Universidad Nacional Autónoma de
México y Universidad Michoacana de San
Nicolás de Hidalgo
Instituto de Física y Matemáticas

Posgrado Conjunto en Ciencias Matemáticas UMSNH-UNAM

Propiedades Distintivas de la Computación Cuántica

T E S I S

que para obtener el grado de

Maestra en Ciencias Matemáticas

presenta

María del Pilar Ramos Huila

Asesor:
Dr Elmar Wagner
Asesor

Morelia, Michoacán, México
Marzo, 2024

Índice general

Propiedades Distintivas de la Computación Cuántica

María del Pilar Ramos Huila

Resumen

La computación cuántica versus la computación clásica, ofrece distintas capacidades que superan a los actuales dispositivos de procesamiento clásicos. Tales diferencias tienen como base la mecánica cuántica, una teoría física que detalla fenómenos que clásicamente no son definibles ni comprensibles. Así, fundamentada en la mecánica cuántica, la computación cuántica tal como se ha concebido en la década de los 90's proporciona una herramienta para diseñar y obtener solución a problemas que no son solubles por la computación clásica, y a proponer nuevos problemas en distintos ámbitos de la ciencia y la tecnología. El objetivo de este trabajo es introducir tales conceptos básicos, como la unidad mínima de información cuántica, el *qubit* de *quantum bit* y el lenguaje de los circuitos cuánticos, determinados por un conjunto de operaciones universales que aproximan a todas las operaciones posibles sobre los qubits, conceptos que fundamentan la computación cuántica y que la distinguen de la computación clásica, por los algoritmos que se derivan de ellos, en particular se estudia aquí la transformada de Fourier cuántica, su implementación circuital y se discuten tres aplicaciones de ella destacadas en la computación cuántica, el algoritmo de estimación de fase, el algoritmo de encontrar el orden y el algoritmo de factorización, que tienen generalizaciones que se aplican a distintas familias de problemas de la teoría de números y del álgebra. A partir de este trabajo se puede dar paso al estudio de los algoritmos cuánticos y de la teoría de la información cuántica. La computación cuántica es un área en auge, que tiene ya implementaciones físicas de algunos pocos qubits, y el reto es obtener una computadora de un número de qubits tal que supere el procesamiento actual de todas las supercomputadoras clásicas.

Palabras Clave: Mecánica Cuántica, Qubit, Circuitos Cuánticos, Transformada de Fourier, Algoritmos Cuánticos.

Abstract

Quantum computing versus classical computing offers distinct capabilities that surpass current classical processing devices. These differences are based on quantum mechanics, a physical theory that details phenomena that are neither classically definable nor comprehensible. Thus, based on quantum mechanics, quantum computing as it has been conceived in the 90's provides a tool to design and obtain solutions to problems that are not solvable by classical computing, and to propose new problems in different fields of science and technology. The aim of this work is to introduce such basic concepts as the minimum unit of quantum information, the quantum bit *qubit* and the language of quantum circuits, determined by a set of universal operations that approximate all possible operations on qubits, concepts that underlie quantum computation and distinguish it from classical computation. In particular, we study here the quantum Fourier transform, its circuital implementation and discuss three applications of it that stand out in quantum computation, the phase estimation algorithm, the order finding algorithm and the factorization algorithm, which have generalizations that apply to different families of problems in number theory and algebra. From this work we can move on to the study of quantum algorithms and quantum information theory. Quantum computing is a booming area, which already has physical implementations of a few qubits, and the challenge is to obtain a computer with a number of qubits that exceeds the current processing of all classical supercomputers.

Introducción

La mecánica cuántica es una teoría física que tiene como objeto de estudio los fenómenos microscópicos, es decir, estudia los fenómenos de los átomos, electrones, fotones y demás partículas subatómicas, que en algunos casos se modelan como partículas y en otros, como ondas, sin ser lo uno ni lo otro; describe su evolución en el tiempo e interacción con su ambiente de forma precisa, sin esto significar que se puedan explicar con la intuición educada por la mecánica clásica determinista.

La mecánica cuántica se fundamenta en diferentes formalismos matemáticos entre ellos, el formalismo de espacios de Hilbert complejos de dimensión infinita y de dimensión finita, y los operadores lineales sobre estos espacios desarrollado por grandes físicos matemáticos como W. Heisenberg, E. Schrödinger, P. Dirac y J. Von Neuman entre otros, en la década de los 30's del siglo pasado, y el formalismo de integrales de camino de R. Feynman desarrollado a finales de la década de los 40's. En particular, la formalización matemática de la mecanica cuántica que vamos a utilizar es el formalismo de operadores lineales sobre el espacio de Hilbert complejo.

Lo que podemos concluir sin entrar en detalles, es que el resultado de la fundamentación matemática dio lugar a una descripción cuántica que profundiza y amplía la comprensión de la naturaleza, hasta alcances a los que no llega la descripción clásica de ella; esto ha producido un replanteamiento de la teoría física y además, en la visión de una construcción tecnológica que haga efectiva la fundamentación matemática y los desarrollos físicos posteriores.

En este sentido, entre los primeros científicos que comienzan a preguntarse por una tecnología cuántica, se encuentran el matemático ruso Y. Manin que en 1980 en su libro *Computable and Uncomputable* menciona la idea del autómata[1] cuántico y el físico teórico R. Feynman que en 1982 publica su artículo *Simulating Physics with Computers* [10], donde estudia las dificultades que tiene la computación clásica para simular un sistema cuántico. Una de las preguntas iniciales que plantea es ¿qué tipos de computadores se van a utilizar para simular la física?, en otras palabras, ¿qué tipos de sistemas de procesamiento de información, pueden obtener exactamente los mismos resultados de la naturaleza (entendida como cuántica)? Y desarrolla el siguiente problema: Los modelos matemáticos de la computación han sido llevados a un punto en el que se ignora la dependencia de la implementación física del computador, e incluso de las leyes físicas que lo gobiernan, dando lugar al modelo de máquinas de Turing o computador universal, por tanto, se plantea la pregunta ¿puede un computador universal simular un sistema cuántico? Feynman muestra como la simulación de un sistema cuántico, no es posible en una computadora clásica, incluso aunque esta sea probabilística. En consecuencia, propone la computación universal cuántica, en el mismo sentido, en que se puede simular cualquier sistema cuántico independiente de la implementación, pero fundamentado en el formalismo de la mecánica cuántica, esto es, por operaciones unitarias y reversibles, que conducirán a diversos resultados que principalmente en la década de los 90's fundamentan la teoría de la computación cuántica.

La computación clásica, también se desarrolló ampliamente en el siglo pasado, definiendo nue-

[1] Un autómata es un modelo computacional que consiste en un conjunto de estados bien definidos, un estado inicial, un alfabeto de entrada y una función de transición.

vas relaciones de producción en todos los ámbitos humanos, que generan una gran cantidad de información a ser procesada diariamente, lo cual representa una necesidad de construir tecnologías con una capacidad de procesamiento cada vez mayor que la actual. Se adjetiva clásica, en el sentido de que los elementos que se utilizan para las operaciones y los fenómenos físicos que suceden en ellos se explican con la teoría física clásica, y el procesamiento de información, es determinado por límites teóricos que a su vez están definidos por los límites de la física clásica. En el estudio teórico de la computación, a saber, los algoritmos, que son un conjunto de instrucciones para obtener un resultado deseado, observamos que el cambio de paradigma, la computación basada en los fundamentos de la mecánica cuántica, ofrece nuevos algoritmos que pueden resolver problemas que no tienen aún solución en la algoritmia clásica, o que resuelven con una gran diferencia en el uso de recursos, como tiempo y espacio. Por ejemplo, en [16] en el 2010, obtienen mediante un algoritmo clásico la factorización de un número de 768 bits, utilizando cientos de computadores en un periodo de 2 años, con un esfuerzo computacional de 10^{20} operaciones. En comparación con la estimación de recursos que requeriría la factorización de un número de 2000 bits realizada en [11], una computadora cuántica, utilizando el algoritmo de factorización propuesto por P. Shor [26], utilizaría aproximadamente 3×10^{11} operaciones cuánticas y un billón de qubits, obtendría el resultado en un día. La ciencia computacional estudia en detalle la cuantificación de recursos requeridos por un algoritmo para resolver una tarea específica, en términos de tiempo y espacio, para ello, utilizan la notación asintótica, para definir el comportamiento esencial de una función, y en esta cuantificación de recursos se destacan las diferencias de la computación clásica y cuántica, descritas en el modelo de circuitos[2]. Este es un tema importante en la ciencia computacional, pero en este trabajo no se realizan tales cuentas, sin embargo, la cuantificación de recursos, se encuentra explícitamente en las referencias principales de este trabajo [8], [21].

Esta gran diferencia en las posibilidades de la computación es un tema importante, no solo en el ámbito científico, sino además, en el ámbito tecnológico y de seguridad de los sistemas de información, dado que se fundamentan en los límites de la computación clásica, su seguridad o encriptación de la información. Entre esta y muchas razones más, grandes empresas a nivel mundial, invierten una gran cantidad de recursos en obtener una computadora cuántica, con todas los desafios que representa. Se puede pensar que en algún momento se conseguirá, si consideramos la idea de que "una tarea de procesamiento de información puede ser siempre traducida en un dispositivo físico" [20].

El trabajo presente introduce el estudio de la computación cuántica, partiendo de la definición de la unidad mínima de información en el contexto cuántico, que se nombra como '*qubit*' y las operaciones sobre los qubits, en el lenguaje de circuitos cuánticos. Con este lenguaje, se introduce una importante herramienta en la computación, que es la transformada de Fourier, que permitirá describir algunos de los más importantes algoritmos cuánticos, como estimar la fase, y encontrar el orden, los cuales conducen al algoritmo de factorización de P. Shor. Estudiar este algoritmo en profundidad y lo que se sigue de él no se abordara aquí; no obstante, las ideas que se presentan constituyen un fundamento para comprender este algoritmo, que es el resultado de aplicar el algoritmo de encontrar el orden, donde el orden es definido como el menor entero positivo r, tal que dados dos números enteros x y N se tiene que $x^r = 1 \mod N$, se obtiene por tanto, el orden en el grupo de enteros módulo N. Sin embargo, es posible traducir la aplicación de este último para encontrar el orden de elementos en un grupo en general [20].

Este trabajo se desarrolla en tres capítulos, como sigue:

- En el capítulo 1 se realiza una breve introducción a la mecánica cuántica, donde, se introducen

[2]En computación se pueden desatacar dos modelos, el modelo de la máquina de Turing, y el modelo circuital, en este trabajo se estudia el modelo circuital.

los conceptos y el lenguaje fundamental de la mecánica cuántica que se requieren para el estudio de computación cuántica.

- En el capítulo 2 se define la unidad mínima de información cuántica llamada qubit como un elemento en el espacio complejo de dimensión 2 denotado $\mathbb{C}^2$, y se estudia su respresentación en una 2-esfera; lo cual permite demostrar que las operaciones sobre un qubit corresponden a rotaciones de puntos en la 2-esfera considerada como subconjunto del espacio euclídeo $\mathbb{R}^3$. Se definen las compuertas[3] cuánticas de un qubit como operadores unitarios $U : \mathbb{C}^2 \to \mathbb{C}^2$ esto es $U \in U(2)$ y se estudia su descomposición en elementos del subgrupo especial unitario $SU(2)$ de $U(2)$. Dado que se obtiene un conjunto infinito de operaciones sobre un qubit, se determina un conjunto finito que aproxima cualquier elemento de $SU(2)$ y, por tanto, a cualquier operación sobre un qubit. También se definen las compuertas de múltiples qubits controladas que se describen por códigos de Gray y diagramas circuitales. Por último se obtiene un conjunto universal de compuertas de múltiples qubits.

- En el capítulo 3 se describen algunos resultados que representan distinguidas diferencias con respecto a la computación clásica. Entre ellas, la aplicación de la transformada de Fourier traducida a los operadores unitarios, en dos algoritmos, el algoritmo de estimación de fase y un caso especial, el algoritmo de encontrar el orden, y una referencia a como se aplica en el algoritmo de factorización de Shor.

- En el apéndice A se encuentra el estudio de la desigualdad de Bell, que permite destacar un aspecto controversial en el surgimiento de la mecánica cuántica.

[3] En analogía con la computación clásica, donde se define una compuerta lógica como una función de operaciones lógicas, con entradas y salidas binarias.

Capítulo 1

Introducción a la Mecánica Cuántica

En este breve capítulo se introduce el lenguaje de la mecánica cuántica que permitirá construir el objeto de estudio.

1.1 Definiciones

Definición 1.1.1. Un espacio de Hilbert es un espacio vectorial $\mathcal{H}$ sobre los complejos $\mathbb{C}$ con un producto interno $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$, el cual determina una norma $\| \cdot \| : \mathcal{H} \to \mathbb{R}$ definida por $\|x\| := \langle x, x \rangle^{1/2}$ para todo $x \in \mathcal{H}$, tal que relativo a la métrica inducida por la norma es un espacio métrico completo.

Definición 1.1.2. Un estado cuántico[1] es un elemento $\psi \in \mathcal{H}$ donde $\mathcal{H}$ es un espacio de Hilbert, el cual debe cumplir que $\|\psi\|^2 = 1$.

El espacio de Hilbert que se considera en todo el trabajo será de dimensión finita, por lo que las transformaciones lineales u operadores lineales $T : \mathcal{H} \to \mathcal{H}$ son continuos [7]. Denotamos $\mathcal{B}(\mathcal{H})$ el conjunto de transformaciones lineales acotadas de $\mathcal{H}$ en $\mathcal{H}$.

Definición 1.1.3. Si $T \in \mathcal{B}(\mathcal{H})$, entonces existe un único operador $T^* \in \mathcal{B}(\mathcal{H})$ tal que para cualesquiera $x, y \in \mathcal{H}$ se cumple que

$$\langle x, Ty \rangle = \langle T^* x, y \rangle. \tag{1.1.1}$$

T^* es llamado el operador adjunto de T. Si $T^* = T$, entonces decimos que T es hermitiano o autoadjunto.

Definición 1.1.4. Un observable en la mecánica cuántica es un operador autoadjunto de $\mathcal{H}$.

Proposición 1.1.5. *Un observable $T \in \mathcal{B}(\mathcal{H})$ es diagonal con respecto a una base ortonormal de $\mathcal{H}$.*

Demostración. Véase [7], pág 55. ■

Consideremos el caso especial de la Proposición 1.1.5, la cual afirma que existe una base ortonormal $\{b_1, b_2, \cdots, b_n\} \subseteq \mathcal{H}$ y $\{\lambda_1, \lambda_2, \cdots, \lambda_n\} \subseteq \mathbb{R}$ tal que $Tb_i = \lambda_i b_i$. En mecánica cuántica, el conjunto de los eigenvalores $\{\lambda_1, \lambda_2, \cdots, \lambda_n\} \subseteq \mathbb{R}$ son los valores posibles de medición, es decir, el experimentador obtiene al aplicar el operador u observable T solamente los valores en este conjunto después de medir. Así, si el sistema físico está en el estado b_j, el experimentador mide λ_j con probabilidad 1 o en otras palabras, mide siempre λ_j.

[1] También se conoce como función de onda.

Definición 1.1.6. Un estado cuántico $\psi \in \mathcal{H}$ que es superposición de los eigenestados $b_1, \ldots, b_n$ de T, se escribe de la siguiente forma

$$\psi = \sum_{j=1}^{n} \alpha_j b_j, \tag{1.1.2}$$

donde, $\alpha_j \in \mathbb{C}$ se conocen como las amplitudes de probabilidad del estado ψ y satisfacen

$$\sum_{j=1}^{n} |\alpha_j|^2 = \|\psi\|^2 = 1. \tag{1.1.3}$$

Definición 1.1.7. El valor esperado de T sobre el estado ψ se define como

$$< T >_\psi \doteq < \psi, T\psi > . \tag{1.1.4}$$

Observamos que el valor esperado del operador T sobre el estado ψ de la Definición 1.1.6 es,

$$< T >_\psi = < \psi, T\psi > = \left(\sum_{i=1}^{n} \alpha_i b_i, T \left(\sum_{j=1}^{n} \alpha_j b_j \right) \right) \tag{1.1.5}$$

$$= \sum_{i,j=1}^{n} \overline{\alpha_i} \alpha_j \lambda_j < b_i, b_j > \tag{1.1.6}$$

$$= \sum_{i,j=1}^{n} \overline{\alpha_i} \alpha_j \lambda_j \delta_{ij} \tag{1.1.7}$$

$$= \sum_{i=1}^{n} \lambda_i |\alpha_i|^2, \tag{1.1.8}$$

donde, $\overline{\alpha_i}$ es el complejo conjugado de α_i y $< b_i, b_j >= \delta_{ij}$ es la función delta de Kronecker. ¿Qué significa en (1.1.8) el factor $|\alpha_i|^2$? Es la probabilidad de obtener λ_i al medir el operador T sobre el estado ψ.

Proposición 1.1.8. *Sea $\theta \in \mathbb{R}$, los estados ψ y $e^{i\theta}\psi$ definen los mismos estados físicos.*

Demostración. Notamos que si $Tb_j = \lambda_j b_j$ entonces

$$T(e^{i\theta} b_j) = \lambda_j (e^{i\theta} b_j) \tag{1.1.9}$$

y $\|e^{i\theta} b_j\|^2 = \|b_j\|^2 = 1$; además,

$$< T >_{e^{i\theta}\psi} = < e^{i\theta}\psi, T(e^{i\theta}\psi) > = e^{-i\theta} e^{i\theta} < \psi, T\psi > = < T >_\psi, \tag{1.1.10}$$

y las amplitudes de probabilidad son iguales. ■

En la proposición anterior, el factor $e^{i\theta}$ lo llamaremos fase global.

1.2 Colapso de la función de onda

Observamos que medir en mecánica cuántica un sistema cuántico es obtener uno de los eigenvalores del operador u observable que actúa sobre él. Además, en (1.1.8) notamos que con probabilidad $|\alpha_j|^2$ se obtiene λ_j. De forma más general, que como se introdujo en la sección 1.1, la Proposición

1.1.5 implica que el observable T con eigenvalores λ_j distintos entre sí, puede ser escrito de la siguiente forma

$$T = \sum_j \lambda_j P_{\lambda_j} \tag{1.2.1}$$

donde P_{λ_j} denota la proyección ortogonal sobre el eigenespacio $\mathcal{V}_{\lambda_j} \doteq \{b \in \mathcal{H} : Tb = \lambda_j b\}$, el cual no es necesariamente de dimensión 1.

Dado que un sistema cuántico es descrito por un estado cuántico $\psi \in \mathcal{H}$, la medición del observable T que actúa en $\mathcal{H}$ produce un efecto sobre el estado cuántico llamado *el colapso de la función de onda*, y esto es, que inmediatamente después de medir donde el resultado obtenido es λ_j, se tiene que el estado ψ colapsa al estado

$$\frac{1}{\|P_{\lambda_j}\psi\|} P_{\lambda_j}\psi. \tag{1.2.2}$$

Luego, colapsar significa que, el estado que antes de medir era una superposición de eigenvectores del operador T, se proyecta o se convierte después de medir en uno de los eigenvectores del eigenespacio correspondiente a λ_j.

1.3 Dinámica Cuántica

La dinámica cuántica está definida por la ecuación de Schrödinger, en la cual el operador $H = H^*$ es el hamiltoniano del sistema físico, es decir, el observable asociado a la energía del sistema. Su expresión es,

$$i\hbar \frac{\partial}{\partial t}\psi(t) = H\psi(t) \tag{1.3.1}$$

con condiciones iniciales $\psi(0) = \psi_0$. En adelante $\hbar$ la consideraremos 1. Se observa que la solución de la ecuación diferencial es

$$\psi(t) = e^{-iHt}\psi_0 = \sum_{k=0}^{\infty} \frac{(-it)^k}{k!} H^k \psi, \tag{1.3.2}$$

dado que $dim(\mathcal{H}) < \infty$, se tiene una serie convergente.

Lema 1.3.1. *El operador $\mathcal{U}(t) = e^{-iHt}$ es un operador unitario.*

Demostración. Observamos que

$$\mathcal{U}(t)\mathcal{U}^*(t) = e^{-iHt}e^{(-iHt)^*} = e^{-iHt}e^{iHt} = 1 = \mathcal{U}^*(t)\mathcal{U}(t). \tag{1.3.3}$$

■

En consecuencia, la dinámica $\psi(t) = \mathcal{U}(t)\psi_0$ siempre esta dada por operadores unitarios.

Lema 1.3.2. *Sea ψ un estado cuántico y $\mathcal{U} \in \mathcal{B}(\mathcal{H})$ un operador unitario entonces $\mathcal{U}\psi$ es un estado cuántico.*

Demostración.

$$\|\mathcal{U}\psi\|^2 = <\mathcal{U}\psi, \mathcal{U}\psi> = <\psi, \mathcal{U}^*\mathcal{U}\psi> = <\psi, \psi> = \|\psi\|^2, \tag{1.3.4}$$

por lo tanto $\mathcal{U}\psi$ es un estado cuántico. ■

Los operadores unitarios son fundamentales en la mecánica cuántica porque envían estados cuánticos en estados cuánticos.

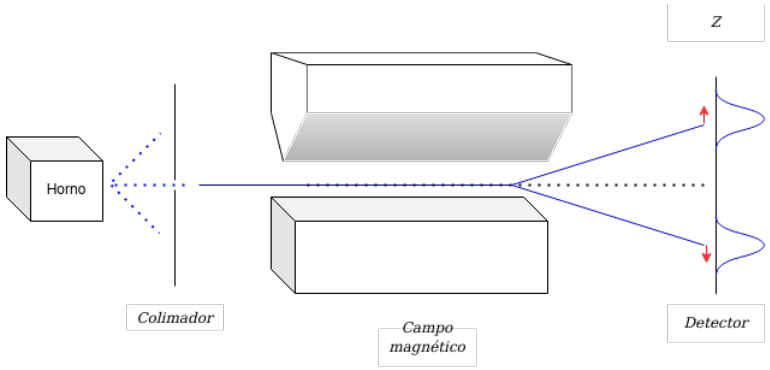

Figura 1.1: Esquema del Experimento de Stern-Gerlach

1.4 Experimento de Stern-Gerlach

El diagrama de la figura 1.1 describe un experimento que nos permitiremos introducir como un ejemplo físico al cual recurrir más adelante. En el experimento de Stern-Gerlach (SG), se utilizaron átomos de plata (Ag), obtenidos por la vaporización de plata en un horno, que salen por un pequeño orificio sin ninguna dirección preferida, por lo que se ubica seguidamente un colimador el cual produce un rayo de átomos que atraviesan un campo magnético, luego se mide en una placa de vidrio o detector la dirección en que fueron desviados los átomos.

El experimento comprobó la cuantización de una importante propiedad cuántica que tienen las partículas llamada espín (en inglés 'spin' que traduce 'girar'). El resultado esperado era una distribución uniforme de los átomos en el detector; en el resultado obtenido se observaba que, si el campo magnético estaba apagado median una mancha concentrada en $z = 0$; si, en cambio, estaba encendido, la interacción del campo con los átomos los desviaba en solo dos rayos opuestos en el eje z como en la figura 1.1.

El experimento es un ejemplo de un observable físico sobre un estado cuántico, a saber: un operador u observable en la dirección z, con dos valores posibles de medición, en este caso: espín "*arriba*" o espín "*abajo*" para cada átomo; por tanto, definimos una base de eigenestados: espín arriba denotado $|\uparrow\rangle$ y espín abajo $|\downarrow\rangle$, donde la notación es debida a Dirac; y las amplitudes de probabilidad, estarían determinadas por las probabilidades de obtener cada estado, esto es, la razón entre el número de átomos con espín arriba entre el número de partículas que participan del experimento, y de forma análoga, se obtiene la probabilidad de medir espín abajo. Además podemos definir los estados "*derecha*" y "*izquierda*" con otro observable, rotando en el eje x el experimento de SG, y determinando una nueva base de eigenvectores.

1.5 Notación de Dirac

Definición 1.5.1. El símbolo $|\cdot\rangle$, que se lee *ket*, denota un vector en el espacio de Hilbert $\mathbb{C}^n$.

En $\mathbb{C}^2$, las siguientes notaciones son equivalentes:

$$\begin{pmatrix}1\\0\end{pmatrix} \doteq |\uparrow\rangle \doteq |0\rangle \text{ y } \begin{pmatrix}0\\1\end{pmatrix} \doteq |\downarrow\rangle \doteq |1\rangle\,, \tag{1.5.1}$$

donde las igualdades se dan por definición.

El conjunto $\{|0\rangle, |1\rangle\}$ es base canónica de $\mathbb{C}^2$ como $\mathbb{C}-$espacio vectorial, esto es, el vector $(z_1, z_2) \in \mathbb{C}^2$ se escribe de forma única en la base como

$$|z\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + z_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = z_1 |0\rangle + z_2 |1\rangle . \tag{1.5.2}$$

En $\mathbb{C}^n$, si el conjunto $\{|v_1\rangle, \cdots, |v_n\rangle\}$ es base, escribimos en general $|v\rangle \in \mathbb{C}^n$ como la combinación lineal

$$|v\rangle = \sum_i^n a_i |v_i\rangle , \tag{1.5.3}$$

con $a_i \in \mathbb{C}$.

Definición 1.5.2. El producto interno del espacio $\mathcal{H} = \mathbb{C}^2$ en la notación de Dirac se escribe $\langle \cdot | \cdot \rangle$, y es equivalente a escribir para $v, w \in \mathcal{H}$,

$$\langle v|w\rangle = (v_1 |0\rangle + v_2 |1\rangle , w_1 |0\rangle + w_2 |1\rangle) = \begin{pmatrix} v_1^* & v_2^* \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = v_1^* w_1 + v_2^* w_2 \tag{1.5.4}$$

En general, en $\mathbb{C}^n$, el producto interno de $|v\rangle$ y $|w\rangle$ con respecto a la base ortonormal $\{|e_i\rangle, i = 1, \cdots, n\}$ lo escribimos como:

$$\langle v|w\rangle = \left(\sum_i a_i |e_i\rangle , \sum_j b_j |e_j\rangle \right) = \sum_i \sum_j \overline{a}_i b_j \langle e_i|e_j\rangle = \sum_{ij} \overline{a}_i b_j \delta_{ij} = \sum_i \overline{a_i} b_i, \tag{1.5.5}$$

donde $\langle e_i|e_j\rangle = \delta_{ij}$.

Definición 1.5.3. La norma del vector $|v\rangle \in \mathbb{C}^n$ en notación de Dirac se escribe de la siguiente forma:

$$\| |v\rangle \| \doteq \sqrt{\langle v|v\rangle} = \sqrt{\left(\sum_i a_i |e_i\rangle , \sum_j a_j |e_j\rangle \right)} = \sqrt{\sum_i \overline{a}_i a_i} = \sqrt{\sum_i |a_i|^2}. \tag{1.5.6}$$

Ejemplo 1.5.1. Definimos el observable Z que representa el espín de una particula en la dirección del eje Z, con eigenvalores $\{-1, 1\}$. Consideramos los eigenestados $|\uparrow\rangle, |\downarrow\rangle$, de modo que $Z|\uparrow\rangle = |\uparrow\rangle$, y $Z|\downarrow\rangle = -|\downarrow\rangle$, con respecto a esta base

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

Dado un estado $|\psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$, donde $|\alpha|^2 + |\beta|^2 = 1$; entonces

$$< Z >_\psi = |\alpha|^2 - |\beta|^2$$

es el valor esperado de Z con respecto a $|\psi\rangle$ donde $|\alpha|^2 =$ la probabilidad de medir $+1$, $|\beta|^2 =$ la probabilidad de medir -1, donde el observable Z representa el espín de una partícula en dirección del eje Z. En esta base, los observables de medir el espín en la dirección X, e Y respecto a $|\psi\rangle$ están dados por $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ con eigenvalores $\lambda \in \{1, -1\}$ como se muestra abajo

$$\det(X - \lambda 1) = \lambda^2 - 1 = 0,$$
$$\det(Y - \lambda 1) = \lambda^2 - 1 = 0.$$

Los valores esperados de X y Y con respecto al estado $|\psi\rangle$ son

$$\begin{aligned} < X >_\psi &=< \alpha|\uparrow\rangle + \beta|\downarrow\rangle, X(\alpha|\uparrow\rangle + \beta|\downarrow\rangle) > \\ &=< \alpha|\uparrow\rangle + \beta|\downarrow\rangle, \beta|\uparrow\rangle + \alpha|\downarrow\rangle > \\ &= \overline{\alpha}\beta + \overline{\beta}\alpha \in \mathbb{R}, \\ < Y >_\psi &=< \alpha|\uparrow\rangle + \beta|\downarrow\rangle, Y(\alpha|\uparrow\rangle + \beta|\downarrow\rangle) > \\ &=< \alpha|\uparrow\rangle + \beta|\downarrow\rangle, i\beta|\uparrow\rangle - i\alpha|\downarrow\rangle > \\ &= i\overline{\alpha}\beta - i\overline{\beta}\alpha \in \mathbb{R} \end{aligned}$$

con base de valores propios $|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$, $|\leftarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$ tal que, en el caso del observable X,

$$\begin{aligned} X|\rightarrow\rangle &= |\rightarrow\rangle, \\ X|\leftarrow\rangle &= -|\leftarrow\rangle \end{aligned}$$

con probabilidad 1.

1.6 Espacio de n partículas

Una herramienta importante en la mecánica cuántica para definir el espacio de n partículas es el producto tensorial de matrices.

Definición 1.6.1. El producto tensorial de dos espacios vectoriales $\mathcal{V}$ y $\mathcal{W}$ sobre $\mathbb{C}$ es un espacio vectorial el cual tiene asociada una aplicación bilineal $u : \mathcal{V}\times\mathcal{W} \to \mathcal{V}\otimes\mathcal{W}$ definida por $(v, w) \to v\otimes w$ donde $v \otimes w$ denota un elemento $\mathcal{V} \otimes \mathcal{W}$ que es llamado producto tensorial de $v \in \mathcal{V}$ y $w \in \mathcal{W}$.

Proposición 1.6.2. *Dada una base $\{e_1, \ldots, e_{n_1}\}$ de un espacio vectorial $\mathcal{V}$ de dimensión n_1 y $\{b_1, \ldots, b_{n_2}\}$ base de un espacio vectorial $\mathcal{W}$ de dimensión n_2. Entonces el conjunto*

$$\{e_k \otimes b_j : 1 \leqslant k \leqslant n_1, 1 \leqslant j \leqslant n_2\} \tag{1.6.1}$$

es una base para $\mathcal{V} \otimes \mathcal{W}$ el cual tiene dimensión n_1n_2.

Demostración. Véase [17], pág 306. ■

La Proposición 1.6.2 se puede generalizar al producto tensorial de k espacios vectoriales, donde la dimensión del producto tensorial es el producto de las dimensiones de cada espacio vectorial.

Sea el conjunto $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ una base para $\mathbb{C}^2 \otimes \mathbb{C}^2$, en la base escribimos los estados generales del producto tensorial como sigue

$$\sum_{j,k=\{0,1\}} \alpha_{jk}|j\rangle \otimes |k\rangle \tag{1.6.2}$$

donde $\sum_{j,k=\{0,1\}} |\alpha_{jk}|^2 = 1$.

Ejemplo 1.6.1. Si consideramos los estados $|\psi\rangle = a_1|0\rangle + a_2|1\rangle$ donde $|a_1|^2 + |a_2|^2 = 1$ y $|\varphi\rangle = c_1|0\rangle + c_2|1\rangle$ tal que $|c_1|^2 + |c_2|^2 = 1$, entonces el producto tensorial $|\psi\rangle \otimes |\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ se obtiene como sigue

$$|\psi\rangle \otimes |\varphi\rangle = (a_1|0\rangle + a_2|1\rangle) \otimes (c_1|0\rangle + c_2|1\rangle) \tag{1.6.3}$$

$$= a_1c_1|0\rangle \otimes |0\rangle + a_1c_2|0\rangle \otimes |1\rangle + a_2c_1|1\rangle \otimes |0\rangle + a_2c_2|1\rangle \otimes |1\rangle \tag{1.6.4}$$

$$= \sum_{j,k=\{0,1\}} \alpha_{jk}|j\rangle \otimes |k\rangle, \tag{1.6.5}$$

donde $\alpha_{jk} = a_jc_k$ y $\sum_{j,k=\{0,1\}} |\alpha_{jk}|^2 = 1$.

Observamos que la expresión (1.6.2) describe todos los estados de $\mathbb{C}^2 \otimes \mathbb{C}^2$ que se obtienen, como el producto tensorial de dos elementos independientes $|\psi\rangle$ y $|\varphi\rangle$ de $\mathbb{C}^2$ y aquellos que no se obtienen de este forma, los cuales describimos en la siguiente sección.

Consideramos $A, B \in \mathcal{M}(2, \mathbb{C})$, donde $\mathcal{M}(n, \mathbb{C})$ es el conjunto de matrices $n \times n$ con coeficientes en los complejos $\mathbb{C}$,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \tag{1.6.6}$$

en particular, consideramos A, B unitarias, entonces el producto tensorial de A y B tiene la siguiente representación

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{12}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ a_{21}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{22}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \end{pmatrix} \in \mathcal{M}(4, \mathbb{C}) \cong End(\mathbb{C}^2 \otimes \mathbb{C}^2), \tag{1.6.7}$$

donde $End(A)$ denota los endomorfismos del espacio A.

Ejemplo 1.6.2. Para $|\psi\rangle = a_1 |0\rangle + a_2 |1\rangle$ y $|\varphi\rangle = c_1 |0\rangle + c_2 |1\rangle$ del ejemplo 1.6.1 la representación matricial del producto tensorial es

$$|\psi\rangle \otimes |\varphi\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \\ a_2 \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1 c_1 \\ a_1 c_2 \\ a_2 c_1 \\ a_2 c_2 \end{pmatrix}. \tag{1.6.8}$$

Ahora calculamos la aplicación del operador A sobre el ket $|\psi\rangle$ producto tensorial el operador B sobre el $|\varphi\rangle$ respecto de la base, obtenemos

$$\begin{aligned} (A \otimes Id)(Id \otimes B) |\psi\rangle \otimes |\varphi\rangle &= (A \otimes B) \sum_{j,k=\{0,1\}} \alpha_{jk} |j\rangle \otimes |k\rangle \\ &= \sum_{j,k=\{0,1\}} \alpha_{jk} A |j\rangle \otimes B |k\rangle \\ &= \alpha_{00} A |0\rangle \otimes B |0\rangle + \alpha_{01} A |0\rangle \otimes B |1\rangle + \alpha_{10} A |1\rangle \otimes B |0\rangle + \alpha_{11} A |1\rangle \otimes B |1\rangle . \end{aligned} \tag{1.6.9}$$

Hemos considerado que una partícula o estado cuántico pertenece al espacio $\mathbb{C}^2 = gen\{|0\rangle, |1\rangle\}$ y sobre el cual se definen observables con dos valores propios distintos. Luego, el espacio de Hilbert de n estados cuánticos está dado por el espacio tensorial $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \bigotimes_{j=1}^{n} \mathbb{C}^2$.

Modelamos estados de dos partículas en $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. Sean T_1, T_2 observables para estados de una partícula. Su producto tensorial, abajo definido, es una observable para estados de dos partículas.

$$(T_1 \otimes T_2)(x \otimes y) \doteq (T_1 x) \otimes (T_2 y) \tag{1.6.10}$$

Si $\{|0\rangle, |1\rangle\} \subseteq \mathbb{C}^2$ son vectores propios de T_1,

$$T_1 |0\rangle = \lambda_0 |0\rangle \tag{1.6.11}$$

$$T_1 |1\rangle = \lambda_1 |1\rangle \tag{1.6.12}$$

y $\{|0\rangle', |1\rangle'\} \subseteq \mathbb{C}^2$ son vectores propios de T_2,

$$T_2 |0\rangle' = \lambda_0' |0\rangle' \tag{1.6.13}$$
$$T_2 |1\rangle' = \lambda_1' |1\rangle' \tag{1.6.14}$$

entonces

$$|0\rangle \otimes |0\rangle', |0\rangle \otimes |1\rangle', |1\rangle \otimes |0\rangle', |1\rangle \otimes |1\rangle'$$

son una base de vectores propios de $T_1 \otimes T_2$, con valores propios $\lambda_0\lambda_0', \lambda_0\lambda_1', \lambda_1\lambda_0', \lambda_1\lambda_1'$, respectivamente.

1.7 Estados entrelazados

Definición 1.7.1. Los estados entrelazados son los vectores $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ tales que

$$|\psi\rangle = \sum_{i,j} \alpha_{ij} |i\rangle \otimes |j\rangle' \notin \{|x\rangle \otimes |y\rangle, |x\rangle, |y\rangle \in \mathcal{H}\}. \tag{1.7.1}$$

Donde $\sum_{ij} |\alpha_{ij}|^2 = 1$. En palabras, no se obtienen como el producto tensorial de dos estados.

Un ejemplo de estados entrelazados son los estados de Bell

$$\frac{1}{\sqrt{2}} \left(|0\rangle |0\rangle' \pm |1\rangle |1\rangle' \right), \quad \frac{1}{\sqrt{2}} \left(|0\rangle |1\rangle' \pm |1\rangle |0\rangle' \right). \tag{1.7.2}$$

Los estados entrelazados tienen una propiedad distinguida, si se mide el observable T_1 en el primer factor, el estado del segundo factor queda completamente determinado por el colapso de la función de onda en el primer factor.

Ejemplo 1.7.1. Consideramos el estado entrelazado de Bell $|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle |0\rangle + |1\rangle |1\rangle)$, y las observables $T_1 \otimes I$ y $I \otimes T_2$ del sistema cuántico. Si un observador mide $T_1 \otimes I$ y obtiene como eigenvalor -1, entonces la función de onda colapsa en el primer factor a $|0\rangle$, por lo tanto, $|\psi\rangle$ colapsa a $|0\rangle |0\rangle$, luego, si se mide $I \otimes T_2$ se obtiene -1 con probabilidad 1.

El entrelazamiento es uno de los fenómenos más particulares de la mecánica cuántica, el cual puso en controversia a grandes físicos, como se describe en el apéndice A.

Capítulo 2

Circuitos Cuánticos

La teoría de la computación clásica fue desarrollada sobre los fundamentos de la física clásica; pero desde que hubo el convencimiento en los físicos de la validez de la teoría cuántica, iniciaron a sugerirse las posibilidades de codificar información de forma análoga a los sistemas clásicos en sistemas cuánticos. Pero el paradigma de la computación cuántica de ninguna forma podía ser equivalente al procesamiento de bits clásicos, de modo que se dio el paso por establecer los fundamentos de una nueva computación, de la cual describimos sus elementos fundamentales:

- El qubit o estado cuántico $|\psi\rangle$ como unidad mínima de información cuántica.
- La evolución del estado cuántico en el tiempo es descrita por un operador unitario $T(t)$ sobre el espacio de Hilbert del estado, es decir, una transformación lineal la cual es biyectiva y preserva la longitud [21]. Debido a que los cambios de estados de la mecánica cuántica deben ser reversibles, el operador unitario $T^{-1} = T^*$ siempre existe.
- **Compuertas cuánticas** El formalismo descrito aquí para la computación cuántica corresponde con lo que se conoce como *arreglo de compuertas cuánticas*, del cual se obtendrán las compuertas universales para el desarrollo de la computación cuántica. Las compuertas cuánticas deben ser reversibles por tanto, tienen el mismo número de entradas que de salidas. Una compuerta de n qubits de entrada lleva a cabo una operación unitaria del grupo $U(2^n)$, es decir, una rotación generalizada en un espacio de Hilbert de dimensión 2^n. Puede ser la aplicación de un operador unitario definido por la evolución en el tiempo del sistema dictada por ell Hamiltoniano o una interacción externa.

2.1 Esfera de Bloch

Definición 2.1.1. Un *qubit* es un estado cuántico $|\psi\rangle \in \mathbb{C}^2$, el cual se define como la unidad mínima de información cuántica.

Por tanto, un qubit $|\psi\rangle$ es un elemento de la 3-esfera $\mathbb{S}^3$, donde

$$\mathbb{S}^3 = \{\alpha\,|0\rangle + \beta\,|1\rangle : |\alpha|^2 + |\beta|^2 = 1\} \subseteq \mathbb{C}^2. \tag{2.1.1}$$

Consideramos el grupo unitario $U(1) = \{z \in \mathbb{C} : |z| = 1\}$, y el espacio proyectivo complejo de dimensión uno $\mathbb{CP}^1 = \mathbb{C}^2 - \{0\}/\sim$, dado por la relación de equivalencia:

$$(z_1, z_2) \sim (\xi_1, \xi_2) \Longleftrightarrow \exists \lambda \in \mathbb{C} \text{ tal que } (z_1, z_2) = \lambda(\xi_1, \xi_2). \tag{2.1.2}$$

Proposición 2.1.2. $\mathbb{CP}^1$ *parametriza los mismos estados de la* 3*-esfera* $\mathbb{S}^3$*, salvo la multiplicación por* $e^{i\theta} \in U(1)$*, donde* $\theta \in \mathbb{R}$*, es decir:*

$$[\alpha\,|0\rangle + \beta\,|1\rangle] = [e^{i\theta}(\alpha\,|0\rangle + \beta\,|1\rangle)]. \tag{2.1.3}$$

Demostración. Reescribimos $\mathbb{CP}^1$ como sigue

$$\mathbb{CP}^1 = \{[(z_1, z_2)] : (z_1, z_2) \in \mathbb{C}^2 - \{0\}\} \tag{2.1.4}$$

$$= \left\{ \left[\frac{(z_1, z_2)}{\|(z_1, z_2)\|} \right] : (z_1, z_2) \in \mathbb{C}^2 - \{0\} \right\} \tag{2.1.5}$$

$$= \{[(z_1, z_2)] : (z_1, z_2) \in \mathbb{S}^3\}. \tag{2.1.6}$$

Por tanto, para $(z_1, z_2), (\xi_1, \xi_2) \in \mathbb{S}^3$, se obtiene que $(z_1, z_2) \sim (\xi_1, \xi_2) \iff \exists \lambda \in \mathbb{C}$ tal que $(z_1, z_2) = \lambda(\xi_1, \xi_2)$; como $1 = \|(z_1, z_2)\| = \|\lambda(\xi_1, \xi_2)\| = |\lambda|\|(\xi_1, \xi_2)\|$, se obtiene que $|\lambda| = 1$ y por tanto $\lambda \in U(1)$. Consideramos $\lambda = e^{i\theta} \in U(1)$ entonces definimos la acción:

$$\pi : U(1) \times \mathbb{S}^3 \to \mathbb{S}^3 \tag{2.1.7}$$

$$(e^{i\theta}, \psi) \longmapsto e^{i\theta}\psi \tag{2.1.8}$$

$$(e^{i\theta}, (\alpha, \beta)) \longmapsto (e^{i\theta}\alpha, e^{i\theta}\beta), \tag{2.1.9}$$

obtenemos que

$$\mathbb{CP}^1 = \frac{\mathbb{S}^3}{U(1)}, \tag{2.1.10}$$

por $(e^{i\theta}z_1, e^{i\theta}z_2) \mapsto [(z_1, z_2)]$ para todo $e^{i\theta} \in U(1)$. ■

Proposición 2.1.3. *Sea* $|\psi\rangle \in \mathbb{S}^3$ *un estado cuántico, entonces* $|\psi\rangle$ *tiene un representante de la forma* $\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle$ *donde* $\theta \in [0, \pi]$ *y* $\varphi \in [0, 2\pi)$*, el cual es un punto en la 2-esfera* $\mathbb{S}^2$*.*

Demostración. Dado que un qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathbb{S}^3$, satisface $|\alpha|^2 + |\beta|^2 = 1$, escribimos $\alpha = |\alpha|e^{i\gamma}$ y $\beta = |\beta|e^{i(\phi+\gamma)}$ [8] y definimos

$$|\alpha| = \cos\frac{\theta}{2} \geqslant 0, \qquad |\beta| = \sin\frac{\theta}{2} \geqslant 0 \tag{2.1.11}$$

luego, nuestro qubit se reescribe de la siguiente forma

$$|\psi\rangle = e^{i\gamma}\cos\frac{\theta}{2}\,|0\rangle + e^{i(\varphi+\gamma)}\sin\frac{\theta}{2}\,|1\rangle \tag{2.1.12}$$

$$= e^{i\gamma}\Big(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\Big), \tag{2.1.13}$$

donde $\theta \in [0, \pi]$ y $\varphi, \gamma \in [0, 2\pi)$ [21]. El término $e^{i\gamma}$ es la fase global del vector $|\psi\rangle$, la cual podemos descartar por la Proposición 1.1.8 y 2.1.2; obtenemos un representante de nuestro estado o qubit sin fase global

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle \tag{2.1.14}$$

con esta expresión podemos representar un qubit mediante θ y φ como un punto en la 2-esfera, la cual se conoce como *Esfera de Bloch* debida al físico Felix Bloch, en la cual se describe la

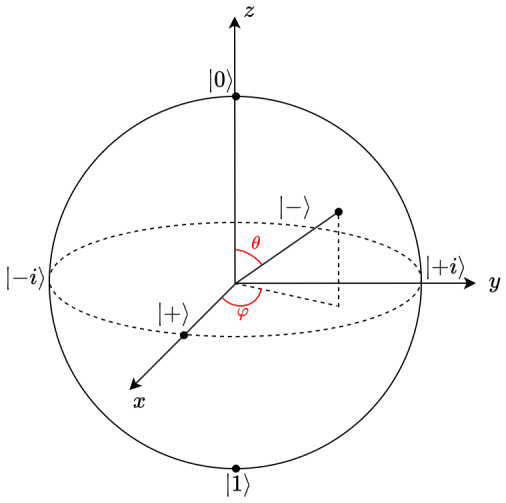

Figura 2.1: Esfera de Bloch

representación geométrica de un vector de estado encajada en el espacio $\mathbb{R}^3$, es decir, se puede escribir en dos parametrizaciones, utilizando coordenadas esféricas, de la siguiente forma:

$$\begin{pmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{pmatrix} \in \mathbb{R}^3 \longleftarrow (\theta,\varphi) \longrightarrow \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \in \mathbb{S}^3 \subseteq \mathbb{C}^2 \tag{2.1.15}$$

donde $\theta \in [0,\pi]$ y $\varphi \in (-\pi,\pi]$. ■

Consideramos los estados en la esfera de Bloch sobre los ejes Z, X y Y, escritos explícitamente como en la expresión (2.1.15) de la siguiente forma:

$$(0,0,1)^T \leftarrow (0,\varphi) \rightarrow |0\rangle \tag{2.1.16}$$

$$(0,0,-1)^T \leftarrow (\pi,\varphi) \rightarrow e^{i\varphi}|1\rangle \rightarrow |1\rangle \tag{2.1.17}$$

$$(1,0,0)^T \leftarrow (\pi/2,0) \rightarrow |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.1.18}$$

$$(-1,0,0)^T \leftarrow (\pi/2,\pi) \rightarrow |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.1.19}$$

$$(0,1,0)^T \leftarrow (\pi/2,\pi/2) \rightarrow |+i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \tag{2.1.20}$$

$$(0,-1,0)^T \leftarrow (\pi/2,-\pi/2) \rightarrow |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \tag{2.1.21}$$

como se observa en la Figura 2.1.

Observamos que, si $\theta = 0$, obtenemos el estado $|\psi\rangle = |0\rangle$, y si $\theta = \pi$ obtenemos $|\psi\rangle = |1\rangle$; además, notamos que el intervalo en el cual varían las amplitudes de probabilidad (2.1.11), $\frac{\theta}{2} \in [0,\pi/2]$, donde las funciones coseno y seno son no negativas. La ubicación de los estados $|0\rangle$ y $|1\rangle$ es definida sobre el eje Z, sin embargo, parece contradictorio dado que son estados ortogonales.

Debemos resaltar que al definir un qubit como la unidad mínima de información cuántica, se desea utilizar los qubits para realizar cálculos o procesar información; en este sentido, observar un

qubit en la esfera de Bloch, la cual es un conjunto infinito de puntos, nos sugiere que un qubit podría almacenar información infinita. Sin embargo, nuestra limitación es que requerimos *medir*; esto es, utilizar un instrumento de medición el cual colapsa el estado cuántico; si $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ es un qubit en la esfera de Bloch antes de medir, se obtiene despúes de medir el estado $|0\rangle$ o $|1\rangle$, según el eigenvalor medido, de modo que, se pierde el qubit como superposición de los dos estados; así que no tenemos información infinita, solo dos valores posibles; no obstante, el estado se puede identificar si se preparan n veces el mismo estado, dado que al medir, obtenemos aproximadamente las probabilidades $|\alpha|^2$ y $|\beta|^2$ y, por tanto, el estado, salvo la fase $e^{i\varphi}$.

Unidad de información clásica vs cuántica

En los sistemas clásicos la unidad de información básica es el *bit*, abreviación de dígito binario; los dispositivos de recepción, transmisión y procesamiento de información trabajan con bits y la lógica booleana, y toda nuestra tecnología se fundamenta en ellos, los cuales se obtienen, o bien como valores de voltaje, o como el paso o no de corriente eléctrica.

Pero ¿qué significa información en los sistemas clásicos?, y ¿por qué la medimos en bits? El concepto de medida de información fue planteado por Claude Shannon [25], quien desarrolló la teoría matemática de la información, definiéndola como medida de incertidumbre. Por ejemplo, en cada lanzamiento de una moneda equilibrada, la incertidumbre es máxima, no podemos afirmar cuál será el resultado, y dado que tenemos dos resultados posibles $\{cara, sello\}$, la cantidad de información es $\log_2 2 = 1$ bit, pero si tenemos un moneda no equilibrada, de tal forma que la probabilidad de que ocurra una de sus caras es $p_c \doteq p_{cara} \in (1/2, 1)$, la medida de incertidumbre definida por $H = p_c \log_2 1/p_c + (1-p_c)\log_2 1/(1-p_c) < 1$ bit, y la medida de información definida por $\log_2 1/p_c$, muestra que la información es cero, cuando la probabilidad es uno, es decir, cuando no hay incertidumbre y por lo tanto el resultado no aporta información, así que la entropía de la información $H = \sum_i p_i \log 1/p_i$ es función de las probabilidades de cada resultado posible, es medida en bits y determina la codificación de la información.

En este sentido, en mecánica cuántica ¿cuánta información aporta un qubit?, de nuevo, un qubit representado en la esfera de Bloch, no puede almacenar información infinita, ya que al medir colapsa en uno de dos posibles resultados, entonces de cada medición solo obtendremos un bit de información.

Así que al considerar los valores propios del observable T como los bits clásicos, es decir, $\{\lambda_1, \lambda_2\} \cong \{0, 1\}$, no habría diferencia entre la computación cuántica y la clásica. Es decir, cuando medimos estamos restringidos a los mismos resultados clásicos de un bit para un qubit, ya que en su infinidad de estados, al introducir el dispositivo de medición de un observable T, se proyectará la medida únicamente en uno de sus dos eigenvectores, es decir, medimos uno de los dos valores propios, a saber, 0 o 1. Concluimos que un qubit es un estado cuántico con una estructura matemática compleja a diferencia del bit clásico; dado que en adelante, estudiaremos los qubits en el espacio de Hilbert complejo, queda definida su distinción respecto a los bits clásicos, a pesar de que al medir no se distinguen.

Implementación física de un Qubit

Un qubit es un sistema cuántico de dos niveles como, por ejemplo, el espín de un electrón, el cual se puede obtener físicamente como se describió en el experimento de Stern Gerlach. Desde la década de los 90's en los que se fundamentó la teoría de la computación cuántica, diversas implementaciones que buscan obtener qubits útiles para el procesamiento de información se han desarrollado, entre

ellas, dispositivos superconductores[1] y trampas de iones. Entre otros sistemas físicos que describen a un qubit encontramos la polarización de un fotón o el espín nuclear [21].

2.2 Compuertas de un Qubit

2.2.1 Descomposición de Operadores Unitarios

Definición 2.2.1. Una compuerta de un qubit es un operador unitario $U \in \mathcal{B}(\mathbb{C}^2)$.

Los operadores unitarios $U \in \mathcal{B}(\mathbb{C}^2)$ son un conjunto infinito, por tanto, tenemos infinitas compuertas de un qubit. A diferencia del cómputo clásico, donde solo se tiene una compuerta lógica para un bit, llamada compuerta *NOT*. Una compuerta cuántica que cambia el estado como la compuerta NOT es el operador X, que intercambia los estados $|0\rangle$ y $|1\rangle$ del qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$, el cual tiene la representación matricial siguiente:

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

La anterior es una de tres matrices importantes en la mecánica cuántica, llamadas matrices de Pauli, a saber,

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.2.1}$$

Observamos que $X = X^*, Y = Y^*$ y $Z = Z^*$, por lo tanto, las matrices de Pauli son observables; con las siguientes propiedades

$$\sigma_k^2 = I, \quad \sigma_i\sigma_j + \sigma_j\sigma_i = 0$$

para todo $i \neq j$. Las matrices de Pauli, serán centrales en el estudio de la computación cuántica, porque como se muestra más adelante, al exponenciarlas corresponden a operadores de rotación sobre el espacio de estados y más aún, actúan como momentos angulares.

Definición 2.2.2. El operador X es la *compuerta cuántica NOT*; la cual se escribe en notación de Dirac de la siguiente forma:

$$X|j\rangle = |j \oplus 1\rangle, \tag{2.2.2}$$

donde, $j \in \{0, 1\}$ y $\oplus$ es la operación suma módulo 2.

La aplicación de las matrices de Pauli, o también llamadas compuertas de Pauli, sobre un qubit $|\psi\rangle$, es la siguiente:

$$\begin{aligned} X(\alpha|0\rangle + \beta|1\rangle) &= X\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle, \\ Z(\alpha|0\rangle + \beta|1\rangle) &= Z\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle, \\ Y(\alpha|0\rangle + \beta|1\rangle) &= Y\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix} = -i\beta|0\rangle + i\alpha|1\rangle. \end{aligned}$$

[1] Entre las empresas que utilizan superconductores se encuentran IBM, Google, Rigetti, Alibaba, Intel, Quantum Circuits y Oxford Quantum Circuits.

Para los algoritmos cuánticos más notables que se implementan en el formalismo de circuitos cuánticos, no sería eficiente considerar el diseño e implementación de un conjunto infinito de compuertas, por tanto, un objetivo fundamental en el diseño de circuitos cuánticos es establecer un modelo universal de compuertas cuánticas, es decir, definir un conjunto finito de ellas, de tal forma que con combinaciones de este conjunto las aproximen a todas [3] [6]. Construimos a continuación la descomposición que nos llevara a identificar un conjunto finito de compuertas universales de un qubit.

Las compuertas cuánticas u operadores unitarios de un qubit $U \in \mathcal{B}(\mathbb{C}^2)$ son representadas por una matriz en el conjunto $\mathcal{M}(2,\mathbb{C})$, con la siguiente propiedad.

Teorema 2.2.3. *Toda matriz unitaria $U \in \mathcal{B}(\mathbb{C}^2)$, se puede escribir como:*

$$U = e^{i\theta} e^{i\alpha Z} e^{i\beta Y} e^{i\gamma Z}, \tag{2.2.3}$$

donde $\theta, \alpha, \beta, \gamma \in \mathbb{R}$, Z y Y matrices de Pauli.

Demostración. El grupo especial unitario $SU(2)$ es definido como:

$$SU(2) = \left\{ \begin{pmatrix} \alpha & \overline{\beta} \\ -\beta & \overline{\alpha} \end{pmatrix} : |\alpha|^2 + |\beta|^2 = 1 \right\} \tag{2.2.4}$$

$$= \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2 \cong \mathbb{H}^* : \left\| \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right\| = 1 \right\} \cong \mathbb{S}^3, \tag{2.2.5}$$

donde $\mathbb{H}^* \doteq \mathbb{H} \setminus \{0\}$ es el grupo multiplicativo de cuaterniones no nulos. Por lo tanto, $SU(2) \cong \mathbb{S}^3$. Sea $U \in \mathcal{M}(2,\mathbb{C})$ unitaria, tal que el $\det(U) = e^{i\phi} \in U(1)$. Si escribimos $U = e^{i\phi/2}(e^{-i\phi/2}U)$, el determinante del término en paréntesis es

$$\det e^{-i\phi/2} U = e^{-i\phi} \det U = 1. \tag{2.2.6}$$

Sea $\theta = -\phi/2$, definimos $V \doteq e^{i\theta}U$, dado que su determinante es 1, $V \in SU(2) \cong \mathbb{S}^3$. Por lo tanto, es suficiente obtener $V = e^{i\alpha Z} e^{i\beta Y} e^{i\gamma Z}$.

Sea $V = \begin{pmatrix} \alpha & \overline{\beta} \\ -\beta & \overline{\alpha} \end{pmatrix}$ donde $\alpha = re^{it}$ y $\beta = \sqrt{1-r^2}e^{is}$, con $r \in [0,1]$ y $s,t \in [0,2\pi)$, esto es:

$$V = \begin{pmatrix} re^{it} & \sqrt{1-r^2}e^{-is} \\ -\sqrt{1-r^2}e^{is} & re^{-it} \end{pmatrix} \tag{2.2.7}$$

$$= \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix} \begin{pmatrix} r & \sqrt{1-r^2}e^{-i(s+t)} \\ -\sqrt{1-r^2}e^{i(s+t)} & r \end{pmatrix} \tag{2.2.8}$$

$$= \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix} \begin{pmatrix} e^{-i(s+t)/2} & 0 \\ 0 & e^{i(s+t)/2} \end{pmatrix} \begin{pmatrix} r & \sqrt{1-r^2} \\ -\sqrt{1-r^2} & r \end{pmatrix} \begin{pmatrix} e^{i(s+t)/2} & 0 \\ 0 & e^{-i(s+t)/2} \end{pmatrix}. \tag{2.2.9}$$

Luego,

$$U = e^{i\phi} \begin{pmatrix} e^{i(t-s)/2} & 0 \\ 0 & e^{-i(t-s)/2} \end{pmatrix} \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} e^{i(s+t)/2} & 0 \\ 0 & e^{-i(s+t)/2} \end{pmatrix} \tag{2.2.10}$$

$$= e^{i\theta} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} e^{i\gamma} & 0 \\ 0 & e^{-i\gamma} \end{pmatrix}, \tag{2.2.11}$$

donde $\alpha = \frac{t-s}{2}$, $r = \cos\beta$ para $\beta \in [0, \pi/2]$, y $\gamma = \frac{t+s}{2}$. Observamos que

$$\begin{aligned} e^{i\alpha Z} &= \sum_{n=0}^{\infty} \frac{(i\alpha)^n}{n!} Z^n = \sum_{k=0}^{\infty} \frac{(i\alpha)^{2k}}{(2k)!} Z^{2k} + \sum_{k=0}^{\infty} \frac{(i\alpha)^{2k+1}}{(2k+1)!} Z^{2k+1} \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k \alpha^{2k}}{(2k)!} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \sum_{k=0}^{\infty} \frac{i(-1)^k \alpha^{2k+1}}{(2k+1)!} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \cos\alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + i \sin\alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha + i\sin\alpha & 0 \\ 0 & \cos\alpha - i\sin\alpha \end{pmatrix} \\ &= \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}. \end{aligned}$$

Análogamente,

$$\begin{aligned} e^{i\beta Y} &= \sum_{n=0}^{\infty} \frac{(i\beta)^n}{n!} Y^n = \sum_{k=0}^{\infty} \frac{(i\beta)^{2k}}{(2k)!} Y^{2k} + \sum_{k=0}^{\infty} \frac{(i\beta)^{2k+1}}{(2k+1)!} Y^{2k+1} \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k \beta^{2k}}{(2k)!} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \sum_{k=0}^{\infty} \frac{i(-1)^k \beta^{2k+1}}{(2k+1)!} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ &= \cos\beta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + i \sin\beta \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix}, \end{aligned}$$

lo cual completa la prueba. ■

Proposición 2.2.4. *Los operadores unitarios $e^{i\alpha Z}$ y $e^{i\beta Y}$ definen una rotación en $\mathbb{R}^3$.*

Demostración. Consideramos la aplicación φ como un encaje de $\mathbb{R}^3 \hookrightarrow \mathcal{M}(2, \mathbb{C})$, como sigue:

$$\begin{aligned} \varphi : \mathbb{R}^3 &\hookrightarrow \mathcal{M}(2, \mathbb{C}), \\ (x_1, x_2, x_3)^T &\mapsto A = \begin{pmatrix} x_3 & x_1 - ix_2 \\ x_1 + ix_2 & -x_3 \end{pmatrix}, \end{aligned}$$

donde A tiene determinante:

$$\det A = -x_3^2 - (x_1^2 + x_2^2) = -(x_1^2 + x_2^2 + x_3^2) = -\left\| \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \right\|_{\mathbb{R}^3}^2.$$

Para toda $U \in SU(2)$, tenemos

$$\det UAU^* = \det U \det U^* \det A = \det A,$$

entonces UAU^* define una transformación invertible e isométrica de $\mathbb{R}^3$. Definimos la siguiente acción

$$\begin{aligned} T : SU(2) \times \mathcal{M}(2, \mathbb{C}) &\to \mathcal{M}(2, \mathbb{C}) \\ (U, A) &\mapsto UAU^*. \end{aligned}$$

Consideramos $U = e^{i\alpha Z}$ actuando sobre $A = \varphi(\mathbf{x})$ donde $\mathbf{x} = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ como sigue,

$$T(e^{i\alpha Z}, A) \doteq e^{i\alpha Z} \triangleright \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} x_3 & x_1 - ix_2 \\ x_1 + ix_2 & -x_3 \end{pmatrix} \begin{pmatrix} e^{-i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{2.2.12}$$

$$= \begin{pmatrix} x_3 & e^{i2\alpha}(x_1 - ix_2) \\ e^{-i2\alpha}(x_1 + ix_2) & -x_3 \end{pmatrix} \tag{2.2.13}$$

Notamos que $\varphi^{-1}(A) \in \mathbb{R}^3$, así que denotamos el vector que se obtiene de aplicar $e^{i\alpha Z}$ de la siguiente forma,

$$e^{i\alpha Z} \triangleright \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \doteq \begin{pmatrix} x_1 \cos 2\alpha + x_2 \sin 2\alpha \\ -x_1 \sin 2\alpha + x_2 \cos 2\alpha \\ x_3 \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha & 0 \\ -\sin 2\alpha & \cos 2\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}. \tag{2.2.14}$$

Por lo tanto, si consideramos x_1, x_2, x_3 los ejes coordenados de $\mathbb{R}^3$, entonces la acción de $e^{i\alpha Z}$ sobre $\mathbb{R}^3$ corresponde a una rotación en el plano x_1, x_2. De forma análoga obtenemos la acción de $e^{i\beta Y}$ sobre $\mathbf{x}$,

$$e^{i\beta Y} \triangleright \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} x_3 & x_1 - ix_2 \\ x_1 + ix_2 & -x_3 \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \tag{2.2.15}$$

$$= \begin{pmatrix} x_1 \sin 2\beta + x_3 \cos 2\beta & x_1 \cos 2\beta - x_3 \sin 2\beta - ix_2 \\ x_1 \cos 2\beta - x_3 \sin 2\beta + ix_2 & -x_1 \sin 2\beta - x_3 \cos 2\beta \end{pmatrix} \tag{2.2.16}$$

por tanto,

$$e^{i\beta Y} \triangleright \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \cos 2\beta - x_3 \sin 2\beta \\ x_2 \\ x_1 \sin 2\beta + x_3 \cos 2\beta \end{pmatrix} = \begin{pmatrix} \cos 2\beta & 0 & -\sin 2\beta \\ 0 & 1 & 0 \\ \sin 2\beta & 0 & \cos 2\beta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \tag{2.2.17}$$

obtenemos una rotacion en el plano x_1, x_3. ■

Consideramos el momento angular $L = (L_x, L_y, L_z)^T \in \mathbb{R}^3$ de una rotación definido por

$$L = mr \times \dot{r}, \tag{2.2.18}$$

donde $r(t) \in \mathbb{R}^3$ y $\dot{r}$ denota la derivada con respecto al tiempo de $r(t)$, y $\times$ denota el producto vectorial en $\mathbb{R}^3$.

Si calculamos el momento angular de $r_z(t) \doteq e^{-itZ/2} \triangleright \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos t \\ \sin t \\ 0 \end{pmatrix}$ y por tanto $\dot{r}_z(t) = \begin{pmatrix} -\sin t \\ \cos t \\ 0 \end{pmatrix}$, obtenemos lo siguiente

$$L = mr_z(t) \times \dot{r}_z(t) = \begin{pmatrix} 0 \\ 0 \\ m \end{pmatrix} \tag{2.2.19}$$

esto es, $L = (0, 0, L_z)$ es paralelo al eje z, donde $L_z = m$.

Análogamente, si consideramos $r_y(t) \doteq e^{-itY/2} \triangleright \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}\cos t\\0\\\sin t\end{pmatrix}$ se obtiene

$$L = \begin{pmatrix}0\\m\\0\end{pmatrix} \tag{2.2.20}$$

esto es, $L = (0, L_y, 0)$ es paralelo al eje y, donde $L_y = m$. Y, si $r_x(t) \doteq e^{-itX/2} \triangleright \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\\cos t\\\sin t\end{pmatrix}$, donde $e^{itX} = \begin{pmatrix}\cos t & i\sin t\\ i\sin t & \cos t\end{pmatrix}$, se obtiene

$$L = \begin{pmatrix}m\\0\\0\end{pmatrix} \tag{2.2.21}$$

esto es, $L = (L_x, 0, 0)$ es paralelo al eje x, donde $L_x = m$. Por lo tanto X, Y y Z representan los observables del momento angular L_x, L_y y L_z, respectivamente.

Consideramos el grupo de rotaciones en $\mathbb{R}^3$ definido por $SO(3) = \{R \in \mathcal{M}(3, \mathbb{R}) : R^T R = I, \det R = 1\}$.

Corolario 2.2.5. *Las compuertas cuánticas $V \in SU(2)$ son representadas sobre $\mathbb{R}^3$ como elementos de $SO(3)$.*

El corolario anterior es equivalente a mostrar que existe un homomorfismo sobreyectivo de $\varphi : SU(2) \to SO(3)$ con $Ker(\varphi) = \{\pm I\}$, del cual se sigue que [24]

$$\frac{SU(2)}{\pm I} \cong SO(3). \tag{2.2.22}$$

Denotamos $R_z(\theta) = e^{-i\theta Z/2}$ la rotación por un ángulo θ alrededor del eje z, y de forma análoga $R_x(\theta) = e^{-i\theta X/2}$ y $R_y(\theta) = e^{-i\theta Y/2}$, por el Teorema 2.2.3, se obtiene el siguiente resultado.

Corolario 2.2.6. *El conjunto de todas las posibles puertas cuánticas de un solo qubit es el grupo unitario de matrices 2×2,*

$$U(2) = \{e^{i\theta} R_z(\alpha) R_y(\beta) R_z(\gamma) : \alpha, \beta, \gamma \in \mathbb{R}\}.$$

Observamos que se han elegido los ejes y y z para describir todo $SU(2)$, sin embargo, basta tomar dos ejes no paralelos.

Proposición 2.2.7. *Una rotación $A \in SU(2)$ se puede escribir de la siguiente forma*

$$R_{\hat{n}}(\theta) = e^{-i\theta \hat{n}\sigma/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}(n_x X + n_y Y + n_z Z), \tag{2.2.23}$$

donde $\hat{n} = (n_x, n_y, n_z)$ es un vector unitario, θ es el ángulo de rotación alrededor del eje $\hat{n}$ y $\sigma = (X, Y, Z)$ denota el vector de matrices de Pauli.

Ejemplo 2.2.1. Compuerta Hadamard, definida como la matriz unitaria:

$$H = \frac{X+Z}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{2.2.24}$$

Se verifica con facilidad que H es autoadjunta y unitaria, esto es, $H = H^*$ y $HH^* = H^*H = I$. La acción de H sobre el estado $|0\rangle$ es,

$$H|0\rangle = H\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{2.2.25}$$

notamos que $H|0\rangle = |+\rangle$ definido en (2.1.18); de forma análoga $H|1\rangle = |-\rangle$ definido en (2.1.19). Por tanto, la acción de H sobre el qubit $|\psi\rangle$ es,

$$H|\psi\rangle = H\Big(\alpha|0\rangle + \beta|1\rangle\Big) = \alpha H|0\rangle + \beta H|1\rangle = \alpha|+\rangle + \beta|-\rangle. \tag{2.2.26}$$

Luego, H se puede descomponer como el producto de una fase relativa $\theta = \pi/2$ y rotaciones alrededor de los ejes x y z, salvo fase global de la siguiente forma:

$$H = e^{i\pi/2}R_z(\pi/2)R_x(\pi/2)R_z(\pi/2).$$

Ejemplo 2.2.2. Compuerta $\pi/8$ denotada por T:

$$T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix} = e^{i\pi/8}\begin{pmatrix}e^{-i\pi/8} & 0\\ 0 & e^{i\pi/8}\end{pmatrix} = e^{i\pi/8}R_z(\pi/4) \tag{2.2.27}$$

Ejemplo 2.2.3. Compuerta Fase denotada como P (*Phase*):

$$P = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix} = e^{i\pi/4}R_z(\pi/2) = T^2. \tag{2.2.28}$$

Vamos a utilizar la siguiente notación

$$|\psi\rangle^{\otimes n} \doteq \underbrace{|\psi\rangle \otimes \cdots \otimes |\psi\rangle}_{\text{n veces}}$$

$$U^{\otimes n}|\psi\rangle^{\otimes n} \doteq \underbrace{U|\psi\rangle \otimes \cdots \otimes U|\psi\rangle}_{\text{n veces}}$$

donde ψ es un qubit y U es una compuerta de un qubit.

Proposición 2.2.8. *Si consideramos un sistema de n qubits, con estado inicial $|\psi_0\rangle = |0\rangle^{\otimes n}$, y aplicamos la compuerta Hadamard en cada qubit obtenemos el estado*

$$|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle, \tag{2.2.29}$$

el cual es la superposición de todas las palabras binarias de n bits.

Demostración.

$$\begin{aligned}
|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} &= H|0\rangle \otimes \cdots \otimes H|0\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \frac{1}{2^{n/2}} \left(\sum_{x_{n-1}=0}^{1} |x_{n-1}\rangle \right) \otimes \cdots \otimes \left(\sum_{x_1=0}^{1} |x_1\rangle \right) \otimes \left(\sum_{x_0=0}^{1} |x_0\rangle \right) \\
&= \frac{1}{2^{n/2}} \sum_{x_{n-1}=0}^{1} \cdots \sum_{x_1=0}^{1} \sum_{x_0=0}^{1} |x_{n-1}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle \\
&= \frac{1}{2^{n/2}} \sum_{x_{n-1},\cdots,x_0=\{0,1\}} |x_{n-1} \cdots x_1 x_0\rangle \qquad (2.2.30) \\
&= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \,. \qquad (2.2.31)
\end{aligned}$$

Donde x en (2.2.31) es un número en base decimal entre $0, \ldots, 2^{n-1}$ y su representación binaria esta dada por los bits $x_{n-1} \cdots x_1 x_0$ como se obtiene en (2.2.30). ■

La proposición anterior es un resultado de gran interés[2], porque se obtiene una superposición de 2^n estados utilizando n compuertas al mismo tiempo. De esta manera, una computadora cuántica puede actuar en paralelo sobre todas las posibles combinaciones de n qubits.

Proposición 2.2.9 (Lema 4.3 [3])**.** *Sea $U \in U(2)$ una compuerta unitaria de un solo qubit. Entonces existen operadores unitarios $A, B, C \in SU(2)$ y un factor de fase global $e^{i\alpha}$, tales que $ABC = I$ y $U = e^{i\alpha} AXBXC$.*

Demostración. Por el Teorema 2.2.3, existen α, β, γ y δ tales que $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$. Fijamos $A = R_z(\beta) R_y(\gamma/2)$, $B = R_y(-\gamma/2) R_z(-(\delta+\beta)/2)$ y $C = R_z((\delta-\beta)/2)$. Tenemos que

$$\begin{aligned}
ABC &= R_z(\beta) R_y(\gamma/2) R_y(-\gamma/2) R_z(-(\delta+\beta)/2) R_z((\delta-\beta)/2) \\
&= e^{-i\beta Z/2} e^{-i\gamma Y/4} e^{i\gamma Y/4} e^{i(\delta+\beta)Z/4} e^{-i(\delta-\beta)Z/4} \\
&= e^{-i\beta Z/2} e^{i\beta Z/2} = I;
\end{aligned}$$

ya que $X = X^*$ notamos que

$$XR_z(-\beta)X^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} = R_z(\beta)$$

$$XR_y(-\gamma)X^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos\gamma/2 & \sin\gamma/2 \\ -\sin\gamma/2 & \cos\gamma/2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\gamma/2 & -\sin\gamma/2 \\ \sin\gamma/2 & \cos\gamma/2 \end{pmatrix} = R_y(\gamma);$$

ya que $X^2 = I$, obtenemos lo siguiente

$$\begin{aligned}
AXBXC &= R_z(\beta) R_y(\gamma/2) X R_y(-\gamma/2) X X R_z(-(\delta+\beta)/2) X R_z((\delta-\beta)/2) \\
&= R_z(\beta) R_y(\gamma/2) R_y(\gamma/2) R_z((\delta+\beta)/2) R_z((\delta-\beta)/2) \\
&= R_z(\beta) R_y(\gamma) R_z(\delta),
\end{aligned}$$

lo cual completa la prueba. ■

[2]En algoritmos cuánticos, como el algoritmo de Deutsch y de Grover, el cual plantea el problema de encontrar el valor de una función binaria de n bits [8], [21]. Un sistema clásico tendría que realizar 2^n mediciones para determinar el valor de la función; sin embargo, a nivel cuántico habría que realizar después de las n compuertas Hadamard una operación que se evaluaría en las 2^n posibles combinaciones.

A partir de esta proposición consideramos la implementación de una compuerta arbitraria $U \in U(2)$, utilizando la descomposición en factores que corresponden a una fase y compuertas de un qubit; tal descomposición la observaremos en un diagrama circuital cuántico, en el cual se interconectan las compuertas por hilos o *canales cuánticos* que no necesariamente corresponden a una conexión física a través de un cable, sino que pueden corresponder a la evolución en el tiempo o a una partícula como un fotón moviéndose de un lugar a otro a través del espacio [21].

2.2.2 Compuertas Universales de un Qubit

Ahora, nos queda por mostrar que las compuertas de un qubit definidas en el Teorema 2.2.3, se pueden obtener de un conjunto finito de elementos de $U(2)$. Consideramos la descomposición de U en una fase $e^{i\varphi} \in U(1)$ y las matrices $A \in SU(2)$. En realidad nos interesa aproximar todo $SU(2)$ dado que la fase global la podemos descartar.

La idea general para proponer un conjunto que aproxime las rotaciones en $SU(2)$ se fundamenta en obtener un ángulo θ mútiplo irracional de π, el cual aproxima con un grado de precisión arbitraria cualquier ángulo α, en el siguiente sentido, $\exists k \in \mathbb{Z}$ tal que $k\theta \approx \alpha \mod 2\pi$, o en otras palabras, la sucesión $k\theta \mod 2\pi$ es densa en el intervalo $[0, 2\pi)$, lo cual implica el siguiente resultado [1].

Teorema 2.2.10. *El conjunto* $\{e^{i\theta n} : n \in \mathbb{Z}\}$ *con* $\theta = \lambda\pi$ *y* $\lambda \in \mathbb{R} \setminus \mathbb{Q}$*, es denso en* $\mathbb{S}^1$*.*

Por lo tanto, se puede aproximar cualquier fase $e^{i\alpha} \approx \left(e^{i\theta}\right)^n \in U(1)$, para algún n.

En general, del Teorema 2.2.3 se sigue que, una rotación arbitraria $A \in SU(2)$, es definida por tres angúlos que determinan la composición de rotaciones sobre dos ejes no pararelos [21]; en particular, como en el Teorema 2.2.3, si elegimos los ejes ortogonales z, y y fijamos un operador $R_z(\theta)$ con θ múltiplo irracional de π, si además contamos con una transformación unitaria H_y tal que, la conjugación $H_y R_z(\theta) H_y^*$ aproxime a una rotación en el eje y por el mismo ángulo θ, entonces podemos aproximar todo $SU(2)$.

Proposición 2.2.11. *El conjunto de rotaciones* $e^{in\theta Z} \in SU(2)$ *con* θ *múltiplo irracional de* π *y* $n \in \mathbb{Z}$*, determina un conjunto denso en el conjunto de rotaciones alrededor del eje* z*, esto es,*

$$\overline{\{e^{in\theta Z} : n \in \mathbb{Z}\}} = \left\{e^{i\alpha Z} : \alpha \in [0, 2\pi)\right\}. \tag{2.2.32}$$

En otras palabras, la proposición anterior afirma lo siguiente.

Corolario 2.2.12. *Sea* θ *múltiplo irracional de* π*, entonces toda rotación en el eje* z *por un ángulo* α *se puede obtener como*

$$(R_z(\theta))^n = R_z(n\theta) \approx R_z(\alpha).$$

para algún $n \in \mathbb{Z}$*.*

Proposición 2.2.13. *Dada* $R_z(\theta)$ *con* θ *múltiplo irracional de* π*, existe un operador unitario* H_y *talque* $H_y R_z(\theta) H_y^* = R_y(\theta)$*.*

Demostración. Definimos $H_y = \frac{Y+Z}{\sqrt{2}}$ operador unitario, observamos que

$$\begin{aligned} H_y R_z(\theta) H_y^* &= \frac{Y+Z}{\sqrt{2}} R_z(\theta) \frac{Y+Z}{\sqrt{2}} \\ &= \left(\frac{Y+Z}{\sqrt{2}}\right) e^{-i\theta Z/2} \left(\frac{Y+Z}{\sqrt{2}}\right) \\ &= \left(\frac{Y+Z}{\sqrt{2}}\right) \left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z\right) \left(\frac{Y+Z}{\sqrt{2}}\right) \\ &= \frac{1}{2}\left(\cos\frac{\theta}{2}(Y^2 + ZY + YZ + Z^2) - i\sin\frac{\theta}{2}(YZY + Z^2Y + YZ^2 + Z^2Z)\right) \\ &= \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = R_y(\theta) \end{aligned}$$

donde $Y^2 = Z^2 = I$, $ZY + YZ = 0$ y $YZY = -Z$; $R_y(\theta)$ es una rotación en el eje y por un ángulo $\theta = \lambda\pi$ con $\lambda \in \mathbb{R} \setminus \mathbb{Q}$. ■

Corolario 2.2.14. *Para cualquier $V = e^{-i\alpha Z/2} e^{-i\beta Y/2} e^{-i\gamma Z/2} \in SU(2)$, donde $\alpha, \beta, \gamma \in [0, 2\pi)$, y dado θ múltiplo irracional de π, existen n, m, k tales que $n\theta \approx \alpha$; $m\theta \approx \beta$; y $k\theta \approx \gamma$ con un grado de precisión arbitraria, tales que*

$$\left(e^{-i\theta Z/2}\right)^n \left(e^{-i\theta Y/2}\right)^m \left(e^{-i\theta Z/2}\right)^k \approx e^{-i\alpha Z/2} e^{-i\beta Y/2} e^{-i\gamma Z/2}.$$

Lema 2.2.15. *Un conjunto universal de compuertas de un qubit es $\{R_z(\theta), H_y\}$.*

En [6] [21] el conjunto universal de compuertas cuánticas de un qubit es $\left\{H = \frac{X+Z}{\sqrt{2}}, T = e^{\pi/8} e^{-i\pi Z/8}\right\}$, el cual permite construir un ángulo irracional como sigue.

Proposición 2.2.16. *El conjunto $\left\{H = \frac{X+Z}{\sqrt{2}}, T = e^{\pi/8} e^{-i\pi Z/8}\right\}$ determina un conjunto universal de compuertas cuánticas de un qubit, tal que la composición de elementos del conjunto produce un ángulo irracional.*

Demostración. Observamos que, salvo fase el producto HTH es

$$\begin{aligned} HTH &= \left(\frac{X+Z}{\sqrt{2}}\right) e^{-i\pi Z/8} \left(\frac{X+Z}{\sqrt{2}}\right) \\ &= \left(\frac{X+Z}{\sqrt{2}}\right) \left(\cos\frac{\pi}{8} - i\sin\frac{\pi}{8} Z\right) \left(\frac{X+Z}{\sqrt{2}}\right) \\ &= \frac{1}{2}\cos\frac{\pi}{8}(X+Z)^2 - \frac{i}{2}\sin\frac{\pi}{8}(X+Z)Z(X+Z) \\ &= \cos\frac{\pi}{8} I - i\sin\frac{\pi}{8} X \\ &= e^{-i\pi X/8}. \end{aligned}$$

Por lo tanto, se puede obtener la compuerta

$$THTH = e^{-i\pi Z/8} e^{-i\pi X/8} = \cos^2\frac{\pi}{8} I - i\sin\frac{\pi}{8}\left(\cos\frac{\pi}{8} X + \sin\frac{\pi}{8} Y + \cos\frac{\pi}{8} Z\right). \tag{2.2.33}$$

La expresión (2.2.33) en la notación (2.2.23), tiene dos componentes, el ángulo de rotación, el cual se despeja del primer término $\cos\pi\lambda = \cos^2\pi/8$, de donde se obtiene que λ es irracional, como se demuestra en [6]; y del segundo término, el vector $(\cos\pi/8, \sin\pi/8, \cos\pi/8)$ determina el eje de

rotación $\hat{n}$, por tanto, se escribe $THTH = e^{-i\pi\lambda\hat{n}\cdot\sigma}$[3]; luego, se define una segunda compuerta, dada por la conjugación $H(THTH)H = e^{-i\pi\lambda\hat{m}\cdot\sigma}$, la cual es una rotación por el mismo ángulo alrededor del eje $\hat{m}$, no paralelo a $\hat{n}$. Por lo tanto, se aproxima cualquier $U \in SU(2)$ de la siguiente forma

$$U \approx (R_{\hat{n}}(\theta))^k (R_{\hat{m}}(\theta))^l (R_{\hat{n}}(\theta))^p \approx R_{\hat{n}}(\alpha) R_{\hat{m}}(\beta) R_{\hat{n}}(\gamma),$$

para algunos $k, l, p \in \mathbb{Z}$ donde $\theta = \lambda\pi$. ■

La diferencia de considerar el conjunto $\{R_z(\theta), H_y\}$ es que describe de una forma más sencilla $SU(2)$ porque partimos de los ejes ortogonales z, y y no se requiere normalizar estos vectores.

2.3 Múltiples Qubits

En la anterior sección se estudiaron las compuertas cuánticas de un qubit y su representación más general (2.2.3); ahora consideramos múltiples qubits. De nuevo, en una analogía con la computación clásica, las principales compuertas lógicas de dos bits son: *AND, OR, XOR, NAND* y *NOR*. Pero una característica fundamental para la implementación física de los circuitos diseñados con estas compuertas es que todas ellas pueden ser obtenidas como configuraciones de únicamente la compuerta NAND, esto la define como una compuerta universal en la computación clásica, es decir, una compuerta lógica universal es aquella que permite obtener, en distintas configuraciones de ella misma, todos los valores de las funciones lógicas.

Definición 2.3.1. Un estado de dos qubits es descrito por un vector $|\Phi\rangle \in \mathbb{C}^4$ de norma 1, donde el espacio de Hilbert $\mathbb{C}^4 \cong \mathbb{C}^2 \otimes \mathbb{C}^2 = gen\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$.

Recordamos que $\mathbb{C}^2$ es el espacio de Hilbert de una partícula, y $\mathbb{C}^{2^n} \cong \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ es el espacio de n partículas.

Los elementos de la base que generan $\mathbb{C}^4$ son denotados de la siguiente forma:

$$\begin{aligned} |0\rangle \otimes |0\rangle &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \doteq |00\rangle, \quad |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \doteq |01\rangle, \\ |1\rangle \otimes |0\rangle &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \doteq |10\rangle, \quad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \doteq |11\rangle. \end{aligned} \tag{2.3.1}$$

El producto tensorial $|i\rangle \otimes |j\rangle$ con $i, j \in \{0, 1\}$ nos permite reconocer el estado de cada qubit de manera individual cuando las partículas no se entrelazan, es decir, una de las partículas está en

[3]En este caso,

$$THTH = \cos^2\frac{\pi}{8} I - i \sin\frac{\pi}{8}\sqrt{1+\cos^2\frac{\pi}{8}} \left(\frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}} X + \frac{\sin\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}} Y + \frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}} Z \right)$$

$$\cos(\pi\theta) = \cos^2\frac{\pi}{8} \quad \sin(\pi\theta) = \sin\frac{\pi}{8}\sqrt{1+\cos^2\frac{\pi}{8}}$$

$$\hat{n} = \frac{1}{\sqrt{1+\cos^2\frac{\pi}{8}}} (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$$

b_1	b_2	$\boldsymbol{r}$
0	0	0
0	1	1
1	0	1
1	1	0

Tabla 2.1: Tabla de verdad de la compuerta lógica XOR clásica.

el estado $|i\rangle$ y la otra partícula en el estado $|j\rangle$. Un estado $|\Phi\rangle \in \mathbb{C}^4$ se escribe en la base de la siguiente forma:

$$|\Phi\rangle = \alpha_{00}\,|0\rangle \otimes |0\rangle + \alpha_{01}\,|0\rangle \otimes |1\rangle + \alpha_{10}\,|1\rangle \otimes |0\rangle + \alpha_{11}\,|1\rangle \otimes |1\rangle\,, \tag{2.3.2}$$

donde $\alpha_{00}, \alpha_{01}, \alpha_{10}$ y $\alpha_{11} \in \mathbb{C}$, tales que $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$; de forma abreviada en adelante escribiremos:

$$|\Phi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle = \sum_{x\in\{0,1\}^2} \alpha_x\,|x\rangle\,, \tag{2.3.3}$$

donde $x \in \{0,1\}^2 = \{00, 01, 10, 11\}$.

2.3.1 Compuertas Reversibles

Estudiamos el proceso de sumar dos bits módulo 2, la compuerta lógica que la implementa es llamada XOR (*eXclusive OR*); la suma módulo 2 clásica se observa en la tabla de verdad 2.1, donde b_1 y b_2 son los bits clásicos a sumar y r es el bit resultado. Definimos la función r como la operación XOR sobre los bits b_1, b_2, de la siguiente forma:

$$\begin{aligned} r : \{0,1\} \times \{0,1\} &\to \{0,1\} \\ (b_1, b_2) &\mapsto b_1 \oplus b_2. \end{aligned}$$

¿Conociendo $r \in \{0,1\}$, podemos obtener la pareja $(b_1, b_2) \in \{0,1\}$ de la cual es resultado?, en otras palabras, ¿existe $r^{-1} : \{0,1\} \to \{0,1\} \times \{0,1\}$? Dado que r no es biyección, no es posible definir r^{-1}. Por otro lado, consideramos la siguiente función:

$$\begin{aligned} R : \{0,1\} \times \{0,1\} &\to \{0,1\} \times \{0,1\} \\ (b_1, b_2) &\mapsto (b_1, b_1 \oplus b_2), \end{aligned}$$

los valores de R se observan en la tabla 2.2. R es biyección y por tanto, nos permite introducir el concepto de reversibilidad: decimos que R es reversible, es decir, podemos obtener $R^{-1}(b_1, r) = (b_1, b_2)$; y en el caso de r afirmar que es una función irreversible. La computación clásica, en general, es irreversible, sin embargo, se pueden modificar los circuitos de tal forma que se vuelva reversible.

- La computación clásica reversible es determinada por aplicaciones biyectivas $R : 2^n \to 2^n$ invertibles.
- Computación cuántica: Consideremos un qubit como el espín de un electrón en la base $\{|\uparrow\rangle\,, |\downarrow\rangle\}$ y definamos dos qubits

$$b_1, b_2 \in gen\{|\uparrow\rangle\,, |\downarrow\rangle\} \cong \mathbb{C}^2 \tag{2.3.4}$$

Entradas		Salidas	
b_1	b_2	$\boldsymbol{b_1}$	$\boldsymbol{r}$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Tabla 2.2: Valores de la función R

El estado inicial de los dos qubits se denota como $S_{inicial} \in gen\{|\uparrow\rangle, |\downarrow\rangle\} \otimes gen\{|\uparrow\rangle, |\downarrow\rangle\}$ y el estado final $S_{final} \in gen\{|\uparrow\rangle, |\downarrow\rangle\} \otimes gen\{|\uparrow\rangle, |\downarrow\rangle\}$. Definimos el operador U_R como sigue

$$U_R : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$$
$$U_R(S_{inicial}) = S_{final}.$$

Luego, $U_R \in \mathcal{M}(4, \mathbb{C})$, tal que $U_R^* U_R = Id = U_R U_R^*$, es decir, es una matriz unitaria.

Dado que la dinámica del sistema cuántico es definida por operadores unitarios, las puertas cuánticas siempre son reversibles porque son una biyección en el espacio de estados. Para n qubits la matriz $U \in \mathcal{M}(2^n, \mathbb{C})$, siempre es una aplicación unitaria

$$U : \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n \text{ veces}} \to \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n \text{ veces}}. \tag{2.3.5}$$

2.3.2 Compuertas Cuánticas de Dos Qubits

Definición 2.3.2. Las compuertas cuánticas de dos qubits son operadores unitarios $U \in \mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ y son representadas por matrices en $\mathcal{M}(2^2, \mathbb{C})$.

Consideraremos las compuertas principales de dos qubits, que permiten introducir operaciones controladas sobre un qubit objetivo.

Compuerta CNOT

Definición 2.3.3. El operador unitario U que actúa sobre los estados de la base de $\mathbb{C}^2 \otimes \mathbb{C}^2$ de la siguiente forma

$$U|00\rangle = U(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle = |00\rangle$$
$$U|01\rangle = U(|0\rangle \otimes |1\rangle) = |0\rangle \otimes |1\rangle = |01\rangle$$
$$U|10\rangle = U(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle = |11\rangle$$
$$U|11\rangle = U(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |0\rangle = |10\rangle,$$

define la operación o compuerta Control NOT o abreviada $CNOT$; de las expresiones anteriores se obtiene la representación matricial de CNOT en la base (2.3.1) como sigue

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}. \tag{2.3.6}$$

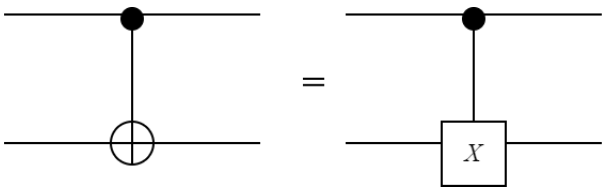

Figura 2.2: Símbolo circuital de CNOT (*Izquierda*). Compuerta X controlada (*Derecha*)

Consideramos las entradas y salidas en la tabla 2.2 como qubits, esto es, $b_i \in \{|0\rangle, |1\rangle\}$ con $i = 1, 2$ y $b_1 \oplus b_2 \in \{|0\rangle, |1\rangle\}$. Observamos que $b_1 \otimes b_2$ y $b_1 \otimes (b_1 \oplus b_2) \in \mathbb{C}^2 \otimes \mathbb{C}^2$. La compuerta CNOT actúa como R sobre la base computacional, es decir, al aplicar CNOT se obtienen las salidas de la tabla 2.2 como qubits,

De (2.3.6) observamos que la acción de la compuerta CNOT está definida por el primer qubit, llamado el qubit de control, esto es, si $b_1 = |0\rangle$, b_2 queda idéntico; y si $b_1 = |1\rangle$, entonces b_2 cambia de estado, en otros términos, CNOT intercambia los dos últimos vectores de la base y b_2 es llamado el qubit objetivo. El símbolo de CNOT se presenta en la figura 2.2. También podemos escribir CNOT de la siguiente forma:

$$|b_1, b_2\rangle \mapsto |b_1, b_1 \oplus b_2\rangle, \tag{2.3.7}$$

donde el qubit objetivo b_2 es invertido o se le aplica la compuerta X cuando b_1 es el estado $|1\rangle$.

La figura 2.2 del lado izquierdo presenta el símbolo estándar de la compuerta $CNOT$ y el lado derecho la operación explícita que realiza, dado que es el primer circuito de más de un qubit que presentamos, se describen en detalle sus elementos a continuación. El diagrama se lee de izquierda a derecha, y por lo tanto, las entradas se ubican en los dos extremos del lado izquierdo, y cada línea es un qubit. Seguidamente, se muestra la operación a ser aplicada al sistema de dos qubits, en este caso, el círculo lleno de color negro sobre la primera línea y el cuadrado con la letra X que se refiere a la compuerta X de un qubit de la Definición 2.2.2 sobre la segunda línea. Sin embargo, el punto negro sobre el primer qubit y la compuerta X sobre el segundo qubit no son independientes, están unidas por una línea. Después de la operación, tenemos dos líneas que indican los dos qubits de salida. En este punto hay que destacar que a diferencia de un circuito clásico, el resultado es decir, el estado del sistema a la derecha puede corresponder a un estado que es superposición y, por tanto, aunque se señala como dos líneas independientes no son necesariamente qubits independientes dado que pueden estar entrelazados. Dibujar el círculo negro indica que la línea sobre la cual este se encuentra es un qubit de control y no hay ninguna operación sobre su estado, pero su estado si activa o no la operación sobre el segundo qubit.

Proposición 2.3.4. *La compuerta $CNOT$ no se puede escribir como el producto tensorial de dos compuertas unitarias, es decir, no hay compuertas $U, V \in U(2)$ tales que $CNOT = U \otimes V$*

Demostración. Un circuito de dos qubits con una compuerta $W = U \otimes V$, se observa en la figura 2.3, y se obtiene como

$$U \otimes V = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \otimes \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} = \begin{pmatrix} u_{11}\begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} & u_{12}\begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \\ u_{21}\begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} & u_{22}\begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \end{pmatrix} \tag{2.3.8}$$

en la base (2.3.1). Observamos que de la representación de CNOT en la misma base dada en (2.3.6) se puede concluir directamente que $CNOT \neq U \otimes V$. ■

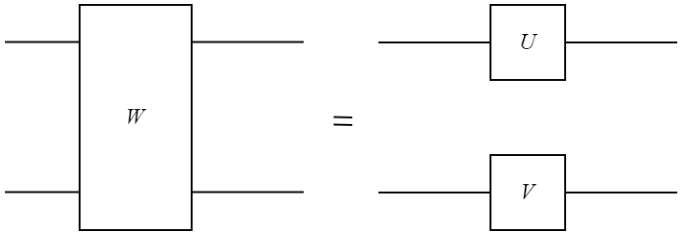

Figura 2.3: Circuito de dos qubits con compuertas separables.

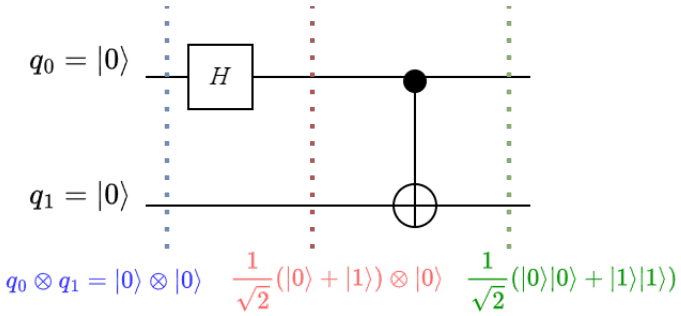

Figura 2.4: Circuito de dos qubits y las compuertas Hadamard y CNOT.

De la proposición anterior podemos decir que $CNOT$ es una compuerta entrelazada [23].

Ejemplo 2.3.1. Consideremos el circuito de la figura 2.4 y los qubits q_0, q_1 en las entradas del circuito con valor inicial $q_0 \otimes q_1 = |0\rangle \otimes |0\rangle$. El estado que se obtiene del circuito es

$$\begin{aligned} CNOT(H|0\rangle \otimes |0\rangle) &= CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) \\ &= \frac{1}{\sqrt{2}}(CNOT(|0\rangle \otimes |0\rangle) + CNOT(|1\rangle \otimes |0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \end{aligned} \tag{2.3.9}$$

el cual es un estado entrelazado de los estados de Bell. De forma análoga, modificando los estados iniciales obtenemos los demás estados de Bell, como sigue:

$$CNOT(H|0\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{2.3.10}$$

$$CNOT(H|1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{2.3.11}$$

$$CNOT(H|1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.3.12}$$

Compuertas de un qubit activadas por un qubit de control

Observamos que CNOT activa la compuerta X sobre el qubit objetivo, si el qubit de control es el estado $|1\rangle$. Pero podemos controlar cualquier compuerta de un qubit, a saber, el operador $U \in U(2)$,

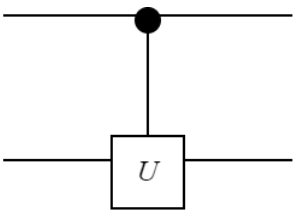

Figura 2.5: Compuerta U controlada.

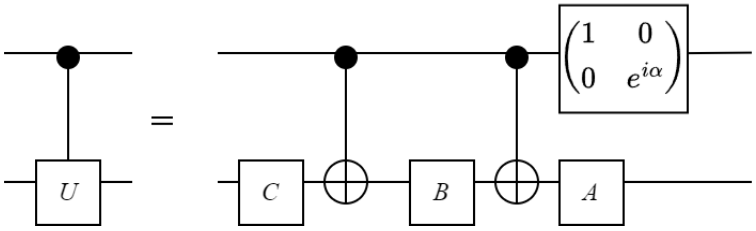

Figura 2.6: Descomposición de la compuerta U controlada en un circuito de dos qubits.

representado por el circuito de la figura 2.5.

Lema 2.3.5. *Dado el operador unitario $U \in U(2)$. Entonces el diagrama circuital de la figura 2.6 implementa la operación de la compuerta U controlada por un qubit.*

Demostración. Por la Proposición 2.2.9, existen compuertas A, B, C, y una fase α tales que $U = e^{i\alpha}AXBXC$ y $ABC = I$. Se obtiene directamente el diagrama circuital de la descomposición de U, como se observa en la figura 2.6. El cual implementa las siguientes operaciones, donde el primer factor es el qubit de control

$$|0\rangle \otimes |x\rangle \mapsto |0\rangle \otimes ABC\,|x\rangle = |0\rangle \otimes |x\rangle$$
$$|1\rangle \otimes |x\rangle \mapsto |1\rangle \otimes e^{i\alpha}AXBXC\,|x\rangle = |1\rangle \otimes U\,|x\rangle\,,$$

lo cual es el resultado deseado. ■

Compuerta Control Cero

En general, el qubit de control no debe ser necesariamente el estado $|1\rangle$, definimos la compuerta que es activada por el estado $|0\rangle$.

Definición 2.3.6. La compuerta X activada por el qubit $|0\rangle$, es definida por la matriz unitaria

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

El diagrama circuital que representa las compuertas controladas por el qubit $|0\rangle$ utiliza un círculo vacío en el qubit de control, como en la figura 2.7.

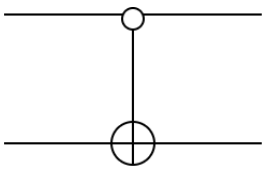

Figura 2.7: Símbolo circuital de la compuerta Control Cero

2.3.3 Compuertas Controladas por Múltiples Qubits

La técnica para establecer un circuito que modela una compuerta cuántica de un qubit U controlada por n qubits, se describe en dos partes; primero, para cualquier compuerta U unitaria, existe su raíz m-ésima V unitaria, es decir, existe V tal que $U = V^m$, por tanto, obtenemos la aplicación de U sobre un estado objetivo por la aplicación de V, m veces. Segundo, construir un circuito que codifique la secuencia de control, de tal forma que la palabra binaria de los bits de control que activan U, sea la única que aplique U al estado objetivo, y cualquier otra combinación de las entradas aplique la identidad. Para ello en computación cuántica como en computación clásica es de gran utilidad el código Gray, dado que permite implementar eficientemente compuertas controladas [3], [19].

Lema 2.3.7. *Para cada $V \in \mathcal{M}(N, \mathbb{C})$ unitaria, $\exists U \in \mathcal{M}(N, \mathbb{C})$ con $UU^* = U^*U = I$ y $\lambda_1, \cdots, \lambda_N \in U(1)$, tal que*

$$U^*VU = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}, \tag{2.3.13}$$

o lo que es equivalente,

$$V = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix} U^*. \tag{2.3.14}$$

Demostración. Dado que V es matriz unitaria, entonces $VV^* = V^*V = I$. Como $\det(V - \lambda I) = 0$ tiene solución en $\mathbb{C}$, entonces existe un estado $e_1 \in \mathbb{C}^N$ tal que $Ve_1 = \lambda_1 e_1$, $\|Ve_1\| = \|\lambda_1 e_1\| = |\lambda_1| = 1$. Además,

$$V^*e_1 = \overline{\lambda}_1 V^*Ve_1 = \overline{\lambda}_1 e_1.$$

Entonces $\mathbb{C}e_1$ es invariante, es decir,

$$V : \mathbb{C}e_1 \to \mathbb{C}e_1, \tag{2.3.15}$$
$$V^* : \mathbb{C}e_1 \to \mathbb{C}e_1. \tag{2.3.16}$$

Consideramos el complemento ortogonal de $\mathbb{C}e_1$

$$\mathcal{H}_{N-1} \doteq (\mathbb{C}e_1)^\perp = \{h \in \mathbb{C}^N :< h, e_1 >= 0\}; \tag{2.3.17}$$

entonces $\forall h \in \mathcal{H}_{N-1}$ tenemos

$$< Vh, e_1 > =< h, V^*e_1 >= \overline{\lambda_1} < h, e_1 >= 0, \tag{2.3.18}$$
$$< V^*h, e_1 > =< h, Ve_1 >= \lambda_1 < h, e_1 >= 0, \tag{2.3.19}$$

por lo tanto, Vh, $V^*h \in \mathcal{H}_{N-1}$, y definimos

$$V_{N-1} \doteq V_N \restriction \mathcal{H}_{N-1} : \mathcal{H}_{N-1} \to \mathcal{H}_{N-1}$$
$$V_{N-1}^* \doteq V_N^* \restriction \mathcal{H}_{N-1} : \mathcal{H}_{N-1} \to \mathcal{H}_{N-1}$$

Por inducción, V es diagonalizable en $\mathbb{C}^N = gen\{e_1, \cdots, e_N\}$ tal que $Ve_k = \lambda_k e_k$, $V^*e_k = \overline{\lambda_k}e_k$, $\lambda_k\overline{\lambda_k} = 1$, $< e_k, e_j >= \delta_{kj}$. En la base $\{e_1, \cdots, e_N\}$ obtenemos

$$V = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}.$$

Sea $U : \mathbb{C}^N \to \mathbb{C}^N$ una matriz unitaria tal que

$$U \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_1, \cdots, U \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = e_N; \tag{2.3.20}$$

tenemos lo siguiente:

$$U^*VU \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \cdots, U^*VU \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \lambda_N \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{2.3.21}$$

En la base canónica,

$$U^*VU = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix},$$

por lo tanto,

$$V = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix} U^*,$$

en la base canónica de $\mathbb{C}^N$. ■

Proposición 2.3.8. *Sea $V \in \mathcal{M}(N, \mathbb{C})$ unitaria y $m \in \mathbb{N}$, entonces V tiene una raíz m-ésima.*

Demostración. Elegimos $\rho_1, \cdots, \rho_N \in U(1)$ tales que:

$$\rho_1^m = \lambda_1, \cdots, \rho_N^m = \lambda_N.$$

Sea U la matriz unitaria del Lema 2.3.7. Definimos

$$W \doteq U \begin{pmatrix} \rho_1 & & \\ & \ddots & \\ & & \rho_N \end{pmatrix} U^*.$$

Tenemos lo siguiente:

$$\begin{aligned} W^m =& U \begin{pmatrix} \rho_1 & & \\ & \ddots & \\ & & \rho_N \end{pmatrix} U^*U \begin{pmatrix} \rho_1 & & \\ & \ddots & \\ & & \rho_N \end{pmatrix} U^*U \cdots U^*U \begin{pmatrix} \rho_1 & & \\ & \ddots & \\ & & \rho_N \end{pmatrix} U^* \\ =& U \begin{pmatrix} \rho_1^m & & \\ & \ddots & \\ & & \rho_N^m \end{pmatrix} U^* = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix} U^* = V. \end{aligned} \tag{2.3.22}$$

Por lo tanto, W es una raíz m-ésima de V. ■

Código Gray

Un código Gray conecta dos números binarios i, j, mediante una secuencia de palabras binarias que se distinguen en dos términos cualesquiera adyacentes solo por un bit, tal secuencia no es única.

Definición 2.3.9. Un código Gray de n bits denotado $\mathcal{G}_n$, es un conjunto de m palabras binarias, el cual se escribe escribe de la siguiente forma

$$\mathcal{G}_n = (g_1, g_2, \cdots, g_m)$$

donde g_i es una palabra binaria de n bits, la cual puede ser expandida como $g_i = g_{i,0}g_{i,1}\ldots g_{i,n-1}$, que se distinguen en dos términos cualesquiera adyacentes solo por un bit, y las m palabras binarias son distintas. Y definimos la reflexión de $\mathcal{G}_n$ como el conjunto

$$\overline{\mathcal{G}_n} = (g_m, \ldots, g_2, g_1).$$

Ejemplo 2.3.2. Un código gray con $g_1 = 01001$ y $g_m = 11010$ se obtiene de la secuencia

$$\mathbf{01001} \to 0100\mathbf{0} \to 010\mathbf{1}0 \to \mathbf{1}1010 \tag{2.3.23}$$

esto es

$$\mathcal{G}_5 = (01001, 01000, 01010, 11010) \tag{2.3.24}$$

de 4 elementos.

A partir de la Definición 2.3.9 del código Gray, se encuentran otras construcciones particulares del código Gray y algunas aún más generales; aquí nos interesa definir una construcción conocida como código Gray reflectivo [19].

Utilizamos en particular un código Gray de k bits, de longitud $m = 2^k$, esto es una 2^k-tupla

$$(g_1, g_2, \ldots, g_{2^k}),$$

de todas las secuencias posibles de k bits ordenadas de tal manera que se distinguen en sus adyacentes solo por un bit.

Definición 2.3.10 ([19])**.** Para un código Gray $\mathcal{G}_{n-1}$ de $n-1$ bits y $m = 2^{n-1}$ y su reflexión $\overline{\mathcal{G}_{n-1}}$ se construye el código Gray reflectivo de n bits de la siguiente forma

$$\mathcal{R}_n = (\mathcal{G}_{n-1} \cdot 0, \overline{\mathcal{G}_{n-1}} \cdot 1),$$

donde, $\cdot$ indica concatenación.

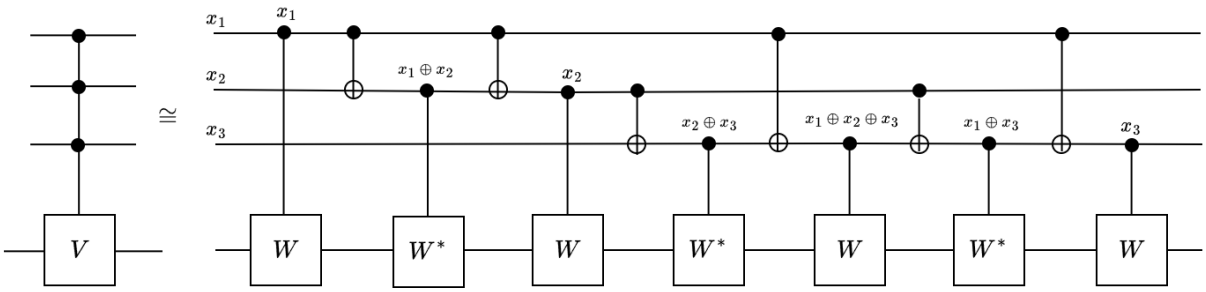

Figura 2.8: Compuerta de un qubit V controlada de 3 qubits (*Izquierda*). Diagrama circuital del código Gray reflectivo(*Derecha*).

La Definición 2.3.10 nos permitirá diseñar un diagrama circuital de un sistema de n qubits de control y un qubit objetivo, que implemente la aplicación de la compuerta V sobre el qubit objetivo cuando todos los qubits de control estén en el estado $|1\rangle$ y en caso contrario, para cualquier otra combinación de los estados de control se aplique la compuerta I, que corresponde a la identidad.

Ejemplo 2.3.3. Consideramos la puerta controlada por 3 qubits V descrita por la figura 2.8 del lado izquierdo y un qubit objetivo que es el qubit al cual se aplica V, el objetivo es obtener el diagrama circuital del lado derecho de V utilizando la Proposición 2.3.8, el Lema 2.3.5, y un código Gray reflectivo que permita la activación de la compuerta V sobre el qubit objetivo cuando los tres qubits de control sean el estado $|111\rangle$ y en otro caso, se aplique la identidad.

Fijamos W unitaria tal que $V = W^4$. Y definimos el código Gray reflectivo de 3 bits para el código Gray de 2 bits $\mathcal{G}_2 = (00, 10, 11, 01)$ siguiente

$$\mathcal{R}_3 = (000, 100, 110, 010, 011, 111, 101, 001). \tag{2.3.25}$$

En el diagrama a la derecha de la figura 2.8 nombramos a los bits de control x_1, x_2, x_3 los cuales corresponden a los tres bits del código Gray reflectivo (2.3.25), asignados de la siguiente forma

$$\underbrace{000}_{x_1x_2x_3}\ ,\ \underbrace{100}_{x_1x_2x_3}\ ,\cdots,\ \underbrace{001}_{x_1x_2x_3}\ .$$

El diagrama circuital que va a implementar la compuerta controlada por 3 qubits V se obtiene como la descomposición en compuertas controladas por un qubit, a saber W o W^*, de tal forma que se implementaría como en el Lema 2.3.5 para cada compuerta controlada por un qubit. El código $\mathcal{R}_3$ lo que indica es, cuáles son los bits[4] que, combinándolos con la suma módulo 2 determina el qubit que controla la compuerta W o W^*. Por ejemplo, partiendo[5] de 100, significa que el qubit x_1 determina la aplicación de W, esto es, si es $x_1 = 1$ se aplica la compuerta W, en caso contrario la identidad como en el Lema 2.3.5. La siguiente palabra binaria del código 110 significa que intervienen los bits x_1x_2, y el bit de control es $x_1 \oplus x_2$, de tal forma que si $x_1 \oplus x_2 = 1$ se aplica la compuerta W^*, en caso contrario, la identidad. Se continúa de la siguiente forma: si la palabra binaria del código $\mathcal{R}_3$ tiene una paridad impar de unos, entonces la suma módulo 2 de sus bits controla la aplicación de W, de lo contrario, si la paridad de 1's es par, la suma módulo 2 de sus bits controla la aplicación

[4]Los estados de entrada y en el diagrama circuital siempre son qubits, sin embargo, en vistas que se identifica la base computacional clásica 0,1 con los estados $|0\rangle, |1\rangle$, se utilizara por razones de la escritura y descripción del ejemplo bits y qubits indistintamente, y cuando se quiera enfatizar se nombrarán los estados como qubits.

[5]Dado que la primera palabra binaria del código $\mathcal{R}_3$ es 000 no hay ningún qubit que ocurra, por tanto, la omitimos.

de W^*. Lo dicho anteriormente se resume en el siguiente esquema [3]:

$$\begin{aligned}
&(100) \quad W \text{ sii } x_1 = 1\\
&(110) \quad W^* \text{ sii } x_1 \oplus x_2 = 1\\
&(010) \quad W \text{ sii } x_2 = 1\\
&(011) \quad W^* \text{ sii } x_2 \oplus x_3 = 1\\
&(111) \quad W \text{ sii } x_1 \oplus x_2 \oplus x_3 = 1\\
&(101) \quad W^* \text{ sii } x_1 \oplus x_3 = 1\\
&(001) \quad W \text{ sii } x_3 = 1
\end{aligned}$$

El qubit $x_1 \oplus x_2$ se obtiene por la aplicación de una compuerta $CNOT$ con qubit de control x_1 y qubit objetivo x_2, tal como en la Definición 2.3.3, y así para las otras operaciones entre los qubits de control. Luego, el diagrama del lado derecho en la figura 2.8 es una descomposición circuital en compuertas controladas por un qubit W y W^*, que implementa la operación deseada. Otra forma de verificar el diagrama circuital que se encuentra establecida en la literatura de la teoria de la computación cuántica [3], es considerar la siguiente expresión: si tomamos por un lado la suma aritmética de los términos al lado derecho del esquema anterior, tal que los terminos que controlan W son positivos y los términos que controlan W^* son negativos, se obtiene que

$$x_1 + x_2 + x_3 + (x_1 \oplus x_2 \oplus x_3) - (x_1 \oplus x_2) - (x_1 \oplus x_3) - (x_2 \oplus x_3) = 4(x_1 \wedge x_2 \wedge x_3) \tag{2.3.26}$$

donde $\wedge$ indica la conjunción lógica, esto es, si $x_1x_2x_3 = 111$ entonces $x_1 \wedge x_2 \wedge x_3 = 1$, de lo contrario $x_1 \wedge x_2 \wedge x_3 = 0$. Por lo tanto, si se cumplen las condiciones de aplicación de W sera exactamente el lado izquierdo igual a 4, lo que significa 4 veces se ha aplicado W o $W^4 = V$, si no se cumplen las condiciones el resultado del lado derecho siempre será cero, lo cual significa que se ha aplicado la identidad; lo cual coincide con multiplicar 4 por el valor binario de la conjunción lógica de x_1, x_2, x_3.

En el caso general, se siguen los mismos pasos del ejemplo anterior.

Proposición 2.3.11. *Una compuerta cualquiera V de un qubit controlada por n qubits, tiene una descomposición en compuertas unitarias de un qubit W y W^*, donde $V = W^{2^{n-1}}$ y compuertas CNOT, definida por un código Gray reflectivo de n bits $\mathcal{R}_n$, del cual se obtiene la siguiente expresión [3],*

$$\begin{aligned}
&\sum_{k_1} x_{k_1} - \sum_{k_1<k_2} x_{k_1} \oplus x_{k_2} + \sum_{k_1<k_2<k_3} x_{k_1} \oplus x_{k_2} \oplus x_{k_3} - \cdots + (-1)^{n-1}(x_1 \oplus x_2 \oplus \cdots \oplus x_n)\\
&\qquad = 2^{n-1} \cdot (x_1 \wedge x_2 \wedge \cdots \wedge x_n)
\end{aligned} \tag{2.3.27}$$

donde, $k_i \in \{1, \ldots, n\}$, que aplica la compuerta W 2^{n-1} veces cuando los qubits de control son todos 1's y de lo contrario aplica la identidad.

2.4 Compuertas Universales

De forma análoga a un sistema de un qubit, tenemos infinitas compuertas para un sistema cuántico de n qubits, por lo tanto, queremos demostrar que existe un conjunto finito de compuertas que aproxime cualquier operación deseada con un grado de precisión arbitrario. Para un sistema de n

qubits el espacio de estados es $\mathcal{H}_n = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, elegimos la base computacional que denotamos de la siguiente forma:

$$|0\rangle \doteq e_0 \doteq |0\ldots0\rangle = \begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix}, \quad |1\rangle \doteq e_1 \doteq |0\ldots10\rangle = \begin{pmatrix}0\\1\\\vdots\\0\\0\end{pmatrix}, \ldots, |2^n-1\rangle \doteq e_{2^n-1} \doteq |1\ldots11\rangle = \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}. \tag{2.4.1}$$

De manera compacta

$$|j\rangle \doteq e_j \doteq |j_{n-1}\cdots j_1 j_0\rangle\,,$$

donde, el indice $j \in \{0,1,\ldots,2^n-1\}$, y en términos de su expansión binaria es $j = \sum_{k=0}^{n-1} j_k 2^k$ con $j_k \in \{0,1\}$ y $k = 0,\ldots n-1$.

El objetivo de esta sección es mostrar que cualquier operación unitaria para cualquier número de qubits puede ser aproximada con arbitraria precisión por las compuertas universales de un qubit del Lema 2.2.15 y compuertas CNOT.

Proposición 2.4.1. *La matriz asociada a un operador unitario arbitrario $U \in \mathcal{B}(\mathcal{H}_n)$ de dimensión 2^n respecto de la base $\{e_j\}_{j=0}^{2^n-1}$ se obtiene exactamente como un producto de matrices unitarias E_{ij}, tales que cada una, actúa única y no trivialmente sobre el subespacio generado por dos estados de la base, e_i, e_j, siempre que $i \neq j$.*

Demostración. Dada $A \in \mathcal{M}(n,\mathbb{R})$ y utilizando el algoritmo de eliminación gaussiana para la triangulación de matrices [27], obtenemos la triangulación de A por la aplicación de matrices elementales Q_{ij}, donde los subíndices indican que sustrae de la fila i un múltiplo de la fila j y lo asigna a la fila i, y además produce un cero en la entrada (i,j), sobre la matriz a la cual se aplica; por lo tanto, se obtiene que $Q_{i_m j_m}\ldots Q_{i_1 j_1} A$ es una matriz triangular superior, donde $m \in \mathbb{N}$. Para $U \in \mathcal{M}(n,\mathbb{C})$ unitaria, se utiliza una descomposición similar, donde cada paso del algoritmo determina una matriz $Q_{ij}(\alpha,\beta)$ que representa la operación de sustraer de $\frac{\beta}{\sqrt{|\alpha|^2+|\beta|^2}}$ por la fila i de $\frac{\alpha}{\sqrt{|\alpha|^2+|\beta|^2}}$ por la fija j y lo asigna a la fila j, y eso produce un 1 en la entrada (i,i) y un cero en la entrada (j,i). Puesto que es unitaria, se obtiene al final una matriz diagonal D. Dado que cada matriz $Q_{ij}(\alpha,\beta)$ es unitaria, su producto es unitario, y definimos $E_{ij} = Q_{ij}^* = Q_{ij}^{-1}$, por tanto podemos escribir las descomposición de U en matrices unitarias como sigue:

$$U = E_{i_1,j_1}(\alpha_1,\beta_1)\cdots E_{i_m,j_m}(\alpha_m,\beta_m)D, \tag{2.4.2}$$

donde

$$E_{i_k,j_k}(\alpha_k,\beta_k) = \frac{1}{\sqrt{|\alpha_k|^2+|\beta_k|^2}} \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & \alpha_k & \cdots & -\overline{\beta}_k & \cdots & 0\\ \vdots & \vdots & \cdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & \beta_k & \cdots & \overline{\alpha_k} & \cdots & 0\\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}, \tag{2.4.3}$$

para cada $k \in \{1, \cdots, m\}$. Por tanto, E_{ij} actúa sobre el subespacio $\mathbb{C}^2 \cong gen\{e_i, e_j\}$ con $i, j \in \{1, ..., N\}$, se le conocen como matrices unitarias de dos niveles. Observamos la acción de E_{ij} sobre los estados de la base:

$$E_{ij}(\alpha, \beta)e_i = \frac{1}{\sqrt{|\alpha_k|^2+|\beta_k|^2}}(\alpha e_i + \beta e_j); \quad E_{ij}(\alpha, \beta)e_j = \frac{1}{\sqrt{|\alpha_k|^2+|\beta_k|^2}}(-\overline{\beta} e_i + \overline{\alpha} e_j); \tag{2.4.4}$$

y para $k \neq i, j$, se tiene que $E_{ij}(\alpha, \beta)e_k = e_k$. ■

Ejemplo 2.4.1. Para ilustrar, consideramos dos electrones y su espín, una compuerta para este sistema es el $SWAP \in \mathcal{M}(4, \mathbb{C})$ que intercambia las direcciones del espín, como sigue: si se encuentran los dos espínes en direcciones iguales, no cambia nada; si se encuentran en direcciones opuestas las intercambia, es decir,

$$|01\rangle \mapsto |10\rangle \ ; \ |10\rangle \mapsto |01\rangle$$

lo cual se traduce en la matriz $E_{23}(0, 1)$, definida de la siguiente forma

$$SWAP \doteq E_{2,3}(0, 1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{1} & 0 \\ 0 & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.4.5}$$

Notamos lo siguiente, $E_{2,3}(0, 1)$ no actúa sobre qubits aislados, y en general, $E_{2,3}(\alpha, \beta) \in End(\mathbb{C}^4) = End(\mathbb{C}^2 \otimes \mathbb{C}^2)$, pero $E_{2,3} \neq E_I \otimes E_D$, donde E_I significa una matriz que actúa sobre el qubit de la izquierda y análogamente E_D una matriz que actúa sobre el qubit de la derecha.

Proposición 2.4.2. *Un operador unitario arbitrario, definido por su descomposición en matrices E_{ij}, puede ser expresado exactamente usando compuertas de un solo qubit y compuertas CNOT.*

La proposición anterior determina el conjunto de compuertas universales para un sistema de n qubits. Antes de su demostración delinearemos algunas ideas importantes para su desarrollo.

Como observamos anteriormente, $E_{ij}(\alpha, \beta)$ actúa sobre el subespacio generado por $\{e_i, e_j\}$, queremos transformar la representación de esta matriz, utilizando la matriz 2×2 que actúa no trivialmente, a saber

$$U_{\alpha\beta} = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \in \mathcal{M}(2, \mathbb{C}). \tag{2.4.6}$$

La idea es, dada $E_{ij}(\alpha, \beta)$, codificar e_i, e_j en un estado de un solo qubit, y aplicar la submatriz 2×2 no trivial $U_{\alpha\beta}$ sobre un qubit, de forma que se obtiene el mismo resultado que al aplicar E_{ij}.

En la sección 2.3.3 estudiamos las puertas controladas por n qubits. Y utilizamos el código Gray Reflectivo de n bits para definir un diagrama circuital que evalúa todas las posibles combinaciones de los qubits de control, de modo que, controla la aplicación de la compuerta U de un qubit sobre el qubit objetivo, cuando los estados de control son todos el estado $|1\rangle$. Observamos que, de forma análoga podemos utilizar la Definición 2.3.9 general del código Gray para transformar un estado cualquiera $|e_s\rangle$ en un estado $|e_p\rangle$ donde $s, p \in \{0, 1, \ldots, 2^n - 1\}$. Para desarrollar esta idea, consideramos primero como definir el diagrama circuital para una puerta controlada por una secuencia distinta de 1's.

Lema 2.4.3. *En un sistema de k qubits. Sean e_i y e_j dos estados de la base tal que difieren únicamente por un qubit. Llevar el estado e_i en el estado e_j es aplicar la compuerta X al qubit distinto, controlado por los demás qubits.*

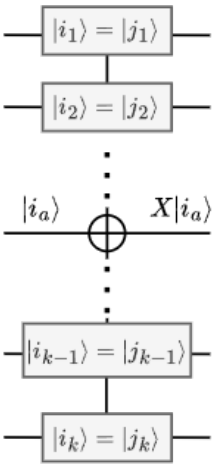

Figura 2.9: Diagrama Circuital general para el cambio de un qubit controlado por las demás entradas.

Demostración. Sea $a \in \{1, \cdots, k\}$ tal que $i_a \neq j_a$ y $i_m = j_m$ para todo $m \neq a$, escribimos

$$e_i = |j_k\rangle \otimes \cdots \otimes |j_{a+1}\rangle \otimes |i_a\rangle \otimes |j_{a-1}\rangle \otimes \cdots \otimes |j_1\rangle\,,$$
$$e_j = |j_k\rangle \otimes \cdots \otimes |j_{a+1}\rangle \otimes |j_a\rangle \otimes |j_{a-1}\rangle \otimes \cdots \otimes |j_1\rangle\,.$$

Proponemos una compuerta controlada por $k-1$ qubits, donde, las entradas $|i_k \cdots i_{a+1}\rangle \otimes |i_{a-1}, \cdots, i_1\rangle$, son los qubits de control, y $|i_a\rangle$ es el qubit objetivo. La compuerta que requerimos actúe sobre el qubit objetivo es X, de tal modo, que si $|i_k \cdots i_{a+1}\rangle \otimes |i_{a-1}, \cdots, i_1\rangle = |j_k \cdots j_{a+1}\rangle \otimes |j_{a-1}, \cdots, j_1\rangle$ el dígito binario $i_a = 0/1$ cambie a $1/0$. ■

El diagrama circuital que describe el lema anterior se observa en la figura 2.9.

Ejemplo 2.4.2. Consideramos $e_i = |0i_2001\rangle$ y $e_j = |0j_2001\rangle$, y aplicamos el Lema 2.4.3. El diagrama circuital se representa en la figura 2.10 donde del lado izquierdo, el diagrama representa la verificación en cada línea del qubit deseado, esto es, que $i_l = j_l$ para todo $l \neq 2$ donde $l = 1, \ldots, 5$, en ese caso, cuando todas las entradas justo antes del círculo negro son $|1\rangle$, entonces se activa la operación X sobre el qubit i_2, de lo contrario, se aplica la identidad al qubit i_2, y cada estado posterior a verificar el control, se devuelve a su estado inicial (por ello la aplicación de X antes y después del control para los estados $|0\rangle$). La figura del lado derecho, simplifica las operaciones de control, resumiendo que, en cada línea donde el círculo es vacío el qubit requerido es el estado $|0\rangle$ y si el círculo es negro entonces el qubit de control es el estado $|1\rangle$, de forma que si la condición en los qubits de entrada se satisface, se activa la compuerta X sobre el qubit i_2, de lo contrario, cualquier otra entrada al circuito, aplica la identidad.

A continuación la demostración de la Proposición 2.4.2.

Demostración. Observamos que por la Proposición 2.4.1 basta considerar puertas que actúan entre

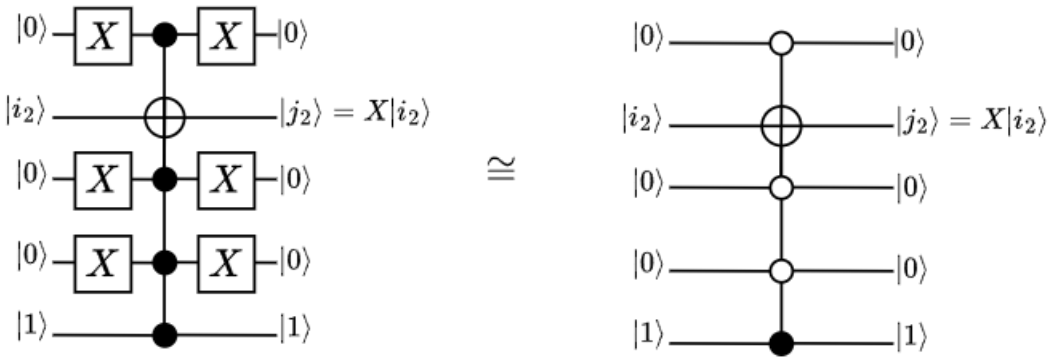

Figura 2.10: Diagrama circuital de la implementación de un paso en un código de Gray, $e_i = |0i_2001\rangle \to e_j = |0j_2001\rangle$.

dos qubits. Por ejemplo

$$E_{i,j}(0,1) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \mathbf{0} & \cdots & \mathbf{1} & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \mathbf{1} & \cdots & \mathbf{0} & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}, \tag{2.4.7}$$

la cual intercambia dos vectores de la base, como en el ejemplo 2.4.1.

Consideramos un sistema de k qubits y una compuerta unitaria $E_{ij}(\alpha,\beta) : \mathbb{C}^{2^k} \to \mathbb{C}^{2^k}$, definida en (2.4.3), la cual actúa no trivialmente sobre e_i y e_j. Queremos implementar E_{ij}. Introducimos el siguiente algoritmo de codificación de Gray para e_i y e_j definidos como sigue. Sea $a \in \{1, \cdots, k\}$ tal que $i_a \neq j_a$ y $i_m = j_m$ para todo $m > a$, es decir,

$$e_i = |j_k\rangle \otimes \cdots \otimes |j_{a+1}\rangle \otimes |i_a\rangle \otimes |i_{a-1}\rangle \otimes \cdots \otimes |i_1\rangle = |j_k \cdots j_{a+1} i_a i_{a-1} \cdots i_1\rangle \tag{2.4.8}$$

y

$$e_j = |j_k\rangle \otimes \cdots \otimes |j_{a+1}\rangle \otimes |j_a\rangle \otimes |j_{a-1}\rangle \otimes \cdots \otimes |j_1\rangle = |j_k \cdots j_{a+1} j_a j_{a-1} \cdots j_1\rangle \tag{2.4.9}$$

Descripción de la aplicación del código Gray

- Si $i_1 = j_1$ no se cambia nada en el primer factor tensorial de la derecha.
- Si $i_1 \neq j_1$ se actúa con CNOT's controlados por las entradas $i_2, \cdots, i_k$ para lograr $i_1 = j_1$; se sigue por inducción, si $i_1 = j_1, \cdots, i_{b-1} = j_{b-1}, i_b \neq j_b$, con $b \leqslant a-1$, aplicamos una transformación construida por CNOTs controlados por $j_1, \cdots, j_{b-1}, i_{b+1}, \cdots, i_k$ para lograr $i_1 = j_1, \cdots, i_b = j_b$.
- Se termina el proceso cuando $i_1 = j_1, \cdots, i_{a-1} = j_{a-1}$, $i_a \neq j_a$, $i_{a+1} = j_{a+1}, \cdots, i_k = j_k$, lo cual se codifica en el operador $V : \mathbb{C}^{2^k} \to \mathbb{C}^{2^k}$ unitario, tal que $Ve_i = |j_k \cdots j_{a+1} i_a j_{a-1} \cdots j_1\rangle$; construido por una composición de CNOTs controlados por las entradas de e_i y e_j.

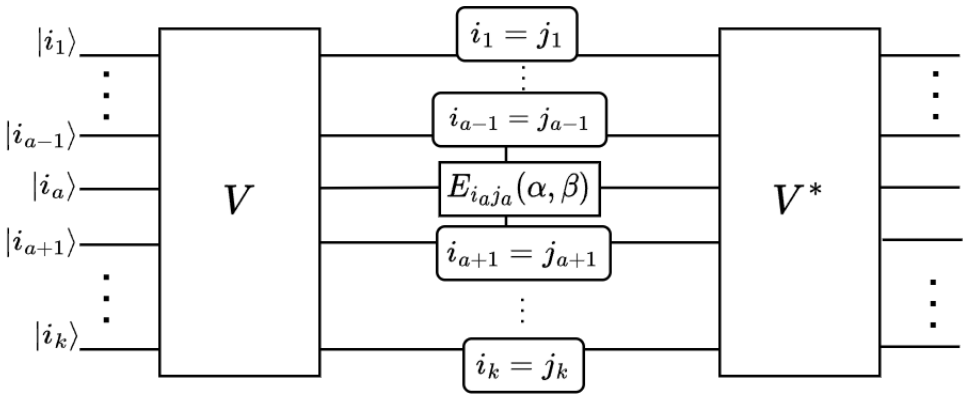

Figura 2.11: Diagrama General de la implementación de la compuerta $E_{ij}(\alpha, \beta)$ unitaria.

- Actuamos con una matriz unitaria en el a-ésimo qubit controlado por $j_1, \cdots, j_{a-1}, j_{a+1}, \cdots, j_k$ $E_{i_a j_a}(\alpha, \beta) : \mathbb{C}^2 \to \mathbb{C}^2$ definida en (2.4.6) con respecto a $V|i_a\rangle$ y $|j_a\rangle$, esto es,

$$E_{i_a j_a}(\alpha, \beta)V|i_a\rangle = \alpha V|i_a\rangle + \beta|j_a\rangle \text{ y } E_{i_a j_a}(\alpha, \beta)|j_a\rangle = \overline{\alpha}|j_a\rangle - \overline{\beta}V|i_a\rangle .$$

- Luego, aplicamos la matriz V^* construida inviertiendo el orden de las CNOTs controlados de V. Obtenemos que,

$$\begin{aligned} V^*E_{i_a j_a}(\alpha, \beta)Ve_i &= V^*E_{i_a j_a}(\alpha, \beta)V|j_k \cdots j_{a+1}, i_a, i_{a-1} \cdots i_1\rangle \\ &= V^*(Id \otimes \cdots \otimes Id \otimes E_{i_a j_a}(\alpha, \beta) \otimes Id \otimes \cdots \otimes Id)V|j_k \cdots j_{a+1}, i_a, i_{a-1} \cdots i_1\rangle \\ &= V^*(\alpha|j_k \cdots j_{a+1} i_a j_{a-1} \cdots j_1\rangle + \beta|j_k \cdots j_{a+1} j_a j_{a-1} \cdots j_1\rangle) \\ &= \alpha V^*|j_k \cdots j_{a+1} i_a j_{a-1} \cdots j_1\rangle + \beta V^*|j_k \cdots j_{a+1} j_a j_{a-1} \cdots j_1\rangle \\ &= \alpha|j_k \cdots j_{a+1}, i_a, i_{a-1} \cdots i_1\rangle + \beta|j_k \cdots j_1\rangle \\ &= \alpha e_i + \beta e_j, \end{aligned}$$

donde $Ve_i = |j_k \cdots j_{a+1} i_a j_{a-1} \cdots j_1\rangle$; $Ve_j = e_j$ y $V^*|j_k \cdots j_{a+1} i_a j_{a-1} \cdots j_1\rangle = e_i$. Luego

$$\begin{aligned} V^*E_{i_a j_a}(\alpha, \beta)Ve_j &= V^*(Id \otimes \cdots \otimes Id \otimes E_{i_a j_a}(\alpha, \beta) \otimes Id \otimes \cdots \otimes Id)|j_k \cdots j_{a+1} j_a j_{a-1} \cdots j_1\rangle \\ &= \overline{\alpha}V^*|j_k \cdots j_1\rangle - \overline{\beta}V^*|j_k \cdots j_{a+1} i_a j_{a-1} \cdots j_1\rangle \\ &= \overline{\alpha}e_j - \overline{\beta}e_i \end{aligned}$$

- Además $V^*E_{i_a j_a}(\alpha, \beta)Ve_l = e_l$, por la acción de la matriz $V^*Ve_l = e_l$ para todo $l \notin \{i, j\}$.

Luego, la operación de E_{ij} se obtiene por su descomposición en las operaciones V y V^* definidas por compuertas CNOT y las comparaciónes de qubits, que se obtienen a su vez por compuertas de un qubit. Lo cual completa la prueba. ■

Observamos un esquema de la implementación de $E_{ij}(\alpha, \beta)$ en la figura 2.11. Se presenta el siguiente ejemplo para ilustrar el algoritmo.

Ejemplo 2.4.3. Describimos el código Gray para la siguiente matriz unitaria en un sistema de 3

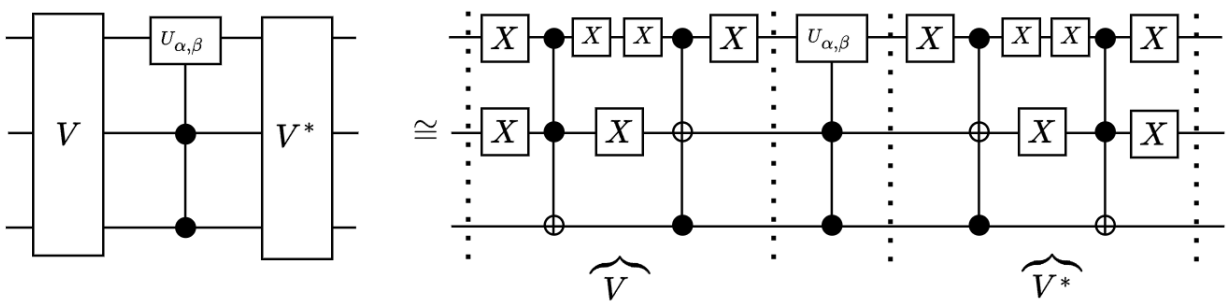

Figura 2.12: Diagrama Circuital de $E_{0,7}(\alpha\beta)$ (*Izquierda*). Descomposición en compuertas X del código Gray (*Derecha*).

qubits:

$$E_{0,7}(\alpha,\beta) = \begin{pmatrix} \alpha & 0 & 0 & 0 & 0 & 0 & 0 & -\overline{\beta} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \beta & 0 & 0 & 0 & 0 & 0 & 0 & \overline{\alpha} \end{pmatrix} \tag{2.4.10}$$

donde, $U_{\alpha\beta}$ es la matriz de dimensión 2×2 formada como en (2.4.6) por los valores de la matriz $E_{0,7}$ que actúan no trivialmente sobre los estados de la base $e_0 = |000\rangle$ y $e_7 = |111\rangle$. Escribimos un código Gray utilizando la Definición 2.3.9 que lleva e_0 en e_7, como sigue

$$\begin{matrix} A & B & C \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{matrix} \tag{2.4.11}$$

el código anterior es definido para e_0 y e_7, es decir, las compuertas CNOT que implementan el código (2.4.11) activan únicamente la puerta $U_{\alpha\beta}$ si la entrada es uno de estos dos estados. El diagrama circuital se presenta en la figura 2.12, donde A es el qubit objetivo y B, C los qubits de control, obtenemos lo siguiente para el estado de entrada $|ABC\rangle = |000\rangle$ y $|ABC\rangle = |111\rangle$:

$$\begin{aligned} |000\rangle \to |001\rangle \to |011\rangle \to (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |11\rangle = \alpha\,|011\rangle + \beta\,|111\rangle \\ \to \alpha\,|001\rangle + \beta\,|111\rangle \to \alpha\,|000\rangle + \beta\,|111\rangle \end{aligned}$$

$$\begin{aligned} |111\rangle \to |111\rangle \to |111\rangle \to (-\overline{\beta}\,|0\rangle + \overline{\alpha}\,|1\rangle) \otimes |11\rangle = -\overline{\beta}\,|011\rangle + \overline{\alpha}\,|111\rangle \\ \to -\overline{\beta}\,|001\rangle + \overline{\alpha}\,|111\rangle \to -\overline{\beta}\,|000\rangle + \overline{\alpha}\,|111\rangle \end{aligned}$$

Por tanto, resumimos:

$$\begin{aligned} E_{0,7}(\alpha,\beta)e_0 &= E_{0,7}(\alpha,\beta)\,|000\rangle = \alpha\,|000\rangle + \beta\,|111\rangle = \alpha e_0 + \beta e_7 \\ E_{0,7}(\alpha,\beta)e_7 &= E_{0,7}(\alpha,\beta)\,|111\rangle = \overline{\alpha}\,|111\rangle - \overline{\beta}\,|000\rangle = \overline{\alpha}e_7 - \overline{\beta}e_0 \\ E_{0,7}(\alpha,\beta)e_l &= e_l, \end{aligned}$$

donde $l \neq 0, 7$. Conseguimos la implementación de $E_{0,7}$ con compuertas CNOT y una compuerta controlada de un qubit.

La Proposición 2.4.1 y 2.4.2, y el Lema 2.2.15 demuestran el siguiente teorema.

Teorema 2.4.4. *$R_z(\theta), H_y, CNOT$ son un conjunto de compuertas cuánticas universales, es decir, toda compuerta unitaria U de n qubits se puede aproximar por composiciones de este conjunto.*

Capítulo 3

Superioridad Cuántica

Se han estudiado los fundamentos básicos de la computación cuántica, en términos de compuertas u operaciones cuánticas unitarias. Ahora, se expone brevemente uno de los fundamentos de los algoritmos cuánticos desarrollados en la década de los 90's [15] [26], los cuales representaron la superioridad que puede ofrecer la computación cuántica respecto a la computación clásica; entre estos algoritmos se encuentran el algoritmo de Deutsch, Grover y Shor. Hasta la fecha, 30 años después del desarrollo de estos algoritmos, se encuentran una gran cantidad de propuestas y aplicaciones de algoritmos cuánticos en diferentes campos, tales como problemas algebraicos [29][1], en el campo de la teoría de la información cuántica [30], complejidad computacional, y recientemente una mejora del reconocido algoritmo de Shor para la factorización en números primos [22]. Resaltamos que el objetivo de este capítulo es presentar algunos resultados destacados en el ámbito de la computación cuántica de una forma básica.

3.1 Transformada de Fourier Cuántica

Definición 3.1.1. La transformación lineal

$$TF : \mathbb{C}_x^N \to \mathbb{C}_y^N$$
$$\mathbf{x} = (x_0, \ldots, x_{N-1}) \mapsto \mathbf{y} = (y_0, \ldots, y_{N-1})$$

tal que

$$y_k \doteq \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}, \tag{3.1.1}$$

para todo $k \in \{0, \ldots, N-1\}$ y N fijo, se le conoce como la transformada de Fourier discreta de $\mathbb{C}^N$.

La transformada de Fourier discreta, se traduce directamente en términos de los estados cuánticos, como sigue.

Definición 3.1.2. El operador lineal QF en el espacio de estados $\mathcal{H}$ de dimensión N, que actúa sobre los estados de la base denotados $|0\rangle, \ldots, |N-1\rangle$ de la siguiente forma

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle, \tag{3.1.2}$$

[1] Hidden Subgroup Problem.

para todo $|j\rangle \in \{|0\rangle, \ldots, |N-1\rangle\}$, y sobre un estado $|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ actúa como sigue

$$\sum_{j=0}^{N-1} x_j |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left[\sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} \right] |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k |k\rangle , \tag{3.1.3}$$

se le conoce como la transformada de Fourier cuántica.

Observamos que y_k son las amplitudes de la transformación de Fourier clásica de las amplitudes x_j tales que $\sum_{k=0}^{N-1} |y_k|^2 = 1$.

De forma análoga, el operador de la transformada de Fourier cuántica inversa QF^{-1}, actúa sobre los estados de la base denotados $|0\rangle, \ldots, |N-1\rangle$ de la siguiente forma

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{-2\pi i jl/N} |l\rangle . \tag{3.1.4}$$

Lema 3.1.3. *El operador lineal QF es unitario.*

Demostración. Para demostrar que QF es un operador unitario, se muestra que preserva el producto interno entre los vectores de la base transformados. Sean $|m\rangle, |n\rangle \in \{0, \ldots, N-1\}$ estados base. Calculamos el siguiente producto interno

$$(QF|m\rangle, QF|n\rangle) = \frac{1}{N} \left(\sum_{l=0}^{N-1} e^{2\pi i ml/N} |l\rangle , \sum_{k=0}^{N-1} e^{2\pi i nk/N} |k\rangle \right) \tag{3.1.5}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i (n-m)k/N}. \tag{3.1.6}$$

Observamos que, si $m = n$, entonces $(QF|n\rangle, QF|n\rangle) = \langle n|QF^* QF|n\rangle = \langle n|n\rangle = 1$. Por otro lado, si $m \neq n$, entonces $x = e^{2\pi i(n-m)/N} \neq 1$ es una N-ésima raíz de la unidad, además

$$(1 + x + \ldots + x^{N-1})(1 - x) = 1 - x^N = 1 - \left(e^{2\pi i(n-m)/N}\right)^N = 0,$$

lo cual implica que

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i (n-m)k/N} = 0. \tag{3.1.7}$$

Lo que completa la prueba. ■

Lema 3.1.4. *La transformada de Fourier (3.1.2) para un sistema de n qubits, donde los estados base del espacio de Hilbert se denotan números decimales $|0\rangle, |1\rangle, \ldots |2^n - 1\rangle$, es equivalente a escribir*

$$|j\rangle \mapsto \frac{1}{2^{n/2}} \left[\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle \right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n} |1\rangle \right) \right], \tag{3.1.8}$$

donde, se ha realizado un cambio en la representación de los estados base de la forma decimal a la forma binaria, esto es, $j = j_1 j_2 \ldots j_n$ y $k = k_1 k_2 \ldots k_n$ donde $j_l, k_l \in \{0, 1\}$ y $l \in \{1, \cdots, n\}$

Demostración.

$$|j\rangle \mapsto \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \tag{3.1.9}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi ij \sum_{l=1}^{n} k_l 2^{-l}} |k_1 \cdots k_n\rangle \tag{3.1.10}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi ijk_1 2^{-1}} |k_1\rangle \otimes \cdots \otimes e^{2\pi ijk_n 2^{-n}} |k_n\rangle \tag{3.1.11}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} e^{2\pi ijk_1 2^{-1}} |k_1\rangle \otimes \cdots \otimes \sum_{k_n=0}^{1} \cdots e^{2\pi ijk_n 2^{-n}} |k_n\rangle \tag{3.1.12}$$

$$= \frac{1}{2^{n/2}} \left[|0\rangle + e^{2\pi ij2^{-1}} |1\rangle\right] \otimes \cdots \otimes \left[|0\rangle + e^{2\pi ij2^{-n}} |1\rangle\right] \tag{3.1.13}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi ij2^{-l}} |1\rangle\right] \tag{3.1.14}$$

$$= \frac{1}{2^{n/2}} \left[|0\rangle + e^{2\pi ij2^{-1}} |1\rangle\right] \otimes \cdots \otimes \left[|0\rangle + e^{2\pi ij2^{-n}} |1\rangle\right] \tag{3.1.15}$$

Dado que $j = j_1 j_2 \cdots j_n = j_1 2^{n-1} + \cdots + j_n 2^0$, donde $j_l = 0, 1$ se obtiene

$$j2^{-1} = j_1 2^{n-2} + \cdots + j_n 2^{-1} = j_1 j_2 \ldots j_{n-1}.j_n = j_1 j_2 \ldots j_{n-1} + 0.j_n \tag{3.1.16}$$

$$\vdots$$

$$j2^{-n} = j_1 2^{-1} + \cdots + j_n 2^{-n} = 0.j_1 j_2 \ldots j_n. \tag{3.1.17}$$

Lo cual conduce al resultado deseado. ■

Ahora, considerando el estado $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ik\omega} |k\rangle$ con $\omega = \frac{j}{N}$ para algún entero j, al aplicar la transformada de Fourier inversa QF^{-1} se produce el estado $|j\rangle$.

Definición 3.1.5 (Definición 3. [20])**.** Para cualquier real ω se define

$$|\tilde{\omega}\rangle \doteq QF^{-1} \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ik\omega} |k\rangle \right).$$

Lema 3.1.6 (Lema 4. [20])**.** *Para N fijo, si $\omega = \frac{j}{N}$, con $j \in \{0, \ldots, N-1\}$, entonces $|\tilde{\omega}\rangle = |j\rangle$; para cualquier otro real $\omega \in (0, 1)$, se tiene que $|\tilde{\omega}\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$, donde*

$$|\alpha_j| = \left| \frac{\sin \pi(N\omega - j)}{N \sin \pi(\omega - j/N)} \right|. \tag{3.1.18}$$

Demostración. La segunda parte del lema se prueba de la siguiente forma

$$
\begin{aligned}
|\alpha_j| = |\langle j|\tilde{\omega}\rangle| =& \frac{1}{\sqrt{N}}\left|\langle j|\, QF^{-1}\left(\sum_{k=0}^{N-1} e^{2\pi i\omega k}\,|k\rangle\right)\right| \\
=& \frac{1}{N}\left|\sum_{k,l=0}^{N-1} e^{2\pi i(\omega-l/N)k}\langle j|l\rangle\right| && (3.1.19)\\
=& \frac{1}{N}\left|\sum_{k=0}^{N-1} e^{2\pi i(\omega-j/N)k}\right| && (3.1.20)\\
=& \frac{1}{N}\left|\frac{1-e^{2\pi iN(\omega-j/N)}}{1-e^{2\pi i(\omega-j/N)}}\right| && (3.1.21)\\
=& \frac{1}{N}\left|\frac{\sin\pi(N\omega-j)}{\sin\pi(\omega-j/N)}\right| && (3.1.22)
\end{aligned}
$$

donde, (3.1.19) se obtiene de aplicar la Definición (3.1.4), y es distinto de cero si $j = l$, como se obtiene en la prueba del Lema 3.1.3. Dado que $\omega \neq \frac{j}{N}$, se tiene que en (3.1.20) el término de la suma $r = e^{2\pi i(\omega-j/N)} \neq 1$, por lo tanto en (3.1.21) se expresa el valor de la suma de los primeros N términos de la serie geométrica; y en (3.1.22) se aplica lo siguiente $|1-e^{2\pi i\beta}| = 2|-i\sin(\pi\beta)e^{i\pi\beta}| = 2|\sin\pi\beta|$. ■

De la representación de la transformada de Fourier en Lema 3.1.4 se puede construir el diagrama circuital de la transformada de Fourier cuántica a partir de las siguientes compuertas elementales.

Lema 3.1.7. *La operación de la compuerta Hadamard definida en 2.2.1, se puede escribir siguiente forma:*

$$
|a\rangle \mapsto \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^a\,|1\rangle\right] = \frac{1}{\sqrt{2}}\left[|0\rangle + e^{2\pi i(0.a)}\,|1\rangle\right] \tag{3.1.23}
$$

donde $a \in \{0,1\}$.

Definición 3.1.8. La compuerta de un qubit controlada por el qubit $|j_l\rangle$, $l = 2,\ldots,n$,

$$
R_{k,l} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}, \tag{3.1.24}
$$

donde $k = 2,\ldots,n$.

Observamos que, cuando el qubit $|j_l\rangle = |1\rangle$ entonces al aplicar la compuerta $R_{k,l}$ al qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ obtenemos,

$$
R_{k,l}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] = \left[\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i2^{-k}}\,|1\rangle)\right].
$$

Proposición 3.1.9. *La transformada de Fourier cuántica aplicada al estado* $|j\rangle = |j_1\ldots j_n\rangle$*, es implementada por el diagrama circuital de figura 3.1 descrito por la siguiente secuencia de operaciones (aplicada de izquierda a derecha)*

$$
H_1R_{2,2}\ldots R_{n-1,n-1}R_{n,n}H_2R_{2,3}\ldots R_{n-2,n-1}R_{n-1,n}\ldots H_{n-1}R_{2,n-1}H_n.
$$

donde H_k *es la compuerta* H *aplicada al qubit* j_k.

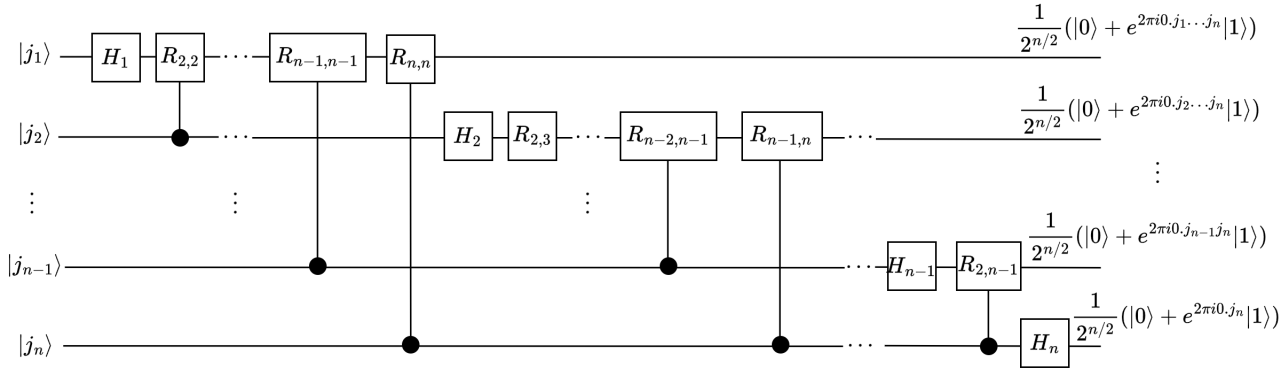

Figura 3.1: Diagrama Circuital de la Transformada de Fourier Cuántica.

Demostración. La demostración de que esta secuencia de operaciones implementa la transforma de Fourier se encuentra en [26] y [21]. ■

Proposición 3.1.10. *El número de compuertas requeridas para implementar el circuito es* $n(n+1)/2$.

Demostración. Notamos que primero aplicamos la compuerta H en el qubit j_1 y $n-1$ compuertas de rotación de un qubit $R_{k,l}$, tenemos n compuertas, luego aplicamos una compuerta H en el qubit j_2 y $n-2$ compuertas de rotación, por tanto, obtenemos $n-1$ y el total se expresa por la suma $n+n-1+\ldots+1$. ■

Ahora, observamos la construcción de la transformada de Fourier inversa en un sistema de 3 qubits.

Ejemplo 3.1.1. [20] Consideramos el estado

$$|\psi\rangle = \frac{1}{2^{3/2}}\left[\left(|0\rangle + e^{2\pi i(4\varphi)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i(2\varphi)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i\varphi}|1\rangle\right)\right]$$

para algún real $\varphi \in [0,1)$ desconocido. Supongamos $\varphi = k2^{-3}$ para algún k entero, el cual se puede escribir de forma binaria como $k = k_1k_2k_3 = k_1 2^2 + k_2 2^1 + k_3 2^0$ donde[2] cada $k_l \in \{0,1\}$ y observamos que

$$\begin{aligned} 4\varphi &= k2^{-1} = k_1k_2 + 0.k_3 \\ 2\varphi &= k2^{-2} = k_1 + 0.k_2k_3 \\ \varphi &= k2^{-3} = 0.k_1k_2k_3. \end{aligned}$$

Reescribiendo el estado anterior, obtenemos lo siguiente

$$\frac{1}{2^{3/2}}\left[\left(|0\rangle + e^{2\pi i(0.k_3)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i(0.k_2k_3)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i 0.k_1k_2k_3}|1\rangle\right)\right]. \tag{3.1.25}$$

El objetivo es determinar k_1, k_2, k_3 y por tanto φ. Por (3.1.23), y dado que $H = H^* = H^{-1}$, se tiene que al aplicar H al primer término del producto tensorial (3.1.25) y se obtiene lo siguiente

$$\frac{1}{2}\left[|k_3\rangle\otimes\left(|0\rangle + e^{2\pi i(0.k_2k_3)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i 0.k_1k_2k_3}|1\rangle\right)\right]. \tag{3.1.26}$$

[2]El entero k puede tener más digitos binarios, pero solamente interesan los últimos tres, por el cociente $k/2^3$, ya que se puede ignorar múltiplos enteros de 2π en el exponente de e.

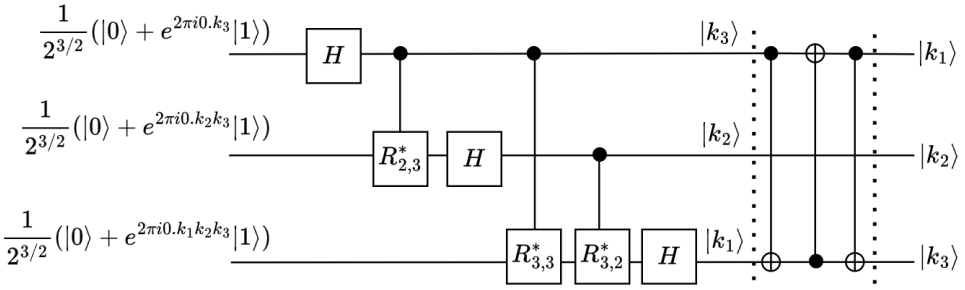

Figura 3.2: Diagrama Circuital de la Transformada de Fourier Inversa de un sistema de 3 qubits.

Ahora, tomando la rotación controlada

$$R^*_{2,3} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i 2^{-2}} \end{pmatrix}$$

y al aplicarla sobre el segundo término, produce el estado

$$\frac{1}{2}\left[|k_3\rangle \otimes \left(|0\rangle + e^{2\pi i(0.k_2k_3 - k_3 2^{-2})}\,|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 0.k_1k_2k_3}\,|1\rangle\right)\right] \tag{3.1.27}$$

$$= \frac{1}{2}\left[|k_3\rangle \otimes \left(|0\rangle + e^{2\pi i(0.k_2)}\,|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 0.k_1k_2k_3}\,|1\rangle\right)\right]. \tag{3.1.28}$$

Al aplicar de nuevo la compuerta H al segundo término del estado anterior, obtenemos

$$\frac{1}{\sqrt{2}}\left[|k_3\rangle \otimes |k_2\rangle \otimes \left(|0\rangle + e^{2\pi i 0.k_1k_2k_3}\,|1\rangle\right)\right] \tag{3.1.29}$$

Ahora conseguimos k_1 de la siguiente forma; aplicamos la rotación $R^*_{3,3}$ controlada por el primer término $|k_3\rangle$ y aplicada al tercer término del producto tensorial, seguido por la rotación $R^*_{3,2}$ controlada por el segundo término $|k_2\rangle$ y aplicada al tercer término, y por último, la compuerta H al tercer término. Obtenemos el estado $|k_3\rangle \otimes |k_2\rangle \otimes |k_1\rangle$, el cual notamos está en orden inverso con respecto a $|k\rangle$. El diagrama circuital se presenta en la figura 3.2, se observa que el orden se puede restablecer aplicando una compocisión de compuertas CNOT que invierta el orden, esta composición es una compuerta llamada SWAP.

La generalización del ejemplo anterior a partir del estado (3.1.8) que codifica el estado $|j\rangle$ en la fase es una construcción circuital de la transformada de Fourier cuántica inversa que permite encontrar la fase relativa entre los estados cuánticos.

3.2 Aplicaciones de la Transformada de Fourier Cuántica

La transformada de Fourier es una herramienta fundamental en la formulación de algoritmos cuánticos [20], [26]. A partir de sus características, como encontrar la periodicidad funciones, va a determinar la posibilidad de encontrar el orden de x módulo N, es decir, determinar el menor $r \in \mathbb{Z}^+$, tal que $x^r = 1 \mod N$, donde $x, N \in \mathbb{Z}$ son coprimos; además, el problema de encontrar el orden conduce directamente al algoritmo de factorización de enteros compuestos, es decir, el problema de encontrar dos factores que lo producen. Aunque el algoritmo de Shor para la factorización representa concretamente la superioridad de la computación cuántica, se tienen grandes retos en la física experimental para implementar este y demás algoritmos. Otra dificultad, que no

se presenta en detalle aquí, es la cantidad de recursos requeridos en un algoritmo, este es un punto de comparación y de medida de desempeño que determina que tan eficiente un algoritmo cuántico es con respecto a un algoritmo clásico que resuelva el mismo problema.

Otra consideración es el uso de "cajas negras" u "oráculos", en algunos pasos de los algoritmos cuánticos. Un oráculo es un circuito que realiza una tarea específica, sin decir explícitamente como funciona. En particular, en el algoritmo de estimación de fase descrito a continuación, se utiliza un oráculo para la definición de un operador controlado, en este caso el oráculo se puede implementar con el método de exponenciación modular, el cual se encuentra descrito en [21, Box 5.2], [26].

3.2.1 Estimación de Fase

Sea U un operador unitario sobre $\mathcal{M}(2^n, \mathbb{C})$, donde n es el número de qubits y $|u\rangle \in \mathbb{C}^{2^n}$ un eigenestado de U, tal que $U|u\rangle = e^{2\pi i\varphi}|u\rangle$, con $\varphi \in [0, 1)$. Escribimos la expansión binaria de φ como

$$\varphi = 0.\varphi_1\varphi_2\varphi_3\cdots = \sum_{l=1,2,\ldots} \varphi_l 2^{-l}$$

con $\varphi_l \in \{0, 1\}$. El objetivo del algoritmo de estimación de fase es encontrar φ. Dado que no podemos determinar un número infinito de términos, consideramos el caso especial donde la representación de φ es finita, esto es $\varphi = 0.\varphi_1\varphi_2\ldots\varphi_t$ para un t fijo. El paso clave, como se vio en el ejemplo 3.1.1, es utilizar la transformada de Fourier inversa, cuando se tiene a φ codificada en la fase de una combinación lineal de todos los estados.

Definición 3.2.1. Un registro de n qubits es un estado $|\psi\rangle \in \mathbb{C}^{2^n}$. Si todos los n qubits son el mismo estado, entonces podemos escribir $|x\rangle^{\otimes n}$. En particular, si $x = 0$ entonces denotamos $|0\rangle^{\otimes n} \doteq |0\rangle$, cuando no hay lugar a confusión.

Definición 3.2.2. Dado U un operador unitario en $\mathcal{M}(2^n, \mathbb{C})$ y $|u\rangle \in \mathbb{C}^{2^n}$ un eigenestado de U, tal que $U|u\rangle = e^{2\pi i\varphi}|u\rangle$, con $\varphi \in [0, 1)$. Se definen las potencias de dos del operador U controladas, por la compuerta controlada U^{2^m} por un qubit, para algún $m \in \mathbb{Z}$, tal que, cuando el qubit de control aplica la compuerta U^{2^m} sobre el eigenestado $|u\rangle$ el estado que se obtiene es $e^{2\pi i\varphi 2^m}|u\rangle$, en caso contrario, se aplica la identidad, esto es $|u\rangle$.

Supongamos que la compuerta controlada U^{2^m} tiene como qubit de control el estado $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, como se observa en el diagrama circuital de la figura 3.3 el estado que se obtiene es

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + e^{2\pi i\varphi 2^m}|1\rangle|u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\varphi 2^m}|1\rangle)|u\rangle\,. \tag{3.2.1}$$

Utilizamos los estados $|\psi_0\rangle, |\psi_1\rangle, \ldots$ para denotar cada registro de todos los qubits del sistema que intervienen en las diferentes operaciones, ordenados por cada paso del procedimiento para la estimación de fase descrito a continuación.

Descripción del procedimiento de la Estimación de Fase φ

- Se utilizan dos registros de entrada. El primero de t qubits, inicializado en $|0\rangle^{\otimes t}$, y el segundo de n qubits, inicializado en el eigenestado $|u\rangle$ de U. Por tanto, se tiene el estado inicial $|\psi_0\rangle = |0\rangle^{\otimes t} \otimes |u\rangle$.
- El número t determina, 1) el número de términos en la expansión binaria de φ, y 2) la probabilidad de éxito en la estimación de φ.

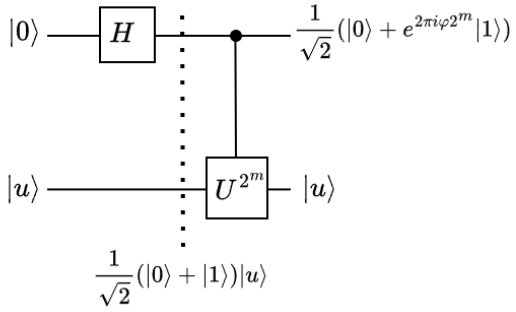

Figura 3.3: Diagrama circuital de la compuerta U^{2^m} controlada por un qubit.

- Se utiliza el oráculo que implementa la operación controlada U^{2^m} con eigenvector $|u\rangle$ y eigenvalor $e^{2\pi i\varphi 2^m}$, con $m = 0, \ldots, t-1$.
- Tenemos los siguientes pasos

1. Aplicar a cada qubit del registro de entrada $|0\rangle^{\otimes t}$ la compuerta H. Obtenemos el estado

$$|\psi_1\rangle = \left(H^{\otimes t}|0\rangle^{\otimes t}\right) \otimes |u\rangle = \frac{1}{\sqrt{2^t}}\left(|0\rangle + |1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + |1\rangle\right) \otimes |u\rangle\,. \tag{3.2.2}$$

2. De la expresión anterior los t primeros qubits van a controlar cada uno la compuerta $U^{2^{t-1-m}}$ con $m = 0, \ldots, t-1$, que actúa sobre el segundo registro $|u\rangle$. El qubit de control de $U^{2^{t-1-m}}$ es el qubit m-ésimo. Se obtiene el siguiente estado

$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}}\left[\left(|0\rangle + e^{2\pi i\varphi 2^{t-1}}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i\varphi 2^{t-2}}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i\varphi 2^{0}}|1\rangle\right)\right] \otimes |u\rangle\,.$$

3. Aplicar la transformada de Fourier inversa QF^{-1} al primer registro del ket $|\psi_2\rangle$, esto es,

$$QF^{-1}\left(\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^{t-1}} e^{2\pi i\varphi k}|k\rangle\right) \otimes |u\rangle \to |\tilde{\varphi}\rangle \otimes |u\rangle\,. \tag{3.2.3}$$

   donde se ha utilizado que (3.1.8) es equivalente a (3.1.2), y $|\tilde{\varphi}\rangle = |0.\varphi_1 \cdots \varphi_t\rangle$ es la aproximación de $|\varphi\rangle$ de t bits.

4. Leer el estado del primer registro para obtener la estimación $\tilde{\varphi}$.

El procedimiento descrito para obtener la fase, evidentemente estima con probabilidad 1 una fase de exactamente t bits; más aún, si φ no tiene una expansión binaria finita, el resultado del algoritmo de estimación de fase, que depende de la transformada de Fourier inversa, es con alta probabilidad una muy buena aproximación a φ [20, Corolario 6.]. Enfatizamos que la fase que se está estimando es una fase observable, a diferencia de la fase global, dado que la última no la podemos medir por la Proposición 1.1.8.

Aplicaciones del Algoritmo de Estimación de Fase

La estimación de fase es un algoritmo cuántico, el cual no tiene contraparte clásica. Principalmente se aplica para obtener los eigenvalores de operadores unitarios como se describe en [20]. Y también

tiene aplicación en el algoritmo de estimación de la energía del estado básico de un Hamiltoniano y la estimación de amplitud de probabilidad de un qubit [18]. Basado en el algoritmo de estimación de fase se encuentra el algoritmo cuántico para sistemas lineales de ecuaciones [12]. Y dado que está intrínsecamente relacionado con la transformada de Fourier cuántica, hace parte de otros algoritmos como un paso para obtener el resultado, esto en el lenguaje de la computación es llamado una subrutina[3] de otros algoritmos que resuelven problemas basados en la transformada de Fourier. Por ejemplo, junto con el algoritmo de encontrar el orden, hacen parte de las subrutinas para resolver el problema del subgrupo oculto que tiene como caso especial el problema del logaritmo discreto. Más aún, los algoritmos cuánticos están divididos en dos partes principalmente, los que utilizan la transforma de Fourier cuántica de manera principal y los algoritmos de búsqueda, que utilizan otras técnicas; el algoritmo de estimación de fase puede ser combinado con el algoritmo de búsqueda cuántica para resolver el problema de contar las distintas soluciones en un problema de búsqueda, lo cual es muy útil para abordar problemas tales como la búsqueda cuántica en una base de datos no estructurada [21].

3.2.2 Encontrar el Orden

En esta sección, consideramos x y $N \in \mathbb{Z}^+$ enteros positivos, tales que $x < N$, y sin factores comúnes.

Definición 3.2.3. El orden de x módulo N es definido como el menor entero positivo r, tal que $x^r = 1 \mod N$.

El problema consiste en estimar r de la definición anterior. A continuación se describe un caso especial del algoritmo de encontrar el orden, que ofrece la idea esencial del algoritmo.

Observamos que el número de bits que especifican a N es $n = \lceil \log N \rceil$ y el orden de x satisface $r \leqslant N$.

Definición 3.2.4. Definimos el operador unitario V_x de la siguiente forma:

$$V_x \left|j\right\rangle \left|k\right\rangle = \left|j\right\rangle \left|k + x^j \mod N\right\rangle, \tag{3.2.4}$$

donde $|j\rangle$ y $|k\rangle$ son dos registros.

En el algoritmo siguiente vamos a utilizar el operador V_x unitario, el cual es fundamental en producir el resultado deseado a nivel cuántico, por ello comentamos algunos detalles de su implementación. El operador V_x tiene una relación o es equivalente en su definición con el operador controlado U^{2^m} de la Definición 3.2.2 para el algoritmo de estimación de fase, ya que, tales operadores se pueden construir eficientemente aplicando principios de la computación clásica reversible, en particular, utilizando el algoritmo de exponenciación modular [21].

Definición 3.2.5. Se define el operador V unitario que actúa sobre dos registros $|m\rangle$ y $|k\rangle$ de la siguiente forma

$$V \left|m\right\rangle \left|k\right\rangle = \left|m\right\rangle \left|k + x \mod N\right\rangle \tag{3.2.5}$$

donde el primer registro es de t qubits, por lo tanto, $|m\rangle = |m_t \dots m_1\rangle$.

[3] Es un término que hace parte de la arquitectura de los procesos computacionales. El algoritmo principal es llamado la rutina, que internamente se apoya en otros algoritmos, que son llamados las subrutinas.

Definición 3.2.6. Dados dos registros $|m\rangle$ y $|k\rangle$, donde el primer registro es de t qubits, por lo tanto, $|m\rangle = |m_t \dots m_1\rangle$. Se define el operador controlado $V^{2^{l-1}}$ por el qubit m_l, con $l \in 1, \dots, t$; como las potencias de dos del operador V de la Definición 3.2.5, el cual actúa de la siguiente forma, cuando $m_l = 1$

$$|m\rangle |k\rangle \mapsto |m\rangle V^{2^{l-1}} |k\rangle = |m\rangle |k + x^{2^{l-1}} \mod N\rangle \tag{3.2.6}$$

y cuando $m_l = 0$

$$|m\rangle |k\rangle \mapsto |m\rangle I |k\rangle = |m\rangle |k\rangle . \tag{3.2.7}$$

Proposición 3.2.7. *El operador V_x de la Definición 3.2.4 se obtiene de la aplicación sucesiva de operadores de potencia de dos $V^{2^{l-1}}$ controladas por el qubit $|m_l\rangle$ para todo $l = 1, \dots, t$ y $m_l \in \{0, 1\}$.*

Demostración. Utilizamos la siguiente notación $V^{m_l 2^{l-1}}$ para la compuerta controlada $V^{2^{l-1}}$ por el qubit $|m_l\rangle$, dado que si $m_l = 0$ se aplica la identidad al qubit objetivo, y si $m_l = 1$ se aplica al qubit objetivo la compuerta $V^{2^{l-1}}$.

La compuerta $V^{2^{l-1}}$ se construye utilizando el algoritmo de exponenciación modular, de tal forma que la aplicación sucesiva de operaciones $V^{2^{l-1}}$ da como resultado el producto de las potencias de dos de x. Tenemos lo siguiente:

$$|m\rangle |k\rangle \mapsto |m\rangle V^{m_t 2^{t-1}} \dots V^{m_1 2^0} |k\rangle \tag{3.2.8}$$

$$= |m\rangle |k + \left(x^{m_t 2^{t-1}}\right) \dots \left(x^{m_1 2^0}\right) \mod N\rangle \tag{3.2.9}$$

$$= |m\rangle |k + x^{\sum_{l=1}^{t} m_l 2^{l-1}} \mod N\rangle \tag{3.2.10}$$

$$= |m\rangle |k + x^m \mod N\rangle . \tag{3.2.11}$$

Lo cual completa la prueba. ■

El algoritmo de exponenciación modular es una algoritmo de la computación clásica reversible y se encuentra desarrollado introductoriamente en [21]. A partir de este algoritmo se obtiene la construcción de los operadores controlados U^{2^m} de la Definición 3.2.2 y del operador V^{2^m} de la Definición 3.2.6 para algún $m \in \mathbb{Z}$, en otras palabras, el algoritmo de exponenciación modular permite obtener operadores que son potencias de dos, de cualquier operador unitario.

Descripción del algoritmo para encontrar el orden r

- Dado N, se elige aleatoriamente $x < N$, y se calcula de forma clásica, utilizando el algoritmo de Euclides que tiene una eficiencia polinomial, el $mcd(x, N)$, donde mcd denota el máximo común divisor de x y N. Si $d = mcd(x, N) \neq 1$, entonces d es un factor no trivial de N. Si $d = 1$, entonces se dice que x y N son coprimos, por lo tanto se ejecuta el algoritmo para encontrar el orden.

- Se utilizan dos registros. El primero de t qubits, tal que t satisface $N^2 < 2^t < 2N^2$ por razones de eficiencia [21]. El segundo registro de n qubits. El estado inicial del sistema es $|\psi_0\rangle = |0\rangle^{\otimes t} |0\rangle^{\otimes n}$ denotado $|0\rangle |0\rangle$.[4]

- Hay una caso especial, cuando r es una potencia de dos, entonces $t = n$. Estudiamos este caso donde el algoritmo que se obtiene es exacto [8].

[4]Se enfatiza que en esta sección utilizamos registros y el estado inicial denotado $|0\rangle |0\rangle$ indica dos registros, el primero de t qubits y el segundo de n qubits.

- Tenemos los siguientes pasos

1. Aplicar al primer registro en cada qubit la compuerta H, lo cual produce el estado[5]

$$|\psi_1\rangle = \left(H^{\otimes t}|0\rangle^{\otimes t}\right)|0\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|0\rangle\,. \tag{3.2.12}$$

2. Aplicar el operador V_x de la Definición 3.2.4 al estado $|\psi_1\rangle$, lo cual produce

$$|\psi_2\rangle = V_x|\psi_1\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}V_x|j\rangle|0\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \mod N\rangle \tag{3.2.13}$$

Observamos que V_x actúa sobre todos los estados base $|j\rangle|0\rangle$ así que en una sola cuenta, obtenemos todas las potencias de $x^j \mod N$. Consideramos el caso especial, cuando r es una potencia de 2 y por tanto, divide a 2^t. Para los valores de j múltiplos de r, se tiene que algunos términos del estado $|\psi_2\rangle$ son

$$|0\rangle|1\rangle + |r\rangle|1\rangle + |2r\rangle|1\rangle + \ldots + |2^t - r\rangle|1\rangle = (|0\rangle + |r\rangle + |2r\rangle + \ldots + |2^t - r\rangle)|1\rangle\,.$$

Dado que $x_j \mod N$ es una función periódica con periodo r, se escribe $j = ar + b$ donde $0 \leqslant a \leqslant \frac{2^t}{r} - 1$ y $0 \leqslant b \leqslant r - 1$. Sustituyendo j en el estado $|\psi_2\rangle$, se obtiene que

$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}}\sum_{b=0}^{r-1}\sum_{a=0}^{\frac{2^t}{r}-1}|ar+b\rangle|x^{ar+b} \mod N\rangle \tag{3.2.14}$$

$$= \frac{1}{\sqrt{2^t}}\sum_{b=0}^{r-1}\sum_{a=0}^{\frac{2^t}{r}-1}|ar+b\rangle|x^{b} \mod N\rangle\,. \tag{3.2.15}$$

3. Medir el segundo registro. Supongamos que el resultado es $|x^{b_0}\rangle$, entonces el estado se convierte en

$$|\psi_3\rangle = \sqrt{\frac{r}{2^t}}\sum_{a=0}^{\frac{2^t}{r}-1}|ar+b_0\rangle|x^{b_0}\rangle\,, \tag{3.2.16}$$

donde, el factor $\sqrt{r}$ se introduce para renormalizar el estado después de la medición. Como se observo en el paso anterior, se quiere determinar el periodo r de los estados del primer registro, por ello, se aplica la transformada de Fourier.

4. Aplicar la transformada de Fourier al primer registro. Recordamos que QF es un ope-

[5] Ver Proposición 2.2.8.

rador lineal, por tanto, se obtiene el siguiente estado

$$|\psi_4\rangle = QF\,|\psi_3\rangle = \sqrt{\frac{r}{2^t}} \sum_{a=0}^{\frac{2^t}{r}-1} \left(\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j(ar+b_0)/2^t} \,|j\rangle \right) |x^{b_0}\rangle \tag{3.2.17}$$

$$= \frac{\sqrt{r}}{2^t} \sum_{j=0}^{2^t-1} \left(\sum_{a=0}^{\frac{2^t}{r}-1} e^{2\pi i j a r/2^t} \right) e^{2\pi i j b_0/2^t} \,|j\rangle\,|x^{b_0}\rangle \tag{3.2.18}$$

$$= \frac{1}{\sqrt{r}} \sum_{j=0}^{2^t-1} \left(\frac{1}{2^t/r} \sum_{a=0}^{\frac{2^t}{r}-1} e^{2\pi i a j/2^t/r} \right) e^{2\pi i j b_0/2^t} \,|j\rangle\,|x^{b_0}\rangle \tag{3.2.19}$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i (k2^t/r) b_0/2^t} \left| \frac{k2^t}{r} \right\rangle |x^{b_0}\rangle \tag{3.2.20}$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i b_0 k/r} \left| \frac{k2^t}{r} \right\rangle |x^{b_0}\rangle\,, \tag{3.2.21}$$

donde, en (3.2.19) se aplico (3.1.7), es decir, el término entre paréntesis es 1 cuando $j = k(2^t/r)$ con $k = 0, 1, \ldots, r-1$ y 0 de lo contrario. Observamos que esto es posible, porque r divide a 2^t, en el caso general, este término no se desvanece y contribuye a la probabilidad del estado $|j\rangle$. La distribución de probabilidad del primer registro del $|\psi_4\rangle$ medida en la base computacional es una distribución equiprobable como se observa en la figura 3.4.

5. Medir el primer registro del estado $|\psi_4\rangle$, del cual se obtendrá k_0 con probabilidad $\frac{1}{r}$. Si $k_0 = 0$ entonces no tenemos información de r, por lo que hay que repetir el algoritmo. Si $k_0 \neq 0$ entonces dividimos $\frac{k_0 2^t}{r}$ entre 2^t, para obtener $\frac{k_0}{r}$.
6. Aplicar el algoritmo de fracciones continuas al número $\frac{k_0}{r}$. Considerando que ni k_0 ni r son conocidos, el algoritmo produce una aproximación racional de ellos. Por tanto, tenemos los dos casos siguientes: 1) k_0 y r sean coprimos, entonces el denominador es el resultado deseado. 2) k_0 y r tienen un factor común.
7. Estudio del caso 2). El denominador de la fracción reducida k_0/r es un factor de r pero no r, digamos $r = r_1 r_2$ y se ha conseguido r_1. Entonces el objetivo es encontrar r_2, esto es, encontrar el orden de x^{r_1}. Por lo tanto, se vuelve a aplicar el algoritmo hasta encontrar r_2. Si lo encuentra, termina el algoritmo; si no, se sigue aplicando recursivamente.

El procedimiento descrito ha considerado el caso cuando r divide a 2^t, esta situación es muy favorable, porque como se observa en la figura 3.4 la distribución de probabilidad plantea que el problema es encontrar el periodo entre los resultados posibles, y por tanto, la aplicación de la transformada de Fourier en el estado $|\psi_3\rangle$ codifica la información de r en el primer registro, sin embargo, no se obtiene directamente al medir, por ello, los pasos siguientes para obtener r o un factor de r.

En el paso 6, el algortimo de fracciones continuas, representa un número real por una secuencia de números enteros, se encuentra descrito en [21, Box 5.3] y más ampliamente en [14]. La aproximación racional que se obtiene, a saber, k_0'/r', se verifica, haciendo un cálculo clásico si $x^{r'} = 1$ mód N, entonces, si es cierto, $r = r'$. En el caso contrario, r' es un factor de r y se sigue el paso 7.

En el paso 7 la recursividad es eficiente en el sentido que el número de repeticiones necesarias para encontrar r es menor que $\log r$ [21].

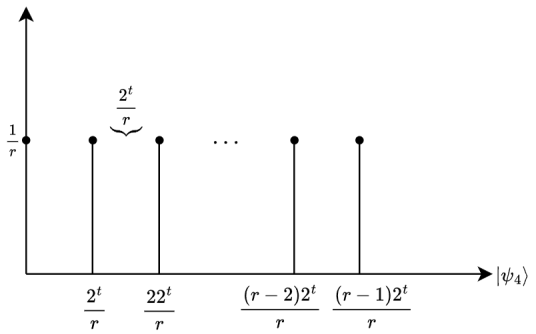

Figura 3.4: Distribución de Probabilidad del estado $|\psi_4\rangle$ en el algoritmo de encontrar el orden.

El caso general del algoritmo cuando r no divide a 2^t es muy parecido, y se obtienen muy buenas aproximaciones en la estimación del orden utilizando el algoritmo de fracciones continuas [21] [26].

3.2.3 Algoritmo de Factorización

Hemos considerado N un número entero positivo, por lo tanto, se puede descomponer de la siguiente forma $N = p_1^{r_1} \cdots p_l^{r_l}$, donde los p_i son primos distintos y los r_i son enteros positivos con $i = 0, \ldots, l$. El problema de la factorización de números enteros positivos, consiste en determinar los p_i y r_i para un N dado.

Al resolver el problema de encontrar el orden se consigue un algoritmo que con alta probabilidad produce un factor primo no trivial de un entero N positivo, como se describe a continuación. Observamos que los casos donde clásicamente se pueden determinar los factores de N son los siguientes: si N es par. Si N es de la forma $N = x^m$ con $x \geqslant 1$ y $m \geqslant 2$ y por tanto, obtener x [21]. Otra forma de encontrar un factor de N, es eligiendo aleatoriamente $x \in \{0, \ldots, N-1\}$, y aplicando el algoritmo de Euclides, determinar el $mcd(x, N)$, si es mayor que 1, entonces el $mcd(x, N)$ es un factor de N, por definición. El caso difícil, es cuando no ocurren ninguna de las situaciones anteriores y el número es muy grande. Describimos como el algoritmo de encontrar el orden se traduce en un algoritmo de factorización.

Dados x y N, si el $mcd(x, N) = 1$ entonces se utiliza el algoritmo de encontrar el orden de x módulo N. Si el orden r es par, entonces

$$x^r = 1 \mod N \tag{3.2.22}$$

lo cual es equivalente a escribir

$$x^r - 1 = 0 \mod N, \tag{3.2.23}$$

por lo tanto, $x^r - 1 = kN$ con $k \in \mathbb{Z}$, y dado que r es par, se tiene que

$$(x^{r/2})^2 - 1 = (x^{r/2} - 1)(x^{r/2} + 1) = kN. \tag{3.2.24}$$

Luego N divide a $(x^{r/2} - 1)(x^{r/2} + 1)$[6] y si $1 < x^{r/2} < N - 1$, entonces los factores satisfacen

$$0 < x^{r/2} - 1 < x^{r/2} + 1 < N, \tag{3.2.25}$$

[6]Para x, y enteros, se dice que x divide a y si existe un entero k tal que $y = kx$.

lo cual implica que $x^{r/2} \pm 1$ no son múltiplos de N y por lo tanto $x^{r/2} + 1$ y $x^{r/2} - 1$ tienen factores de N.

Por lo tanto, calculando el $mcd(x^{r/2}+1, N)$ y $mcd(x^{r/2}-1, N)$ obtenemos factores no triviales de N con alta probabilidad. Un estudio del algoritmo de Factorización de Shor se encuentra detallado en [8], [21], [26].

Este problema es fundamental en los sistemas de seguridad clásicos tales como el sistema criptográfico de clave publica RSA que se fundamenta en utilizar dos factores primos de 1024 bits (309 dígitos decimales), y la seguridad se basa en que encontrar tales números primos es un problema para la computación clásica prácticamente insoluble.

Algunos de los algoritmos clásicos más eficientes como la *Criba General de Campos Numéricos*[7] que factoriza enteros de más de 100 dígitos, no logran romper el sistema, es decir, encontrar tales factores primos, dado que la cantidad de tiempo de ejecución depende exponencialmente del número de bits que definen el tamaño del número a ser factorizado. El algoritmo cuántico de factorización, creado en 1994 por Peter Shor, lograría un tiempo de ejecución polinomial en el tamaño de la entrada. Tal diferencia en el tiempo de ejecución revela la potencia de un computador cuántico con respecto a un computador clásico.

[7] Algoritmo de John M. Pollard creado en 1988.

Capítulo 4

Conclusiones

El estudio de cada capítulo del presente trabajo desarrolla de forma básica las ideas principales que fundamentan la teoría de la computación cuántica. Por lo tanto, son una base importante para introducirse en el estudio de esta área, que se encuentra en su punto de mayor investigación y experimentación, y en el que además, se encuentran gran cantidad de desafíos. En Estados Unidos, las principales empresas que han demostrado la supremacía cuántica son IBM y Google; sin embargo, hay muchas más alrededor del mundo, que se encuentran en la carrera por desarrollar una computadora cuántica. Uno de los resultados interesantes que, afirma obtuvo Google en el 2019, es realizar cálculos en menos de cinco minutos que le tomaría a un computador clásico, el más avanzado de esa fecha, aproximadamente 10.000 años. Y computadoras cuánticas por IBM han sido puestas en la nube para que cualquier persona interesada pueda comenzar a programar circuitos cuánticos.

El interés de este trabajo consistió en presentar las propiedades de la computación cuántica que la distinguen de la computación clásica, se presentaron algunas de estas características basadas en los fundamentos matemáticos que modelan lo que se puede lograr a nivel cuántico, teniendo en cuenta que los resultados presentados no tienen equivalente clásico y por eso son distintivos o propios de la computación cuántica. En este estudio, se desarrolló el formalismo de operadores unitarios para la computación cuántica, los cuales determinan un sistema físico con características totalmente en oposición al determinismo de la computación clásica. Entre las ideas principales que se han presentado de la computación cuántica y que la distinguen de la computación clásica son: el qubit el cual define la unidad mínima de información en un computador cuántico, y es un estado cuántico -descrito por un sistema cuántico de dos niveles, como el que se obtiene en el experimento de Stern-Gerlach- elemento de un espacio Hilbert complejo; las operaciones cuánticas son operadores unitarios, que implican reversibilidad. La potencia de la computación cuántica se encuentra manifiesta en los algoritmos cuánticos[1]. Presentamos dos algoritmos en detalle que utilizan la transformada de Fourier cuántica; tales algoritmos se pueden generalizar para obtener resultados en problemas de teoría de números y del álgebra que no tenían una solución clásica, como el problema del subgrupo oculto y el logaritmo discreto, que se encuentran ampliamente discutidos en la literatura [20] [21], y que utilizan las herramientas desarrolladas por el algoritmo de estimación de fase y de encontrar el orden. El resultado indudable de máxima comparación que distingue la computación cuántica de la clásica es el algoritmo de Shor, el cual fue implementado por primera vez en una computadora de 7 qubits desarrollada por IBM en 2001, para factorizar el número 15. Tales empresas afirman que en unos cuantos años obtendrán una computadora cuántica

[1]Se encuentra un catálogo exhaustivo de algoritmos cuánticos en el siguiente enlace https://quantumalgorithmzoo.org

con la cantidad suficiente de qubits para obtener resultados a problemas de mayor capacidad que clásicamente son insolubles.

La computación cuántica implica grandes dificultades, que son el reto de las actuales investigaciones, debido a las condiciones que determinan su implementación, tales como, la temperatura para conseguir un sistema de qubits lo suficientemente aislado, que al mismo tiempo sea un sistema cuántico robusto, en el sentido de la conectividad de qubits, el cual permita mantener en un espacio de tiempo los estados cuánticos y proveer de las condiciones óptimas para su evolución deseada en el tiempo. En este sentido, otro requisito actual es la preparación de estados iniciales y la medición final en los estados de salida, donde problemas tales como la decoherencia y el ruido, sean mitigados por medio de técnicas de la teoría de corrección de errores cuántica, que hace parte de la teoría de la información cuántica.

Es importante destacar que en los procesos de computación cuántica, que se predice ofrecen una mayor eficiencia en cuanto al uso de recursos y al tiempo de ejecución, para ciertos problemas que implican costos gigantescos para la computación clásica, hay apoyo de operaciones clásicas que ya son eficientemente implementadas y que en comparación con los costos de hacer todas las operaciones cuánticas, resulta más útil un sistema híbrido. Por ejemplo, en el algoritmo de Shor, la primera parte, utilizar el algoritmo de encontrar el orden es cuántica, y la segunda parte, calcular el máximo común divisor para obtener los factores, y verificar que los resultados son los correctos, implementada clásicamente, ofrece una solución eficiente. Así que lo más evidente es que el desarrollo tecnológico de estas décadas, apueste a una aplicación híbrida de los sistemas de cómputo, esto es, un mundo con más posibilidades en términos de investigación científica, simulación de sistemas cuánticos, etc., y en el desarrollo de nuevos sistemas de seguridad y de comunicaciones.

Apéndice A

Desigualdad de Bell

En la teoría de la computación e información cuántica, se evidencia y es vital entender las diferencias de los fenómenos en la mecánica clásica y la mecánica cuántica, no con el propósito de *explicar* en el sentido en que se explica en la mecánica clásica [28], si no con el propósito de comprender como procesar la información en sistemas físicos cuánticos y como resolver problemas que los sistemas de procesamiento de información clásicos no pueden resolver. Aquí queremos destacar uno de los aspectos más controversiales en el desarrollo de la mecánica cuántica, planteado por Albert Einstein, un notable opositor a la interpretación probabilística de la teoría cuántica. Por ejemplo, en 1927, después de proponer a W. Heisenberg y N. Bohr muchos experimentos mentales para refutar el principio de incertidumbre, no obtuvo ningún resultado, y las demostraciones de ellos no lograban convencerle de que la interpretación de la mecánica cuántica era correcta. En [13], Heisenberg describe un encuentro que tuvo con Einstein poco antes de su muerte:

"*La frase -Pero no va a creer usted que Dios juega a los dados- la profería una y otra vez casi como un reproche. Las diferencias entre las dos concepciones yacían en realidad más hondo. En la física anterior, Einstein podía arrancar siempre de la imagen de un mundo objetivo que se desenvuelve en el espacio y en el tiempo y que nosotros, en cuanto físicos, solo observamos desde afuera, por así decirlo. Las leyes de la naturaleza determinan su transcurso en el tiempo. En la teoría cuántica ya no era posible esa idealización. Las leyes de la naturaleza versaban aquí sobre la modificación temporal de lo posible y de lo probable. Pero las decisiones que conducen de lo posible a lo fáctico solo cabe registrarlas estadísticamente, no predecirlas. Lo cual es, en el fondo, como quitarle el suelo de debajo de los pies a la representación de la realidad de la física clásica. A una modificación tan radical no se podía acostumbrar Einstein.*"

La idea de Einstein quedo plasmada en el artículo [9] de 1935 que, en conjunto con B. Podolsky y N. Rosen, imponían algunas nociones comunes de como debería obrar la 'Naturaleza', para mostrar que la teoría cuántica no era una teoría completa, por lo que existían variables ocultas que aún no se habían descubierto y harían de la teoría cuántica una teoría completa. Sin embargo, 30 años después de planteada la paradoja EPR (Eistein, Podolsky, Rosen) quedo demostrada su invalidez [5]. Nombraremos algunos conceptos que introdujeron, los cuales permitirán comprender la diferencia esencial del mundo clásico y cuántico. La *causalidad*, que se refiere a que no puede haber transmisión de información con velocidad más rápida que la velocidad de la luz; la *localidad*, que afirma que el resultado de una medición sobre un sistema no es afectado por las operaciones que se realizan en un sistema espacialmente aislado con el cual tuvo interacción en el pasado, y el *realismo* que afirma que independientemente de la observación las propiedades físicas tienen un valor definido.

La característica de los experimentos que demostraron la invalidez de las hipótesis que asumía la paradoja EPR de variables ocultas locales, es un resultado conocido como la desigualdad de Bell; para obtenerla realizaremos un experimento del cual haremos dos análisis, primero, desde el sentido

común, y luego un análisis mecánico cuántico. El resultado experimental demostró que el análisis correcto coincide con el análisis cuántico y además, revelo que las hipótesis que condujeron a la desigualdad de Bell son incorrectas.

Descripción del Experimento Cuántico

- Consideramos tres personajes, Charlie, Alice y Bob, que representan tres puntos distintos de manipulación de los estados cuánticos. Se quiere realizar un experimento de probabilidad descartando que Alice y Bob se puedan comunicar y que puedan deducir el resultado de medir por leyes de conservación. Nos interesa definir una variable aleatoria en el caso clásico y un observable en el caso cuántico, que determine la correlación de las medidas realizadas individualmente por Alice y Bob.

- Charlie prepara un estado entrelazado $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, de tal forma que puede repetir el procedimiento experimental para obtener de nuevo el mismo estado. Supongamos que el estado de las dos partículas es descrito por el espín de dos electrones, es decir, por superposiciones de la base $\{|\downarrow\rangle \otimes |\downarrow\rangle, |\downarrow\rangle \otimes |\uparrow\rangle, |\uparrow\rangle \otimes |\downarrow\rangle, |\uparrow\rangle \otimes |\uparrow\rangle\}$, por lo tanto, el estado entrelazado se escribe en la base anterior de la siguiente forma

$$|\psi\rangle = \frac{|\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle}{\sqrt{2}} \doteq \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}, \tag{A.0.1}$$

  donde, el ket del lado izquierdo del producto tensorial corresponde a una partícula y el ket del lado derecho a la otra; en la base computacional $\{|0\rangle, |1\rangle\}$, obtenemos de forma equivalente[1]:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}\right) = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

  En A.0.1 el espín tiene valores $\{\pm 1\}$ en la dirección del eje z.

- Charlie envía una partícula del par a Alice, y la otra partícula a Bob, y consideramos el punto A como Alice y B como Bob.

- Consideramos las matrices de Pauli $Q \doteq \sigma_z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ y $R \doteq \sigma_x = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ y definimos los operadores

$$S \doteq \frac{-1}{\sqrt{2}}(Q + R), \tag{A.0.2}$$

$$P \doteq \frac{1}{\sqrt{2}}(Q - R). \tag{A.0.3}$$

  Las matrices de Pauli σ_x y σ_z son operadores autoadjuntos, esto es, satisfacen que $\sigma_i\sigma_i^* = \sigma_i^*\sigma_i = I$ para $i = \{x, z\}$, y son llamados observables. Luego, por propiedades del producto tensorial $((A \otimes B)^* = A^* \otimes B^*)$ se obtiene que S, P son observables. Denotamos el espectro del observable T, es decir, el conjunto de valores propios de T como $\mathcal{E}(T)$[2].

[1] Utilizando la notación de Dirac descrita en la sección 1.5.

[2] Que en este caso coincide el espectro con el conjunto de valores propios por ser un operador autoadjunto.

Descripción de la medición un observable

- En A tenemos dos aparatos de medición, que miden los observables Q y R. Medir Q en la esfera de Bloch (ver sección 2.1) es considerar un aparato, digamos un imán alineado con el eje z, donde el norte del imán se encuentra en $z > 0$. Una rotación del instrumento en el plano xz por $\pi/2$ lleva el imán en alineación con el eje x y, por tanto, medimos R, donde el instrumento tiene ahora el norte en la dirección de $x > 0$. Afirmamos, que es posible alternar las dos posiciones del aparato de forma vertical y horizontal en el plano xz aleatoriamente. Los valores que se obtienen de medir Q y R, son los valores propios del observable, en este caso, $\mathcal{E}(Q) = \mathcal{E}(R) = \{\pm 1\}$.

- En B se quiere medir S y P. Para medir S inclinamos el aparato de medición R por un ángulo de $\pi/4$ en el plano xz en sentido positivo, Se obtiene el norte del aparato en $x > 0, z > 0$. Y para medir P inclinamos el aparato por un ángulo de $3\pi/4$ en el plano xz, el norte del aparato se ubica en $x < 0, z > 0$. De forma análoga, los valores que medimos son los valores propios en el espectro de cada observable, que en este caso son, $\mathcal{E}(S) = \mathcal{E}(P) = \{\pm 1\}$.

- No hay causalidad por la separación espacial entre A y B, y la inclinación del aparato de medición es totalmente aleatoria El experimento es diseñado para que al recibir A y B su partícula, realicen mediciones con sus aparatos al mismo tiempo y la elección del aparato que va a realizar la medición sea de forma aleatoria. Por lo tanto, las mediciones que realiza A no pueden modificar el resultado que obtenga B (o viceversa), ya que las influencias físicas no se pueden propagar a una velocidad mayor que la de la luz.

Análisis Clásico

- En el caso clásico, las variables Q, R, S, P corresponden a números reales y no a operadores. Consideramos que A va a medir las propiedades físicas Q, R y B mide las propiedades físicas S y P, las cuales tienen los siguientes valores posibles:

$$\begin{aligned} Q &\in \mathcal{E}(\sigma_z) = \{\pm 1\}, \\ R &\in \mathcal{E}(\sigma_x) = \{\pm 1\}, \\ S &\in \mathcal{E}\left(\frac{-1}{\sqrt{2}}(\sigma_z + \sigma_x)\right) = \{\pm 1\} \\ P &\in \mathcal{E}s\left(\frac{1}{\sqrt{2}}(\sigma_Z - \sigma_X)\right) = \{\pm 1\}. \end{aligned}$$

En el caso clásico se define la variable aleatoria T, que mediría las correlaciones de las variables aleatorias Q, R, S, P como sigue

$$T = QS + RP + RS - QP = Q(S - P) + R(S + P). \tag{A.0.4}$$

Observamos que, si $S = P \Rightarrow S - P = 0$, y si $S \neq P \Rightarrow S + P = 0$, además máx$(S + P) =$ máx$(S - P) = 2$, obtenemos que los valores posibles de T, son $\{-2, 2\}$. En consecuencia, el valor promedio de T, calculado como el valor esperado de la variable aleatoria T, es

$$\mathbb{E}[T] = \mathbb{E}[QS + RP - RS - QP] = \mathbb{E}[QS] + \mathbb{E}[RP] + \mathbb{E}[RS] - \mathbb{E}[QP] \leqslant 2. \tag{A.0.5}$$

A.0.5 es conocida como la desigualdad de Bell, y es parte de un conjunto de desigualdades conocidas como desigualdades de Bell, debido a quien la formuló por primera vez [4],[21].

Análisis Cuántico

- Ahora, consideramos de nuevo Q, R, S y P como observables y se define el operador

$$T = Q \otimes S + R \otimes P + R \otimes S - Q \otimes P = QS + RP + RS - QP$$

- Calculamos el valor esperado de los observables QS, RP, RS y QP en el sentido de la mecánica cuántica; en detalle para $\langle QS \rangle_\psi$:

$$\langle QS \rangle_\psi = \left\langle \frac{1}{\sqrt{2}} \sigma_z \otimes -\sigma_z - \sigma_x \right\rangle_\psi = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \right\rangle_\psi$$

$$= \frac{1}{2\sqrt{2}} \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \middle| \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \middle| \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$$

$$= \frac{1}{2\sqrt{2}} \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} -1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} -1 \\ -1 \end{pmatrix} \right\rangle$$

$$= \frac{1}{2\sqrt{2}} \left(\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\rangle + \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} -1 \\ -1 \end{pmatrix} \right\rangle \right)$$

$$= \frac{1}{2\sqrt{2}} \left(\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\rangle + \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \end{pmatrix} \right\rangle \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \end{pmatrix} \right\rangle \right)$$

$$= \frac{1}{2\sqrt{2}}(1+1) = \frac{1}{\sqrt{2}}.$$

  De forma análoga, obtenemos

$$\langle RS \rangle_\psi = \langle RP \rangle_\psi = \frac{1}{\sqrt{2}}, \quad \langle QP \rangle_\psi = -\frac{1}{\sqrt{2}}.$$

  Por tanto,

$$\langle T \rangle_\psi = \langle QS \rangle_\psi + \langle RS \rangle_\psi + \langle RP \rangle_\psi - \langle QP \rangle_\psi = \frac{4}{\sqrt{2}} = 2\sqrt{2} \approx 2{,}8284. \tag{A.0.6}$$

  Observamos que en A.0.5 el valor promedio de T no puede exceder dos, pero la mecánica cuántica predice que el valor promedio será mayor que dos.

¿Cuál de los dos análisis se verifica en la naturaleza? Se diseñó un experimento real para resolver la pregunta en [2], el cual verifico la predicción A.0.6, es decir, un valor superior a 2. Así que las hipótesis que fueron planteadas por EPR y que han llevado a las desigualdades de Bell deben ser incorrectas. Las hipótesis que definieron A.0.5 fueron:

- El realismo, es decir, las propiedades físicas Q, R, P y S se asumen como cantidades con valores definidos independientes de la medición.
- La localidad, es decir, la hipótesis de que la medición en A no tiene efectos sobre la medición realizada en B.

Concluimos, primero, que el mundo no es localmente realístico [9], que estas dos concepciones de la realidad deben ser transformadas para conducirnos a una mejor comprensión de la mecánica cuántica. Y segundo, que el fenómeno de entrelazamiento sugiere un interés particular por ser totalmente ajeno a los fenómenos clásicos y a nuestra comprensión intuitiva de cómo debería funcionar el mundo, nos damos cuenta de que no podemos imponer ninguna regla basada en nuestro sentido común (sentido común entrenado por la física clásica) en los fenómenos de la mecánica cuántica, pero más aún, nos sugiere pensar en que aprovechar esta propiedad de la naturaleza puede llevarnos a enfrentar problemas complejos de la actual computación clásica y plantearnos nuevas formas de concebir y procesar la información.

Bibliografía

[1] Boris Hasselblatt Anatole Katok. *Introduction to the Modern Theory of Dynamical Systems*. Encyclopedia of Mathematics and its Applications 54. Cambridge University Press, 1995. 20

[2] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, Jul 1982. URL: https://link.aps.org/doi/10.1103/PhysRevLett.49.91, doi:10.1103/PhysRevLett.49.91. 59

[3] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52:3457–3467, 1995. 14, 19, 28, 32

[4] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. URL: https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195, doi:10.1103/PhysicsPhysiqueFizika.1.195. 58

[5] Guy Blaylock. The EPR Paradox, Bell's Inequality, and the Question of Locality. *American Journal of Physics*, 78:111–120, 2009. URL: http://dx.doi.org/10.1119/1.3243279, doi:10.1119/1.3243279. 56

[6] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999. arXiv:quant-ph/9906054. 14, 21

[7] J.B. Conway. *A Course in Functional Analysis*. Graduate Texts in Mathematics. Springer New York, 1994. 1

[8] F. de Lima Marquezino, R. Portugal, and C. Lavor. *A Primer on Quantum Computing*. SpringerBriefs in Computer Science. Springer International Publishing, 2019. v, 10, 19, 49, 53

[9] A. Einstein, Podolsky, B., and N. Rosen. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? *Physical Review*, 47:777–780, 1935. doi:http://dx.doi.org/10.1103/PhysRev.47.777. 56, 60

[10] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982. doi:10.1007/BF02650179. iv

[11] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86, 2012. doi:10.1103/physreva.86.032324. v

[12] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.*, 103:150502, Oct 2009. URL: https://link.aps.org/doi/10.1103/PhysRevLett.103.150502, doi:10.1103/PhysRevLett.103.150502. 48

[13] W. Heisenberg. *Encuentros y conversaciones con Einstein y otros ensayos*. Biblioteca fundamental de nuestro tiempo. Alianza, 1980. URL: https://books.google.com.mx/books?id=euRxzwEACAAJ. 56

[14] A. Ya. Khinchin. *Continued Fractions*. Dover Books on Mathematics. Mir Publishers, 1997. 51

[15] A. Yu. Kitaev. Quantum measurements and the abelian stabilizer problem, 1995. arXiv:quant-ph/9511026. 40

[16] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit rsa modulus. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, pages 333–350, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. v

[17] John M. Lee. *Introduction to Topological Manifolds*. Graduate Texts in Mathematics. Springer New York, NY, 2010. 6

[18] Lin Lin. Lecture notes on quantum algorithms for scientific computation, 2022. arXiv:2201.08309. 48

[19] Olivia Di Matteo, Anna McCoy, Peter Gysbers, Takayuki Miyagi, R. M. Woloshyn, and Petr Navrátil. Improving Hamiltonian encodings with the Gray code. *Physical Review A*, 103, 2021. doi:10.1103/physreva.103.042405. 28, 30

[20] Michele Mosca. *Quantum Computer Algorithms*. Phd thesis, University of Oxford, 1999. URL: https://www.karlin.mff.cuni.cz/~holub/soubory/moscathesis.pdf. v, 42, 44, 45, 47, 54

[21] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. v, 9, 10, 13, 19, 20, 21, 44, 46, 48, 49, 51, 52, 53, 54, 58

[22] Oded Regev. An efficient quantum factoring algorithm, 2023. arXiv:2308.06572. 40

[23] Konstantin Sakharovskiy. Universal quantum gates. 2022. URL: http://urn.fi/URN:NBN:fi:jyu-202205272927. 26

[24] Jun John Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, 1994. URL: https://cds.cern.ch/record/1167961. 17

[25] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, pages 379–423, 1948. 12

[26] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997. doi:10.1137/s0097539795293172. v, 40, 44, 45, 46, 52, 53

[27] Gilbert Strang. *Linear Algebra and Its Applications, Fourth Edition*. 2005. 33

[28] K. Vogtmann V. I. Arnold, A. Weinstein. *Mathematical Methods Of Classical Mechanics*. Graduate Texts in Mathematics. Springer, 1989. 56

[29] Wim van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems, 2002. arXiv:quant-ph/0211140. 40

[30] Qisheng Wang, Ji Guan, Junyi Liu, Zhicheng Zhang, and Mingsheng Ying. New quantum algorithms for computing quantum entropies and distances, 2022. arXiv:2203.13522. 40