Aritmética Utilizando la Transformada Cuántica de Fourier

Erick Jesús Ríos González

13 de mayo de 2024

1 Motivación

La transformada cuántica de Fourier nos permite cambiar de una base computacional a la base de Fourier. Nos permite pasar de la base usual (base computacional):

$$|0\rangle \,\&\, |1\rangle$$

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

a la base:

$$|+\rangle \,\&\, |-\rangle$$

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

Es decir, tomando un ejemplo podemos pasar de la siguiente representación de tres qubits:

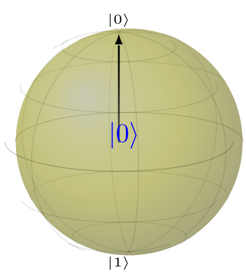

Figura 1: *
Qubit 1: $|0\rangle$

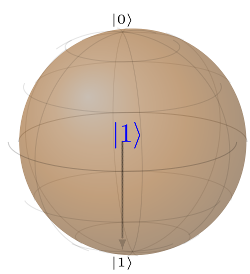

Figura 2: *
Qubit 2: $|1\rangle$

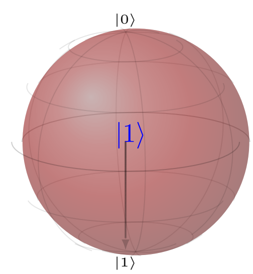

Figura 3: *
Qubit 3: $|1\rangle$

Figura 4: La esfera de Bloch es una forma de representación gráfica del estado de un qubit. En la parte superior de la esfera colocamos el estado $|0\rangle$, mientras que en la parte inferior el estado $|1\rangle$. En el resto de la esfera colocamos todos los posibles estados en superposición.

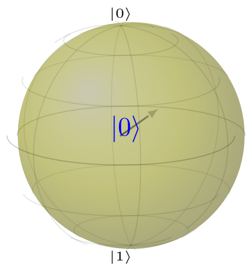

Figura 5: *
Qubit 1: $|0\rangle$

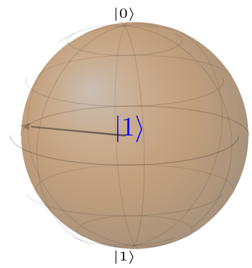

Figura 6: *
Qubit 2: $|1\rangle$

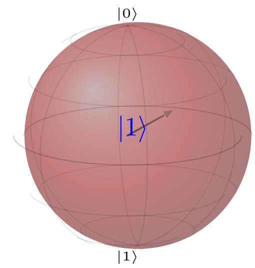

Figura 7: *
Qubit 3: $|1\rangle$

Figura 8: La esfera de Bloch es una forma de representación gráfica del estado de un qubit. En la parte superior de la esfera colocamos el estado $|0\rangle$, mientras que en la parte inferior el estado $|1\rangle$. En el resto de la esfera colocamos todos los posibles estados en superposición.

2 Representación Binaria de un Estado

Definición 2.1: Representación Binaria

La representación binaria es un sistema de numeración en el que los números se expresan como combinaciones de potencias de 2, utilizando únicamente los dígitos 0 y 1. Cada dígito en una representación binaria se llama un bit. Por ejemplo, un número binario de n bits se puede expresar como:

$$\sum_{i=0}^{n-1} b_i \cdot 2^i = b_{n-1}b_{n-2}\dots b_1 b_0$$

donde b_i es el i-ésimo bit, con i variando desde 0 hasta $n-1$ de derecha a izquierda.

Sea $y \in \mathbb{N} \cup \{0\}$. Utilizando la `Definición 3.1` proponemos la representación binaria de y como:

$$y = y_n y_{n-1} \dots y_0$$

Para un sistema de qubits esta representación sería:

$$y = |y_n y_{n-1} \dots y_0\rangle$$

Ejemplo:
Sea $y = 3$, la rrepresentación binaria de y utilizando un sistema de qubits sería:

$$|3\rangle = |011\rangle$$

Necesitamos introducir notación para fracciones binarias, lo cual nos ayudará a reescribir la Transformada Cuántica de Fourier (QFT) de manera simplista.

Definición 2.2

Para $a_1, \dots, a_m \in \{0, 1\}$ definimos

$$0.a_1 a_2 \dots a_m := \frac{a_1}{2} + \frac{a_2}{4} + \dots + \frac{a_m}{2^m} = \sum_{l=1}^{m} a_l \cdot 2^{-l}.$$

3 La Transformada Cuántica de Fourier (QFT)

Definición 3.1: Transformada Integral

Una transformada integral es una operación lineal que convierte una función, $f(x)$, en otra función, $F(u)$, a través de la siguiente integral:

$$F(u) = \int_a^b f(x)K(x,u)\,dx$$

La función $K(x,u)$, conocida como el núcleo de la transformada, y los límites de la integral se especifican para una transformada particular.

El cambio de la base computacional a una base de Fourier se puede describir como una transformada integral:

$$\{x\} \to \{y\}$$

$$IT[x] = ker(x,y)\{y\}$$

O en notación de nuestros vectores en el espacio de Hilbert:

$$QFT\,|x\rangle = ker(x,y)\,|y\rangle$$

Especificamente el núcleo que es de nuestro interés para esta transformada lo podemos denotar como:

$$QFT\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}}\,|y\rangle$$

Con lo que hemos obtenido nuestra primera definición de la Transformada Cuántica de Fourier:

Definición 3.2: Transformada Cuántica de Fourier

Definimos la Transformada Cuántica de Fourier como:

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} e^{\frac{2\pi i x y}{y}}\,|k_i\rangle\,.$$

De esta manera, podemos escribir QFT para cualquier vector $|x\rangle$ utilizando el siguiente lema:

Lema 3.1

Sea $n \in \mathbb{N}$ y

$$x = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{n-1} x_j 2^j, \quad \text{donde } x_j \in \{0,1\} \text{ para } j \in \{0,\dots,n-1\}.$$

Entonces la acción de la transformada cuántica de Fourier F sobre cualquier vector $|x\rangle$ de la base computacional de $\mathcal{H}_n$ puede escribirse como

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \left(|0\rangle + e^{2\pi i 0.x_j\dots x_0}|1\rangle\right).$$

4 Ejemplo 1+2

Primero comenzamos por hacer la representación binaria de los números $A = 1$ y $B = 2$, pero como el número A va a ser el que cargué la suma tenemos que agregarle un qbit más para evitar los límites de la suma modular.

$$A = 1 = 001_2$$

$$B = 2 = 10_2$$

Sea $A = a_2a_1a_0$ y $B = b_1b_0$ las representaciones binarias de A y B respectivamente, usando el teorema de reperesntación de Riez, podemos hacer la siguiente representación para nuestro ejemplo:

$$|001_2\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle$$

$$|10_2\rangle = |1\rangle \otimes |0\rangle$$

Para nuestro ejemplo seguiremos el siguiente circuito:

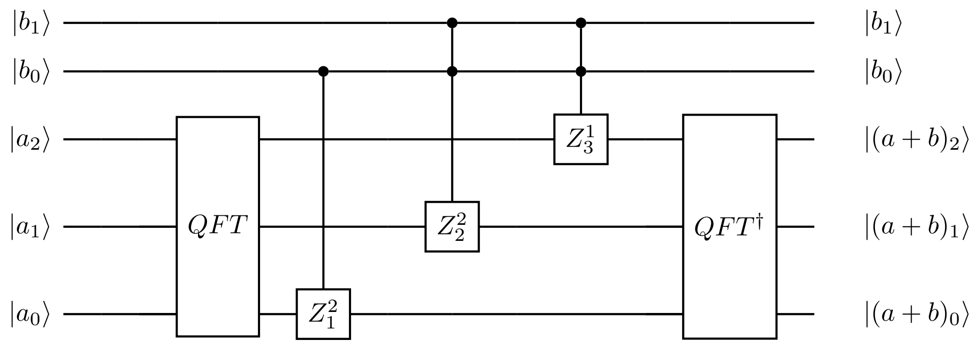

Figura 9: Circuito cuántico para sumar dos números binarios

Ahora que ya sabemos como vamos a operar usaremos el `Lema 1.1` y la `Deficinición 1.1` para aplicar la QFT de nuestro número A:

$$QFT\,|A\rangle = QFT\,|001\rangle = \frac{1}{\sqrt{8}} \bigotimes_{j=0}^{2} (|0\rangle + \exp[2\pi i 0.a_j \ldots a_0]\,|1\rangle)$$

$$= \frac{1}{\sqrt{8}} [(|0\rangle + \exp[2\pi i 0.a_0]\,|1\rangle) \otimes (|0\rangle + \exp[2\pi i 0.a_1a_0]\,|1\rangle) \otimes (|0\rangle + \exp[2\pi i 0.a_2a_1a_0]\,|1\rangle)]$$

$$= \frac{1}{\sqrt{2}} (|0\rangle + \exp[2\pi i 0{,}1]\,|1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + \exp[2\pi i 0{,}01]\,|1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + \exp[2\pi i 0{,}001]\,|1\rangle)$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle + \exp[2\pi i \frac{a}{2}]\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp[2\pi i \frac{a}{2^2}]\,|1\rangle\right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + \exp[2\pi i \frac{a}{2^3}]\,|1\rangle\right)$$

$$= \underbrace{\frac{1}{\sqrt{2}} [(|0\rangle + \exp[2\pi i 0{,}1]\,|1\rangle)]}_{|\phi(a_2)\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}} [(|0\rangle + \exp[2\pi i 0{,}01]\,|1\rangle)]}_{|\phi(a_1)\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}} [(|0\rangle + \exp[2\pi i 0{,}001]\,|1\rangle)]}_{|\phi(a_0)\rangle}$$

Despues de la aplicación de QFT a el número A ahora tenemos que nuestro circuito se ha modificado de la siguiente forma:

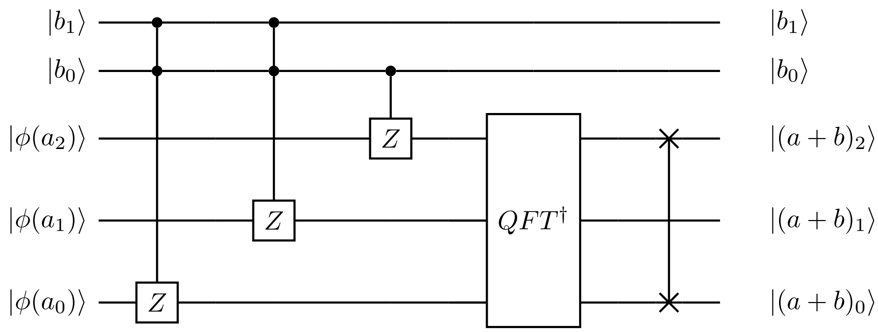

Figura 10: Circuito cuántico para sumar dos números binarios, después de haber aplicado QFT

Ahora procedemos a aplicar la compuerta Z tomando como control los qbits descritos en nuestro diagrama. Comenzando por el qbit $|\phi(a_0)\rangle$ (qbit objetivo) y $|b_0\rangle$ (qbit control) aplicamos Z:

$$Z_3^2\,|\phi(a_0)\rangle = \frac{1}{\sqrt{2}} Z_3^2\,|(|0\rangle + \exp[2\pi i 0{,}001]\,|1\rangle)\rangle$$

$$= \frac{1}{\sqrt{2}}\,(|0\rangle + (\exp[2\pi i 0{,}001]\exp[2\pi i 0{,}010])\,|1\rangle)$$

$$= \frac{1}{\sqrt{2}}\,(|0\rangle + (\exp[2\pi i(0{,}001 + 0{,}010)])\,|1\rangle)$$

$$= \frac{1}{\sqrt{2}}\,(|0\rangle + (\exp[2\pi i(0{,}011)])\,|1\rangle)$$

Con lo cual hemos obtenido un nuevo elemento, el cual denotamos $|\phi(a_0)''\rangle$:

$$\underbrace{\frac{1}{\sqrt{2}}\,|(|0\rangle + \exp[2\pi i(0{,}011)]\,|1\rangle)\rangle}_{|\phi(a_0)''\rangle}$$

Haciendo un procedimiento análogo con los otros dos qbits, tenemos que para $|\phi(a_1)\rangle$:

$$Z_2^2\,|\phi(a_1)\rangle = \frac{1}{\sqrt{2}} Z_2^2\,|(|0\rangle + \exp[2\pi i 0{,}01]\,|1\rangle)\rangle$$

$$= \frac{1}{\sqrt{2}}\,(|0\rangle + (\exp[2\pi i(0{,}01 + 0{,}10)])\,|1\rangle)$$

$$= \frac{1}{\sqrt{2}}\,(|0\rangle + (\exp[2\pi i(0{,}11)])\,|1\rangle)$$

Con lo cual hemos obtenido un nuevo elemento, el cual denotamos $|\phi(a_1)''\rangle$

$$\underbrace{\frac{1}{\sqrt{2}}\,|(|0\rangle + \exp[2\pi i(0{,}11)]\,|1\rangle)\rangle}_{|\phi(a_1)''\rangle}$$

Finalmente para $|a_2\rangle$ la rotación nos queda:

$$Z_1^1\,|\phi(a_2)\rangle = \frac{1}{\sqrt{2}} Z_1^1\,|(|0\rangle + \exp[2\pi i 0{,}0]\,|1\rangle)\rangle$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle + (\exp[2\pi i(0{,}1 + 0{,}0)]) |1\rangle \right)$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle + (\exp[2\pi i(0{,}1)]) |1\rangle \right)$$

Con lo cual hemos obtenido un nuevo elemento, el cual denotamos $|\phi(a_2)'\rangle$

$$= \underbrace{\frac{1}{\sqrt{2}} \left| (|0\rangle + \exp[2\pi i(0{,}1)] |1\rangle) \right\rangle}_{|\phi(a_2)'\rangle}$$

Vemos que ahora nuestro diagrama se ha modificado a:

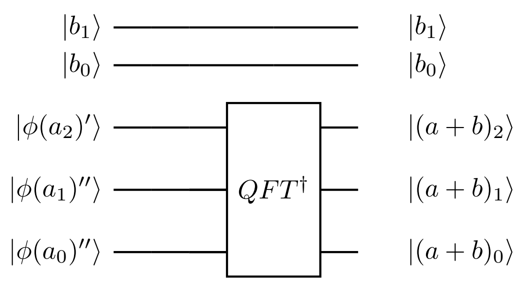

Figura 11: Circuito cuántico para sumar dos números binarios, después de haber aplicado QFT, recordemos que un último paso de $QFT^\dagger$ es hacer un swap entre y las rotaciones correspondientes

Finalmente aplicamos $QFT^\dagger$ al ket conformado por $|\phi(a_2)'\phi(a_1)''\phi(a_0)''\rangle$, esta operación se puede ver como:

$$QFT^\dagger |\phi(a_2)' \otimes \phi(a_1)'' \otimes \phi(a_0)''\rangle = QFT^\dagger |\phi(a_2)'\rangle \otimes QFT^\dagger |\phi(a_1)''\rangle \otimes QFT^\dagger |\phi(a_0)''\rangle$$

Recordemos que $QFT^\dagger$ realiza un swap, para este ejemplo, entre $|\phi(a_2)'\rangle$ y $|\phi(a_1)''\rangle$. Para de esta manera obtener la componente $|(a+b)_2\rangle$, $|(a+b)_1\rangle$ y $|(a+b)_0\rangle$.

$$= \left| |0\rangle \otimes |1\rangle \otimes |1\rangle \right\rangle$$

$$= |011\rangle$$

$$\implies 011_2 = 3_{10} = 1 + 2$$