$ de pasos.

4. Algoritmo de Deutsch

El algoritmo de Deutsch, [8], es un algoritmo cuántico que consiste en determinar si una función $f : \{0,1\} \to \{0,1\}$ es constante o balanceada. La cuestión que este algoritmo resuelve puede verse como un caso particular del problema del subgrupo oculto. Una generalización de este algoritmo para una función actuando sobre $\{0,1\}^n$ es el algoritmo de Deutsch-Jozsa [11].

Definición 4.1. *Sea G un grupo, sea $K \subseteq G$ un subgrupo de G y sea $g \in G$. Las clases laterales por la izquierda y por la derecha de K en G respecto g son las órbitas gK y Kg, respectivamente.*

Definición 4.2. *Sea G un grupo finitamente generado, sea X un conjunto finito, y sea $f : G \to X$ una función que sea constante sobre las clases laterales por la izquierda (derecha) de un cierto subgrupo $K \subseteq G$ y distinta para cada clase lateral. El problema del subgrupo oculto es el problema de determinar un conjunto generador de K, usando f como una caja negra.*

Definición 4.3. *Sea $f : \{0,1\}^n \to \{0,1\}^m$ una función, la puerta oráculo $\mathrm{O_f}$ es la transformación unitaria que actúa de la siguiente manera sobre la base:*

$$\mathrm{O_f} : |j\rangle_n \otimes |k\rangle_m \mapsto |j\rangle_n \otimes |k \oplus f(j)\rangle_m$$

4.1. Desarrollo

El objetivo de este algoritmo es determinar si dada una función $f : \{0,1\} \to \{0,1\}$ como una caja negra, esta es constante. Tenemos dos casos, o bien $f(0) = f(1)$ o bien $f(0) \neq f(1)$. En términos del problema del subgrupo oculto, $G = (\{0,1\}, \oplus)$, $X = \{0,1\}$, y K es o bien $\{0\}$ o bien $\{0,1\}$, dependiendo de f.

Clásicamente, deberíamos evaluar tanto $f(0)$ como $f(1)$ para saber si la función es o no constante. Con un ordenador cuántico, una única evaluación es suficiente. Para seguir este primer algoritmo cuántico como ejemplo, lo desarrollaremos también algebraicamente.

1 $|\psi_0\rangle_{1,1} \leftarrow |0\rangle \otimes |1\rangle$

Inicializamos dos qubits, el primero en $|0\rangle$ y el segundo en $|1\rangle$

$$|\psi_0\rangle_{1,1} = |0\rangle \otimes |1\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

2 $|\psi_1\rangle_{1,1} \leftarrow \mathrm{H}^{\otimes 2}(|\psi_0\rangle_{1,1})$

Aplicamos la puerta de Hadamard a ambos qubits, cambiándolos así de la base computacional a la base $\{|+\rangle, |-\rangle\}$

$$|\psi_1\rangle_{1,1} = \mathrm{H}^{\otimes 2}(|0\rangle \otimes |1\rangle) = \mathrm{H}(|0\rangle) \otimes \mathrm{H}(|1\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |+\rangle \otimes |-\rangle$$

$$|\psi_1\rangle_{1,1} = \mathrm{H}^{\otimes 2}(|0\rangle \otimes |1\rangle) = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

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

3 $|\psi_2\rangle_{1,1} \leftarrow \mathrm{O}_f(|\psi_1\rangle_{1,1})$

Aplicamos ahora la puerta oráculo definida al principio de la sección para la función caja negra dada $f : \{0,1\} \to \{0,1\}$.

$$\begin{aligned} |\psi_2\rangle_{1,1} &= \mathrm{O}_f(|\psi_1\rangle_{1,1}) = \mathrm{O}_f(|+\rangle \otimes |-\rangle) \\ &= \mathrm{O}_f\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |-\rangle \\ &= \frac{\mathrm{O}_f(|0\rangle \otimes |-\rangle) + \mathrm{O}_f(|1\rangle \otimes |-\rangle)}{\sqrt{2}} \\ &= \frac{(-1)^{f(0)}|0\rangle \otimes |-\rangle + (-1)^{f(1)}|1\rangle \otimes |-\rangle}{\sqrt{2}} \end{aligned}$$

Comprobemos rápidamente el último paso, tomamos por ejemplo $\mathrm{O}_f(|0\rangle \otimes |-\rangle)$ y desarrollamos:

$$\begin{aligned} \mathrm{O}_f(|0\rangle \otimes |-\rangle) &= \mathrm{O}_f\left(\frac{|0\rangle \otimes |0\rangle}{\sqrt{2}} - \frac{|0\rangle \otimes |1\rangle}{\sqrt{2}}\right) \\ &= \begin{cases} \dfrac{|0\rangle \otimes |1\rangle}{\sqrt{2}} - \dfrac{|0\rangle \otimes |0\rangle}{\sqrt{2}} = -|0\rangle \otimes |-\rangle & \text{si } f(0) = 1 \\ \dfrac{|0\rangle \otimes |0\rangle}{\sqrt{2}} - \dfrac{|0\rangle \otimes |1\rangle}{\sqrt{2}} = |0\rangle \otimes |-\rangle & \text{si } f(0) = 0 \end{cases} \end{aligned}$$

4 $|\psi_3\rangle_{1,1} \leftarrow (\mathrm{H} \otimes \mathrm{I})(|\psi_2\rangle_{1,1})$

Por último, aplicamos la puerta de Hadamard al primer qubit. Sobre el segundo qubit aplicamos la identidad, es decir, queda intacto.

$$\begin{aligned} |\psi_3\rangle_{1,1} &= (\mathrm{H} \otimes \mathrm{I})(|\psi_2\rangle_{1,1}) = (\mathrm{H} \otimes \mathrm{I})\left(\frac{(-1)^{f(0)}|0\rangle \otimes |-\rangle + (-1)^{f(1)}|1\rangle \otimes |-\rangle}{\sqrt{2}}\right) \\ &= \left(\frac{(-1)^{f(0)}\,\mathrm{H}\,|0\rangle + (-1)^{f(1)}\,\mathrm{H}\,|1\rangle}{\sqrt{2}}\right) \otimes |-\rangle = \left(\frac{(-1)^{f(0)}|+\rangle + (-1)^{f(1)}|-\rangle}{\sqrt{2}}\right) \otimes |-\rangle \\ &= \left(\frac{\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle}{2}\right) \otimes |-\rangle \\ &= (-1)^{f(0)}|f(0) \oplus f(1)\rangle \otimes |-\rangle \end{aligned}$$

Para entender el último paso debemos tener en cuenta que si $f(0) = f(1)$ entonces $(-1)^{f(0)} - (-1)^{f(1)} = 0$. Por tanto sólo la sobrevivirá el término $|0\rangle$. Lo contrario pasa cuando $f(0) \neq f(1)$, en este caso el término que no se cancela es $|1\rangle$. Fijémonos que si $f(0) = f(1)$ entonces $|f(0) \oplus f(1)\rangle = |0\rangle$, mientras que si $f(0) \neq f(1)$ entonces $|f(0) \oplus f(1)\rangle = |1\rangle$.

5 | $\tilde{\delta} \leftarrow$ Medimos el primer registro de $|\psi_3\rangle_{1,1}$

Finalmente, medimos el primer registro. Estamos pues midiendo $|f(0) \oplus f(1)\rangle$, por tanto $\tilde{\delta} \in \{0, 1\}$. Como hemos explicado antes, si obtenemos $\tilde{\delta} = 0$ entonces $f(0) = f(1)$. En cambio, si medimos $\tilde{\delta} = 1$ entonces $f(0) \neq f(1)$. En términos del problema del subgrupo oculto, si $\tilde{\delta} = 0$, tenemos que $K = \{0, 1\}$; si $\tilde{\delta} = 1$, entonces $K = \{0\}$.

Hemos visto pues que un problema que clásicamente necesita dos evaluaciones, puede ser resuelto por un algoritmo cuántico con una sola evaluación. Este fue uno de los primeros ejemplos de las ventajas que podría suponer la computación cuántica.

5. Algoritmo de Shor

El algoritmo de Shor, [9], tiene como objetivo la factorización de un número entero compuesto, $N = pq$, donde p y q son primos. Como veremos a continuación, el algoritmo se basa en un problema equivalente que trata de buscar el periodo r de la función $f_N(b) = a^b \bmod N$, donde a es un entero aleatorio coprimo con N, [10].

Previo al desarrollo del algoritmo, veamos la conexión entre encontrar el periodo de $f_N(b)$ y la factorización de N, así como las herramientas matemáticas necesarias para la total comprensión de este.

5.1. Bases de teoría de números para el algoritmo de Shor

Comencemos con la ecuación cuadrática

$$x^2 \equiv 1 \bmod N. \tag{5.1}$$

Esta ecuación tiene las soluciones triviales $x \equiv \pm 1 \bmod N$. Además, si N es un número compuesto, existen al menos dos soluciones no triviales de la ecuación, digamos $x \equiv \pm b \bmod N$. Por tanto, $(b-1)(b+1) \equiv 0 \bmod N$. Si además suponemos que $b \pm 1 \not\equiv 0 \bmod N$, tenemos que N divide $(b-1)(b+1)$, pero N no divide $(b \pm 1)$. Así pues, el máximo común divisor, gcd, entre N y $(b \pm 1)$ es un factor no trivial de N. El máximo común divisor puede calcularse con el algoritmo de Euclides de manera eficiente, [12].

En resumen, si encontramos x tal que $x^2 \equiv 1 \bmod N$ y $x \not\equiv \pm 1 \bmod N$, podemos encontrar un factor no trivial de N. Sea $a < N$, a coprimo con N, nos proponemos encontrar el periodo r de $a \bmod N$. Recordemos que el orden de $a \bmod N$, siendo el $\gcd(a, N)=1$ se define como:

$$O_N = \min\{r \in \mathbb{Z}_{>0} : a^r \equiv 1 \mathrm{mod} N\}.$$

Este orden r es a su vez el periodo de la función f_N. Si r es par y ponemos

$$x \equiv a^{r/2},$$

entonces x cumple $x^2 \equiv 1 \bmod N$ y $x \not\equiv \pm 1 \bmod N$, lo que nos permitirá encontrar un factor no trivial de N. Es así como encontramos la relación entre la factorización de N y el periodo de f_N.

Para que la factorización de N sea efectiva, es necesario que ni r ser impar ni $a^{r/2}$ sea una solución trivial de la Ec.(5.1). Sin embargo, la probabilidad de que esto pase es adecuadamente pequeña conforme indica el siguiente teorema.

Teorema 5.1. *Sea $N \in \mathbb{Z}_{\geq 0}$ impar cuya factorización en producto de primos es*

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Sea a un entero aleatorio tal que $1 < a < N$ y $\gcd(a, N) = 1$; y sea $r = O_N(a)$. Entonces:

$$\mathrm{Prob}\left[(2 \mid r) \wedge \left(a^{r/2} \not\equiv \pm 1 \mathrm{mod} N\right)\right] \geq 1 - \frac{1}{2^{k-1}}.$$

Demostración. Véase [13], Apéndice B. □

Este teorema puede particularizarse fácilmente para los casos en los que N no es de la forma p^α, $2p^\alpha$. De manera que

$$\text{Prob}\left[(2 \mid r) \wedge \left(a^{r/2} \not\equiv \pm 1 \text{mod} N\right)\right] \geq \frac{1}{2}.$$

Los casos en los que $N = p^\alpha$ pueden ser reconocidos por un algoritmo clásico probabilístico de manera efectiva.

Por último, la probabilidad de que $\gcd(a, N) = 1$ tomando a aleatorio tal que $1 \leq a \leq N$ es mayor que $1/\log N$. Recapitulando, para $N = pq$ donde p, q son primos, si conseguimos calcular el orden r de a aleatorio, obtendremos un factor no trivial de N con probabilidad mayor a $1/(2\log N)$.

5.2. Exponenciación binaria

Sea a un número entero, podemos calcular a^N, N siendo un entero no negativo, mediante el algoritmo de exponenciación binaria. Este algoritmo es clave para la eficiencia de algunos procesos en los que se calculan grandes potencias de números.

Sea a la base, a^N la potencia que queremos calcular, el algoritmo puede expresarse recursivamente de la siguiente manera:

$$a^N = \begin{cases} 1 & \text{si } N = 0 \\ a \cdot a^{N-1} & \text{si } N \text{ es impar} \\ \left(a^{N/2}\right)^2 & \text{si } N \text{ es par.} \end{cases}$$

Con un total de $O(\log N)$ operaciones, asumiendo que la multiplicación de dos números de $\log N$ bits toma $O((\log N)^2)$ de tiempo, podemos concluir que la complejidad total de esta transformación es del orden de $O((\log N)^3)$.

Ejemplos 5.2.

- Queremos calcular a^N, donde $N = 16 = 2^4$. Comenzamos calculando a^2 y elevamos al cuadrado hasta obtener la potencia deseada

$$a^2 \to a^4 \to a^8 \to a^{16}$$

- Queremos calcular a^N, donde $N = 17$. Escribiendo N en base 2 tenemos $N = 2^4 + 2^0$. Como N es impar, calculamos $a^{17} = a \cdot a^{16}$, donde a^{16} es la potencia calculada en el ejemplo anterior.

5.3. Fracciones continuas

Definición 5.3. *Una fracción continua simple es una expresión de la forma*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{\ddots}}}}$$

donde $a_0 \in \mathbb{Z}_{\geq 0}$ *y* $a_i \in \mathbb{Z}_{>0}$.

Notación 5.4. *Escribimos*

$$[a_0; a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}.$$

si el número de términos es finito, y

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{\ddots}}}}.$$

si el número de términos es infinito.

Proposición 5.5. *Cualquier número real puede representarse con una fracción continua.*

En particular, cualquier número racional puede representarse con una fracción continua finita. La demostración de este enunciado puede encontrarse en [14], Proposición 1. De hecho, asumiendo $a_n = 1$, esta representación es única. Dado $q \in \mathbb{Q}_{>0}$, podemos calcular los componentes de su fracción continua de la siguiente manera:

$$\begin{aligned} a_0 &\leftarrow \lfloor q \rfloor \\ q_0 &\leftarrow q - a_0 \\ a_{k+1} &\leftarrow \lfloor 1/q_k \rfloor \\ q_{k+1} &\leftarrow 1/q_k - a_{k+1} \end{aligned}$$

Ejemplo 5.6. Queremos desarrollar la fracción continua del racional 415/93, con ayuda del algoritmo anterior.

$$\begin{aligned} a_0 &\leftarrow \lfloor \frac{415}{93} \rfloor = 4 & q_0 &\leftarrow \frac{415}{93} - 4 \\ a_1 &\leftarrow \lfloor \frac{1}{\frac{415}{93} - 4} \rfloor = 2 & q_1 &\leftarrow \frac{1}{\frac{415}{93} - 4} - 2 \\ a_2 &\leftarrow \lfloor \frac{1}{\frac{1}{\frac{415}{93} - 4} - 2} \rfloor = 6 & q_2 &\leftarrow \frac{1}{\frac{1}{\frac{415}{93} - 4} - 2} - 6 \\ a_3 &\leftarrow \lfloor \frac{1}{\frac{1}{\frac{1}{\frac{415}{93} - 4} - 2} - 6} \rfloor = 7 \end{aligned}$$

Así pues, obtenemos

$$\frac{415}{93} = 4 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{7}}}.$$

Definición 5.7. *Sea $\alpha = [a_0; a_1, a_2, \ldots]$, la convergente k de α es el número racional resultante al truncar la fracción continua de α en la posición k, $\alpha_k = [a_0; a_1, a_2, \ldots, a_k]$.*

Podemos escribir la convergente k de α como

$$\alpha_k = \frac{p_k}{q_k},$$

de forma reducida donde p_k, q_k son números enteros y $q_k > 0$.

Proposición 5.8. *El numerador p_k y el denominador q_k de la convergente k de $\alpha = [a_0; a_1, a_2, \ldots]$ pueden calcularse mediante las siguientes relaciones de recurrencia:*

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_1 a_0 + 1, & q_1 &= a_1, \end{aligned}$$

para $k \geq 2$

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2}, \\ q_k &= a_k q_{k-1} + q_{k-2}. \end{aligned}$$

La demostración de esta proposición se puede encontrar en [14], Teorema 2.

Ejemplo 5.9. Sea $\frac{668}{261} = [0; 2, 1, 1, 3, 1, 2, 2, 4]$. Buscamos su convergente 3, con ayuda del algoritmo anterior.

$$\begin{aligned} p_0 &= 0, & q_0 &= 1, \\ p_1 &= 1, & q_1 &= 2, \\ p_2 &= 1, & q_2 &= 3, \\ p_3 &= 2, & q_3 &= 5. \end{aligned}$$

Por tanto, la convergente 3 de $\frac{668}{261}$ es $\alpha_3 = \frac{2}{5}$.

Teorema 5.10. *Sea β un número real arbitrario. Si el número racional $\frac{a}{b}$, donde $b > 1$ y gcd(a,b)=1, satisface*

$$\left|\beta - \frac{a}{b}\right| < \frac{1}{2b^2},$$

entonces, $\frac{a}{b}$ es una de las convergentes $\frac{p_k}{q_k}$ de la fracción continua de β.

Demostración. Véase [15], Teorema 2.5.2. □

5.4. Parte clásica

Sea $N \in \mathbb{Z}_{\geq 0}$, el algoritmo de Shor aplica los siguientes pasos para la factorización de N.

𝟙

$a \leftarrow$ entero aleatorio $1 < a < N$
$d \leftarrow \gcd(x, N)$

Tomamos un entero aleatorio a tal que $1 < a < N$. Utilizamos el algoritmo de Euclides para encontrar el máximo común divisor d entre a y N, [12]. La complejidad computacional de este paso es del orden de $O((\log N)^3)$. Si por casualidad $d > 1$, entonces d ya sería un factor de N.

2 | $r \leftarrow O_N(a)$

Calculamos el orden de dicho a. Esta parte la desarrollaremos con ayuda de un algoritmo cuántico, que explicaremos en el siguiente apartado. En este punto se encuentra la gran diferencia entre los algoritmos clásicos y los cuánticos. Determinar el orden de un elemento a mod N es un problema difícil de resolver clásicamente, el mejor algoritmo clásico es de una complejidad computacional super-polinomial.

3 | Comprobar que r es par.

Si este paso falla, deberíamos volver al primer paso y escoger otro número aleatorio a tal que $1 < a < N$.

4 | Comprobar que $a^{r/2} \pm 1 \not\equiv 0 \mod N$

Sea $x = a^{r/2} \mod N$. Comprobemos que $x \pm 1 \not\equiv 0 \mod N$. Si esta condición se cumple, $\gcd(x+1, N)$, $\gcd(x-1, N)$ son divisores no triviales de N.

Si este paso falla, deberíamos volver al primer paso y escoger otro número aleatorio a tal que $1 < a < N$.

5 | $d_1 \leftarrow \gcd(a^{r/2}+1, N)$
$d_2 \leftarrow \gcd(a^{r/2}-1, N)$

Utilizamos el algoritmo de Euclides para calcular el máximo común divisor, d_1=gcd($a^{r/2}+1, N$), d_2=gcd($a^{r/2}-1, N$). Podemos concluir que d_1, d_2 son factores no triviales de N, cumpliendo entonces con el objetivo del algoritmo.

$$a^2 - 1 \equiv (a^{r/2}+1)(a^{r/2}-1) \equiv 0 \mod N$$

Ejemplo 5.11. Veamos la implementación del algoritmo de Shor sobre $N = 21$. Escogemos $a = 5$, que es coprimo con 21, gcd(5, 21)=1. En el segundo paso, debemos calcular el orden de 5 mod21. En este caso, podemos desarrollarlo manualmente sin necesidad del algoritmo cuántico.

z	1	2	3	4	5	6
$5^z \mod 21$	5	4	20	16	17	1

Por tanto, el orden de 5 mod 21 es $r = 6$, que es par. En el paso 4, vemos que $5^{r/2}+1 \equiv 0 \mod N$, por lo tanto debemos volver a empezar y escoger otro a.

Sea ahora $a = 19$, que es coprimo con 21, gcd(19, 21)=1.

z	1	2	3	4	5	6
$19^z \mod 21$	19	4	13	16	10	1

Por tanto, el orden de 19 mod 21 es $r = 6$, que es par. En este caso, se cumple que $x \pm 1 = 19^{r/2} \pm 1 = 13 \pm 1 \not\equiv 0 \mod N$. Podemos pasar al último paso del algoritmo y concluir que al menos uno de los factores de $N = 21$ está contenido en $\gcd(21, x \pm 1)$. En este caso, encontramos ambos factores en este paso

$$\begin{cases} \gcd(21,14) = 7 \\ \gcd(21,12) = 3 \end{cases}$$
$$\rightarrow N = 3 \cdot 7.$$

La limitación de los ordenadores clásicos reside en el cálculo del orden de a mod N. Para ello, el algoritmo de Shor incluye una parte cuántica.

5.5. Parte cuántica

Sean N, a dos enteros positivos tal que $1 < a < N$, el objetivo de esta parte del algoritmo de Shor es encontrar el orden de a mod N. Este problema es equivalente a encontrar el periodo de la función:

$$\begin{aligned} f_N : \mathbb{Z}_{>0} &\longrightarrow \mathbb{Z}_{>0} \\ y &\longmapsto a^y \bmod N. \end{aligned}$$

𝟙 $|\psi_0\rangle_{t,n} \leftarrow |0\rangle_t \otimes |0\rangle_n$

Inicializamos dos registros de longitud t y n respectivamente donde $n = \lceil \log_2 N \rceil$ y $t = 2n$, con todos los qubits inicializados a 0.

𝟚 $|\psi_1\rangle_{t,n} \leftarrow (\mathrm{H}^{\otimes t} \otimes \mathrm{I}^{\otimes n})|\psi_0\rangle_{t,n}$

Al aplicar la puerta de Hadamard, el primer registro pasa a ser una superposición de todos los estados de la base computacional, con igual probabilidad. La amplitud de estos estados viene dada por $1/\sqrt{2^t}$

$$|\psi_1\rangle_{t,n} = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_t \otimes |0\rangle_n.$$

𝟛 $|\psi_2\rangle_{t,n} \leftarrow \mathrm{M}_{a,N}\,|\psi_1\rangle_{t,n}$

Sean n, t, x, y N definidas como en el contexto de este algoritmo, la puerta de exponenciación modular es el operador unitario que actúa de la siguiente manera sobre los estados de la base:

$$\mathrm{M}_{a,N} : |j\rangle_t \otimes |k\rangle_n \rightarrow |j\rangle_t \otimes |k + a^j \bmod N\rangle_n$$

Esta transformación se lleva acabo en $O((\log N)^3)$ pasos, calculándola con ayuda del algoritmo de exponenciación binaria, [12].

$$\begin{aligned} |\psi_2\rangle_{t,n} &= \mathrm{M}_{a,N}(|\psi_1\rangle_{t,n}) \\ &= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \mathrm{M}_{a,N}(|j\rangle_t \otimes |0\rangle_n) \\ &= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle_t \otimes |a^j \mathrm{mod} N\rangle_n. \end{aligned}$$

Supondremos que r es potencia de 2, es decir r divide 2^t, para desarrollar el algoritmo de una manera más clara y sencilla. El caso en que r no divide 2^t se desarrolla en la sección 5.5.1.

$$|\psi_2\rangle_{t,n} = \frac{1}{\sqrt{2^t}} \sum_{b=0}^{r-1} \left[\left(\sum_{x=0}^{\frac{2^t}{r}-1} |xr+b\rangle_t \right) \otimes |a^b \mathrm{mod} N\rangle_n \right]$$

4 | $\tilde{\delta} \leftarrow$ Medimos el segundo registro.
$|\psi_3\rangle_t \leftarrow |\psi_2\rangle_{t,n}$ Una vez medido el segundo registro.

Nótese que al medir el segundo registro, efectivamente estamos limitando el primer registro a ser de la forma $b, b+r, b+2r, \ldots, b+(\frac{2^t}{r}-1)r$. Por tanto, sea $\tilde{\delta} = a^{b_0} \bmod N$, donde $b_0 \in \{0, \ldots, r-1\}$, la medida obtenida; el estado después de la medida es:

$$|\psi_3\rangle_t = \sqrt{\frac{r}{2^t}} \sum_{x=0}^{\frac{2^t}{r}-1} |xr+b_0\rangle_t.$$

5 | $|\psi_4\rangle_t \leftarrow \mathrm{QFT}_t(|\psi_3\rangle_t)$.

Recordemos que la transformada cuántica de Fourier, sobre un estado de n qubits $|j\rangle_n$, se define como:

$$\mathrm{QFT}\,|k\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2\pi i jk/2^n} |k\rangle_n.$$

Para encontrar pues el periodo r, utilizaremos la transformada cuántica de Fourier sobre t qubits, QFT_t, aplicada al primer registro.

$$\begin{aligned}
|\psi_4\rangle_t = \mathrm{QFT}_t(|\psi_3\rangle_t) &= \sqrt{\frac{r}{2^t}} \sum_{x=0}^{\frac{2^t}{r}-1} \mathrm{QFT}_t\,|xr+b_0\rangle_t \\
&= \sqrt{\frac{r}{2^t}} \sum_{x=0}^{\frac{2^t}{r}-1} \left(\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{-2\pi i(xr+b_0)j/2^t} |j\rangle_t \right) \\
&= \frac{1}{\sqrt{r}} \left(\sum_{j=0}^{2^t-1} \left[\frac{r}{2^t} \sum_{x=0}^{\frac{2^t}{r}-1} e^{\frac{-2\pi i x j}{2^t/r}} \right] e^{-2\pi i b_0 j/2^t} |j\rangle_t \right).
\end{aligned}$$

Para simplificar este resultado, recordemos la siguiente propiedad:

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{-2\pi i kj/N} = \begin{cases} 1 \text{ si } N \mid j \\ 0 \text{ si no.} \end{cases} \tag{5.2}$$

En nuestro caso, $N = 2^t/r$. Por lo tanto, solo sobreviven los términos del primer sumatorio tal que k es divisible por $2^t/r$; es decir, términos de la forma $k\frac{2^t}{r}$. De esta manera, tenemos:

$$|\psi_4\rangle_t = \frac{1}{\sqrt{r}} \left(\sum_{k=0}^{r-1} e^{-2\pi i \frac{k}{r} b_0} |k\frac{2^t}{r}\rangle_t \right). \tag{5.3}$$

Como hemos visto en la sección 3.4, puede calcularse con un número $t(t-1)/2$ de operaciones elementales. Esta implementación crece cuadráticamente con la longitud del input, t. Podemos afirmar que es un cálculo eficiente, con una complejidad $O((\log N))^2)$.

6 | $\tilde{\omega} \leftarrow$ Medimos $|\psi_4\rangle_t$.

Por último, medimos el registro, obteniendo un $k_0 \in \{0, \ldots, r-1\}$ equiprobablemente (en el caso en que r sea múltiplo de 2):

$$\tilde{\omega} = k_0 \frac{2^t}{r}$$

Si obtenemos $\tilde{\omega} = 0$, tendremos que repetir el proceso desde el principio. En caso de que $\tilde{\omega} \neq 0$, sabemos $\frac{\tilde{\omega}}{2^t}$ y que esto será equivalente a la fracción reducida de $\frac{k_0}{r}$. Si llamamos c al denominador de esta fracción reducida, podemos comprobar $a^c \bmod N$. Si $a^c \not\equiv 1 \bmod N$, entonces c es un factor de r. En este caso, podemos repetir la parte cuántica del algoritmo de Shor, intentando esta vez encontrar el orden de a^c. Repitiendo este proceso un número finito de veces deberíamos encontrar r. Si, por el contrario, $a^c \equiv 1 \bmod N$, habremos encontrado el orden r de a y podemos continuar con la parte clásica del algoritmo.

5.5.1. Parte cuántica generalizada

Retomemos ahora desde el tercer paso de la parte cuántica del algoritmo de Shor, sin suponer ahora que r es una potencia de 2. Es decir, la periodicidad es imperfecta. En el dominio $D = \{0, 1, \ldots, 2^t - 1\}$ tenemos un número finito de periodos completos cuando r es una potencia de 2, ya que $2^t/r = M$, $M \in \mathbb{Z}$. Sin embargo, cuando r no es una potencia de dos, un periodo queda incompleto y podríamos expresar 2^t como $2^t = M'r + s$, con $1 \leq s < r$. La diferencia entre este caso y el anterior radica en la probabilidad de medir un estado tras aplicar la QFT. En el caso de que r sea una potencia de 2 vemos que por la propiedad de la Ec.(5.2), obtenemos una superposición de estados equiprobables. En cambio, si no aplicamos esta propiedad, no obtenemos la equiprobabilidad de estados $|k\frac{2^t}{r}\rangle$ y por lo tanto debemos obtener el periodo r de diferente manera. Volviendo a la parte cuántica del algoritmo de Shor, tras la primera medida tenemos el estado:

$$|\psi_3\rangle_t = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |jr + l\rangle_t,$$

donde se ha definido A tal que

$$A = \begin{cases} M' + 1 = \lfloor \frac{2^t}{r} \rfloor + 1 & \text{si } l < s \\ M' = \lfloor \frac{2^t}{r} \rfloor & \text{si } l \geq s. \end{cases}$$

4 | $|\psi_4\rangle_t \leftarrow \mathrm{QFT}_t(|\psi_3\rangle_t)$.

$$|\psi_4\rangle_t = \mathrm{QFT}_t\,|\psi_3\rangle_t = \frac{1}{\sqrt{A}}\sum_{x=0}^{A-1}\mathrm{QFT_t}\,|xr+l\rangle_t$$
$$= \sum_{j=0}^{2^t-1}\frac{1}{\sqrt{2^t}\sqrt{A}}\sum_{x=0}^{A-1}e^{2\pi i(xr+l)j/2^t}|j\rangle_t \tag{5.4}$$

Cada uno de estos estados tiene una amplitud

$$|\alpha_j| = \frac{1}{\sqrt{2^t}\sqrt{A}}\left|\sum_{x=0}^{A-1}e^{2\pi i(xr+l)j/2^t}\right|$$

Por tanto ahora la probabilidad de medir un estado k es:

$$\mathrm{Prob}(j) = \frac{1}{A2^t}\left|\sum_{x=0}^{A-1}e^{2\pi i(xr+l)j/2^t}\right|^2$$

En primer lugar vemos que la siguiente suma involucrada en el cálculo de la QFT, es una serie geométrica de razón $z = 2\pi ijr/2^t$

$$s_j = \sum_{x=0}^{A-1}e^{2\pi ixrj/2^t} \tag{5.5}$$

El resultado de sumar esta serie es

$$s_j = \begin{cases}\dfrac{1-z^A}{1-z} & \text{si } z \neq 1\\ A & \text{si } z = 1.\end{cases}$$

En el caso anterior, vemos que hay interferencia constructiva para exactamente $rj \equiv 0 \mod 2^t$, es decir r divide 2^t, $2^t/r = A$. En particular para los múltiplos $j\frac{2^t}{r}$, $z = 1$; para $z \neq 1$, obteníamos una suma de raíces A-ésimas que acababan sumando 0. Cada uno de los estados $k\frac{2^t}{r}$ aparecía con probabilidad $1/r$, mientras que los demás estados, tenían una probabilidad 0 de ser medidos.

En el caso en que r no divide 2^t, generalmente z no es una raíz A-ésima de la unidad, y la probabilidad de un estado de ser medido no es exactamente cero para muchos términos. Para poder estudiar este caso, buscamos demostrar que al medir un estado después de aplicar QFT, obtendremos un entero M cercano a un múltiplo de $2^t/r$ con una probabilidad apropiadamente alta.

Consideremos ahora los r múltiplos de $2^t/r$:

$$0, \frac{2^t}{r}, 2\frac{2^t}{r}, \ldots, (r-1)\frac{2^t}{r}$$

Estos múltiplos generalmente no son enteros, pero cada uno de ellos está como mucho a $1/2$ de un entero j. Fijémonos que $k\frac{2^t}{r}$ no puede estar nunca a exactamente a la mitad entre dos enteros ya que $r < N$ y $2^t > N^2$. Así pues, consideramos los j tal que:

$$\left|j - k\frac{2^t}{r}\right| < \frac{1}{2} \tag{5.6}$$

A partir de esta desigualdad, con el desarrollo en fracciones continuas, podremos encontrar r.

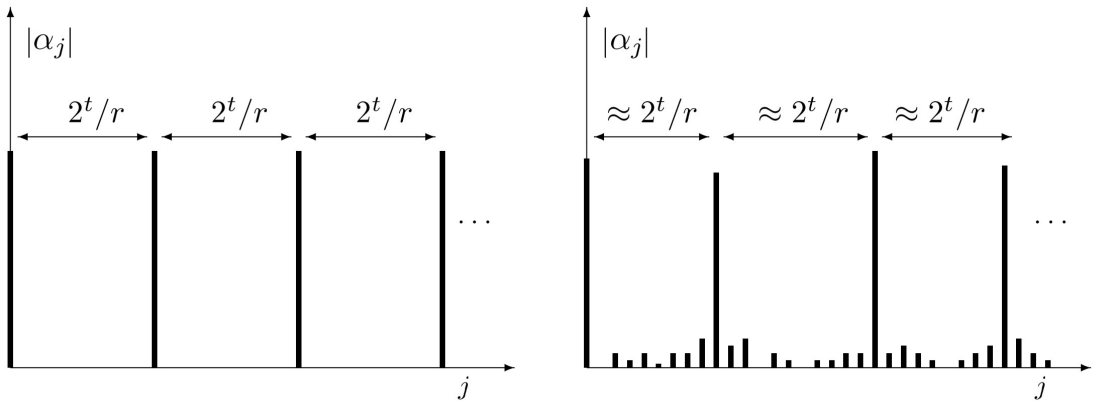

Figura 4: Representación de las amplitudes de los estados después de aplicar QFT, $\mathrm{QFT}\,|j\rangle$. En la izquierda se representa el caso de periodicidad exacta; en la derecha, el de periodicidad imperfecta. Fuente: [16].

Teorema 5.12. *Digamos que medimos el estado después de aplicar la* QFT*, Ec.(5.4). Sea j un entero tal que*

$$\left| j - k\frac{2^t}{r} \right| < \frac{1}{2}.$$

Entonces, mediremos j con probabilidad

$$Prob(j) > \gamma/r,$$

donde $\gamma \approx 4/\pi^2$.

Esto nos dice que la QFT, seguida de una medida, nos da una alta probabilidad de obtener un valor cercano a un múltiplo de $2^t/r$. Veamos de donde viene este resultado.

Demostración. En primer lugar, tenemos que para cualquier j

$$\mathrm{Prob}(j) = |\alpha_j|^2 = \frac{1}{A2^t} \left| \frac{1 - z^A}{1 - z} \right|^2,$$

con $z = e^{2\pi i j r/2^t} = e^{2\pi i (jr \bmod 2^t)/2^t}$. Por otro lado, podemos reescribir la Ec.(5.6) como:

$$-\frac{r}{2} < jr \bmod 2^t < \frac{r}{2}$$

Si escribimos ahora $\theta_j = 2\pi(jr \bmod 2^t)/2^t$, tenemos que $|\theta_j| < \pi r/2^t$. Además, $A < 2^t/r + 1$. Por tanto,

$$|A\theta_j| < \frac{\pi r}{2^t} A < \pi(1 + \frac{r}{2^t})$$

Llamemos $\pi(1 + \frac{r}{2^t}) = A\theta_{max}$. Tenemos que para todo j,

$$0 \leq |A\theta_j/2| < A\theta_{max}/2 < \pi. \tag{5.7}$$

Por otro lado,

$$\begin{aligned} \left| \frac{1 - e^{iA\theta_j}}{1 - e^{i\theta_j}} \right|^2 &= \left| \frac{1 - e^{-iA\theta_j}}{1 - e^{-i\theta_j}} \right| \left| \frac{1 - e^{iA\theta_j}}{1 - e^{i\theta_j}} \right| = \left| \frac{2 - 2\cos A\theta_j}{2 - 2\cos\theta_j} \right|^2 \\ &= \left(\frac{\sin A\theta_j/2}{\sin\theta_j/2} \right)^2 \end{aligned}$$

Entonces,

$$\begin{aligned}\text{Prob}(j) &= \frac{1}{A2^t}\left(\frac{\sin A\theta_j/2}{\sin\theta_j/2}\right)^2 \\ &> \frac{1}{A2^t}\left(\frac{\sin A\theta_j/2}{\theta_j/2}\right)^2,\end{aligned}$$

donde hemos usado que $\sin x < x$ para $x \in (0, \pi)$.

$$\begin{aligned}\text{Prob}(j) &> \frac{A}{2^t}\left(\frac{\sin A\theta_j/2}{A\theta_j/2}\right)^2 \\ &> \frac{A}{2^t}\left(\frac{\sin A\theta_{max}/2}{A\theta_{max}/2}\right)^2,\end{aligned}$$

donde hemos utilizado Ec.(5.7) para deducir la útlima desigualdad.

Tenemos, además, que $A > 2^t/r - 1$. Así es que $A/2^t > \frac{1}{r} - \frac{1}{2^t}$. Con todo esto,

$$\text{Prob}(j) > \left(\frac{1}{r} - \frac{1}{2^t}\right)\left(\frac{\sin A\theta_{max}/2}{A\theta_{max}/2}\right)^2 = \frac{1}{r}\left(1 - \frac{r}{2^t}\right)\left(\frac{\sin A\theta_{max}/2}{A\theta_{max}/2}\right)^2 > \frac{\gamma}{2}, \qquad (5.8)$$

para γ constante.

Veamos ahora que $4/(\pi^2 r)$ es una cota inferior de γ. Si consideramos el caso en que N es muy grande, podemos ignorar los términos $r/2^t < 1/N$. Entonces, $A\theta_{max}/2 = \frac{\pi}{2}(1 + r/2^t) \approx \pi/2$. Por tanto, la Ec.(5.8) para N grande queda:

$$\text{Prob}(j) > \frac{4}{\pi^2 r}.$$

□

De acuerdo con el anterior razonamiento, para cada valor de $k = 0, \ldots, r-1$, obtendremos un valor de j con una probabilidad mayor a γ/r. Nos interesan especialmente los casos en los que k es coprimo con r. Existen $O(r/\log\log r)$ de estos casos. Por tanto, la probabilidad de encontrar j válido para nuestros cálculos es $O(1/\log\log r) > O(1/\log\log N)$; y con $O(\log\log N)$ repeticiones podemos encontrar un valor de j con una probabilidad constante específica.

5 | $\tilde{\omega} \leftarrow$ Medimos $|\psi_4\rangle_t$.

Una vez medimos, utilizamos las fracciones continuas para recuperar el periodo. La Ec.(5.6), es equivalente a:

$$|rj - k2^t| \leq r/2, \qquad (5.9)$$

para algún $0 \leq k \leq r-1$. Por tanto, por Teorema 5.12 tenemos que

$$\text{Prob}(j) > \frac{4}{\pi^2}\frac{1}{r}$$

La Ec.(5.9) que puede ser reescrita como:

$$\left|\frac{j}{2^t} - \frac{k}{r}\right| \leq \frac{1}{2 \cdot 2^t}.$$

Tengamos en cuenta ahora, que en al comenzar el algoritmo de Shor hemos escogido la longitud de los qubits t tal que $2^t > N^2$, por tanto podemos reescribir la última desigualdad en términos de N. Además, tenemos que $r \leq N$, por tanto:

$$\left| \frac{j}{2^t} - \frac{k}{r} \right| \leq \frac{1}{2 \cdot r^2}.$$

Así pues, por el Teorema 5.10 podemos afirmar que $\frac{k}{r}$ es una de las convergentes $\frac{p_k}{q_k}$ de la expansión en fracciones continuas de $\frac{j}{2^t}$, que conocemos. Para encontrar el periodo calculamos las convergentes de $\frac{k}{r}$ según se ha explicado en la Proposición 5.8. En algún momento de este cálculo de las convergentes, encontraremos un denominador mayor que N. Teniendo en cuenta que $r \leq N$, tomamos la convergente directamente anterior, el denominador de la cual es probablemente r. Esta convergente estará en su forma más reducida, por lo que es posible que haya habido cancelación entre numerador y denominador. Si una vez obtenido ese denominador, digamos c, comprobamos que $a^c \not\equiv 1 \mod N$, podemos comprobar si $2c$ o $3c$ son r, lo cual no toma demasiado tiempo.

Ejemplo 5.13. Queremos utilizar el algoritmo de Shor para encontrar los factores de $N = 209$. Para empezar, tomamos a tal que $1 < a < 209$. Por ejemplo, $a = 12$, que satisface la condición gcd(209,12)=1. Inicializamos nuestro sistema, preparando $n = \lceil \log_2 209 \rceil = 8$ y $t = 2n = 16$ qubits tal que:

$$|\psi_0\rangle_{16,8} \leftarrow |0\rangle_{16} \otimes |0\rangle_8$$

Aplicamos entonces al primer registro la puerta de Hadamard, obteniendo una superposición de estados equiprobables:

$$|\psi_1\rangle_{16,8} \leftarrow (\mathrm{H}^{\otimes 16} \otimes \mathrm{I}^{\otimes 8}) \left(|0\rangle_{16} \otimes |0\rangle_8\right)$$

$$|\psi_1\rangle_{16,8} = \frac{1}{\sqrt{2^{16}}} \sum_{j=0}^{2^{16}-1} |j\rangle_{16} \otimes |0\rangle_8$$

Después aplicamos la puerta modular, obteniendo así las potencias de 12 mod 209 en el segundo registro

$$|\psi_2\rangle_{16,8} \leftarrow \mathrm{M}_{12,209} \left(|\psi_1\rangle_{16}\right)$$

$$|\psi_2\rangle_{16,8} = \frac{1}{\sqrt{2^{16}}} \sum_{j=0}^{2^{16}-1} \mathrm{M}_{12,209} \, |j\rangle_{16} \otimes |0\rangle_8 = \frac{1}{\sqrt{2^{16}}} \sum_{j=0}^{2^{16}-1} |j\rangle_{16} \otimes |12^j \bmod 209\rangle_8$$

$$\begin{aligned} |\psi_2\rangle_{16,8} = \frac{1}{\sqrt{2^{16}}} \Big(& |0\rangle|1\rangle + |1\rangle|12\rangle + |2\rangle|144\rangle + |3\rangle|56\rangle + |4\rangle|45\rangle + |5\rangle|122\rangle + \\ & |6\rangle|1\rangle + |7\rangle|12\rangle + |8\rangle|144\rangle + |9\rangle|56\rangle + |10\rangle|45\rangle + |11\rangle|122\rangle + \\ & |12\rangle|1\rangle + |13\rangle|12\rangle + |14\rangle|144\rangle + |15\rangle|56\rangle + |16\rangle|45\rangle + |17\rangle|122\rangle + \ldots \Big) \end{aligned}$$

$$|\psi_2\rangle_{16,8} = \frac{1}{\sqrt{2^{16}}}\Big[\Big(|0\rangle + |6\rangle + |12\rangle + |18\rangle + \dots\Big) \otimes |1\rangle$$
$$\Big(|1\rangle + |7\rangle + |13\rangle + |19\rangle + \dots\Big) \otimes |12\rangle$$
$$\Big(|2\rangle + |8\rangle + |14\rangle + |20\rangle + \dots\Big) \otimes |144\rangle$$
$$\Big(|3\rangle + |9\rangle + |15\rangle + |21\rangle + \dots\Big) \otimes |56\rangle$$
$$\Big(|4\rangle + |10\rangle + |16\rangle + |22\rangle + \dots\Big) \otimes |45\rangle$$
$$\Big(|5\rangle + |11\rangle + |17\rangle + |23\rangle + \dots\Big) \otimes |122\rangle\Big]$$

$\tilde{\delta} \leftarrow$ Medimos el segundo registro.
$|\psi_3\rangle_{16} \leftarrow |\psi_2\rangle_{16,8}$ Una vez medido el segundo registro.

Medimos el segundo registro obteniendo $\tilde{\delta} \in \{1, 12, 144, 56, 45, 122\}$. Pongamos que medimos $\tilde{\delta} = 122$. Por tanto, el estado después de la medida es:

$$|\psi_3\rangle_{16} = \frac{1}{\sqrt{10923}}\Big[|5\rangle + |11\rangle + |17\rangle + |23\rangle + \dots\Big] = \frac{1}{\sqrt{10923}}\sum_{x=0}^{10922}|xr+5\rangle$$

$|\psi_4\rangle_{16} \leftarrow \mathrm{QFT}_{16}(|\psi_3\rangle_{16})$.

$$\begin{aligned}|\psi_4\rangle_{16} = \mathrm{QFT}_{16}(|\psi_3\rangle_{16}) &= \frac{1}{\sqrt{10923}}\sum_{x=0}^{10922}\mathrm{QFT}_{16}\,|xr+5\rangle_{16} \\ &= \frac{1}{\sqrt{10923}}\sum_{x=0}^{10922}\left(\frac{1}{\sqrt{2^{16}}}\sum_{j=0}^{2^{16}-1}e^{2\pi i(xr+5)j/2^{16}}|j\rangle_{16}\right) \\ &= \frac{1}{\sqrt{2^{16}}}\sum_{j=0}^{2^{16}-1}\left(\left[\frac{1}{\sqrt{10923}}\sum_{x=0}^{10922}e^{2\pi i\frac{6xj}{2^{16}}}\right]e^{2\pi i\frac{5j}{2^{16}}}|j\rangle_{16}\right)\end{aligned}$$

Por tanto, la probabilidad de medir un estado j viene dada por el módulo al cuadrado de la siguiente amplitud:

$$\alpha_j = \frac{1}{\sqrt{2^{16}10923}}\left(\sum_{x=0}^{10922}e^{2\pi i\frac{6xj}{2^{16}}}\right)e^{2\pi i\frac{5j}{2^{16}}}.$$

Obtenemos entonces la siguiente distribución de probabilidad:

$$|\alpha_j|^2 = \frac{1}{2^{16}10923}\left|\sum_{x=0}^{10922}e^{2\pi i\frac{6xj}{2^{16}}}\right|^2.$$

$\tilde{\omega} \leftarrow$ Medimos $|\psi_4\rangle_{16}$.

Digamos que medimos $\tilde{\omega} = 54613$, por ejemplo.

$$\left|\frac{54613}{65536} - \frac{k}{r}\right| \leq \frac{1}{2 \cdot r^2},$$

donde k/r es una de las convergentes de la expansión en fracciones continuas de $\alpha = \frac{54613}{65536}$. En particular, esta $\alpha = [0; 1, 4, 1, 5460, 2]$. Sabiendo que $r < N$, tomamos el valor inmediatamente anterior a 5460; es decir, calculamos la tercera convergente, obteniendo

$$\frac{k}{r} = \frac{5}{6}.$$

De donde deducimos que $r = 6$. En efecto, $12^6 \equiv 1 \bmod 209$. Además, comprobamos también que $r = 6$ es par y que $12^3 \not\equiv \pm 1 \bmod 209$. Finalmente, podemos calcular los factores no triviales de 209:

$$d_1 = \gcd(12^3 + 1, 209) = 19$$
$$d_2 = \gcd(12^3 - 1, 209) = 11$$

Hemos factorizado $209 = 11 \cdot 19$.

6. Distribución cuántica de claves

Como hemos visto, la criptografía de clave pública basada en RSA tiene el riesgo de ser atacada por los ordenadores cuánticos. Aunque todavía no se ha logrado construir uno con suficiente capacidad para factorizar números de las magnitudes utilizadas en RSA, ya ha comenzado la búsqueda de alternativas a la criptografía tradicional. Una de esas alternativas es la criptografía cuántica; en particular, la Distribución Cuántica de Claves, en inglés Quantum Key Distribution (QKD), [17].

El protocolo BB84, [18], desarrollado por Charles Bennett y Gilles Brassard en 1984, es uno de los primeros y más conocidos métodos de criptografía cuántica. Su propósito es permitir que dos partes, Alice y Bob, compartan una clave secreta que puede ser usada para cifrar y descifrar mensajes con la seguridad garantizada por las propiedades de la mecánica cuántica. El protocolo BB84 utiliza la naturaleza cuántica del sistema para verificar si ha habido cualquier intento de interceptar y medir la clave por parte de un tercero, Eve. En esta sección haremos una pequeña introducción al método de criptografía cuántica BB84.

Este protocolo se basa en la propiedad de los sistemas cuánticos mencionada en el Postulado 4 de la mecánica cuántica. Es decir, una vez que se mide el estado de un sistema cuántico, la función que lo describe se proyecta sobre el subespacio correspondiente al resultado de la medida.

Ejemplo 6.1. Sea la función que describe el sistema cuántico de dos qubits inicialmente:

$$|\psi\rangle_i = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle.$$

Medimos el primer qubit y obtenemos $\tilde{\omega} = 0$. Después de la medida, el primer qubit quedará en el estado $|0\rangle$; por tanto, la función que describa el sistema será:

$$|\psi\rangle_f = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle.$$

Ejemplo 6.2. Sea $|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Si hacemos una medida sobre este estado en la base $\{|0\rangle, |1\rangle\}$, obtendremos $\tilde{\delta} = 0, 1$ equiprobablemente. Digamos que obtenemos, por ejemplo, $\tilde{\delta} = 1$. El estado quedará pues proyectado

$$|\psi'\rangle = |1\rangle.$$

Así pues, en las medidas posteriores en esta misma base, ya no mediremos $\tilde{\delta} = 0, 1$ equiprobablemente; mediremos $\tilde{\delta} = 1$ en la totalidad de los casos.

Digamos que Alice y Bob quieren intercambiar una clave mediante la distribución cuántica de claves. Deberán seguir los siguientes pasos.

1. Alice crea dos registros de longitud N. En uno de ellos, Alice guarda una cadena de bits aleatorios. Para la información del segundo registro, Alice elige aleatoriamente cómo codificar cada bit, si en la base $Z = \{|0\rangle, |1\rangle\}$ o en la base $X = \{|+\rangle, |-\rangle\}$. En el segundo registro, guarda la base en la que ha decidido codificar cada bit.

2. Alice codifica cada bit según la base escogida. El valor 0 del bit se corresponde con $|0\rangle$ en la base Z y con $|+\rangle$ en la base X. El valor 1 del bit se corresponde con $|1\rangle$ en la base Z y con $|-\rangle$ en la base X. Así pues, Alice ha creado un registro de longitud N de qubits.

Trasmisión cuántica													
Bits aleatorios de Alice	0	1	1	0	1	0	0	0	1	1	0	1	0
Base aleatoria de envío	X	Z	X	Z	Z	X	X	Z	X	Z	X	Z	Z
Elementos enviados por Alice	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$
Base aleatoria de recepción	Z	X	X	X	Z	Z	X	Z	X	Z	Z	Z	X
Elementos recibidos por Bob	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$
Discusión pública													
Coincidencia de bases			✓		✓		✓	✓	✓	✓		✓	
Datos aleatorios compartidos			1				0						
Confirmación			✓				✓						
Resultado													
Bits compartidos en secreto					1			0	1	1		1	

Cuadro 1: Ejemplo del intercambio de clave entre dos participantes, Alice y Bob, mediante la distribución de claves cuántica.

3. Alice comparte el registro de N qubits a Bob.
4. Bob elige aleatoriamente en qué base medir cada uno de los qubits.
5. Bob mide cada qubit según su elección de bases.
6. Alice comparte públicamente el registro con la información de bases de codificación de los qubits. Así, Bob puede comprobar qué qubits ha medido en la misma base que han sido codificados. De estos qubits, Bob podrá recuperar el bit que Alice ha codificado, obteniendo así una cadena de bits compartidos en secreto.

En este proceso, es posible detectar si un tercero, Eve, intercepta el intercambio de qubits. Veamos, con un ejemplo, cómo podría detectarse. Digamos que Alice prepara sus qubits tal que en la posición n, ha codificado el bit 0 en la base X. Así pues el qubit n que envía es un $|+\rangle$. Si Eve mide el qubit antes de que llegue a Bob, y decide medirlo en la base Z, equiprobablemente, medirá $|0\rangle$ o $|1\rangle$. Digamos que mide $|0\rangle$ por ejemplo, proyectándolo así en este subespacio. Es decir, el qubit n pasa a ser $|0\rangle$ con probabilidad 1. Cuando Bob recibe este qubit, y lo mide en la base X, obtiene $|+\rangle$ o $|-\rangle$ equiprobablemente. Entonces, Alice y él comparan bases, se dan cuenta que han utilizado la misma para codificar y medir el qubit n y por tanto, el bit de información debería haberse intercambiado correctamente. Sin embargo, si Bob mide $|-\rangle$, se dan cuenta que lo que debería haber llegado como un $|+\rangle$, o un 0 codificado, ha sido medido como un $|-\rangle$, o un 1 codificado. Así, pueden detectar a Eve.

Para comprobar que no ha habido interceptaciones, una vez se ha comprobado en qué qubits las bases de envío y recepción son la misma, Alice y Bob pueden compartir públicamente algunos de los registros en los que creen que coinciden. Si en estos registros, no hay sospecha de interceptación, toman el intercambio de clave como válido y crean una clave con el resto de bits que se han compartido en secreto.

7. Conclusiones

En este estudio, hemos explorado el desarrollo y la relevancia del Algoritmo de Shor, destacando su vínculo con la criptografía. Tras los primeros capítulos introductorios de criptografía, mecánica cuántica y el algoritmo de Deutsch, hemos desarrollado los pasos del algoritmo de Shor, aprovechando los principios de la teoría de números para relacionar la factorización de $N = pq$ con la determinación del periodo de una función. Analizando paso a paso la complejidad del algoritmo de Shor, hemos podido apreciar la potencial ventaja de los ordenadores cuánticos en ciertos procesos. El algoritmo de factorización de Shor presenta, en su totalidad, una complejidad de $O((\log N)^3)$, ciertamente más eficiente que la alternativa clásica de complejidad $O(e^{(\log N)^{1/3}})$. Por último, hemos explorado una introducción a la distribución cuántica de claves como una alternativa criptográfica segura ante el avance de los ordenadores cuánticos.

Referencias

[1] N. Kolbitz, *A course in number theory and cryptography*. Springer, New York, 1994.

[2] C. Pomerance and P. Erdős, "A Tale of Two Sieves," 1998.

[3] S. Rubinstein-Salzedo, *Cryptography*. Springer, Palo Alto, 2018.

[4] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," *Phys. Rev. A*, vol. 5101, 1994.

[5] A. Barenco et al., "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, no. 3457, 1995.

[6] R. Jozsa, "Quantum algorithms and the Fourier transform," *Proc. R. Soc. Lond. A*, vol. 454, pp. 323-337, 1997.

[7] Qiskit Community, "Quantum Fourier Transform," [Online]. Available: `https://github.com/Qiskit/textbook/blob/main/notebooks/ch-algorithms/quantum-fourier-transform.ipynb`. Accessed: 2024.

[8] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A*, vol. 400, pp. 97-117, 1985.

[9] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, pp. 124-134, 1994.

[10] S. J. Lomonaco, "Shor's quantum factoring algorithm," in *AMS Proceedings of Symposium in Applied Mathematics*, vol. 58, 2008.

[11] J. Ossorio-Castillo and J. M. Tornero, "Quantum computing from a mathematical perspective: a description of the quantum circuit model," 2018.

[12] G. Hardy and E. Wright, *An Introduction To The Theory Of Numbers*, 4th ed. Oxford University Press, 1975.

[13] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Rev. Mod. Phys.*, vol. 68, no. 733, 1996.

[14] P. Guerzhoy, "A short introduction to continued fractions," Department of Mathematics, Temple University.

[15] T. Sauer, "Continued fractions, class notes for Mathematics with an emphasis on Digital Image Processing," FORWISS, University of Passau, 2019.

[16] N. Datta, "Class notes for Quantum information and computation, Part IIC," DAMTP, University of Cambridge, 2020.

[17] P. W. Shor, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, no. 441, 2000.

[18] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7-11, 2014.