Pontificia Universidad Javeriana Cali

ESTIMACIÓN Y BÚSQUEDA DE SOLUCIONES DE SISTEMAS DE ECUACIONES LINEALES POR MEDIO DE ALGORITMOS DE COMPUTACIÓN CUÁNTICA.

por

Santiago Restrepo

Tesis de grado presentado a la directiva de la carrera de matemáticas aplicadas en cumplimiento de los requisitos para la concesión del título de Matemático Aplicado por parte de la Pontificia Universidad Javeriana Cali

Tutor académico

Dr. Andrés Rivera

Cali, Colombia

5 de mayo de 2025

ESTIMACIÓN Y BÚSQUEDA DE SOLUCIONES DE SISTEMAS DE ECUACIONES LINEALES POR MEDIO DE ALGORITMOS DE COMPUTACIÓN CUÁNTICA

por

Santiago Restrepo

Tesis de grado presentado a la directiva de la carrera de matemáticas aplicadas en cumplimiento de los requisitos para la concesión del título de Matemático Aplicado por parte de la Pontificia Universidad Javeriana Cali

Tutor Académico

Dr. Andrés Rivera

Cali, Colombia

5 de mayo de 2025

Declaración

Yo, **Santiago Restrepo** declaro que este trabajo monográfico es obra y esfuerzo propios y que no ha sido presentada antes. Todas las fuentes de información consultadas para realizar este documento, se han citado y hecho constar su procedencia.

Firma: SRA

Fecha: Mayo 05 de 2025

Aprobación

Esta tesis titulada ***Estimación y búsqueda de soluciones de sistemas de ecuaciones lineales por medio de algoritmos de computación cuántica***, ha sido aprobada por los siguientes directores.

Director de tesis:
Dr. Andrés Rivera *Firma:*  *Fecha:* Mayo 05 de 2025

Dedicatoria

Dedico este trabajo, principalmente, a Dios por darme la sabiduría y la salud suficiente para poder llevar a cabo este arduo proceso, desde el inicio hasta el final, e iluminarme fielmente en épocas de mucha dificultad. Sin embargo, también dedico este trabajo al señor Jaime Aurelio Caicedo, una persona brillante, pero además, muy especial e importante para mí, pues fue aquel que tomó el rol de maestro y guía en una época donde no sabía cuál era mi camino en la vida. A esta persona le debo el haber estudiado esta carrera, al compartirme su amor y motivación por las matemáticas. Por ello, le estaré eternamente agradecido.

Agradecimientos

Me gustaría comenzar expresando mi más profundo agradecimiento a mi tutor de tesis, el Dr. Andrés Rivera, por ser mi guía en todo este trabajo. El Dr. Andrés Rivera aceptó dirigir esta tesis completamente propuesta por mí y sobre la cual él no tenía conocimientos en los temarios relacionados con la computación cuántica. Sin embargo, junto a mí, se embarcó en un proceso de aprendizaje y análisis conjunto hasta finalmente culminar este documento, un hecho que vale la pena destacar.

Además, deseo reconocer el papel de mi familia, especialmente de mis padres Hernando y Claudia, mis abuelas Ligia y Delia y mis dos hermanas Sara e Isabel, por su inquebrantable apoyo y aliento a lo largo de mi estudio. Gracias a ellos, pude encontrar una motivación adicional en el desarrollo de este trabajo y fueron un soporte constante en el transcurso de toda mi carrera. Por último, destaco al doctor Andrés Amador, quien actuó como consejero y acompañante en toda la realización de la tesis, mostrando frecuentemente su preocupación e interés por que todo salga bien al final.

Resumen

La búsqueda de las soluciones (o, en muchos casos, aproximaciones de ellas) de un sistema de ecuaciones lineales es un problema común y transversal en casi todas las ramas de la ciencia y la ingeniería. Es bien sabido que el análisis relacionado con este tipo de ecuaciones ha permitido modelar, comprender y predecir comportamientos globales o locales de múltiples variables interconectadas, de acuerdo a las condiciones intrínsecas del contexto. En la actualidad, existen varios algoritmos y métodos que permiten resolver este tipo de ecuaciones, extendidos casos donde se manejan muchos datos, sin embargo, hay ocasiones donde estos algoritmos no son del todo efectivos, por ejemplo, cuando el problema planteado a resolver implica un costo computacional demasiado alto y no es posible resolverlo por limitaciones del hardware disponible, o cuando el tiempo de procesamiento mínimo es tan eleveado que ya no se vuelve factible esperar por una posible o no solución. Lo anterior ha hecho que se planteen nuevos algoritmos, incluyedo aquellos que emergen en como herramientas pilares de otros campos. En este sentido, la computación cuántica es una teoría que ofrece una vía alterna para encontrar o aproximar las soluciones de esta clase de sistemas de ecuaciones. De hecho, con los avances realizados estos últimos años, actualmente existen algoritmos cuánticos útiles para este fin.

En este documento se presenta en detalle el algoritmo cuántico desarrollado por Harrow, Hassidim y Lloyd en [1], el cual permite resolver el sistema matricial

$$A\mathbf{x} = \mathbf{b},$$

siendo $A \in \mathbb{M}_{N\times N}$ una matriz hermitiana. Para la implementación de este método se requiere el uso de subrutinas de otros algoritmos, tales como, el algoritmo de la estimación cuántica de fase (QFE) y el modelado de sistemas cuánticos. Todos estos insumos para analizar el algoritmo HHL (conocido así en la comunidad científica en mención de sus creadores) serán presentados y explicados a lo largo de este trabajo.

Índice general

Índice de figuras

Índice de cuadros

Introducción

A lo largo de la historia, las matemáticas han sido utilizadas para resolver muchos retos, acertijos y problemas numéricos, formulados por aquellos dedicados exclusivamente a ese tipo de estudios. Sin embargo, con el paso del tiempo, tales cuestionamientos dejarían de estar limitados solo a este campo, y extenderían su alcance hasta plantear aplicaciones directas en otros escenarios, como por ejemplo el uso de modelos matemáticos en favor de la simulación de dinámicas y comportamientos reales. Hoy en día, las matemáticas se consolidan como la base y un complemento esencial que cualquier ingeniería o ciencia puede utilizar; de hecho, el presente trabajo hace muestra de ese complemento aplicado a una de las ramas de la computación más complejas hoy en día. Se comienza con una exploración en el campo del álgebra lineal con el propósito de conformar una lista de herramientas y conceptos matemáticos que puedan ser utilizados a fin de plasmar correctamente ciertas definiciones de la computación cuántica, la ciencia de interés en este documento. Lo anterior conduciría en preguntas como: ¿Qué es la computación cuántica? ¿Qué potenciales aplicaciones ofrece? ¿Desde hace cuánto se viene desarrollando?. Sin pretender dar una respuesta profunda y detallada a estas preguntas, la computación cuántica es un enfoque de la informática que aprovecha principios de la mecánica cuántica para realizar cálculos. Sus orígenes se remontan a principios del año 1980 con el nacimiento de las primeras teorías sobre el uso de la mecánica cuántica como posible sistema diseñable (ver [2]), y a partir de entonces se ha convertido en una de las ramas de la ciencia más atractivas para los físicos e ingenieros que buscan convertir estos conceptos en sistemas computacionales funcionales que logren sobrepasar el rendimiento de los sistemas utilizados hoy día. Sin entrar en detalles intrínsecos de la física teórica asociada, los conceptos de la mecánica cuántica utilizados en este documento son relativamente básicos, al igual que su aplicación en la descripción de los algoritmos cuánticos que permitan finalmente estimar la solución de un sistema de ecuaciones lineales, limitado a ciertas condiciones puntuales.

La finalidad detrás de la implementación del algoritmo no es comparar su eficiencia frente a otros existentes, ni tampoco utilizarlo para determinar en qué aspectos la computación cuántica es superior o inferior a la computación clásica. Por el contrario, lejos de buscar alguna comparación, al realizar este trabajo nos hemos visto fascinados por las potenciales oportunidades que estos temas ofrecen y cómo se puede sorprendentemente facilitar la comprensión de algunos conceptos, aplicando un punto de vista numérico-algebraico, sin necesidad de saber de mecánica cuántica en sí, o temarios avanzados de la Física. Por ende, la motivación principal de este documento es introducir al lector en este nuevo campo, despertando su posible interés mediante un algoritmo que ofrece una forma alternativa de resolución frente a planteamientos conocidos como los sistemas lineales, todo lo anterior, utilizando simples conceptos matemáticos que van desde la teoría de matrices hasta los espacios vectoriales complejos.

Objetivos de investigación

Objetivo Principal

El objetivo principal de este trabajo de grado es analizar en detalle los componentes principales del algoritmo de computación cuántica desarrollado por A. Harrow, A. Hassidim y S. Lloyd en [1], para la resolución de sistemas de ecuaciones lineales $Ax = b$ con $A \in \mathbb{M}_{N\times N}$ una matriz hermitiana. La explicación de cualquier concepto necesario se hará utilizando la teoría de álgebra lineal sobre espacios vectoriales complejos sin entrar en detalles en aspectos de la física.

Objetivos específicos

i. Establecer los conceptos y definiciones matemáticas necesarios para lograr un entendimiento introductorio de las nociones más sencillas de algoritmos cuánticos.

ii. Introducir la unidad básica de información manejada en la computación cuántica conocida como cúbit, aplicando los espacios vectoriales complejos a modo de complemento.

iii. Representar la acción de modificación de la información dentro de estos sistemas, tales como la utilización de estados, puertas y circuitos cuánticos, por medio de la teoría de matrices y el álgebra lineal.

iv. Explicar el funcionamiento del algoritmo HHL, detallando cada una de sus etapas, utilizando estimación de fase cuántica, transformaciones unitarias y medición, para concluir con un ejemplo analítico.

Estructura del documento

Para una mejor lectura, se ha dividido el documento de la siguiente forma. Después de la introducción, en el capítulo 1 se describen brevemente los conceptos algebraicos y matemáticos necesarios en el marco teórico del documento. Dichos conceptos parten de la teoría de los números y espacios complejos, elementos fundamentales en teoría de matrices, el concepto de valor y vectores propios, y finaliza con el teorema espectral para matrices hermitianas.

En el capítulo 2 se introduce formalmente al lector a algunos conceptos fundamentales de la computación cuántica, principalmente, detallando matemáticamente el concepto de cúbit y cómo se pueden "representar" geométricamente mediante la esfera de Bloch a través de su fase asociada. Así mismo, se extiende el concepto de cúbit a múltiples cúbits vía operadores lineales sobre espacios vectoriales complejos, en particular, mediante el producto tensorial entre espacios vectoriales.

El concepto de puertas (operadores unitarios) y circuitos cuánticos se introduce en el capítulo 3. Se definen y ejemplifican algunas puertas cuánticas básicas para luego detallar las más importantes en nuestro trabajo, tales como la puerta de Hadamard y la transformada cuántica de Fourier. Finalizando el capítulo, se invoca de nuevo el concepto de fase de un cúbit para dar paso a dos puertas cuánticas claves en el desarrollo teórico de los capítulos posteriores: las puertas de rotación y rotación controlada sobre un n-cúbit.

El capítulo 4 está dedicado a explicar enteramente el algoritmo de estimación cuántica de fase, iniciando con un detallado ejemplo del mismo y continuando con la implementación paso a paso en general.

El documento termina con el capítulo 5, en el cual se explica e implementa matemáticamente el algoritmo HHL como meta final de este trabajo. Es aquí donde se conjugan todos los conceptos vistos en capítulos previos. Seguidamente, presentamos

Las conclusiones finales de este trabajo, esbozando las futuras líneas de estudio e investigación.

Capítulo 1

Marco teórico y elementos preliminares

El punto de partida de este marco teórico tiene como objetivo la introducción y definición de conceptos fundamentales y propiedades clave del álgebra lineal y los números complejos. Comenzaremos definiendo fórmulas fundamentales de los números complejos; seguiremos definiendo lo que es un espacio vectorial complejo junto con algunas operaciones de uso dentro de ese mismo espacio y terminaremos al definir lo que son las matrices hermitianas unitarias y qué propiedades presentan cada una de ellas.

1.1. Una pincelada sobre los números complejos y los espacios vectoriales complejos

A lo largo de todo el documento consideraremos el siguiente campo escalar

$$\mathbb{C} = \{z = a + bi \,|\, a, b \in \mathbb{R}\},$$

conocido como el campo de los números complejos, siendo i la variable compleja que satisface la ecuación cuadrática $z^2 = -1$. Para cada número complejo $z = a + bi$, al número real a se le conoce como la parte real de z, $(a = Re(z))$ y al número real b se le conoce como la parte imaginaria de z $(b = Im(z))$. Resaltemos algunas de las más importantes operaciones en $\mathbb{C}$.

- **Suma**. Dados $z = a + bi \in \mathbb{C}$ y $w = c + di \in \mathbb{C}$ la suma entre ellos se define por

$$z + w = a + c + (b + d)i.$$

- **Conjugado de un número complejo**. Dado $z = a + bi \in \mathbb{C}$, su conjugado es el número $\overline{z} \in \mathbb{C}$ dado por

$$\overline{z} = a - bi.$$

- **Módulo de un número complejo**. Dados $z = a+bi \in \mathbb{C}$, su módulo es el número $|z| \in \mathbb{R}$ dado por

$$|z| = \sqrt{a^2 + b^2}.$$

- **Multiplicación**. Dados $z = a + bi \in \mathbb{C}$ y $w = c + di$, la multiplicación entre z y w es el número complejo zw dado por

$$zw = ac - bd + (ab + cd)i.$$

- **Inverso de un número complejo**. Dado $z = a + bi \in \mathbb{C}$, $z \neq 0$, el inverso multiplicativo de z, es el número complejo z^{-1} dado por

$$z^{-1} = \frac{a - bi}{|z|^2}.$$

- **Forma polar de un número complejo**. Para cada número complejo $z = a+bi \in \mathbb{C}$, se define la relación

$$a = |z|\cos\theta, \quad b = |z|\sin\theta, \quad \theta \in \mathbb{R}.$$

En cuyo caso,

$$\begin{aligned} z = a + bi &= |z|\cos\theta + |z|\sin\theta\, i = |z|(\cos\theta + \sin\theta\, i) \\ &= |z|e^{i\theta}, \quad e^{i\theta} := \cos\theta + \sin\theta\, i, \quad \theta \in \mathbb{R}. \end{aligned}$$

La expresión anterior para z se conoce como su forma polar, en donde θ es llamado *argumento* de z. En particular, al ángulo $\theta \in (-\pi, \pi]$ se le llama argumento principal de z y se denota como $\theta_z := \arg(z)$.

Consideremos ahora la ecuación polinomial en $\mathbb{C}$

$$w^m = z, \quad \text{con} \quad z = |z|e^{i\theta}, \tag{1.1}$$

para $m \in \mathbb{N}$. A partir de la fórmula de Moivre se deduce que

$$w_k = |z|^{1/m} e^{i\varphi_k}, \quad \text{con} \quad \varphi_k = \frac{\theta + 2k\pi}{m}, \quad \text{y} \quad k = 0, 1, 2 \ldots m-1,$$

son las m-soluciones de la ecuación (1.1). En particular, para $z = 1$, y tomando $\theta = \arg(1) = 0$, tenemos

$$w_k = e^{i\varphi_k}, \quad \text{con} \quad \varphi_k = \frac{2k\pi}{m}, \quad \text{y} \quad k = 0, 1, 2 \ldots, m-1.$$

En adelante, a lo largo del texto, denotamos por $w = e^{i2\pi/m}$ una de las m-ésimas raíces de $z = 1$. El uso de este número complejo en particular será crucial más adelante.

1.1.1. Espacios vectoriales complejos

Consideremos un conjunto no vacío $\mathcal{V}$ (A los elementos de $\mathcal{V}$ se les llamará *vectores*). Este conjunto es capaz de definir una particular estructura matemática conocida como *espacio vectorial complejo* $\mathcal{Z}$, si se cumple que cada elemento $\mathbf{z} \in \mathcal{Z}$ puede escribirse como una combinación lineal compleja de vectores en $\mathcal{V}$, es decir: para todo $\mathbf{z} \in \mathcal{Z}$ existen números $z_j \in \mathbb{C}$ tales que

$$\mathbf{z} = z_1\mathbf{v}_1 + z_1\mathbf{v}_2 + \cdots + z_m\mathbf{v}_m, \tag{1.2}$$

para algunos vectores $\mathbf{v}_j \in \mathcal{V}$ y $m \in \mathbb{N} \cup \{\infty\}$. Continuando a partir de aquí. Un subconjunto de vectores $\mathcal{B} \subseteq \mathcal{V}$ es una base de $\mathcal{Z}$, si cada elemento $\mathbf{z} \in \mathcal{Z}$ se puede escribir en la forma (1.2) de manera única y con elementos $\mathbf{v}_j \in \mathcal{B}$. Más aún, si $m < \infty$ en tal caso, se dice que $\mathcal{Z}$ es un espacio vectorial complejo m-dimensional (de dimensión finita e igual a m).

Ejemplo 1. *Para $m = 2$, si definimos el subconjunto $\mathcal{B}_E = \{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ en donde*

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad y \quad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

se comprueba que $\mathcal{B}_E$ es una base de $\mathcal{Z} = \mathbb{C}^2$. En efecto, dado cualquier vector $\mathbf{z} \in \mathbb{C}^2$ se tiene

$$\mathbf{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + z_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rightarrow \mathbf{z} = z_1\mathbf{e}_1 + z_2\mathbf{e}_2.$$

Bajo el concepto de la estructura $\mathcal{Z}$ se define entre sus elementos la siguiente operación.

Definición 1. *(Producto interno en $\mathbb{C}^m$) Sean $\boldsymbol{o}$,$\boldsymbol{p} \in \mathbb{C}^m$, en la forma*

$$\boldsymbol{o} = \begin{pmatrix} o_1 \\ o_2 \\ \dots \\ o_m \end{pmatrix} \quad y \quad \boldsymbol{p} = \begin{pmatrix} p_1 \\ p_2 \\ \dots \\ p_m \end{pmatrix}.$$

El producto interno es la función bilineal $\langle\cdot|\cdot\rangle : \mathbb{C}^m \times \mathbb{C}^m \rightarrow \mathbb{C}$, dada por la siguiente operación:

$$\langle \boldsymbol{o}|\boldsymbol{p}\rangle = \sum_{s=1}^{m} \overline{o}_s p_s.$$

Esta función satisface las siguientes propiedades:

†) $\langle \mathbf{x}|\mathbf{x}\rangle$ es un número real no negativo.

†) $\langle \mathbf{x}|\mathbf{y}\rangle = \overline{\langle \mathbf{y}|\mathbf{x}\rangle}$.

†) $\langle z_1\mathbf{x} + z_2\mathbf{w}|\mathbf{y}\rangle = \overline{z}_1\langle \mathbf{x}|\mathbf{y}\rangle + \overline{z}_2\langle \mathbf{w}|\mathbf{y}\rangle$ con $z_1, z_2 \in \mathbb{C}$ y $\mathbf{x}, \mathbf{w}, \mathbf{y} \in \mathbb{C}^m$.

A partir de la definición de producto interno, se desprenden los siguientes conceptos:

‡) La *norma de un vector* $\mathbf{x}$ es el número real

$$|\mathbf{x}| = \sqrt{\langle \mathbf{x}|\mathbf{x}\rangle} = \sqrt{\sum_{s=1}^{m} |x_s|^2},$$

en donde $|x_s|^2 = [\mathrm{Re}(x_s)]^2 + [\mathrm{Im}(x_s)]^2$.

‡) Dos vectores $\mathbf{o}, \mathbf{p}$ se dicen que son *ortogonales* si $\langle \mathbf{o}|\mathbf{p}\rangle = 0$.

‡) Un conjunto de vectores $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ se dice que forma un *conjunto ortonormal* si todos los vectores que lo conforman tienen norma uno y son todos ortogonales entre sí, esto es $\langle \mathbf{v}_r|\mathbf{v}_s\rangle = \sigma_{rs}$ con $\sigma_{ss} = 1$ y $\sigma_{sr} = 0$ si $s \neq r$.

Ejemplo 2. *Retomando $\mathbb{C}^2$ con base $\mathcal{B}_E$, nótese que para los vectores $\boldsymbol{e}_1, \boldsymbol{e}_2$ se cumple la condición de ortonormalidad, como se ve a continuación.*

$$\langle \boldsymbol{e}_1|\boldsymbol{e}_2\rangle = 1 \cdot 0 + 0 \cdot 1 = 0.$$

1.2. Notaciones fundamentales $\langle\cdot|$ bra y ket $|\cdot\rangle$

Con el propósito de movernos hacia la computación cuántica, en adelante, será conveniente que todo vector $\mathbf{v}$ perteneciente a cualquier espacio vectorial m-dimensional se denote en la forma: $|v\rangle$. Esta notación es conocida como la notación *ket de Dirac*, introducida en [3, 4]. Así pues.

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \cdots \\ v_m \end{pmatrix}.$$

En forma análoga, el vector transpuesto conjugado de $|v\rangle$ será representado por la notación *bra de Dirac*.

$$\langle v| = (\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_m).$$

Tomando en cuenta lo anterior, la combinación lineal compleja definida para espacios vectoriales complejos queda de la siguiente forma:

$$|z\rangle = z_1 |v_1\rangle + z_1 |v_2\rangle + \cdots + z_m |v_m\rangle,$$

donde $z_j \in \mathbb{C}$ y $|v_j\rangle \in \mathcal{V}$.

A partir de lo anterior, el operador *producto interno* será representado por la notación bracket de Dirac, por el juego de palabras Bra y Ket.

$$\langle\gamma|\delta\rangle := \langle\gamma|\,|\delta\rangle = (\overline{\gamma}_1, \overline{\gamma}_2, \ldots, \overline{\gamma}_n) \begin{pmatrix} \delta_1 \\ \delta_2 \\ \cdots \\ \delta_n \end{pmatrix} = \overline{\gamma}_1\delta_1 + \overline{\gamma}_2\delta_2 + \cdots + \overline{\gamma}_n\delta_n = \sum_{s=1}^{n} \overline{\gamma}_s\delta_s,$$

En el espacio vectorial complejo bidimensional para los vectores $|e_1\rangle$ y $|e_2\rangle$ es usual reservar una notación más simple, dada por $|e_1\rangle = |0\rangle$ y $|e_2\rangle = |1\rangle$. En tal caso, denotaremos los vectores base,

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

En adelante, esta base ortonormal $B_E = \{|0\rangle, |1\rangle\}$ se conocerá como la *base estándar* o *base canónica*. Otra base $\mathbb{C}^2$ a la cual nos referiremos a lo largo del documento es la *Base de Hadamard* dada por

$$B_H = \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\} = \left\{ |H^{\nearrow}\rangle, |H^{\nwarrow}\rangle \right\}.$$

Es claro que:

$$|H^{\nearrow}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{y} \quad |H^{\nwarrow}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Por último, utilizamos letras mayúsculas para denotar a todo operador lineal entre espacios vectoriales. Cabe mencionar que, dado cualquier operador lineal $A : \mathcal{V} \to \mathcal{W}$ con $\mathcal{V}, \mathcal{W}$ espacios vectoriales de dimensión n y m respectivamente, existe una matriz $\mathbb{M}_{m\times n}$ que lo representa respecto a la base de $\mathcal{V}$ y $\mathcal{W}$.

Así mismo, la conjugada de cualquier matriz $A \in \mathbb{M}_{m\times n}$ se denotará por $A^* \in \mathbb{M}_{m\times n}$, y su traspuesta $A^T \in \mathbb{M}_{n\times m}$.

Ejemplo 3. *Considere la matriz*

$$A = \begin{pmatrix} 1 & -2i \\ \frac{7}{5} + 6i & 8 + \frac{1}{8}i \end{pmatrix}.$$

Un cálculo directo muestra que la matriz conjugada A^* y la matriz traspuesta A^T son respectivamente

$$A^* = \begin{pmatrix} 1 & 2i \\ \frac{7}{5} - 6i & 8 - \frac{1}{8}i \end{pmatrix} \quad y \quad A^T = \begin{pmatrix} 1 & \frac{7}{5} + 6i \\ -2i & 8 + \frac{1}{8}i \end{pmatrix}.$$

1.2.1. Producto externo

Consideremos dos espacios vectoriales $\mathcal{V}$, $\mathcal{W}$ donde ambos tienen definida la función producto interno $\langle\cdot|\cdot\rangle$. Tomemos cualquier par de vectores $|v\rangle$, $|w\rangle$ en $\mathcal{V}$ y $\mathcal{W}$ respectivamente. Se define el producto externo $|\cdot\rangle\langle\cdot|$, como la función $|w\rangle\langle v| : \mathcal{V} \to \mathcal{W}$ definida por

$$|w\rangle\langle v|\,(|\tilde{v}\rangle) := |w\rangle\langle v|\tilde{v}\rangle = \langle v|\tilde{v}\rangle\,|w\rangle\,, \quad \text{con} \quad |\tilde{v}\rangle \in \mathcal{V}.$$

Esta función satisface las siguientes propiedades:

†) $|w\rangle\langle v| = |v\rangle\langle w|$ cuando $|v\rangle = |w\rangle$

†) $|w\rangle\langle v|\,(|c\tilde{v}\rangle) \equiv c\langle v|\tilde{v}\rangle\,|w\rangle$ para $c \in \mathbb{C}$

†) $|w\rangle\langle v|\,(c_1\,|v_1\rangle + c_2\,|v_2\rangle) = |w\rangle\langle v|\,(c_1\,|v_1\rangle) + |w\rangle\langle v|\,(c_2\,|v_2\rangle)$ para $c_1, c_2 \in \mathbb{C}$

†) $|w_1\rangle\langle v_1|\,[|v_2\rangle\langle w_2|\,(|\tilde{w}\rangle)] = |w_1\rangle\langle v_1|v_2\rangle\langle w_2|\tilde{w}\rangle$

Note que la segunda y tercera propiedad nos dice que el producto externo es una aplicación lineal entre espacios vectoriales. Más aún, a partir de lo anterior, nótese que es posible formar combinaciones lineales de productos externos al tomar un par de vectores $|v_k\rangle \in \mathcal{V}$ y $|w_k\rangle \in \mathcal{W}$ respectivamente para cada función, esto de la siguiente forma:

$$\big(\sum_k a_k\,|w_k\rangle\langle v_k|\,\big)(|\tilde{v}\rangle) = \sum_k a_k\langle v_k|\tilde{v}\rangle\,|w_k\rangle\,,$$

con $k \in \mathbb{N} > 0$. De esta idea, se plantea una importante relación que toma como base el concepto de producto externo.

Definición 2. *(Relación de completitud) Sea el conjunto de vectores $B = \{k : |k\rangle\}$ una base ortonormal del correspondiente espacio vectorial $\mathcal{V}$ dotado con la función producto interno $\langle\cdot|\cdot\rangle$. Entonces, para cada vector $|v\rangle \in \mathcal{V}$ se cumple*

$$|v\rangle = \sum_k a_k\,|k\rangle\,, \quad \textit{con} \quad a_k = \langle k|v\rangle \in \mathbb{C}.$$

Por lo tanto,

$$\big(\sum_k |k\rangle\langle k|\,\big)\,|v\rangle = \sum_k \langle k|v\rangle\,|k\rangle = |v\rangle\,.$$

La anterior ecuación es cierta para todo vector $|v\rangle \in \mathcal{V}$, en consecuencia,

$$\sum_k |k\rangle\langle k| = I, \qquad I := \textit{operador identidad,}$$

Esta expresión es conocida como la ***relación de completitud.***

De la relación anterior nace una forma de escribir operadores lineales en términos de productos externos. Sean $\mathcal{V}$ y $\mathcal{W}$ dos espacios vectoriales distintos con sus respectivas bases ortonormales $B_{\mathcal{V}} = \{s : |v_s\rangle\}$ y $B_{\mathcal{W}} = \{r : |w_r\rangle\}$. Si tomamos cualquier operador lineal $A : \mathcal{V} \to \mathcal{W}$, por la relación de completitud se tiene

$$\begin{aligned} A =& I_{\mathcal{W}} A I_{\mathcal{V}}, \\ A =& \Big(\sum_r |w_r\rangle \langle w_r| \Big) \Big[A \Big(\sum_s |v_s\rangle \langle v_s| \Big) \Big], \\ A =& \sum_{sr} |w_r\rangle \langle w_r|A|v_s\rangle \langle v_s| = \sum_{sr} \langle w_r|A|v_s\rangle \, |w_r\rangle \langle v_s| \, . \end{aligned}$$

De esta última expresión se puede deducir que el término $\langle w_r|A|v_s\rangle$ corresponde a la r-ésima columna y la s-ésima fija de la representación matricial del operador lineal A respecto a las bases $B_{\mathcal{V}}$ y $B_{\mathcal{W}}$.

1.2.2. Matrices hermitianas, adjuntas y unitarias

Sea A cualquier matriz sobre el espacio normado $\mathcal{V}$. Se define la conjugada hermitiana de la matriz A como la matriz $A^\dagger = (A^*)^T$. En particular, esta matriz es la única matriz que junto con A cumple la siguiente relación:

$$\langle v|A|w\rangle = \langle A^\dagger \, |v\rangle \, |w\rangle,$$

para cualquier par de vectores $|v\rangle \, , |w\rangle \in \mathcal{V}$.

Entre las propiedades más destacadas de la conjugada hermitiana se tienen:

1. $\big(A \, |v\rangle \, \big)^\dagger = \langle v| \, A^\dagger$, para todo vector $|v\rangle \in \mathcal{V}$.
2. $\big(\, |v\rangle \, \langle w| \, \big)^\dagger = |w\rangle \, \langle v|$, para cualquier par de vectores $|v\rangle \, , |w\rangle \in \mathcal{V}$.
3. $\big(A^\dagger\big)^\dagger = A$.

Además, dadas dos matrices A y B se cumple $(AB)^\dagger = B^\dagger A^\dagger$.

Ejemplo 4. *Considere el operador lineal A: $\mathbb{C}^2 \to \mathbb{C}^2$ con representación matricial (para cierta base concreta):*

$$A = \begin{pmatrix} 1+3i & \frac{1}{3} - \frac{1}{\sqrt{2}} i \\ 2 & 5-4i \end{pmatrix}.$$

Por lo tanto, un cálculo directo muestra que la conjugada hermitiana de esta matriz es

$$A^\dagger = \begin{pmatrix} 1-3i & \frac{1}{3} + \frac{1}{\sqrt{2}} i \\ 2 & 5+4i \end{pmatrix}^T = \begin{pmatrix} 1-3i & 2 \\ \frac{1}{3} + \frac{1}{\sqrt{2}} i & 5+4i \end{pmatrix}.$$

De la definición de conjugada hermitiana, se desprenden los siguientes conceptos:

a. Dado un operador $A : \mathcal{V} \to \mathcal{W}$ (o su correspondiente matriz A) se dice que es un ***operador autoadjunto o hermitiano*** si

$$A = A^\dagger.$$

b. Dado un operador $N : \mathcal{V} \to \mathcal{W}$, (o su correspondiente matriz N) se dice que es un ***operador normal*** si
$$NN^\dagger = N^\dagger N.$$

c. Dado un operador $U : \mathcal{V} \to \mathcal{W}$, (o su correspondiente matriz U) se dice que es un ***operador unitario*** si
$$UU^\dagger = U^\dagger U = I,$$
con I la matriz identidad.

Ejemplo 5. *Considere los siguientes operadores A, N, U. Cada uno con sus respectivas representaciones matriciales*

$$A = \begin{pmatrix} 7 & \frac{1}{2} + 9i \\ \frac{1}{2} - 9i & 0 \end{pmatrix}, \quad N = \begin{pmatrix} \frac{1}{2} & i \\ i & \frac{1}{2} \end{pmatrix} \quad y \quad U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

A continuación se calculan las conjugadas hermitianas

$$A^\dagger = \begin{pmatrix} 7 & \frac{1}{2} + 9i \\ \frac{1}{2} - 9i & 0 \end{pmatrix}, \quad N^\dagger = \begin{pmatrix} \frac{1}{2} & -i \\ -i & \frac{1}{2} \end{pmatrix} \quad y \quad U^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

No es difícil comprobar que A es un operador hermitiano, N es un operador normal y U es un operador unitario.

Los operadores unitarios serán fundamentales para los propósitos de este trabajo, razón por la cual nos enfocaremos más en este tipo de matrices; de hecho, una de las propiedades geométricas más notables es que preservan el producto interno entre vectores. En efecto, para cualquier par de vectores $|v\rangle, |w\rangle \in \mathcal{V}$ y para cualquier operador unitario $U : \mathcal{V} \to \mathcal{V}$ se deduce
$$\langle U|v\rangle\, |U|w\rangle\rangle = \langle U^\dagger U|v\rangle\, |w\rangle = \langle I|v\rangle\, |w\rangle = \langle v|w\rangle.$$
La expresión anterior implica que todo operador unitario transforma bases ortonormales en bases ortonormales. En efecto, si $U : \mathcal{V} \to \mathcal{W}$ es un operador unitario, con $B = \{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ una base ortonomal de $\mathcal{V}$, entonces

$$B' = \{U|v_1\rangle, U|v_2\rangle, \ldots, U|v_n\rangle\},$$

es una base ortonormal de $\mathcal{W}$. En efecto,

$$\langle U|v_r\rangle\, |U|v_s\rangle\rangle = \langle v_r|v_s\rangle = \begin{cases} 1, & \text{si} \quad r = s, \\ 0, & \text{si} \quad r \neq s. \end{cases}$$

Más aún, se comprueba que todo operador lineal $A : \mathcal{V} \to \mathcal{W}$ que transforma bases ortonormales en bases ortonormales es un operador unitario. En efecto, Sea $A : \mathcal{V} \to \mathcal{W}$ un operador lineal que transforma la base ortonormal $B = \{|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle\}$ de $\mathcal{V}$ en la base ortonormal $B' = \{A|v_1\rangle, A|v_2\rangle, \ldots, A|v_n\rangle\}$ de $\mathcal{W}$.

Por lo tanto, $\langle A|v_r\rangle\, |A|v_s\rangle\rangle = \sigma_{rs}$ con $\sigma_{ss} = 1$ y $\sigma_{sr} = 0$ si $s \neq r$. De igual forma, $\langle v_r|v_s\rangle = \sigma_{rs}$ con $\sigma_{ss} = 1$ y $\sigma_{sr} = 0$ si $s \neq r$. En consecuencia,

$$\langle A|v_r\rangle\, |A|v_s\rangle\rangle = \langle v_r|v_s\rangle,$$
$$\langle AA^\dagger|v_r\rangle\, |v_s\rangle = \langle v_r|v_s\rangle.$$

de donde se deduce $AA^\dagger = I$, probándose así que A es un operador unitario.

Entre los muchos casos presentes de operadores unitarios definidos en $\mathbb{C}^2$ destacamos dos en particular. El primer caso es un grupo de matrices conocidas como las ***Matrices de Pauli***

$$\sigma_x \equiv X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y \equiv Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{y} \quad \sigma_z \equiv Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

El segundo caso es el ***operador de Hadamard*** cuya matriz que lo representa en la base $\mathcal{B}_E$ está dada por

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

Se comprueba que esta matriz es unitaria, en efecto,

$$HH^\dagger = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I.$$

1.2.3. Valores y vectores propios

Sea $A \in \mathbb{M}_{m\times m}(\mathbb{C})$. Se dice que $\lambda \in \mathbb{C}$, es un *valor propio de* A si existe algún vector $|v\rangle \in C^m$, no nulo ($|v\rangle \neq \mathbf{0}$), que cumple la siguiente ecuación vectorial

$$A\,|v\rangle = \lambda\,|v\rangle\,. \tag{1.3}$$

Al vector $|v\rangle$ que satisface (1.3) se le identifica como *vector propio de* A, asociado al valor propio λ. De otro lado, cada valor propio de A puede tener uno o varios vectores propios asociados; en particular, se define el *espacio propio asociado al valor propio* λ *de* A al subespacio vectorial

$$E_\lambda = \{|v\rangle \in \mathbb{C}^m : (A - \lambda I)\,|v\rangle = 0\}\,.$$

Veamos algunas de las propiedades más destacadas de los valores propios de matrices hermitianas.

Teorema 1. *Los valores propios de una matriz hermitiana son números reales.*

Demostración. Sea $A \in \mathbb{M}_{m\times m}(\mathbb{C})$ hermitiana y $\lambda \in \mathbb{C}$ un valor propio de A con $|v\rangle \in \mathbb{C}^m$ un vector propio asociado a λ. Entonces

$$A\,|v\rangle = \lambda\,|v\rangle \quad \Rightarrow \quad (A\,|v\rangle)^\dagger = (\lambda\,|v\rangle)^\dagger \quad \Leftrightarrow \quad \langle v|\,A^\dagger = \overline{\lambda}\,\langle v|\,.$$

Multiplicando por $|v\rangle$ y dado que $A = A^\dagger$ se cumple

$$\langle v|A|v\rangle = \langle A\,|v\rangle\,|v\rangle,$$

pero $A\,|v\rangle = \lambda\,|v\rangle$, luego

$$\lambda\langle v|v\rangle = \overline{\lambda}\langle v|v\rangle,$$

luego $\lambda = \overline{\lambda}$, por lo tanto, λ es un número real. □

Teorema 2. *Sea* $A \in \mathbb{M}_{m\times m}(\mathbb{C})$ *una matriz hermitiana. Sean* $\lambda_1 \neq \lambda_2$ *valores propios de* A*. Entonces, los correspondientes espacios propios* E_{λ_1} *y* E_{λ_2} *son espacios ortogonales entre sí.*

Demostración. Sean E_{λ_r} el espacio propio asociado al valor propio λ_r. Considere $|v_1\rangle \in E_{\lambda_1}$, y $|v_2\rangle \in E_{\lambda_2}$ arbitrarios. Entonces:

$$\begin{aligned}\lambda_1\langle v_1|v_2\rangle &= \langle \lambda_1 v_1|v_2\rangle = \langle Av_1|v_2\rangle,\\ &= \langle v_1|A^\dagger v_2\rangle = \langle v_1|Av_2\rangle,\\ &= \langle v_1|\lambda_2 v_2\rangle = \lambda_2\langle v_1|v_2\rangle.\end{aligned}$$

Ahora bien, puesto que $\lambda_1 \neq \lambda_2$, se deduce que

$$\big(\lambda_1 - \lambda_2\big)\langle v_1|v_2\rangle = 0, \quad \Rightarrow \quad \langle v_1|v_2\rangle = 0.$$

Probándose así que E_{λ_1} y E_{λ_2} son espacios vectoriales ortogonales entre si. □

Ejemplo 6. *Considere la siguiente matriz*

$$A = \begin{pmatrix} 2 & 1+i & 0 \\ 1-i & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Es claro que A es hermitiana, es decir, $A = A^\dagger$. Los respectivos valores propios son todos reales y dados por

$$\lambda_1 = 1, \quad \lambda_2 = 4 \quad y \quad \lambda_3 = 4.$$

De estos valores propios, hállese los respectivos vectores propios asociados.

$$|v_1\rangle = \begin{pmatrix} -1-i \\ 1 \\ 0 \end{pmatrix} \quad |v_2\rangle = \begin{pmatrix} \frac{1}{2}+\frac{1}{2}i \\ 1 \\ 0 \end{pmatrix}, \quad y \quad |v_3\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

Se comprueba directamente que $\langle v_1|v_2\rangle = 0$, $\langle v_1|v_3\rangle = 0$ y $\langle v_2|v_3\rangle = 0$, mostrándose así que todos los espacios propios son ortogonales entre sí.

De los valores y vectores propios en matrices hermitianas también se construye una relación que define una manera de escribir operadores hermitianos en términos de sus valores y vectores propios asociados. En efecto, sea $A : \mathcal{V} \to \mathcal{V}$ un operador hermitiano. Sea el teorema:

Teorema 3. *(Teorema espectral para matrices hermitianas) Sea A una matriz hermitiana $A \in \mathbb{M}_{m\times m}$. Entonces existe una base ortonormal para $\mathbb{C}^m$ constituida por vectores propios de A. En forma equivalente, si A es hermitiana, existe una matriz unitaria U tal que $U^{-1}AU$ es una matriz diagonal (A es unitariamente semejante a una matriz diagonal)*

Demostración. La prueba de este importante resultado se puede consultar en diversos libros de álgebra lineal. Presentamos una demostración usando el Lema de Schur [5], el cual afirma la existencia de una matriz unitaria U tal que la matriz $S = U^\dagger AU$ es triangular superior. Como A es hermitiana, entonces S también lo es, en efecto

$$\begin{aligned}(S^*)^T &= [(U^\dagger AU)^*]^T,\\ &= [(AU)^*]^T[(U^\dagger)^*]^T = [(U)^*]^T[(A)^*]^T[(U^\dagger)^*]^T,\\ S^\dagger &= U^\dagger A[U^\dagger]^\dagger = U^\dagger AU = S.\end{aligned}$$

Como S es triangular, entonces debe ser diagonal. □

Ejemplo 7. *Considere la siguiente matriz hermitiana*

$$A = \begin{pmatrix} \frac{5}{4} & 0 \\ 0 & \frac{3}{4} \end{pmatrix}.$$

Es fácil ver que los valores propios correspondientes son $\lambda_1 = \frac{5}{4}$, $\lambda_2 = \frac{3}{4}$ *y sus vectores propios asociados* $|0\rangle$ *y* $|1\rangle$ *respectivamente, forman una base en* $\mathbb{C}^2$*. Pero además, un cálculo directo muestra que la matriz unitaria* U *que cumple el Lema de Schur es:*

$$U = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

El teorema espectral nos garantiza la existencia de una base ortonormal $B_{\mathcal{V}} = \{|u_s\rangle\}$ conformada por los vectores propios asociados al operador A, esto es:

$$A\,|u_s\rangle = \lambda_s\,|u_s\rangle\,,$$

en donde $|u_s\rangle$ es un vector propio asociado al valor propio λ_s del operador A. En tal caso, por la relación de completitud, se tiene:

$$A = \sum_{rs} \langle u_s|A|u_r\rangle\,|u_s\rangle\,\langle u_r| = \sum_{rs} \langle A^\dagger\,|u_s\rangle\,|u_r\rangle\,|u_s\rangle\,\langle u_r|\,,$$
$$A = \sum_{rs} \langle A\,|u_s\rangle\,|u_r\rangle\,|u_s\rangle\,\langle u_r| = \sum_{rs} \lambda_s\langle u_s|u_r\rangle\,|u_s\rangle\,\langle u_r|\,,$$

obteniendo eventualmente la expresión

$$A = \sum_r \lambda_r\,|u_r\rangle\,\langle u_r|\,,$$

que define una forma de expresar un operador hermitiano como combinación lineal de productos externos de sus vectores propios asociados, esto bajo la base estándar y sobre los vectores propios normalizados. Más aún, si A es invertible, es simple comprobar que A^{-1} se puede expresar en la forma

$$A^{-1} = \sum_r \lambda_r^{-1}\,|u_r\rangle\,\langle u_r|\,.$$

En efecto, sea A una matriz hermitiana, $\lambda \in \mathbb{C}$ un valor propio y $|v\rangle$ su vector propio asociado, luego por definición y dado que A es invertible ($\lambda \neq 0$) tenemos:

$$A\,|v\rangle = \lambda\,|v\rangle \;\Rightarrow\; A^{-1}A\,|v\rangle = \lambda A^{-1}\,|v\rangle \;\Rightarrow\; \lambda^{-1}\,|v\rangle = A^{-1}\,|v\rangle\,.$$

Lo anterior muestra que si $\lambda \neq 0$ es un valor propio de A, la matriz A^{-1} tiene a λ^{-1} como valor propio, con el mismo vector propio asociado $|v\rangle$ de λ, esto es, tanto λ como λ^{-1} comparten el mismo vector propio asociado, justificando la expresión

$$A^{-1} = \sum_r \lambda_r^{-1}\,|u_r\rangle\,\langle u_r|\,.$$

Así por ejemplo, el sistema lineal $A\,|x\rangle = |b\rangle$ con $|b\rangle = \sum_s b_s\,|u_s\rangle$ tiene solución única

$$\begin{aligned} |x\rangle = A^{-1}\,|b\rangle &= \Big(\sum_r \lambda_r^{-1}\,|u_r\rangle\,\langle u_r|\Big)\Big(\sum_s b_s\,|u_s\rangle\Big), \\ &= \sum_{r,s} \lambda_r^{-1} b_s \langle u_r|u_s\rangle\,|u_r\rangle = \sum_r \lambda_r^{-1} b_r\,|u_r\rangle\,. \end{aligned} \tag{1.4}$$

Ejemplo 8. *Considere la matriz hermitiana*

$$A = \begin{pmatrix} 2 & 1+i \\ 1-i & 3 \end{pmatrix}.$$

Un cálculo directo comprueba que sus valores propios son $\lambda_1 = 4$, $\lambda_2 = 1$ *con vectores propios asociados. Los correspondientes espacios propios* E_{λ_1} *y* E_{λ_2} *están generados por los vectores*

$$|s_1\rangle = \begin{pmatrix} 1 \\ 1-i \end{pmatrix} \quad y \quad |s_2\rangle = \begin{pmatrix} -(1+i) \\ 1 \end{pmatrix},$$

respectivamente. Es claro, y como ha de esperarse que $\langle s_1|s_2\rangle = 0$. *Ahora bien, elegimos los vectores ortogonales*

$$|v_1\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1-i \end{pmatrix} \quad y \quad |v_2\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} -(1+i) \\ 1 \end{pmatrix}.$$

Definamos la matriz $U = [|v_1\rangle \ |v_2\rangle]$ *y su inversa* U^{-1} *dadas explícitamente por*

$$U = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & -(1+i) \\ 1-i & 1 \end{pmatrix} \quad y \quad U^{-1} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1+i \\ -(1-i) & 1 \end{pmatrix},$$

Note que $U^{-1} = U^{\dagger}$, *es decir,* U *es una matriz unitaria. Más aún:*

$$U^{-1}AU = \frac{1}{3} \begin{pmatrix} 1 & 1+i \\ -(1-i) & 1 \end{pmatrix} \begin{pmatrix} 2 & 1+i \\ 1-i & 3 \end{pmatrix} \begin{pmatrix} 1 & -(1+i) \\ 1-i & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix},$$

verificándose así el teorema espectral 3. Es fácil comprobar que $A = \lambda_1 |v_1\rangle \langle v_1| + \lambda_2 |v_2\rangle \langle v_2|$. *En efecto, para la aplicación lineal* $|v_1\rangle \langle v_1|$ *se cumple*

$$|v_1\rangle \langle v_1| (|0\rangle) = \frac{1}{3} \begin{pmatrix} 1 \\ 1-i \end{pmatrix}, \qquad |v_1\rangle \langle v_1| (|1\rangle) = \frac{1}{3} \begin{pmatrix} 1+i \\ 2 \end{pmatrix},$$

mientras que para la aplicación lineal $|v_2\rangle \langle v_2|$ *tenemos*

$$|v_2\rangle \langle v_2| (|0\rangle) = \frac{1}{3} \begin{pmatrix} 2 \\ -(1-i) \end{pmatrix}, \qquad |v_2\rangle \langle v_2| (|1\rangle) = \frac{1}{3} \begin{pmatrix} -(1+i) \\ 1 \end{pmatrix}.$$

A partir de aquí se deduce:

$$|v_1\rangle \langle v_1| := \frac{1}{3} \begin{pmatrix} 1 & 1+i \\ 1-i & 2 \end{pmatrix} \quad y \quad |v_2\rangle \langle v_2| := \frac{1}{3} \begin{pmatrix} 2 & -(1+i) \\ -(1-i) & 1 \end{pmatrix},$$

y así obtenemos

$$\begin{pmatrix} 2 & 1+i \\ 1-i & 3 \end{pmatrix} = 4 |v_1\rangle \langle v_1| + |v_2\rangle \langle v_2|.$$

Así mismo, se demuestra que y por consecuencia, que $A^{-1} = \lambda_1^{-1} |v_1\rangle \langle v_1| + \lambda_2^{-1} |v_2\rangle \langle v_2|$ *y que su inversa es*

$$A^{-1} = \frac{1}{4} \begin{pmatrix} 3 & -(1+i) \\ -(1-i) & 2 \end{pmatrix} = \lambda_1^{-1} |v_1\rangle \langle v_1| + \lambda_2^{-1} |v_2\rangle \langle v_2|.$$

.

1.3. Conclusiones

La teoría de matrices y los números complejos son la parte de la estructura matemática fundamental de la computación cuántica. En particular, y como veremos más adelante, el teorema espectral para matrices hermitianas es una de las piedras angulares en la construcción de algunos de los más recientes e importantes algoritmos cuánticos, entre ellos, el algoritmo de Kitaev (ver [2]) y el algoritmo HHL (ver [1]). Se considera de igual forma que las definiciones anteriores son necesarias a la hora de introducirse formalmente en el mundo de la computación cuántica. En el siguiente capítulo se explora mejor esta introducción y qué es lo más importante a tener en cuenta, por ejemplo, cuando se explora la unidad básica de información en sistemas cuánticos.

Capítulo 2

Cúbits y la esfera de Bloch

El presente capítulo, inspirado en [2, 6, 7] introduce algunos conceptos básicos relacionados con la unidad fundamental de información que se maneja en los sistemas cuánticos, el *bit cuántico* (del inglés quantum bit) o en forma abreviada *cúbit* (qubit). Comenzamos con una interpretación de un cúbit desde la Física, mediante la descripción del un fenómeno físico conocido como la *polarización de un fotón*. Seguidamente, daremos una representación matemática de los posibles estados de un cúbit por medio de la *Esfera de Bloch*, y finalizamos definiendo los diversos espacios que pueden formarse al aplicar ciertos operadores entre uno o más cúbits. Esencialmente, el lector puede interpretar el propósito de este capítulo como el de introducir los primeros conceptos sobre sistemas y circuitos cuánticos.

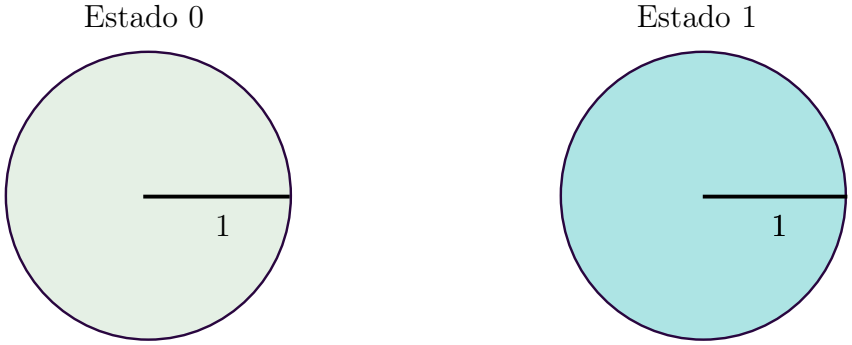

Figura 2.1: Representación esquemática de dos caras de una moneda (de radio 1) como ejemplo de un bit: un sistema físico con dos únicos estados posibles $\{0, 1\}$.

2.1. Un bit, un fotón ... un cúbit

En informática, cuando se habla de un *bit*, pensamos en la representación sobre un caso cualquiera de elección entre dos estados igualmente probables. Un ejemplo de esto serían los "posibles estados" en que puede estar una moneda: estado 0 (cara) o estado 1 (sello), como se muestra en la Figura 2.1. En computación clásica, un bit es la unidad mínima de información que se emplea en la teoría de la información para representar sistemas sustentados en un código binario, con dígitos 0 y 1. Los bits pueden agruparse para obtener distintas combinaciones. Así, por ejemplo, un modelo de 2-bits tiene 4 posibles estados, y un modelo de 8-bits tiene 256 posibles estados. Sin embargo, ¿qué ocurre cuando ya

no pensamos en sistemas clásicos? ¿Qué podemos decir o definir cuando consideramos sistemas cuánticos? Se podría pensar que en este tipo de sistemas ya no se manejan bits clásicos y que, en vez de eso, se maneja lo que se conoce como bit cuántico o cubit, pero ¿qué es un cubit?
Frente a estas preguntas podemos iniciar dando una respuesta conveniente como la siguiente: Un bit cuántico o *cúbit* es un objeto matemático con ciertas propiedades que extiende el concepto de bit de la computación clásica a la emergente teoría de la computación cuántica. Sin embargo, muy posiblemente lo ambiguo en esta definición todavía genere problemas para concluir concretamente lo que es un cubit en realidad. Es por ello que presentamos la siguiente y elegante visualización física del concepto de cúbit presentada en [7] aplicando una analogía frente al fenómeno físico que describe la polarización de un fotón.

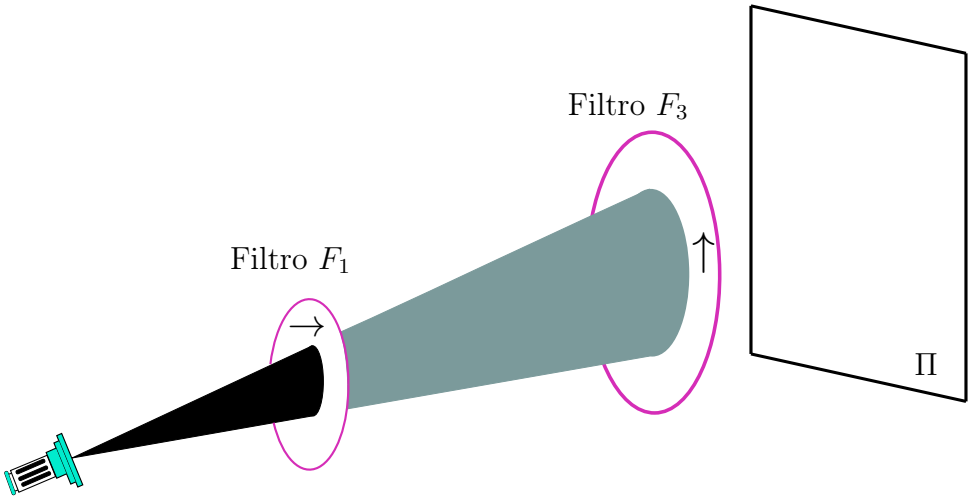

Figura 2.2: Representación esquemática de un rayo de luz que pasa por dos filtros con direcciones preferentes horizontal ($\rightarrow$) y vertical ($\uparrow$) respectivamente.

2.1.1. Polarización de un fotón

Considérese una fuente de luz (digamos un rayo láser) que apunta a una superficie plana y fija (pantalla) denotada Π. A continuación, se colocan dos filtros ópticos polarizadores denotados F_1 y F_3 entre la fuente de luz y la pantalla. El filtro F_1 en dirección horizontal ($\rightarrow$) ubicado entre la fuente de luz y el filtro F_3. Como es de esperar, la intensidad de la luz sobre la pantalla es ahora reducida y dependerá de la dirección en la que apunte el filtro F_3. Por ejemplo, si este último está en dirección vertical ($\uparrow$) (ver Figura 2.2), el rayo de luz no alcanza la pantalla. Continuamos el experimento dejando el filtro F_3 en dirección vertical y ubicando un filtro adicional denotado F_2 entre F_1 y F_3 en una dirección de θ. Para la mayoría de los ángulos θ se observa que el rayo de luz vuelve a alcanzar la pantalla (ver Figura 2.3). Más aún, se puede observar experimentalmente que la intensidad de la luz que pasa por los tres filtros es máxima si la dirección del filtro F_2 es diagonal ($\nearrow$, es decir, con $\theta = \pi/4$).

¿Cómo se explica el fenómeno anterior? La mecánica cuántica brinda una explicación a este experimento y da, a falta de una mejor palabra, una elegante respuesta. Considérese dos etapas: Primero, se modela el estado de polarización de un fotón y, segundo, se modela la interacción del fotón y cada filtro polarizador.

En la primera etapa, el estado de polarización de un fotón se modela representándolo por medio de un vector unitario, apuntando en una apropiada dirección. Las direcciones vertical ($\uparrow$) y horizontal ($\rightarrow$) se representan con los vectores de la base estándar $|0\rangle$ y $|1\rangle$ respectivamente. Así, una arbitraria polarización $|v\rangle$ de un rayo de luz se puede representar por medio de la combinación lineal.

$$|v\rangle = a\,|0\rangle + b\,|1\rangle\,,$$

con $a, b \in \mathbb{C}$. (llamados *amplitudes de* $|v\rangle$) seleccionados específicamente para satisfacer la condición:

$$|a|^2 + |b|^2 = 1.$$

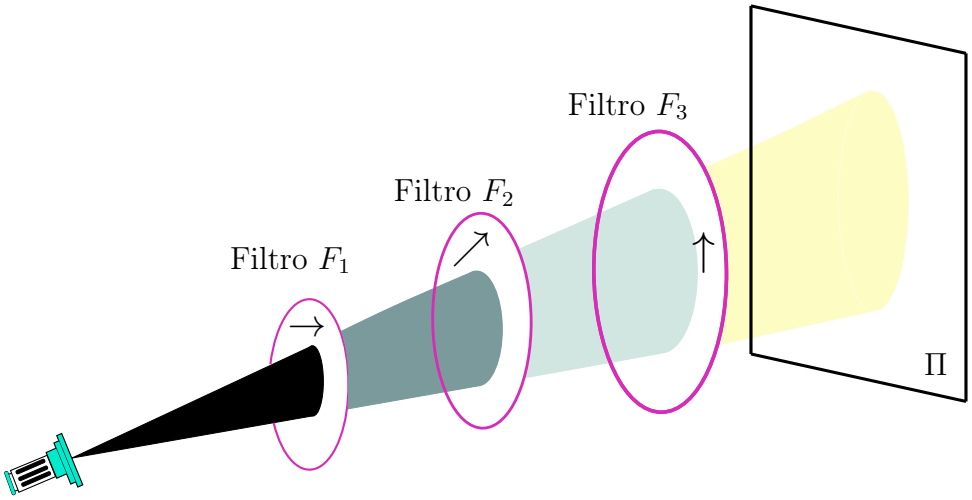

Figura 2.3: Representación esquemática de un rayo de luz que pasa por tres filtros con direcciones preferentes horizontal ($\rightarrow$), diagonal ($\nearrow$) y vertical ($\uparrow$) respectivamente.

Cuando $a, b \neq 0$, se dice que $|v\rangle$ es una *superposición* de los estados base $|0\rangle$ y $|1\rangle$. Ahora bien, cada filtro polarizador tiene una dirección preferente de polarización. Si un fotón con dirección preferente $|v\rangle$ colisiona con un filtro polarizador con dirección preferente $|0\rangle$ el fotón lo atravesará con probabilidad $|a|^2$ y será absorbido con probabilidad $|b|^2$. Explicando mejor lo anterior, la probabilidad de que un fotón atraviese el filtro es el cuadrado de la magnitud de la amplitud de su polarización en la dirección preferente del filtro y la probabilidad de que el fotón sea absorbido es el cuadrado de la magnitud de la amplitud en la dirección ortogonal al eje preferente del filtro. Además, cualquier fotón que atraviese un determinado filtro ahora estará polarizado en la dirección preferente del mismo. *Esta naturaleza probabilística de la interacción y el cambio de estado resultante son características de todas las interacciones entre cúbits y dispositivos de medición*. Más adelante exploraremos mejor estas interacciones y su naturaleza probabilística. De momento, continuemos con el experimento:

Cuando un fotón atraviesa el filtro F_1, este queda polarizado con dirección preferente $|1\rangle$ como se mencionó anteriormente. Posteriormente, dicho fotón colisiona ahora en el filtro F_2, para el cual suponemos que tiene dirección preferente ($\nearrow$), es decir, en la dirección $|H^{\nearrow}\rangle$. Un cálculo directo muestra que

$$|1\rangle = \frac{1}{\sqrt{2}}\,|H^{\nearrow}\rangle - \frac{1}{\sqrt{2}}\,|H^{\nwarrow}\rangle\,.$$

Por ende, luego de atravesar el filtro F_1, la probabilidad de que el fotón atraviese ahora el filtro F_2 es $\left(1/\sqrt{2}\right)^2 = 1/2$. Ahora, después de atravesar el filtro F_2, el fotón queda polarizado con dirección preferente $|H^{\nearrow}\rangle$. Posteriormente, el fotón colisionará con la pantalla en la dirección preferente. $|0\rangle$. pero sabemos que

$$|H^{\nearrow}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

Así que la probabilidad de que atraviese el filtro F_3 es $\left(1/\sqrt{2}\right)^2 = 1/2$. Por último, note que en ausencia del filtro F_2, un fotón que atraviesa el filtro F_1 no tendría posibilidad de atravesar el filtro F_3, ya que la amplitud de su polarización en la dirección $|0\rangle$ (dirección preferente del filtro F_3) es cero. De esta manera, la mecánica cuántica permite explicar la interacción de un fotón por medio de un apropiado uso de vectores unitarios.

Tomando en cuenta el anterior experimento, nos volvemos a preguntar: ¿Qué es un cúbit? Pues bien, el espacio de los posibles estados [1] de polarización de un fotón es un ejemplo de cúbit. Así pues, *cualquier sistema mecánico cuántico que pueda modelarse mediante un espacio vectorial complejo bidimensional puede ser visto como un cúbit.* A dichos sistemas se les conoce como *sistemas cuánticos de dos estados*, por ejemplo, el espín de un electrón y la polarización de un fotón. Es importante resaltar que "dos estados"no significa que el espacio de estados del sistema cuántico presente tan solo dos estados posibles; por el contrario, presenta *un continuo de estados posibles*, los cuales pueden escribirse como una combinación lineal, o superposición, de solo dos estados, denotados estados base. Es decir, cada estado puede representarse por un vector unitario de la forma $|v\rangle = a|0\rangle + b|1\rangle$ en este caso para los vectores $|0\rangle$ y $|1\rangle$. Cabe aclarar además que los dos estados base deben quedar prefijados previamente durante todo el análisis, deben ser linealmente independientes y, por último, deben formar una base en $\mathbb{C}^2$, en el caso del fotón, dicha base es $\mathcal{B}_E = \{|0\rangle, |1\rangle\}$.

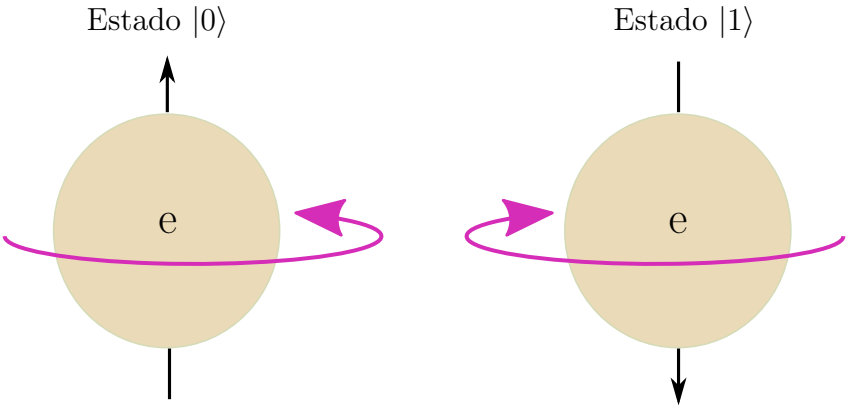

Figura 2.4: Representación esquemática de los estados fundamentales del espín de un electrón e.

Por ejemplo, moviéndonos al caso del espín de un electrón. (ver Figura 2.4)

$$|0\rangle := |\uparrow\rangle \quad \text{(spin arriba)}, \qquad |1\rangle := |\downarrow\rangle \quad \text{(spin abajo)}.$$

[1] En cualquier sistema físico, al conjunto de sus posibles estados se conoce como *espacio de estados del sistema.*

Para el caso de la polarización de un fotón presentada anteriormente, tenemos

$$|0\rangle := |\uparrow\rangle \quad \text{(dirección vertical)}, \qquad |1\rangle := |\rightarrow\rangle \quad \text{(dirección horizontal)}.$$

En resumen, cuando se habla de un cúbit, sus estados se representan vectorialmente (en este caso bajo la base $\mathcal{B}_E$) en la forma $|v\rangle = a\,|0\rangle + b\,|1\rangle$ y bajo la condición de amplitud $|a|^2 + |b|^2 = 1$. Más aún, dos estados $|v\rangle$ y $|\tilde{v}\rangle$:

$$|v\rangle = a\,|0\rangle + b\,|1\rangle \quad \text{y} \quad |\tilde{v}\rangle = \tilde{a}\,|0\rangle + \tilde{b}\,|1\rangle\,,$$

representan *el mismo estado cuántico* si existe $c \in \mathbb{C}$ con $|c| = 1$ tal que

$$a\,|0\rangle + b\,|1\rangle = c(\tilde{a}\,|0\rangle + \tilde{b}\,|1\rangle) \quad \Leftrightarrow \quad |v\rangle = c\,|\tilde{v}\rangle\,,$$

lo que permite definir en $\mathbb{C}^2$ la siguiente relación de equivalencia

$$|v\rangle \sim |\tilde{v}\rangle \quad \equiv \quad |v\rangle = c\,|\tilde{v}\rangle\,, \quad \text{para algún} \quad c = e^{i\phi}, \quad \phi \in \mathbb{R}.$$

En adelante, al espacio vectorial $\mathbb{C}^2$ bajo la relación de equivalencia $\sim$ lo identificaremos como el *espacio complejo proyectivo de dimensión uno*, y se denotará por $\mathbf{CP}^1$, esto es

$$\mathbf{CP}^1 = \{a\,|0\rangle + b\,|1\rangle\} \,/\, \sim$$

En este punto conviene resaltar que a $\mathbf{CP}^1$ podemos darle la interpretación geométrica de una esfera. Veamos esto con un poco más de detalle.

2.1.2. La esfera de Bloch

Considérese la siguiente correspondencia entre $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ y un estado

$$\beta \mapsto \begin{cases} \frac{1}{\sqrt{1+|\beta|^2}}\,|0\rangle + \frac{\beta}{\sqrt{1+|\beta|^2}}\,|1\rangle & \text{si} \quad \beta \neq \infty, \\ |1\rangle \quad \text{si} \quad \beta = \infty, \end{cases}$$

cuya inversa está dada por

$$a\,|0\rangle + b\,|1\rangle \mapsto \begin{cases} b/a := \beta, & \text{si} \quad a \neq 0, \\ \infty \quad \text{si} \quad a = 0,\ b = 1. \end{cases}$$

Para cada punto en $\overline{\mathbb{C}}$ (cuyos elementos ahora son estados de un cúbit), se les puede definir una correspondencia uno a uno con la esfera S^2 por medio de la proyección estereográfica (inversa) $\mathcal{S} : \overline{\mathbb{C}} \mapsto S^2$, definida de la siguiente forma:

$$\mathcal{S}(\beta) = \begin{cases} \left(\frac{2r}{1+|\beta|^2}, \frac{2s}{1+|\beta|^2}, \frac{1-|\beta|^2}{1+|\beta|^2}\right), & \text{si} \quad \beta = r + si \neq \infty, \\ (0,0,-1), & \text{si} \quad \beta = \infty. \end{cases}$$

Ejemplo 9. *Sean los siguientes estados:*

$$|\boldsymbol{i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \quad y \quad |\text{-}\boldsymbol{i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle).$$

Aplicando la correspondencia, tenemos que para $|\boldsymbol{i}\rangle$ se define $\beta = i$ y para $|\text{-}\boldsymbol{i}\rangle$ se define $\beta = -i$. Gracias a $\mathcal{S}$, los puntos de la esfera asociados a los estados $|\boldsymbol{i}\rangle$ y $|\text{-}\boldsymbol{i}\rangle$ respectivos son $(0,1,0)$ y $(0,-1,0)$. Así mismo, un cálculo directo comprueba las siguientes asignaciones.

$$\begin{aligned} |0\rangle &\mapsto (0,0,1), & |H^{\nearrow}\rangle &\mapsto (1,0,0), \\ |1\rangle &\mapsto (0,0,-1) & |H^{\nwarrow}\rangle &\mapsto (-1,0,0). \end{aligned}$$

Esta representación geométrica de un sistema cuántico de dos estados como puntos de una esfera unitaria se conoce como la *esfera de Bloch*. A continuación se plantea una formulación matemática concreta utilizando coordenadas polares. Dicha formulación parte de la forma de visualizar la esfera de Bloch planteada por el profesor O. Perdomo en `https://www.youtube.com/watch?v=F5b17pOsWPk&t=255s`, explicada a continuación:

Considérese una moneda de dos caras, de tal forma que en cada cara hay un segmento de longitud a y b respectivamente, para cada lado. Nótese que los estados fundamentales

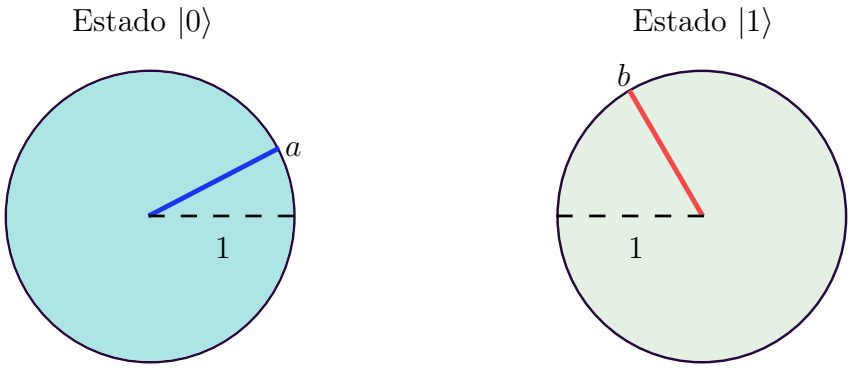

Figura 2.5: Representación esquemática de los estados fundamentales en un cúbit, como caras de una moneda (de radio 1). En cada estado fundamental, ubicamos un número complejo a, b (en forma aleatoria) con módulo $|a| = 1$, $|b| = 1$ respectivamente.

$|0\rangle$, $|1\rangle$ de un cúbit se pueden visualizar como las caras de una moneda cualquiera (de radio 1), como se muestra en la Figura 2.5. De otro lado, los posibles estados en un cúbit que se expresan como superposición de los estados fundamentales se pueden visualizar como nuestra moneda (de radio 1), la cual, en una cara, tiene dibujado un segmento de longitud $|a|$ y la otra un segmento de longitud $|b|$ los cuales satisfacen $|a|^2 + |b|^2 = 1$. Cada segmento representa un número complejo a y b ubicados aleatoriamente.

A continuación, imagínese que nuestra moneda se guarda en una caja negra, la cual se agita antes de volver a abrirse para sacar de nuevo y observar solo uno de los lados de la moneda. Pues bien, $|a|^2$ es la probabilidad de que al ver nuestra moneda, ella esté en la cara que representa el estado $|0\rangle$ y $|b|^2$ es la probabilidad de que al ver nuestra moneda, ella esté en la cara que representa el estado $|1\rangle$. Por ejemplo, si nuestra moneda representa el estado

$$|v\rangle = \left(\frac{1}{5} + \frac{2}{5}i\right)|0\rangle + \left(\frac{2}{\sqrt{5}}\right)|1\rangle .$$

Entonces la probabilidad $|a|^2 = 1/5$ implica que el 20 % de las veces se observará nuestra moneda por la cara que representa el estado $|0\rangle$, mientras que la probabilidad $|b|^2 = 4/5$ representa el 80 % de las veces que se observará la moneda por la cara que representa el estado $|1\rangle$.

Siguiendo la idea anterior, dada una moneda representante de un estado en superposición $|v\rangle = a\,|0\rangle + b\,|1\rangle$, lo podemos escribir de forma equivalente usando coordenadas polares, por medio de la siguiente expresión

$$|v\rangle = a\,|0\rangle + b\,|1\rangle = r_a e^{i\theta_a}\,|0\rangle + r_b e^{i\theta_b}\,|1\rangle ,$$

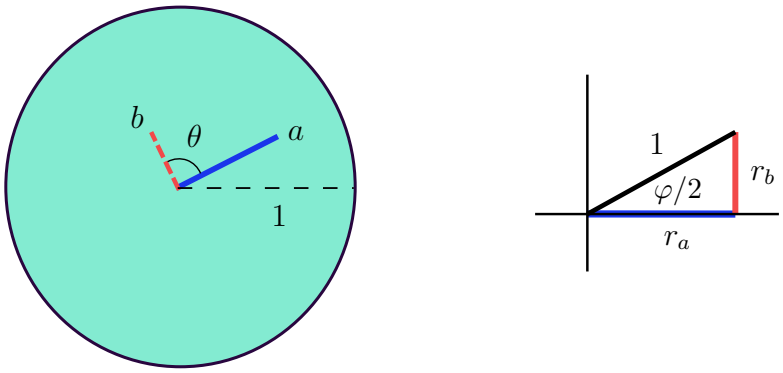

Figura 2.6: (Izq.) Representación esquemática de un estado $|v\rangle = a\,|0\rangle + b\,|1\rangle$ como superposición de los estados fundamentales $|0\rangle$ y $|1\rangle$ de un cúbit. En cada lado, de nuestra moneda (de radio 1) ubicamos un número complejo a, b (en forma aleatoria) con módulo $|a| = r_a$, $|b| = r_b$, y que además satisfacen $r_a^2 + r_b^2 = 1$. El número complejo $\beta = b/a$ se escribe en forma polar $\beta = |\beta|e^{i\theta}$ con $\theta \in [0, 2\pi]$. (Der.) Relación entre el ángulo φ y los segmentos r_a y r_b.

donde

$$a = r_a e^{i\theta_a} \quad \text{y} \quad b = r_b e^{i\theta_b},$$

con $r_a, r_b \in \mathbb{R}$ y $\theta_a, \theta_b \in \mathbb{R}$, los respectivos módulos y argumentos de a y b. Ahora, de la relación de equivalencia entre estados cuánticos, podemos multiplicar por el número complejo $e^{-i\theta_a}$ (de módulo 1) y obtener (aplicando un cálculo rápido).

$$|v\rangle \sim |\tilde{v}\rangle \quad \text{con} \quad |\tilde{v}\rangle = r_a\,|0\rangle + r_b e^{i(\theta_b - \theta_a)}\,|1\rangle\,.$$

A continuación, se define (ver Figura 2.6)

$$\varphi = 2\arccos r_a = 2\arcsin r_b, \quad \text{y} \quad \theta = \theta_b - \theta_a, \quad \varphi \in [0, \pi], \quad \theta \in [0, 2\pi].$$

Lo anterior se cumple gracias a la condición de amplitud ($|a|^2 + |b|^2 = 1$) para $r_a = |a|$ y $r_b = |b|$. De esta forma se obtiene la siguiente equivalencia para nuestra superposición $|v\rangle$:

$$|\tilde{v}\rangle = \cos\frac{\varphi}{2}\,|0\rangle + \sin\frac{\varphi}{2}e^{i\theta}\,|1\rangle\,, \qquad \varphi \in [0, \pi], \quad \theta \in [0, 2\pi].$$

En este punto, abrimos un paréntesis para recordar que todas *las propiedades físicas de un estado no cambian bajo la relación de equivalencia*. Esto justifica el por qué podemos identificar cada estado en la esfera de Bloch de la forma anterior. Luego

$$|v\rangle \equiv \cos\frac{\varphi}{2}\,|0\rangle + \sin\frac{\varphi}{2}e^{i\theta}\,|1\rangle\,, \qquad \varphi \in [0, \pi], \quad \theta \in [0, 2\pi],$$

en consecuencia

$$|v\rangle \mapsto \begin{cases} \tan(\frac{\varphi}{2})\cos\theta + \tan(\frac{\varphi}{2})\sin\theta\, i := \beta, & \text{si} \quad \varphi \neq \pi, \\ \infty \quad \text{si} \quad \varphi = \pi,\ \theta = 0. \end{cases}$$

Finalmente, un cálculo directo muestra que $\mathcal{S}$ queda escrita de la forma:

$$\mathcal{S}(\beta) = \begin{cases} \big(\sin\varphi\cos\theta, \sin\varphi\sin\theta, \cos\varphi\big), & \text{si} \quad \varphi \neq \pi, \\ (0, 0, -1), & \text{si} \quad \varphi = \pi,\ \theta = 0, \end{cases}$$

lo que corresponde justamente a las conocidas coordenadas esféricas para el caso $\varphi \neq \pi$.

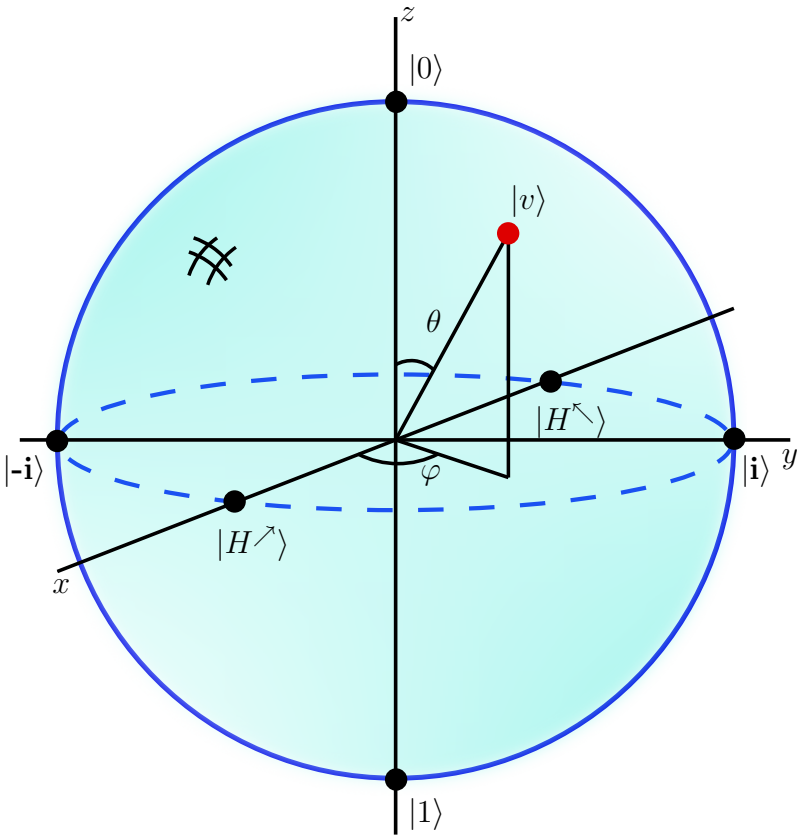

Figura 2.7: Representación gráfica de la esfera de Bloch.

Ejemplo 10. *Sean* $\varphi = \frac{\pi}{2}$ *y* $\theta = 0$. *Al evaluar en la expresión* $|v\rangle \equiv \cos\frac{\varphi}{2}|0\rangle + \sin\frac{\varphi}{2}e^{i\theta}|1\rangle$ *se tiene el estado*

$$|H^{\nearrow}\rangle = \cos\frac{\pi}{4}|0\rangle + \sin\frac{\pi}{4}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

representado por el punto $(1,0,0)$ *en la esfera de Bloch. Sean ahora* $\varphi = \frac{\pi}{2}$ *y* $\theta = \frac{\pi}{2}$. *Se tiene ahora el estado*

$$|\boldsymbol{i}\rangle = \cos\frac{\pi}{4}|0\rangle + \sin\frac{\pi}{4}e^{i\pi/2}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle,$$

representado por el punto $(0,1,0)$ *en la esfera de Bloch.*

2.2. De un cúbit a múltiples cúbits

Después de comprender un poco el concepto de lo que es un cúbit, a continuación consideramos sistemas formados no por uno, sino por varios cúbits, ya sean dos cúbits, tres cúbits y hasta, n-cúbits. Iniciemos definiendo algunos espacios vectoriales que serán fundamentales más adelante. Se comienza con la suma directa.

Definición 3. *(Suma Directa) Considérese dos espacios vectoriales* $\mathcal{V}$ *y* $\mathcal{W}$ *con bases*

$$\hat{\mathcal{B}}_V = \{|v_1\rangle, |v_1\rangle, \ldots, |v_n\rangle\} \quad y \quad \hat{\mathcal{B}}_W = \{|w_1\rangle, |w_1\rangle, \ldots, |w_m\rangle\},$$

respectivamente. La suma directa de $\mathcal{V}$ *y* $\mathcal{W}$ *es el espacio vectorial denotado por* $\mathcal{V} \oplus \mathcal{W}$ *cuya base es* $\hat{\mathcal{B}}_V \bigcup \hat{\mathcal{B}}_W$ *dada por*

$$\hat{\mathcal{B}}_V \bigcup \hat{\mathcal{B}}_W = \{|v_1\rangle, |v_1\rangle, \ldots, |v_n\rangle, |w_1\rangle, |w_1\rangle, \ldots, |w_m\rangle\}.$$

Así mismo, para los vectores $|r\rangle \in \mathcal{V}$ *y* $|s\rangle \in \mathcal{W}$

$$|r\rangle = \begin{pmatrix} r_1 \\ \ldots \\ r_n \end{pmatrix} \quad y \quad |s\rangle = \begin{pmatrix} s_1 \\ \ldots \\ s_m \end{pmatrix},$$

se define

$$|r\rangle \oplus |s\rangle = \begin{pmatrix} r_1 \\ \ldots \\ r_n \end{pmatrix} \oplus \begin{pmatrix} s_1 \\ \ldots \\ s_m \end{pmatrix} = \begin{pmatrix} r_1 \\ \ldots \\ r_n \\ s_1 \\ \ldots \\ s_m \end{pmatrix}.$$

De la definición anterior se deduce que:

- $\dim \mathcal{V} \oplus \mathcal{W} = \dim \mathcal{V} + \dim \mathcal{W} = n + m$.
- Cada elemento de $|z\rangle \in Z = \mathcal{V} \oplus \mathcal{W}$ se escribe en la forma $|z\rangle = |v\rangle \oplus |w\rangle$, para algún $|v\rangle$ y $|w\rangle$ en $\mathcal{V}$ y $\mathcal{W}$ respectivamente.

Así mismo, para este nuevo espacio vectorial $Z = \mathcal{V} \oplus \mathcal{W}$, también se define el operador producto interno dado por

$$(\langle v_2| \oplus \langle w_2|)(\langle v_1| \oplus \langle w_2|) := \langle v_2|v_1\rangle + \langle w_2|w_1\rangle.$$

En física, una de las aplicaciones de la suma directa se aprecia muy bien en la descripción de los posibles estados de un sistema mecánico usando la teoría de la mecánica clásica. Por ejemplo, si tenemos tres cuerpos P_1, P_2 y P_3 para los que se asume que sus respectivos estados están completamente descritos por dos variables, digamos x_i y p_i (posición y momentum de P_i), entonces el espacio de estado de todo el sistema se escribe en la forma

$$\begin{pmatrix} x_1 \\ p_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ p_2 \end{pmatrix} \oplus \begin{pmatrix} x_3 \\ p_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \\ x_3 \\ p_3 \end{pmatrix}.$$

En resumen y en forma general, el espacio de estados de N objetos clásicos, en donde cada uno es completamente caracterizado por un vector en un espacio bidimensional (dos parámetros), puede ser completamente descrito por un espacio vectorial $2N$-dimensional.

La aplicación de los espacios vectoriales formados por sumas directas no describe en su totalidad el tipo de espacio de estados de N sistemas cuánticos, por ende, se define el segundo espacio vectorial conocido como producto tensorial.

Definición 4. *(Producto tensorial) Considérese nuevamente dos espacios vectoriales $\mathcal{V}$ y $\mathcal{W}$ con bases*

$$\hat{\mathcal{B}}_V = \{|v_1\rangle, |v_1\rangle, \ldots, |v_n\rangle\} \quad y \quad \hat{\mathcal{B}}_W = \{|w_1\rangle, |w_1\rangle, \ldots, |w_m\rangle\},$$

el producto tensorial de $\mathcal{V}$ y $\mathcal{W}$ es el espacio vectorial denotado por $V \otimes W$ cuya base está conformada por nm-vectores de la forma $|v_r\rangle \otimes |w_s\rangle$, en donde $\otimes$ denota el producto tensorial, esto es, un operador binario que satisface:

†) *Para $|v_r\rangle$ en $\mathcal{V}$, $|w\rangle$ en $\mathcal{W}$ respectivamente, y $a \in \mathbb{C}$ se cumple:*

$$\begin{aligned}(a|v_1\rangle + |v_2\rangle) \otimes |w\rangle = (a|v_1\rangle) \otimes |w\rangle + |v_2\rangle \otimes |w\rangle = |v_1\rangle \otimes (a|w\rangle) + |v_2\rangle \otimes |w\rangle, \\ = a(|v_1\rangle \otimes |w\rangle) + |v_2\rangle \otimes |w\rangle.\end{aligned}$$

†) *Para $|v_1\rangle$ en $\mathcal{V}$, $|w_r\rangle$ en $\mathcal{W}$ respectivamente, se cumple:*

$$|v_1\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v_1\rangle \otimes |w_1\rangle + |v_1\rangle \otimes |w_2\rangle.$$

Así mismo, para los vectores $|r\rangle \in \mathcal{V}$ y $|s\rangle \in \mathcal{W}$

$$|r\rangle = \begin{pmatrix} r_1 \\ \ldots \\ r_n \end{pmatrix} \quad y \quad |s\rangle = \begin{pmatrix} s_1 \\ \ldots \\ s_m \end{pmatrix}.$$

Se define

$$|r\rangle \otimes |s\rangle = \begin{pmatrix} r_1|s\rangle \\ \ldots \\ r_n|s\rangle \end{pmatrix}.$$

De la definición anterior se concluye, además, que todos los elementos de $\mathcal{V} \otimes \mathcal{W}$ tienen la forma

$$|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle + \cdots + |v_k\rangle \otimes |w_k\rangle,$$

con $k = \min(n, m)$ para algúnos $|v_r\rangle \in \mathcal{V}$ y $|w_s\rangle \in \mathcal{W}$. Más aún, todos los elementos de $\mathcal{V} \otimes \mathcal{W}$ se pueden escribir en la forma

$$\alpha_1(|v_1\rangle \otimes |w_1\rangle) + \alpha_2(|v_2\rangle \otimes |w_2\rangle) + \cdots + \alpha_{nm}(|v_n\rangle \otimes |w_m\rangle).$$

Respetando la notación clásica para el producto tensorial, en adelante se escribe:

$$|v\rangle\,|w\rangle := |v\rangle \otimes |w\rangle.$$

Pero a partir de esta notación, definimos otra más compacta y comprensible para un estado en el producto tensorial de n-espacios vectoriales:

$$|\beta_{n-1}\beta_{n-2}\ldots\beta_1\beta_0\rangle := |\beta_{n-1}\rangle \otimes |\beta_{n-2}\rangle \otimes \ldots |\beta_1\rangle \otimes |\beta_0\rangle.$$

De esto se deduce a continuación la notación $|v\rangle^{\otimes k}$ que significa hacer el producto tensorial del $|v\rangle$ consigo mismo k-veces, es decir:

$$|v\rangle^{\otimes k} := |v\rangle \otimes |v\rangle \underbrace{\otimes \cdots \otimes |v\rangle \otimes |v\rangle}_{k-veces}.$$

Así por ejemplo, para el estado en un cúbit con base canónica $\mathcal{B}_E$, se tiene

$$|\nearrow\rangle^{\otimes 2} := |\nearrow\rangle \otimes |\nearrow\rangle = \frac{1}{\sqrt{2}^2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle), \quad \text{y} \quad |\nearrow\rangle^{\otimes 3} := |\nearrow\rangle \otimes |\nearrow\rangle \otimes |\nearrow\rangle = \ldots$$

Por último, se mencionan dos propiedades del espacio producto tensorial:

- ▷ Se comprueba directamente que $\dim(\mathcal{V}\otimes\mathcal{W}) = \dim(\mathcal{V})\cdot\dim(\mathcal{W})$. Por lo tanto, el producto tensorial entre n-espacios vectoriales de dos dimensiones tiene dimensión 2^n.

- ▷ Algunos (quizás la mayoría) de los estados en $\mathcal{V}\otimes\mathcal{W}$ *no se pueden expresar* como el producto tensorial entre un elemento en $\mathcal{V}$ y un elemento en $\mathcal{W}$. A dichos estados se les llama *estados entrelazados* (*entagled states*).

Ejemplo 11. *Sean $\mathcal{V}$ y $\mathcal{W}$ dos espacios vectoriales de dimensión dos con sus respectivas bases ortonormales.*

$$\hat{\mathcal{B}}_V = \{|v_0\rangle, |v_1\rangle\} \quad y \quad \hat{\mathcal{B}}_W = \{|w_0\rangle, |w_1\rangle\}.$$

Entonces, para $|v\rangle = a_0|v_0\rangle + a_1|v_1\rangle$ y $|w\rangle = b_0|w_0\rangle + b_1|w_1\rangle$ se tiene

$$\begin{aligned}|v\rangle\otimes|w\rangle &= \sum_{r,s=0}^{1} a_r b_s |v_r\rangle\otimes|w_s\rangle = \sum_{s=0}^{1}\big(a_0 b_s|v_0\rangle|w_s\rangle + a_1 b_s|v_1\rangle|w_s\rangle\big),\\ &= a_0b_0|v_0\rangle\otimes|w_0\rangle + a_0b_1|v_0\rangle\otimes|w_1\rangle + a_1b_0|v_1\rangle\otimes|w_0\rangle + a_1b_1|v_1\rangle\otimes|w_1\rangle,\end{aligned}$$

el cual lo podemos reescribir en la forma

$$|v\rangle\otimes|w\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{2.1}$$

con

$$a = v_0w_0, \quad b = v_0w_1, \quad c = v_1w_0, \quad y \quad d = v_1w_1.$$

Nótese que

$$\det\begin{pmatrix} a & b\\ c & d\end{pmatrix} = ad - bc = 0. \tag{2.2}$$

Lo anterior dice que: un estado $|v\rangle\otimes|w\rangle$ en $\mathcal{V}\otimes\mathcal{W}$ dado por (2.1) ***no es un estado en entrelazado o en entrelazamiento cuántico*** *si y solo si sus correspondientes amplitudes (coeficientes respecto a las bases $\hat{\mathcal{B}}_V$ y $\hat{\mathcal{B}}_W$) satisfacen* (2.2).

Ejemplo 12. *Defínase un sistema 2-cúbits como el producto tensorial de dos cúbits por separado, cada uno definido con la base estándar $\mathcal{B}_\mathcal{E}$. Considerese los estados*

$$|v\rangle = \frac{\boldsymbol{i}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{\boldsymbol{i}}{2\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|11\rangle \quad y \quad |w\rangle = \frac{1}{2}|00\rangle - \frac{\boldsymbol{i}}{2}|01\rangle + \frac{\boldsymbol{i}}{2\sqrt{2}}|10\rangle,$$

los cuales en forma vectorial quedan expresados como

$$|v\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}\frac{\boldsymbol{i}}{2}\\ \frac{\sqrt{3}}{2}\\ \frac{\boldsymbol{i}}{2}\\ \frac{\sqrt{3}}{2}\end{pmatrix} \quad y \quad |w\rangle = \begin{pmatrix}\frac{1}{2}\\ -\frac{\boldsymbol{i}}{2}\\ \frac{\boldsymbol{i}}{\sqrt{2}}\\ 0\end{pmatrix}.$$

El no entrelazamiento o entrelazamiento de cada estado puede demostrarse a partir de la condición (2.2) *del Ejemplo 11. En efecto, para*

$$|v\rangle = \frac{1}{2}|01\rangle - \frac{\boldsymbol{i}}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle \quad \to \quad a = \frac{\boldsymbol{i}}{2\sqrt{2}}, \quad b = \frac{\sqrt{3}}{2\sqrt{2}}, \quad c = \frac{i}{2\sqrt{2}} \quad y \quad d = \frac{\sqrt{3}}{2\sqrt{2}},$$

donde claramente se tiene que $ad = bc$, por lo que $|w\rangle$ no es un estado entrelazado, más aún,

$$|v\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{\boldsymbol{i}}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle).$$

De manera análoga, para el estado $|w\rangle$

$$|w\rangle = \frac{1}{2}|00\rangle - \frac{\boldsymbol{i}}{2}|01\rangle + \frac{\boldsymbol{i}}{\sqrt{2}}|10\rangle \rightarrow \quad a = \frac{1}{2}, \quad b = -\frac{i}{2}, \quad c = \frac{i}{\sqrt{2}} \quad y \quad d = 0.$$

De donde, $ad \neq bc$. Mostrándose así que $|w\rangle$ es un ejemplo de un estado de entrelazamiento cuántico en un 2-cúbit.

Ejemplo 13. *[La base de Bell] Utilizando el mismo sistema del ejemplo anterior, se define otra de las bases usuales en un sistema de 2-cúbits, esta dada por*

$$\mathcal{B}_b = \left\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\right\},$$

en donde

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{2}|11\rangle \quad y \quad |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{2}|10\rangle,$$

la cual es muy útil en la teoría de procesamiento y teletransportación cuántica. A continuación, se muestra a partir de la condición (2.2) del Ejemplo 11 por qué los estados de la base de Bell también son estados en entrelazamiento cuántico. Retomando $|\Phi^\pm\rangle$

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{2}|11\rangle \rightarrow \quad a = \frac{1}{\sqrt{2}}, \quad b = 0, \quad c = 0 \quad y \quad d = \frac{1}{2}.$$

Se observa que $ad = \pm\frac{1}{\sqrt{8}}$ es distinto a $bc = 0$ mostrando que es un estado en entrelazamiento cuántico. Ahora para $|\Psi^\pm\rangle$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{2}|10\rangle \rightarrow \quad a = 0, \quad b = \frac{1}{\sqrt{2}}, \quad c = \frac{1}{2} \quad y \quad d = 0.$$

Se observa que $ad = 0$ distinto a $bc = \pm\frac{1}{\sqrt{8}}$ mostrando de igual forma que este también es un estado en entrelazamiento cuántico.

La condición de no entrelazamiento cuántico se extiende manera natural a espacios vectores $\mathcal{V}$ y $\mathcal{W}$ con dimensiones $N \geq 2$, basta con replicar lo hecho en el ejemplo anterior, construir la correspondiente matriz $N \times N$ y calcular su determinante.

Los espacios vectoriales formados por productos tensoriales son aquellos que permiten representar distintos sistemas cuánticos conformados por dos o más cúbits. Veamos esto con más detalle. Considere n-cúbits, cada uno representado por un espacio vectorial $\mathcal{V}_r$, con base estándar $\mathcal{B}_E^r = \{|0\rangle_r, |1\rangle_r\}$, para $r \in \{0, 1, \ldots, n-1\}$. Por lo expuesto antes, si queremos conformar un sistema de n-cúbits con una base conformada por 2^n vectores, basta con tomar el espacio vectorial $V_{n-1} \otimes V_{n-2} \otimes \cdots \otimes V_1 \otimes V_0$. Por ejemplo, para el caso $n = 2$, la base de $V_1 \otimes V_0$ está dada por

$$\mathcal{B}_2 = \{|0\rangle_1 \otimes |0\rangle_0, |0\rangle_1 \otimes |1\rangle_0, |1\rangle_1 \otimes |0\rangle_0, \otimes |1\rangle_1 \otimes |1\rangle_0\},$$
$$\mathcal{B}_2 = \{|0\rangle_1 |0\rangle_0, |0\rangle_1 |1\rangle_0, |1\rangle_1 |0\rangle_0, |1\rangle_1 |1\rangle_0\},$$

la cual, según la definición anterior, se escribe de esta forma:

$$\mathcal{B}_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

Para el caso $n = 3$ la base de $V_2 \otimes V_1 \otimes V_0$ está dada por

$$\mathcal{B}_3 = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}.$$

En general, la base de $V_{n-1} \otimes V_{n-2} \otimes \cdots \otimes V_1 \otimes V_0$ se escribe en la forma

$$\mathcal{B}_n = \{|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |11\ldots0\rangle, |1\ldots11\rangle\}.$$

En este punto, cabe mencionar, y como veremos a lo largo del documento, que las bases frecuentemente utilizadas en la estructuración de algoritmos cuánticos son

$$\mathcal{B}_E = \{|0\rangle, |1\rangle\} \quad \text{y} \quad \mathcal{B}_H = \left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\} := \{|H^{\nearrow}\rangle, |H^{\nwarrow}\rangle\},$$

respectivamente, en cuyo caso, para el caso de un 2-cúbit, sus estados se expresan en la forma

$$|v\rangle|w\rangle = a_0b_0|0\rangle|H^{\nearrow}\rangle + a_0b_1|0\rangle|H^{\nwarrow}\rangle + a_1b_0|1\rangle|H^{\nearrow}\rangle + a_1b_1|1\rangle|H^{\nwarrow}\rangle.$$

2.2.1. Operadores lineales y producto interno sobre $\mathcal{V} \otimes \mathcal{W}$

A continuación se detallan ciertos aspectos de los operadores lineales en sistemas de varios cúbits. Considérese dos operadores lineales $L_1 : \mathcal{V} \to \mathcal{V}$ y $L_2 : \mathcal{W} \to \mathcal{W}$. El producto tensional entre L_1 y L_2 denotado por $L_1 \otimes L_2$, actúa sobre estados $|v\rangle \otimes |w\rangle$ de $\mathcal{V} \otimes \mathcal{W}$ en la siguiente forma

$$(L_1 \otimes L_2)(|v\rangle \otimes |w\rangle) := L_1|v\rangle \otimes L_2|w\rangle.$$

A partir de esta definición, se tiene directamente

$$(L_1 \otimes L_2)(L_3 \otimes L_4) = (L_1L_3 \otimes L_2L_4),$$

para $L_3 : \mathcal{V} \to \mathcal{V}$ y $L_4 : \mathcal{W} \to \mathcal{W}$. Incluso, se puede extender la definición anterior a cualquier estado de $\mathcal{V} \otimes \mathcal{W}$ preservando la propiedad de linealidad

$$(L_1 \otimes L_2)\Big(\sum_r \alpha_r |v_r\rangle \otimes |w_r\rangle\Big) = \sum_r \alpha_r L_1|v_r\rangle \otimes L_2|w_r\rangle.$$

La correspondiente operación de producto interno sobre $\mathcal{V}$ y $\mathcal{W}$ también se puede extender sobre $\mathcal{V} \otimes \mathcal{W}$. En efecto:

$$\langle \sum_r \alpha_r |v_r\rangle \otimes |w_r\rangle, \sum_s \beta_s |\hat{v}_s\rangle \otimes |\hat{w}_s\rangle\rangle = \sum_{r,s} \alpha_r\beta_s \langle v_r, \hat{v}_s\rangle\langle w_r, \hat{w}_s\rangle,$$

define un correcto producto interno en $\mathcal{V} \otimes \mathcal{W}$.

A partir de lo anterior, es posible extender definiciones previas como operadores adjuntos, unitarios, normales y hermitianos, y aún más, para operadores lineales de la forma

$L_1 : \mathcal{V} \to \tilde{\mathcal{V}}$ y $L_2 : \mathcal{W} \to \tilde{\mathcal{W}}$. En tal caso, cualquier operador lineal $\mathcal{L} : \mathcal{V} \otimes \mathcal{W} \to \tilde{\mathcal{V}} \otimes \tilde{\mathcal{W}}$ es de la forma $\mathcal{L} := \sum_s c_s L_{1,s} \otimes L_{2,s}$ dado por

$$\mathcal{L}(|v\rangle \otimes |w\rangle) = \big(\sum_s c_s L_{1,s} \otimes L_{2,s}\big)(|v\rangle \otimes |w\rangle) = \sum_s c_s L_{1,s} |v\rangle \otimes L_{2,s} |w\rangle .$$

Con el objetivo de expresar mejor lo anterior, a continuación se hace uso de la *notación de Kronecker*. Suponga que $\dim(\mathcal{V}) = n$, $\dim(\tilde{\mathcal{V}}) = m$, $\dim(\mathcal{W}) = q$, $\dim(\tilde{\mathcal{W}}) = p$ y que los operadores $L_1 : \mathcal{V} \to \tilde{\mathcal{V}}$ y $L_2 : \mathcal{W} \to \tilde{\mathcal{W}}$ tienen representación matricial $A = (a_{rs}) \in \mathbb{M}_{m\times n}(\mathbb{C})$ y $B = (b_{rs}) \in \mathbb{M}_{p\times q}(\mathbb{C})$ en para algunas bases respectivas de $\mathcal{V}$, $\tilde{\mathcal{V}}$ y $\mathcal{W}$, $\tilde{\mathcal{W}}$. Entonces, el operador $L_1 \otimes L_2 : \mathcal{V} \otimes \mathcal{W} \to \tilde{\mathcal{V}} \otimes \tilde{\mathcal{W}}$ tiene representación matricial

$$L_1 \otimes L_2 \equiv A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1}B & a_{12}B & \cdots & a_{mn}B \end{pmatrix}_{mp\times nq}$$

Bajo esta notación, cada submatriz $a_{rs}B$ es una matriz proporcional a B con constante de proporcionalidad la matriz a_{rs}. Así, por ejemplo,

$$\begin{pmatrix} i \\ 2 \end{pmatrix} \otimes \begin{pmatrix} -i \\ 1 \end{pmatrix} = \begin{pmatrix} iB \\ 2B \end{pmatrix} = \begin{pmatrix} i\begin{pmatrix} -i \\ 1 \end{pmatrix} \\ 2\begin{pmatrix} -i \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ i \\ -2i \\ 2 \end{pmatrix}.$$

En el caso de las matrices de Pauli Y e Z tenemos

$$Y \otimes Z = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & i \\ i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}.$$

A partir de lo anterior y de la notación $|v\rangle^{\otimes k}$ se deduce para el caso de los operadores lineales.

$$L^{\otimes k} := L \otimes L \underbrace{\otimes \cdots \otimes L \otimes L}_{k-veces}.$$

2.3. Conclusiones

Como se puede evidenciar a lo largo de este capítulo, los contenidos vistos sirvieron para introducir al lector, de manera informal, en la computación cuántica. Por medio de analogías hechas a fenómenos físicos como la polarización de un fotón, se establecieron conceptos fundamentales relacionados con la unidad básica de información conocida como cúbit, algo que el lector inicialmente desconocía y que se espera que tenga una mejor visión y entendimiento a partir de este punto. Para reforzar este entendimiento, también se plantea una representación gráfica respecto a las rotaciones de los estados de un cúbit, por medio de una figura geométrica conocida como la esfera de Bloch. Es importante aclarar que esta esfera es una posible representación hecha no directamente al estado de un cúbit, sino a su forma equivalente. Así mismo, no se considera esta representación

como la única válida; más bien, es la única que se toma en cuenta en este trabajo al momento de representar cúbits de forma individual. El lector puede además darse cuenta de que, entre los conceptos adicionales descritos, está la inclusión del ángulo de fase y el entrelazamiento entre estados, que actúan como una división de clases entre estados ya no de uno, sino de un sistema formado por múltiples qubits, implicando al lector que no todos los estados son iguales entre sí. A lo largo de este trabajo, tales conceptos tendrán mayor relevancia. De momento, el siguiente capítulo introduce las puertas cuánticas y su uso dentro de los circuitos cuánticos para aplicar diversas transformaciones a los estados base.

Capítulo 3

Puertas cuánticas

Este capítulo introduce formalmente el concepto de puertas y circuitos cuánticos. Comenzamos describiendo el efecto de las puertas cuánticas en los estados como si fueran transformaciones lineales aplicadas a un vector, continuamos mencionando algunas de las puertas cuánticas más utilizadas en los circuitos y finalmente concluimos detallando los elementos más importantes de nuestro algoritmo HHL, tales como la transformada de Fourier cuántica, su inversa y la puerta de cambio de fase.

3.1. Puertas cuánticas como transformaciones lineales

Considere $\mathcal{V}$ como un espacio vectorial asociado a un cúbit. Considere ahora el operador lineal $|0\rangle\langle 0| : \mathcal{V} \to \mathcal{V}$. La matriz representante de este operador, descrita respecto a cualquier base, es simplemente la matriz cuyas columnas son los valores del operador sobre los vectores de esa base en cuestión. Por ejemplo, si la base es $\mathcal{B}_E = \{|0\rangle, |1\rangle\}$ entonces:

$$\begin{cases} (|0\rangle\langle 0|)(|0\rangle) & = \langle 0|0\rangle |0\rangle = |0\rangle \\ (|0\rangle\langle 0|)(|1\rangle) & = \langle 0|1\rangle |0\rangle = |\varnothing\rangle \end{cases} \quad \Leftrightarrow \quad |0\rangle\langle 0| \equiv \begin{pmatrix} |0\rangle & |\varnothing\rangle \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

De forma análoga se demuestra que

$$|0\rangle\langle 1| \equiv \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle\langle 0| \equiv \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{y} \quad |1\rangle\langle 1| \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

en consecuencia, respecto a la base estándar, se cumple que toda matriz $A = (a_{rs})$ con $r, s \in \{1, 2\}$ representa la transformación lineal

$$L : \mathcal{V} \to \mathcal{V} \quad L : a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|,$$

es decir

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|.$$

A partir de lo anterior, se verifica de manera directa la relación de completitud. Considérese ahora un sistema de 2-cúbits, cada uno con respectivas bases $\mathcal{B}_E^i = \{|0\rangle_s, |1\rangle_s\}$, $s = 1, 2$. Al aplicar el producto tensorial entre ambos cúbits para formar el sistema, se obtiene la base:

$$\mathcal{B}_2 = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\},$$

en donde hemos usado la representación binaria (decimal) para cada elemento de dicha base, es decir

$$|00\rangle \Leftrightarrow |0\rangle\,, \quad |01\rangle \Leftrightarrow |1\rangle\,, \quad |10\rangle \Leftrightarrow |2\rangle\,, \quad |11\rangle \Leftrightarrow |3\rangle\,.$$

Finalmente, se tiene que la matriz $A = (a_{rs})$ con $r, s \in \{0, 1, 2, 3\}$ representa la transformación lineal (respecto a $\mathcal{B}_2$)

$$L : \sum_{r,s=0}^{3} a_{rs} \,|r\rangle \langle s| = \sum_{r=0}^{3} \Big(\sum_{s=0}^{3} a_{rs} \,|r\rangle \langle s| \Big),$$

logrando una expresión equivalente a la definida en la relación de completitud.

Ejemplo 14. *Sea la matriz*

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Si se toma esta matriz como representación del operador lineal $L : \mathcal{V} \otimes \mathcal{V} \to \mathcal{V} \otimes \mathcal{V}$ entonces

$$\begin{aligned} L &= |0\rangle \langle 2| + |1\rangle \langle 1| + |2\rangle \langle 0| + |3\rangle \langle 3| \\ L &= |00\rangle |10\rangle + |01\rangle |01\rangle + |10\rangle |00\rangle + |11\rangle |11\rangle\,. \end{aligned}$$

Esta transformación intercambia los vectores $|00\rangle$ y $|10\rangle$ y deja los otros dos igual.

Generalizando lo anterior para espacios de múltiples cúbits, considérese ahora el espacio vectorial $\mathcal{V} = V_{n-1} \otimes V_{n-2} \otimes \cdots \otimes V_1 \otimes V_0$ con base $\mathcal{B}_n$ (ver Sección 2.2). Si se define el operador lineal $L : \mathcal{V} \to \mathcal{V}$ con representación matricial $A = (a_{rs})$ con $r, s \in \{0, 1, \ldots, 2^n - 1 := N\}$, entonces, usando la representación binaria de los elementos en la base estándar, se deduce lo siguiente:

- $a_{rs} = \langle r|A|s\rangle$.
- $|v\rangle = \sum_{k=0}^{N} v_k \,|k\rangle$ entonces

$$\begin{aligned} L\,|v\rangle &= \Big(\sum_{r=0}^{N} \sum_{s=0}^{N} a_{rs} \,|r\rangle \langle s| \Big) \Big(\sum_{k=0}^{N} v_k \,|k\rangle \Big) \\ L\,|v\rangle &= \sum_{r=0}^{N} \sum_{s=0}^{N} \sum_{k=0}^{N} a_{rs} v_k \,|r\rangle \langle s| \;|k\rangle = \sum_{r=0}^{N} \sum_{s=0}^{N} a_{rs} v_s \,|r\rangle\,. \end{aligned}$$

Extendiéndonos un poco más, si $\mathcal{V}$ es un espacio vectorial N-dimensional con base $\{v_k\}$ entonces el operador lineal $L : \mathcal{V} \to \mathcal{V}$, $|v\rangle \to L\,|v\rangle := \mathcal{B}\,|v\rangle$, con $\mathcal{B} = (b_{ij})$ puede escribirse en la forma

$$L := \sum_{r,s=0}^{N} b_{rs} \,|v_r\rangle \langle v_s|\,,$$

respecto a la base $\{v_k\}$.

A partir de todo lo anterior, y dado un sistema cuántico $\mathcal{V}$, se entenderá en este trabajo por *transformación cuántica*, a toda función definida sobre los espacios de estados de $\mathcal{V}$ en sí mismo, y que además sea una transformación lineal del espacio vectorial asociado al espacio de estados del sistema cuántico. Sin embargo, no se considerarán todas las transformaciones lineales, solo aquellas que respetan propiedades relacionadas con la medición cuántica y la superposición. Así pues, si $U : \mathcal{V} \to \mathcal{V}$ es dicha transformación lineal tal que:

$$U(\sum_{r=1}^{m} a_r |\psi_r\rangle) = \sum_{r=1}^{m} a_r U(|\psi_r\rangle),$$

para cualquier superposición $|\psi\rangle = \sum_{r=1}^{m} a_r |\psi_r\rangle$,
entonces, se desea esencialmente que vectores unitarios sean enviados a vectores unitarios, lo que implica que subespacios ortogonales se envíen a subespacios ortogonales. Esta condición asegura que medir un estado y luego aplicar una transformación sobre el estado resultante de la medición da el mismo resultado que primero aplicar la transformación al estado original y luego medir el estado resultante en la base transformada. Matemáticamente, lo anterior se expresa así: *Para cualquier par de estados $|\psi\rangle$ y $|\phi\rangle$, el producto interno entre sus imágenes, $U|\psi\rangle$ y $U|\phi\rangle$, debe ser igual al producto interno entre $|\psi\rangle$ y $|\phi\rangle$, es decir*

$$\langle U\psi|U\phi\rangle = \langle\psi|U^\dagger U|\phi\rangle = \langle\psi|\phi\rangle,$$

por lo tanto $U^\dagger U = I$. En otras palabras, para cualquier transformación cuántica U, su transformación adjunta es igual a su transformación inversa, lo que es lo mismo que decir que U es una *transformación unitaria*. Por ende, la condición de operador unitario es suficiente; el conjunto de transformaciones admisibles sobre un sistema cuántico corresponde exactamente al *conjunto de operadores unitarios sobre el espacio vectorial complejo* asociado al espacio de estados del sistema cuántico. Dado que los operadores unitarios preservan el producto interior, estos mapean bases ortonormales a bases ortonormales. Lo contrario también es cierto: cualquier transformación lineal que mapea una base ortonormal a una base ortonormal es una transformación unitaria. Finalmente, un cálculo directo muestra que:

- El producto U_1U_2 de dos transformaciones unitarias U_1 y U_2 es de nuevo una transformación unitaria.

- Si U_1 es una transformación unitaria en X_1 y U_2 es una transformación unitaria en X_2 entonces $U_1 \otimes U_2$ es una transformación unitaria en $X_1 \otimes X_2$.

3.2. Ejemplos de puertas cuánticas

A continuación se describen algunas de las puertas más usadas en circuitos cuánticos. Recordemos que, aparte de tener representación matricial unitaria, consideramos como *puerta cuántica* a cualquier estado de transformación cuántica que actúe solo sobre un pequeño número de cúbits. A las secuencias de puertas cuánticas se les conoce como *arreglos cuánticos* o también *circuitos cuánticos*.

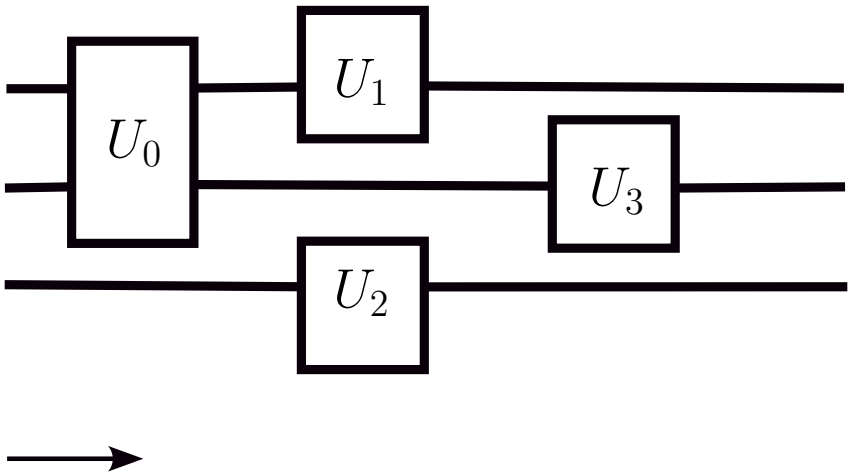

Figura 3.1: Representación esquemática de un circuito cuántico sobre un 3-cúbit, conformado por cuatro puertas cuánticas U_0, U_1, U_2 y U_3. Cada línea horizontal representa un cúbit. La transformación U_0 actúa sobre un 2-cúbit, mientras que U_1, U_2 y U_3 actúan cada una sobre un cúbit. Cuando decimos que un operador U actúa sobre el j-ésimo cúbit de un sistema cuántico de n-cúbit, significa que se aplica el operador $\mathcal{U} = I \otimes I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I \otimes I$ en todo sistema de n-cúbit, siendo I el operador identidad sobre un cúbit, aplicado sobre todos y cada uno de los restantes cúbits del sistema. El flujo de los datos y la aplicación de cada puerta cuántica van de izquierda a derecha.

3.2.1. Puertas de Pauli

Entre todas las posibles transformaciones unitarias que actúan sobre un cúbit, destacan las puertas de Pauli, representadas (bajo la base estándar) por las matrices de Pauli.

$$I := |0\rangle\langle 0| + |1\rangle\langle 1| \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X := |1\rangle\langle 0| + |0\rangle\langle 1| \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$Y := -|1\rangle\langle 0| + |0\rangle\langle 1| \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad Z := |0\rangle\langle 0| - |1\rangle\langle 1| \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

en donde I es la transformación identidad, X se conoce como *negación* (la transformación en computación clásica conocida como **NOT** sobre los bits $|0\rangle$ y $|1\rangle$), Z cambia la fase relativa de un estado en superposición respecto a la base estándar y $Y = ZX$, es la composición de las dos puertas X y Z.

3.2.2. Puerta de Hadamard

Otra de las transformaciones unitarias destacadas es la puerta de Hadamard. Una puerta cuántica que es, además, muy utilizada dentro del circuito que define el algoritmo HHL. La representación bajo la base estándar está dada por:

$$L_H : \mathcal{V} \to \mathcal{V} \quad L_H : \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \Big),$$

es decir, tiene como representación matricial la matriz de Hadamard.

$$L_H(|0\rangle) = |H^{\nearrow}\rangle\,, \quad L_H(|1\rangle) = |H^{\nwarrow}\rangle \quad \text{lo que equivale a tener} \quad H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

A continuación, si se considera el operador $L_H^{\otimes k} : \mathcal{V}^{\otimes k} \to \mathcal{V}^{\otimes k}$. Se comprueba (como se verá más adelante) que

$$H^{\otimes k} = \frac{1}{\sqrt{2^k}} \sum_{r,s=0}^{2^k-1} (-1)^{r\cdot s} \left|r\right\rangle \left\langle s\right| . \tag{3.1}$$

Donde la notacion $r \cdot s$ representa:

$$r \cdot s := (r_0, s_1, \ldots, r_{k-1}) \cdot (s_0, s_1, \ldots, s_{k-1}) = \sum_{m=0}^{k-1} r_m s_m.$$

Dada la importancia del operador de Hadamard para los propósitos de este trabajo, a continuación se observa una expresión más amigable de la fórmula (3.1). Comencemos con un caso simple, $k = 2$ y consideremos un estado base $|y\rangle = |y_1 y_0\rangle$ escrito en forma binaria. Aplicando el operador $H^{\otimes 2}$ tenemos

$$H^{\otimes 2} \left|y\right\rangle = (H \otimes H)(|y_1 y_0\rangle) = (H \left|y_1\right\rangle) \otimes (H \left|y_0\right\rangle),$$

dado que y_r solo puede tomar el valor "0" o "1" entonces $H \left|y_r\right\rangle$ solo puede ser $|H^{\nearrow}\rangle$ o $|H^{\nwarrow}\rangle$. De aquí se deduce que $H \left|y_i\right\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{y_i} \left|1\right\rangle)$ por lo tanto

$$\begin{aligned}
H^{\otimes 2} \left|y\right\rangle &= \frac{1}{2}(|0\rangle + (-1)^{y_1} \left|1\right\rangle) \otimes (|0\rangle + (-1)^{y_0} \left|1\right\rangle), \\
H^{\otimes 2} \left|y\right\rangle &= \frac{1}{2}\big(\left|00\right\rangle + (-1)^{y_0} \left|01\right\rangle + (-1)^{y_1} \left|10\right\rangle + (-1)^{y_0+y_1} \left|11\right\rangle \big), \\
H^{\otimes 2} \left|y\right\rangle &= \frac{1}{2}\big(|0\rangle + (-1)^{y_0} \left|1\right\rangle + (-1)^{y_1} \left|2\right\rangle + (-1)^{y_0+y_1} \left|3\right\rangle \big).
\end{aligned}$$

A partir de este punto, es notable resaltar

$$y_0 = 1 \cdot y = (01) \cdot (y_1 y_0), \quad y_1 = 2 \cdot y = (10) \cdot (y_1 y_0). \quad \text{y} \quad y_0 + y_1 = 3 \cdot y = (11) \cdot (y_1 y_0),$$

en consecuencia,

$$H^{\otimes 2} \left|y\right\rangle = \frac{1}{2}\big(|0\rangle + (-1)^{1\cdot y} \left|1\right\rangle + (-1)^{2\cdot y} \left|2\right\rangle + (-1)^{3\cdot y} \left|3\right\rangle \big) = \frac{1}{2} \sum_{r=0}^{3} (-1)^{r\cdot y} \left|r\right\rangle .$$

De forma general, para un estado base $|y\rangle = |y_{k-1} y_{k-2} \ldots y_1 y_0\rangle$ se deduce que

$$\begin{aligned}
H^{\otimes k} \left|y\right\rangle &= \frac{1}{2^{k/2}}(|0\rangle + (-1)^{y_{k-1}} \left|1\right\rangle) \otimes (|0\rangle + (-1)^{y_{k-2}} \left|1\right\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{y_0} \left|1\right\rangle), \\
H^{\otimes k} \left|y\right\rangle &= \frac{1}{2^{k/2}} \sum_{r=0}^{2^k-1} (-1)^{r\cdot y} \left|r\right\rangle = \frac{1}{2^{k/2}} \sum_{r=0}^{2^k-1} \Big(\sum_{s=0}^{2^k-1} (-1)^{r\cdot s} \langle s|y\rangle \Big) \left|r\right\rangle , \\
H^{\otimes k} \left|y\right\rangle &= \frac{1}{2^{k/2}} \sum_{r,s=0}^{2^k-1} (-1)^{r\cdot s} \left|r\right\rangle \left\langle s\right| (|y\rangle).
\end{aligned}$$

En particular, si $|y\rangle = |00\cdots00\rangle = |0\rangle_k$ se deduce igualmente que

$$H^{\otimes k}|0\rangle_k = \frac{1}{2^{k/2}}(|0\rangle + (-1)^{y_{k-1}}|1\rangle) \otimes (|0\rangle + (-1)^{y_{k-2}}|1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{y_0}|1\rangle),$$
$$H^{\otimes k}|0\rangle_k = \frac{1}{2^{k/2}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle),$$
$$H^{\otimes k}|0\rangle_k = \frac{1}{2^{k/2}}\big(\,|00\cdots00\rangle + |00\cdots01\rangle \cdots |11\cdots11\rangle\,\big),$$
$$H^{\otimes k}|0\rangle_k = \frac{1}{2^{k/2}}\Big(\,|0\rangle + |1\rangle \cdots |2^k-2\rangle + |2^k-1\rangle\,\Big) = \frac{1}{2^{k/2}}\sum_{r=0}^{2^k-1}|r\rangle\,.$$

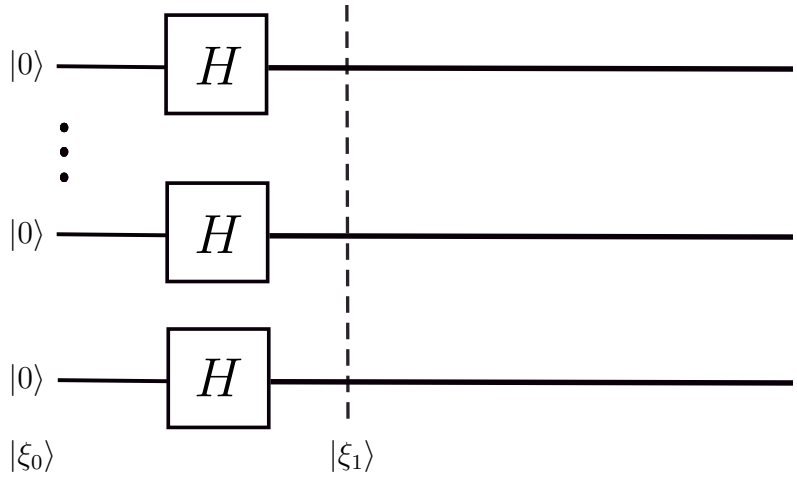

Figura 3.2: Esquema de un circuito cuántico conformado por k-cúbits del tipo $|0\rangle$ y k-puertas cuánticas de Hadamard H. La puerta $H^{\otimes k}$ actúa sobre $|\xi_0\rangle = |0\rangle_k$. El nuevo estado en superposición homogénea es $|\xi_1\rangle = H^{\otimes k}|0\rangle_k = \frac{1}{2^{k/2}}\sum_{r=0}^{2^k-1}|r\rangle$.

Por lo tanto, a partir del estado $|0\rangle_k$ y usando la puerta de Hadamard $H^{\otimes k}$ es posible crear un estado de superposición homogéneo (es decir, un estado de superposición con todos los coeficientes iguales) de los estados base del espacio vectorial 2^k-dimensional $\mathbb{C}^{2^k}$. Esto tiene un mayor significado si pensamos en mediciones. Recordemos que, al medir un estado de superposición, la norma al cuadrado de los coeficientes que acompañan los vectores base determina la probabilidad con la que, al medir dicho estado, este se encuentra en ese estado base en específico. Ahora bien, si hablamos de un estado de superposición homogéneo, sus coeficientes, al ser iguales, indican que todos los estados base tienen la misma probabilidad de ser obtenidos en la medición. El estado base $|0\rangle_k$ de un n-cúbit o, lo que es equivalente, de $\mathbb{C}^{2^k}$ es especial, pues es el usual *estado inicial de todo registro cuántico.*

Ejemplo 15. *Sea un sistema 2-cúbit, cada uno con base estándar. A continuación se*

calculan los estados $H^{\otimes 2}|0\rangle$ *y* $H^{\otimes 2}|3\rangle$

$$
\begin{aligned}
H^{\otimes 2}|0\rangle &= H^{\otimes 2}|00\rangle = (H^{\otimes}|0\rangle \otimes H^{\otimes}|0\rangle),\\
H^{\otimes 2}|0\rangle &= \frac{1}{2^{2/2}}(|0\rangle + (-1)^0|1\rangle) \otimes (|0\rangle + (-1)^0|1\rangle),\\
H^{\otimes 2}|3\rangle &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle).
\end{aligned}
$$

$$
\begin{aligned}
H^{\otimes 2}|3\rangle &= H^{\otimes 2}|11\rangle = (H^{\otimes}|1\rangle \otimes H^{\otimes}|1\rangle),\\
H^{\otimes 2}|3\rangle &= \frac{1}{2^{2/2}}(|0\rangle + (-1)^1|1\rangle) \otimes (|0\rangle + (-1)^1|1\rangle),\\
H^{\otimes 2}|3\rangle &= \frac{1}{2}(|0\rangle - |1\rangle - |2\rangle + |3\rangle).
\end{aligned}
$$

3.3. La transformada de Fourier cuántica

A continuación, se describe el operador conocido como la transformada de Fourier cuántica. Este operador tiene especial importancia en nuestro trabajo debido a que es una pieza fundamental en el algoritmo HHL. Considere un espacio vectorial $\mathcal{V}$ de dimensión m, y dos estados

$$
|x\rangle = \begin{pmatrix} x_0 \\ x_1 \\ \dots \\ v_{m-1} \end{pmatrix} \quad \text{y} \quad |y\rangle = \begin{pmatrix} y_0 \\ y_1 \\ \dots \\ y_{m-1} \end{pmatrix}.
$$

Se considera a $|y\rangle$ como el estado resultante de aplicar la *Transformada de Fourier Discreta (TFD)* en $|x\rangle$ si se cumple:

$$
|y\rangle = (TFD)(|x\rangle), \quad \Leftrightarrow \quad y_s = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} w^{-sj} x_j,
$$

donde $w \in \mathbb{C}$ es la m-ésima raíz de la ecuación polinomial definida en (1.1). Más aún:

- Para todo $q \in \mathbb{Z}$ se cumple

$$
\sum_{k=0}^{m-1} w^{qk} = \begin{cases} 0, & \text{si} \quad q \neq 0, \ \textbf{(Interferencia destructiva)} \\ m, & \text{si} \quad q = 0, \ \textbf{(Interferencia constructiva)} \end{cases}.
$$

- Para todo $k \in \mathbb{Z}$ se cumple $w^{m-k} = w^{-k}$.

Luego, ¿qué es la transformada de Fourier discreta? Es un mapeo de una lista de datos en otros, simbolizado $TFD(|x\rangle) = |y\rangle$ cuyo mapeo en cada dato está representado por

$$
y_s = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} e^{-i2\pi sj/m} x_j.
$$

Nótese que lo anterior se puede escribir en forma matricial. En efecto, para $|y\rangle = \Omega\,|x\rangle$ se tiene

$$\begin{pmatrix} y_0 \\ y_1 \\ \cdots \\ y_{m-1} \end{pmatrix} = \frac{1}{\sqrt{m}} \begin{pmatrix} w^{-0\cdot 0} & w^{-0\cdot 1} & \cdots & w^{-0\cdot(m-1)} \\ w^{-1\cdot 0} & w^{-1\cdot 1} & \cdots & w^{-1\cdot(m-1)} \\ \vdots & \vdots & \cdots & \vdots \\ w^{-(m-1)\cdot 0} & w^{-(m-1)\cdot 1} & \cdots & w^{-(m-1)\cdot(m-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \cdots \\ x_{m-1} \end{pmatrix},$$

donde y_s corresponde a la serí de potencias $\sum_{j=0}^{N-1} x_j w^{-sj}$ ponderada con los coeficientes x_j. A la matriz involucrada se le denota Ω.

Ejemplo 16. *Suponga que* $|x\rangle = \dfrac{1}{\sqrt{m}} \begin{pmatrix} 1 \\ 1 \\ \cdots \\ 1 \end{pmatrix}$.

Note que $|x| = \sqrt{\langle x|x\rangle} = 1$. *Por lo tanto, gracias a la interferencia destructiva y constructiva, se cumple*

$$y_s = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} w^{-sj} x_j = \begin{cases} 0, & si \quad s \neq 0, \\ \dfrac{1}{m} \displaystyle\sum_{j=0}^{m-1} w^{-sj}, & si \quad s = 0. \end{cases} .$$

Por ende, $|y\rangle = \begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$ *con* $|y| = \sqrt{\langle y|y\rangle} = 1$.

A partir de la definición de la transformada de Fourier discreta (TFD). Se define a continuación la transformada de Fourier cuántica (TFC). Supóngase que nuestro espacio vectorial $\mathcal{V}$ de dimensión m, tiene como base $\mathcal{B} = \{|r\rangle : r = 0, 1, \cdots, m-1\}$. Es decir, nuestra base, es la base canónica escrita en forma binaria. Así pues, la *Transformada de Fourier cuántica, (TFC) es un mapeo* $\mathcal{V} \to \mathcal{V}$ *definido exactamente igual a la transformada de Fourier discreta cuando los vectores base de* $\mathcal{V}$ *son los vectores canónicos* $|r\rangle$. Es claro que (TFC) es una puerta cuántica. En consecuencia, es una transformación unitaria.

Ahora, considere $m = 2^n$. Se puede asumir, sin pérdida de generalidad, que $\mathcal{V}$ es un n-cúbit, esto es, podemos asumir $\mathcal{V} = \mathbb{C}^{2^n}$. La matriz Ω definida anteriormente es la matriz unitaria $\mathcal{U}_{TFC}$ que representa al operador unitario TFC en la base canónica $\mathcal{B} = \{|r\rangle : r = 0, 1, \ldots, 2^n - 1\}$,

$$\mathcal{U} = \mathcal{U}_{TFC} := \frac{1}{2^{n/2}} \begin{pmatrix} w^{-0\cdot 0} & w^{-0\cdot 1} & \cdots & w^{-0\cdot(2^n-1)} \\ w^{-1\cdot 0} & w^{-1\cdot 1} & \cdots & w^{-1\cdot(2^n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ w^{-(2^n-1)\cdot 0} & w^{-(2^n-1)\cdot 1} & \cdots & w^{-(2^n-1)\cdot(2^n-1)} \end{pmatrix}.$$

A continuación, se describen algunas de las propiedades más importantes de la transformación de Fourier cuántica $\mathcal{U}_{TFC}$.

i) $\mathcal{U}$ es simétrica, es decir $\mathcal{U}_{rs} = \mathcal{U}_{sr}$.

ii) $\mathcal{U}$ es unitaria, es decir para cualesquiera $|\psi\rangle$ y $|\phi\rangle$ se cumple

$$\langle \mathcal{U}\psi|\mathcal{U}\phi\rangle = \langle\psi|\mathcal{U}^{\dagger}\mathcal{U}|\phi\rangle = \langle\psi|\phi\rangle.$$

iii) Sean $|j\rangle$ y $|k\rangle$ vectores base, entonces $\mathcal{U}\,|j\rangle = \dfrac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} w^{-kj}\,|k\rangle$. De esta relación se deduce

$$\mathcal{U}_{TFC}\Big(\sum_{j=0}^{2^n-1} x_j\,|j\rangle\Big) = \sum_{j=0}^{2^n-1} x_j\,\mathcal{U}(|j\rangle) = \frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1} x_j \sum_{k=0}^{2^n-1} w^{-kj}\,|k\rangle\,,$$

$$\mathcal{U}_{TFC}\Big(\sum_{j=0}^{2^n-1} x_j\,|j\rangle\Big) = \sum_{k=0}^{2^n-1}\Big(\frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1} w^{-kj}x_j\Big)\,|k\rangle = \sum_{k=0}^{2^n-1} y_k\,|k\rangle\,,$$

siendo y_k la transformadas de Fourier discreta de x_j.

Ejemplo 17. *Sea $m = 2^1$ (tenemos 1-cúbit). En este caso $w = e^{i2\pi/2}$, asi que*

$$\mathcal{U} = \frac{1}{\sqrt{2}}\begin{pmatrix} w^{-0\cdot 0} & w^{-0\cdot 1} \\ w^{-(2-1)\cdot 0} & w^{-1\cdot 1}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & w^{-1}\end{pmatrix},$$

$$\mathcal{U} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & e^{-i2\pi/2}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1\end{pmatrix} = H.$$

Esto nos dice que, en el caso de un 1-cúbit, la transformada de Fourier cuántica es simplemente la transformación de Hadamard.

Ejemplo 18. *Sea $m = 2^2$ (tenemos 2-cúbit). En este caso $w = e^{i2\pi/4} = i$. Por lo tanto*

$$\mathcal{U} = \frac{1}{\sqrt{4}}\begin{pmatrix} w^{-0\cdot 0} & w^{-0\cdot 1} & w^{-0\cdot 2} & w^{-0\cdot 3} \\ w^{-1\cdot 0} & w^{-1\cdot 1} & w^{-1\cdot 2} & w^{-1\cdot 3} \\ w^{-2\cdot 0} & w^{-2\cdot 1} & w^{-2\cdot 2} & w^{-2\cdot 3} \\ w^{-3\cdot 0} & w^{-3\cdot 1} & w^{-3\cdot 2} & w^{-3\cdot 3}\end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i^{-1} & i^{-2} & i^{-3} \\ 1 & i^{-2} & i^{-4} & i^{-6} \\ 1 & i^{-3} & i^{-6} & i^{-9}\end{pmatrix},$$

$$\mathcal{U} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i\end{pmatrix}.$$

Ejemplo 19. *Véase que $\mathcal{U}$ es una matriz unitaria. En efecto, considérense la r-ésima columna y la s-ésima columna de $\mathcal{U}$. Las cuales están dadas por*

$$|r\rangle = \frac{1}{\sqrt{m}}\begin{pmatrix} w^{-0\cdot r} \\ w^{-1\cdot r} \\ \cdots \\ w^{-(m-1)\cdot r}\end{pmatrix}, \quad y \quad |s\rangle = \frac{1}{\sqrt{m}}\begin{pmatrix} w^{-0\cdot s} \\ w^{-1\cdot s} \\ \cdots \\ w^{-(m-1)\cdot s}\end{pmatrix},$$

respectivamente. Por lo tanto, el producto interno entre estos vectores está dado por

$$\langle r|s\rangle = \frac{1}{m}\sum_{l=0}^{m-1}(w^{-l\cdot r})^* w^{-l\cdot s} = \frac{1}{m}\sum_{l=0}^{m-1}(e^{(-i2\pi l\cdot r)/m})^* e^{(-i2\pi l\cdot s)/m},$$

$$\langle r|s\rangle = \frac{1}{m}\sum_{l=0}^{m-1}(e^{(-i2\pi l\cdot(-r))/m})e^{(-i2\pi l\cdot s)/m} = \frac{1}{m}\sum_{l=0}^{m-1}(w^{-l\cdot -r})w^{-l\cdot s},$$

$$\langle r|s\rangle = \frac{1}{m}\sum_{l=0}^{m-1} w^{-l\cdot(s-r)} = \begin{cases} 0, & if \quad r \neq s, \\ 1, & if \quad r = s. \end{cases},$$

con $m = 2^n$. Lo anterior prueba que las columnas de $\mathcal{U}$ son ortonormales. Por lo tanto, $\mathcal{U}$ es unitaria.

A continuación, se muestra una forma más conveniente para expresar la transformada de Fourier cuántica. Para esto, es necesario definir una nueva forma de expresar ciertos números reales.

Definición 5. *Dado un número real $\psi \in [0,1]$ (en notación decimal con expresión finita) su expresión binaria de n-dígitos (también conocida como fracción binaria de n-dígitos) se define como*

$$\psi = [0.\psi_1\psi_2\cdots\psi_n] \quad \Leftrightarrow \quad \psi = \sum_{s=1}^{n} \psi_s 2^{-s},$$

en donde cada $\psi_s \in \{0,1\}$.

Por ejemplo, si $\psi = \dfrac{1}{2}$ y $\phi = \dfrac{3}{4}$ (en notación decimal) entonces $\psi = 0.1$ y $\phi = 0.11$ en notación binaria respectivamente. En efecto

$$[0.1] = \frac{1}{2}, \quad \text{y} \quad [0.11] = \frac{1}{2} + \frac{1}{2^2} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}.$$

A partir de la definición anterior, se comprueba

$$0 \leq [0.\psi_1\psi_2\cdots\psi_n] \leq 1 - \frac{1}{2^n} \quad \Leftrightarrow \quad 0 \leq 2^n[0.\psi_1\psi_2\cdots\psi_n] \leq 2^n - 1,$$

y extendiéndonos más, también se puede observar

$$\begin{aligned} 2\psi &= 2\sum_{s=1}^{n} \psi_s 2^{-s} = \psi_1 + [0.\psi_2\psi_3\cdots\psi_n] \equiv [\psi_1.\psi_2\cdots\psi_n], \\ 2^2\psi &= 2^2\sum_{s=1}^{n} \psi_s 2^{-s} = 2\psi_1 + \psi_2 + [0.\psi_3\psi_4\cdots\psi_n] \equiv [2\psi_1 + \psi_2.\cdots\psi_n], \end{aligned}$$

donde, para cada $1 \leq l \leq n$ se tiene finalmente que

$$[0.\psi_l\psi_{l+1}\cdots\psi_n] = \psi_l 2^{-1} + \psi_{l+1}2^{-2} + \cdots + \psi_n 2^{-(n-l+1)} = \sum_{s=l}^{n} \psi_s 2^{-(s-l+1)}.$$

A partir de este punto, dado un estado base $|k\rangle \in \mathcal{B} = \{|r\rangle : r = 0, 1, \ldots, 2^n - 1\}$. Su expresión escrita en fracción binaria queda en la forma

$$\begin{aligned} k &= k_1 2^{n-1} + k_2 2^{n-2} + \cdots + k_{n-1}2^1 + k_n 2^0 = \sum_{s=1}^{n} k_s 2^{n-s}, \qquad k_s \in \{0,1\}, \\ k &= 2^n[0.k_1k_2\ldots k_n], \\ |k\rangle &= |k_1k_2\ldots k_n\rangle \equiv \bigotimes_{s=1}^{n} |k_s\rangle, \end{aligned}$$

donde k_1 y k_n son el bit menos y más significativo, respectivamente. Bajo la anterior notación, la transformada de Fourier cuántica sobre cada elemento $|j\rangle$ de la base $\mathcal{B}$ se expresa en la siguiente forma:

$$
\begin{aligned}
2^{n/2}\mathcal{U}(|j\rangle) &= \sum_{k=0}^{2^n-1} w^{-kj}\,|k\rangle = \sum_{k\in\{0,1\}^n} w^{-kj}\,|k\rangle \\
2^{n/2}\mathcal{U}(|j\rangle) &= \sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} w^{-j\sum_{l=1}^{n}k_l 2^{n-l}}\bigotimes_{s=1}^{n}|k_s\rangle\,, \\
2^{n/2}\mathcal{U}(|j\rangle) &= \sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\prod_{l=1}^{n} w^{-jk_l 2^{n-l}}\bigotimes_{s=1}^{n}|k_s\rangle = \sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{s=1}^{n}\Big(w^{-jk_s 2^{n-s}}\,|k_s\rangle\Big), \\
2^{n/2}\mathcal{U}(|j\rangle) &= \sum_{k_1=0}^{1}\cdots\sum_{k_{n-1}=0}^{1}\bigotimes_{s=1}^{n-1}\Big(w^{-jk_s 2^{n-s}}\,|k_s\rangle\Big)\otimes\big(\,|0\rangle+\omega^{-j2^0}\,|1\rangle\,\big), \\
2^{n/2}\mathcal{U}(|j\rangle) &= \bigotimes_{s=1}^{n}\sum_{k_s=0}^{1} w^{-jk_s 2^{n-s}}\,|k_s\rangle = \bigotimes_{s=1}^{n}\Big[\,|0\rangle + w^{-j2^{n-s}}\,|1\rangle\,\Big], \\
2^{n/2}\mathcal{U}(|j\rangle) &= \bigotimes_{s=1}^{n}\Big[\,|0\rangle + \exp -i2\pi\sum_{l=1}^{n} j_l 2^{n-l}2^{-s}\,|1\rangle\,\Big], \\
2^{n/2}\mathcal{U}(|j\rangle) &= \bigotimes_{s=1}^{n}\Big[\,|0\rangle + \prod_{l=s+1-n}^{s}\exp -i2\pi j_{l+n-s}2^{-l}\,|1\rangle\,\Big], \\
2^{n/2}\mathcal{U}(|j\rangle) &= \bigotimes_{s=1}^{n}\Big[\,|0\rangle + \prod_{l=1}^{s}\exp -i2\pi j_{l+n-s}2^{-l}\,|1\rangle\,\Big].
\end{aligned}
$$

Obteniendo finalmente la expresión.

$$
\mathcal{U}(|j\rangle) = \frac{1}{2^{n/2}}\bigotimes_{s=1}^{n}\Big[\,|0\rangle + \prod_{l=1}^{s}\exp -i2\pi j_{l+n-s}2^{-l}\,|1\rangle\,\Big]. \tag{3.2}
$$

Así por ejemplo, con $n=1$ (1-cúbit) para $j\in\{0,1\}$ se tiene

$$
\mathcal{U}(|j\rangle) = \frac{1}{\sqrt{2}}\bigotimes_{s=1}^{1}\Big[\,|0\rangle + \prod_{l=1}^{s}\exp -i2\pi j_{l+1-s}2^{-l}\,|1\rangle\,\Big] = \frac{1}{\sqrt{2}}\big(\,|0\rangle + e^{-i2\pi j/2}\,|1\rangle\,\big),
$$

de donde,

$$
\mathcal{U}(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \quad \text{y} \quad \mathcal{U}(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle).
$$

que, como se observó anteriormente, corresponde al operador de Hadamard.

Ahora, si $n=2$ (2-cúbits) para $j\in\{0,1\}^2$

$$
\begin{aligned}
\mathcal{U}(|j\rangle) &= \frac{1}{2}\bigotimes_{s=1}^{2}\Big[\,|0\rangle + \prod_{l=1}^{s}\exp -i2\pi j_{l+2-s}2^{-l}\,|1\rangle\,\Big], \\
\mathcal{U}(|j\rangle) &= \frac{1}{2}\big(\,|0\rangle + e^{-i2\pi j_2/2}\,|1\rangle\,\big)\otimes|0\rangle + e^{-i2\pi(j_1/2+j_2/2^2)}\,|1\rangle\,\big), \\
\mathcal{U}(|j\rangle) &= \frac{1}{2}\big(\,|0\rangle + e^{-i2\pi[0.j_2]}\,|1\rangle\,\big)\otimes|0\rangle + e^{-i2\pi[0.j_1 j_2]}\,|1\rangle\,\big),
\end{aligned}
$$

en consecuencia

$$\begin{aligned}
\mathcal{U}(|00\rangle) &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle),\\
\mathcal{U}(|01\rangle) &= \frac{1}{2}(|0\rangle + e^{-i2\pi(1/2)}|1\rangle) \otimes (|0\rangle + e^{-i2\pi(0/2+1/2^2)}|1\rangle),\\
\mathcal{U}(|10\rangle) &= \frac{1}{2}(|0\rangle + e^{-i2\pi(0/2)}|1\rangle) \otimes (|0\rangle + e^{-i2\pi(1/2+0/2^2)}|1\rangle),\\
\mathcal{U}(|11\rangle) &= \frac{1}{2}(|0\rangle + e^{-i2\pi(1/2)}|1\rangle) \otimes (|0\rangle + e^{-i2\pi(1/2+1/2^2)}|1\rangle).
\end{aligned}$$

En general, se llega a la siguiente expresión

$$\begin{aligned}
\mathcal{U}(|j_1 j_2 \dots j_n\rangle) = \frac{1}{2^{n/2}}\big[(|0\rangle + e^{-i2\pi[0.j_n]}|1\rangle) \otimes \frac{1}{2^{n/2}}(|0\rangle + e^{-i2\pi[0.j_{n-1}j_n]}|1\rangle) \otimes \dots\\
\dots \otimes (|0\rangle + e^{-i2\pi[0.j_2\cdots j_{n-1}j_n]}|1\rangle) \otimes (|0\rangle + e^{-i2\pi[0.j_1 j_2\cdots j_{n-1}j_n]}|1\rangle).
\end{aligned}$$

A continuación se presenta la transformada cuántica de Fourier inversa TFCI como el mapeo $\mathcal{V} \to \mathcal{V}$ cuya matriz unitaria en la base estándar $\mathcal{B} = \{|r\rangle : r = 0, 1, \dots, N-1\}$, es simplemente $\mathcal{U}^{-1}$, la cual está dada por

$$\mathcal{U}^{-1} = \mathcal{U}_{TFC}^{-1} := \frac{1}{2^{n/2}} \begin{pmatrix} w^{0\cdot 0} & w^{0\cdot 1} & \cdots & w^{0\cdot(2^n-1)} \\ w^{1\cdot 0} & w^{1\cdot 1} & \cdots & w^{1\cdot(2^n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ w^{(2^n-1)\cdot 0} & w^{(2^n-1)\cdot 1} & \cdots & w^{(2^n-1)\cdot(2^n-1)} \end{pmatrix},$$

y en su notación binaria

$$\begin{aligned}
\mathcal{U}^{-1}(|j_1 j_2 \dots j_n\rangle) = \frac{1}{2^{n/2}}\big[(|0\rangle + e^{i2\pi[0.j_n]}|1\rangle) \otimes \frac{1}{2^{n/2}}(|0\rangle + e^{i2\pi[0.j_{n-1}j_n]}|1\rangle) \otimes \dots\\
\dots \otimes (|0\rangle + e^{i2\pi[0.j_2\dots j_{n-1}j_n]}|1\rangle) \otimes (|0\rangle + e^{i2\pi[0.j_1 j_2\dots j_{n-1}j_n]}|1\rangle).
\end{aligned}$$

Finalmente, un cálculo directo muestra que $\mathcal{U}^{-1}\mathcal{U} = \mathcal{U}\mathcal{U}^{-1} = I$.

3.4. Cambio de fase

A continuación se presenta el concepto de cambio de fase de un estado, en forma de puerta cuántica. La definición de fase relativa en esta sección es otro concepto fundamental a tener en cuenta al momento de trabajar con el algoritmo HHL. La puerta de cambio de fase $U_{P,S,\Phi}$ que, por su traducción en inglés, se conoce como *P-gate* (Phase gate), es una puerta que actúa sobre un cúbit y que, tal como predice su nombre, *cambia la fase relativa entre los dos estados base (véase sección 2.1.2)*. De manera más precisa, sobre los estados base $|0\rangle$ y $|1\rangle$, $U_{PS,\Phi}$ está dado por

$$U_{PS,\Phi}|0\rangle = |0\rangle, \quad \text{y} \quad U_{PS,\Phi}|1\rangle = e^{i\Phi}|1\rangle,$$

donde Φ se conoce como la *fase* y $e^{i\Phi}$ es el *factor de fase.* Lo anterior en forma matricial queda en la forma

$$U_{PS,\Phi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix}.$$

Nótese que $U_{P,S,\Phi}$ no tiene ningún efecto sobre el estado $|0\rangle$, mientras que sí lo tiene sobre el estado $|1\rangle$ al cambiar su fase.

$$U_{PS,\Phi}|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\Phi} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\Phi}|1\rangle .$$

Así pues, para un cúbit arbitrario $|v\rangle = a|0\rangle + b|1\rangle$, se tiene

$$U_{PS,\Phi}|v\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ e^{i\Phi}b \end{pmatrix} = a|0\rangle + e^{i\Phi}b|1\rangle .$$

Tal y como se presentó en la sección 2.1.2, si $a = |a|e^{i\theta_a}$ y $b = |b|e^{i\theta_b}$, en donde θ_a, θ_b son las fases de a y b respectivamente, entonces su fase relativa cambia de θ_b/θ_a a $(\theta_b + \Phi)/\theta_a$. De esta manera se entiende la razón por la cual la puerta cuántica de cambio de fase solo debe afectar uno de los estados; de lo contrario, ambos cúbits $|v\rangle$ y $U_{P,S,\Phi}|v\rangle$ serían el mismo estado cuántico.

Ejemplo 20. *Un ejemplo notable de una puerta de cambio de fase es la puerta de Pauli σ_z que se conoce como la puerta Z (Z-gate), la cual se obtiene cuando $\Phi = \pi$. Lo que hace especial a la puerta Z es su relación con la base de Hadamard $\mathcal{B}_H$. Noté que*

$$U_{PS,\pi}|H^{\nearrow}\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ e^{i\pi}/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |H^{\nwarrow}\rangle ,$$
$$U_{PS,\pi}|H^{\nwarrow}\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ -e^{i\pi}/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |H^{\nearrow}\rangle .$$

Por lo tanto, vemos cómo la puerta Z cambia el orden de los estados base en $\mathcal{B}_H$, es decir, la puerta Z actúa sobre $\mathcal{B}_H$ como la puerta de Pauli σ_x (puerta X) actúa sobre la base canónica $\mathcal{B}_E$ [1]

3.4.1. Fase controlada

A continuación, en un sistema 2-cúbit, se define la *puerta de cambio de fase controlada* de la siguiente forma:

$$U_{CPS,\Phi}|xy\rangle = e^{i(x\cdot y)\Phi}|xy\rangle ,$$

donde $x, y \in \{0, 1\}$ son simplemente los correspondientes números en el primer y segundo cúbit, respectivamente. Por lo tanto

$$U_{CPS,\Phi}|00\rangle = e^{i(0\cdot 0)\Phi}|00\rangle = |00\rangle , \qquad U_{CPS,\Phi}|01\rangle = e^{i(0\cdot 1)\Phi}|01\rangle = |01\rangle ,$$
$$U_{CPS,\Phi}|10\rangle = e^{i(1\cdot 0)\Phi}|10\rangle = |10\rangle , \qquad U_{CPS,\Phi}|11\rangle = e^{i(1\cdot 1)\Phi}|11\rangle = e^{i\Phi}|11\rangle .$$

Lo anterior se entiende de la siguiente forma: Si el primer cúbit es $|0\rangle$ (como ocurre para $|00\rangle$ y $|01\rangle$), nada se aplica al segundo cúbit. Pero, cuando el segundo cúbit es $|1\rangle$, un cambio de fase es aplicado. Por ejemplo, para los estados $|10\rangle\, y\, |11\rangle$ se aplica un cambio de fase al segundo cúbit. Ahora note que, para $|10\rangle$ el cambio de fase no afecta al cúbit $|0\rangle$ por lo que $|10\rangle$ queda invariante. Mientras que para $|11\rangle$ el cambio de fase actúa sobre el

[1] Otra forma de referirse a la puerta X es: puerta **NOT**, la cual sobre la base canónica cambia el estado base $|0\rangle$ en el estado base $|1\rangle$ y viceversa.

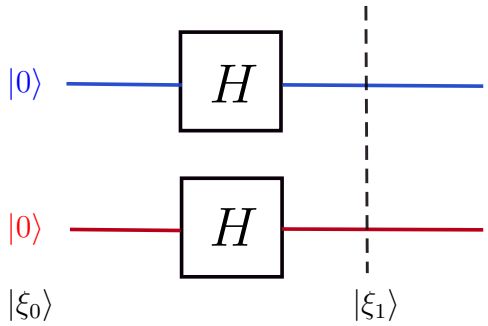

Figura 3.3: Esquema de un circuito cuántico conformado por 2-cúbits del tipo $|0\rangle$ y dos puertas cuánticas de Hadamard H

segundo cúbit $|1\rangle$ quedando en la forma $e^{i\Phi}|1\rangle$. De esta forma, el 2-cúbit se transforma en $e^{i\Phi}|11\rangle$. La versión matricial de lo presentado anteriormente está dada por lo siguiente:

$$U_{CPS,\Phi} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\Phi} \end{pmatrix} \equiv \begin{pmatrix} I & 0 \\ 0 & U_{PS,\Phi} \end{pmatrix}.$$

Ahora bien, para un estado en superposición $|\Upsilon\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, se tiene

$$U_{CPS,\Phi}|\Upsilon\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\Phi} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ e^{i\Phi}\delta \end{pmatrix} = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + e^{i\Phi}\delta|11\rangle.$$

Ejemplo 21. *Considere el circuito dado en la Figura 3.3. Iniciamos con el 2-cúbit* $|\xi_0\rangle = |0\rangle \otimes |0\rangle$. *El primer cúbit* $|0\rangle$ *lo llamaremos el cúbit de control, mientras que el segundo cúbit* $|0\rangle$ *será el cúbit objetivo. Tenemos:*

$$|\xi_0\rangle = |00\rangle \rightarrow |\xi_1\rangle = H^{\otimes 2}|00\rangle = \frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big).$$

Por lo tanto, si aplicamos la puerta $U_{CPS,\pi}$ *(la puerta de control Z) sobre* $|\xi_1\rangle$ *tenemos:*

$$U_{CPS,\pi}|\xi_1\rangle = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\big).$$

A continuación, aplicamos las mismas operaciones para el resto de vectores base estándar de un 2-cúbit $|01\rangle, |10\rangle$ *y* $|11\rangle$.

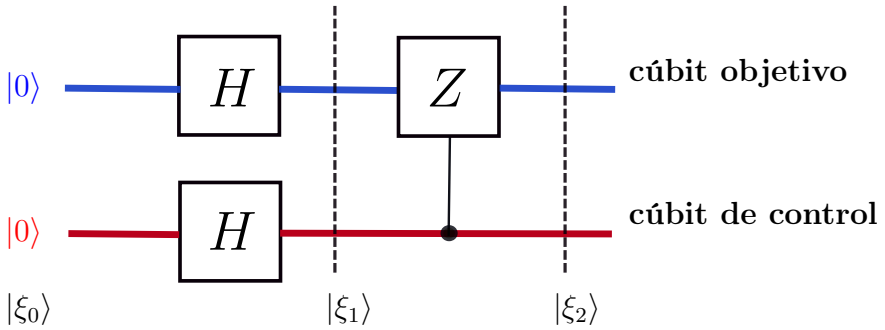

Figura 3.4: Esquema de un circuito cuántico conformado por 2-cúbits del tipo $|0\rangle$, 2-puertas cuánticas de Hadamard H y una puerta controlada tipo Z, donde $|\xi_2\rangle = U_{CPS,\pi}\,|\xi_1\rangle$

Para $|\xi_0\rangle = |01\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big),$$
$$U_{CPS,\pi}\,|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big).$$

Para $|\xi_0\rangle = |10\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle - |10\rangle - |11\rangle\,\big),$$
$$U_{CPS,\pi}\,|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle - |10\rangle + |11\rangle\,\big).$$

Para $|\xi_0\rangle = |11\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle - |10\rangle + |11\rangle\,\big),$$
$$U_{CPS,\pi}\,|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle - |10\rangle - |11\rangle\,\big).$$

La operación sobre el circuito original se representa en la Figura 3.4. Nótese que cada resultado anterior lo podemos codificar como las columnas de la matriz que representa dicho circuito

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

A continuación, se generaliza el efecto de rotación controlada para cualquier matriz unitaria. Para ello es necesario recordar algunos detalles de la esfera de Bloch.

3.4.2. Rotación arbitraria de un cúbit

A partir de la posibilidad de poder mapear ("representar") un cúbit como una esfera en $\mathbb{R}^3$ (esfera de Bloch), se puede observar de manera abstracta las "rotaciones" hechas a ese cúbit en cuestión. En la mayoría de los circuitos cuánticos que se explorarán en este trabajo, las puertas cuánticas serán justamente eso: rotaciones de cúbits. A continuación, se presenta una representación matricial de estas rotaciones.

$$U_{\theta,\phi,\psi} := \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\psi}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\psi+\phi)}\cos\frac{\theta}{2} \end{pmatrix}.$$

La matriz anterior depende de tres parámetros: Los *ángulos de Euler* θ, ϕ, ψ. Esta puerta representa todas las posibles puertas sobre un cúbit siempre que no nos preocupemos por la fase global de un estado. Cuando no es permitido descartar la fase global de un cúbit, es necesario añadir un factor de fase γ de manera que

$$U_{\theta,\phi,\psi,\gamma} := e^{i\gamma}\begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\psi}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\psi+\phi)}\cos\frac{\theta}{2} \end{pmatrix}.$$

Ejemplo 22. *Un cálculo directo muestra que las puertas de Pauli, σ_x, σ_y y σ_z se pueden expresar en la forma*

$$\sigma_x = U_{\pi,0,\pi,0} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = U_{\pi,0,\pi/2,0} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = U_{0,0,\pi,0} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ejemplo 23. *Para ciertos valores de $\theta, \phi, \psi, \gamma$ tambien es posible definir nuevas puertas cuánticas que actúen como la forma negativa de las puertas de Pauli vistas en el ejemplo anterior, en efecto*

$$U_{\pi,2\pi,\pi,0} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad U_{\pi,\frac{3\pi}{2},\frac{3\pi}{2},0} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad U_{2\pi,\frac{\pi}{2},\frac{\pi}{2},0} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

que representan las puertas $-\sigma_x, -\sigma_y, -\sigma_z$ respectivamente

Al igual que se hizo para la puerta $U_{PS,\Phi}$, en donde se definió la puerta de control $U_{CPS,\Phi}$, se presenta a continuación una versión general de una puerta de control. En este caso, se involucran dos cúbits, por lo que no es posible ignorar la fase global de cada cúbit. Así pues, la puerta de control unitaria $C - U_{\theta,\phi,\lambda,\gamma}$ está dada en su forma matricial por

$$C - U_{\theta,\phi,\lambda,\gamma} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\gamma}\cos\frac{\theta}{2} & -e^{i(\gamma+\lambda)}\sin\frac{\theta}{2} \\ 0 & 0 & e^{i(\gamma+\phi)}\sin\frac{\theta}{2} & e^{i(\gamma+\lambda+\phi)}\cos\frac{\theta}{2} \end{pmatrix}.$$

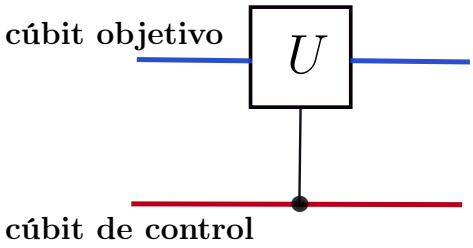

Figura 3.5: Esquema de un circuito cuántico conformado por 2-cúbits y una puerta de control $C - U_{\theta,\phi,\lambda,\gamma}$. La interpretación de este símbolo es: aplicamos el operador identidad sobre el cúbit objetivo si el cúbit de control es $|0\rangle$ y aplicamos la puerta U si el cúbit de control es $|1\rangle$.

Luego, por definición, se tiene que

$$\begin{aligned}
(C - U_{\theta,\phi,\lambda,\gamma})\,|00\rangle &= I\,|0\rangle \otimes I\,|0\rangle = |00\rangle\,.\\
(C - U_{\theta,\phi,\lambda,\gamma})\,|01\rangle &= I\,|0\rangle \otimes I\,|1\rangle = |01\rangle\,.\\
(C - U_{\theta,\phi,\lambda,\gamma})\,|10\rangle &= I\,|1\rangle \otimes U_{\theta,\phi,\lambda,\gamma}\,|0\rangle\,,\\
&= |1\rangle \left(e^{i\gamma}\sin\frac{\theta}{2}\,|0\rangle + e^{i(\gamma+\phi)}\sin\frac{\theta}{2}\,|1\rangle\right),\\
&= e^{i\gamma}\sin\frac{\theta}{2}\,|10\rangle + e^{i(\gamma+\phi)}\sin\frac{\theta}{2}\,|11\rangle\,.\\
(C - U_{\theta,\phi,\lambda,\gamma})\,|11\rangle &= I\,|1\rangle \otimes U_{\theta,\phi,\lambda,\gamma}\,|1\rangle\,,\\
&= |1\rangle \left(e^{i(\gamma+\lambda)}\sin\frac{\theta}{2}\,|0\rangle + e^{i(\gamma+\lambda+\phi)}\cos\frac{\theta}{2}\,|1\rangle\right),\\
&= e^{i(\gamma+\lambda)}\sin\frac{\theta}{2}\,|10\rangle + e^{i(\gamma+\lambda+\phi)}\cos\frac{\theta}{2}\,|11\rangle\,.
\end{aligned}$$

Lo anterior implica que si el cúbit de control respecto a la correspondiente base es $|0\rangle$ entonces no se modifica el cúbit objetivo, y si el cúbit de control es $|1\rangle$ entonces se aplica la puerta unitaria U sobre el cúbit objetivo. Por último, un cálculo directo comprueba que

$$C - U_{\theta,\phi,\lambda,\gamma} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_{\theta,\phi,\lambda,\gamma}.$$

Ejemplo 24. *Un cálculo directo muestra que*

$$C - U_{\pi,0,\pi,0} := \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

La matriz anterior representa la puerta de Pauli σ_x, que esta vez actúa como puerta de control y solo se aplica al segundo cúbit cuando el primer cúbit es 1, para un sistema de 2 cúbits. Esta puerta también es conocida como la puerta CNOT.

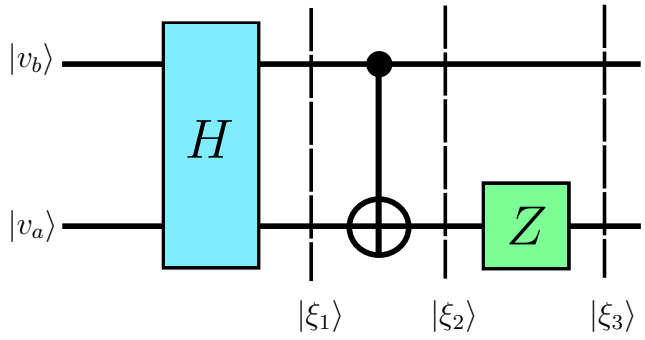

Figura 3.6: Esquema de un circuito cuántico conformado por 2-cúbits $|\xi_0\rangle = |v_a\rangle \otimes |v_b\rangle$, dos puertas de Hadamard, una puerta CNOT controlada y la puerta Z, también conocida como la puerta de Pauli σ_z. El cúbit de control es $|v_b\rangle$ y el cúbit objetivo es $|v_a\rangle$.

Ejemplo 25. *Sea el circuito de la figura 3.6. A continuación se halla su respectiva representación matricial, bajo la base estándar, siguiendo el mismo planteamiento del ejemplo 21*

Para $|\xi_0\rangle = |00\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big),$$
$$|\xi_2\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big),$$
$$|\xi_3\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big).$$

Para $|\xi_0\rangle = |01\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big),$$
$$|\xi_2\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle - |10\rangle + |11\rangle\,\big),$$
$$|\xi_3\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle - |10\rangle - |11\rangle\,\big).$$

Para $|\xi_0\rangle = |10\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle - |10\rangle - |11\rangle\,\big),$$
$$|\xi_2\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle - |10\rangle - |11\rangle\,\big),$$
$$|\xi_3\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle - |10\rangle + |11\rangle\,\big).$$

Para $|\xi_0\rangle = |11\rangle$

$$|\xi_1\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle - |10\rangle + |11\rangle\,\big),$$
$$|\xi_2\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big),$$
$$|\xi_3\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big).$$

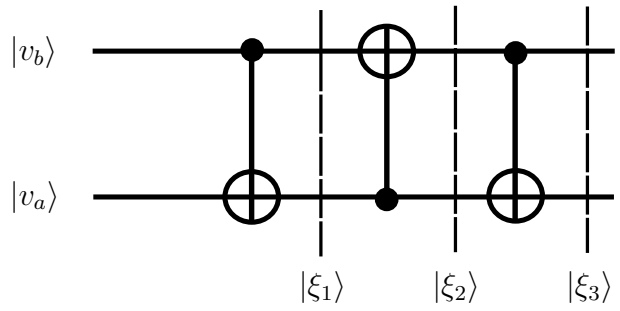

Figura 3.7: Esquema de un circuito cuántico conformado por 2-cúbits $|\xi_0\rangle = |v_a v_b\rangle$ y 3 puertas de control CNOT. En este circuito, el cúbit de control y el cúbit objetivo cambian en cada paso, a diferencia de ejemplos anteriores

Luego la representacion matricial del circuito esta dado por

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

Ejemplo 26. *Sea el circuito de la figura 3.7. A continuación se halla su respectiva representación matricial, bajo la base estándar, siguiendo el mismo planteamiento del ejemplo 21*

$$\begin{array}{llll} |\xi_0\rangle = |00\rangle & |\xi_0\rangle = |01\rangle & |\xi_0\rangle = |10\rangle & |\xi_0\rangle = |11\rangle, \\ |\xi_1\rangle = |00\rangle & |\xi_1\rangle = |01\rangle & |\xi_1\rangle = |11\rangle & |\xi_1\rangle = |10\rangle, \\ |\xi_2\rangle = |00\rangle & |\xi_2\rangle = |11\rangle & |\xi_2\rangle = |01\rangle & |\xi_2\rangle = |10\rangle, \\ |\xi_3\rangle = |00\rangle & |\xi_3\rangle = |10\rangle & |\xi_3\rangle = |01\rangle & |\xi_3\rangle = |11\rangle. \end{array}$$

Luego la representación matricial está dada por

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

3.5. Conclusiones

Como se pudo observar en este capítulo, la importancia de las matrices unitarias radica en su uso como representación matemática hacia las puertas cuánticas utilizadas en este trabajo, esto gracias a su propiedad de mantener las características entre los vectores al aplicar operaciones. Al hablar de circuitos y puertas cuánticas, el lector puede apreciar que se hace especial énfasis en la puerta de Hadamard y la transformada de Fourier cuántica (TFC). De hecho, el uso de la puerta de Hadamard para obtener estados de superposición

homogéneos a partir de estados base y la TFC como el operador más complejo visto hasta ahora juegan un papel fundamental en el desarrollo del algoritmo HHL. Pero antes, se presenta al lector el algoritmo de estimación cuántica de fase en el capítulo siguiente, un algoritmo que estima la fase de los valores propios de alguna matriz de rotación unitaria y que sirve como última herramienta a tener en cuenta antes de finalmente dar paso al algoritmo HHL.

Capítulo 4

Estimación cuántica de fase

A partir de los conceptos sobre computación cuántica vistos en capítulos previos, se presenta en este capítulo el algoritmo cuántico de estimación de fase. Se comienza introduciendo el concepto de fase a partir de la definición de valor propio visto en la sección 1.4.6. Se continúa introduciendo el algoritmo de manera informal mediante un ejemplo extenso dividido en dos casos puntuales aplicados a un sistema de 1 y 2 cúbits; se prosigue explicando ya de manera detallada cada paso del algoritmo y las puertas cuánticas implicadas dentro del mismo para finalizar con algunos ejemplos, no solo de este, sino también de otros algoritmos básicos que ayuden al lector a comprender mejor cómo manejar operaciones entre circuitos cuánticos.

Considérese una matriz unitaria $U \in \mathbb{M}_{m\times m}(\mathbb{C})$ donde $\lambda \in \mathbb{C}$ es un correspondiente valor propio con vector propio asociado $|v\rangle$. Siguiendo la demostración del Teorema 1 (Capítulo 1), nótese que $U|v\rangle = \lambda|v\rangle$ equivale a $\langle v|U^\dagger = \lambda^*\langle v|$. Por lo tanto,

$$\langle v|U^\dagger U|v\rangle = \lambda^*\langle v|\lambda v\rangle \quad \Rightarrow \quad \langle v|v\rangle = |\lambda|\langle v|v\rangle,$$

probándose así que cualquier propio λ de U tiene módulo $|\lambda| = 1$. Por ende, todo valor propio de una matriz unitaria se puede expresar en la forma $\lambda = e^{i\theta_\lambda}$ con $\theta_\lambda \in [0, 2\pi]$ un argumento de λ. Para propósitos prácticos, se supondrá a partir de este punto que $\theta_\lambda = 2\pi\psi_\lambda$ con $\psi_\lambda \in [0, 1]$. El principal objetivo del *algoritmo de estimación cuántica de fase* (que denotamos por QPE por las siglas en inglés de *Quantum Phase Estimation*) consiste en (como bien se deduce del nombre) estimar ψ_λ (fase del valor propio λ). A continuación se hace uso de un ejemplo con el objetivo de dar una introducción al funcionamiento de este algoritmo.

Ejemplo 27. *Sea la siguiente matriz unitaria* $U = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}$. *Un cálculo directo muestra que el espectro de* U *está dado por* $\rho(U) = \{i, -1\}$. *Con* $\lambda_0 = i$ *y* $\lambda_1 = -1$, *se deduce que*

$$\lambda_0 = e^{i2\pi/4} \quad y \quad \lambda_1 = e^{i2\pi/2},$$

por lo tanto, $\psi_{\lambda_0} = 1/4$ *y* $\psi_{\lambda_1} = 1/2$ *son las correspondientes fases. De otro lado, los vectores propios* $|b_0\rangle$ *y* $|b_1\rangle$ *asociados a cada valor propio son*

$$|b_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad y \quad |b_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

respectivamente. ¿Cuál es entonces el objetivo del algoritmo? Es estimar ψ_{λ_0} *y* ψ_{λ_1}.

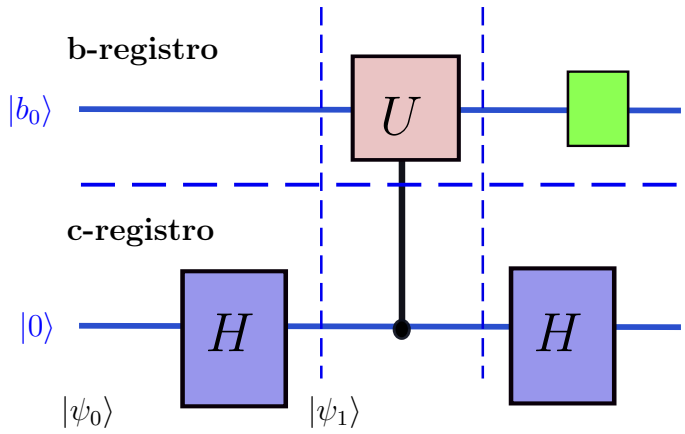

Figura 4.1: Circuito correspondiente al algoritmo de estimación cuántica de fase sobre el primer valor propio $\lambda_0 = e^{i2\pi/4}$ de la puerta cuántica U del Ejemplo 27.

El algoritmo consta de dos tipos de entradas: ***cúbits menos significativos*** *(llamados* ***b-registros****) y los* ***cúbits más significativos*** *(llamados* ***c-registros****). Para este ejemplo, el cúbit menos significativo será uno de los vectores propios de U.*

A continuación, dado que U es una matriz 2×2, solo será necesario un cúbit para registrar un vector propio (esto tomando en cuenta que la representación vectorial de un cúbit es $\mathbb{C}^2$). Se toma $|b_1\rangle$. En tal caso,

$$\begin{aligned} U|b_0\rangle = \lambda_0|b_0\rangle \quad y \quad U^2|b_0\rangle = \lambda_0^2|b_0\rangle, \\ U|b_1\rangle = \lambda_1|b_1\rangle \quad y \quad U^2|b_1\rangle = \lambda_1^2|b_1\rangle. \end{aligned}$$

Ahora bien, el resultado final del algoritmo depende de la cantidad de cúbits inscritos en el c-registro. A partir de esto se divide este ejemplo en dos casos particulares.

Caso 1. ***c*-registro con un solo cúbit.** *La entrada en el c-registro será el cúbit $|0\rangle$. En total tenemos 1+1=2 cúbits en nuestro circuito (ver Figura 4.1). Tal como se aprecia en el circuito, iniciamos con*

$$|\psi_0\rangle = |0\rangle|b_0\rangle.$$

Primero se aplica una puerta Hadamard en el c-registo para obtener el cúbit $H|0\rangle$. Posteriormente, el nuevo estado en el circuito está dado por

$$\begin{aligned} |\psi_1\rangle &= (H \otimes I)|\psi_0\rangle|b_0\rangle, \\ |\psi_1\rangle &= H|0\rangle \otimes |b_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|b_0\rangle, \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|b_0\rangle + |1\rangle|b_0\rangle). \end{aligned}$$

Avanzando en el circuito, se aplica ahora la puerta de control U. De esta forma

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|b_0\rangle + |1\rangle U|b_0\rangle), \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|b_0\rangle + |1\rangle\lambda_0|b_0\rangle) = \frac{1}{\sqrt{2}}\sum_{s=0}^{1}\lambda_0^s|s\rangle|b_0\rangle. \end{aligned}$$

El objetivo del proceso anterior es escribir cierta información correspondiente al valor propio λ_0 en la fase relativa del primer cúbit en superposición del c-registro. Es decir, esencialmente, todo el objetivo fue implementar la siguiente transformación.

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \mapsto \frac{1}{\sqrt{2}}(|0\rangle + \lambda_0 |1\rangle).$$

Con la transformación hecha, ahora se busca extraer la información de λ_0. Para extraer la información de la fase a partir de este último estado, se aplica la TFC, que en el caso de un cúbit en el c-registro equivale a aplicar la puerta de Hadamard H. (ver Ejemplo 17). De forma más precisa, aplicamos el operador $H \otimes I$ sobre el estado actual del circuito, esto es:

$$|\psi_4\rangle = H \otimes I\Big(\frac{1}{\sqrt{2}} \sum_{s=0}^{1} \lambda_0^s |s\rangle |b_0\rangle \Big),$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}} \sum_{s=0}^{1} \lambda_0^s H |s\rangle |b_0\rangle = \frac{1}{\sqrt{2}} \sum_{s=0}^{1} (e^{i2\pi\psi_{\lambda_0}})^s \Big(\frac{1}{\sqrt{2}} \sum_{k=0}^{1} w^{-ks} |k\rangle \Big) |b_0\rangle ,$$

con $w = e^{i2\pi/2}$. De esta forma, se llega a la siguiente expresión

$$|\xi_4\rangle = \frac{1}{2} \sum_{s,k=0}^{1} w^{s(2\psi_{\lambda_0}-k)} |k\rangle |b_0\rangle = \frac{1}{2} \sum_{k=0}^{1} \Big(\sum_{s=0}^{1} w^{s(2\psi_{\lambda_0}-k)} |k\rangle \Big) |b_0\rangle ,$$

$$|\xi_4\rangle = \frac{1}{2}\big((1 + w^{2\psi_{\lambda_0}}) |0\rangle + (1 + w^{(2\psi_{\lambda_0}-1)}) |1\rangle \big) |b_0\rangle ,$$

para así obtener

$$|\xi_4\rangle = \frac{1}{2}\big((1 + w^{2\psi_{\lambda_0}}) |0\rangle + (1 - w^{2\psi_{\lambda_0}}) |1\rangle \big) |b_0\rangle .$$

Se observa a continuación que este estado en superposición posee información de la fase ψ_{λ_0} en cada amplitud. Lo anterior en primera instancia significaría que es posible obtener la información deseada de la fase en cualquier medición hecha al estado de superposición (no importa con qué estado base caiga. Siempre tendrá la información de la fase), sin embargo, de esta expresión final pueden resultar extraños comportamientos. Supóngase el siguiente estado.

$$|v_\alpha\rangle = \frac{1}{2}\big((1 + e^{i2\pi\alpha}) |0\rangle + (1 - e^{i2\pi\alpha}) |1\rangle \big).$$

Al medir $|v_\alpha\rangle$, las probabilidades $P_0(\alpha)$ y $P_1(\alpha)$ de obtener el estado $|0\rangle$ y $|1\rangle$ son

$$P_0(\alpha) = \Big|\frac{1 + e^{i2\pi\alpha}}{2}\Big|^2 = \cos^2(\pi\alpha) \quad y \quad P_1(\alpha) = \Big|\frac{1 + e^{i2\pi\alpha}}{2}\Big|^2 = \mathrm{sen}^2(\pi\alpha),$$

respectivamente. De la Tabla 4.1 se observa que si medimos el estado

$$|v_{1/4}\rangle = \frac{1}{2}\big((1 + \lambda_0) |0\rangle + (1 - \lambda_0) |1\rangle \big),$$

es equiprobable obtener el estado cero $|0\rangle$ o el estado $|1\rangle$ con valor de probabilidad $p = 0.5$. Lo anterior no es tan beneficioso para nuestro ejemplo porque se sabe que el estado propio

Distribución de probabilidades respecto de α						
$\alpha = 0$	$\alpha = 1/8$	$\alpha = 1/4$	$\alpha = 1/2$	$\alpha = 3/4$	$\alpha = 7/8$	$\alpha = 1$
$P_0 = 1$	$P_0 = \frac{2+\sqrt{2}}{4}$	$P_0 = 0.5$	$P_0 = 0$	$P_0 = 0.5$	$P_0 = \frac{2+\sqrt{2}}{4}$	$P_0 = 1$
$P_1 = 0$	$P_1 = \frac{2-\sqrt{2}}{4}$	$P_1 = 0.5$	$P_1 = 1$	$P_1 = 0.5$	$P_0 = \frac{2-\sqrt{2}}{4}$	$P_1 = 0$

Cuadro 4.1: Probabilidad de las mediciones para el estado $|v_\alpha\rangle$

correspondiente a λ_0 *es* $|0\rangle$*. Sin embargo, si se considera ahora el valor propio* λ_1 *y se procede de la misma forma, se obtiene*

$$|\xi_4\rangle = \frac{1}{2}\big((1 + w^{2\psi\lambda_1})\,|0\rangle + (1 - w^{2\psi\lambda_1})\,|1\rangle\big)\,|b_1\rangle = |1\rangle\,|b_1\rangle\,.$$

De vuelta a la Tabla 4.1, se puede observar que con $\alpha = 0$ *medimos con total certeza (es decir, con probabilidad* $p = 1$*) un estado (en el c-registro) que nos dice exactamente cuál es la fase, el valor propio e incluso el vector propio correspondiente. Entonces, ¿qué hace al método ser efectivo o no a la hora de estimar la fase de un estado propio? Véase ahora lo que ocurre cuando se ingresan dos cúbits en el c-registro.*

Caso 2. *c*-registro con dos cúbits. *Considérese ahora que en el c-registro se tienen dos cúbits de estado base* $|0\rangle$*. En general, los cúbits en el c-registro serán usados para registrar un valor asociado a* ψ *el cual es* $2^n\psi$ *siendo* n *el número de cúbits en el c-registro. Así que, para este caso, se tiene* $2^n\psi = 4\psi$*. En total tenemos* $2 + 1 = 3$ *cúbits en nuestro circuito. A diferencia del Caso 1. Ahora se considera el vector propio* $|b_1\rangle$ *solo por variar un poco. Tal como se aprecia en el circuito 4.2, se inicia con*

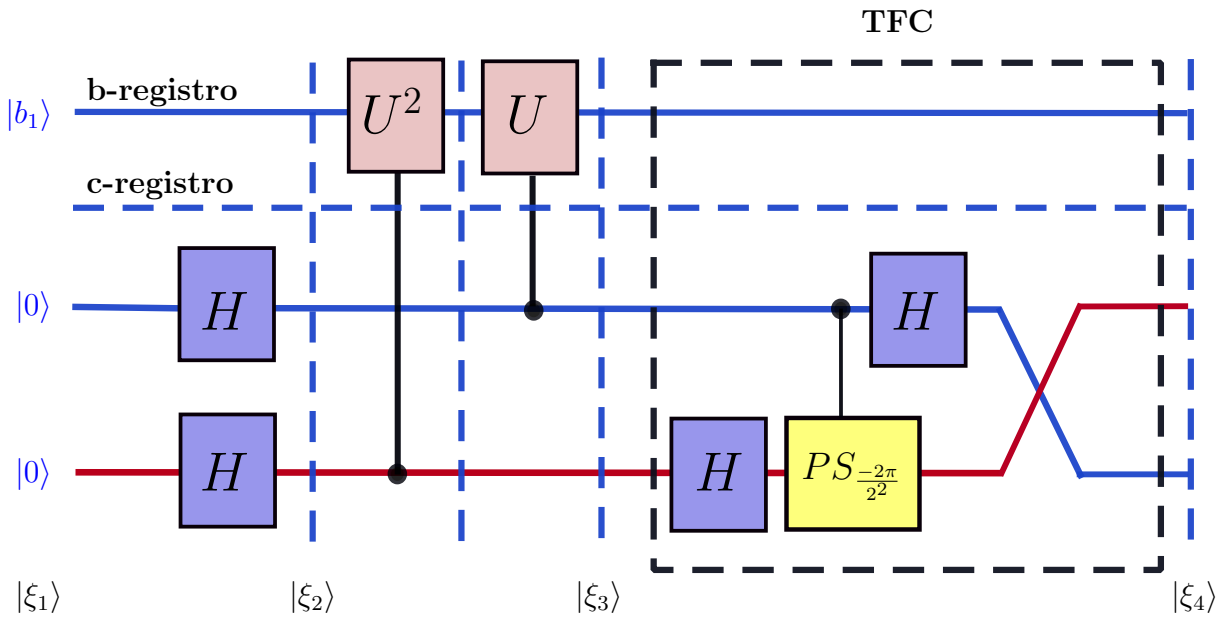

Figura 4.2: Circuito correspondiente al algoritmo de estimación cuántica de fase sobre el segundo valor propio $\lambda_1 = e^{i2\pi/2}$ de la puerta cuántica U del Ejemplo 27.

$$|\xi_1\rangle = |0\rangle\,|0\rangle\,|b_1\rangle\,.$$

El algoritmo ahora inicia con dos puertas cuánticas de Hadamard H actuando sobre cada estado $|0\rangle$ (tal y como en los circuitos 3.3 y 3.4 del ejemplo 21) para crear una superposición uniforme en el c-registro. Por ende $|\xi_1\rangle \to |\xi_2\rangle$ en donde

$$\begin{aligned}
|\xi_2\rangle &= H \otimes H \otimes I(|0\rangle\,|0\rangle\,|b_1\rangle),\\
|\xi_2\rangle &= \frac{1}{\sqrt{2}^2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |b_1\rangle\,,\\
|\xi_2\rangle &= \frac{1}{\sqrt{2}^2}\big(\,|00\rangle\,|b_1\rangle + |01\rangle\,|b_1\rangle + |10\rangle\,|b_1\rangle + |11\rangle\,|b_1\rangle\,\big).
\end{aligned}$$

Avanzando por el circuito, a continuación se implementan las puertas de control. Cada cúbit de control actúa como el bit de control de la puerta U o U^2. El cúbit $|0\rangle$ (el bit menos significativo) en el c-registro es el cúbit de control de la puerta $U = U^{2^0}$. Mientras que el cúbit $|1\rangle$ (el bit más significativo) en el c-registro es el cúbit de control de la puerta $U^2 = U^{2^1}$. De esta forma:

$$\begin{aligned}
|\xi_3\rangle &= \frac{1}{\sqrt{2}^2}\big(\,|00\rangle\,|b_1\rangle + |01\rangle\,U\,|b_1\rangle + |10\rangle\,U^2\,|b_1\rangle + |11\rangle\,U^2U\,|b_1\rangle\,\big),\\
|\xi_3\rangle &= \frac{1}{\sqrt{2}^2}\big(\,|00\rangle\,U^0U^0\,|b_1\rangle + |01\rangle\,U^0U\,|b_1\rangle + |10\rangle\,U^2U^0\,|b_1\rangle + |11\rangle\,U^2U\,|b_1\rangle\,\big),\\
|\xi_3\rangle &= \frac{1}{\sqrt{2}^2}\big(\,|00\rangle\,U^{0+0}\,|b_1\rangle + |01\rangle\,U^{0+1}\,|b_1\rangle + |10\rangle\,U^{2+0}\,|b_1\rangle + |11\rangle\,U^{2+1}\,|b_1\rangle\,\big).
\end{aligned}$$

En forma binaria, la expresión anterior queda en la forma

$$\begin{aligned}
|\xi_3\rangle &= \frac{1}{\sqrt{2}^2}\big(\,|0\rangle\,U^0\,|b_1\rangle + |1\rangle\,U^1\,|b_1\rangle + |2\rangle\,U^2\,|b_1\rangle + |3\rangle\,U^3\,|b_1\rangle\,\big),\\
&= \frac{1}{\sqrt{2}^2}\sum_{s=0}^{3}|s\rangle\,U^s\,|b_1\rangle = \frac{1}{\sqrt{2}^2}\sum_{s=0}^{3}\lambda_1^s\,|s\rangle\,|b_1\rangle = \frac{1}{\sqrt{2}^2}\sum_{s=0}^{3}(e^{i2\pi/2})^s\,|s\rangle\,|b_1\rangle\,.
\end{aligned}$$

A continuación, el siguiente paso en el circuito es aplicar el operador TFC. Se recuerda que dados dos vectores base $|s\rangle$ y $|k\rangle$ se tiene

$$\mathcal{U}\,|s\rangle = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} w^{-ks}\,|k\rangle\,. \tag{4.1}$$

Se aplica entonces el operador $\mathcal{U} \otimes I$ sobre $|\xi_3\rangle$ (siempre sobre el c-registro y no sobre el b-registro)

$$\begin{aligned}
|\xi_4\rangle &= \mathcal{U} \otimes I\Big(\frac{1}{\sqrt{2}^2}\sum_{s=0}^{3}(e^{i2\pi/2})^s\,|s\rangle\,|b_1\rangle\,\Big),\\
|\xi_4\rangle &= \frac{1}{\sqrt{2}^2}\sum_{s=0}^{3}(e^{i2\pi/2})^s\mathcal{U}\,|s\rangle\,|b_1\rangle = \frac{1}{\sqrt{2}^2}\sum_{s=0}^{3}w^{2s}\Big(\frac{1}{2}\sum_{k=0}^{3}w^{-ks}\,|k\rangle\,\Big)\,|b_1\rangle\,,
\end{aligned}$$

con $w = e^{i2\pi/4}$. De esta forma, se obtiene la siguiente expresión

$$|\xi_4\rangle = \frac{1}{4}\sum_{s,k=0}^{3} w^{s(2-k)}\,|k\rangle\,|b_1\rangle = \frac{1}{4}\sum_{k=0}^{3}\Big(\sum_{s=0}^{3} w^{s(2-k)}\,|k\rangle\Big)\,|b_1\rangle\,.$$

Es aquí donde recordamos el Ejemplo 16 de la Sección 3.3, en donde entra en juego la interferencia destructiva siempre que $k \neq 2$ o constructiva si $2-k=0$, esto es, $k=2$. Por lo tanto

$$|\xi_4\rangle = \frac{1}{4}\sum_{k=0}^{3}\Big(\sum_{s=0}^{3} w^{s(2-k)}\Big)\,|k\rangle\,|b_1\rangle = |2\rangle\,|b_1\rangle\,.$$

Lo anterior tiene un significado mayor. Se sabe bien que $\psi_{\lambda_1} = 1/2$ y que además su valor asociado en el c-registro es $2^n\psi_{\lambda_1}$. Pues justamente, el resultado $k=2$ coincide con el producto $2^n\psi_{\lambda_1}$ para $n=2$ (el número de cúbits en el c-registro). Lo anterior es más que una coincidencia, pues, en general, para el algoritmo de estimación cuántica de fase QPE, si medimos el estado $|k\rangle$ en un n-cubít c-registro siendo el $|b\rangle$-registro un vector propio asociado al valor propio $\lambda = e^{i2\pi\psi}$ la fase satisface la igualdad

$$2\pi\psi = 2\pi k/2^n \quad \Leftrightarrow \quad \psi = k/2^n,$$

concluyendo así nuestro ejemplo.

4.1. Ahora si...el algoritmo QPE

Detallando algunas observaciones puntuales del ejemplo anterior. Nótese que en el caso 2 se evaluó el valor de fase $\psi_{\lambda_1} = 1/2$ para computar el estado $|\xi_4\rangle$. Lo anterior no tendría mucha lógica para los propósitos de este algoritmo, que es estimar un valor de fase desconocido. ¿Para qué fue todo lo anterior si en el algoritmo usamos el valor de la fase que queremos estimar, conociendo de antemano cada valor propio? A continuación se explora en detalle el algoritmo QFE para dar respuesta a este y a otros posibles inconvenientes generados. Cabe aclarar que la última afirmación del Caso 2 tiene una razón de ser que se observará más adelante.

El algoritmo de estimación de fase tiene el objetivo de *estimar la fase* de los valores propios de una matriz de rotación unitaria U, los cuales, se sabe bien, son raíces de la unidad. Este algoritmo actúa sobre dos grupos de cúbits y consta de tres etapas. El primer grupo será formado por n_b-cúbits llamados b-registro (identificados como los cúbits menos significativos) que se denotan por

$$|b\rangle_{n_b} = \sum_{s=0}^{2^{n_b}-1} \beta_s\,|s\rangle\,,$$

con $\beta_s \in \mathbb{C}$. El segundo grupo está conformado por n-cúbits llamados c-registro (estos se identifican como los cúbits más significativos) que están dados por

$$|0\rangle_n := |0\rangle^{\otimes n} = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle\,.$$

De esta manera, el estado inicial del algoritmo es el $(n+n_b)$-cúbit

$$|\xi_0\rangle = |0\rangle_n \otimes |b\rangle_{n_b}\,.$$

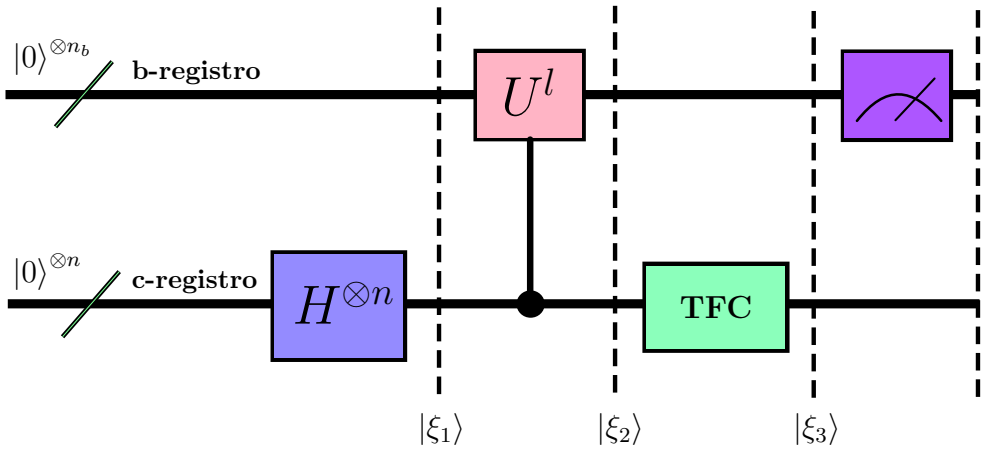

Figura 4.3: Circuito correspondiente al algoritmo de estimación cuántica de fase de forma general. La puerta controlada U^l se aplica en el l-ésimo cubit del b-registro y el paso final representa la medición aplicada a $|\xi_3\rangle$.

En la etapa 1 del algoritmo se realiza la superposición de n-cúbits de estado en el c-registro por medio de puertas de Hadamard. En la etapa 2 se realiza una *rotación controlada* de una componente de los c-registros por medio de puertas cuánticas tipo U^{2^l} con $l \in \{0, 1, \ldots n-1\}$ y en la etapa 3 se aplica la Transformada de Fourier cuántica TFC sobre un estado base, para que dicho estado sea rotado a una superposición entre todos los estados base en donde los coeficientes de dicha superposición son las potencias de la N-ésima raíz de la unidad, siendo $N = 2^n$, eso último con el propósito de medir un estado base y extraer la información de la fase valor propio asociada al vector propio del b-registro, codificada en el c-registro. A continuación se describe cada etapa del algoritmo.

Etapa 1. Las puertas de Hadamard son aplicadas a los cúbits en el c-registro para crear un estado de superposición uniforme.

$$|\xi_0\rangle \to |\xi_1\rangle = (H^{\otimes n} \otimes I)\,|\xi_0\rangle\,,$$
$$|\xi_1\rangle = \frac{1}{2^{\frac{n}{2}}}(|0\rangle + |1\rangle)^{\otimes n}\,|0\rangle_n\,|b\rangle_{n_b}\,.$$

Etapa 2. Las puertas controladas son aplicadas al cúbit $|b\rangle$ tomando a los cúbits en el c-registro como los cúbits de control. El número n de cúbits en el c-registro determina el número de puertas de control, las cuales, como se ha dicho antes, son de la forma U^{2^l}. Así, el cúbit $|c_{l-1}\rangle$ en el c-registro es el cúbit de control de la puerta $U^{2^{l-1}}$ que actúa sobre el b-registro. Por lo tanto, el cúbit más significativo $|c_{n-1}\rangle$ es el cúbit de control de la puerta $U^{2^{n-1}}$ mientras que el cúbit menos significativo es el cúbit de control de la puerta $U^0 = U$. Suponga que $\lambda = e^{i2\pi\phi}$ es un valor propio de U con vector propio asociado $|b\rangle$. En consecuencia,

$$U\,|b\rangle = e^{i2\pi\phi}\,|b\rangle \quad \Leftrightarrow \quad U^{2^l}\,|b\rangle = e^{(i2\pi\phi)2^l}\,|b\rangle\,.$$

Cuando el cúbit de control es $|0\rangle$, entonces I se aplica al vector $|b\rangle$ mientras que si el cúbit de control es $|1\rangle$, U se aplica al vector $|b\rangle$. Lo anterior equivale a multiplicar el

número complejo $e^{(i2\pi\phi)2^l}$ al estado $|1\rangle$ del c_l registro. De esta forma

$$|\xi_2\rangle = \frac{1}{2^{\frac{n}{2}}}(|0\rangle + e^{(i2\pi\phi)2^{n-1}}|1\rangle) \otimes (|0\rangle + e^{(i2\pi\phi)2^{n-2}}|1\rangle) \otimes (|0\rangle + e^{(i2\pi\phi)2^{n-3}}|1\rangle)\dots$$
$$\dots(|0\rangle + e^{(i2\pi\phi)2^2}|1\rangle) \otimes (|0\rangle + e^{(i2\pi\phi)2}|1\rangle) \otimes (|0\rangle + e^{(i2\pi\phi)2^0}|1\rangle)|b\rangle_{n_b},$$
$$|\xi_2\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{s=0}^{2^{n-1}} e^{(i2\pi\phi)s}|s\rangle|b\rangle_{n_b}.$$

Nótese que esta última expresión con $w = e^{i2\pi/2^n}$ se puede expresar en la forma

$$|\xi_2\rangle = \mathcal{U}^{-1}(|2^n\phi\rangle)|b\rangle_{n_b}.$$

Etapa 3. Se aplica el operador TFC al c-registro para extraer la información de la fase consignada en los cúbits de dicho registro.

$$|\xi_3\rangle = \mathcal{U}\otimes I(\frac{1}{2^{\frac{n}{2}}}\sum_{s=0}^{2^{n-1}} e^{(i2\pi\phi)s}|s\rangle|b\rangle_{n_b}) = \frac{1}{2^{\frac{n}{2}}}\sum_{s=0}^{2^{n-1}} e^{(i2\pi\phi)s}\mathcal{U}|s\rangle|b\rangle_{n_b}.$$

A partir de (4.1) el estado final del método está dado por

$$\begin{aligned}|\xi_3\rangle &= \frac{1}{2^{\frac{n}{2}}}\sum_{s=0}^{2^n-1} e^{(i2\pi\phi)s}\Big(\frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} w^{-ks}|k\rangle\Big)|b\rangle_{n_b},\\ |\xi_3\rangle &= \frac{1}{2^n}\sum_{k=0}^{2^n-1}\Big(\sum_{s=0}^{2^n-1} w^{(2^n\phi-k)s}\Big)|k\rangle|b\rangle_{n_b}.\end{aligned} \tag{4.2}$$

Se observa que el último estado obtenido es una combinación lineal de los estados base $|k\rangle|b\rangle_{n_b}$ en la forma

$$|\xi_3\rangle = \sum_{k=0}^{2^n-1}\alpha_k|k\rangle|b\rangle_{n_b} \quad \text{con} \quad \alpha_k = \frac{1}{2^n}\sum_{s=0}^{2^n-1} w^{(2^n\phi-k)s}. \tag{4.3}$$

En general, $w^{(2^n\phi-k)s} = e^{i2\pi(\phi-\frac{k}{2^n})s} \neq 1$ para $k \neq 2^n$. A partir de aquí, los coeficientes α_k son sumas de distintos números complejos (distintas fases). En consecuencia

$$\lim_{n\to\infty}\alpha_k = 0, \quad \text{si} \quad k \neq 2^n.$$

De lo anterior, supóngase que $2^n\phi \in \mathbb{Z}^+$, luego existe un k tal que $2^n\phi - k = 0$. Del resultado visto en el Ejemplo 16 de la sección 3.3 se deduce que solo el estado $|k\rangle$ tendrá amplitud $\sum_{s=0}^{2^n-1} w^{(2^n\phi-k)s} = 2^n$ y los demás tendrán amplitud $\sum_{s=0}^{2^n-1} w^{(2^n\phi-k)s} = 0$. A partir de aquí se tiene

$$2^n|\xi_3\rangle = \Big(\sum_{s=0}^{2^n-1} w^{(2^n\phi)s}|0\rangle + \dots \sum_{s=0}^{2^n-1}|2^n\phi\rangle + \dots + \sum_{s=0}^{2^n-1} w^{(2^n\phi-(2^n-1))s}|2^n-1\rangle\Big)|b\rangle_{n_b},$$
$$2^n|\xi_3\rangle = \sum_{s=0}^{2^n-1}|2^n\phi\rangle|b\rangle_{n_b},$$

por lo tanto

$$|\xi_3\rangle = |2^n\phi\rangle\,|b\rangle_{n_b}\,.$$

Se observa que en el c-registro la amplitud no nula corresponde al estado $|2^n\phi\rangle$. Más aún, dicha amplitud es $e^{i2\pi} = 1$. En resumen, si $2^n\phi$ es entero positivo y medimos el estado $|2^n\phi\rangle$ de un c-registro conformado por n cúbits y para la matriz unitaria U el b-registro $|b\rangle_{n_b}$ es un vector propio asociado al valor propio $\lambda = e^{i2\pi\phi}$ entonces

$$2\pi\phi = 2\pi\frac{k}{2^n}.$$

¿Qué ocurre si $2^n\phi \notin \mathbb{Z}^+$? Sea ν el entero más cercano a $2^n\phi$. En tal caso, se tiene

$$2^n\phi = \nu + 2^n\varepsilon, \quad \text{con} \quad 0 \leq |2^n\varepsilon| \leq \frac{1}{2}.$$

Al sustituir lo anterior en (4.2)

$$|\xi_3\rangle = \sum_{k=0}^{2^n-1} \tilde{\alpha}_k\,|k\rangle\,|b\rangle_{n_b} \quad \text{con} \quad \tilde{\alpha}_k = \frac{1}{2^n}\sum_{s=0}^{2^n-1} w^{(\nu-k)s} w^{2^n\varepsilon s}.$$

A continuación, se busca ahora la probabilidad $P(\nu)$ de que al medir el estado $|\xi_3\rangle$ se obtenga el estado $|\nu\rangle$ sobre el c-registro. Se aplica entonces la fórmula de probabilidad usada para la obtención de los valores de la tabla 4.1.

$$P(\nu) = |\langle\nu|\xi_4\rangle|^2 = \Big|\sum_{k=0}^{2^n-1}\tilde{\alpha}_k\langle\nu|k\rangle\Big|^2 = \big|\tilde{\alpha}_\nu\big|^2 = \frac{1}{2^n}\Big|\sum_{s=0}^{2^n-1} w^{2^n\epsilon s}\Big|^2 = \frac{1}{2^n}\Big|\sum_{s=0}^{2^n-1} e^{i2\pi\epsilon s}\Big|^2,$$

en consecuencia, se tiene que las probabilidades finales de medición son

$$P(\nu) = \begin{cases} 1 & \text{si} \quad \varepsilon = 0, \\ \dfrac{1}{2^{2n}}\left|\dfrac{1-e^{i2\pi 2^n\varepsilon}}{1-e^{i2\pi\varepsilon}}\right|^2 & \text{si} \quad \varepsilon \neq 0, \end{cases} = \begin{cases} 1 & \text{si} \quad \varepsilon = 0, \\ \dfrac{1}{2^{2n}}\dfrac{sen^2(2^n\pi\varepsilon)}{sen^2(\pi\varepsilon)} & \text{si} \quad \varepsilon \neq 0. \end{cases}$$

Note que la probabilidad de obtener el estado $|\nu\rangle$ decrece monotonamente con n. Más aún, el estado final es $|\nu\rangle$ si $\varepsilon = 0$, y en caso contrario, $\varepsilon \neq 0$, se tiene

$$P(\nu) \geq \frac{1}{2^{2n}}\frac{sen^2(2^n\pi 2^{-n}/2)}{sen^2(\pi 2^{-n}/2)} \geq \frac{1}{2^{2n}}\frac{1}{sen^2(\pi 2^{-n}/2)} \geq \lim_{n\to\infty}\frac{4}{\pi^2}\frac{1}{\left(\frac{sen(\pi 2^{-n}/2)}{\pi 2^{-n}/2}\right)^2} = \frac{4}{\pi^2}.$$

Así que, la probabilidad de obtener el estado $|v\rangle$ es por lo menos $4/\pi^2 \approx 40{,}5\,\%$ lo cuál es bastante bueno, pero se puede mejorar usando más cúbits auxiliares, ver Cap.5 Sec. 2 [2].

4.2. Conclusiones

Ya avanzado a este punto en la lectura del documento, el lector tiene claros todos los conceptos necesarios a entender antes de poder comprender siquiera el funcionamiento del algoritmo HHL. El algoritmo QPE es el último de estos conceptos previos y, a pesar de ser parte del mismo algoritmo HHL, posee una finalidad distinta, como bien el lector pudo

observar en este capítulo. Dependiendo de la matriz y la cantidad de cúbits a considerar en el c-registro, se determina la precisión de estimación final que da el algoritmo respecto a la fase de los valores propios asociados, como bien se pudo observar en el desarrollo del ejemplo 25 y los resultados finales observados en los dos casos puntuales. Sin embargo, el lector también podrá haber notado que, a final de cuentas, todo se reduce al paso final del algoritmo. Las probabilidades de obtener el estado correspondiente que guarda la información respecto a la fase buscada a estimar es lo que determina el éxito de los pasos aplicados, y dicho éxito difiere fuertemente incluso en la misma fase (ya sea si es un entero positivo o no). Cuando no se obtiene el estado deseado, es necesario repetir los pasos del algoritmo hasta que la medición final dé como resultado este estado deseado. Lo anterior es clave a tener en cuenta para poder comenzar a introducir formalmente el algoritmo HHL en el siguiente capítulo.

Capítulo 5

El algoritmo HHL

Hemos llegado al capítulo final de este documento, en él presentamos un estudio detallado de la estructura y ejecución de uno de los más recientes algoritmos cuánticos para la resolución de sistemas lineales. Dicho algoritmo llega a la comunidad científica en 2009, publicado en [1] por sus autores Aram Harrow, Avinatan Hassidim y Seth Lloyd, ganando una alta popularidad, siendo actualmente conocido como el *algoritmo HHL*. Este algoritmo usa QPE como subrutina para estimar los valores de la matriz del sistema, así como el uso de la Transformada de Fourier Inversa. Así pues, lo visto en los capítulos previos nos permitirá entender cada paso de este nuevo método de resolver sistemas lineales

$$A\left|x\right\rangle = \left|b\right\rangle, \tag{5.1}$$

con $A \in \mathbb{M}_{N\times N}(\mathbb{C})$ una matriz hermitiana e invertible y $\left|b\right\rangle \in \mathbb{C}^N$. En adelante asumimos que $N = 2^n$ con $n \in \mathbb{N}$. En el caso que A no sea hermitiana, se considera la matriz $\tilde{A} \in \mathbb{M}_{2N\times 2N}(\mathbb{C})$ dada por

$$\tilde{A} = \begin{pmatrix} \mathbf{0} & A \\ A^\dagger & \mathbf{0} \end{pmatrix},$$

para la cual es fácil de comprobar que es hermitiana, es decir, $\tilde{A} = \tilde{A}^\dagger$. Ahora bien, usando la relación de completitud (Capítulo 1) en combinación con el Teorema Espectral para operadores hermitianos, podemos expresar A y A^{-1} en la forma (ver Capítulo 2)

$$A = \sum_{r=0}^{N-1} \lambda_r \left|u_r\right\rangle\left\langle u_r\right| \quad \text{y} \quad A^{-1} = \sum_{r=0}^{N-1} \lambda_r^{-1} \left|u_r\right\rangle\left\langle u_r\right|,$$

respectivamente, con $\mathcal{B} = \{\left|u_1\right\rangle, \left|u_2\right\rangle, \ldots, \left|u_N\right\rangle\}$ una base ortonormal de $\mathbb{C}^N$ conformada por vectores propios de A asociados a los correspondientes valores propios λ_r, es decir:

$$\left\langle u_r|u_s\right\rangle = \begin{cases} 1, & \text{si} \quad r = s, \\ 0, & \text{si} \quad r \neq s \end{cases} \qquad \text{y} \quad Au_r = \lambda_r u_r,$$

con $r = 1, \ldots, N$. De esta forma, la solución (única) (5.1) está dada por

$$\left|x\right\rangle = A^{-1}\left|b\right\rangle = \Big(\sum_{r=0}^{N-1} \lambda_r^{-1} \left|u_r\right\rangle\left\langle u_r\right|\Big)\left|b\right\rangle.$$

Representando $|b\rangle$ en la base $\mathcal{B}$, entonces $|b\rangle = \sum_{s=0}^{N-1} \beta_s |u_s\rangle$ con $\beta_s \in \mathbb{C}$, se tiene

$$\begin{aligned} |x\rangle &= \Big(\sum_{r=0}^{N-1} \lambda_r^{-1} |u_r\rangle \langle u_r| \Big) |b\rangle = \sum_{r,s=0}^{N-1} \lambda_r^{-1} |u_r\rangle \langle u_r| (b_s |u_s\rangle), \\ |x\rangle &= \sum_{s=0}^{N-1} b_s \lambda_s^{-1} |u_s\rangle . \end{aligned} \tag{5.2}$$

El objetivo principal del algoritmo HHL es "expresar" (quizás es más adecuado decir: *estimar*) la solución de (5.1) en la forma (5.2) la cual estará *impresa* o registrada en el b-registro del circuito cuántico correspondiente. Es necesario resaltar que "imprimir" (codificar) $|x\rangle$ en el b-registro, se hace por medio respecto a la base estándar $\mathcal{B}_E = \{|0\rangle, |1\rangle\}$, así que las soluciones no son directamente $b_s\lambda_s^{-1}$ (que son las correspondientes amplitudes-soluciones respecto a la base $\mathcal{B}$), pero este impasse puede resolverse si obtenemos las correctas amplitudes (coeficientes) en la base $\mathcal{B}_E$, y esto es solo posible si los cúbits no están entrelazados con otros cúbits. Parece un poco confuso lo anterior, (ciertamente lo es!) pero a lo largo de la descripción del algoritmo y su posterior ejemplo numérico se verá esto con mayor claridad. Por último, mencionamos que este algoritmo involucra la estimación de los valores propios de A por medio de la subrutina (QPE) y el uso de la transformada de Fourier Cuántica (TFC) por lo que necesitaremos preparar nuestros estados de inicio, $|u_r\rangle$ y $|b\rangle$, esto es, deben ser vectores unitarios que puedan ser representados en un computador cuántico. Así, por ejemplo, se requiere:

$$\sum_{s=0}^{N-1} |b_s|^2 = 1 \quad \text{y} \quad \sum_{s=0}^{N-1} |\lambda_s^{-1} b_s|^2 = 1. \tag{5.3}$$

Iniciemos así con los pasos de este algoritmo, los cuales, como veremos, serán muy familiares a los algoritmos vistos antes.

Paso 1. ***Estado de inicio***. Consideremos el un estado inicial $|\Upsilon_0\rangle$ dado en la forma

$$|\Upsilon_0\rangle = |0\rangle \otimes |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n_b} \quad \Leftrightarrow \quad |\Upsilon_0\rangle = |0\rangle \otimes \underbrace{|0\cdots 0\rangle}_{n} \otimes \underbrace{|0\cdots 0\rangle}_{n_b}.$$

En el estado de inicio $|\Upsilon_0\rangle$, el cual es un $(1+n+n_b)$-cúbit, los cúbits menos significativos van a registrar las amplitudes de $|b\rangle$ (es decir, las coordenadas β_s de $|b\rangle$ en la base ortonormal $\mathcal{B}$). Por lo que el estado $|0\rangle^{\otimes n_b}$ se rota para obtener el estado de inicio

$$|\xi_0\rangle = |0\rangle \otimes |0\rangle^{\otimes n} \otimes |b\rangle_{n_b},$$

siendo $|b\rangle \in \mathbb{C}^N$ con $N = 2^{n_b}$.

Paso 2. ***Estimación cuántica de fase. (QPE)*** El propósito de usar QPE es estimar la fase de los valores propios de la matriz de rotación unitaria $U := e^{i\tau A}$ siendo τ un parámetro libre cuyo propósito es ajustar una versión en $\mathbb{Z}$ de los valores propios de A. Así pues, al aplicar la etapa 1 de QFE, el estado inicial $|\xi_0\rangle$ es ahora transformado al estado

$$\begin{aligned} |\xi_0\rangle \to |\xi_1\rangle &= (I \otimes H^{\otimes n} \otimes I) |\xi_0\rangle , \\ &= |0\rangle \frac{1}{2^{\frac{n}{2}}} (|0\rangle + |1\rangle)^{\otimes n} |0\rangle_n |b\rangle_{n_b} . \end{aligned}$$

La etapa 2 del algoritmo ***QPE*** se aplica con las puerta de control U^{2^l} con U la puerta de control dada por $U = \exp[i\tau A]$, *matriz exponencial de* $i\tau A$. En este punto, es importante resaltar lo siguiente:

Obs. 1. Dada una matriz $B \in \mathbb{M}_{m\times m}(\mathbb{C})$, con ρ un valor propio de B y $|\nu\rangle$ el vector propio asociado entonces
$$\exp[B]\,|\nu\rangle = e^{\rho}\,|\nu\rangle\,,$$
esto es, e^{ρ} es un valor propio de $\exp[B]$ con vector propio asociado $|\nu\rangle$.

Obs. 2. Dado que $|b\rangle$ se escribe como combinación lineal de los vectores propios de A, entonces $U\,|b\rangle = \sum_s \beta_s U\,|u_s\rangle$ siendo u_s vector propio tanto de U como de A.

De estas dos observaciones se deduce que bajo el supuesto: $|b\rangle$ *sea un vector propio de* A *con valor propio* $e^{i2\pi\phi}$, es decir,
$$U\,|b\rangle = e^{i2\pi\phi}\,|b\rangle\,, \tag{5.4}$$
el estado $|\xi_1\rangle$ es transformado en el estado $|\xi_2\rangle$ dado por

$$|\xi_2\rangle = |0\rangle\frac{1}{2^{\frac{n}{2}}}\sum_{s=0}^{2^{n-1}} e^{(i2\pi\phi)s}\,|s\rangle\,|b\rangle_{n_b}\,.$$

Ahora, la etapa 3 de QPE nos brinda el estado $|\xi_3\rangle = (I\otimes\mathcal{U}\otimes I)\,|\xi_2\rangle$ (ver ecuación (4.2) con $w = e^{i2\pi/2^n}$) dado por

$$\begin{aligned}|\xi_3\rangle &= |0\rangle\frac{1}{2^{\frac{n}{2}}}\sum_{s=0}^{2^n-1} e^{(i2\pi\phi)s}\left(\frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} w^{-ks}\,|k\rangle\right)|b\rangle_{n_b}\,,\\ &= |0\rangle\frac{1}{2^n}\sum_{k=0}^{2^n-1}\left(\sum_{s=0}^{2^n-1} w^{(2^n\phi-k)s}\right)|k\rangle\,|b\rangle_{n_b} = |0\rangle\frac{1}{2^n}\sum_{k=0}^{2^n-1}\left(\sum_{s=0}^{2^n-1} e^{i2\pi(\phi-\frac{k}{2^n})s}\right)|k\rangle\,|b\rangle_{n_b}\,.\end{aligned}$$

Dada la propiedad de interferencia constructiva (destructiva) solo los estados $|k\rangle$ que satisfacen la condición $\phi - k/N = 0, (\phi - k/N \neq 0)$ tendrán amplitud finita con valor $\sum_{s=0}^{2^n-1} e^0 = 2^n$ ($\sum_{s=0}^{2^n-1} e^{i2\pi(\phi-\frac{k}{2^n})s} = 0$). Así que, ignorando los estados con amplitud cero, podemos expresar el estado $|\xi_3\rangle$ en la forma

$$\xi_3 = |0\rangle\frac{1}{2^n}\sum_{s=0}^{2^n-1} e^{2\pi s\cdot 0}\,|N\phi\rangle\,|b\rangle_{n_b} = |0\rangle\,|N\phi\rangle\,|b\rangle_{n_b}\,. \tag{5.5}$$

En conclusión, si $|b\rangle = |u_s\rangle$ entonces de la observación Obs. 1., se sigue

$$U\,|b\rangle = e^{i\lambda_s\tau}\,|u_s\rangle \quad\Leftrightarrow\quad e^{i2\pi\phi}\,|u_s\rangle = e^{i\lambda_s\tau}\,|u_s\rangle\,,$$

lo que implica $i\lambda_s\tau = i2\pi\phi$, es decir: $\lambda_s\tau = 2\pi\phi$. En consecuencia, (5.5) queda en la forma

$$|\xi_3\rangle = |0\rangle\,|N\lambda_s\tau/2\pi\rangle\,|b\rangle_{n_b}$$

Por lo tanto, y como ya lo sabíamos al estudiar el algoritmo QPE, el c-registro se usa para "imprimir" la información de A, que es, por supuesto, los valores propios λ_j y cuya precisión sabemos bien que depende del número de n-cúbits en el c-registro. La puntada

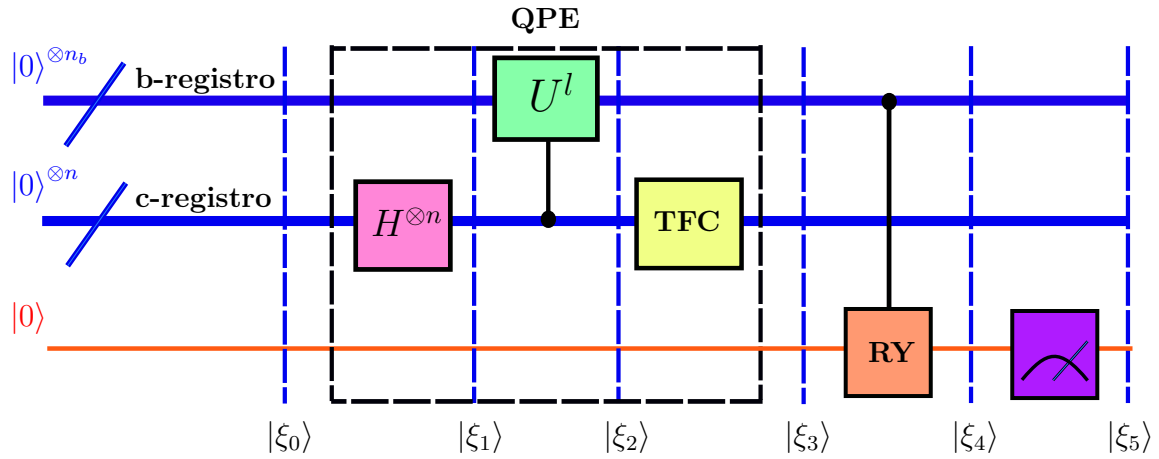

Figura 5.1: Diagrama del algoritmo cuántico HHL entre los pasos 1 al 3. Se aplica la puerta controlada U^l al l-ésimo cúbit del b-registro, la línea roja representa el cúbit auxiliar que se mide cuando se pasa de $|\xi_4\rangle$ hacia $|\xi_5\rangle$

.

final la brinda la observación Obs.2. y el principio de superposición, quedando así en su forma final

$$|\xi_3\rangle = |0\rangle \sum_{s=0}^{2^{n_b}-1} b_s \, |N\lambda_s\tau/2\pi\rangle \, |u_s\rangle \, .$$

En general, los valores propios λ_s no son números enteros, pero, ¡es aquí donde el parámetro τ entra en juego!, pues podemos elegir τ de forma que $\zeta_s = N\lambda_s\tau/2\pi$ sean enteros, dando por hecho que ζ_s es una escala de λ_s, por lo que escribimos finalmente

$$|\xi_3\rangle = |0\rangle \sum_{s=0}^{2^{n_b}-1} b_s \, |\zeta_s\rangle \, |u_s\rangle \, .$$

Paso 3. ***Rotación controlada y medición del cúbit auxiliar.***
El siguiente paso convoca la rotación del cúbit auxiliar que hemos llevado a lo largo de todo el algoritmo. Nos referimos a ese único cúbit $|0\rangle$. Para este fin, se aplica la siguiente puerta

$$RY(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

con $\theta = \theta(\zeta_s)$ dado por $\theta = 2 \arccos(\varrho/\zeta_s)$ con $\varrho \leq \zeta_s$ una constante. Note que la rotación $RY(\theta)$ de $|0\rangle$ depende de los valores propios codificados en el c-registro y corresponde a la puerta $U_{\theta,0,0}$ vista en el Capítulo 7, sección 7.2. En consecuencia, multiplicando $RY(\theta)$ con $\theta = 2 \arccos(\varrho/\zeta_s)$ se obtiene

$$\begin{aligned} RY(\theta)|0\rangle &= \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}, \\ &= \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle \end{aligned}$$

Llegamos entonces al estado $|\xi_4\rangle = (RY(\theta) \otimes I \otimes I) \, |\xi_3\rangle$ dado por

$$|\xi_4\rangle = \left(\sqrt{1 - \frac{\varrho^2}{\zeta_s^2}}|0\rangle + \frac{\varrho}{\zeta_s}|1\rangle \right) \sum_{s=0}^{2^{n_b}-1} b_s \, |\zeta_s\rangle \, |u_s\rangle \, .$$

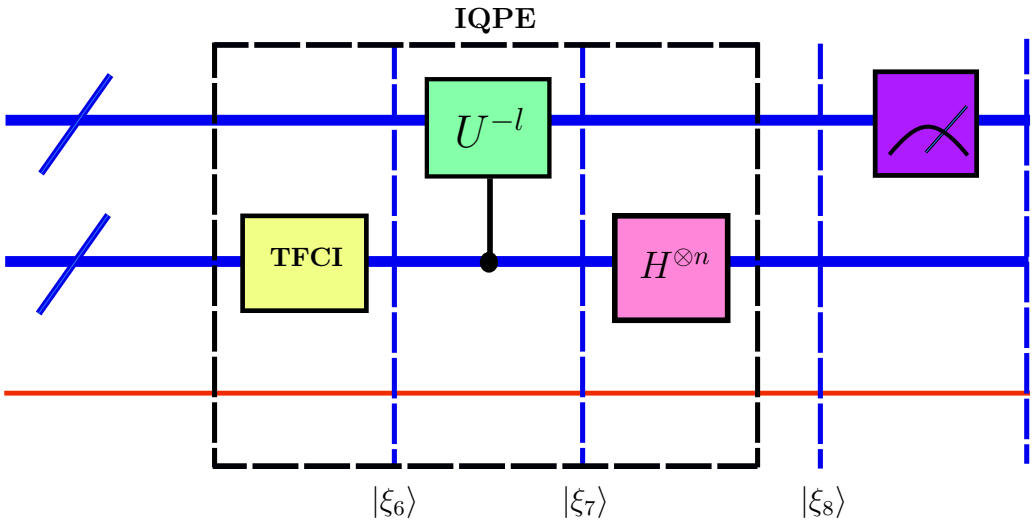

Figura 5.2: Diagrama del algoritmo cuántico HHL del paso 4. El paso final representa la medición del estado $|\xi_8\rangle$

La utilidad de este paso radica en la medición del cúbit auxiliar después de su rotación. En efecto, al medir $RY(\theta)|0\rangle$, este colapsará en uno de los estados fundamentales $|0\rangle$ o $|1\rangle$. Si la medición colapsa en $|0\rangle$, el resultado se descarta y se repiten de nuevo los pasos 1-3 hasta que la medición colapse en $|1\rangle$. Por lo tanto, el estado final de interés que brinda el nuevo estado $|\xi_4\rangle$ es

$$|\xi_5\rangle = \frac{1}{\sqrt{\Lambda}}|1\rangle \sum_{s=0}^{2^{n_b}-1} \frac{\varrho b_s}{\zeta_s} |\zeta_s\rangle |u_s\rangle , \quad \text{con} \quad \Lambda = \sum_{s=0}^{2^{n_b}-1} \left|\frac{\varrho b_s}{\zeta_s}\right|^2 .$$

Note que el coeficiente $1/\sqrt{\Lambda}$ emerge debido a la normalización del estado $|\xi_5\rangle$ después de su medición. De otro lado, dado que $\left|\frac{\varrho}{\lambda_s}\right|^2$ es la probabilidad de obtener el estado $|1\rangle$ cuando el cúbit auxiliar es medido, y como se desea tras una medición del mismo, observar el estado fundamental $|1\rangle$ es conveniente elegir ϱ lo más grande posible (preferiblemente $\varrho = \min_s \lambda_s$).

Ahora bien, en este punto vale la pena mirar atrás y ver qué llevamos hasta ahora en comparación con lo que se desea obtener, que es justamente la expresión (5.2). Así:

$$\text{Llevamos:} \quad |\xi_5\rangle = \frac{1}{\sqrt{\Lambda}}|1\rangle \sum_{s=0}^{2^{n_b}-1} \frac{\varrho b_s}{\zeta_s} |\zeta_s\rangle |u_s\rangle , \quad \text{Queremos:} \quad |x\rangle = \sum_{s=0}^{N-1} b_s \lambda^{-1} |u_s\rangle \langle u_s|$$

con $\zeta_s \propto \lambda_s$. Parece que no se va por buen camino, pero es todo lo contrario. Solo podemos llegar a buen término si el b-registro es medido en la base $\mathcal{B}$, esto es, respecto a la base de los vectores propios, y no respecto a la base estándar $\mathcal{B}_E$. Sin embargo, el b-registro está en entrelazamiento con $|\zeta_s\rangle$ del c-registro, esto es, no podemos factorizar $|\xi_5\rangle$ como producto tensorial entre los estados en el b-registro y aquellos en el c-registro. Para resolver esta situación es donde entra el siguiente y último paso del algoritmo.

Paso 4. ***Estimación cuantica de fase inversa.*** $(QPE)^{-1}$ En esta parte del algoritmo simplemente se deshace lo hecho sobre el c-registro en el Paso 2, esto es, aplicamos el

operador $\mathcal{U}^{-1}$ (Operador Transformada de Fourier Inversa) en el c-registro y obtenemos $|\xi_6\rangle = (I \otimes \mathcal{U}^{-1} \otimes I)\,|\xi_5\rangle$

$$\begin{aligned}|\xi_6\rangle &= \frac{1}{\sqrt{\Lambda}}|1\rangle \sum_{s=0}^{2^{n_b}-1} \frac{\varrho b_s}{\zeta_s}\mathcal{U}^{-1}\,|\zeta_s\rangle\,|u_s\rangle\,,\\ &= \frac{1}{\sqrt{\Lambda}}|1\rangle \sum_{s=0}^{2^{n_b}-1} \frac{\varrho b_s}{\zeta_s}\Big(\frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{i2\pi k\zeta_s/N}\,|k\rangle\Big)\,|u_s\rangle\,,\end{aligned}$$

Continuamos con las puertas de control (rotación) inversa U^{-1}. De nuevo, cuando el l-ésimo cúbit es $|0\rangle$, $|u_s\rangle$ no se afecta, pero si es $|1\rangle$, U^{-2^l} se aplica a $|u_s\rangle$. Por lo tanto

$$\begin{aligned}|\xi_7\rangle &= \frac{1}{2^{n/2}\sqrt{\Lambda}}|1\rangle \sum_{s=0}^{2^{n_b}-1} \frac{\varrho b_s}{\zeta_s}\Big(\sum_{k=0}^{2^n-1} e^{-i\lambda_s\tau k}e^{i2\pi k\zeta_s/N}\,|k\rangle\Big)\,|u_s\rangle\,,\\ &= \frac{1}{2^{n/2}\sqrt{\Lambda}}|1\rangle \sum_{s=0}^{2^{n_b}-1} \frac{\varrho b_s}{\zeta_s}\Big(\sum_{k=0}^{2^n-1} |k\rangle\Big)\,|u_s\rangle\,, \quad \text{puesto que} \quad \zeta_s = N\lambda_s\tau/2\pi.\end{aligned}$$

Se prueba fácilmente que

$$\sqrt{\Lambda} = \frac{2\pi}{N|\tau|}\sqrt{\sum_{s=0}^{2^{n_b}-1}\Big|\frac{b_s\varrho}{\lambda_s}\Big|^2} = \frac{2\pi}{N|\tau|}\sqrt{\Lambda^*} \qquad \text{y} \qquad \frac{\varrho b_s}{\zeta_s} = \frac{2\pi\,\varrho}{N\tau}\frac{b_s}{\lambda_s},$$

en consecuencia

$$|\xi_7\rangle = \frac{\varrho^*}{2^{n/2}\sqrt{\Lambda^*}}|1\rangle\Big(\sum_{s=0}^{2^n-1}|k\rangle\Big)\sum_{s=0}^{2^{n_b}-1}\frac{b_s}{\lambda_s}\,|u_s\rangle = \frac{\varrho^*}{2^{n/2}\sqrt{\Lambda^*}}|1\rangle\Big(\sum_{s=0}^{2^n-1}|k\rangle\Big)\,|x\rangle\,,$$

con $\varrho^* = \varrho\tau/|\tau|$. En este punto se ha logrado que el c-registro y el b-registro ahora no estén entrelazados. La puntada final es aplicar puertas de Hadamard (inversas) sobre el c-registro y obtener

$$|\xi_8\rangle = \frac{\varrho^*}{\sqrt{\Lambda^*}}|1\rangle\,|0\rangle^{\otimes n}\,|x\rangle\,, \quad \text{con} \quad \Lambda^* = \sum_{s=0}^{2^{n_b}-1}\Big|\frac{b_s\varrho}{\lambda_s}\Big|^2.$$

Si $\varrho*$ es real [1] podemos "cancelarlo" y de (5.3) se tiene

$$|\xi_8\rangle = \frac{1}{\sqrt{\sum_{s=0}^{2^{n_b}-1}\Big|\frac{b_s}{\lambda_s}\Big|^2}}|1\rangle\otimes|0\rangle^{\otimes n}\otimes|x\rangle = |1\rangle\otimes|0\rangle^{\otimes n}\otimes|x\rangle\,.$$

Como se puede apreciar, la solución del sistema lineal (5.1) dada por (5.2) ha quedado codificada en el b-registro.

[1] Esto implica que $|\xi_8\rangle$ será proporcional a $|x\rangle$.

5.1. Aplicación del algoritmo HHL. Ejemplo analítico.

Terminamos este capítulo presentando un ejemplo de cómo se implementa el algoritmo HHL. Para ello, consideramos un sistema lineal en $\mathbb{R}^2$ para una familia específica de matrices simétricas. Se seguirá en detalle los cuatro pasos del algoritmo expuestos en la sección anterior. El lector podrá apreciar que los cálculos son algo "extensos", por lo que ejemplos para sistemas de más variables no son tan fáciles de exponer. Es aquí donde una implementación numérica es más adecuada, por ejemplo, usando el código libre en [8, 9].

Siguiendo las ideas en [10], consideremos $a, c \in \mathbb{R}$, con $0 \neq a$ y $a \neq c$ y la matriz

$$\mathcal{A}_{a,c} := \begin{pmatrix} a & c \\ c & a \end{pmatrix}.$$

Un cálculo directo muestra que los valores propios de $\mathcal{A}_{a,c}$ están dados por

$$\lambda_0 = a - c \quad \text{y} \quad \lambda_1 = a + c.$$

Más aún, los vectores propios asociados (ortonormales) a λ_0 y λ_1 respectivamente, son

$$u_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \quad \text{y} \quad u_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

respectivamente. Mostremos analíticamente la implementación del algoritmo HHL sobre el sistema lineal

$$\mathcal{A}_{a,c} \left| x \right\rangle = \left| 1 \right\rangle, \tag{5.6}$$

cuya solución sabemos bien que está dada por

$$\left| \mathbf{x} \right\rangle = \frac{1}{a^2 - c^2} \begin{pmatrix} -c \\ a \end{pmatrix}.$$

Aquí nos detenemos para hacer el siguiente supuesto:

$$(H) \qquad \frac{a+c}{a-c} = 2^{n-1} \quad \Leftrightarrow \quad c = \frac{(2^{n-1}-1)a}{2^{n-1}+1}.$$

La hipótesis *(H)* permite codificar en un 2^n-cúbit (esto conformará nuestro c-registro) a λ_0 como el estado $\left| 10\cdots 0 \right\rangle$ y a λ_1 como el estado $\left| 00\cdots 1 \right\rangle$, en otras palabras, si $\zeta_s = N\lambda_s\tau/2\pi$, con $\tau = \dfrac{2\pi}{N(a-c)}$, (con $N = 2^n$), se deduce

$$\zeta_0 = \frac{N\lambda_0\tau}{2\pi} = 1 = \left| 00\cdots 1 \right\rangle \quad \text{y} \quad \zeta_1 = \frac{N\lambda_1\tau}{2\pi} = \frac{a+c}{a-c} = 2^{n-1} = \left| 10\cdots 0 \right\rangle.$$

Por otro lado, para nuestro sistema lineal (5.6), el vector $\left| b \right\rangle = \left| 1 \right\rangle$ es un vector 2-dimensional, el cuál se puede codificar usando 1-cúbit, por lo tanto $n_b = 1$. Con el fin de computar numéricamente cada paso del algoritmo, fijamos el valor $n = 2$. Para cualquier otro valor, las cuentas numéricas son análogas pero obviamente mucho más extensas. En consecuencia, $c = a/3$, además

$$\lambda_0 = \frac{2a}{3}, \quad \lambda_1 = \frac{4a}{3}, \quad \zeta_0 = \left| 01 \right\rangle, \quad \zeta_1 = \left| 10 \right\rangle \quad \text{y} \quad \tau = \frac{3\pi}{a},$$

además, la solución de (5.6) está dada por

$$|\mathbf{x}\rangle = \frac{1}{8a}\begin{bmatrix}-3\\9\end{bmatrix}. \tag{5.7}$$

Observe que, las coordenadas $\mathbf{x}_0$ y $\mathbf{x}_1$ de $|\mathbf{x}\rangle$ satisfacen

$$|\mathbf{x}_0|^2 = \frac{9}{64a^2}, \qquad |\mathbf{x}_1|^2 = \frac{81}{64a^2} \quad \Leftrightarrow \quad \frac{|\mathbf{x}_0|^2}{|\mathbf{x}_1|^2} = \frac{1}{9}, \quad \forall a \neq 0.$$

Ahora, vamos paso a paso con el algoritmo. El cual, como sabemos, inicia con la preparación de un estado inicial, seguido del ***QPE.***

1. El estado inicial será el $(1+1+2)$-cúbit $\Upsilon_0 = |0\rangle \otimes \underbrace{|00\rangle}_{n} \otimes \underbrace{|0\rangle}_{n_b}$. Ahora rotamos el estado $|0\rangle$ para obtener $|b\rangle = |1\rangle$. Para ello, aplicamos la puerta de Pauli X. Así:

$$\begin{aligned}|\xi_0\rangle &= (I \otimes I \otimes X)\,|0\rangle\,,\\ &= |0\rangle \otimes |00\rangle \otimes |1\rangle\,.\end{aligned}$$

2. Sobre el c-registro actúan dos puertas de Hadamard $H^{\otimes 2}$ para crear un estado en superposición equiprobable, es decir:

$$\begin{aligned}|\xi_1\rangle &= (I \otimes H^{\otimes 2} \otimes I)\,|1\rangle)\,|\xi_0\rangle\,,\\ &= |0\rangle \otimes H^{\otimes 2}(|00\rangle) \otimes |1\rangle_b\,,\\ &= |0\rangle \otimes \frac{1}{2}(|0\rangle + |1\rangle)^{\otimes 2} \otimes |1\rangle_b\,,\\ &= \frac{1}{2}\big(|0\rangle \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |1\rangle_b\big),\\ &= \frac{1}{2}\big(\,|0001\rangle + |0011\rangle + |0101\rangle + |0111\rangle\,\big).\end{aligned}$$

Antes de aplicar las puertas de control, es necesario escribir el vector del b-registro $|1\rangle$, en la base de vectores propios $\mathcal{B} = \{|u_0\rangle\,, |u_1\rangle\}$, esto es:

$$|1\rangle_b = \frac{1}{\sqrt{2}}\,|u_0\rangle + \frac{1}{\sqrt{2}}\,|u_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \quad \Leftrightarrow \quad \beta_0 = \beta_1 = \frac{1}{\sqrt{2}}.$$

En consecuencia,

$$\begin{aligned}|\xi_2\rangle &= \frac{1}{2}\big(|0\rangle \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |1\rangle_b\big),\\ |\xi_2\rangle &= \frac{1}{2\sqrt{2}}\big(|0\rangle \otimes (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \big(\,|u_0\rangle + |u_1\rangle\,\big)\big),\\ &= \frac{1}{2\sqrt{2}}\big(\,|000\rangle\,|u_0\rangle + |001\rangle\,|u_0\rangle + |010\rangle\,|u_0\rangle + |011\rangle\,|u_0\rangle +\\ &\qquad |000\rangle\,|u_1\rangle + |001\rangle\,|u_1\rangle + |010\rangle\,|u_1\rangle + |011\rangle\,|u_1\rangle\,\big).\end{aligned}$$

Ahora construyamos las puertas de control. Primero, por el Teorema Espectral para matrices hermitianas (en este caso, para matrices simétricas y reales) tenemos que

$$\mathcal{A}_D = V^\dagger \mathcal{A} V,$$

con $\mathcal{A}_D$ una matriz diagonal y V una matriz unitaria, es decir, la representación matricial de $\mathcal{A}$ en la base de vectores propios $\mathcal{B}$ es una matriz diagonal. Más aún

$$\mathcal{A}_D = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix} = \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}^\dagger \begin{pmatrix} a & a/3 \\ a/3 & a \end{pmatrix} \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}.$$

Se define la puerta de control

$$U := \exp i\mathcal{A}\tau = \exp i(V^\dagger \mathcal{A}_D V) = V^\dagger \exp i\mathcal{A}_D V,$$

dada explícitamente por

$$\begin{aligned} U = V^\dagger \exp i\mathcal{A}_D V &= \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}^\dagger \begin{pmatrix} e^{i\pi/2} & 0 \\ 0 & e^{i\pi} \end{pmatrix} \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}, \\ &= \frac{1}{2}\begin{pmatrix} 1+i & -1-i \\ -1-i & -1+i \end{pmatrix}. \end{aligned}$$

Note que U está escrita respecto a la canónica B_E. De lo anterior se comprueba directamente que

$$U^2 = \frac{1}{4}\begin{pmatrix} 1+i & -1-i \\ -1-i & -1+i \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Cabe mencionar que U y U^2 (matrices de rotación/control) son matrices unitarias 4-paramétricas (con fase global), más aún

$$U = U_{\frac{\pi}{2},\frac{\pi}{2},-\frac{\pi}{2},\frac{3\pi}{4}} \quad \text{y} \quad U^2 = U_{\pi,0,\pi,0}.$$

Ya que tenemos las puertas de control listas, ahora aplicamos U y U^2 recordando que si tengo el estado $|k\rangle_c$ la fase del estado $|u_s\rangle$ en el b-registro cambia a $k\phi_s$ con $\phi_s = \zeta_s/N = \lambda_s\tau/2\pi$, es decir, multiplicamos por $\exp(i\zeta_s/4) = \exp(i\lambda_s\tau/2\pi)$. Así por ejemplo

$$|0\rangle \otimes \big(\, |00\rangle\,|u_s\rangle + |01\rangle\,|u_s\rangle + |10\rangle\,|u_s\rangle + |11\rangle\,|u_s\rangle \,\big),$$

cambia al estado

$$|0\rangle \otimes \big(\, |00\rangle\,|u_s\rangle + |01\rangle\, e^{2\pi i\phi_s}\,|u_s\rangle + |10\rangle\, e^{2\pi i 2\phi_s}\,|u_s\rangle + |11\rangle\, U^2 e^{2\pi i 3\phi_s}\,|u_s\rangle \,\big), \quad s = 0, 1.$$

Por lo tanto, con $\phi_0 = 1/4$ y $\phi = 1/2$ se tiene $|\xi_2\rangle \to |\xi_3\rangle$ con

$$\begin{aligned} |\xi_3\rangle = \frac{1}{2\sqrt{2}}\big(\, &|000\rangle\,|u_0\rangle + |001\rangle\, e^{i\pi/2}\,|u_0\rangle + |010\rangle\, e^{i\pi}\,|u_0\rangle + |011\rangle\, e^{i3\pi/2}\,|u_0\rangle + \\ &|000\rangle\,|u_1\rangle + |001\rangle\, e^{i\pi}\,|u_1\rangle + |010\rangle\, e^{i2\pi}\,|u_1\rangle + |011\rangle\, e^{i3\pi}\,|u_1\rangle \,\big) \\ = \frac{1}{2\sqrt{2}}\big(\, &|000\rangle\,|u_0\rangle + |001\rangle\, i\,|u_0\rangle + |010\rangle\,(-1)\,|u_0\rangle + |011\rangle\,(-i)\,|u_0\rangle + \\ &|000\rangle\,|u_1\rangle + |001\rangle\,(-1)\,|u_1\rangle + |010\rangle\, e^{i2\pi}\,|u_1\rangle + |011\rangle\,(-1)\,|u_1\rangle \,\big). \end{aligned}$$

Finalmente,

$$\begin{aligned} |\xi_3\rangle = \frac{1}{2\sqrt{2}}\Big[\, &|000\rangle\,\big(\,|u_0\rangle + |u_1\rangle\big) + |001\rangle\,\big(i\,|u_0\rangle - |u_1\rangle\big) + |010\rangle\,\big(-|u_0\rangle + |u_1\rangle\big), \\ &- |011\rangle\,\big(i\,|u_0\rangle + |u_1\rangle\big)\Big]. \end{aligned}$$

A continuación aplicamos la Transformada Cuántica de Fourier sobre el c-registro, esto es, con

$$\mathcal{U} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}.$$

De aquí, sabemos bien que:

$$\begin{aligned}
\mathcal{U}\,|00\rangle &= \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big),\\
\mathcal{U}\,|01\rangle &= \frac{1}{2}\big(\,|00\rangle - i\,|01\rangle - |10\rangle + i\,|11\rangle\,\big),\\
\mathcal{U}\,|10\rangle &= \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big),\\
\mathcal{U}\,|11\rangle &= \frac{1}{2}\big(\,|00\rangle + i\,|01\rangle - |10\rangle - i\,|11\rangle\,\big),
\end{aligned}$$

Después de algunos cálculos, se deduce

$$\begin{aligned}
|\xi_3\rangle = \frac{1}{4\sqrt{2}}|0\rangle \otimes \Big[&\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big) \otimes \big(\,|u_0\rangle + |u_1\rangle\,\big) +\\
&\big(\,|00\rangle - i\,|01\rangle - |10\rangle + |11\rangle\,\big) \otimes \big(i\,|u_0\rangle - |u_1\rangle\,\big) +\\
&\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big) \otimes \big(-|u_0\rangle + |u_1\rangle\,\big) +\\
&\big(\,|00\rangle + i\,|01\rangle - |10\rangle - i\,|11\rangle\,\big) \otimes \big(-i\,|u_0\rangle - |u_1\rangle\,\big)\Big],\\
= \frac{1}{\sqrt{2}}|0\rangle \otimes &\Big(\,|01\rangle \otimes |u_0\rangle + |10\rangle \otimes |u_1\rangle\,\Big),\\
= |0\rangle \otimes &\Big(\frac{1}{\sqrt{2}}\,|01\rangle \otimes |u_0\rangle + \frac{1}{\sqrt{2}}\,|10\rangle \otimes |u_1\rangle\,\Big) = |0\rangle\big(\beta_0\,|01\rangle\,|u_0\rangle + \beta_1\,|10\rangle\,|u_1\rangle\,\big),\\
= |0\rangle &\Big(\sum_{j=0}^{2^1-1} \beta_j\,|\zeta_i\rangle\,|u_j\rangle\,\Big),
\end{aligned}$$

en donde β_0 y β_1 son la expresión de $|b\rangle = |1\rangle$ en la base de vectores propios $\mathcal{B}$. Notar cómo el c-registro está en entrelazamiento cuántico con el b-registro.

4. Seguimos ahora con la rotación del cúbit auxiliar $|0\rangle$, es decir

$$|\xi_3\rangle \to |\xi_4\rangle = (RY(\theta) \otimes I \otimes I)\,|\xi_3\rangle\,,$$

en donde

$$RY(\theta)|0\rangle = \Big(\sqrt{1 - \frac{\varrho^2}{\zeta_s^2}}|0\rangle + \frac{\varrho}{\zeta_s}|1\rangle\Big), \quad \text{con} \quad \varrho = \min \zeta_s = 1, \quad s = 0, 1.$$

Por lo tanto,

$$\begin{aligned}
|\xi_4\rangle &= \Big(\sqrt{1 - \frac{\varrho^2}{\zeta_s^2}}|0\rangle + \frac{\varrho}{\zeta_s}|1\rangle\Big) \otimes \Big(\sum_{s=0}^{2^1-1} \beta_s\,|\zeta_s\rangle\,|u_s\rangle\,\Big),\\
&= \frac{1}{\sqrt{2}}|1\rangle\,|01\rangle\,|u_0\rangle + \frac{1}{\sqrt{2}}\Big(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\Big)\,|10\rangle\,|u_1\rangle\,.
\end{aligned}$$

Es aquí donde se hace la primera medición del algoritmo. Si en la medición del estado auxiliar es en dirección del estado $|1\rangle$ se tiene

$$|\xi_5\rangle = \frac{1}{\mathcal{N}\sqrt{2}}|1\rangle\big(\,|01\rangle\,|u_0\rangle + \frac{1}{2}\,|10\rangle\,|u_1\rangle\,\big) \quad \text{con} \quad \mathcal{N} = \sqrt{\Big|\frac{\beta_0}{\lambda_0}\Big|^2 + \Big|\frac{\beta_1}{\lambda_1}\Big|^2} = \sqrt{\frac{1}{2} + \frac{1}{2\sqrt{2}}},$$
$$= \sqrt{\frac{8}{5}}\Big(\frac{1}{\sqrt{2}}|1\rangle\,|01\rangle\,|u_0\rangle + \frac{1}{2\sqrt{2}}|1\rangle\,|10\rangle\,|u_1\rangle\,\Big).$$

4. *Y ahora, el camino de vuelta...* Con el fin de ejecutar el proceso inverso del algoritmo, iniciamos aplicando la puerta $\mathcal{U}^{-1}$ (Transformada inversa de Fourier) de nuevo sobre el c-registro. Sabemos bien que

$$\mathcal{U}^{-1} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix},$$

y al igual que en el punto **2.** se tiene

$$\mathcal{U}^{-1}\,|01\rangle = \frac{1}{2}\big(\,|00\rangle + i\,|01\rangle - |10\rangle - i\,|11\rangle\,\big),$$
$$\mathcal{U}^{-1}\,|10\rangle = \frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big).$$

Obteniéndose $|\xi_6\rangle = (I \otimes \mathcal{U}^{-1} \otimes I)\,|\xi_5\rangle$ con

$$|\xi_6\rangle = \sqrt{\frac{8}{5}}\Big(\frac{1}{\sqrt{2}}|1\rangle\frac{1}{2}\big(\,|00\rangle + i\,|01\rangle - |10\rangle - i\,|11\rangle\,\big)\,|u_0\rangle + \frac{1}{2\sqrt{2}}|1\rangle\frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big)\,|u_1\rangle\,\Big).$$

Seguidamente, se aplican las puertas de control U^{-2} y U^{-1} sobre el c-registro, las cuales están dadas por

$$U^{-1} = U_{-\frac{\pi}{2},\frac{\pi}{2},-\frac{\pi}{2},-\frac{3\pi}{4}} = \frac{1}{2}\begin{pmatrix} -1-i & -1+i \\ -1+i & -1-i \end{pmatrix}, \quad \text{y} \quad U^{-2} = U_{\pi,0,\pi,0} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

respectivamente. Ahora bien, al igual que antes, la fase del b-registro se multiplica por $\exp -i\lambda_s\tau k$ si el estado en el c-registro es $|k\rangle_c$. Así por ejemplo, para λ_0 se comprueba fácilmente que

$$|00\rangle \to |00\rangle\,, \qquad |01\rangle \to -i\,|01\rangle\,,$$
$$|10\rangle \to -\,|10\rangle\,, \qquad |11\rangle \to i\,|11\rangle\,,$$

mientras que, para λ_1 tenemos

$$|00\rangle \to |00\rangle\,, \qquad |01\rangle \to -\,|01\rangle\,,$$
$$|10\rangle \to |10\rangle\,, \qquad |11\rangle \to -\,|11\rangle\,.$$

De esta forma, llegamos al estado

$$\begin{aligned}|\xi_7\rangle &= \sqrt{\frac{8}{5}}\Big(\frac{1}{\sqrt{2}}|1\rangle\frac{1}{2}\big(\,|00\rangle+|01\rangle+|10\rangle+|11\rangle\,\big)\,|u_0\rangle+\\ &\qquad\frac{1}{2\sqrt{2}}|1\rangle\frac{1}{2}\big(\,|00\rangle+|01\rangle+|10\rangle+|11\rangle\,\big)\,|u_1\rangle\Big),\\ &= \frac{1}{2}\sqrt{\frac{8}{5}}\Big(|1\rangle\big(\,|00\rangle+|01\rangle+|10\rangle+|11\rangle\,\big)\Big(\frac{1}{\sqrt{2}}\,|u_0\rangle+\frac{1}{2\sqrt{2}}\,|u_1\rangle\Big),\\ &= \frac{1}{2}\Big(\frac{2a}{3}\Big)\sqrt{\frac{8}{5}}\Big(|1\rangle\big(\,|00\rangle+|01\rangle+|10\rangle+|11\rangle\,\big)\Big(\frac{3}{2a\sqrt{2}}\,|u_0\rangle+\frac{3}{4a\sqrt{2}}\,|u_1\rangle\Big).\end{aligned}$$

Por último, aplicamos de nuevo al c-registro dos puertas de Hadamard $H^{\otimes 2}$ (recordemos que $H^{\otimes 2}=H^{-\otimes 2}$)

$$H^{\otimes 2}\big(\,|00\rangle+|01\rangle+|10\rangle+|11\rangle\,\big)=2\,|00\rangle\,,$$

por lo tanto,

$$|\xi_8\rangle=\Big(\frac{2a}{3}\Big)\sqrt{\frac{8}{5}}\Big(|1\rangle\,|00\rangle\,\Big(\frac{\lambda_0^{-1}}{\sqrt{2}}\,|u_0\rangle+\frac{\lambda_1^{-1}}{\sqrt{2}}\,|u_1\rangle\Big).$$

Y ahora, la pincelada final, observe que (¡y como era de esperarse!)

$$\frac{\lambda_0^{-1}}{\sqrt{2}}\,|u_0\rangle+\frac{\lambda_1^{-1}}{\sqrt{2}}\,|u_1\rangle=\frac{3}{4a}\begin{pmatrix}-1\\1\end{pmatrix}+\frac{3}{8a}\begin{pmatrix}1\\1\end{pmatrix}=\frac{1}{8a}\begin{pmatrix}-3\\9\end{pmatrix}=\frac{-3}{8a}\,|0\rangle+\frac{9}{8a}\,|1\rangle\,,$$

en consecuencia

$$\begin{aligned}|\xi_8\rangle &= \frac{2\sqrt{8}}{8\sqrt{5}}\Big(|1\rangle\,|00\rangle\,\big(-|0\rangle+3\,|1\rangle\,\big),\\ &= |1\rangle\otimes|00\rangle_c\otimes\frac{1}{2}\sqrt{\frac{2}{5}}\Big(-|0\rangle+3\,|1\rangle\,\Big)_b\end{aligned}$$

El lector puede ver que en el b-registro ha quedado codificado el vector $|b\rangle$ con probabilidades de medición

$$\Big|\frac{1}{2}\sqrt{\frac{2}{5}}\Big|^2\quad\text{y}\quad\Big|\frac{3}{2}\sqrt{\frac{2}{5}}\Big|^2,$$

respectivamente, cuyo cociente tiene las cuáles tiene y con razón entre ellas de $\dfrac{1}{9}$ como se esperaba.

5.2. Conclusiones

Se ha llegado oficialmente al final de este documento. Lo mostrado en el último capítulo es, como corresponde, la descripción completa del algoritmo HHL, un algoritmo proveniente de la computación cuántica, planteado con el objetivo de ofrecer una alternativa en la resolución de los problemas de sistemas lineales, sujeta a la condición de que la matriz de coeficientes sea en su defecto hermitiana. Sin embargo, más que eso, en este trabajo este algoritmo también representa el fruto de una serie de conceptos de la Física y la mecánica cuántica, los cuales fueron descritos con éxito mediante definiciones matemáticas. El mayor logro realizado en este trabajo no es el hecho de presentar este algoritmo, una

idea ya planteada anteriormente por otros investigadores, por el contrario, la forma en que se describió. Desglosar algunos de los conceptos relacionados de la mecánica cuántica computacional y explicarlos utilizando un enfoque distinto que facilite el entendimiento de cualquier matemático con conocimientos básicos del álgebra lineal y los números complejos es lo que le da valor especial a este trabajo.

Se espera que a partir de este punto el lector tenga ya un entendimiento concreto sobre algunos conceptos de la computación cuántica y pueda operar con facilidad dos de los algoritmos mostrados en este documento, tales como el algoritmo QPE descrito en el Capítulo 4 y el algoritmo HHL descrito en el Capítulo 5. Lo que viene a continuación es el uso de los conocimientos adquiridos en este documento en futuros proyectos que nutran su inmersión hacia esta ciencia y permitan visualizar más aplicaciones potenciales.

Bibliografía

[1] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Phys. Rev. Lett.*, vol. 103, p. 150502, Oct 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.103.150502

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ser. 10th Anniversary Edition. Cambridge University Press, 2010.

[3] P. A. M. Dirac, "A new notation for quantum mechanics," *Math. Proc. Camb.*, vol. 35, p. 416–418, 1939. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0375960123005182

[4] H. Grassmann, "History of mathematics sources," *A.M.S.*, no. 3, 1862.

[5] A. J. A. Charris, *Tópicos en tería de matrices.* Universidad Nacional de Colombia, 1995.

[6] H. Y. Wong, *Introduction to Quantum Computation. From a Layperson to a Programmer in 30 Steps.* Springer, 2022.

[7] E. Rieffel and W. Polak, *Quantum Computing. A Gentle Introduction.* MIT Press, 2011.

[8] quantum-computing.igm.com. [Online]. Available: https://quantum.ibm.com/

[9] qiskit. [Online]. Available: https://www.ibm.com/quantum/qiskit

[10] A. Zaman, H. J. Morrell, and H. Y. Wong, "A step-by-step hhl algorithm walkthrough to enhance understanding of critical quantum computing concepts," *IEEE Access*, vol. 11, pp. 77 117–77 131, 2023. [Online]. Available: https://arxiv.org/abs/2108.09004