Introducción a la Computación Cuántica

José Castro

October 6, 2004

Chapter 1

Introducción

Thomas Young, el cual no solo fue físico sino también Egiptólogo y responsable de haber descrifrado la piedra de Rosetta, se le acredita haber ideado, tal vez uno de los experimentos más importantes en la historia de la física: a inicios del siglo XIX Young logro demostrar que la luz es una onda. El experimento que devisó, llamado el experimento de dos ranuras, ha sido utilizado en otras áreas para demostrar la naturaleza de ondas de muchos otros fenómenos físicos, así que es instructivo repasar su confección.

En el experimento, una fuente de luz es ubicada en un cuarto oscuro, el cual se encuentra totalmente dividido por una pantalla. Del otro lado de la pantalla se encuentra una pared con un material fotosensible. La luz no puede atravesar la pantalla y afectar la pared, así que abrimos (con un cuchillo) una ranura delgada y vertical en la pantalla. Si observamos el patrón generado por la luz que atraviesa la ranura y marca la pared, podremos ver que el efecto es una gradación continua de claro a oscuro, con la mayor concentración de claro inmediatamente detrás del punto donde se ha efectuado la ranura en linea directa con la fuente de luz. Sin embargo, si efectuamos otra ranura paralela a la anterior en la pantalla, el patrón generado en la pared ahora es una secuencia de rayas verticales. El razonamiento detrás del experimento es que este tipo de patrón *solo se puede explicar si consideramos que la luz se propaga mediante ondas y que son las ondas que pasan por cada una de las ranuras las que estan efectuando interferencia entre ellas.*

Si bien no existe nada extraño en decir que la luz está conformada por ondas, hoy sabemos que también esta conformada por partículas, y cuando Young efectuó su experimento ya existía evidencia que la luz se propaga mediante partículas. Más aún, lo extraño del caso es que si la fuente de luz

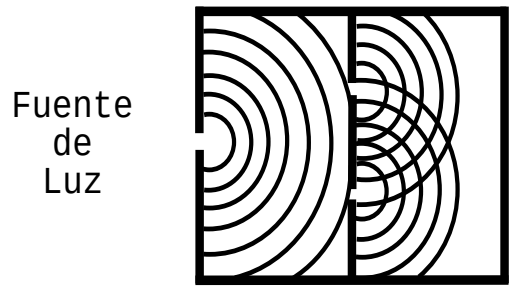


Figure 1.1: Experimento de las 2 ranuras, el patrón de interferencia generado por la luz se puede explicar suponiendo que la luz se propaga mediante ondas

se reduce lo suficiente como para que emita solo un fotón a la vez, y se expone el material fotosensible por suficiente tiempo, el patrón de interferencia sigue existiendo, y cabe la pregunta ¿con quién está interfiriendo el fotón? No queda más que concluir que el fotón está interfiriendo consigo mismo! Pero aquí no termina la paradoja. Puede ser que especulemos que el fotón, por alguna razón, está pasando por ambas ranuras al mismo tiempo, así que ubicamos un detector de fotones en ambas ranuras para saber por cuál ranura está pasando el fotón. Los resultados de este experimento indican que el fotón pasa por solo una ranura, pero también se produce una consecuencia extraña: el patrón de interferencia desaparece y la imagen en el material fotosensible es concordante con el modelo de luz transmitida mediante partículas. En otras palabras, el patrón de interferencia solo existe cuando no sabemos por cuál ranura pasó el fotón, o bien, cuando el fotón *podría haber pasado* por cualquier ranura. Una vez que sabemos que el fotón pasó por una ranura y por la otra no, el patrón de interferencia desaparece[1].

En este experimento encontramos gran cantidad de las paradojas planteadas por la física subatómica a la física clásica y que conllevaron al desarrollo de la mecánica cuántica: la dualidad onda-partícula, la interferencia no-local, y la imposibilidad de observar un estado subatómico sin interferir en él. Éstas paradojas requirieron más de un siglo para ser resueltas, y aún más, para que sus respuestas puedan ser digeridas por la comunidad científica en general.

[1]En honor a la verdad, todas estas conclusiones no fueron obvias cuando Young efectuó su experimento; algunos de ellos se han hecho con electrones, y solo hasta 1974. Para una exposición web del experimento puede verse http://www.colorado.edu/physycs/2000/schoedinger/two-slit2.html

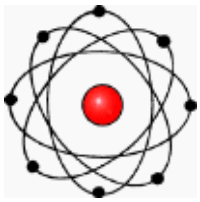


Figure 1.2: El modelo planetario del átomo de Rutherford

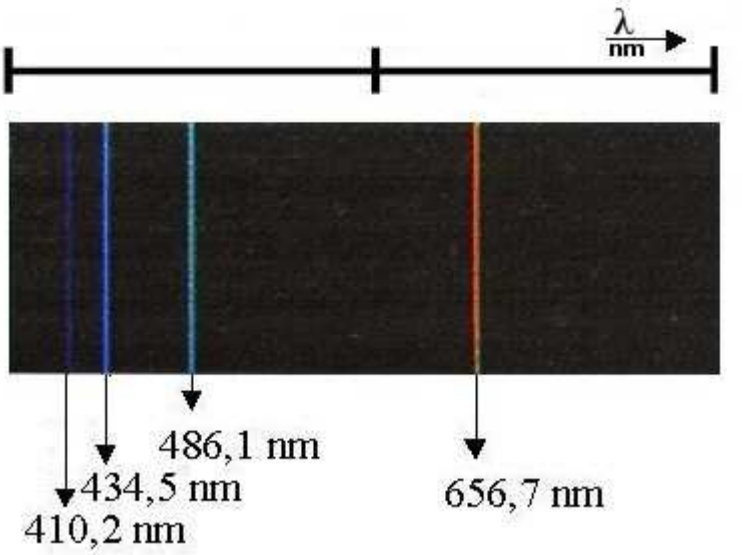


Figure 1.3: Espectro de luz del átomo de Hidrógeno

1.1 Max Karl Ernst Ludwig Planck (1858-1947) y la noción de Quantum

La primer pieza del rompecabezas está en el trabajo de Max Planck. Planck entra a trabajar en la Universidad de Berlín en 1889 como reemplazo de su antiguo maestro Kirchhoff, quien recientemente habia muerto, y se mantuvo ahí hasta su retiro en 1926. Poco después de su ingreso, Plack se interesa por el problema del cuerpo negro, inicialmente planteado por Kirchhoff. En este problema se contempla las propiedades de un cuerpo que absorbe todas las frecuencias de luz y que entonces, cuando es calentado, debería irradiar todas las frecuencias de luz.

Pero el problema es que la cantidad de altas frecuencias en el espectro es mayor que la cantidad de bajas frecuencias. Si un cuerpo negro irradiara todas las frecuencias electromagnéticas uniformemente entonces casi toda la energía se irradiaría en el espectro de altas frecuencias (algo así como pedir un número aleatorio uniformemente distribuido entre cero y 1,000,000). Este problema de las altas frecuencias es conocido como la *catástrofe violeta* por el color que tienen las frecuencias más altas de la luz.

En la vida real esto no sucede, y los modelos continuos de la física clásica de finales del siglo pasado no podían explicarlo. Tanto Wien como Rayleigh tenían aproximaciones del problema; las ecuaciones de Wien funcionaban bien para frecuencias altas pero no en las bajas, las de Rayleigh hacian lo inverso.

En 1900, Planck desarrolló una ecuación relativamente sencilla que describía a cabalidad la radiación emitida por un cuerpo negro en todo el espectro de luz. Su ecuación se basaba en una suposición medular: la energía no es infinitamente divisible, sino que al igual que la materia, se componía de partículas, las cuales Planck denominó *quanta* (de la palabra en Latin para *¿cuanto?*) o bien, *quantum* en singular.

Bajo la suposición de que la energía solo puede ser absorbida y despedida en unidades enteras de *quanta*, Plack fue capaz de encontrar las ecuaciones del cuerpo negro y establecer el valor de la constante que determina la razón entre la frecuencia de radiación y el tamaño del cuantum $h = 6.6262 \times 10^{-34}$ ahora considerada una de las constantes fundamentales de la naturaleza.

El concepto de quanta era tan revolucionario, que el mismo Plack no podía aceptarlo completamente. Einstein lo utilizó para explicar el efecto fotoeléctrico y ambos recibieron premios Nobel por sus trabajos, pero curiosamente ambos se reusaban a aceptar los cuanta como entidades reales y se abogaron a tratar de explicarlos mediante modelos clásicos.

1.2 Niels Henrik David Bohr (1885-1962)

El siguiente paso importante fue dado por Niels Bohr. Bohr entra en la Universidad de Copenhagen en 1903 y, según cuentan, era un crack para jugar al fútbol (su hermano menor era aún mejor y logró medalla de plata en 1908 con el equipo olímpico Danés). Bohr obtuvo un doctorado en 1911 y con una beca se fue a profundizar su educación en Cambridge bajo la tutela de J. J. Thomson, y luego a Manchester, con Rutherford.

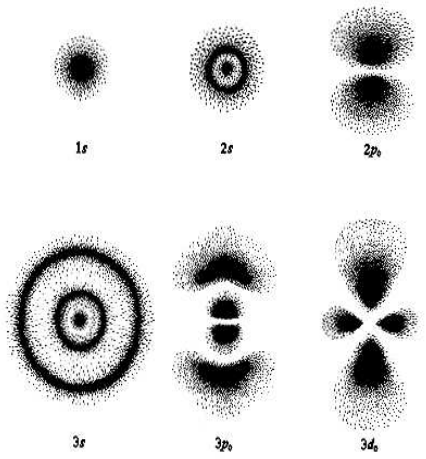


Figure 6-12. Probability density plots of some hydrogen atomic orbitals. The density of the dots represents the probability of finding the electron in that region.

Figure 1.4: Modelo de átomo de Bohr, Tomado de Internet, sin su permiso

Rutherford había planteado el modelo planetario del átomo con un pequeño núcleo rodeado de una nube de electrones. Bohr especulaba que si se unía el modelo planetario de Rutherford con el concepto de quanta de Plack, entonces podría ser posible explicar cómo las sustancias emitían y absorbían energía radiante. Estas emisiones y absorciones se sabía que eran responsables de las extrañas líneas encontradas en el espectro de los elementos descubiertas por Fraunhofer un siglo antes.

Bohr empezó estudiando el átomo de hidrógeno. Lorentz había sugerido que las radiaciones provenían de la oscilación del electrón en la órbita del átomo de hidrógeno, y que las radiaciones se efectuaban cuando la carga eléctrica del electrón se aceleraba o desaceleraba. Bohr por el contrario, propuso que el átomo no irradiaba mientras el electrón se mantuviera en órbita, sino más bien, cuando este cambiaba de órbita y que estas órbitas solo se dan en puntos discretos.

La propuesta de Bohr por si misma no resolvió todos los interrogantes, pero fue suficiente para girar la física subatómica en la dirección cuántica. Bohr había propuesto solo órbitas circulares, pero Sommerfeld desarrolló las ecuaciones para orbitas elípticas también. Bohr no había podido desarrollar modelos para átomos más complejos que el hidrógeno pero había sugerido

que las órbitas de los electrones debían existir en capas, una noción que Pauli logró formalizar.

Bohr publicó sus resultados en la edición de Julio de 1913 de *Philosophical Magazine*. Las nociones de Bohr contaron con una enorme oposición. Bohr había sustituido la mecánica clásica por un modelo 4-dimensional, nada fácil de digerir y que contradecia los modelos clásicos conocidos.

Sin embargo, la teoría de Bohr tenía enormes atractivos ya que:

1. Su concordancia con los datos encontrados en el espectro del átomo de hidrógeno era increíble.

2. Proveía una explicación teórica de las fórmulas empíricas y las constantes que se habían elaborado previamente.

Eventualmente, Bohr ganó la contienda y recibió el premio Nobel de 1922 por este trabajo. Elogios sobre la genialidad de Bohr en proponer y elaborar su teoría abundan. Einstein, en sus notas autobiográficas de 1948, se asombra de cómo datos contradictorios y nada claros sobre el espectro del átomo de hidrógeno, le permiten a Bohr deducir las características del átomo y sus órbitas, conjunto con el papel que éstas juegan en las propiedades de los elementos.

De aqui en adelante la mecánica cuántica se desarrolla muy rápidamente. Hasta este momento la mecánica cuántica utilizaba espacio euclideo y tensores cartesianos. En 1924 Satyendra Nath Bose propone que las partículas en si no son las que se conservan, sin mas bien la independencia estadística de las partículas. Louis de Broglie en su trabajo Doctoral extiende la dualidad onda–partícula de los fotones a todas las partículas. En 1926 Schrödinger publica un artículo con sus ecuaciones para el átomo de hidrógeno e introduce la mecánica de ondas. En el mismo año Dirac resuelve las ecuaciones de las leyes estipuladas por Planck. En 1927 Heisenberg propone su principio de incertidumbre, Heisemberg utiliza una mecánica de matrices que rivaliza con la mecánica de ondas de Schrödinger. En 1932 von Neumann formaliza la teoría utilizando álgebra de operadores.

1.3 Alan Turing (1912–1954) y la Computabilidad

Pero ¿qué tiene que ver toda esta historia de la física con la computación? Para ello conviene dar un giro en el relato y recordar la memoria de Alan Turing. Alan Mathison Turing, nace en Padington Inglaterra el 23 de Junio de 1912. Segundo y último hijo de Julius Mathison y Ethel Sara Turing, en un hogar inglés de clase media alta. Desde joven muestra características excéntricas, solitarias, y geniales. Turing estudia en el King's College de Cambridge. Para 1933 Turing había desarrollado interés en la *Principia Mathematica* de Russell y Whitehead. En ella Bertrand Russel había ideado un programa para contestar una de las preguntas propuestas por Hilbert a inicios del siglo como reto a la matemática: formalizar todo el conocimiento matemático existente dentro de la lógica. Sin embargo, el objetivo de esta empresa fue burlado por Kurt Gödel cuando demostró en 1931 que todo sistema formal (en particular la lógica) es incompleto: para todo sistema formal, existen verdades que son imposibles de expresar en él.[2]

En 1935 en una exposición del topólogo M. H. A. Newman, Turing se enteró que existían otras preguntas planteadas por Hilbert que aún no tenían respuesta, en particular se interesó por el problema de la decidibilidad, o bien el *Entscheidungsproblem*, esto es: ¿Existe un método por el cual se logre determinar para cualquier afirmación matemática X si ésta es decidible o no?

Para contestar esta pregunta, Turing desarrolló una teoría totalmente novedosa y original. Sin basarse en ningún otro resultado matemático, desarrolló la noción de máquina de Turing y a partir de ésta pudo definir con precisión el concepto de algoritmo. Dentro de su modelo podían exis-

[2]Este resultado se ha utilizado por algunos para afirmar que la verdad es más grande que la lógica, y que por lo tanto no debe ser analizada. Nótese, sin embargo, que la verdad inexpresable de Gödel no es universal, sino mas bien particular al sistema formal utilizado (dado un sistema formal X, existe una verdad Y que no se puede expresar en X, llamada su cláusula G). El teorema de Gödel no conduce, como han tratado de extrapolar algunos, a que existen verdades ilógicas, o bien, que la verdad no se debe analizar con el ojo crítico de la lógica. Todo pensamiento ilógico es falso, ya que conduce a contradicción, así que la lógica no pierde, por el teorema de Gödel, la facultad de falsificar teorías carentes de fundamento. Las verdades apuntadas por Gödel, no pueden ser expresadas en el formalismo matemático escogido, y sin embargo son evidentes. Esto no ha de confundirse con ciertos pensamientos fundamentalistas, que apelan a la "*autoevidencia*" de la verdad, y utilizan esta presuposición para impedir el análisis lógico de su cosmología.

tir un sin fin de máquinas distintas, pero la complejidad de este problema quedó resuelta gracias al concepto de *máquina universal de Turing*. Turing argumenta convincentemente, que todas las máquinas capaces de efectuar cómputos son *polinomialmente* equivalentes a una máquina universal de Turing. Armado con estas herramientas, Turing contestó negativamente el Entscheidungsproblem planteado por Hilbert: no existe un procedimiento que pueda determinar la decidibilidad de cualquier afirmación.

Lamentablemente para Turing, poco antes de publicar sus resultados, el Logicista Alonzo Church logró resolver el mismo problema utilizando formalismos de la lógica matemática, y la tesis de que todas las máquinas capaces de efectuar cómputos son polinomialmente equivalentes llego a conocerse como la Tesis Church–Turing.

Dentro del campo de la computación, sin embargo, Turing cuenta hoy con mucho mayor peso que Church. Entre los motivos que hacen que el enfoque de Turing sea más atractivo son:

1. La propuesta de Turing es fresca y no requiere de ningún conocimiento previo de lógica o matemática.

2. La propuesta de Turing es constructiva. Turing diseña y analiza una máquina que es *mecánica* y físicamente realizable.

Lo que no es inmediatamente obvio de esta propuesta, y no lo fue por muchos años, es que Turing amarra la noción de computabilidad con las propiedades de la física clásica. En retrospectiva, es claro que las máquinas analizadas por Turing dependían fuertemente de sus propiedades físicas. Entre ellas están:

- *Principio de Localidad*: Los eventos no tienen repercusiones a la distancia, todo sucede en un punto y se propaga a partir de ese momento hacia otros puntos próximos a través del tiempo.

- *Principio de Unicidad*: Un sistema solo puede estar en un estado a la vez, no puede estar en la superposición de dos estados al mismo tiempo.

- *Principio de Objetividad*: Un observador puede consultar el estado completo de un sistema sin interferir en él.

Estas tres propiedes, aunque parecen evidentes[3], no son ciertas en la mecánica

[3]El que parezcan evidentes, nos hace cuestionar qué tan íntimamente ligados están la lógica con la física clásica, un tema que por si mismo, es digno de contemplación

cuántica. Entonces, cabe preguntarse: ¿Es cierta la tesis de Church–Turing para sistemas cuánticos?

1.4 Hacia una interpretación física de la computabilidad

Que la computabilidad y la información están íntimamente ligadas con la física, es algo de lo cual se ha ido cobrado conciencia lentamente. Claude E. Shannon desarrolla en 1948 su teoría de la información en su artículo *A Mathematical Theory of Communication*, y liga el concepto de información con las propiedades físicas de la entropía[4]. Rolf Lauder, estipula su principio en 1961 de que la *eliminación* de información es un proceso disipador (consume energía). Por el contrario, en 1973 Charles Bennet demostró que cualquier cómputo (exepto el borrado) se puede efectuar con base en operaciones reversibles, lo cual indica que en principio, mientras no se efectúe eliminación de información en una computadora, no es necesario que exista disipación o consumo de energía.

Las conclusiones de Bennet y Lauder permitieron a Bennet en 1982 conciliar la paradoja del demonio de Maxwell con la segunda ley de la termodinámica. En la paradoja del demonio de Maxwell, el demonio es un observador insigne que vigila las moléculas que transitan por la única entrada de un cuarto totalmente cerrado. El demonio de Maxwell observa la velocidad de la molécula y si ésta está por debajo de un cierto umbral, la deja entrar al cuarto, de lo contrario la rebota y le impide su ingreso. De la misma manera, el demonio de Maxwell permite salir del cuarto sólo moléculas con una velocidad superior al umbral. La segunda ley de termodinámica mantiene que en todo sistema físico cerrado la entropía aumenta conforme avanza el tiempo. Si suponemos, lo cual es posible, que la medición de la velocidad de la molécula se lleva a cabo sin gastar o disipar energía (utilizando la misma energía de la molécula, por ejemplo), y que el proceso de obstaculizar el paso de la molécula puede en principio gastar menos energía que la que tiene la molécula, el demonio de Maxwell estaría disminuyendo el nivel de entropía del cuarto (enfriándolo) sin generar ningún tipo de calor. La respuesta que

[4]Dicen que Von Neumann, conociendo la propuesta de Shannon antes de ser impresa, le aconsejo que la llamara entropía porque, en sus propias palabras: "Nadie sabe bien lo que significa la entropía, así que en una discusión siembre vas a tener la ventaja".

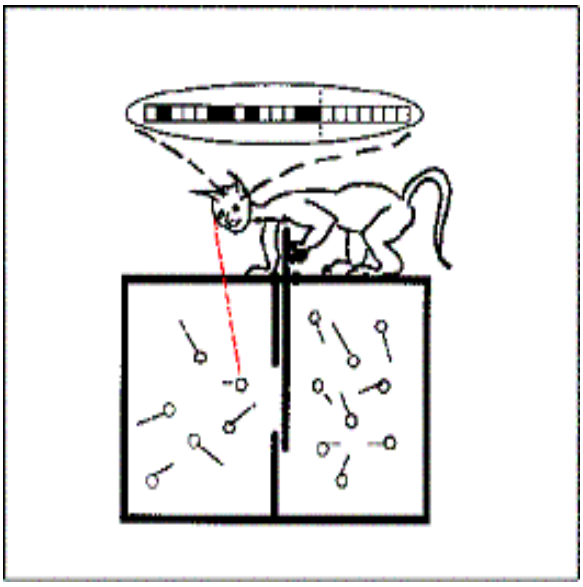


Figure 1.5: Demonio de Maxwell separando las moléculas calientes de las frias, el demonio se ve obligado a almacenar información sobre las moléculas

da Bennet a esta paradoja es que, si bien es posible que el demonio enfríe el cuarto, en el proceso de hacerlo está registrando información sobre las moléculas, si suponemos que la memoria del demonio es finita, eventualmente tendrá que borrar la información que guardó y es en ese momento que consume energía y por tanto aumenta el nivel de entropía del sistema.

Lo interesante del caso es que, si bien la entropía de información y la entropía física no son lo mismo, en este experimento mental del demonio de Maxwell existe una correspondencia y *preservación* entre ellas. La memoria del demonio inicia en blanco y por lo tanto con entropía cero. Conforme el demonio va obteniendo información de las moléculas, graba la información en su memoria y aumenta la entropía de ésta. El demonio de Maxwell reduce la entropía del sistema físico, pero en el proceso aumenta la entropia de su información. Cuando su memoria se encuentra saturada, se ve obligado borrarla, reduciendo la entropía de su información pero disipando energía y así aumentando la entropía física. La entropía física se transforma en entropía de información y vice-versa.

1.5 Inicios de la Computación Cuántica

La moraleja de todo esto es que la información y la computación son procesos físicos, y si este es el caso, entonces es de esperar que la naturaleza radicalmente distinta de los sistemas cuánticos afecten los tipos de cómputos que podamos efectuar con ellos.

Richard Feynman en 1982 se interesa por una pregunta relacionada. Su interrogante era ¿será posible simular un proceso cuántico en un computador convencional? Para entender esta pregunta necesitamos desarrollar un poco de notación.

En un computador convencional, la unidad mínima de información es el *bit* el cual puede estar en alguno (pero no ambos) de dos estados posibles 0 o 1. Por el contrario, en un computador cuántico, la unidad mínima de información es el *qubit*. Matemáticamente, el qubit es representado por un vector normalizado de dos dimensiones en un espacio complejo, en notación de *dirac* el qubit se representa como $|\psi\rangle$ donde

$$|\psi\rangle \in \mathrm{C}^2$$

Ya que nos interesa representar información binaria, podemos denominar a los vectores de una base arbitraria de C^2 como $|0\rangle$ y $|1\rangle$. Es común, aunque no necesario, que $|0\rangle$ y $|1\rangle$ correspondan a la base canónica en C^2 esto es

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

Entonces la representación de $|\psi\rangle$ en esta base está dada por

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

donde se cumple que

$$|\alpha|^2 + |\beta|^2 = 1$$

Cuando leemos el estado de un qubit mediante un operador de lectura, lo único que podremos leer es alguno de los estados clásicos $|0\rangle$ o $|1\rangle$. Sin embargo, el qubit puede estar en un estado superpuesto entre $|0\rangle$ y $|1\rangle$. Cuando este es el caso, el coeficiente $|\alpha|^2$ corresponde a la probabilidad de leer un $|0\rangle$ mientras que el coeficiente $|\beta|^2$ corresponde a la probabilidad de leer un $|1\rangle$ del qubit. Por este motivo los coeficientes α y β se les llama amplitudes de probabilidad.

Una posible implementación física de un qubit es utilizando fotones de luz. Supongamos que tenemos una pistola de fotones capaz de lanzar uno a uno fotones con polarización arbitraria, y convenimos que fotones con polarización horizontal corresponden a un $|0\rangle$ mientras que fotones con polarización vertical corresponden a un $|1\rangle$[5]. Para establecer comunicación sincrónica entre dos puntos A y B con linea de vista, basta con lanzar fotones polarizados bajo el esquema anterior del punto A y poner un vidrio polarizado verticalmente en el punto receptor B. Si el fotón pasa a través del vidrio polarizado, sabemos que es un $|1\rangle$, de lo contrario el fotón representa un $|0\rangle$.

Claro está, nada impide que mandemos un fotón polarizado en un ángulo de 45^o. En este caso el resultado es que aleatoriamente los fotones pasan la pantalla polarizada verticalmente un 50% de las veces. Más aún, el vidrio polarizado altera irremediablemente la polarización del fotón y la colapsa a una polarización vertical tal que, si ponemos otro vidrio polarizado verticalmente detrás de éste, el 100% de los fotones que pasaron el primer vidrio pasarán el segundo (otro ejemplo de que la lectura de información cuántica altera el contenido de esta información).

Nótese que la información que obtenemos del sistema cuántico es binaria (el fotón pasa o no), pero el estado cuántico es continuo (en este caso, un ángulo de polarización $\theta \in [0, 2\pi]$)

Podríamos argumentar que un computador convencional también contiene un estado interno que es básicamente continuo y que nosotros escojemos interpretar estos estados como valores binarios, así las cosas tenemos varias opciones:

1. Los qubits se pueden simular mediante un computador convencional.

2. Los qubits solo agregan ruido al proceso y son equivalente a voltajes en un computador analógico.

3. Los qubits no se pueden simular mediante un computador convencional.

Feynman entonces continúa con el modelo de una memoria cuántica conformada por N qubits. Resulta ser que para representar los N qubits no basta con saber el estado de cada qubit por separado. Dada una memoria

[5]Es mas común en este esquema utilizar el spin de la partícula para representar el valor del qubit; pero aquí, por motivos de ilustración, utilizaremos el concepto más intuitivo de polarización

de cinco qubits, por ejemplo, esta puede estar en el estado

$$b_0 = |0\rangle,\ b_1 = |1\rangle,\ b_2 = |1\rangle,\ b_3 = |0\rangle,\ b_4 = |1\rangle$$

Lo que se puede abreviar como

$$|0\rangle|1\rangle|1\rangle|0\rangle|1\rangle = |01101\rangle = |13\rangle$$

pero así como un qubit puede estar en la superposición de $|0\rangle$ y $|1\rangle$, esta memoria de cinco qubits también puede estar en cualquier superposición de los posibles $2^N = 32$ estados. La fórmula que expresa el estado más general de esta memoria cuántica es

$$\sum_{i=0}^{2^N-1} \alpha_i |i\rangle \tag{1.1}$$

donde

$$\sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1$$

Nótese que la expresión de este estado requiere de una cantidad exponencial (con respecto al número de qubits en la máquina) de coeficientes complejos. Si queremos simular una memoria cuántica de 1K qubits, entonces ocuparíamos ¡2^{1024} coeficientes complejos! suma obviamente imposible (2^{70} ya está cerca de la cantidad de átomos que se encuentran en el universo conocido).

Aún todavía, podemos argumentar que estos coeficientes puede que no sean necesarios para lograr la simulación, ya que lo que nos interesa realmente es el resultado leído de la memoria cuántica despues de un cómputo. Pero este planteamiento es equivalente a la suposición de variable escondida que tanto buscó Einstein, y que John Bell demuestra en 1964 que es falsa: *no existe ningún algoritmo local probabilístico que pueda reproducir los estados de un sistema cuántico arbitrario.* Por lo tanto, a menos que encontremos una forma de hacer cómputos en espacio exponencial EXPSPACE, es probable que estados cuánticos complejos no sean viables de simular en un computador convencional.

1.5.1 El algoritmo de Shor

La pregunta que Feynman dejó sin contestar, es si ésta complejidad cuántica puede servir de algo computacionalmente, porque al fin y al cabo, la complejidad se encuentra en las amplitudes de probabilidad que determinan el

estado del sistema cuántico, valores que no pueden ser leídos. Esta pregunta fue contestada con un rotundo SI cuando Peter Shor, de los laboratorios de AT&T demostró en 1994 que, en principio, un computador cuántico puede factorizar un número eficientemente.

El algoritmo de Shor se convirtio rápidamente en la *killer application* de la computación cuántica. La factorización de números tiene la propiedad de que es fácil verificar si dos numeros p y q dividen a m, pero si solo conocemos m, es muy difícil encontrar p y q. Es ampliamente considerado (aunque no ha si demostrado) que la factorización de números en sus factores primos es *superpolinomial* en $\log(n)$. El algoritmo más rápido que se conoce ejecuta en tiempo

$$\text{tiempo} \simeq e^{[c(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}]}$$

donde $c = \left(\frac{64}{9}\right)^{\frac{1}{3}} \sim 1.9$. debido a esta dificultad, muchos esquemas de encriptamiento tales como el RSA y el encriptamiento con llave pública, se basan en la factorización de números para protejer la información.

El algoritmo de Shor, por el contrario, es capaz de encontrar los factores primos de un número arbitrario n en tiempo $O[(\ln n)^3]$. esto significa que cómputos que antes se consideraban imposibles ahora podrían calcularse en cuestión de dias. El algoritmo de Shor pone en peligro los actuales esquemas de seguridad utilizados en Internet.

1.6 Presente y futuro de la computación cuántica

El algoritmo de Shor, sin embargo, es un conjunto de ecuaciones sobre el papel, y es válido preguntarse si sus esquemas son implementables. La situación de la computación cuántica es, hoy en dia, similar a la que en algún momento se encontró Charles Babbage con su *motor analítico*: se sabe a cabalidad como implementarlo pero se carece de la tecnología necesaria para hacerlo una realidad. Algunos expertos son más pesimistas y consideran que la computación cuántica jamás sera una realidad. Se basan en el hecho que los algoritmos cuánticos tales como el de Shor utilizan una propiedad de los sitemas cuánticos llamada *superposición* (entanglement), éstos estados superpuestos son sumamente inestables[6] y rápidamente decaen (a este fenómeno

[6]la inestabilidad de los estados superpuestos se ha utilizado para contestar la paradoja del gato de Schrödinger. Bajo la teoría de la mecánica cuántica es posible que exista

se le llama *decoherencia*). Hasta la fecha solo ha sido posible crear la superposición de tres qubits a la vez, mucho menos un sistema tan complejo como un computador (o un gato).

Es importante notar que un sistema cuántico es analógico determinístico (dada la equación 1.1) pero que lo que podemos observar (medir) de él siempre es discreto probabilístico. Este hecho sumado al fenómeno de la decoherencia hace que los sistemas cuánticos esten perenemente propensos a errores. Pero estos obstáculos no han desalentado la investigación en computación cuática, por el contrario, en los últimos 10 años el reconocimiento de este problema ha propiciado el desarrollo de la *Teoría de Información Cuántica* y de los códigos de detección y recuperación de errores cuánticos. La idea fundamental aquí es utilizar redundancia para garantizar que las compuertas cuánticas nos generen los resultados deseados. Hoy se cuenta con resultados teóricos que ponen cotas inferiores realistas a la precisión que deben tener las compuertas cuánticas para que las computadoras cuánticas sean una realidad. El gobierno Norteamericano, con el objetivo de acelerar el proceso, ha creado el *Quantum Computing Roadmap*: un plan de investigación cuyo objetivo es tener un conjunto de herramientas funcionando para el 2012 que conformen la base de pruebas (*test bed*) de la computación cuántica. El Quantum Insititute edita un documento anual que elabora un diagnóstico del avance en la computación cuántica, este documento se puede encontrar en http://qist.lanl.gov/. El roadmap identifica los siguientes retos tecnológicos que necesitan ser atacados para construir un computador cuántico.

- **Almacenamiento** : guardar qubits por cantidades largas de tiempo.
- **Aislamiento** : aislar qubits del ambiente para reducir el efecto de decoherencia.
- **Lectura** : medir qubits confiablemente.
- **Compuertas** : manipular y operar con los qubits individual y colectivamente.

un gato en un estado superpuesto $|gato\rangle = \frac{1}{\sqrt{2}}(|vivo\rangle + |muerto\rangle)$. Pero este estado es sumamente improbable, la incapacidad de aislar el gato de su contexto hace que el gato constantemente se encuentre *medido* por su ambiente, efectivamente eliminando la superposición de estados

- **Precisión** : la precisión de los qubits debe ser la suficiente para efectuar cómputos confiablemente.

Las tecnologías de Trampa de Iones, *Cavity QED*, resonancia magnética nuclear (NMR) y sistemas ópticos se identifican como las más promisorias para resolver estos problemas, sin descartar la posibilidad que una nueva tecnología surja que pueda mejorar el estado del arte en la manipulación de qubits.

1.7 El protocolo BB84

Parar terminar esta breve introducción discutiremos el protocolo de encriptamiento BB84, el cual esta al alcance de la tecnología actual y ofrece la posibilidad de establecer comunicaciones punto a punto cien por ciento seguras.

Supongamos que Alice desea enviar un mensaje a Bob y quiere eliminar toda posibilidad de que Eve se entere del contenido del mensaje. Supongamos también que esto sucede en el año 2020, asi que Eve cuenta con una palm pilot cuántica que le permite descifrar llaves basadas en protocols RSA y de llave pública. El mensaje m de Alice mide N bits y esto se lo comunica a Bob mediante un canal convencional. Alice y Bob disponen también de un canal cuántico, que por motivos de ilustración, supondremos que es una pistola de fotones polarizados tal y como se presentó en la sección 1.5 utilizando linea de vista o una fibra óptica[7]. Alice decide enviar $4N$ bits por el canal cuántico. Pero Alice también decide utilizar dos maneras distintas para representar los valores de $|0\rangle$ y $|1\rangle$ por este canal.

Utiliza la base canónica con fotones polarizados verticalmente para representar un $|1\rangle$ y horizontalmente para representar un $|0\rangle$. Pero también utiliza una base transversal, utilizando una polarización de 45^o para representar un $|0'\rangle$ y de 135^o para representar un $|1'\rangle$. Matemáticamente esto lo expresamos

[7]La calidad de la fibra óptica actual permite enviar fotones sin que estos reboten en la pared de la fibra, de este modo la polarización o spin del fotón se conserva hasta que la fibra necesite de una repetidora

como

$$|0\rangle \stackrel{def}{=} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{1.2}$$

$$|1\rangle \stackrel{def}{=} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.3}$$

$$|0'\rangle \stackrel{def}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.4}$$

$$|1'\rangle \stackrel{def}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.5}$$

Alice decide enviar los $4N$ qubits por el canal cuántico de la siguiente manera: escoje aleatoriamente la base con que va a enviar el qubit, luego escoje aleatoriamente el valor del qubit (0 ó 1), lo envia y repite el proceso para todos los $4N$ qubits. Bob desconoce en cual base esta enviando Alice cada uno de los qubits, asi que Bob decide que lo mejor es escojer aleatoriamente una base, orientar su vidrio polarizado para leer un qubit en esa base y leer el qubit cruzando los dedos de que la base que escojio haya sido la correcta. Bob obtiene el valor binario correcto si la base que Bob escoje coincide con la base en que fue enviada el qubit; si por el contrario, Bob escoje la base equivocada entonces el bit que Bob recibe es *totalmente* aleatorio.

Una vez enviados los $4N$ qubits Alice y Bob se comunican por el canal convencional y comparten la información de *las bases* que utilizaron para enviar/leer los qubits. En este momento tanto Alice como Bob saben cuales fueron los qubits que fueron enviados y leidos en la misma base, así que en buena teoría todos estos qubits deben ser equivalentes. Estos bits compartidos suman mas o menos $2N$ en total, Alice selecciona al azar N bits de estos, le comunica a Bob cuales fueron los escojidos (por posición y no por valor). Con estos bits tanto Alice como Bob construyen una llave k de N bits. Por el canal convencional Alice manda su mensaje m cifrado tal que para cada bit $m[i]$ de m Alice envia $m[i] \oplus k[i]$. Bob utiliza su llave k para extraer el valor de m.

¿Qué sucede entonces, si Eve trata de escuchar la comunicación entre Alice y Bob? Eve tiene completo acceso al canal convencional pero debe estar claro que Eve no podrá leer nada de este canal si desconoce la llave k que compartieron Alice y Bob por el canal cuántico. Pero si Eve trata de leer el canal cuántico se encontrará en las mismas condiciones que Bob: va a tener que escojer aleatoriamente una base y esperar que sea la base correcta.

Cuando Alice y Bob intercambian bases Eve puede corroborar cuales qubits leyó y retransmitió correctamente. Las probabilidades indican que de los $2N$ qubits que Alice y Bob coinciden en base, Eve solo haya leido y retransmitido correctamente la mitas (N qubits), y de estos Alice escoje al azar la mitad para formar parte de la llave k, asi que en términos generales lo mejor que puede esperar Eve es obtener con seguridad la mitad de los bits de la llave k (si escoje el resto al azar entoces su esperanza es obtener tres cuartas partes de la llave). Por otra parte, si Eve retransmite correctamente solo la mitad de los $2N$ bits en que coinciden en base Alice y Bob, Bob tendrá N bits correctos de los cuales Alice escoje la mitad para formar parte de la llave. De esta forma Bob también término con 3 cuartas partes de la llave k.

Lo que necesitan ahora Alice y Bob es un protocolo que les garantice que con tres cuartas partes de la llave no sea posible reconstruir el mensaje (algo no muy complicado). De esta forma si Bob recibe basura despues de decodificar el mensaje se dará cuenta que Eve ha estado escuchando la conversación pero tendrá seguridad de que Eve también recibió basura. Eve puede tratar de reducir sus probabilidades de ser detectada leyendo solo unos qubits y dejando pasar intactos otros, pero este esquema solo reduce la cantidad de la llave que logra obtener sin obtener ningún beneficio en la lectura del mensaje.

1.8 ejercicios

1. Encuentre errores en el texto anterior, haga un comentario de una página sobre la temática de este capítulo.

2. El principio de entropía indica que los sistemas tienden a desorganizarse ya que los estados desorganizados son mas probables (hay más de ellos) que los estados organizados. La evolución y los sistemas vivientes, por el contrario, tienden con el tiempo a desarrollar organizaciones cada vez más complejas. Algunas personas utilizan esta observación para argumentar que los sistemas vivos y la evolución contradicen la segunda ley de la termodinámica (entropía). ¿Esta usted de acuedo con esta opinión? ¿Si no es así, cómo es que la evolución se ajusta a la segunda ley de termodinámica?

3. También relacionado a la entropía, las teoriás del Big Bang indican que el universo empezó con una explosión el la masa y la energía estaban

bastante uniformemente distribuidas por todo el universo. ¿Es este un estado con mayor o menor entropía que el actual? ¿Cómo justifica la ciencia el aumento de complejidad en la organización de la materia?

4. El presente capítulo sugirió que los sistemas cuánticos tienen una complejidad computacional distinta a las máquinas de Turing. ¿Serán los sitemas cuánticos equivalentes a NP?

5. Un modelo de computación utilizado para ilustrar que los cómputos no necesariamente consumen energía es el modelo de computación con bolas de billar. Construya una trayectoria de bolas de billar que sirva para implementar la siguente compuerta lógica

A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

6. El protocolo BB84 presentado en este capítulo fue simplificado por motivos de exposición. ¿Encuentra usted alguna forma en que Eve pueda engañar a Alice y Bob dentro del esquema planteado y leer el mensaje sin que estos se den cuenta? ¿Cómo puede hacer para arreglar este problema?

Chapter 2

El Modelo Matemático

2.1 Espacios Vectoriales

Definición 2.1.1. Un *Grupo* G es un conjunto con un operador "$\cdot$" que cumple con:

1. *Asociatividad*: $\forall (a,b,c) \in G \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. *Elemento Neutro*: $\exists e \in G$ tal que $\forall a \in G \quad a \cdot e = e \cdot a = a$
3. *Inverso*: $\forall a \in G, \exists a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$

Definición 2.1.2. Un *Grupo Abeliano* G es un grupo que además cumple con tener conmutatividad.

$$\forall (a,b) \in G \quad a \cdot b = b \cdot a$$

Definición 2.1.3. Un *Campo* F es un conjunto dotado de dos operadores: suma y multiplicación, tal que:

1. La suma de F es un grupo abeliano con elemento neutro 0 e inversos $-a \; \forall a \in F$
2. La multiplicación de F es un grupo abeliano en $F - \{0\}$ con elemento neutro 1 e inversos $a^{-1} \; \forall a \in F - \{0\}$
3. Es *distributivo*: $\forall (a,b,c) \in F \quad a \cdot (b + c) = a \cdot b + a \cdot c$

Definición 2.1.4. Un *Espacio Vectorial* $\mathcal{A}$ tiene tres objetos:

1. Un grupo abeliano $(V, +)$ con elementos llamados *vectores* y cuya operación binaria "+" se le llama *suma*.

2. Un campo F de números (usualmente los números reales o los complejos) cuyos elementos se les llama *escalares*.

3. Una operación de *multiplicación con escalares* denotada por "$\cdot$":

$$\cdot : F \times V \to V$$

que cumple con las siguentes propiedades:

$$\begin{aligned} c \cdot (\alpha + \beta) &= c \cdot \alpha + c \cdot \beta && (2.1)\\ (c + c') \cdot \alpha &= c \cdot \alpha + c' \cdot \alpha && (2.2)\\ (c \cdot c') \cdot \alpha &= c \cdot (c' \cdot \alpha) && (2.3)\\ 1 \cdot \alpha &= \alpha && (2.4) \end{aligned}$$

para todo $c, c' \in F$ y $\alpha, \beta \in V$

Observación 2.1.1. El operador de "$\cdot$" para el campo F no es el mismo que para la operación con el espacio vectorial en el punto 3 de la definición anterior.

Observación 2.1.2. El operador de "+" para el campo F no es el mismo que para la operación del espacio vectorial en el punto 1 de la definición anterior.

Observación 2.1.3. Es común eliminar el uso del "$\cdot$" para denotar la multiplicación de un escalar por un vector y escribir $c\alpha$ en vez de $c \cdot \alpha$.

Definición 2.1.5. Un conjunto de vectores $v_i \in V$ con $i \in \{0, 1, \ldots n-1\}$ se le dice *linealmente independiente* si cumple con que $\forall (c_0, c_1, \ldots, c_{n-1}) \in F$

$$\left(\sum_{i=0}^{n-1} c_i v_i \right) = 0 \Longrightarrow c_i = 0 \quad \forall i \in \{0, 1, \ldots, n-1\}$$

Definición 2.1.6. Un conjunto de vectores $v_i \in V$ con $i \in \{0, 1, \ldots n-1\}$ se le dice *linealmente dependientes* si no son linealmente independientes

Definición 2.1.7. Un *subespacio* $\mathcal{S}$ de un espacio vectorial $\mathcal{A}$ es un subconjunto de $\mathcal{A}$ que cumple con que para todo $\alpha, \beta \in \mathcal{S}$ y $c \in F$

- $\alpha + \beta \in \mathcal{F}$

- $c\alpha \in \mathcal{F}$

Teorema 2.1.1. *Dado un un conjunto de k vectores $v_0, v_1, \ldots, v_{k-1}$. el conjunto de vectores formado por todas las posibles combinaciones lineales de los v_i conforma un subespacio vectorial.*

Teorema 2.1.2. *Dado un espacio vectorial $\mathcal{A}$, un subespacio $\mathcal{S}$ de $\mathcal{A}$, y un conjunto de k vectores $v_0, v_1, \ldots, v_{k-1}$. Si $\mathcal{S}$ contiene a todos los vectores v_i, entonces también contiene a toda combinación lineal de los vectores v_i*

Proof. Ejercicio □

Corolario 2.1.3 (2.1.2). *Dado un conjunto de k vectores $v_0, v_1, \ldots, v_{k-1}$. el espacio vectorial formado por la combinación lineal de estos vectores es el subespacio vectorial más pequeño que los contiene.*

Definición 2.1.8. Se llama *Base* de un espacio vectorial $\mathcal{A}$ a un conjunto de vectores v_i tales que:

- El espacio vectorial formado por las combinaciones lineales de los v_i es igual a $\mathcal{A}$.
- Los v_i son linealmente independientes.

Definición 2.1.9. Un espacio vetorial $\mathcal{A}$ es de *dimensión finita*, si existe una base de $\mathcal{A}$ que tiene una cantidad finita de elementos.

2.2 Espacios Vectoriales Reales n–dimensionales

Un espacio euclídeo es un espacio vectorial con dimensión finita en los números reales. En particular tenemos la siguiente definición.

Definición 2.2.1. Un espacio vectorial con vectores $v \in R^n$ se llama espacio euclídeo si para cada par de vectores $\alpha, \beta, \gamma \in R^n$ y $c \in R$ existe una operación llamada producto interno denotada por (α, β) que cumple con las siguentes propiedades

1. $(\alpha, \beta) = (\beta, \alpha)$
2. $(c\alpha, \beta) = c(\alpha, \beta)$
3. $(\alpha + \gamma, \beta) = (\alpha, \beta) + (\gamma, \beta)$

4. $(\alpha, \alpha) \geq 0$

5. $(\alpha, \alpha) = 0 \Leftrightarrow \alpha = 0$

Definición 2.2.2. El largo de un vector α en espacio euclídeo se denota por $|\alpha|$ y se define como

$$|\alpha| = \sqrt{(\alpha, \alpha)}$$

Teorema 2.2.1. *Dados dos vectores α y β en un espacio euclídeo. El* ángulo *ϕ entre los vectores es igual a*

$$\phi = \arccos\left[\frac{(\alpha, \beta)}{|\alpha||\beta|}\right] \longrightarrow \cos(\phi) = \frac{(\alpha, \beta)}{|\alpha||\beta|}$$

Proof. (Ejercicio). □

Definición 2.2.3. Dos vectores α y β se dicen *ortogonales* si $(\alpha, \beta) = 0$

Definición 2.2.4. n vectores $v_0, v_1, \ldots, v_{n-1}$ forman una *base ortogonal* de un espacio euclídeo n–dimensional si son ortogonales dos a dos.

Definición 2.2.5. n vectores $v_0, v_1, \ldots, v_{n-1}$ forman una *base ortonormal* de un espacio euclídeo n–dimensional si son una base ortogonal y $\forall v_i,\ |v_i| = 1$.

Observación 2.2.1. Es posible demostrar que todo espacio euclídeo de n–dimensiones posee bases ortogonales, dada una base ortogonal $v_0, v_1, \ldots v_{n-1}$, es posible expresar todo vector α como:

$$\alpha = a_0 v_0 + a_1 v_1 + \cdots + a_{n-1} v_{n-1}$$

Teorema 2.2.2. *Si $v_0, v_1, \ldots v_{n-1}$ es una base de un espacio euclídeo n–dimensional. y*

$$\alpha = a_0 v_0 + a_1 v_1 + \cdots + a_{n-1} v_{n-1}$$

Entonces se le llama proyección del vector *α al vector v_k de la base a*

$$(\alpha, v_k) = a_k$$

Proof. (Ejercicio) □

Teorema 2.2.3. *Si $v_0, v_1, \ldots v_{n-1}$ es una base de un espacio euclídeo n–dimensional. y*

$$\begin{aligned} \alpha &= a_0 v_0 + a_1 v_1 + \cdots + a_{n-1} v_{n-1} \\ \beta &= b_0 v_0 + b_1 v_1 + \cdots + b_{n-1} v_{n-1} \end{aligned}$$

Entonces

$$(\alpha, \beta) = \sum_{i=0}^{n-1} a_i b_i$$

Proof. (Ejercicio) □

Definición 2.2.6. Una *Transformación lineal* en un espacio euclídeo es una función A que cumple con

1. $A(\alpha + \beta) = A(\alpha) + A(\beta)$
2. $A(c\alpha) = cA(\alpha)$

Definición 2.2.7. Una función $B(;)$ de dos parámetros en un espacio vectorial se dice bilineal si

1. Para un β fijo, $B(\alpha, \beta)$ es una función lineal de α.
2. Para un α fijo, $B(\alpha, \beta)$ es una función lineal de β.

Observación 2.2.2. Una funcion bilineal B es simétrica si $B(\alpha, \beta) = B(\beta, \alpha)$. Un ejemplo de una función bilineal es el producto interno.

2.3 Operadores Lineales y Matrices

Definición 2.3.1. Una *matriz* $M = [a_{ij}]$ es un arreglo rectangular de elementos del campo F con n filas y m columnas

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}$$

Observación 2.3.1. Una matriz M de n filas y m columnas se puede interpretar como una transformación lineal de un espacio vectorial de m dimensiones a uno de n dimensiones. Si $n = m$ entonces M es una transformación lineal dentro del mismo espacio vectorial.

Definición 2.3.2. Una *matriz cuadrada* M es una matriz donde $n = m$.

Definición 2.3.3. La transpuesta de una matriz de n filas y m columnas $M = [a_{ij}]$ es una matriz M^T de m filas y n columnas

$$M^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{pmatrix}$$

Observación 2.3.2. Toda transformación lineal en un espacio vectorial se puede representar mediante una matriz. De aquí en adelante se hablará indistintamente de transformación lineal, matriz u operador.

Definición 2.3.4. El *espacio de filas* de una matriz M es el espacio generado por los n vectores fila de la matriz.

Definición 2.3.5. El *espacio de columnas* de una matriz M es el espacio vectorial generado por los m vectores columna de la matriz.

Definición 2.3.6. Una matriz $M = [a_{ik}]$ de n filas y m columnas, y otra matriz $N = [b_{kj}]$ de m *filas* y s columnas, se pueden multiplicar y dan como resultado una matriz $P = [p_{ij}]$ de n filas y s columnas tal que

$$p_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}$$

Definición 2.3.7. Las *operaciones elementates* sobre las filas de una matriz son

1. intercambiar dos filas de la matriz.
2. multiplicar el vector fila por un escalar c.
3. sumar el múltiplo de una fila i a una otra fila j.

Definición 2.3.8. Dos matrices son *equivalentes por filas* si se puede obtener una mediante operaciones elementales sobre la otra

Definición 2.3.9. Cuando $n = m$ se le llama la *matriz identidad* a la matriz $I = [a_{ij}]$ donde $a_{ij} = \delta_{ij}$ y δ_{ij} es la función Kronecker delta. Por ejemplo

$$I^6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Definición 2.3.10. Una *matriz de permutación* es una matriz identidad con las filas intercambiadas.

Definición 2.3.11. Una matriz M es *no singular* si sus filas o columnas son linealmente independientes.

Definición 2.3.12. El determinante de una matriz cuadrada $M = [a_{ij}]$ se define como

$$det(M) = |M| = \sum_{\Phi} \text{signo}(\Phi) a_{1,\phi_1} a_{2,\phi_2} \cdots a_{n,\phi_n}$$

donde Φ varía sobre todas las posibles permutaciones de los números del 1 al n y

$$\Phi = (\phi_1, \phi_2, \phi_3, \ldots, \phi_n)$$

además signo(ϕ) corresponde a la posición lexicográfica de la permutación, tal que las permutaciones pares tienen signo 1 y las impares tienen signo -1.

Observación 2.3.3. El determinante de una matriz $M = [a_{ij}]$ también se puede expresar como

$$\sum_{j=1}^{n} a_{ij} M_{ij}$$

Para i arbitrario y donde

$$M_{ij} = \frac{\partial |M|}{\partial a_{ij}}$$

Teorema 2.3.1. *Si N es el resultado de intercambiar dos filas de una matriz cuadrada $M = [a_{ij}]$, entonces*

$$|N| = -|M|$$

Teorema 2.3.2. *Si una matriz M tiene filas linealmente dependientes entre sí, entonces $|M| = 0$.*

Definición 2.3.13. Una matriz cuadrada es *triangular superior* si todas las entradas por debajo de la diagonal son iguales a 0.

Definición 2.3.14. Una matriz cuadrada es *triangular inferior* si todas las entradas por debajo de la diagonal son iguales a 0.

Definición 2.3.15. Una matriz cuadrada es *triangular* si es triangular superior o triangular inferior.

Teorema 2.3.3. *El determinante de una matriz triangular es la multiplicación de los elementos en su diagonal*

$$|M| = \prod_{i=1}^{n} a_{ii}$$

Teorema 2.3.4. *Una matriz M no singular tiene inversa M^{-1} tal que*

$$MM^{-1} = M^{-1}M = I$$

Definición 2.3.16. El *polinomio característico* de una matriz M es

$$c(\lambda) = |M - \lambda I|$$

Definición 2.3.17. El *trazo* de una matriz $M = [a_{ij}]$ es la suma de los elementos en su diagonal

$$Tr(M) = \sum_{i=1}^{n} a_{ii}$$

Teorema 2.3.5. *El trazo de una matriz cumple con que para toda matriz M y N*

1. $Tr(MN) = Tr(MN)$
2. $Tr(M + N) = Tr(M) + Tr(N)$
3. $Tr(cM) = cTr(M)$

2.4 Operadores Hermitios en espacio euclídeo complejo

Todas las definiciones y teoremas expuestos en las secciones anteriores son válidos en el campo de los números complejos. Definimos un número complejo como:

Definición 2.4.1. Un número *complejo* $\alpha \in C$ es un número de la forma

$$\alpha = a + bi$$

donde a y b son números reales y

$$i = \sqrt{-1}$$

Definición 2.4.2. Si $\alpha = a + bi$ es un número complejo, entonces se llama el conjugado de α al número complejo denotado por α^* igual a

$$\alpha^* = a - bi$$

Observación 2.4.1. Nótese que $\alpha\alpha^* = \alpha^*\alpha = a^2 + b^2 \geq 0$

La observación anterior nos permite definir un producto interno en los espacios vectoriales de números complejos con las siguientes características

Definición 2.4.3. Dados $\alpha \in C^n$ y $\beta \in C^n$ donde $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ y $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$. Se define el producto interno entre α y β como (α, β)

$$(\alpha, \beta) = \sum_{i=1}^{n} \alpha_i^* \beta_i$$

Teorema 2.4.1. *El producto interno en un espacio vectorial de números complejos cumple con que*

1. $(\alpha, \beta) = (\beta, \alpha)^*$
2. $(\alpha, \alpha) \geq 0$
3. $(\alpha, \alpha) = 0 \Longrightarrow \alpha = 0$

Observación 2.4.2. El producto interno nos permite definir una norma en el espacio vectorial n–dimensional de números complejos. El producto interno implica una norma, pero la norma no necesariamente implica un producto interno. Un espacio vectorial con solo norma se le llama un espacio de Banach. A los otros les llamaremos espacio de Hilbert.

Definición 2.4.4. Sea $A = [a_{ij}]$ una matriz de números complejos a_{ij}. Se define la matriz $A^* = [a^*_{ij}]$ como la matriz de los conjugados de los elementos de A

Definición 2.4.5. Sea $A = [a_{ij}]$ una matriz cuadrada de números complejos a_{ij}. Se define *la matriz adjunta* de A a la matriz $A^\dagger$ definida como $A^\dagger = (A^*)^T$ igual a

$$A^\dagger = \begin{pmatrix} a^*_{11} & a^*_{21} & \cdots & a^*_{n1} \\ a^*_{12} & a^*_{22} & \cdots & a^*_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a^*_{1n} & a^*_{2n} & \cdots & a^*_{nn} \end{pmatrix}$$

Teorema 2.4.2. *Para todas dos matrices A y S*

$$Tr(S^\dagger AS) = Tr(SAS^\dagger) = Tr(A)$$

Definición 2.4.6. Un operador A es *normal* si $A^\dagger A = AA^\dagger$

Definición 2.4.7. Un operador A es *Hermitio* si $A^\dagger = A$

Observación 2.4.3. Los operadores Hermitios tienen la propiedad de ser doblemente lineales con el producto interno en C^n. Es claro que si A es Hermitio entonces también es normal.

Definición 2.4.8. Una matriz U es unitaria si cumple que

$$UU^\dagger = U^\dagger U = I$$

Teorema 2.4.3. *Dado un operador unitatio U y vectores α, β*

$$(U\alpha, U\beta) = (\alpha, \beta)$$

o bien con notación mas concisa

$$U\alpha \cdot U\beta = \alpha \cdot \beta$$

Definición 2.4.9. Dados dos operadores A y B se define el *conmutador* de A y B a

$$[A, B] = AB - BA$$

Observación 2.4.4. A y B conmutan si $[A, B] = 0$.

Observación 2.4.5. También se define el *anticonmutador* de A y B como

$$\{A, B\} = AB + BA$$

Se dice que A y B anticonmutan si $\{A, B\} = 0$.

2.5 Espacios de Hilbert y notación de Dirac

Históricamente, un espacio de Hilbert es un espacio de dimensión infinita con escalares complejos. Por ejemplo el conjunto de funciones de variable real y valor complejo en el intervalo [0,1]

$$\{f \mid f : [0, 1] \to C\}$$

es un espacio de Hilbert. Sin embargo, en física los modelos que utilizamos son de dimensión finita, y como son derivados de estos espacios también se les llama espacios de Hilbert, en este caso espacios de Hilbert n–dimensionales. También, como pueden ser representados por una base finita, se les llama espacios de Hilbert *separables*. La literatura de mecánica cuántica ha seguido la convención de llamar un espacio euclídeo n–dimensional de variable compleja por el nombre de espacio de Hilbert n–dimensional $\mathcal{H}^n$. Nosotros seguiremos aquí esta convención.

Definición 2.5.1. Utilizando notación de Dirac. Un vector en un espacio de Hilbert $\mathcal{H}^n$ se denota por un `ket` $|\psi\rangle$. Por convención, vamos a interpretar este valor como un vector columna[1]

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

[1]La definición de `ket` realmente es más genérica que lo que estamos estipulando aquí. El `ket` representa el estado de un sistema cuántico, que en nuestra notación escojemos modelarlo como un vector columna. La notación `ket` también se utiliza cuando estamos representando el estado cuántico con un espacio de Hilbert infinito (función) y formalmente el vector solo representa las características del sistema cuántico que escojemos modelar.

Definición 2.5.2. La contraparte de un `ket` es un `bra` que conjuntamente conforman un `braket`. Si tenemos un `ket` $|\psi\rangle$ igual a

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

entonces el `bra` correspondiente se denota por $\langle\psi|$ y es igual al vector fila[2]

$$\langle\psi| = (\alpha_1^*, \alpha_2^*, \ldots, \alpha_n^*)$$

Definición 2.5.3. La multiplicación de un `bra` con un `ket` produce un escalar (número complejo). Si tenemos dos estados cuánticos $|\psi\rangle$ y $|\varphi\rangle$ tal que

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

y

$$|\varphi\rangle = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

Entonces el `braket` formado por ambos se denota por $\langle\psi|\varphi\rangle$ y es igual a

$$\langle\psi|\varphi\rangle = \sum_{i=1}^{n} \alpha_i^* \beta_i$$

Observación 2.5.1. El `braket` tal como esta definido anteriormente es equivalente al producto interno en números complejos. Se utiliza la notación $\langle\psi|\varphi\rangle$ en vez de $\langle\psi||\varphi\rangle$ por ser más concisa.

Observación 2.5.2. Así como el producto interno produce un escalar, también podemos definir el producto externo. Este producto genera una matriz, en mecánica cuántica a veces se utiliza indistintamente el `ket` de un estado con su matriz asociada.

[2]De nuevo, esto es una restricción de la notación, de la misma forma en que lo es nuestra definición del `ket`.

Definición 2.5.4. El *producto externo* de dos estados cuánticos $|\psi\rangle$ con componentes α_i, y el estado $|\varphi\rangle$ con componentes β_i es igual a la matriz $|\psi\rangle\langle\varphi|$ igual a:

$$|\psi\rangle\langle\varphi| = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} (\beta_1^*, \beta_2^*, \ldots, \beta_n^*) = \begin{pmatrix} \alpha_1\beta_1^* & \alpha_1\beta_2^* & \cdots & \alpha_1\beta_n^* \\ \alpha_2\beta_1^* & \alpha_2\beta_2^* & \cdots & \alpha_2\beta_n^* \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n\beta_1^* & \alpha_n\beta_2^* & \cdots & \alpha_n\beta_n^* \end{pmatrix}$$

Definición 2.5.5. Un espacio de Hilbert n–dimensional $\mathcal{H}^n$ tiene una *base canónica* determinada por los `kets` $|0\rangle$, $|1\rangle$, hasta el `ket` $|n-1\rangle$ tal que

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |i\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Observación 2.5.3. Los `bra` también pueden expresarse de esta manera, tenemos entonces el conjunto de la base canónica denotado por $\langle 0|$, $\langle 1|$, …, $\langle i|$, …, $\langle n-1|$.

Observación 2.5.4. Todo `ket` $|\psi\rangle \in \mathcal{H}^n$ puede espresarse como una combinación lineal de la base canónica

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

Observación 2.5.5. Los vectores $|\varphi\rangle$ y $\langle\varphi|$ se les llama duales y cumplen con la propiedad que

$$\begin{aligned} (|\varphi\rangle)^\dagger &= \langle\varphi| \\ (\langle\varphi|)^\dagger &= |\varphi\rangle \end{aligned}$$

Teorema 2.5.1. *El producto interno de vectores* `ket` *que representan estados cuánticos satisfaces la desigualdad de Schwartz*

$$\langle\varphi|\varphi\rangle\langle\psi|\psi\rangle \geq |\langle\varphi|\psi\rangle|^2$$

Definición 2.5.6. Dada una matriz u operador A, se llaman *valor propio* λ y *vector propio* $|\phi\rangle$ de la matriz a los valores que cumplen con que

$$A|\phi\rangle = \lambda|\phi\rangle$$

Teorema 2.5.2. *Los* valores propios *de una matriz u operador A son las soluciones a la equación del polinomio característico de la matriz*

$$|A - \lambda I| = 0$$

Observación 2.5.6. De acuerdo con el teorema fundamental del álgebra. Todo polinomio sobre los números complejos tiene por lo menos una raíz compleja. En nuestro caso realmente tiene n donde n es la dimensión del espacio.

Observación 2.5.7. Cualquier operador A puede descomponerse de la siguiente como

$$A = \sum_i \lambda_i |a_i\rangle\langle c_i|$$

con a_i y c_i arbitrarios y λ_i valores propios de la matriz.

Cuando un operador A se puede descomponer en

$$A = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i|$$

donde $|\varphi_i\rangle$ es un valor propio asociado con λ_i entonces la descomposición del operador es única

Teorema 2.5.3. *Los valores propios de un operador Hermitio son reales*

Definición 2.5.7. El producto tensor de dos matrices A y B, donde A es una matriz de n filas y m columnas

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}$$

y B es una matriz de p filas y q columnas

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1q} \\ b_{21} & b_{22} & \cdots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pq} \end{pmatrix}$$

es la matriz $C = A \otimes B$ de np filas y mq columnas definida por

$$C = A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{pmatrix}$$

donde $C = (c_{ij})$ y $c_{ij} = a_{i \div p, j \div q} b_{i|p, j|q}$ tal que $\div$ representa división entera y $|$ representa el resto de la división entera.

2.6 Relevancia física de los operadores y matrices

Nuestro interés con operadores se referirá al caso de operadores lineales en un espacio vectorial. Específicamente rotaciones en el espacio. Es claro que una rotación en un espacio vectoral es un operador lineal que cumple con que:

$$A(\alpha x + \beta y) = \alpha A(x) + \beta A(y)$$

Matemáticamente, las matrices son la representación natural de un operador lineal en un espacio vectorial de dimension finita.

Sea $e_1, \ldots, e_n$ una base de un espacio vectorial de dimension n. Sea f un operador lineal. Para todo elemento de la base tenemos que

$$f(e_i) = \sum_{k=1}^{n} f_{ki} e_i$$

Ahora bien, sea $u = f(v)$. Dado de que u y v son vectores en el espacio, ambos se puede expresar como

$$u = \sum_{k=1}^{n} u_k e_k$$

$$v = \sum_{i=1}^{n} v_i e_i$$

Pero por linealidad también sabemos que

$$u = f(v) = f\left(\sum_{i=1}^{n} v_i e_i\right) = \sum_{i=1}^{n} v_i f(e_i) =$$

$$\sum_{i=1}^{n} v_i \sum_{k=1}^{n} f_{ki} e_k = \sum_{i=1}^{n} \sum_{k=1}^{n} v_i f_{ki} e_k =$$

$$\sum_{k=1}^{n} \sum_{i=1}^{n} v_i f_{ki} e_k = \sum_{k=1}^{n} e_k \sum_{i=1}^{n} v_i f_{ki}$$

$$\Rightarrow u_k = \sum_{i=1}^{n} v_i f_{ki} = \sum_{i=1}^{n} f_{ki} v_i$$

Esta relación que acabamos de deducir es válida para cualquier operador lineal en un espacio vectorial de dimensión finita. Si expresamos nuestros vectores como combinaciones lineales de los elementos de la base y ordenamos los escalares de forma adecuada, tenemos entonces la expresión natural de operadores lineales mediante matrices donde:

$$\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

Esto nos indica que cualquier operador lineal sobre un espacio vectorial finito tiene una expresión matricial relativa a una base. Pero que si cambiamos la base la matriz que representa al operador también ha de cambiar. Dicho de otro modo, una matriz siempre corresponderá a un operador lineal, pero un operador lineal se representará en muchas matrices distintas dependiendo de la base que utilicemos.

Existen, sin embargo, propiedades que se obtienen de la matriz que son independientes de la base en que se expresa el operador. Estas son:

1. Los valores y vectores propios de la matriz.

2. El determinante de la matriz.

3. La traza de la matriz.

Debido a que estos valores son independientes de la matriz, se suele hablar de los valores propies del *operador*, lo mismo es válido para las otras características. Los valores y vectores propios son útiles para encontrar una base en la cual el operador tiene una matriz diagonal. En particular, si el operador

tiene valores y vectores propios λ_i, v_i, entonces la expresión del operador en la base $v_1, \ldots, v_n$ es

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$$

y el determinante del operador sera $\prod_{i=1}^{n} \lambda_i$

Por su parte, el determinante tiene la interpretación física como el grado de extensión o contracción que sufre un area del espacio al ser transformada por el operador. Esto es: sea A un conjunto de puntos arbitrario en el espacio vectorial. Entonces, para un operador f lineal, el determinante es igual a

$$det(f) = \frac{\int_{f(A)} dx}{\int_A dx}$$

2.7 Descomposición espectral de un operador ortonormal

Sea N un operador con vectores propios ortonormales en un espacio vectorial complejo de dimension finita. Si los vectores propios de N denotados por $|n_i\rangle$ forman una base del espacio vectorial y tienen la propiedad de que

$$N|n_i\rangle = \lambda_i|n_i\rangle$$

entonces todo vector en el espacio $|\Psi\rangle \in \mathcal{H}^n$ se puede representar como

$$|\Psi\rangle = \sum_i \alpha_i|n_i\rangle$$

Ahora bien, si aplicamos el operador N a este vector tenemos que

$$N|\Psi\rangle = N\sum_i \alpha_i|n_i\rangle = \sum_i \alpha_i N|n_i\rangle = \sum_i \alpha_i\lambda_i|n_i\rangle$$

Definase el proyector P_i a la matriz formada por el producto externo del vector propio $|n_i\rangle$ consigo mismo

$$P_i = |n_i\rangle\langle n_i|$$

Si multiplicamos P_i con el estado $|\Psi\rangle$ tenemos

$$P_i|\Psi\rangle = P_i \sum_j \alpha_j |n_j\rangle = \sum_j \alpha_j P_i |n_j\rangle = \sum_j \alpha_j |n_i\rangle\langle n_i|n_j\rangle = \alpha_i |n_i\rangle$$

y por lo tanto tenemos que

$$N|\Psi\rangle = \sum_i \alpha_i \lambda_i |n_i\rangle = \sum_i \lambda_i \alpha_i |n_i\rangle = \sum_i \lambda_i P_i |\Psi\rangle = \left(\sum_i \lambda_i P_i\right) |\Psi\rangle$$

lo cual implica que

$$N = \sum_i \lambda_i P_i$$

A esta expresión se le llama la *descomposición espectral* del operador.

2.8 Rotaciones en espacios vectoriales complejos

Recordando que un número complejo se expresa como $a + ib$ y que este valor tiene una representación natural en plano cartesiano. Extenderemos la definición de e^x para incluir números complejos. En particular recordemos que

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} \cdots$$

$$\cos(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} = 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \cdots$$

$$\sin(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!} = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots$$

Ahora bien, por estas equivalencias e^{ix} es igual a

$$e^{ix} = \sum_{n=0}^{\infty} \frac{(ix)^n}{n!} = 1 + ix + \frac{(ix)^2}{2} + \frac{(ix)^3}{3!} + \frac{(ix)^4}{4!} + \frac{(ix)^5}{5!} \cdots =$$

$$1 + ix + \frac{i^2x^2}{2} + \frac{i^3x^3}{3!} + \frac{i^4x^4}{4!} + \frac{i^5x^5}{5!} \cdots =$$

$$1 + ix - \frac{x^2}{2} - i\frac{x^3}{3!} + \frac{x^4}{4!} + i\frac{x^5}{5!} \cdots =$$

$$\left(1 - \frac{x^2}{2} + \frac{x^4}{4!} + \cdots\right) + i\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right) =$$

$$\cos(x) + i\sin(x)$$

Esta propiedad nos indica que $e^{i\theta}$ corresponde a una rotacion en el círculo de centro 0 y radio 1 por el ángulo de θ. En nuestro caso las operaciones efectuadas sobre qubits serán rotaciones, ya que la magnitud de los vectores no es relevante.[3]

Sabemos también que $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}$ lo cual indica que

$$\cos(\alpha+\beta) + i\sin(\alpha+\beta) = (\cos(\alpha) + i\sin(\alpha))(\cos(\beta) + i\sin(\beta))$$

y esto implica que

$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$$

$$\sin(\alpha+\beta) = \cos(\alpha)\sin(\beta) + \sin(\alpha)\sin(\beta)$$

2.9 Matrices de Pauli

Cuando se representa un qubit $|\psi\rangle$ existe un conjunto de rotaciones básicas que se puede aplicar al estado del qubit. Estas rotaciones básicas se encuentran representadas por las *matrices de Pauli* denominadas σ_x, σ_y y σ_z. Concretamente

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

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

[3]El principio de incertidumbre indica que no se puede saber dos propiedades de una partícula cuántica al mismo tiempo, asi que si nuestro modelo utiliza la orientacion o *spin* para representar el qubit, no será posible leer o utilizar su magnitud al mismo tiempo

Estas matrices tienen la propiedad de ser autoadjuntas, tal que

$$\sigma_x^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$\sigma_y^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \times \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$\sigma_z^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

2.10 La esfera de Bloch

Si interpretamos un estado cuántico de 1 solo qubit como el spin de una partícula, cada una de las matrices de Pauli tiene relevancia física y corresponden a una dirección de rotación en la dirección del spin. Esta representación del qubit se le llama la *esfera de Bloch*.

En particular si queremos rotar un qubit en la dirección x por un ángulo θ, el estado del qubit resultante se debe multiplicar por $e^{i\sigma_x\theta/2}$. Esta expresión aunque parece extraña (estamos elevando a e al valor de una matriz) se puede despejar de la siguiente manera:

$$e^{i\sigma_x\theta} = \sum_{n=0}^{\infty} \frac{(i\sigma_x)^n}{n!} =$$

$$I + i\sigma_x\theta + i^2\frac{\sigma_x^2\theta^2}{2} + i^3\frac{\sigma_x^3\theta^3}{3!} + i^4\frac{\sigma_x^4\theta^4}{4!} + i^5\frac{\sigma_x^5\theta^5}{5!}\cdots =$$

$$I + i\sigma_x\theta - \frac{\sigma_x^2\theta^2}{2} - i\frac{\sigma_x^3\theta^3}{3!} + \frac{\sigma_x^4\theta^4}{4!} + i\frac{\sigma_x^5\theta^5}{5!}\cdots =$$

$$I + i\sigma_x\theta - I\frac{\theta^2}{2} - i\sigma_x\frac{\theta^3}{3!} + I\frac{\theta^4}{4!} + i\sigma_x\frac{\theta^5}{5!}\cdots =$$

$$I\left(1 - \frac{\theta^2}{2} + \frac{\theta^4}{4!}\cdots\right) + i\sigma_x\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!}\cdots\right) =$$

$$I\cos(\theta) + i\sigma_x\sin(\theta)$$

Utilizando un análisis similar podemos deducir que

$$e^{i\sigma_y\theta} = I\cos(\theta) + i\sigma_y\sin(\theta)$$

$$e^{i\sigma_z\theta} = I\cos(\theta) + i\sigma_z\sin(\theta)$$

Ahora bien, por razones físicas a las cuales no nos referiremos, una rotación en la esfera de Bloch en la direccion $\vec{n}$ nos da una matriz de rotación determinada por

$$\mathcal{R}_{\vec{n}}(\theta) = e^{-i\sigma_{\vec{n}}\theta/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_{\vec{n}}$$

Mas concretamente, para rotaciones en x tenemos que:

$$\mathcal{R}_x(\theta) = e^{-i\sigma_x\theta/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_x =$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} - i\begin{pmatrix} 0 & \sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & 0 \end{pmatrix} =$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

Para rotaciones en y tenemos que

$$\mathcal{R}_y(\theta) = e^{-i\sigma_y\theta/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_y =$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} - i\begin{pmatrix} 0 & -i\sin\left(\frac{\theta}{2}\right) \\ i\sin\left(\frac{\theta}{2}\right) & 0 \end{pmatrix} =$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

y para rotaciones en z tenemos

$$\mathcal{R}_z(\theta) = e^{-i\sigma_z\theta/2} = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)\sigma_z =$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} - i\begin{pmatrix} \sin\left(\frac{\theta}{2}\right) & 0 \\ 0 & -\sin\left(\frac{\theta}{2}\right) \end{pmatrix} =$$

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) - i\sin\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) + i\sin\left(\frac{\theta}{2}\right) \end{pmatrix}$$

Por otra parte, dado un estado cuántico $|\varphi\rangle$ las matrices de Pauli conforman una base tal que es posible representar la matriz proyección del estado

$$|\varphi\rangle\langle\varphi| = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$$

donde x, y, y z, corresponden a las coordenadas del qubit en la esfera de Bloch.

Esta representación permite tambien expresar la esfera de Bloch mediante tres ángulos un ángulo de latitud θ, uno de longitud ϕ, y otro ángulo de fase γ que corresponde a valores no observables del qubit. Bajo esta representacion un qubit arbitrario

$$|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

Cumple con que

$$\alpha_0 = e^{i\gamma}\cos\left(\frac{\theta}{2}\right), \quad \alpha_1 = e^{i\gamma}e^{i\phi}\left(\frac{\theta}{2}\right)$$

2.11 Mediciones

En el modelo matemático de mecánica cuántica, una medición corresponde a un operador A con vectores propios $|n_i\rangle$ ortonormales, donde los observables son los valores propios λ_i de la matriz correspondiente al operador. En particular, si nos encontramos en el estado cuántico $|\phi\rangle$ y tratamos de observar/medir el estado por medio del operador A, vamos a obtener λ_i con probabilidad $||P_i|\phi\rangle||$ donde $P_i = |n_i\rangle\langle n_i|$ se llama la matriz proyección de λ_i y el estado resultante es

$$\frac{P_i|\phi\rangle}{\sqrt{\langle\phi|P_i|\phi\rangle}}$$

Chapter 3

Computertas Cuánticas

3.1 Generalidades

3.2 Compuertas de 1 Qubit

Compuertas de 1 Qubit tenemos las matrices de Pauli presentadas en el capítulo anterior, las cuales abreviaremos y utilizaremos como $X = \sigma_x$, $Y = \sigma_y$ y $Z = \sigma_z$. Además la compuerta X tambien us el nombre del CNOT ya que invierte los valores $|0\rangle$ y $|1\rangle$.

Una compuerta sumamente importante es la compuerta de Hadamard. Esta compuerta existe en su versión de 1 qubit y de n qubits. En particular para 1 qubit la compuerta es:

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

Notese que

$$H^2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \times \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$$

Por el momento basta observar que aplicar la compuerta de Hadamard a un qubit $|0\rangle$ nos da una superposición entre los valores $|0\rangle$ y $|1\rangle$

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

La compuerta de Hadamard es sumamente util para efectuar paralelismo cuántico, ya que al quedar en un estado superpuesto cualquier algoritmo que se calcule sobre el resultado de la compuerta de Hadamard se efectuara para todos las posibles configuraciones de entradas.

Otro tipo de compuerta de 1 qubit corresponde a las llamadas rotaciones de fase condicionales. Estas se representan por $\mathcal{R}(\theta)$ y corresponden a la matrix

$$\mathcal{R}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Notese que esta compuerta no altera el valor del qubit si este es $|0\rangle$, pero si altera el qubit si este es $|1\rangle$. Aún asi, un valor de $|1\rangle$ no pasa a ser $|0\rangle$ sino que es *rotado* sobre el plano complejo. Por esto su nombre de cambio de fase condicional.

De estas compuertas tenemos

$$T = \mathcal{R}\left(\frac{\pi}{4}\right) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$T' = \mathcal{R}\left(-\frac{\pi}{4}\right) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}$$

$$S = \mathcal{R}\left(\frac{\pi}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

3.3 Compuertas de 2 Qubits

3.3.1 compuerta CNOT

La compuerta mas coún de 2 qubits es la compuerta CNOT. Esta compuerta intercambia el valor del segundo qubit si el primer qubit es igual a 1. Este comportamiento da la tabla de verdad

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Si representamos estos valores $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ como sus respectivos vectores en $\mathcal{C}^4$ tenemos que la matriz $CNOT$ de transición de este circuito cuántico debe cumplir con las siguientes equaciones

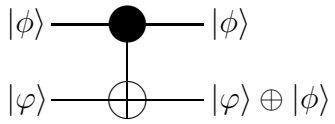
$$CNOT \times \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad CNOT \times \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$CNOT \times \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad CNOT \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

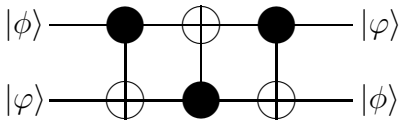
lo cual indica que

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

este circuito cuántico también le corresponde el diagrama de conexión siguiente

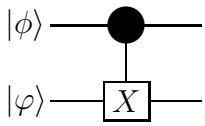


La compuerta CNOT puede ser utilizada para intercambiar qubits, el circuito que implementa el intercambio es el siguiente.

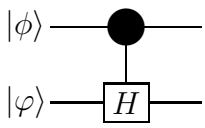


3.3.2 Compuertas controladas genéricas

Las compuertas de 2 qubits suelen ser compuertas controladas, de las cuales 1 qubit funge el papel de bit de control, y el otro qubit es el qubit controlado. De hecho el CNOT es un caso particular de este tipo de compuertas donde el qubit de control es el primer qubit y el segundo es el controlado. La transformación utilizada para el segundo qubit es la matriz de Pauli $\sigma_x = X$ tal que el cirquito del CNOT también se puede representar como



Utilizando esta notación podemos efectuar compuertas controladas de Hadamard, T, T' u otras. Por ejemplo, una compuerta de Hadamard controlada se representa gráficamente mediante el circuito



Su tabla de verdad da

a	b	a'	b'
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$2^{-2}(\|0\rangle + \|1\rangle)$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$2^{-2}(\|0\rangle - \|1\rangle)$

esta tabla conduce al conjunto de equaciones

$$cH \times \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad cH \times \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$cH \times \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad cH \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ -1 \end{pmatrix}$$

lo cual indica que

$$cH = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2^{-2} & 2^{-2} \\ 0 & 0 & 2^{-2} & -(2^{-2}) \end{pmatrix} = \begin{pmatrix} I_2 & \mathbf{0}_{2\times 2} \\ \mathbf{0}_{2\times 2} & H \end{pmatrix}$$

3.4 Compuertas de 3 Qubits

Las compuertas cuánticas de 1 y 2 qubits son útiles pero no son suficientes para implementar un computador cuántico. La razón de esto es que la mecánica cuántica exige que las compuertas cuánticas sean reversibles, y hasta mediados de los años 70 no se conocian operadores lógicos reversibles que también fueran universales.

Por ejemplo, sabemos que la compuerta lógica NAND es universal ya que todas las operaciones lógicas necesarias para efectuar computos arbitrariamente complejos se pueden efectuar con ella.

$$\begin{aligned} \text{NOT a} &= \text{a NAND a} \\ \text{a OR b} &= (\text{a NAND a}) \text{ NAND } (\text{b NAND b}) \\ \text{a AND b} &= (\text{a NAND b}) \text{ NAND } (\text{a NAND b}) \end{aligned}$$

sin embargo la compuerta NAND no es reversible, ya que conociendo las salidas de la compuerta no es posible saber con toda seguridad cuales fueron las entradas. Esto se puede ver facilmente en la tabla de verdad del NAND a continuación

Tabla del NAND

a	b	c'
0	0	1
0	1	1
1	0	1
1	1	0

la cual no tiene las misma cantidad de entradas que de salidas, y tiene mas de una posible configuración inicial para una salida de 1 (lo cual indica que conociendo la salida no es posible conocer la entrada).

Las compuertas de 3 qubits mas conocidas la compuerta de Fredkin y la compuerta de Toffoli.

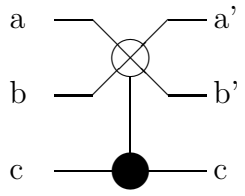
3.4.1 La compuerta de Fredkin

La compuerta de Fredkin es una compuerta con tres entradas a, b, y c, donde el qubit c corresponde al qubit de control. Su lógica indica que si c = 1 entonces los bits a y b son intercambiados, de lo contrario la compuerta no efectua ninguna modificación. Esta definición nos da la tabla de verdad

Tabla de FREDKIN

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

La compuerta de Fredkin puede representarse gráficamente como



Esta compuerta se representa matricialmente como

$$Fredkin = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

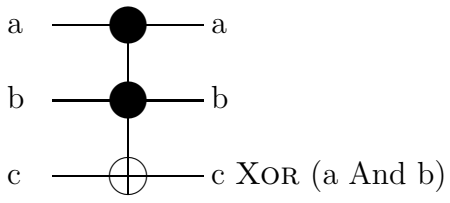
3.4.2 La compuerta de Toffoli

La compuerta de Toffoli es una compuerta controlada con entradas a, b y c, tal que la entrada c cambia de valor si las primeras 2 entradas son 1. Se puede interpretar como un CNOT con 2 qubits de control, su tabla de verdad es

Tabla de TOFFOLI

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

La compuerta de Toffoli puede representarse gráficamente como



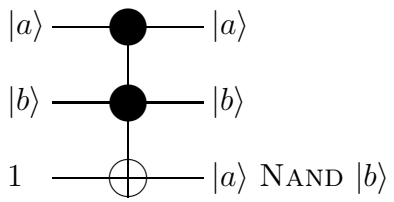
y su matriz de transición esta dada por

$$Toffoli = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

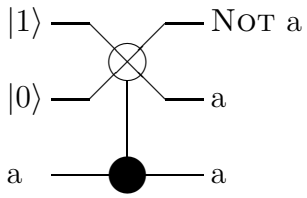
3.4.3 Compuertas Universales

Tanto la compuerta de Fredkin como la de Toffoli son compuertas reversibles universales. Reversibles porque conocidas las salidas siempre es posible deducir las entradas (la matriz que representa el circuito es reversible, y en este caso es la misma matriz).

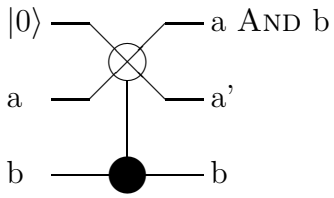
Para demostrar que son universales basta con demostrar que ambas pueden implementar el circuito Nand, ya que esta compuerta lógica es universal. En el caso de la compuerta Toffoli tenemos el siguiente circuito, el cual es equivalente a un Nand



En cuanto a la compuerta de Fredkin, esta puede implementar tanto el NOT como el AND, y estos dos en conjunto se utilizan para implementar un NAND el Not esta dado por



y el AND por La compuerta de Fredkin puede representarse gráficamente como



3.5 El teorema de no clonación

Es importante subrayar aqui, que las compuertas presentadas son compuertas lógicas que funcionan bien para valores binarios pero no necesariamente para qubits arbitrarios $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. Si esto fuera asi el circuito anterior tendria la capacidad de *clonar* un qubit, lo cual se puede demostrar que es imposible para un qubit arbitrario. Mas concretamente

Teorema 3.5.1. *No existe un circuito cuántico capaz de duplicar el valor de un estado cuantico arbitrario.*

Proof. Supongamos, por contradicción, que si existe este circuito, con matriz de transición G. Sean $|\phi\rangle$ y $|\varphi\rangle$ dos qubits arbitrarios. Podemos asumir que

$$G(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

y que

$$G(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Ahora bien, considerese el estado

$$|\xi\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle + |\varphi\rangle)$$

por definición de la compuerta sabemos que debe ser cierto que

$$G(|\xi\rangle \otimes |0\rangle) = |\xi\rangle \otimes |\xi\rangle =$$

$$\frac{1}{2}(|\phi\rangle + |\varphi\rangle) \otimes (|\phi\rangle + |\varphi\rangle) =$$

$$\frac{1}{2}(|\phi\phi\rangle + |\phi\varphi\rangle + |\varphi\phi\rangle + |\varphi\varphi\rangle) \tag{3.1}$$

pero por linealidad tambien sabemos que

$$G(|\xi\rangle \otimes |0\rangle) = G\left(\frac{1}{\sqrt{2}}(|\phi\rangle + |\varphi\rangle) \otimes |0\rangle\right) =$$

$$\frac{1}{\sqrt{2}}(G(|\phi\rangle \otimes |0\rangle) + G(|\varphi\rangle \otimes |0\rangle)) =$$

$$\frac{1}{\sqrt{2}}(|\phi\rangle \otimes |\phi\rangle) + |\varphi\rangle \otimes |\varphi\rangle)) =$$

o mas concisamente

$$\frac{1}{\sqrt{2}}(|\phi\phi\rangle) + |\varphi\varphi\rangle)) = \tag{3.2}$$

y claramente las equaciones 3.1 y 3.2 no pueden ser iguales para valores arbitrarios de $|\phi\rangle$ y $|\varphi\rangle$. QED. □

3.6 La transformada de Welsh–Hadamard

La transformada de Welsh–Hadamard, o Hadamard (en corto) ya fue presentada en las compuertas de 1 qubit, si recordamos esto da la compuerta

$$H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

La compuerta de Hadamard se puede generalizar para espacios vectoriales de tamaño 2^n. En particular la fórmula inductiva esta dada por

$$H_{2^n} = \begin{cases} 1 & \text{si } n = 0 \\ \frac{1}{\sqrt{2}} \begin{pmatrix} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & -H_{2^{n-1}} \end{pmatrix} & \text{si } n > 1 \end{cases}$$

Teorema 3.6.1. *Una compuerta de Welsh–Hadamard de tamaño 2^n es igual al producto tensor de n compuertas de Hadamard de tamaño 2, tal que*

$$H_{2^n} = \underbrace{H_2 \otimes H_2 \otimes \cdots \otimes H_2}_{n \text{ veces}}$$

Proof. Por inducción, para $n = 1$ sabemos que

$$H_{2^1} = H_2 = \underbrace{H_2}_{1 \text{ vez}}$$

Ahora bien, suponemos que

$$H_{2^n} = \underbrace{H_2 \otimes H_2 \otimes \cdots \otimes H_2}_{n \text{ veces}}$$

entonces

$$H_{2^{n+1}} \overset{def}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} H_{2^n} & H_{2^n} \\ H_{2^n} & -H_{2^n} \end{pmatrix} =$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes H_{2^n} =$$

$$H_2 \otimes H_{2^n} =$$

$$H_2 \otimes \underbrace{H_2 \otimes H_2 \otimes \cdots \otimes H_2}_{n \text{ veces}} =$$

$$\underbrace{H_2 \otimes H_2 \otimes H_2 \otimes \cdots \otimes H_2}_{n+1 \text{ veces}}$$

□

Estas propiedades conducen al siguiente teorema, el cual es muy util en algunos algoritmos cuánticos.

Teorema 3.6.2. *La transformada de Welsh–Hadamard cumple con*

$$H_{2^n}|\underbrace{00\cdots0}_{n\ veces}\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$$

$$H_{2^n}|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}(-1)^{\vec{k}\cdot\vec{j}}|k\rangle$$

Donde $\vec{k}$ y $\vec{j}$ son los vectores que contienen la representación binaria de k y de j y su multiplicación es el producto interno de ambos.

Proof. Por inducción, el caso base para $n = 1$ debe demostrar que

$$H_2|b\rangle = \frac{1}{\sqrt{2}}\sum_{j=0}^{1}(-1)^{\vec{j}\cdot\vec{b}}|j\rangle$$

para todo $b \in \{0, 1\}$. Es fácil corroborar este caso y lo dejamos como ejercicio al lector.

Para el caso inductivo, asumimos como hipótesis de inducción que

$$H_{2^n}|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}(-1)^{\vec{k}\cdot\vec{j}}|k\rangle$$

y debemos demostrar que

$$H_{2^{n+1}}|m\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^{n+1}-1}(-1)^{\vec{i}\cdot\vec{m}}|i\rangle$$

para efectuar esta prueba es importante resaltar varios puntos

- el valor de k varia de 0 a $2^n - 1$, su representación como una secuencia de bits $\vec{k}$ contiene n bits.
- el valor de j también varia sobre el mismo rango y por lo tanto tiene una representación equivalente de n bits
- los valores de m e i varian entre 0 y $2^{n+1}-1$ asi que sus representaciones como una sequencia de bits contienen $n + 1$ bits.

- si $k < 2^n$, la representación binaria de $k + 2^n = 1\vec{k}$ (concatenar un 1 al frente de $\vec{k}$)
- todo vector base $|i\rangle$ con $n+1$ qubits es o bien de la forma $|0\rangle \otimes |k\rangle$ o de la forma $|1\rangle \otimes |k\rangle$ donde $|k\rangle$ es un vector base de n qubits. Además $|1\rangle \otimes |k\rangle = |k + 2^n\rangle$
- todo vector base $|m\rangle$ con $n+1$ qubits es o bien de la forma $|0\rangle \otimes |j\rangle$ o de la forma $|1\rangle \otimes |j\rangle$ donde $|j\rangle$ es un vector base de n qubits. Además $|1\rangle \otimes |j\rangle = |j + 2^n\rangle$
- si $i, b \in \{0, 1\}$ entonces

$$(-1)^{ib}(-1)^{\vec{k}\cdot\vec{j}} = (-1)^{(i\vec{k})\cdot(b\vec{j})}$$

donde $b\vec{j}$ es la concatenación del bit b a la sequencia de bits $\vec{j}$

Supondremos, sin perdida de generalidad, de que $|m\rangle = |b\rangle \otimes |j\rangle$ con $b \in \{0, 1\}$ y $|j\rangle$ un vector base de n qubits, esto tambien implica que la representacion binaria de $m = \vec{m}$ se puede expresar como $\vec{m} = b\vec{j}$ donde $\vec{j}$ es la representación binaria del vector base j. Ahora bien

$$H_{2^{n+1}}|m\rangle = (H_2 \otimes H_{2^n})(|b\rangle \otimes |j\rangle) =$$

$$(H_2|b\rangle) \otimes (H_{2^n}|j\rangle) =$$

$$\left(\frac{1}{\sqrt{2}}\sum_{i=0}^{1}(-1)^{i\cdot b}|i\rangle\right) \otimes \left(\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}(-1)^{\vec{k}\cdot\vec{j}}|k\rangle\right) =$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{i=0}^{1}\sum_{k=0}^{2^n-1}(-1)^{i\cdot b}(-1)^{\vec{k}\cdot\vec{j}}|i\rangle \otimes |k\rangle =$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{i=0}^{1}\sum_{k=0}^{2^n-1}(-1)^{(i\vec{k})\cdot(b\vec{j})}|i\rangle \otimes |k\rangle =$$

$$\frac{1}{\sqrt{2^{n+1}}}\left(\left[\sum_{k=0}^{2^n-1}(-1)^{(0\vec{k})\cdot(b\vec{j})}|0\rangle \otimes |k\rangle\right] + \left[\sum_{k=0}^{2^n-1}(-1)^{(1\vec{k})\cdot(b\vec{j})}|1\rangle \otimes |k\rangle\right]\right) =$$

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{k=0}^{2^n-1}(-1)^{(0\vec{k})\cdot(b\vec{j})}|k\rangle + \sum_{k=0}^{2^n-1}(-1)^{(1\vec{k})\cdot(b\vec{j})}|k + 2^n\rangle\right) =$$

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{k=0}^{2^n-1}(-1)^{\vec{k}\cdot\vec{m}}|k\rangle+\sum_{k=0}^{2^n-1}(-1)^{(\overrightarrow{k+2^n})\cdot\vec{m}}|k+2^n\rangle\right)=$$

$$\frac{1}{\sqrt{2^{n+1}}}\left(\sum_{i=0}^{2^n-1}(-1)^{\vec{i}\cdot\vec{m}}|i\rangle+\sum_{i=2^n}^{2^{n+1}-1}(-1)^{\vec{i}\cdot\vec{m}}|i\rangle\right)=$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{i=0}^{2^{n+1}-1}(-1)^{\vec{i}\cdot\vec{m}}|i\rangle$$

□

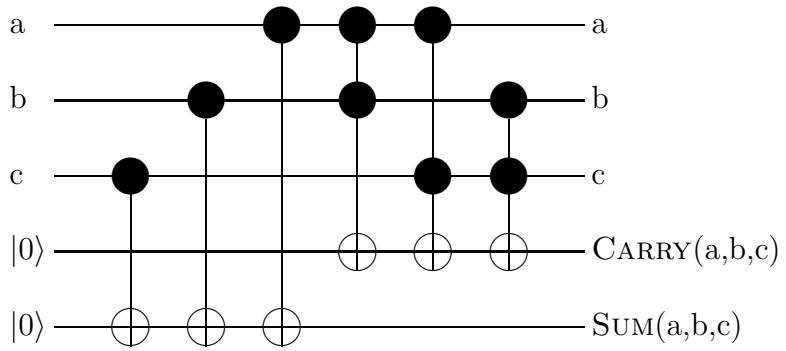
3.7 Full Adder Cuántico

El full–adder es una operación binaria básica que implementa la suma de bits. El full–adder cuenta con 3 entradas y dos salidas llamadas Sum y Carry. La tabla de verdad de estas operaciones esta dada por

Full Adder

a	b	c	Sum	Carry
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

El circuito cuántico que implementa esta operación es



3.8 Transformada de Fourier Cuántica

Jean Baptieste Joseph Fourier, imaginaba que la superficie del mar no era mas que la suma de funciones senosoidales. El razonaba que oscilaciones en la superficie del agua son creadas por ondas que se propagan en el medio, y estas se encuentran caracterizadas por funciones senosoidales. Por ejemplo, cuando lanzamos una piedra en un estanque de agua totalmente quieta, las ondas senosoidales son claramente visibles, si lanzamos mas piedras empiezan a surgir patrones mas complejos. Entonces cabe la pregunta, ¿Qué tan complejos pueden ser los patrones generados por la suma de funciones senosoidales?

Resulta ser que un gran número de funciones se puede representar como la suma de senosoidales. La representación de funciones mediante senosoidales es un esquema que tiene una gran relevancia física ya que existen gran cantidad de fenómenos físicos que son provocados por oscilaciones y por lo tanto caracterizables mediante senosoidales.

3.8.1 La Transformada de Fourier

Fourier comienza diciendo que cualquier función periódica $s(x)$ con periodo T, tal que $s(x+T) = s(x)$, puede expresarse en el intervalo $[\frac{-T}{2}, \frac{T}{2}]$ como la suma de senosoidales de la forma

$$s(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(2\pi n f x) + b_n \cos(2\pi n f x)$$

donde $f = \frac{1}{T}$ y se le llama *frecuencia*, y los coeficientes a_n y b_n estan definidos por las fórmulas

$$a_0 = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(x)dx$$

$$a_n = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(x)\cos(2\pi nfx)dx$$

$$b_n = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(x)\sin(2\pi nfx)dx$$

Notese que para cualesquiera valor de n y m distintos se cumple que

$$\int_{-\frac{T}{2}}^{T2} \sin(2\pi nfx)\sin(2\pi mfx)dx = 0$$

y lo mismo es cierto para los cosenos. Esta propiedad permite ver a las funciones trigonométricas como una base para construir funciones.

La transformada de Fourier, es una trasnformación matemática que traduce un problema del ámbito de amplitudes y tiempo al ámbito de frecuencias. Por ejemplo, la transformada de Fourier de una señal de sonido obtiene las frecuencias fundamentales del sonido que se escucha (las notas musicales). La transformada de fourier es útil para el procesamiento digital de señales, tales como voz, imagenes, u otros.

3.8.2 La Transformada de Fourier discreta

El planteamiento básico de la trasformada de fourier se puede especificar tanto en el campo discreto como en el continuo. Sin embargo, para nuestros casos nos interesara la transformada de Fourier discreta, el planteamiento de la trasformada es el siguiente.

Dada una funcion $f(x)$ tal que contamos con N muestras de $f(x)$ denominadas $f_0, f_1, \ldots, f_{N-1}$. Se llama trasformada de Fourier discreta de $\{f_0, \ldots, f_{N-1}\}$ al conjunto de valores $\{F_0, F_1, \ldots, F_{N-1}\}$ definido como

$$F_k = \frac{1}{N}\sum_{j=0}^{N-1} f_j \omega_N^{jk} \tag{3.3}$$

donde

$$\omega_N = e^{-\frac{2i\pi}{N}}$$

Es importante resaltar las siguientes propiedades

1. ω_N es una raiz N-ésima de 1, tal que
$$\omega_N^N = \left(e^{-\frac{2i\pi}{N}}\right)^N = e^{-\frac{2i\pi N}{N}} = e^{-2i\pi} = \cos(2\pi) - i\sin(2\pi) = 1$$
2. ω_N^j es también una raiz N-ésima de 1 ya que
$$\left(\omega_N^j\right)^N = \omega_N^{jN} = \omega_N^{Nj} = \left(\omega_N^N\right)^j = 1^j = 1$$
3. todos los ω_N^j son distintos para $j \in \{0, \ldots, N-1\}$
4. $\omega_N^2 = \omega_{N/2}$ ya que
$$\omega_N^2 = \left(e^{-\frac{2i\pi}{N}}\right)^2 = e^{-\frac{2i\pi 2}{N}} = e^{-\frac{2i\pi}{N/2}} = \omega_{N/2}$$
5. $\omega_N^{N/2} = -1$ ya que
$$\omega_N^{N/2} = \left(e^{-\frac{2i\pi}{N}}\right)^{N/2} = e^{-\frac{2i\pi N}{N2}} = e^{-i\pi} = \cos(\pi) - i\sin(\pi) = -1$$

Dada la ecuación 3.3 y las anteriores propiedades, la transformada de Fourier discreta puede expresarse como una multiplicación de matrices de la forma

$$\Omega\vec{f} = \vec{F}$$

donde

$$\vec{f} = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix}, \quad \vec{F} = \begin{pmatrix} F_0 \\ F_1 \\ \vdots \\ F_{N-1} \end{pmatrix},$$

$$\Omega = \begin{pmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ 1 & \omega_N & \cdots & \omega_N^j & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \cdots & \omega_N^{2j} & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega_N^k & \cdots & \omega_N^{kj} & \cdots & \omega_N^{k(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega_N^{N-1} & \cdots & \omega_N^{(N-1)j} & \cdots & \omega_N^{(N-1)^2} \end{pmatrix}$$

Bajo esta notación, la trasformada de Fourier se convierte en una multiplicación de una matriz por un vector, y su complejidad computacional es $O(N^2)$

3.8.3 La Transformada de Fourier rápida (FFT)

La complejidad computacional de la trasformada de Fourier discreta puede mejorarse considerablemente si se utiliza la propiedad de que los valores de ω_N^j tienden a repetirse y si suponemos que N es divisble entre 2, con estas condiciones tenemos que

$$F_k = \frac{1}{N}\sum_{j=0}^{N-1} f_j \omega_N^{jk} =$$

$$\frac{1}{N}\sum_{j\in\{0,1,\ldots,N-1\}} f_j \omega_N^{jk} =$$

$$\frac{1}{N}\left(\sum_{j\in\{0,2,\ldots,N-2\}} f_j \omega_N^{jk} + \sum_{j\in\{1,3,\ldots,N-1\}} f_j \omega_N^{jk}\right) =$$

$$\frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j}\omega_N^{2jk} + \frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_N^{(2j+1)k} =$$

$$\frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j}\omega_N^{2jk} + \omega_N^k \frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_N^{2jk} =$$

$$\frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j}\left(\omega_N^2\right)^{jk} + \omega_N^k \frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j+1}\left(\omega_N^2\right)^{jk} =$$

$$\frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{jk} + \omega_N^k \frac{1}{N}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{jk} =$$

$$\frac{1}{2}\left(\underbrace{\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{jk}}_{\text{Transf. par}} + \omega_N^k \underbrace{\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{jk}}_{\text{Transf. impar}}\right) \tag{3.4}$$

Ahora bien, el valor de k en la ecuación 3.4 puede variar de 0 a $N-1$, lo cual indica que solo para los valores de $k \in \{0, 1, \ldots \frac{N}{2} - 1\}$ tanto la transformada par como la impar son transformadas de Fourier con $N/2$ puntos.

Sin embargo, todos los valores mayores o iguales a $\frac{N}{2}$ se pueden expresar como $k+\frac{N}{2}$ donde $k \in \{0, 1, \ldots \frac{N}{2}-1\}$ y para estos la ecuación 3.4 se expresa como

$$F_{k+\frac{N}{2}} = \frac{1}{2}\left(\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{j(k+\frac{N}{2})} + \omega_N^{k+\frac{N}{2}}\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{j(k+\frac{N}{2})}\right) =$$

$$\frac{1}{2}\left(\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{jk}\omega_{N/2}^{jN/2} + \omega_N^k\omega_N^{N/2}\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{jk}\omega_{N/2}^{jN/2}\right) =$$

$$\frac{1}{2}\left(\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{jk}\left(\omega_{N/2}^{N/2}\right)^j + \omega_N^k\left(\omega_N^{N/2}\right)\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{jk}\left(\omega_{N/2}^{N/2}\right)^j\right) =$$

$$\frac{1}{2}\left(\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{jk}(1)^j + \omega_N^k(-1)\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{jk}(1)^j\right) =$$

$$\frac{1}{2}\left(\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j}\omega_{N/2}^{jk} - \omega_N^k\frac{1}{N/2}\sum_{j=0}^{N/2-1} f_{2j+1}\omega_{N/2}^{jk}\right)$$

3.8.4 La Transformada de Fourier Cuántica (QFT)

La transformada de Fourier cuántica toma un estado $|\varphi\rangle$ y lo transforma en un estado $|\phi\rangle$ tal que

$$|\varphi\rangle = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix}, \quad |\phi\rangle = \begin{pmatrix} F_0 \\ F_1 \\ \vdots \\ F_{N-1} \end{pmatrix},$$

$$|\varphi\rangle \xrightarrow{QFT} |\phi\rangle$$

donde los F_k son los coeficientes de la transformada de Fourier de $f_0, \ldots, f_{N-1}$. Como los estados cuánticos deben estar normalizados, la transformada de Fourier cuántica cumple con la siguiente ecuación

$$F_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} f_j\omega^{jk}$$

Si el estado cuántico además corresponde a una secuencia de qubits podemos decir que $N = 2^n$ y la expresión se traduce a

$$F_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} f_j \omega^{jk} \tag{3.5}$$

También sabemos que el coeficiente F_k multiplica al ket base $|k\rangle$ asi que

$$QFT|\varphi\rangle = \sum_{k=0}^{2^n-1} F_k|k\rangle =$$

$$\sum_{k=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} f_j \omega^{jk} \right) |k\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} f_j \sum_{k=0}^{2^n-1} \omega^{jk}|k\rangle \tag{3.6}$$

Y como f_j es el coeficiente del vector base $|j\rangle$, entonces por linealidad la ecuación 3.5 es equivalente a decir que

$$QFT|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} w^{jk}|k\rangle \tag{3.7}$$

ya que

$$QFT|\varphi\rangle = QFT \sum_{j=0}^{2^n-1} f_j|j\rangle =$$

$$\sum_{j=0}^{2^n-1} f_j QFT|j\rangle =$$

$$\sum_{j=0}^{2^n-1} f_j \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega^{jk}|k\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} f_j \sum_{k=0}^{2^n-1} \omega^{jk}|k\rangle = \textit{ecuación } 3.6$$

Derivación del circuito de la QFT

Utilizaremos la equación 3.7 para derivar la forma que debe tener el circuito de la QFT, antes de esto haremos ciertas suposiciones notacionales

1. $k \in \{0, 1, \ldots, 2^n - 1\}$ y el ket $|k\rangle$ corresponde a una secuencia de n qubits tal que

$$|k\rangle = |k_1 k_2 \cdots k_n\rangle = |k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle$$

$$k = k_1 2^{n-1} + k_2 2^{n-2} + \cdots + k_{n-1} 2 + k_n = \sum_{s=1}^{n} k_s 2^{n-s}$$

   con $k_s \in \{0, 1\}$.

2. $j \in \{0, 1, \ldots, 2^n - 1\}$ y el ket $|j\rangle$ corresponde a una secuencia de n qubits tal que

$$|j\rangle = |j_0 j_1 \cdots j_{n-1}\rangle = |j_0\rangle \otimes |j_1\rangle \otimes \cdots \otimes |j_{n-1}\rangle$$

$$j = j_0 2^{n-1} + j_1 2^{n-2} + \cdots + j_{n-2} 2 + j_{n-1} = \sum_{s=0}^{n-1} j_s 2^{n-(s+1)}$$

   con $j_s \in \{0, 1\}$.

Con estas definiciones el circuito cuántico de la transformada de Fourier debe cumplir con

$$QFT|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} w^{jk} |k\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1 \in \{0,1\}} \sum_{k_2 \in \{0,1\}} \cdots \sum_{k_n \in \{0,1\}} w^{j \sum_{s=1}^{n} k_s 2^{n-s}} |k_1 k_2 \cdots k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1 \in \{0,1\}} \sum_{k_2 \in \{0,1\}} \cdots \sum_{k_n \in \{0,1\}} e^{(2i\pi j (\sum_{s=1}^{n} k_s 2^{n-s}))/2^n} |k_1 k_2 \cdots k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1 \in \{0,1\}} \sum_{k_2 \in \{0,1\}} \cdots \sum_{k_n \in \{0,1\}} e^{(2i\pi j \sum_{s=1}^{n} k_s 2^{-s})} |k_1 k_2 \cdots k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1 \in \{0,1\}} \sum_{k_2 \in \{0,1\}} \cdots \sum_{k_n \in \{0,1\}} e^{(2i\pi j \sum_{s=1}^{n} k_s 2^{-s})} |k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1\in\{0,1\}} \sum_{k_2\in\{0,1\}} \cdots \sum_{k_n\in\{0,1\}} \left(\prod_{s=1}^{n} e^{2i\pi j k_s 2^{-s}} \right) |k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1\in\{0,1\}} \sum_{k_2\in\{0,1\}} \cdots \sum_{k_n\in\{0,1\}} \left(\prod_{s=1}^{n} e^{2i\pi j k_s 2^{-s}} \right) \bigotimes_{s=1}^{n} |k_s\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1\in\{0,1\}} \sum_{k_2\in\{0,1\}} \cdots \sum_{k_n\in\{0,1\}} \bigotimes_{s=1}^{n} \left(e^{2i\pi j k_s 2^{-s}} |k_s\rangle \right) =$$

$$\frac{1}{\sqrt{2^n}} \bigotimes_{s=1}^{n} \sum_{k_s\in\{0,1\}} \left(e^{2i\pi j k_s 2^{-s}} |k_s\rangle \right) =$$

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \sum_{k_s\in\{0,1\}} \left(e^{2i\pi j k_s 2^{-s}} |k_s\rangle \right) =$$

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \left(e^{2i\pi j\times 0\times 2^{-s}} |0\rangle + e^{2i\pi j\times 1\times 2^{-s}} |1\rangle \right) =$$

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2i\pi j 2^{-s}} |1\rangle \right) =$$

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + e^{2i\pi j 2^{-s}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) =$$

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{2i\pi j 2^{-s}} \end{pmatrix} \tag{3.8}$$

Ahora analizando el término

$$e^{2i\pi j 2^{-s}} = e^{2i\pi (\sum_{m=0}^{n-1} j_m 2^{n-(m+1)}) 2^{-s}} =$$

$$e^{2i\pi \sum_{m=0}^{n-1} j_m 2^{n-s-(m+1)}} =$$

$$e^{2i\pi \sum_{m=0}^{n-1} j_m 2^{(n-s-1)-m}} =$$

$$e^{\sum_{m=0}^{n-1} 2i\pi j_m 2^{(n-s-1)-m}} =$$

$$\prod_{m=0}^{n-1} e^{2i\pi j_m 2^{(n-s-1)-m}} =$$

$$\prod_{m=0}^{n-s-1} e^{2i\pi j_m 2^{(n-s-1)-m}} \times \prod_{m=n-s}^{n-1} e^{2i\pi j_m 2^{(n-s-1)-m}} \tag{3.9}$$

Ahora bien, notese que el término de la izquierda es $e^{2i\pi M}$ donde M es entero, y esta expresión es igual a 1. Asi que la ecuacion 3.9 da igual a

$$\prod_{m=n-s}^{n-1} e^{2i\pi j_m 2^{(n-s-1)-m}}$$

y la ecuación 3.8 expresando j en notación binaria es igual a

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \prod_{m=n-s}^{n-1} e^{2i\pi j_m 2^{(n-s-1)-m}} \end{pmatrix} =$$

$$\bigotimes_{s=1}^{n} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{2i\pi 0.j_{n-s} j_{n-s+1} \cdots j_{n-1}} \end{pmatrix} =$$