UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

INTRODUCCIÓN A LA TEORÍA DE LA INFORMACIÓN CUÁNTICA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A :

DANIEL GIBRÁN MENDOZA VÁZQUEZ

DIRECTOR DE TESIS:
DR. OCTAVIO HÉCTOR CASTAÑOS GARZA
2010

1.Datos del alumno	1.Datos del alumno
Apellido paterno	Mendoza
Apellido materno	Vázquez
Nombre(s)	Daniel Gibrán
Teléfono	55418811
Universidad Nacional Autónoma de México	Universidad Nacional Autónoma de México
Facultad de Ciencias	Facultad de Ciencias
Carrera	Ciencias de la Computación
Número de cuenta	300163971
2.Datos del tutor	2.Datos del tutor
Grado	Dr.
Nombre(s)	Octavio Héctor
Apellido paterno	Castaños
Apellido materno	Garza
3.Datos del sinodal 1	3.Datos del sinodal 1
Grado	Dr.
Nombre(s)	Eduardo
Apellido paterno	Nahmad
Apellido materno	Achar
4.Datos del sinodal 2	4.Datos del sinodal 2
Grado	Dr.
Nombre(s)	José de Jesús
Apellido paterno	Galaviz
Apellido materno	Casas
5.Datos del sinodal 3	5.Datos del sinodal 3
Grado	Dr.
Nombre(s)	Ramón
Apellido paterno	Lopez
Apellido materno	Peña
6.Datos del sinodal 4	6.Datos del sinodal 4
Grado	L. en M. A. C.
Nombre(s)	José Hugo Max
Apellido paterno	Nava
Apellido materno	Kopp
7.Datos del trabajo escrito.	7.Datos del trabajo escrito.
Título	Introducción a la Teoría de la Información Cuántica
Número de páginas	153 p.
Año	2010

Dedicado a:

A mi madre, que me he enseñado lo valioso de la vida, mi padre, que ha sido un ejemplo de trabajo, mi hermano que siempre ha sido mi soporte y a Gabriel, mi sobrino, una nueva razón para seguir.

A mi abuelo, por su alegría y sus consejos, que siempre me inspiraron seguir adelante.

Cinco minutos bastan para soñar toda una vida,
así de relativo es el tiempo.
Mario Benedetti.

Indice

Introducción

El progreso en las ciencias de la computación en los últimos años se ha dado en un ambiente multidisciplinario. Dentro de este ambiente se encuentra la mecánica cuántica, que nos ofrece nuevas formas de procesamiento y de transmisión de información. Formas que rompen con los esquemas elaborados en la teoría de la información y el cómputo clásico. En la actualidad la tecnología tiende a un mejor desempeño y una miniaturización de sus componentes, entrando en juego la llamada ley de Moore (1970 Gordon Moore, co-fundador de la Corporación Intel), que establece que la rapidez de la evolución tecnológica logra que la potencia de una computadora se duplique aproximadamente cada 18 meses, permitiendo alcanzar en un momento dado los límites físicos del procesamiento clásico de la información. Se debe de entender a una computadora como cualquier medio físico capaz de almacenar y procesar información a través de la ejecución de algoritmos.

La miniaturización de los instrumentos electrónicos a dimensiones menores a los 10 nanómetros ocasionarán el surgimiento de los efectos cuánticos. Es uno de los propósitos de este trabajo el indicar cómo se usan esas propiedades cuánticas para obtener mejores capacidades de cómputo.

En los sistemas cuánticos se procesa información a través de la manipulación controlada de los bits cuánticos que se han denotado por la palabra qubits. Su potencial proviene de dos principios básicos: (i) El qubit puede existir en una mezcla de dos estados posibles el $\mid 0\rangle$ y $\mid 1\rangle$ al mismo tiempo. (ii) Qubits separados pueden entrelazarse de tal manera que el destino de uno de ellos esté amarrado al de otro, aún si no vuelven a estar en contacto.

Por estos dos hechos como veremos a lo largo del trabajo se tiene que una computadora cuántica podría almacenar y procesar más información que un sistema convencional y su capacidad crecerá en forma exponencial con el número de qubits.

En 1961 Rolf Landauer, científico alemán, planteó que la información tiene una manifestación física: cuando se pierde en un circuito irreversible, la información se convierte en entropía y se disipa como calor. Este fue el primer acercamiento de la teoría de la información desde un punto de vista físico, pero fue hasta 1981 cuando Richard Feymann, físico del California Institute of Technology, propuso durante la "Primer Conferencia sobre la Física de la Computación" que los sistemas físicos, incluidos los de nivel cuántico, podrían ser simulados de una manera más eficiente por computadoras cuánticas que por una computadora clásica.

Más tarde en 1985, el físico israelí David Deutsch introdujo la idea de la primer computadora cuántica universal. Fue a partir de esta fecha que surgió la idea de que una computadora cuántica podría ejecutar diferentes algoritmos cuánticos.

En 1994 surgió el primer algoritmo cuántico, el algoritmo de factorización de Shor, rompiendo con todos los paradigmas hasta ese momento conocidos en computación, combinando principios de la mecánica cuántica con la teoría de números. Este algoritmo pone en riesgo los sistemas criptográficos manejados en la actualidad, reduciendo el tiempo de ejecución del algoritmo de factorización de manera exponencial.

Aprovechando las ventajas de la mecánica cuántica se realiza un cómputo más eficiente que el cómputo clásico, naciendo así una nueva manera de manejar la información y una nueva área en física y computación teórica.

La computación cuántica ofrece un nuevo enfoque en la resolución de problemas computacionales. Se ha demostrado que en ciertos problemas la complejidad de un algoritmo clásico puede ser mucho mayor a la complejidad de la misma tarea realizada por un algoritmo cuántico, destacando algoritmos en el área de búsquedas algorítmicas y en criptografía cuántica. Además la teoría de la información cuántica ofrece nuevos protocolos de transmisión de información entre dos sistemas cuánticos distantes.

Como veremos en el desarrollo del trabajo, si existieran las computadoras cuánticas se podrían, como lo indicó Feynman, resolver problemas que no lo pueden hacer las computadoras convencionales. En cuanto a la comunicación cuántica, pueden diseñarse sistemas criptográficos, el arte de la comunicación secreta, que sean inviolables por las propiedades de un sistema cuántico, permitiéndose entonces el intercambio seguro de información sobre redes sin el peligro de una intromisión.

Esta relevancia ha dado lugar al establecimiento de programas de desarrollo de la teoría de la información cuántica que podemos decir está dividida en tres grandes ramas: la computación cuántica, la comunicación cuántica y la criptografía cuántica. Estas tres ramas serán descritas en el presentre trabajo.

En particular en el "NIST" [1] se tiene un esfuerzo coordinado de aproximadamente 10 grupos de investigación y otros tres adicionales que han construido un prototipo de procesador cuántico de 10 qubits [1].

Para el establecimiento de los qubits consideran sistemas efectivos de dos niveles que pueden enredarse para realizar operaciones lógicas. Utilizan haces láser para controlar los estados internos y de movimiento de iones atrapados o átomos neutros. Otros grupos usan microondas para controlar sistemas cuánticos microscópicos de átomos artificiales consistiendo de circuitos superconductores integrados [2, 3].

Para las comunicaciones cuánticas se han desarrollado detectores de un solo fotón. Entre los logros de la comunidad científica encontramos la demostración del proceso de teletransportación de estados atómicos que ha causado un gran impacto. Finalmente podemos mencionar que se han realizado investigaciones para desarrollar métodos prácticos para la corrección de errores en el manejo de datos para computación cuántica, en particular se ha considerado la creación de datos redundantes, bajo el entendimiento de que si alguien no entiende un concepto lo repites varias veces y eventualmente se conseguirá el entendimiento.

La finalidad de este trabajo es elaborar una completa introducción a la teoría de la información cuántica, entender su proceso de elaboración, sus capacidades, sus limitantes y sus diferencias con el cómputo clásico.

[1] NIST, National Institute of Standard and Technology, Estados Unidos.

El primer capítulo se desarrolla en las herramientas matemáticas necesarias para trabajar con la teoría de la información cúantica, junto con los postulados que rigen la mecánica cuántica (descripción, medición y evolución de un sístema cuántico). Se define uno de los fenómenos más interesantes para la teoría de la información cuántica, el entrelazamiento cuántico, explotar este fenómeno permite desarrollar nuevas maneras de procesar información (teleportación cuántica y codificado denso) y mejorar las complejidades, esto es en los tiempos para la realización de problemas de cálculo, en el desarrollo de algoritmos computacionales.

En el segundo capítulo se establecen las bases sobre las que se empieza a construir cualquier procesamiento de información cuántica (algoritmos cuánticos), su representación y su medición. Al igual que en el computo clásico se definen compuertas cuánticas que nos ayudan a expresar las operaciones básicas que actúan sobre los bits cuánticos. Posteriormente, se realiza una descripción de los algoritmos cuánticos más importantes. Finalmente se da una breve discusión sobre la universalidad de la computadora cuántica.

En el Capítulo 3 se estudia una de las aplicaciones con mayor crecimiento en la teoría de la Información Cuántica: la Comunicación Cuántica. Dentro de ella se trata a la criptografía cuántica, la codificación cuántica y la teleportación cuántica, sus ventajas sobre la comunicación clásica y una serie de ejemplos que nos ayudan a entender estos nuevos procesos de información.

Finalmente en el Capítulo 4 también se describe como medir la información recibida a través de canales cuánticos, su analogía con la información clásica y su utilidad. Como puede realizarse la compresión de información cuántica y cómo medir la cantidad de información accesible sobre un canal cuántico.

Finalmente quiero mencionar que ninguna otra rama de la física y de la computación involucra de una manera tan amplia y estrecha una relación entre la teoría, la experimentación y la tecnología.

Capítulo 1

Fundamentos de la Mecánica Cuántica

En esta sección introduciremos las bases matemáticas fundamentales para empezar a trabajar con la Teoría de Información Cuántica, trabajaremos sobre espacios vectoriales discretos, debido a que los sistemas cuánticos que manejaremos (computadora cuántica) son sistemas físicos discretos, no continuos. Se dará una breve introducción a la notación de Dirac y su aplicación en la mecánica cuántica. Una vez establecidas las bases matemáticas se describirán los Postulados de la Mecánica Cuántica: Descripción del estado de un sistema, descripción de cantidades físicas, medición de cantidades físicas, reducción del paquete de ondas, evolución temporal, postulado de simetrización y variables de espín. Finalmente se definirá el enredamiento cuántico, su importancia en el cómputo cuántico y los sistemas de dos niveles.

1.1. Antecedentes

Delta de Kronecker

La delta de Kronecker, $\delta_{n,m}$ es un símbolo que representa dos posibes valores, dependiendo de sus índices,

$$\delta_{n,m} \begin{cases} 1 & , n = m \\ 0 & , n \neq m \end{cases}.$$

Dado que el símbolo sólo es diferente de cero cuando sus índices son iguales, las sumas que incluyen la delta de Kronecker pueden ser simplificadas fácilmente

$$\sum_m \delta_{mn} B_m = 0 \cdot B_1 + 0 \cdot B_2 + \cdots + 1 \cdot B_n + \cdots = B_n$$

Notación de Dirac

En 1930 en el libro Principios de la Mecánica Cuántica Paul Dirac introdujo una poderosa notación para poder describir estados cuánticos y funciones lineales, también conocida como notación Bra-Ket. Con la notación de Dirac podemos representar un estado base de n elementos con una cadena binaria de longitud n, mientras que con la representación de

vectores columna necesitariamos 2^n componentes para definir el mismo vector.

Ket

Asociamos a cada función de onda un vector (o ket) en un espacio vectorial lineal ξ ,

$$\psi \longrightarrow \mid \psi\rangle$$

tal que la información cuántica del sistema se almacena en sí mismo. La información de este vector ket puede verse como un vector columna. Un ket nos ayuda a definir el estado de un sistema físico.
Si tenemos dos estados cuánticos distintos $\mid \alpha_1\rangle$ y $\mid \alpha_2\rangle$ entonces el ket

$$\mid \psi\rangle = c_1 \mid \alpha_1\rangle + c_2 \mid \alpha_2\rangle \tag{1.1.1}$$

donde c_i es un número complejo, es también un posible estado del sistema.

Bra

Dirac definió un vector bra como una función lineal que asocia un número complejo a todo ket de ξ mediante el producto escalar. Asumimos que para cada ket $\mid \alpha\rangle$ existe un bra, y lo denotamos como $\langle\alpha \mid$. El bra es llamado el dual de el vector ket. Entonces se puede referir al vector bra $\langle\alpha \mid$ como un vector renglón, permitiendo asi el producto de un vector renglón con un vector columna $\langle\alpha \mid \beta\rangle$.
El bra asociado al ket $\mid \psi\rangle$ definido en la ecuación (1.1.1) está dado por

$$\langle\gamma \mid = c_1^*\langle\alpha_1 \mid + c_2^*\langle\alpha_2 \mid \tag{1.1.2}$$

La norma del ket es real, no negativo, y se define como: $\| \mid \psi\rangle \| \equiv \sqrt{\langle\psi \mid \psi\rangle} \geq 0$, donde la norma es igual a cero únicamente si el ket $\mid \psi\rangle$ es cero.

Producto Interno

El producto interno de un par de vectores $\mid \alpha\rangle, \mid \beta\rangle$ es un número complejo denotado por

$$\langle\alpha \mid \beta\rangle = \langle\beta \mid \alpha\rangle^* \tag{1.1.3}$$

donde $\langle\alpha \mid \alpha\rangle \geq 0$. Si su producto interno es cero entonces los vectores son ortogonales.

Producto externo

Se define el produto externo como

$$\mid \alpha\rangle\langle\beta \mid$$

que denota un operador que mapea el ket $\mid \rho\rangle$ a otro ket mediante el bra $\langle\beta \mid$

$$\mid \alpha\rangle\langle\beta \mid \rho\rangle = c \mid \alpha\rangle$$

donde $c = \langle \beta \mid \rho \rangle$.
Con este producto externo podemos construir un operador de proyección $P = \mid \alpha\rangle\langle\alpha \mid$, con $\langle \alpha \mid \alpha \rangle = 1$, tal que $P^2 = P \cdot P = \mid \alpha\rangle\langle\alpha \mid\mid \alpha\rangle\langle\alpha \mid = \mid \alpha\rangle\langle\alpha \mid = P$.

Sea $\mid a_i\rangle = \langle \alpha_i \mid \alpha \rangle$ para $i = 1, \ldots n$ y $\mid \alpha \rangle \in \xi$ entonces

$$\left(\sum_{i=1}^{N} \mid \alpha_i\rangle\langle\alpha_i \mid \right) \mid \alpha \rangle = \sum_{i=1}^{N} \mid \alpha_i\rangle\langle\alpha_i \mid \alpha \rangle = \sum_{i=1}^{N} a_i \mid \alpha \rangle = \mid \alpha \rangle$$

Entonces en una base discreta de dimensión N, el operador identidad puede escribirse

$$I = \sum_{i,j=1}^{N} \mid \alpha_i\rangle\delta_{i,j}\langle\alpha_j \mid = \sum_{i=1}^{N} \mid \alpha_i\rangle\langle\alpha_i \mid, \tag{1.1.4}$$

donde $\delta_{i,j} = 0$ para todo $i \neq j$ y $\delta_{i,j} = 1$ para $i = j$.

Espacio de Hilbert

Los espacios de Hilbert [4], creados por el matemático David Hilbert, fueron formalizados por John Von Neumann y se convirtieron en el soporte matemático de la física y mecánica cuántica del primer cuarto del siglo XX.
Un espacio de Hilbert es un espacio vectorial H completo[1] con respecto a la norma vectorial con producto interno $\langle f, g \rangle$. Donde la norma se encuentra definida por

$$\| f \| = \sqrt{\langle f, f \rangle}. \tag{1.1.5}$$

Dado un espacio de Hilbert H de dimensión 2^n (consideramos un espacio de estas dimensiones debido a que sera la dimensión de los espacios que nos interesan en la teoría de la información cuántica).Un conjunto de 2^n vectores $B = \{\mid b_m\rangle\} \subseteq H$ es llamado una base ortonormal en H si

$$\langle b_n \mid b_m \rangle = \delta_{n,m} \qquad \forall\, b_m, b_n \in B \tag{1.1.6}$$

y todo $\mid \psi\rangle \in H$ puede ser escrito como

$$\mid \psi\rangle = \sum_{b_n \in B} \psi_n \mid b_n\rangle \qquad \text{para algún } \psi_n \in \mathbb{C}. \tag{1.1.7}$$

Los valores de ψ_n satisfacen $\psi_n = \langle b_n \mid \psi \rangle$ y son los coeficientes de $\mid \psi\rangle$ con respecto a la base $\{\mid b_n\rangle\}$.
Un ejemplo de una base ortonormal para un H de dimensión 4 es $\{\mid 00\rangle, \mid 01\rangle, \mid 10\rangle, \mid 11\rangle\}$ que es conocida como base computacional. En estas bases se etiquetan los 2^n vectores bases en la notación de Dirac mediante cadenas binarias de longitud n.

[1]Completo significa que cualquier sucesión de Cauchy de elementos del espacio converge a un elemento en el espacio. Una sucesión de Cauchy es una sucesión tal que la distancia entre dos términos se va reduciendo a medida que se avanza en la sucesión.

Operadores lineales

Un operador lineal A en H asocia a cada vector (ket) $\mid \psi\rangle$ otro ket, $\mid \psi\,'\rangle = A \mid \psi\rangle \epsilon\, H$ en una correspondencia lineal:

$$A\left[\lambda_1 \mid \psi_1\rangle + \lambda_2 \mid \psi_2\rangle\right] = \lambda_1 A \mid \psi_1\rangle + \lambda_2 A \mid \psi_2\rangle \;\forall\; \lambda_{1,2} \,\epsilon\, \mathbb{C}$$

Se define la acción de un operador compuesto AB sobre un ket $\mid \psi\rangle$ como $A\left[B \mid \psi\rangle\right]$. Si los operadores no conmutan entre sí , el orden de la aplicación hace una diferencia. Definimos el conmutador de dos operadores como el operador compuesto $[A, B] \equiv AB - BA$. Si $[A, B] \neq 0$ entonces $AB \mid \psi\rangle \neq BA \mid \psi\rangle$.

Un operador lineal A actúa sobre un ket $\mid \psi\rangle = \sum_i a_i \mid u_1\rangle$ produciendo otro ket $A \mid \psi\rangle$ al cual le corresponden componentes $b_i = \langle u_i \mid A\,\psi\rangle$ dadas por:

$$b_i = \langle u_i \mid A\psi\rangle = \langle u_i \mid A \sum_j a_j \mid u_j\rangle = \sum_j a_j \langle u \mid A \mid u_j\rangle = \sum_j \alpha_{ij} a_j,$$

donde definimos $\alpha_{ij} = \langle u \mid A \mid u_j\rangle$ y el conjunto $\{\mid u_i\rangle, \forall_i\}$ son los estados propios de $\hat{A}$.

Operador Autoadjunto

Dado un operador lineal A se le asocia otro operador $A^\dagger$ (el adjunto de A) a través de la relación

$$\langle \Theta \mid A \mid \psi\rangle^* = \langle \psi \mid A^\dagger \mid \Theta\rangle.$$
$$A^\dagger = (A^*)^T.$$

Un operador que cumple con la iguadad $A = A^\dagger$ se la llama **hermiteano**. Si adicionalmente el dominio de A es el mismo que el de $A^\dagger$ entonces el operador es autoadjunto. Esta distinción es únicamente relevante en espacios de dimensión infinita. Estos operadores son importantes en la Teoría de la Información Cuántica porque representan observables físicas. Los valores propios de un operador hermiteano son reales.

Operadores Unitarios

Un operador unitario se define por la relación:

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

Una propiedad importante de los operadores unitarios es que conservan la norma dado que $\langle \psi \mid \psi\rangle = \langle \psi \mid U^\dagger U \mid \psi\rangle$. Por otro lado cabe destacar que los valores propios de un operador unitario tienen módulo 1. Entonces se pueden definir en términos de fases reales, $\varphi\,\epsilon\,[0,\, 2\pi]$ con valor propio $e^{i\varphi}$.

Producto Tensorial

El producto tensorial es una forma de combinar espacios, operadores y vectores. Suponiendo que H_1 y H_2 son espacios de Hilbert de dimensión n y m respectivamente. Entonces el espacio generado por el producto tensorial $H_1 \otimes H_2$ es un nuevo y más grande espacio

de Hilbert de dimensión $n \times m$. El producto tensorial de dos vectores $\mid \psi_1\rangle$ y $\mid \psi_2\rangle$ cuyos espacios son H_1 y H_2 respectivamente es un vector en $H_1 \otimes H_2$ denotado como $\mid \psi_1\rangle \otimes \mid \psi_2\rangle$. Suponiendo que A y B son dos operadores lineales sobre H_1 y H_2 respectivamente entonces $A \otimes B$ es el operador lineal en $H_1 \otimes H_2$ definido por

$$(A \otimes B)\,(\mid \psi_1\rangle \otimes \mid \psi_2\rangle) = A \mid \psi_1\rangle \otimes B \mid \psi_2\rangle \tag{1.1.8}$$

1.2. Postulados

1.2.1. Descripción del estado de un sistema

Un estado cuántico es un objeto matemático que describe completamente un sistema cuántico. Podemos caracterizar el estado cuántico de una partícula por medio de un vector de estado, perteneciente a un espacio vectorial de estados $\xi \in \mathcal{H}$. Un vector de estado indica el estado en que se encuentra un sistema cuántico.

Cualquier elemento o vector del espacio ξ es llamado *vector ket* o *ket* y es representado bajo el símbolo $\mid \varphi\rangle$ (Ver Preliminares). El simbolo dentro del vector (en nuestro ejemplo φ) nos sirve para distinguir el *vector ket* de otros vectores. Asociamos a cada función de onda un vector ket en el espacio ξ, de modo que toda la información sobre el estado cuántico del sistema a describir está contenido en el mismo.

Postulado 1: **En un tiempo dado t_0, el estado de un sistema físico está definido especificando el ket $\mid \varphi(t_0)\rangle$, perteneciente al espacio de estados ξ.**

Como ξ es un espacio vectorial el primer postulado implica el principio de superposición: una combinción lineal de vectores de estado es un vector de estado. Esto tiene fuertes implicaciones en la Teoría de la Información Cuántica ya que clásicamente un sistema de dos estados $(\mid 0\rangle, \mid 1\rangle)$ puede ser usado para represetar un bit de información, pero cuánticamente el estado también puede estar "simultáneamente" en una combinación lineal de estados $(\mid \varphi\rangle = \lambda_1 \mid 0\rangle + \lambda_2 \mid 1\rangle)$.

1.2.2. Descripción de cantidades físicas

Postulado 2: **Toda cantidad física medible, $\mathcal{A}$ está descrita por un operador A actuando en el espacio ξ , y este operador es un observable, es decir un operador hermiteano cuyos vectores propios son una base de ξ.**

Es decir todo observable físico esta representado por operadores hermiteanos que operan sobre los vectores ket y sus eigenvectores constituyen una base del espacio. Un operador hermíteano definido sobre un espacio de Hilbert es un operador lineal que, sobre un cierto dominio, coincide con su propio operador adjunto (Ver Antecedentes). Una propiedad importante de estos operadores es que sus eigenvalores son siempre números reales y por lo tanto nuestro operador tendrá que ser Hermiteano. Otra propiedad importante de los operadores Hermiteanos es que sus vectores propios son ortogonales. Algunos operadores comunes en mecánica cuántica son: operador momento, operador posición, operador de momento angular, etc. A diferencia de la mecánica clásica la mecánica cuántica describe de

manera diferente el estado de un sistema y sus cantidades físicas asociadas. Un estado es representado por un vector y una cantidad física por un operador.

1.2.3. Medición de cantidades físicas

El operador asociado con la energía de un sistema es conocido como operador Hamiltoniano. La conexión entre el operador Hamiltoniano $\mathcal{H}$ y la energía total de una partícula se relacionan de la siguiente manera: las únicas energías posibles son los valores propios del operador $\mathcal{H}$. Esta relación puede ser extendida a todas las cantidades físicas.

Postulado 3: El único resultado posible de la medición de $\mathcal{A}$ es uno de los valores propios correspondientes a la observable.

Una medición de A siempre nos dará un valor real dado que por definición A es Hermiteano.
Si tenemos un observable A entonces podemos obtener los siguientes espectros (recordemos que un espectro es el conjunto de valores propios de A).

- Caso de un espectro discreto con valores propios no-degenerados: A cada valor propio a_n de A se le asocia un único vector propio $\mid u_n\rangle$:

  $$A \mid u_n\rangle = a_n \mid u_n\rangle.$$

  Como A es un observable el conjunto de los $\mid u_n\rangle$, que en nuestro caso está normalizado, constituyen una base en ξ , y el vector estado $\mid \psi\rangle$ puede ser escrito como:

  $$\mid \psi\rangle = \sum_n c_n u_n. \tag{1.2.1}$$

  La probabilidad $P(a_n)$ de encontrar a_n cuando medimos la observable A está dada por:

  $$P(a_n) = \mid c_n \mid^2 = \left|\langle u_n \mid \psi\rangle\right|^2 \tag{1.2.2}$$

  recordemos que $\mid u_n\rangle$ es el vector propio de A asociado con el valor propio a_n.

- Caso de un espectro discreto con valores propios degenerados: Si algunos valores propios de a_n son degenerados entonces varios vectores propios ortonormalizados $\mid u_n^i\rangle$ corresponden a

  $$A \mid u_n^i\rangle = a_n \mid u_n^i\rangle\,; \quad i = 1, 2, \ldots, g_n, \tag{1.2.3}$$

  donde g_n indica el orden de la degeneración del propio de a_n. Como los $\{\mid u_n^i\rangle\}$ constituyen una base en el subespacio propio E_n asociado con el valor propio a_n de A entonces$\mid \psi\rangle$ puede desarrollarse

  $$\mid \psi\rangle = \sum_n \sum_{i=1}^{g_n} c_n^i \mid u_n^i\rangle, \tag{1.2.4}$$

En este caso la probabilidad $P(a_n)$ esta dada por

$$P(a_n) = \sum_{i=1}^{g_n} \mid c_n^i \mid^2 = \sum_{i=1}^{g_n} \left|\langle u_n^i \mid \psi\rangle\right|^2 \tag{1.2.5}$$

donde g_n es el grado de degeneración de a_n.
Como el valor propio de a_n es degenerado entonces la probabilidad $P(a_n)$ será independiente de la base $\{\mid u_n^i\rangle\}$ escogida en E_n.

Notemos que el caso del espectro discreto con valores propios no degenerados se obtiene de la ecuación (1.2.5) si tomamos $g_n = 1$.

- Caso de un espectro continuo y no degenerado: Sea el sistema de vectores propios ortonormales $\mid v_\alpha\rangle$ de A dado por

$$A \mid v_\alpha\rangle = \alpha \mid v_\alpha\rangle. \tag{1.2.6}$$

que forma una base continua en E, de manera que $\mid \psi\rangle$ puede ser expandido como

$$\mid \psi\rangle = \int d\alpha\, c(\alpha) \mid v_\alpha\rangle. \tag{1.2.7}$$

Como los posibles resultados de una medición de A forman un conjunto continuo, se define una densidad de probabilidad. Entonces la probabilidad $dP(\alpha)$ de obtener un valor entre α y $d\alpha$ será

$$dP(\alpha) = p(\alpha)\, d\alpha, \tag{1.2.8}$$

con

$$p(\alpha) = \mid c_\alpha \mid^2 = \left|\langle v_\alpha \mid \psi\rangle\right|^2. \tag{1.2.9}$$

Un importante resultado de este postulado es que dados dos kets $\mid \psi\rangle$ y $\mid \psi^{'}\rangle$ tal que

$$\mid \psi^{'}\rangle = e^{i\theta} \mid \psi\rangle, \tag{1.2.10}$$

donde θ es un número real, si $\mid \psi\rangle$ está normalizada entonces $\mid \psi^{'}\rangle$ también lo estará

$$\langle \psi^{'} \mid \psi^{'}\rangle = \langle \psi \mid e^{-i\theta} e^{i\theta} \mid \psi\rangle = \langle \psi \mid \psi\rangle = 1. \tag{1.2.11}$$

Las probabilidades dadas por una medición arbitraria serán las mismas para $\mid \psi\rangle$ y $\mid \psi^{'}\rangle$ dado que para cualquier $\mid u_n^i\rangle$

$$\left|\langle u_n^i \mid \psi^{'}\rangle\right|^2 = \left|e^{i\theta}\langle u_n^i \mid \psi\rangle\right|^2 = \left|\langle u_n^i \mid \psi\rangle\right|^2. \tag{1.2.12}$$

Fases globales no afectan las predicciones físicas (las fases relativas de los coeficientes de una expansión si lo hacen)[5]. Entonces dos vectores estado proporcionales representan el mismo estado físico. Cabe destacar que este postulado de medición no tiene una versión clásica análoga. La mecánica clásica asume que las mediciones pueden ser realizadas sin afectar al sistema. El postulado de medición de la mecánica cuántica describe un diferente escenario. Si nosotros conocemos todo lo que podemos saber de un estado en el sistema únicamente podemos predecir la probabilidad del resultado de la medición.

1.2.4. Reducción del paquete de ondas

Supongamos que queremos medir en un tiempo dado una cantidad física $\mathcal{A}$. Si el ket $\mid \psi\rangle$, que representa el estado de un sistema inmediatamente antes de la medición, es conocido, entonces nuestro postulado de medición (en el caso de un espectro continuo no degenerado) nos permite predecir las probabilidades de los distintos resultados posibles. Pero cuando la medición es realmente realizada, únicamente uno de estos posibles resultados es obtenido. Inmediatamente después de la medición ya no podemos hablar de la probabilidad de haber obtenido tal valor sino de la certeza de conocer el valor de la medición. Se obtiene nueva información y por lo tanto el estado del sistema después de la medición es diferente a $\mid \psi\rangle$. Suponiendo que al medir $\mathcal{A}$ obtenemos el valor propio a_n del observavble $\mathcal{A}$. Entonces el estado del sistema inmediatamente después de la medición está dado por el vector propio $\mid v_n\rangle$ asociado con a_n es

$$\mid \psi\rangle \xrightarrow{(a_n)} \mid v_n\rangle \tag{1.2.13}$$

Si realizamos una segunda medición de $\mathcal{A}$ inmediatamente después de nuestra primer medición (i.e. antes de que el sistema tenga tiempo de evolucionar), entonces siempre encontraremos el mismo resutado a_n ya que el estado de sistema inmediatamente antes a la segunda medición es $\mid v_n\rangle$.
Cuando el valor propio obtenido a_n es degenerado entonces la ecuación (1.2.13) puede ser generalizada de la siguiente manera. Si la expansión del estado $\mid \psi\rangle$ inmediatamente antes de la medición la denotamos como en (1.2.4)

$$\mid \psi\rangle = \sum_n \sum_{i=1}^{g_n} c_n^i \mid u_n^i\rangle \tag{1.2.14}$$

la modificación del vector estado debido a la medición queda como

$$\mid \psi\rangle \xrightarrow{(a_n)} \frac{1}{\sqrt{\sum_{i=1}^{g_n} |c_n^i|^2}} \sum_{i=1}^{g_n} c_n^i \mid u_n^i\rangle, \tag{1.2.15}$$

donde $\sum_{i=1}^{g_n} c_n^i \mid u_n^i\rangle$ es el vector $\mid \psi_n\rangle$, es decir, la proyección de $\mid \psi\rangle$ en el subespacio asociado a a_n. Los coeficientes de c_n^i son los mismos obtenidos en la expansión de $\mid \psi\rangle$

$$c_n^i = \langle u_n^i \mid \psi\rangle, \tag{1.2.16}$$

donde

$$\langle \psi_n \mid \psi_n\rangle = \sum_{i=1}^{g_n} \left|c_n^i\right|^2. \tag{1.2.17}$$

Entonces podemos escribir $\mid \psi_n\rangle$ como

$$\mid \psi_n\rangle = \sum_{i=1}^{g_n} \mid u_n^i\rangle\langle u_n^i \mid \psi\rangle = P_n \mid \psi\rangle, \tag{1.2.18}$$

donde $P_n = \sum_{i=1}^{g_n} \mid u_n^i\rangle\langle u_n^i \mid$. En la ecuación 1.2.15 el vector se encuentra normalizado debido a que la probabilidad total debe ser uno.

Entonces el estado de un sistema inmediatamente después de la medición es la proyección normalizada

$$\mid \psi\rangle \xrightarrow{(a_n)} \frac{P_n \mid \psi\rangle}{\sqrt{\langle \psi \mid P_n \mid \psi\rangle}}. \tag{1.2.19}$$

Por lo tanto el estado de un sistema inmediatamente después de la medición siempre será un vector propio de A con el valor propio a_n.

1.2.5. Evolución Temporal

La evolución temporal de un vector estado está dado por la ecuación de Schrödinger

$$i\hbar \frac{d}{dt} \mid \psi(t)\rangle = H(t) \mid \psi(t)\rangle, \tag{1.2.20}$$

donde $H(t)$ es el observable asociado con la energía total del sistema. H es el operador Hamiltoniano del sistema y se obtiene del Hamiltoniano clásico. Recordemos que si conocemos el Hamiltoniano del sistema entonces podemos conocer su dinámica completamente.
Es decir la evolución dinámica de un sistema cuántico es reversible y determinista. Como la ecuación (1.2.20) es lineal entonces una combinación lineal de sus soluciones será también solución. Recordemos que $\mid \psi\rangle$ y $e^{i\theta} \mid \psi\rangle$ representan el mismo estado. Se define un operador evolución $U(t_0, t)$ que al aplicarse a$\mid \psi(t_0)\rangle$ nos da $\mid \psi(t)\rangle$. Podemos expresar la ecuación (1.2.20) como

$$\frac{d \mid \psi\rangle}{\mid \psi\rangle} = -i\hbar H(t)dt. \tag{1.2.21}$$

Si integramos (1.2.21) obtenemos

$$\mid \psi(t)\rangle = T\left\{exp\left[-\frac{i}{h}\int_{t_o}^{t} H(t')dt'\right]\right\} \mid \psi(t_0)\rangle = U \mid \psi(t_0)\rangle, \tag{1.2.22}$$

donde el símbolo $T\{\}$ significa integral odenada temporalmente.
Si el sistema que se está describiendo es conservativo, su energía es una constante del movimiento y el operador H no depende del tiempo. Entonces el operador de evolución entre t_1 y t_2 es

$$U(t_i, t_2) = e^{-\frac{i}{\hbar}H(t_2 - t_1)}. \tag{1.2.23}$$

Como el hamiltoniano es hermiteano, $U^\dagger U = 1$. La evolución temporal de un sistema cuántico cerrado está descrita por un operador unitario. Después de la evolución el estado de sistema será

$$\mid \psi(t)\rangle = U \mid \psi(t_0)\rangle. \tag{1.2.24}$$

1.2.6. Postulado de simetrización

Dos o más particulas son indistinguibles si ningún valor de expectación de cualquier observable se ve afectado por las permutaciones de las partículas. En un sistema de N partículas indistinguibes, los únicos posibles estados del sistema son aquellos descritos por vectores que son (respecto a las permutaciones de las partículas):

Completamente simétricos: En este caso las partículas son llamadas bosones

$$\mid \psi_{a,b}\rangle = \tfrac{1}{\sqrt{2}} \left\{ \mid \varphi\rangle_a \mid \chi\rangle_b + \mid \chi\rangle_a \mid \varphi\rangle_b \right\}.$$

Completamente antisimétricos: En este caso las partículas son llamadas fermiones.

$$\mid \psi_{a,b}\rangle = \tfrac{1}{\sqrt{2}} \left\{ \mid \varphi\rangle_a \mid \chi\rangle - \mid \chi\rangle_a \mid \varphi\rangle_b \right\}.$$

1.2.7. Variables de espín

El grado de libertad intrinseco de una partícula es conocido como espín. Decimos que una partícula tiene espín s si su grado de libertad intrinseco puede ser descrito por una representación del grupo de rotaciones de dimensión $2s+1$. Por ejemplo el espín $\frac{1}{2}$ puede ser descrito por una representación de dimensión 2.
Un electrón tiene espín $\frac{1}{2}$, entonces una diferencia de polarización de 180^{o} (arriba y abajo) significa ortogonalidad.

Definimos $\overrightarrow{S}$ como un vector de operadores

$$\overrightarrow{S} = (S_x, S_y, S_z), \tag{1.2.25}$$

tal que las componentes de $\overrightarrow{S}$ satiface las relaciones de conmutación del momento angular

$$[S_x, S_y] = i\hbar S_z \tag{1.2.26}$$
$$[S_y, S_z] = i\hbar S_x \tag{1.2.27}$$
$$[S_z, S_x] = i\hbar S_y \tag{1.2.28}$$

Estas relaciones de conmutación pueden escribirse de una manera más compacta en términos del producto vectorial

$$\overrightarrow{S} \times \overrightarrow{S} = i\hbar \overrightarrow{S} \tag{1.2.29}$$

que también puede ser escrito como

$$[S_i, S_j] = i\hbar \varepsilon_{i,j,k} S_k \tag{1.2.30}$$

donde

$$\varepsilon_{i,j,k} \begin{cases} +1 & si\ (i,j,k)\ es\ (1,2,3), (3,1,2), (2,3,1) \\ -1 & si\ (i,j,k)\ es\ (3,2,1), (1,3,2), (2,1,3) \\ 0 & i=j\ ;\ j=k\ ;\ k=i \end{cases}$$

Como cualquier momento angular, existe un espacio de Hibert H_s asociado con un espín que soporta valores propios de espín. Un conjunto de vectores base para este espacio de Hibert puede ser construido a partir de vectores propios simultaneos de los operadores $S^2 = |S|^2$ y S_z. Los valores propios asociado los denotamos por s y m_s . S^2 y S_z satisfacen las ecuaciones de valores propios siguientes:

$$S^2 \mid s\, m_s\rangle = \hbar s(s+1) \mid s\, m_s\rangle, \tag{1.2.31}$$
$$S_z \mid s\, m_s\rangle = \hbar m_s \mid s\, m_s\rangle. \tag{1.2.32}$$

Notemos que

$$S^2 = S_x^2 + S_y^2 + S_z^2 \tag{1.2.33}$$

y es un operador tal que conmuta con sus componentes

$$\left[S^2, S_i\right] = 0. \tag{1.2.34}$$

El espacio de Hilbert del espín H_s debe unirse al espacio de Hilbert H_r asociado con las variables clásicas de posición y momento $\overrightarrow{R}$ y $\overrightarrow{P}$. Esto es logrado realizando el producto tensorial de espacios

$$H = H_s \otimes H_r, \tag{1.2.35}$$

por supuesto las varibles de espín conmutan con $\overrightarrow{R}$ y $\overrightarrow{P}$

$$[S_i, R_j] = [S_i, P_j] = 0. \tag{1.2.36}$$

Como el electrón es una partícula cargada, el espín del electrón da lugar a un momento magnético $\overrightarrow{\mu}$ intrínseco o de espín. La relación que existe entre el vector momento magnético y el espín es $\overrightarrow{\mu} = 2\frac{\mu_B \overrightarrow{S}}{\hbar}$, es una cantidad donde

$$\mu_B = \frac{e\hbar}{2m} \qquad \text{Magnetón de Bohr.} \tag{1.2.37}$$

A continuación se discuten experimentos y conceptos muy importantes tanto en el desarrollo de la teoría de la información cuántica como en el establecimiento de los qubits.

1.3. Experimento de la doble rendija

Una manera sencilla de ilustrar algunas peculiaridades de la Mecánica Cuántica es el experimento de la doble rendija de Young [19], que en 1981 se realizó por primera vez con el objetivo de responder la pregunta de si la luz es un haz de partículas o una onda. Durante el transcurso de los años grandes científicos diferenciaron en referencia a esta pregunta. Maxwell afirmaba que la luz era claramente una onda, posteriormente Einstein le regresó a la luz su descripción como partícula en su teoría del efecto fotoeléctrico. El experimento de Young realiza una completa descripción de este fenómeno que sólo puede ser obtenida si aceptamos la dualidad onda-partícula de la luz. Una fuente S emite un haz de luz la cual puede pasar a través de dos rejillas O_1 y O_2 o O_1 u O_2 antes de impactar una pantalla de proyección o una placa fotográfica.

La intensidad de la luz $I(x)$ en un punto x, es proporcional al cuadrado del módulo del campo eléctrico $E(x)$ en el mismo punto. Entonces la intensidad de la luz observada a través de la rejilla O_1 cuando la rejilla O_2 se encuentra cerrada , viene dada por

$$I_1(x) \propto |E_1(x)|^2, \tag{1.3.1}$$

donde $E_1(x)$ es el campo eléctrico producido en x a través de O_1. Análogamente cuando la rejilla O_2 es cerrada se observa

$$I_2(x) \propto |E_2(x)|^2. \tag{1.3.2}$$

Si abrimos ambas rejillas ambos campos se suman algebraicamente

$$E(x) = E_1(x) + E_2(x), \tag{1.3.3}$$

y por lo tanto la intensidad de la luz resultante es

$$I(x) \propto |E(x)|^2 = |E_1(x) + E_2(x)|^2 , \tag{1.3.4}$$

por lo tanto

$$I(x) \neq I_1(x) + I_2(x). \tag{1.3.5}$$

Este resultado va de acuerdo a la teoría de que la luz es una onda.
¿Qué pasa si lanzamos fotones uno por uno?

- Si la cantidad de fotones es limitada, entonces se observan puntos de impacto localizados, por lo tanto se comporta como partícula.
- Si la cantidad de fotones es lo suficientemente grande, entonces aparece un patrón de interferencia, lo que implica que su comporta como ondas.

Esta interferencia sólo es plasmada si no existe un observable; esto implica que no podremos conocer su posición sino únicamente $p(x)$, la probabilidad de que un fotón se plasme en el punto x.

Entonces la descripción de la luz como onda y como partícula no son mutuamente excluyentes, por lo tanto la luz se comporta simultáneamente como onda y partícula.

1.4. El gato de Schrödinger

Para explicar la ambivalencia existente en el proceso de la medición se describe a continuación el experimento legendario del gato de Schrödinger.

Para observar un sistema físico, se hace interactuar con un aparato, el que debe describirse cuánticamente. Pero por otro lado el resultado de la observación es registrada por el aparato en forma clásica, entonces necesitándose una traducción del formalismo del espacio de Hilbert a un lenguaje clásico. Este experimento es el prototipo de ejemplo de la teoría de la información. En donde se establece que los ingredientes esenciales de una medición son el objeto, un aparato y una interacción qe produce una correlación entre variables dinámicas del objeto y las variables del aparato. El gato de Schrödinger permite comparar las dos interpretaciones de la mecánica cuántica de un vector estado, en una de ellas se considera que un estado puro $\mid \psi\rangle$ determine en forma completa un sistema individual y en la otra que únicamente describe las propiedades estadísticas de un ensamble de sistemas preparado en forma similar.

En 1935 Schrödinger atacó el problema de coherencia de la mecánica cuántica, este problema nos ayudará a entender algunas propiedades de la mecánica cuántica. El experimento mental ideado por Schrödinger es el siguiente:

Un gato está encerrado en una cámara de acero (Figura 1.4.1), junto con el siguiente aparato (que debe ser protegido frente a una posible injerencia por parte del gato): en un contador Geiger hay una minúscula cantidad de una sustancia radioactiva, tan pequeña que tal vez, en el transcurso de una hora, uno de los átomos se desintegre, pero también, con

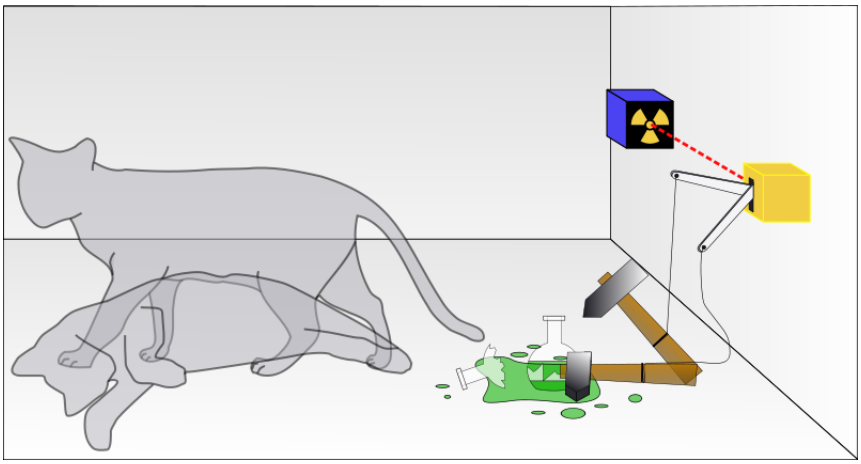


Figura 1.4.1: Experimento del gato de Schrödinger

igual probabilidad, ninguno lo haga; si sucede, el tubo del contador Geiger se descarga y, a través de un dispositivo libera un martillo que rompe un pequeño frasco de ácido cianhídrico. Si se deja este sistema aislado durante una hora, podríamos decir entonces que el gato seguirá vivo si ningún átomo se ha desintegrado. La función de onda de este sistema expresaría esto incluyendo el gato vivo y el gato muerto mezclados o esparcidos en partes iguales, junto con el estado del átomo radioactivo.

Entonces podemos describir la función de onda del estado antes de abrir la caja como

$$\frac{1}{\sqrt{2}} \mid vivo\rangle \mid nd\rangle + \frac{1}{\sqrt{2}} \mid muerto\rangle \mid d\rangle, \tag{1.4.1}$$

donde $\mid nd\rangle$ significa que el átomo no ha decaído y $\mid d\rangle$ que el atomo decae.
Este es un estado correlacionado y también es una superposición de estados macroscópicos diferentes que es típico del proceso de medición.

1.5. Entrelazamiento cuántico

A mediados de los 30´s Einstein, Podolsky y Rosen (EPR) junto con Schrödinger reconocieron una interesante propiedad de la mecánica cuántica que marcó a la física del siglo XX.

Einstein, Podolsky y Rosen describieron el entrelazamiento cuántico en su intento de atribuir valores (elementos de la realidad) a las magnitudes físicas antes de efectuar la medición y el mencionar que la teoría cuántica no es completa[2] excluyendo la posibilidad de acción a distancia (Principio de Localidad). Pero la mecánica cuántica nos arroja resultados contrarios a estos supuestos.

[2]Teoria Completa: A todo elemento de la realidad le corresponde una contraparte de la teoría física.

En 1965 Bell formalizó las conclusiones obtenidas por EPR de la siguiente manera: los resultados obtenidos por una medición se encuentran determinados por las propiedades de las partículas y son independientes de la medición (realismo) y los resultados obtenidos en determinada posición son independientes de cualquier acción realizada fuera de su entorno cercano (localidad). Bell demostró que estos resultados pueden observarse durante experimentos en el laboratorio en forma de las llamadas desigualdades de Bell, de la misma manera también demostró que la mecánica cuántica viola estas desigualdades (Ver 1.6).
En 1935 inspirado por el artículo EPR Schrödinger analizando algunas consecuecias físicas en el formalismo cuántico descubrió un aspecto fundamental del entrelazamiento: *El mejor conocimiento posible de un todo no incluye el mejor conocimiento posible de sus partes.*
Esta propiedad implica la existencia de estados globales de sistemas compuestos que no pueden ser escritos como un producto de estados de cada uno se los subsistemas.

Este fenómeno, conocido como enredamiento o entrelazamiento subraya un órden intrínseco de correlaciones estadísticas entre subsistemas compuestos de sistemas cuánticos. Una manera sencilla de explicar esto es suponer la existencia de dos sistemas cuánticos A y B. Si estos sistemas están entrelazados, significa que los valores de ciertas propiedades del sistema A se correlacionan con los valores que asumirá las propiedades del sistema B. Estas correlaciones se pueden mantener incluso si ambos sistemas se encuentren espacialmente separados.

Por definición, un estado en un espacio de Hibert H se encuentra entrelazado si no puede ser escrito como un producto tensorial de sus estados

$$\mid \psi\rangle \neq \mid \Phi_1\rangle \otimes \mid \Phi_2\rangle. \tag{1.5.1}$$

Los estados que no se encuentran entrelazados son llamados estados separables.

Dicho aspecto del entrelazamiento fue formalizado a mediados de ls 90´s en términos de desigualdades de entropías[3] (Ver Capitulo 3).

La violación de las desigualdades de Bell por estados entrelazados es una característica de los estados cuánticos entrelazados que implica la existencia de información cuántica negativa, aportando un recurso extra en las comunicaciones cuánticas. Posteriormente se descubrió que la capacidad de transmitir información cuántica era posible cuando la entropía de salida del sistema excedía la entropía total del sistema.

Actualmente el entrelazamiento cuántico dió origen a varios descubrimientos relacionados con la información y el cómputo cuántico: Criptografía Cuántica mediante el teorema de Bell, el codificado denso (Capítulo 3) y la teleportación cuántica (Capítulo 3). Todos estos efectos están basados en el entrelazamiento cuántico y han sido demostrados en el laboratorio. Estos resultados dieron origen a lo que conocemos como Información Cuántica la cual incorpora al entrelazamiento como una noción central.

Desafortunadamente el entrelazamiento cuántico tiene una estructura muy compleja, es muy frágil al ambiente y no puede ser aumentado si los sistemas no se encuentran en contacto directo.

Al parecer la aplicación más interesante del entrelazamiento cuántico se da en la criptografía cuántica. Se puede interpretar dicho entrelazamiento como un equivalente cuántico del significado de privacidad. La herramienta básica de esta privacidad es la llave privada

[3]Entropía: Cantidad de información de una variable dada.

secreta. Si los sistemas se encuentran en un entrelazamiento puro entonces dichos sistemas están correlacionados y ningún otro sistema puede estar correlacionado a ellos.

1.6. Estados de Bell

Un estado de Bell o también conocido como par EPR, es definido como un estado de máximo entrelazamiento cuántico de dos qubits. Un estado se encuentra maximamente entrelazado si podemos construir a partir de él cualquier otro estado de la base usando operaciones locales y comunicaciones clásicas (LOCC). Una operación local es aquella operación que no actúa en dos qubits simultáneamente. Cualesquiera otros estados pueden ser formados a través de operaciones unitarias actuando en este estado. Los estados de Bell forman una base ortogonal del espacio de estados cuánticos de dos qubits denominada base de Bell.

$$
\begin{aligned}
|\,\phi^{+}\rangle &= \frac{1}{\sqrt{2}}\left((|\,00\rangle + |\,11\rangle)\right), \\
|\,\phi^{-}\rangle &= \frac{1}{\sqrt{2}}\left((|\,00\rangle - |\,11\rangle)\right), \\
|\,\psi^{+}\rangle &= \frac{1}{\sqrt{2}}\left((|\,01\rangle + |\,10\rangle)\right), \\
|\,\psi^{-}\rangle &= \frac{1}{\sqrt{2}}\left((|\,01\rangle - |\,10\rangle)\right).
\end{aligned}
$$

1.7. Desigualdades de Bell

En 1965 Bell afirmó que todo teoría de variables ocultas y local tiene necesariamente algunas predicciones incompatibles con la Mecánica Cuántica (Teorema de Bell). De este resultado surgen las desigualdades de Bell que toda teoría realista y local debe de satisfacer. Cabe destacar que la mecánica cuántica en general no satisface estas desigualdades.

Suponiendo que tenemos un emisor de partículas: Este emisor prepara dos partículas y las reparte una a Alice y otra a Bob. Una vez que Alice recibe su partícula, realiza una medición sobre ella. Supongamos que Alice cuenta con dos aparatos diferentes de medición tal que ella puede escoger que aparato usar. Si Alice usa el primer aparato las propiedades físicas de la medición vienen dadas por P_Q , de la misma manera para el segundo aparato las propiedades físicas vienen dadas por P_R. Alice escoge aleatoriamente cuál de los dos aparatos usar. Al realizar la medición Alice podrá obtener como resultado -1 o $+1$. Suponiendo que la partícula de Alice tiene un valor Q para la propiedad P_Q. De la misma manera se tiene un valor R para P_R . Similarmente Bob es capaz de medir una de las siguientes propiedades P_S o P_T encontrando los valores S o T respectivamente cada uno con valor -1 o $+1$. Al igual que Alice, Bob escoge aleatoriamente que aparato de medida usar. Una vez que escogieron su aparato de medida, Alice y Bob realizan su medición, tal que la medición realizada por Alice (Bob) no pueda perturbar el resultado de Bob (Alice). El resultado de estas mediciones están regidas por el principio de localidad. Calcularemos el valor de

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T. \tag{1.7.1}$$

Como $R, Q = \pm 1$ entonces $(Q+R)S = 0$ o $(R-Q)T = 0$. En cualquiera de los dos casos obtenemos que $QS + RS + RT - QT = \pm 2$. Se define ahora $p(q,r,s,t)$ como la probabilidad de que el sistema antes de la medición se encuentra en un estado donde, $Q = q, R = r, S = s$ y $T = t$. Estas probabilidades dependen en la forma en que el emisor prepara los estados y si encontramos algún ruido externo. Se denota $E(\cdot)$ como el coeficiente de correlación, entonces

$$\begin{aligned} E\left(QS + RS + RT - QT\right) &= \sum_{q,r,s,t} p(q,r,s,t)(qs + rs + rt - qt) \\ &\leq \sum_{q,r,s,t} p(q,r,s,t) \times 2 \\ &= 2. \end{aligned} \tag{1.7.2}$$

Por otro lado

$$\begin{aligned} E\left(QS + RS + RT - QT\right) &= \sum_{q,r,s,t} p(q,r,s,t)qs + \sum_{q,r,s,t} p(q,r,s,t)rs \\ &\quad + \sum_{q,r,s,t} p(q,r,s,t)rt - \sum_{q,r,s,t} p(q,r,s,t)qt \\ &= E(QS) + E(RS) + E(RT) - E(QT). \end{aligned} \tag{1.7.3}$$

Por (1.7.2) y (1.7.3) se obtiene la desigualdad de Bell

$$E(QS) + E(RS) + E(RT) + E(QT) \leq 2, \tag{1.7.4}$$

esta desigualdad también es conocida como CHSH por Clauser, Horne, Shimony y Holt [21]. Se prepara el mismo experimento pero ahora nuestro emisor prepara sistemas cuánticos de dos qubits tales que se encuentren en el estado

$$|\,\varphi\rangle = \frac{|\,01\rangle - |\,10\rangle}{\sqrt{2}}. \tag{1.7.5}$$

El emisor envía el primer qubit a Alice y el segundo qubit a Bob. Alice y Bob realizan mediciones sobre los siguientes observables:

$$\begin{aligned} Q &= Z_1 \qquad S = \frac{-Z_2 - X_2}{\sqrt{2}} \\ R &= X_1 \qquad T = \frac{Z_2 - X_2}{\sqrt{2}}, \end{aligned} \tag{1.7.6}$$

donde X y Z toman la forma

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.7.7}$$

Si medimos los valores medios (correlaciones cuánticas) con respecto al estado $|\,\varphi>$ de estos observables se obtiene

$$\langle QS\rangle = \frac{1}{\sqrt{2}}; \quad \langle RS\rangle = \frac{1}{\sqrt{2}}; \quad \langle RT\rangle = \frac{1}{\sqrt{2}}; \quad \langle QT\rangle = \frac{1}{\sqrt{2}}, \tag{1.7.8}$$

entonces

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}. \tag{1.7.9}$$

Por lo tanto la desigualdad de Bell no es satisfecha bajo la teoría de la mecánica cuántica.

Este resultado junto con el entrelazamiento es aprovechado en computación e información cuántica, esencialmente en la teleportación, codificado denso y el protocolo de Ekert de criptografía cuántica *(Ver Capítulo 3)*.

1.8. Cuantificación del entrelazamiento

Definir si un estado se encuentra entrelazado o no es relativamente sencillo pero medir o cuantificar la cantidad de entrelazamiento del estado no lo es. Algunas condiciones necesarias [7] que cualquier tipo de medición de entrelazamiento E sobre un estado σ debe de satisfacer las siguientes postulados:

- No-negatividad: $E(\sigma) \geq 0$
- $E(\sigma) = 0$ sí y solo sí σ es separable.
- Operaciones Locales Unitarias no modifican el valor *E(σ)*.
- E no aumenta su promedio sobre operaciones locales clásicas: $E(\sigma) \geq \sum_i p_i E(\rho_i)$, donde el estado ρ_i bajo operaciones locales es obtenido con probabilidad p_i.
- E es continua
- E es aditiva (sobre estados puros) : $E(\mid \varphi^{AB}\rangle \otimes \mid \phi^{AB}\rangle) = E(\mid \varphi^{AB}\rangle) + E(\mid \phi^{AB}\rangle)$.

Entropia de Von Neumann: Esta medición del entrelazamiento es más sencilla de calcular. Dado un estado puro ρ_{AB}, un estado puro es un estado donde su vector estado $\mid \psi\rangle$ es exactamente conocido, de dos subsistemas A y B, se define el estado $\rho_A = tr_B \{\rho_{AB}\}$, tr_B es la traza parcial sobre el qubit B y $\rho_B = tr_A \{\rho_{AB}\}$, es la traza parcial sobre el qubit A. Entonces la entropía de Von Neumann está dada por [7]

$$S(\rho_A) = -tr\left(\rho_A \ln \rho_A\right) = -tr\left(\rho_B \ln \rho_B\right). \tag{1.8.1}$$

En este caso la cantidad de entrelazamiento es cero si el estado es separable y para un sistema compuesto de dos qubits es $ln2$ si el estado se encuentra máximamente entrelazado. Se verá más a fondo esta entropía en el Capitulo 4: Teoría Cuántica de la Información.

Se puede también caracterizar la cantidad de entrelazamiento de un estado calculando la concurrencia C, es decir, la cantidad de traslape entre un estado $\mid \psi\rangle$ y otro estado $\mid \widetilde{\psi}\rangle$

$$C \mid \psi\rangle = \left|\langle \psi \mid \widetilde{\psi}\rangle\right|,$$

donde $\mid \widetilde{\psi}\rangle = Y \otimes Y \mid \psi^*\rangle$ y $\mid \psi^*\rangle$ es el complejo conjugado del estado y Y un operador de Pauli. La concurrencia también puede ser calculada usando el operador densidad (Ver Capitulo 4), observando los valores propios de la matriz densidad resultante de $\rho\left(Y \otimes Y\right)\rho^{\dagger}\left(Y \otimes Y\right)$.

La idea inicial de realizar una cuantificación del entrelazamiento fue dada por Bennett en 1996, definida por el costo de entrelazamiento.

Costo de Entrelazamiento: Es una medición de entrelazamiento entre dos sistemas (Alice y Bob). Se define el costo de la creación de entrelazamiento de un estado ρ por:

$$E_C(\rho) = min \sum_i p_i S(\rho_A^i), \tag{1.8.2}$$

donde $S(\rho_A)$ es la entropía de Von Neumann (ver ecuación 1.8.1) y el mínimo es tomado sobre todas las posibles realizaciones del estado, p_i denota la probabilidad de que el estado se encuentre en $\mid \psi_i\rangle$ y $\rho_A^i = tr_B\left(\mid \psi_i\rangle\langle\psi_i \mid\right)$.

1.9. Dinámica de partículas con Espín

Como partículas de espín $1/2$ son el paradigma de un sistema de dos niveles a continuación discutimos la dinámica clásica y cuántica de partículas con espín. Como veremos más adelante los sistemas de dos niveles tienen un papel relevante en el establecimiento de los qubits.

La dinámica de espín puede ser descrita usando una teoría cuasi-clásica. El espín de una partícula es análogo a su momento angular intrínseco. Este momento angular intrínseco es un vector, no escalar, y por lo tanto el espín también es un vector este espín intrínseco siempre se encontrará presente. Una propiedad importante para determinar la dinámica del espín en un campo magnético es su momento magnético. La propiedad principal de un electrón o espín nuclear es que su momento magnético $\vec{\mu}$ es paralelo al momento angular de espín $\overrightarrow{S}$, y entonces puede escribirse

$$\vec{\mu} = \pm\gamma\overrightarrow{S}. \tag{1.9.1}$$

donde γ es la magnitud de la razón giromagnética. El signo positivo corresponde al espín del protón y muchos otros espines nucleares. El signo negativo corresponde al espín del electrón y algunos espines nucleares. Esto significa que la dirección del momento magnético es opuesta a la dirección del espín. Debido a que el momento magnético es proporcional al momento angular de espín, si una partícula no tiene espín entonces dicha partícula tampoco tendrá momento magnético.

Es bien conocido que un campo magnético uniforme $\overrightarrow{B}$ no produce una fuerza neta sobre un momento magnético. La fuerza actuando sobre el polo Norte positiva es balanceada por la fuerza actuando sobre el polo sur. La torca $\vec{\tau}$ producida por el campo magnético es igual a la razón de cambio de la dirección del espín

$$\vec{\tau} = \frac{d\overrightarrow{S}}{dt} = \vec{\mu} \times \vec{B}. \tag{1.9.2}$$

Multiplicando por $-\gamma$ se deriva la ecuación de movimiento cuasi-clásica para el momento

magnético, que en componentes cartesianas es

$$\begin{aligned} \dot{\mu}_x &= -\gamma(\mu_y B_z - \mu_z B_y), \\ \dot{\mu}_y &= -\gamma(\mu_z B_x - \mu_x B_z), \\ \dot{\mu}_z &= -\gamma(\mu_x B_y - \mu_y B_x). \end{aligned} \tag{1.9.3}$$

Si $\overrightarrow{B} = B_0\hat{z}$, entonces se tiene

$$\begin{aligned} \dot{\mu}_x &= -\gamma B_0 \mu_y, \\ \dot{\mu}_y &= \gamma B_0 \mu_x, \\ \dot{\mu}_z &= 0, \end{aligned} \tag{1.9.4}$$

con $\overrightarrow{\mu}(t) = \mu_x(t)\hat{x} + \mu_y(t)\hat{y} + \mu_z(t)\hat{z}$. Si volvemos a derivar las ecuaciones en (1.9.4) y escribimos $\omega = -\gamma B$ (ω es conocida como frecuencia de Larmor), obtenemos

$$\begin{aligned} \ddot{\mu}_x &= -\omega^2 \mu_x, \\ \ddot{\mu}_y &= -\omega^2 \mu_y. \end{aligned} \tag{1.9.5}$$

Las soluciones para $\mu_x(t)$ y $\mu_y(t)$ son

$$\begin{aligned} \mu_x(t) &= \mu_x(0)\cos\,\omega t + \mu_y(0)\sin\,\omega t, \\ \mu_y(t) &= \mu_y(0)\cos\,\omega t - \mu_x(0)\sin\,\omega t, \\ \mu_z(t) &= 0. \end{aligned} \tag{1.9.6}$$

Otra solución sería la siguiente: se tienen dos direcciones de equilibrio para el vector momento magnético $\bar{\mu}$: las direcciones positivas y negativas del eje z. Sea $\mu_z = \mu_0$, y corresponde a una energía magnética mínima:

$$U_m = -B_0\mu_0. \tag{1.9.7}$$

Consideremos el caso $\mu_1 = \sqrt{\mu_x^2 + \mu_y^2} \neq 0$, entonces conviene definir

$$\mu_\pm = \mu_x \pm i\mu_y \tag{1.9.8}$$

y entonces las ecuaciones (1.9.4) pueden escribirse $\dot{\mu}_\pm = \pm i\gamma B_0 \dot{\mu}_\pm$ cuyas soluciones son inmediatamente dadas por

$$\mu_\pm(t) = \mu_\pm(0)\, e^{\pm i\omega_b t}, \tag{1.9.9}$$

que describe un movimiento de precesión en contra del movimiento de las manecillas del reloj del momento magnético alrededor de la dirección del campo magnético; a ésta se le llama precesión de Larmor y a $w_b = \gamma B_0$ frecuencia de Larmor. Se concluye entonces que las integrales de movimiento son $\mu_z = \mu_0$ y $\mu = \sqrt{\mu_x^2 + \mu_y^2 + \mu_z^2}$.

Sea el movimiento del momento magnético en la presencia de un campo magnético de radio frecuencia $\overrightarrow{B_1}$. Sea $\overrightarrow{B_1}$ un campo polarizado en el plano XY rotando en contra de las manecillas del reloj, es decir,

$$B_{1x} = B_1 cos\,\omega t \qquad , B_{1y} = B_1 sen\, wt. \tag{1.9.10}$$

Substituyendo en la ecuación (1.9.3), $\overrightarrow{B} = B_0\hat{k} + \overrightarrow{B_1}$, se obtienen las ecuaciones diferenciales

$$\begin{aligned} \dot{\mu}_+ &= i\gamma\left(B_o\mu_+ - B_1\mu_z e^{i\omega t}\right), \\ \dot{\mu}_z &= i\gamma/2\left(B_1\mu_- e^{i\omega t} - B_1\mu_+ e^{i\omega t}\right). \end{aligned} \tag{1.9.11}$$

Para simplificar las ecuaciones se escriben en un sistema de coordenadas rotante por un ángulo $\phi = \omega t$ alrededor del eje z y entonces las ecuaciones anteriores para el vector de momento magnético toman la forma

$$\begin{aligned}
\dot{\mu}_{+}^{'} &= i\gamma\left(B_0 - \frac{w}{\gamma}\right)\mu_{+}^{'} - i\gamma B_1 \mu_z^{'}, \\
\dot{\mu}_{-}^{'} &= -i\gamma\left(B_0 - \frac{w}{\gamma}\right)\mu_{-}^{'} + i\gamma B_1 \mu_z^{'}, \\
\dot{\mu}_z^{'} &= \frac{i\gamma}{2} B_1\left(\mu_{-}^{'} - \mu_{+}^{'}\right).
\end{aligned} \tag{1.9.12}$$

$$\frac{d}{dt}\begin{pmatrix} \mu_{+}^{'} \\ \mu_z^{'} \\ \mu_{-} \end{pmatrix} = i\gamma \begin{pmatrix} B_0 - \frac{w}{\gamma} & -B_1 & 0 \\ -\frac{B_1}{2} & 0 & \frac{B_1}{2} \\ 0 & B_1 & -(B_0 - \frac{w}{\gamma}) \end{pmatrix} \begin{pmatrix} \mu_{+}^{'} \\ \mu_z^{'} \\ \mu_{-} \end{pmatrix}$$

que describen el movimiento de un momento magnético en un campo magnético efectivo de la forma

$$\vec{B}_{\text{eff}} = \left(B_1, 0, B_0 - \frac{\omega}{\gamma}\right). \tag{1.9.13}$$

De tal manera que la ecuación (1.9.12) describe el movimiento del vector magnético $\overline{\mu^{'}}$ precesando alrededor del campo magnético efectivo. En el sistema de referencia del laboratorio se tiene un movimiento complicado del vector magnético $\overrightarrow{\mu}$: la precesión de Larmor alrededor del campo efectivo $\vec{B}_{\text{eff}}$, que al mismo tiempo rota alrededor del eje z con frecuencia w.

1.9.1. Tratamiento mecánico cuántico

El vector de estado un sistema está dado por

$$\mid \psi(t) >= \alpha(t) \mid 0\rangle + \beta(t) \mid 1\rangle = \begin{pmatrix} \alpha\,(t) \\ \beta\,(t) \end{pmatrix}, \tag{1.9.14}$$

donde $\mid 0\rangle$ y $\mid 1\rangle$ son vectores propios del operador proyección S_z con valores propios $+\hbar/2$ y $-\hbar/2$ respectivamente.
El operador Hamiltoniano $H(t)$ para un electrón en un campo magnético es $H(t) = -\frac{\hbar\gamma}{2}\bar{\sigma}\cdot\beta$, y utilizando la representación matricial de las matrices de Pauli toma la forma

$$\begin{aligned}
H(t) &= \hbar\tfrac{\omega_0}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
&\quad + \hbar\tfrac{\omega_1}{2}\left[\begin{pmatrix} 0 & \cos\,\omega t \\ \cos\,\omega t & 0 \end{pmatrix} + \begin{pmatrix} 0 & -i\,\sin\,wt \\ i\,\sin\,wt & 0 \end{pmatrix}\right] \\
&= \tfrac{\hbar}{2}\begin{pmatrix} \omega_0 & \omega_1 e^{-i\omega t} \\ \omega_1 e^{i\omega t} & -\omega_0 \end{pmatrix}
\end{aligned} \tag{1.9.15}$$

donde se usó $\bar{B} = B_0\hat{k} + \bar{B}_1$, $w_0 \equiv \gamma B_0$, y $w_1 = \gamma B_1$.
Se puede resolver ahora la ecuación de Schrödinger

$$i\hbar\frac{d}{dt} \mid \tilde{\psi}(t)\rangle = \tilde{H} \mid \tilde{\psi}(t)\rangle, \tag{1.9.16}$$

donde $\mid \psi(t)\rangle$ está definido en (1.9.14) y H en (1.9.15) describe la interacción del espín con un campo magnético variable:

$$i\hbar\frac{\partial}{\partial t}\begin{pmatrix}\alpha\left(t\right)\\ \beta\left(t\right)\end{pmatrix}=\frac{\hbar}{2}\begin{pmatrix}\omega_0 & \omega_1 e^{-i\omega t}\\ \omega_1 e^{i\omega t} & -\omega_0\end{pmatrix}\begin{pmatrix}\alpha\left(t\right)\\ \beta\left(t\right)\end{pmatrix}. \tag{1.9.17}$$

Se tiene entonces el par de ecuaciones diferenciales

$$\begin{aligned} i\frac{\partial\alpha\left(t\right)}{\partial t}&=\frac{w_0}{2}\alpha\left(t\right)+\frac{\omega_1}{2}e^{-i\omega t}\beta\left(t\right),\\ i\frac{\partial\beta\left(t\right)}{\partial t}&=\frac{\omega_1}{2}e^{i\omega t}\alpha\left(t\right)-\frac{w_0}{2}\beta\left(t\right). \end{aligned} \tag{1.9.18}$$

Se propone $\alpha(t)=e^{-i\frac{w_0}{2}t}g_+$ y $\beta(t)=e^{i\frac{w_0}{2}t}g_-$, obteniéndose las ecuaciones diferenciales

$$\begin{aligned} \dot{g}_+&=-i\frac{w_1}{2}e^{-i(w-w_0)t}g_-,\\ \dot{g}_-&=-i\frac{w_1}{2}e^{-i(w-w_0)t}g_+. \end{aligned} \tag{1.9.19}$$

Estas ecuaciones diferenciales, con la condición lineal $g_+(0)=1$ y $g_-(0)=0$, pueden resolverse en forma inmediata:

$$\begin{pmatrix}\alpha(t)\\ \beta(t)\end{pmatrix}=\begin{pmatrix}e^{-i\frac{\omega_0}{2}t}cos(\frac{w_1 t}{2})\\ e^{i\frac{\omega_0}{2}t}sin(\frac{w_1 t}{2})\end{pmatrix}, \tag{1.9.20}$$

donde se tomó $w=w_0$. Este vector de estado describe la dinámica del espín del electrón en un tiempo arbitrario t.

Todos los resultados mencionados en el presente capítulo son aprovechados completamente por la teoría de la información cuántica. En los siguientes capítulos se verá como estos recursos pueden ser utilizados para poder realizar procesos computacionales y protocolos de comunicación.

Capítulo 2

Computación cuántica

Un bit cuántico es la unidad mínima y elemental de la información cuántica, es el elemento básico de una computadora cuántica. Definimos un bit clásico como un sistema físico de dos estados distinguibles y extendemos esta definición del bit clásico para introducir el concepto de bit cuántico.
Para poder realizar cualquier cómputo cuántico se necesita definir un estado inicial, implementar una serie de transfomaciones unitarias sobre el estado inicial y medir el estado de salida. Definimos la medición del estado de un qubit con la ayuda de una esfera de radio unidad en $\mathbb{R}^3$ definida como Esfera de Bloch, donde cada punto de la esfera representa el estado de un qubit de nuestro sistema.
Se representa y se define una computadora cuántica a través del modelo de un circuito cuántico, que nos facilita el manejo del cómputo y nos ayuda a observar y a distinguir las propiedades que el cómputo cuántico hace uso de la mecánica cuántica. Con la ayuda de estos circuitos se introducen y se definen las compuertas cuánticas básicas de la computación cuántica. Se demuestra la universalidad de ciertas compuertas y se define su importancia para la computación cuántica.
Después de esto nos enfocamos a definir y desarrollar algunos de los más importantes algoritmos del cómputo cuántico. Finalmente realizamos un breve análisis de la Máquina Universal de Turing Cuántica (MUTC).

2.1. El Qubit

Un bit clásico es un sistema de dos estados distinguibles usualmente representados por 0 y 1. Podemos representar los dos estados de un bit clásico (Cbit) por un par de vectores ortonormales de 2 dimensiones de la siguiente manera[10]:

$$|\,0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{Representación del Cbit 0 como vector columna,}$$

$$|\,1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{Representación del Cbit 1 como vector columna.}$$

Para representar los 4 estados que podemos representar con 2 Cbits los representaremos como el producto tensorial de dos pares de vectores ortogonales en 4 dimensiones.

$$| 0\rangle \otimes | 0\rangle = | 00\rangle = | 0\rangle_2,$$

$$| 0\rangle \otimes | 1\rangle = | 01\rangle = | 1\rangle_2,$$

$$| 1\rangle \otimes | 0\rangle = | 10\rangle = | 2\rangle_2.$$
$$| 1\rangle \otimes | 1\rangle = | 11\rangle = | 3\rangle_2.$$

El subíndice "2" en la última representación nos ayuda a identificar cuantos Cbits describe el vector.
Entonces podríamos describir los estados de n Cbits como los 2^n vectores ortonormales en 2^n dimensiones como:

$$| x\rangle_n, \quad 0 \leq x < 2^n - 1 \tag{2.1.1}$$

dado por los n productos tensoriales de n espacios vectoriales de dos dimensiones.

La regla general de la representación de $| x\rangle_n$ es 1 en la posición X y 0 en el resto de las posiciones, así de la siguiente manera podríamos expresar el vector columna $| 4\rangle_3$:

$$| 4\rangle = | 100\rangle = | 1\rangle \otimes | 0\rangle \otimes | 0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Si al sistema de numeración de nuestra base clásica le introducimos el valor $\sqrt{-1}$, podremos entonces lograr grandes simplificaciones entre ciertas relaciones referidas a los números reales. Entonces extendemos el conjunto de los estados de la base clásica hasta los vectores unitarios arbitrarios de todo el espacio consistente de las combinaciones lineales (superposiciones) de los estados básicos clásicos con coeficientes complejos (amplitudes). Llameremos a esta extensión bit cuántico o Qubit, entonces el estado general de un Qubit es una superposición de los dos estados de la base clásica:

$$| \varphi\rangle = \alpha | 0\rangle + \beta | 1\rangle \quad , \quad \alpha, \beta \ \varepsilon \ \mathbb{C}$$

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

Ahora el estado general de n-Qubits tiene la siguiente forma:

$$| \varphi\rangle = \sum_{0 \leq x < 2^n - 1} \alpha_x | x\rangle_n \tag{2.1.2}$$

con las amplitudes complejas restringidas sólo por la condición de normalización.
Por otro lado como un factor de fase global no afecta al estado físico, podemos escoger a α como real y positivo. Con excepción del estado base $\mid 1\rangle$ en que $\alpha = 0$ y $\beta = 1$. Entonces el estado genérico del qubit lo podríamos escribir como:

$$\mid \varphi\rangle = \cos\frac{\theta}{2} \mid 0\rangle + e^{i\phi}\sin\frac{\theta}{2} \mid 1\rangle. \tag{2.1.3}$$

De tal manera que el Qubit reside en un espacio vectorial parametrizado por las variables continuas α y β (θ y ϕ).
Pareciera que esta extensión nos puede llevar a almacenar una cantidad infinita de información en un solo Qubit, contrario a lo que teníamos en el caso del Cbit. Sin embargo esto no es cierto ya que la mecánica cuántica nos dice que para extraer dicha información tenemos que realizar un proceso de medición y esta medición únicamente nos podrá regresar un solo bit de información.
Por lo tanto con el resutado de las mediciones sabremos que el respectivo estado cuántico se encuentra en un estado $\mid 0\rangle$ o $\mid 1\rangle$ con probabilidades

$$p_0 = \mid \alpha \mid^2 = \cos\frac{\theta}{2}, \;\; p_1 = \mid \beta \mid^2 = \sin^2\frac{\theta}{2},$$

respectivamente, de acuerdo a los postulados de la mecánica cuántica.

2.2. Representación y Medición del estado de un qubit

Se puede realizar la representación geométrica de un Qubit y de las transformaciones que pueden operar sobre él a tráves de la *Esfera de Bloch*.
Dicha esfera es representada por una esfera de radio unidad en R^3 con coordenadas Cartesianas ($x = \cos\phi \sin\theta$, $y = \sin\phi \sin\theta$, $z = \cos\theta$) donde cada punto de la esfera representa un estado puro del espacio de Hilbert de dimensión compleja 2, que en nuestro caso caracteriza a nuestro sistema de bits cuánticos.
Un vector de Bloch corresponde a un vector cuyos componentes (x,y,z) corresponden a un solo punto pertenenciente a las esfera de Bloch, satisfaciendo la condicion de normalización $x^2 + y^2 + z^2 = 1$.

2.3. Definición de la Esfera de Bloch

La Esfera de Bloch es una representación geométrica del espacio de estados puros de un sistema cuántico de dos niveles, a traves de puntos pertencientes a una esfera unitaria.
Sabemos que un qubit puede ser escrito de la siguiente manera generalizada:

$$\mid \varphi\rangle = e^{i\gamma}(\cos\frac{\theta}{2} \mid 0\rangle + e^{i\phi}\sin\frac{\theta}{2} \mid 1\rangle), \tag{2.3.1}$$

donde θ, ϕ y γ son numeros reales. θ y ϕ definen un punto en la *Esfera de Bloch.* $e^{i\gamma}$ es un factor que no tiene ningun efecto observable, es decir, que para cualquier valor de γ el estado del Qubit está representado por el mismo punto en la *Esfera de Bloch.*
Entonces podemos escribir el estado del Qubit como

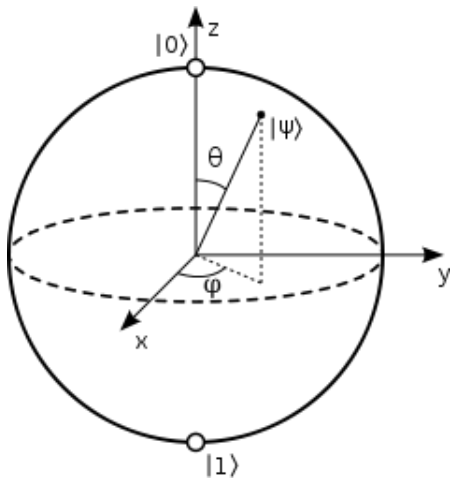


Figure 2.2.1: Esfera de Bloch

$$| \varphi\rangle = \cos\frac{\theta}{2} \mid 0\rangle + e^{i\phi} \sin\frac{\theta}{2} \mid 1\rangle. \tag{2.3.2}$$

2.3.1. Deducción de la Esfera de Bloch

La *Esfera de Bloch* es una generalización de un número complejo z con $\mid z \mid^2 = 1$ como un punto en un círculo unitario.
Sea $z = x + iy \mid x\ ,\ y$ pertenecen a los reales,

$$\mid z \mid^2 = z * z\ = (x\ - iy)\ (x\ + iy)\ = x^2\ + y^2 \tag{2.3.3}$$

con $x^2 + y^2 = 1$, la ecuación de un círculo de radio uno, con centro en el origen.
En coordenadas polares para un $z = x + iy$ arbitrario, podemos escribir $x = r \cos\theta$, $y = r \sin\theta$, entonces

$$z = r\,(cos\,\theta\ +\ i\,sin\,\theta). \tag{2.3.4}$$

Por la Fórmula de Euler $e^{i\theta} = \cos\theta + i\ sin\ \theta$

$$z = r\,e^{i\theta} \tag{2.3.5}$$

y si es un círculo unitario $r = 1$, entonces z = $e^{i\theta}$.
Así dado el estado de un Qubit general

$$| \varphi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle,$$

podemos expresar dicho estado en coordenadas polares de la siguiente manera:

$$| \varphi\rangle = r_\alpha e^{i\phi_\alpha} \mid 0\rangle + r_\beta e^{i\theta_\beta} \mid 1\rangle. \tag{2.3.6}$$

Podemos multiplicar el estado por un factor de fase global $e^{i\gamma}$ sin modificar el resultado de medir el observable, esto es,

$$\mid e^{i\gamma}\alpha \mid^2 = (e^{i\gamma}\alpha) * (e^{i\gamma}\alpha) = (e^{-i\gamma}\alpha*)(e^{i\gamma}\alpha) = \alpha * \alpha = |\alpha|^2 .$$

Multiplicando por $e^{-i\phi_\alpha}$ tenemos

$$\mid \varphi'\rangle = r_\alpha \mid 0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)} \mid 1\rangle = r_\alpha \mid 0\rangle + r_\beta e^{i\phi} \mid 1\rangle, \tag{2.3.7}$$

donde $\phi = \phi_\beta - \phi_\alpha$, además $\langle\varphi' \mid \varphi'\rangle = 1$.
Regresando a las coordenadas cartesianas para nuestro coeficiente $\mid 1\rangle$

$$\mid \varphi'\rangle = r_\alpha \mid 0\rangle + (x + iy) \mid 1\rangle \tag{2.3.8}$$

y la constante de nomalización se obtiene de

$$\mid r_\alpha \mid^2 + \mid x + iy \mid^2 = r_\alpha^2 + (x + iy) * (x - iy) = r_\alpha^2 + x^2 + y^2 = 1, \tag{2.3.9}$$

que es la ecuación de la esfera unitaria en el espacio de coordenadas cartesianas.
Las coordenadas cartesianas y las coordenadas polares están relacionadas por

$$\begin{aligned} x &= r\,\sin\theta\,\cos\phi, \\ y &= r\,\sin\theta\,\sin\phi, \\ z &= r\cos\theta, \end{aligned}$$

En la ecuación anterior renombramos r_α como z y como r = 1 tenemos

$$\begin{aligned} \mid \varphi'\rangle &= z \mid 0\rangle + (sin\theta\cos\phi + i(\sin\theta\sin\phi) \mid 1\rangle, \\ &= \cos\theta \mid 0\rangle + \sin\theta\,(\cos\phi + i\sin\phi) \mid 1\rangle, \\ &= \cos\theta \mid 0\rangle + e^{i\phi}\sin\theta \mid 1\rangle. \end{aligned}$$

Renombramos $\mid \varphi'\rangle = \mid \varphi\rangle$ y $\theta = \theta'$

$$\mid \varphi\rangle = \cos\theta' \mid 0\rangle + e^{i\phi}\sin\theta' \mid 1\rangle. \tag{2.3.10}$$

Notemos que si $\theta' = 0 \Rightarrow \mid \varphi\rangle = \mid 0\rangle$ y si $\theta' = \frac{\pi}{2} \Rightarrow \mid \varphi\rangle = e^{i\phi} \mid 1\rangle$. Entonces si $0 \leq \theta' \leq \frac{\pi}{2}$ podremos generar todos los puntos de la Esfera de Bloch.
No hay necesidad de considerar ambos hemisferios de la esfera ya que dichos puntos sólo difieren por un factor de fase global -1.

Entonces definimos $\theta = 2\theta'$

$$\mid \varphi\rangle = \cos\frac{\theta}{2} \mid 0\rangle + e^{i\phi}\sin\frac{\theta}{2} \mid 1\rangle. \tag{2.3.11}$$

2.4. Medición

Como tenemos un gran número de qubits preparados identicamente en principio podemos medir el estado de un qubit $\mid \varphi\rangle$.
Nos ayudaremos de la esfera de Bloch para realizar la medición de nuestro estado, basándonos en que podemos medir las coordenadas x,y,z de un qubit en nuestra esfera de la

siguiente manera:
Usaremos las matrices de Pauli $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ y los multiplicaremos por nuestro estado $\mid \varphi\rangle$, entonces

$\sigma_x \mid \varphi\rangle = \mathrm{e}^{i\phi} \sin\frac{\theta}{2} \mid 0\rangle + \cos\frac{\theta}{2} \mid 1\rangle,$

$\sigma_y \mid \varphi\rangle = -ie^{\phi}\sin\frac{\theta}{2} \mid 0\rangle + i \cos\frac{\theta}{2} \mid 1\rangle,$

$\sigma_z \mid \varphi\rangle = \cos\frac{\theta}{2} \mid 0\rangle$ - $\mathrm{e}^{i\phi} \cos\frac{\theta}{2} \mid 1\rangle.$

Si calculamos el valor esperado tendremos

$\langle\varphi \mid \sigma_x \mid \varphi\rangle = \sin\theta \cos\phi = \mathrm{x},$

$\langle\varphi \mid \sigma_y \mid \varphi\rangle = \sin\theta \, sin\phi = \mathrm{y},$

$\langle\varphi \mid \sigma_z \mid \varphi\rangle = \cos\theta = \mathrm{z}.$

Observamos entonces que las coordenadas (x,y,z) pueden ser obtenidas con cierta precisión arbitraria.
Por otro lado tenemos:

$$p_0 - p_1 = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta = z.$$

Entonces obtenemos z por medio de la diferencia de probabilidades de encontrar 0 o 1 de una medición de σ_z, y si tenemos una gran cantidad N de sistemas idénticos preparados en el estado $\mid \varphi\rangle$ podremos estimar z con mayor precisión de acuerdo a nuestro valor de N.
Estimamos z como N_0 / N - N_1 / N donde N_0 y N_1 nos indican el número de veces que obtuvimos 0 y 1 en nuestra medición.
Análogamente podemos obtener las coordenadas x, y operando mediante transformaciones de rotación apropiadas sobre el qubit.

2.5. Circuito cuántico

Definimos una computadora clásica como una cinta finita dividida en n estados o celdas, cada cinta tiene un estado inicial y un estado final distinguible. En cada celda de la cinta puede ser escrito un símbolo a partir de un alfabeto Σ. Una cabeza de escritura-lectura está posicionada en cada paso sobre la celda de nuestra cinta dirigida por una unidad de control. La computadora se detiene cuando la unidad de control alcanza un estado final.

El conjunto de operaciones elementales actúan sobre estados de 1 o 2 bits y pueden ser combinadas de tal manera que se pueden realizar operaciones o funciones más complejas.

Este mismo modelo puede ser representado en computación cuántica. Ahora en vez de cbits tenemos qubits y en vez de una cinta o regsitro clásico tendremos un registro cuántico de n estados.

El estado de una computadora cuántica de n-qubits es

$$\begin{aligned} \mid \varphi\rangle &= \sum_{i=0}^{2^n-1} c_i \mid i\rangle \\ &= \sum_{i_{n-1}=0}^{1} \ldots \sum_{i_1=0}^{1} \sum_{i_0=0}^{1} c_{i_{n-1}\ldots i_1,i_0} \mid i_{n-1}\rangle \otimes \ldots \otimes \mid i_1\rangle \otimes \mid i_o\rangle, \end{aligned} \tag{2.5.1}$$

donde $\sum \mid c_i \mid^2 = 1$ y el ket $\mid i\rangle$ está definido por el entero $i = i_{n-1}2^{n-1} + \cdots + i_1 2 + i_0$, con i_k denotando dígitos binarios. Entonces el estado de una computadora cuántica de n-qubits está construida como el producto tensorial de n-espacios de Hilbert de 2 dimensiones.
Se puede observar el principio de superposición en la ecuación anterior denotando que podemos registrar el estado $\mid i\rangle$ de nuestra base computacional en una superposición de n-qubits, mientras que en el caso clásico en el que tenemos n cbits podemos registrar o almacenar un solo entero i. Por lo tanto, la cantidad de operaciones que podemos realizar con una computadora cuántica crece exponencialmente gracias a este principio de superposición, lo que aparentemente nos trae un nuevo poder de cómputo.

Para poder realizar algún cómputo cuántico necesitamos:

1. Definir un estado inicial $\mid \varphi_i\rangle$ (estado fiducial[1]) y preparar dicho estado en nuestra computadora cuántica.
2. Manipular u operar la función de onda con nuestra computadora cuántica a través de transformaciones unitarias U, tal que $\mid \varphi_f\rangle = \mathrm{U} \mid \varphi_i\rangle$
3. Al finalizar nuestro algoritmo, realizar una medición estándar en nuestra base computacional, por ejemplo, medir la polarización a lo largo del eje z mediante el operador de Pauli σ_z de cada uno de los qubit.

2.6. Compuertas cuánticas de un solo qubit

Una compuerta cuántica es un circuito cuántico básico operando en un cierto número de qubits, i.e., nos ayudan a procesar uno o más qubits de acuerdo a los axiomas de la mecánica cuántica. Las compuertas cuánticas son reversibles, contrarias a la mayoría de las compuertas clásicas (compuertas lógicas) (Figura 2.6.1). Dichas compuertas cuánticas las representamos por medio de matrices unitarias, las que preservan la condición de normalización. Las compuertas cuánticas tendrán entonces el mismo número de qubits de entrada que de salida.

Las compuertas cuánticas de un solo qubit están representadas por matrices unitarias de 2×2.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

De manera general podemos expresar una compuerta cuántica A de un solo qubit como

[1]El termino "fiducial" es usado como término de referencia al origen o al cero

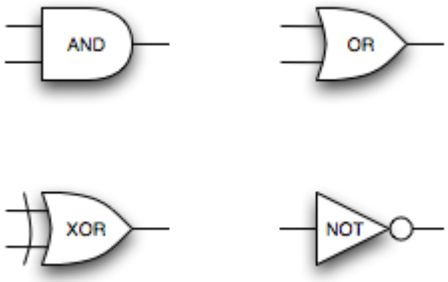


Figure 2.6.1: Representación clásica de compuertas booleanas

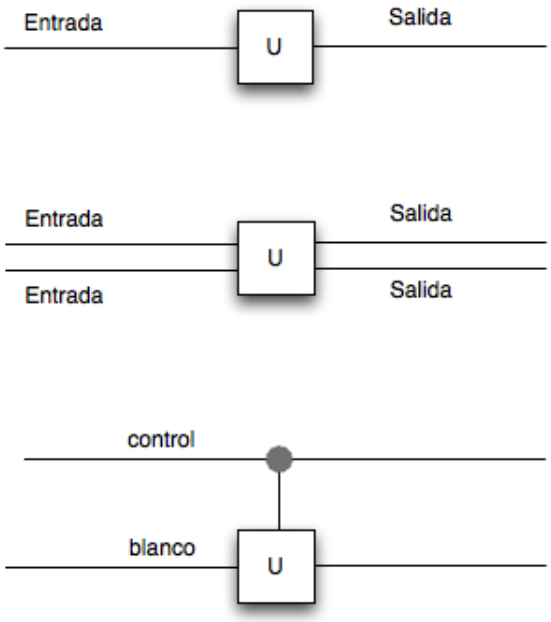


Figure 2.6.2: Representación de Compuertas Cuánticas

$$| \varphi\rangle \underrightarrow{A} | \mathcal{X}\rangle. \tag{2.6.1}$$

Donde A es un operador lineal unitario invertible.
Entonces $A \ | \varphi\rangle \ = | \mathcal{X}\rangle$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}.$$

Existen 3 maneras generales para representar esquemáticamente una compuerta cuántica en notación de circuitos (Figura 2.6.2), un operador arbitrario de un qubit U_1, un operador arbitrario de dos qubits U_2 y un operador de dos qubits-controlado donde U es aplicado al qubit *blanco* si el qubit control es inicializado.

2.6.1. Compuerta Hadamard

La compuerta de Hadamard nos convierte nuestra base computacional $\{|\,0\rangle, |\,1\rangle\}$ en la nueva base $\{|\,+\rangle, |\,-\rangle\}$ que forma una superposición de nuestra base computacional.
La compuerta de Hadamard es una matriz de 2×2 definida como

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

La acción de H está dada entonces por

$$\begin{aligned} H \;|\,0\rangle \;&=\; \frac{1}{\sqrt{2}}\,(\,|\,0\rangle + \;|\,1\rangle) \;\equiv |\,+\rangle, \\ H \;|\,1\rangle \;&=\; \frac{1}{\sqrt{2}}\,(\,|\,0\rangle - \;|\,1\rangle) \;\equiv |\,-\rangle. \end{aligned} \tag{2.6.2}$$

Cabe destacar que $H^2 = I$ y $H^{-1} = H$. Como H es hermiteana $\Rightarrow \left(H^T\right)^* = H$.

2.6.2. Compuerta de corrimiento de fase

Esta compuerta convierte $|\,0\rangle$ en $|\,0\rangle$ y $|\,1\rangle$ en $e^{i\delta}\;|\,1\rangle$. Como una fase global no tiene significado físico, los estados de la base computacional $|\,0\rangle\,,\;|\,1\rangle$ no cambian.
Dicha compuerta está definida como

$$R_z(\delta) \;=\; \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}.$$

La acción de dicha compuerta sobre un qubit generico $|\;\varphi\rangle$ se comporta de la siguiente manera:

$$R_z(\delta)\;\;|\,\varphi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\,\sin\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i(\phi+\delta)}\;\sin\frac{\theta}{2} \end{bmatrix}.$$

Como fases relativas son observables, el estado del qubit ha cambiado debido a la aplicación de la compuerta de corrimiento de fase. Dicha compuerta genera una rotación en dirección contraria a las manecillas del reloj a través de un ángulo δ sobre el eje z de la *Esfera de Bloch.*

Cualquier operación unitaria sobre un solo qubit puede ser construida únicamente a partir de nuestras compuertas de Hadamard y de la compuerta de corrimiento de fase. Toda transformación unitaria mueve el estado de un qubit de un punto sobre de la Esfera de Bloch a otro punto de la misma.

2.6.3. Rotación de la Esfera de Bloch

Otra clase de transformaciones unitarias útiles son las rotaciones de la Esfera de Bloch sobre un eje arbitrario.
Las matrices de Pauli *X, Y, Z* cuando son exponenciadas dan como resultado operadores de rotación, que rotan el vector de Bloch ($\sin\theta\,\cos\phi$, $\sin\theta\,\sin\phi$, $\cos\theta$), sobre el eje $\hat{x}$, $\hat{y}$ o $\hat{z}$:

$$R_x(\theta) \;\equiv\; e^{-i\theta\frac{X}{2}},$$

$$R_y(\theta) \equiv e^{-i\theta\frac{Y}{2}},$$

$$R_z(\theta) \equiv e^{-i\theta\frac{Z}{2}},$$

Para una función exponencial tenemos

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + ... \tag{2.6.3}$$

Ahora consideremos $e^{i\theta A}$

$$e^{i\theta A} = I + i\theta A - \frac{(\theta A)^2}{2!} - i\frac{(\theta A)^3}{3!} + ... \tag{2.6.4}$$

En el caso en que $A^2 = I$,

$$e^{i\theta A} = I + i\theta A - \frac{\theta^2 I}{2!} - i\frac{\theta^3 A}{3!} + ...$$

$$= (1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} + ...)\, I + i\,(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} + ...)\, A$$

$$\therefore\ e^{i\theta A} = \cos(\theta)\, I \ +\ i\ \sin(\theta)\, A \tag{2.6.5}$$

Las matrices de Pauli tienen la propiedad que $X^2 = Y^2 = Z^2 = I$ entonces podemos evaluar los operadores de rotación con el resultado anterior:

$$R_x(\theta) \equiv e^{-i\theta\frac{X}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},$$

$$R_y(\theta) \equiv e^{-i\theta\frac{Y}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{2.6.6}$$

$$R_z(\theta) \equiv e^{-i\theta\frac{Z}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}.$$

Si $\hat{n}$= (n_x, n_y, n_z) es un vector real unitario, entonces el operador $R_{\hat{n}}(\theta) \equiv e^{-i\theta\hat{n}\cdot\vec{\sigma}/2}$ rota el vector de Bloch por un ángulo θ sobre el eje $\hat{n}$ y $\vec{\sigma}$ denota el vector cuyas componente son las matrices de Pauli $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Además $(\hat{n}\cdot\vec{\sigma})^2 =$ I entonces podremos escribir

$$\begin{aligned} R_{\hat{n}}(\theta) &= \cos(\frac{\theta}{2})\, I - i\sin(\frac{\theta}{2})\, \hat{n}\cdot\vec{\sigma} \\ &= \cos(\frac{\theta}{2})\, I - i\sin(\frac{\theta}{2})\ (n_x X + n_y Y + n_z Z)\,. \end{aligned} \tag{2.6.7}$$

De manera particular como cualquier operador es una rotación sobre nuestro qubit, entonces un qubit puede ser escrito como una combinación lineal de los operadors I, X, Y, Z.

2.7. Compuertas de control y generación de entrelazamiento

Una de las propiedades más conocidas de la mecánica cuántica, es el fenómeno de entrelazamiento cuántico, observado en sistemas cuánticos compuestos. Propiedad predicha en 1935 por Einstein, Podolsky y Rosen en la formulación de la ahora conocida como paradoja EPR. Este fenómeno cuántico, sin equivalente clásico, nos dice que los estados cuánticos de dos o más objetos se deben describir haciendo referencia a los estados cuánticos de todos los objetos del sistema, es decir, los objetos están ligados de tal manera que uno no puede ser descrito adecuadamente sin una mención total del resto de los objetos, sin importar que los objetos estén separados espacialmente (Capítulo 1 y 4).

El espacio de Hilbert H asociado con un sistema compuesto es el producto tensorial de los espacios de Hibert $\mathcal{H}_i$ asociados con los componentes i. En el caso de un sistema cuántico bipartito tenemos

$$H \ = \ H_1 \otimes H_2.$$

Podemos construir una base del espacio de Hilbert H a partir del producto tensorial de los vectores base de H_1 *y* H_2 , si nuestros espacios de Hilbert H_1 *y* H_2 son de dos dimesiones y tienen como vectores base, respectivamente,

$$\{\mid 0\rangle_1, \mid 1\rangle_1\}, \qquad\qquad \{\mid 0\rangle_2, \mid 1\rangle_2\},$$

entonces una base del espacio de Hilbert definido por H está dado por los 4 vectores:

$$\begin{aligned} &\mid 0\rangle_1 \otimes \mid 0\rangle_2 \quad , \\ &\mid 0\rangle_1 \otimes \mid 1\rangle_2 \quad , \\ &\mid 1\rangle_1 \otimes \mid 0\rangle_2 \quad , \\ &\mid 1\rangle_1 \otimes \mid 1\rangle_2 \quad . \end{aligned}$$

El principio de superposición nos dice que el estado más general en el espacio de Hilbert H no es el producto tensorial de los estados pertenecientes a H_1 *y* H_2 , sino un superposición arbitraria de dichos estados:

$$\mid \varphi\rangle = \sum_{i,j=0}^{1} c_{ij} \mid i\rangle_1 \otimes \mid j\rangle_2 \ = \ \sum_{i,j} c_{ij} \mid i,j\rangle. \tag{2.7.1}$$

donde en el estado $\mid i,j\rangle, i$ se refiere al primer qubit y j al segundo qubit.
Por definición, un estado en H está entrelazado si NO puede ser escrito como un simple producto tensorial de un estado $\mid \alpha\rangle_1$ perteneciendo a H_1 y de un estado $\mid \beta\rangle_2$ perteneciente a H_2.
Si podemos escribir

$$\mid \varphi\rangle = \mid \alpha\rangle_1 \otimes \mid \beta\rangle_1, \tag{2.7.2}$$

decimos que el estado $\mid \varphi\rangle$ es separable.

Ejemplos:
Sea $\mid \varphi_1\rangle = \frac{1}{\sqrt{2}}(\mid 00\rangle + \mid 11\rangle)$. Decimos que está entrelazado, ya que no puede ser descompuesto como producto tensorial de los estados del sistema.

Sea $\mid \varphi_2\rangle = \frac{1}{\sqrt{2}}(\mid 01\rangle + \mid 11\rangle)$. Decimos que es separable, ya que puede ser escrito de la siguiente manera: $\mid \varphi_2\rangle = \frac{1}{\sqrt{2}}(\mid 0\rangle + \mid 1\rangle) \otimes \mid 1\rangle$.

En general un estado separable de n-qubits tiene únicamente $2n$ parámetros reales mientras que el estado más general enredado tiene $2(2^n - 1)$ estados.
Cabe destacar que con las compuertas cuánticas de un solo qubit no es posible generar entrelazamiento en un sistema de n-qubits. Además, si iniciamos de un estado separable podemos mover a nuestro deseo cualquier qubit en la Esfera de Bloch. Cualquier estado del tipo $\mid \psi_i\rangle$ puede ser transformado por compuertas actuando sobre el qubit i en cualquier superposición de estados de nuestra base, pero el estado de nuestro sistema de n-qubits seguirá siendo separable.

Para preparar un estado entrelazado necesitaremos interacciones entre qubits y lo haremos con una compuerta de 2-qubits.

2.7.1. CNOT (NO-controlada)

La compuerta que es capaz de generar entrelazamiento será la compuerta CNOT (NO-controlada). Esta compuerta actúa en los estados de la base computacional,
$\{\mid i_1 i_0\rangle = \mid 00\rangle, \mid 01\rangle, \mid 10\rangle, \mid 11\rangle\}$.

$$CNOT\,(\mid x\rangle \mid y\rangle) = \mid x\rangle \mid x \oplus y\rangle,$$

con $x, y = 0, 1$ y $\oplus$ indicando adición módulo 2. El primer qubit en la compuerta CNOT actúa como *qubit de control* y el segundo como *qubit blanco.* La compuerta cambia el estado de nuestro *qubit blanco* si el *qubit de control* está en el estado $\mid 1\rangle$, y no hace nada si el *qubit de control* se encuentra en el estado $\mid 0\rangle$.
La compuerta CNOT puede ser descrita por el siguiente operador:

$$\text{CNOT} = \mid 00\rangle\langle 00 \mid + \mid 01\rangle\langle 01 \mid + \mid 10\rangle\langle 11 \mid + \mid 11\rangle\langle 10 \mid .$$

La representación matricial de la compuerta CNOT está dada por

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

donde las componentes $(\text{CNOT})_{ij}$ de esta matriz están dadas por
$(\text{CNOT})_{ij} = \langle i \mid \text{CNOT} \mid j\rangle$.

La compuerta CNOT puede ser aplicada a cualquier superposición de los estados de la base computacional.

La compuerta CNOT puede generar estados entrelazados.
Ejemplo:

$$\text{CNOT}\left(\alpha \mid 0\rangle + \beta \mid 1\rangle\right) \mid 0\rangle \;=\; \alpha \mid 00\rangle + \beta \mid 11\rangle,$$

que es un estado no separable ($\alpha, \beta \neq 0$).
También podemos definir compuertas CNOT generalizadas, que dependen de la posición del qubit de control, ya sea el primero o segundo qubit.

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

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

A cambia el segundo qubit si el primero es $\mid 1\rangle$ (CNOT estándar),
B cambia el segundo qubit si el primero es $\mid 0\rangle$,
C cambia el primer qubit si el segundo qubit es $\mid 1\rangle$,
D cambia el primer qubit si el segundo qubit es $\mid 0\rangle$.

Otras compuertas a destacar son:

CPHASE: Aplica un corrimiento de fase al qubit blanco sólo cuando el qubit de control se encuentra en el estado $\mid 1\rangle$.

$$\text{CPHASE}(\delta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{bmatrix}.$$

cuando $\delta = \pi$ se tiene la compuerta CMINUS.

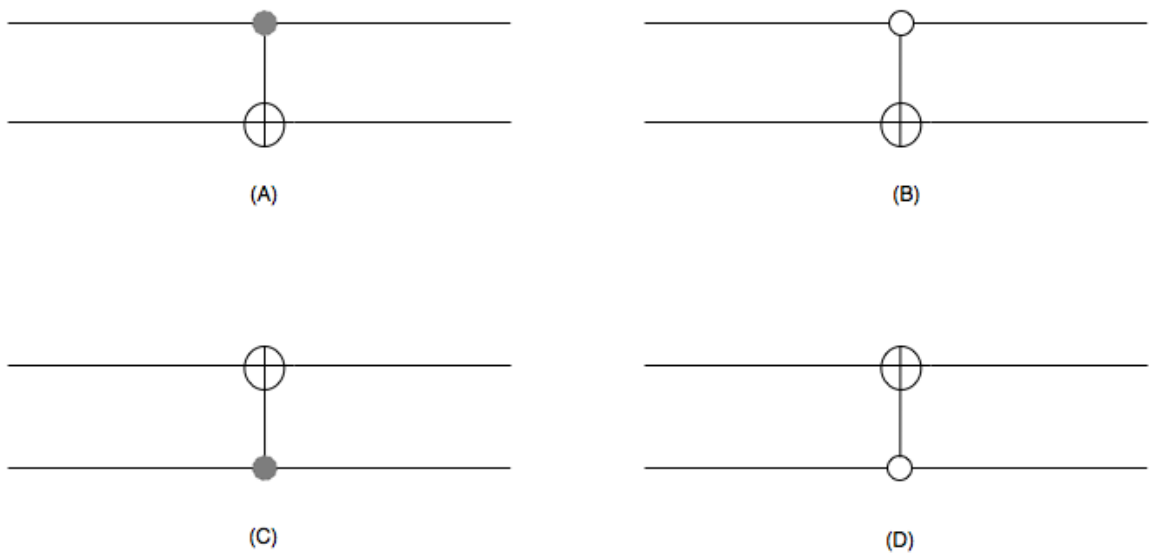


Figure 2.7.1: Representación de las compuertas cuánticas CNOT a través de circuitos. El qubit control es dibujado con un círculo lleno si el qubit blanco es cambiado cuando el bit control está en $\mid 1\rangle$, un círculo vacío es dibujado cuando el blanco cambia si el bit control es $\mid 0\rangle$.

2.7.2. Bases de Bell

Definimos los estados entrelazados Bases de Bell de la siguiente manera:

$$\mid \phi^{+}\rangle = \frac{1}{\sqrt{2}}\left((\mid 00\rangle + \mid 11\rangle)\right),$$

$$\mid \phi^{-}\rangle = \frac{1}{\sqrt{2}}\left((\mid 00\rangle - \mid 11\rangle)\right),$$

$$\mid \psi^{+}\rangle = \frac{1}{\sqrt{2}}\left((\mid 01\rangle + \mid 10\rangle)\right),$$

$$\mid \psi^{-}\rangle = \frac{1}{\sqrt{2}}\left((\mid 01\rangle - \mid 10\rangle)\right),$$

que pueden ser obtenidas a partir de la base computacional, mediante el circuito de la Figura 2.7.2 donde se tienen dos qubits al primero se le aplica una transformación de Hadarmard y posteriormente se utiliza la compuerta CNOT(A).

Dicho círcuito produce las siguientes transfomaciones:

$$AH \mid 00\rangle = \mid \phi^{+}\rangle, \qquad AH \mid 01\rangle = \mid \psi^{+}\rangle,$$

$$AH \mid 10\rangle = \mid \phi^{-}\rangle, \qquad AH \mid 11\rangle = \mid \psi^{-}\rangle.$$

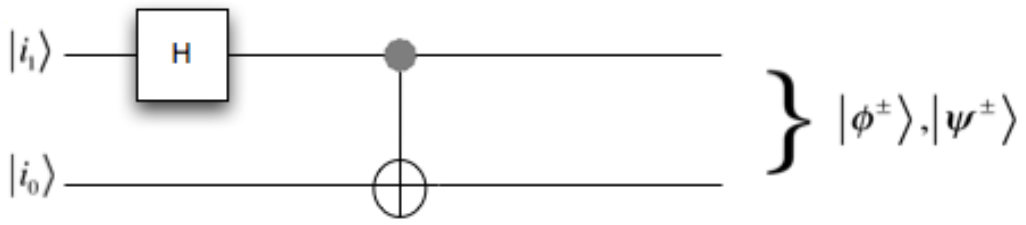


Figure 2.7.2: Círcuito que transforma los estados de la base computacional a los estados de Bell.

2.8. Compuertas Cuánticas Universales

Una computadora clásica es capaz de generar cualquier cómputo de gran complejidad a partir únicamente de la combinación de operaciones elementales (NAND y COPY), es decir, a partir de estas operaciones podemos implementar cualquier función lógica, en esta característica radica la gran utiidad de modelo de círcuito del cómputo clásico. La compuerta NAND produce salida cero si y sólo si ambas entradas son uno. La compuerta COPY convierte un bit en dos bits iguales.
En Computacion Cuántica existe un resultado similar, cualquier operación unitaria en el espacio de Hilbert H de n-qubits puede descomponerse en una secuencia de compuertas de 1-qubit y de 2-qubits CNOT.

Sea U una transformación arbitraria sobre 1-qubit, definimos *control-U* como la operación donde U actúa sobre el *qubit blanco* sólo si el *qubit de control* se encuentra en $|\ 1\rangle$:

$$|\ i_1\rangle\ |\ i_0\rangle \rightarrow |\ i_1\rangle U^{i_1}\ |\ i_o\rangle. \tag{2.8.1}$$

Como una matriz U es unitaria si y sólo si *(sii)* sus renglones y columnas son ortonormales, entonces cualquier matriz unitaria de 2×2 puede ser escrita

$$\begin{aligned} U &= \begin{bmatrix} e^{i(\alpha+\beta)/2}\cos\frac{\theta}{2} & -e^{i(\alpha-\beta)/2}\sin\frac{\theta}{2} \\ e^{i(\beta-\alpha)/2}\sin\frac{\theta}{2} & e^{-i(\alpha+\beta)/2}\cos\frac{\theta}{2} \end{bmatrix} \\ &= \begin{pmatrix} e^{i\alpha/2} & o \\ o & e^{-i\alpha/2} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{pmatrix} \\ &= R_z(\alpha)\, R_y(\theta)\, R_z(\beta)\ , \end{aligned}$$

donde α, β, θ son parámetros reales, y se utlizan los resultados (2.6.6).
Es inmediato que las matrices R satisfacen la propiedad de grupo, entonces
$\mathrm{R}(\theta+\phi) = \mathrm{R}(\theta)\ \mathrm{R}(\phi)$, además $\mathrm{R}(0) = \mathrm{I} \Rightarrow \mathrm{R}(\theta)^{-1} = \mathrm{R}(-\theta)$

Sea $\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ la matriz de Pauli en la dirección del eje X que tiene la propiedad $X \cdot R(\theta) = R(-\theta)\ X$.

Definimos las matrices siguientes:

$$\begin{aligned} A &= R_z(\alpha)\, R_y(\theta/2), \\ B &= R_y(-\theta/2)\, R_z(-\frac{\beta+\alpha}{2}), \\ C &= R_z(\frac{\beta-\alpha}{2}). \end{aligned}$$

tales que el producto :

$$\begin{aligned} \text{ABC} &= R_z(\alpha)\, R_y(\theta/2)\, R_y(-\theta/2)\, R_z(-\tfrac{\beta+\alpha}{2}) R_z(\tfrac{\beta-\alpha}{2}) \\ &= \text{R}_z(\alpha)\ \ R_z(\text{-}\tfrac{\beta+\alpha}{2})\, \text{R}_z(\tfrac{\beta-\alpha}{2}) \\ &= \text{R}_z(\alpha)\ \ \text{R}_z(-\alpha) \\ &= \text{I}. \end{aligned}$$

En forma similar se prueba que

$$\begin{aligned} \text{AXBXC} &= R_z(\alpha)\, R_y(\theta/2) X\, R_y(-\theta/2)\, R_z(-\tfrac{\beta+\alpha}{2}) X R_z(\tfrac{\beta-\alpha}{2}) \\ &= R_z(\alpha)\, R_y(\theta/2)\ R_y(\theta/2) X\, R_z(-\tfrac{\beta+\alpha}{2}) X R_z(\tfrac{\beta-\alpha}{2}) \\ &= R_z(\alpha)\, R_y(\theta/2)\ R_y(\theta/2)\, R_z(\tfrac{\beta+\alpha}{2}) X X R_z(\tfrac{\beta-\alpha}{2}) \\ &= R_z(\alpha)\, R_y(\theta)\, R_z(\beta) \\ &= U. \end{aligned}$$

Se concluye únicamente que puede realizarse la compuerta control-U mediante el producto de transformaciones de un solo qubit (A, B, C) y compuertas de dos qubits CNOT.

2.8.1. Compuerta Toffoli

Las compuertas cuánticas como ya hemos mencionado operan sobre qubits de manera reversible, mientras que en la manera clásica las compuertas lógicas operan sobre bits en la mayoría de los casos de manera irreversible. Es posible construir compuertas clásicas que son reversibles; la idea general es el copiar algunos de los bits de entrada a la salida para que los bits de entrada sean recuperados a partir del resultado y de los bits de salida extras. Representaremos esta idea a través de la compuerta Toffoli.

La compuerta Toffoli tiene 3 bits de entrada y 3 bits de salida, que llamaremos *a,b,c* ϵ $\{0, 1\}$, con la propiedad que aplica una operación NOT al bit blanco únicamente si los dos bits de control son uno.

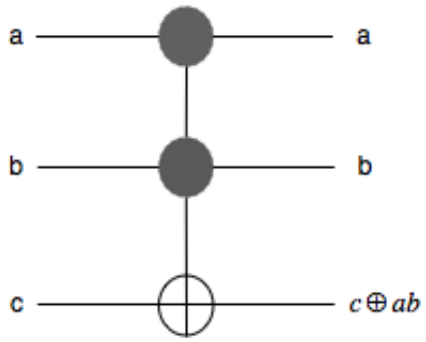


Figure 2.8.1: Compuerta clásica Toffoli

En la Fig. 2.8.1 el término $c \oplus ab$, la operación $\oplus$ es la adición módulo 2 y ab es la multiplicación usual, i.e., aplica una operación NOT al bit *blanco* sólo si los dos bits de control son 1.
Podemos escribir la compuerta Toffoli como una tabla de entrada-salida de la siguiente manera:

$$(0,0,0) \longmapsto (0,0,0),$$

$$(0,0,1) \longmapsto (0,0,1),$$

$$(0,1,0) \longmapsto (0,1,0),$$

$$(0,1,1) \longmapsto (0,1,1),$$

$$(1,0,0) \longmapsto (1,0,0),$$

$$(1,0,1) \longmapsto (1,0,1),$$

$$(1,1,0) \longmapsto (1,1,1),$$

$$(1,1,1) \longmapsto (1,1,0).$$

Es inmediato encontrar que si aplicamos 2 veces la compuerta Toffoli nos da la identidad. Entonces la compuerta Toffoli es invertible, siendo igual a su inversa. Por lo tanto la compuerta Toffoli es reversible.

Es importante notar que la redundancia en la salida de la compuerta Toffoli que reproduce indénticamente los bits a y b es la manera de evitar el borrado de información, que es

una condición necesaria para permitir la reversibilidad.[2]
Para demostrar que toda compuerta clásica puede ser obtenida a partir de la compuerta de Toffoli basta con demostrar que la operación NAND (la negación de la compuerta AND) puede ser construida en dicho modo, esto es, [24]

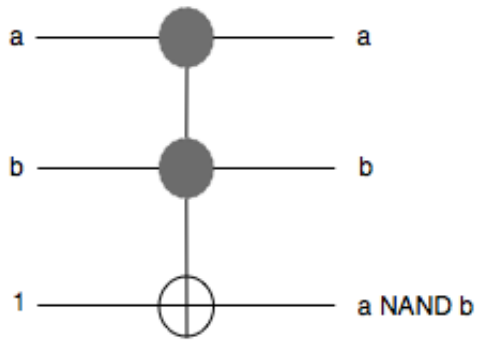


Figure 2.8.2: Obtención de la operación NAND a partir de la compuerta Toffoli

La compuerta clásica Toffoli tiene también su versión cuántica. Está definida a tráves de la tripleta de estados $|\, abc\rangle$. Hablando cuánticamente la compuerta Toffoli tiene la siguiente acción sobre la cadena de bits cuánticos: $|\, abc\rangle \longrightarrow |\, ab(c \oplus ab)\rangle$. De la misma manera que la compuerta Toffoli clásica, podemos escribir una tabla de entrada-salida:

$$|\, 000\rangle \longrightarrow |\, 000\rangle,$$

$$|\, 001\rangle \longrightarrow |\, 001\rangle,$$

$$|\, 010\rangle \longrightarrow |\, 010\rangle,$$

$$|\, 011\rangle \longrightarrow |\, 011\rangle,$$

$$|\, 100\rangle \longrightarrow |\, 100\rangle,$$

$$|\, 101\rangle \longrightarrow |\, 101\rangle,$$

$$|\, 110\rangle \longrightarrow |\, 111\rangle,$$

$$|\, 111\rangle \longrightarrow |\, 110\rangle.$$

La representación por medio de circuitos de la compuerta cuántica está dada por:

[2]En 1961 Rolf Landauer descubrió que el único proceso irreversible en computación es el borrado de información.

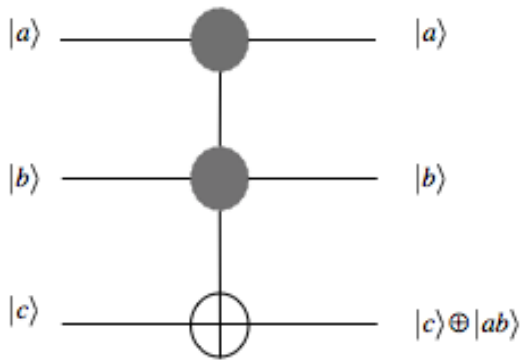


Figure 2.8.3: Compuerta Cuántica Toffoli

La compuerta Toffoli es un componente básico en la implementación de casi todo algoritmo cuántico. Entonces una computadora cuántica construida de esta manera nos permite hacer cualquier cosa que una computadora clásica puede hacer. A continuación se presenta una generalización de la compuerta Toffoli ($C^2 - NOT$).

2.8.2. Compuerta C^k-U

Aplica una transformación arbitraria U al qubit blanco si todos los qubits de control toman el valor uno. Estas compuertas pueden ser implementadas por medio de compuertas elementales, particularmente por compuertas de un solo qubit y compuertas CNOT.
La compuerta Toffoli es un caso particular de dicha compuerta para k=2.
Además cualquier operador unitario genérico U^n actuando en un espacio de Hilbert de n-qubits puede ser descompuesto por la compuerta C$^k - U$, donde U^n puede ser descompuesto como (ver Barenco *et. al.,* 1995)

$$U^n = \prod_{i=1}^{2^n-1} \prod_{j=0}^{i-1} V_{ij},$$

donde V_{ij} induce una rotación de los estados $\mid i\rangle$, $\mid j\rangle$ de acuerdo a una matriz unitaria de 2×2. La idea de implementar V_{ij} en una computadora cuántica es el reducir las rotaciones de los ejes $\mid i\rangle$ y $\mid j\rangle$ a una rotación controlada en un solo qubit. [12] Las compuertas Toffoli pueden implementarse usando compuertas CNOT, control-U y Hadamard. Las compuertas $C^k - U$ pueden descomponerse en Toffoli y compuertas control-U. Finalmente una compuerta de n-qubits puede descomponerse en compuertas $C^k - U$. Por lo tanto las compuertas de un solo qubit y la CNOT son compuertas universales de la computación cuántica.

2.8.3. Preparación del estado inicial

La preparación, en general, de un estado en cómputo cuántico requiere un número de compuertas que es exponencial en el número de qubits. La computadora cuántica tiene una ventaja exponencial en los requerimientos de memoria. Un vector de onda de n-qubits es

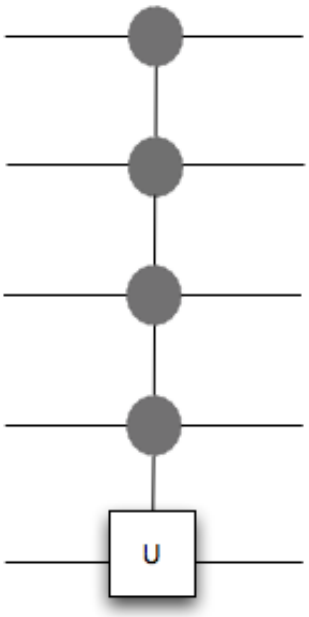


Figure 2.8.4: Compuerta $C^k - U$ para $k = 4$.

determinado por 2^n números complejos y los coeficientes de su expansión definidos sobre la base computacional. Una computadora clásica necesita $m2^n$ bits para almacenar 2^n números complejos, donde m es el número de bits requerido para almacenar un número complejo con una precisión dada. La gran capacidad de memoria del cómputo cuántico permite manejar este mismo problema con solo n qubits.

Como ilustración se considera la construcción de un estado genérico de tres qubits $\mid \psi\rangle = \sum_{i=0}^{7} a_i \mid i\rangle$ mediante la acción de 7 rotaciones controladas sobre el estado fiducial $\mid 000\rangle$, i.e.,

$$\mid \psi\rangle = \prod_{i=1}^{7} R_y(-2\Theta_i) \mid 000\rangle.$$

donde $R_y(-2\Theta_i) = e^{-i\Theta_i\sigma_i}$. En forma más precisa se requiere una rotación en el eje y del primer qubit, dos rotaciones controladas por el primer qubit y de blanco el segundo qubit y finalmente 4 rotaciones del tipo $C^2 - R_y$ sobre los tres qubits. De esta manera se obtienen las amplitudes $\mid a_i\rangle$ de los coeficientes del desarrollo del estado de tres qubits. Para determinar las fases se aplican 4 componentes de un solo qubit de la forma

$$\Gamma_0 = \begin{bmatrix} e^{i\gamma_0} & 0 \\ 0 & e^{i\gamma_1} \end{bmatrix},$$

$$\Gamma_1 = \begin{bmatrix} e^{i\gamma_2} & 0 \\ 0 & e^{i\gamma_3} \end{bmatrix},$$

$$\Gamma_2 = \begin{bmatrix} e^{i\gamma_4} & 0 \\ 0 & e^{i\gamma_5} \end{bmatrix},$$

$$\Gamma_3 = \begin{bmatrix} e^{i\gamma_6} & 0 \\ 0 & e^{i\gamma_7} \end{bmatrix}.$$

donde $a_i = \mid a_i \mid e^{i\gamma_i}$.

Una operación en una computadora cuántica se dice que es implementada eficientemente si se requiere un número de compuertas elementales polinomial en el número de qubits. Por ejemplo la superposición no sesgada de todos los estados de la base computacional,

$$\mid \psi\rangle = \sum_{i=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \mid i\rangle, \tag{2.8.2}$$

es obtenida después de la aplicación de n compuertas de Hadamard (una para cada qubit) al estado $\mid 0\rangle$.

2.8.4. Errores Unitarios

Cualquier cómputo cuántico está dado por una secuencia de compuertas cuánticas aplicadas a un estado inicial:

$$\mid \psi_n\rangle = \prod_{i=1}^{n} U_i \mid \psi_0\rangle. \tag{2.8.3}$$

Como los operadores unitarios forman un conjunto continuo, cualquier implementación podrá tener algún error. Supóngase que los errores son también unitarios, por lo que en vez de los operadores U_i se aplican ahora los operadores unitarios imperfectos V_i.

Sea $\mid \psi_i\rangle$ el estado obtenido después de i pasos (transformaciones unitarias V_i) se tiene que

$$\mid \psi_i\rangle = U_i \mid \psi_{i-1}\rangle.$$

Si aplicamos el operador imperfecto V_i obtenemos

$$V_i \mid \psi_{i-1}\rangle = \mid \psi_i\rangle + \mid E_i\rangle,$$

donde definimos

$$\mid E_i\rangle = (V_i - U_i) \mid \psi_{i-1}\rangle.$$

Si $\mid \widetilde{\psi}_i\rangle$ denota la función de onda del cómputo cuántico después de la aplicación de i transformaciones unitarias imperfectas se obtiene

$$\begin{aligned} \widetilde{\mid \psi_1\rangle} &= \mid \psi_1\rangle + \mid E_1\rangle, \\ \mid \widetilde{\psi}_2\rangle &= V_2 \mid \widetilde{\psi}_1\rangle = \mid \psi_2\rangle + \mid E_2\rangle + V_2 \mid E_1\rangle. \end{aligned}$$

Por lo tanto después de n iteraciones se obtendrá la expresión

$$\begin{aligned} \mid \widetilde{\psi}_n\rangle = \mid \psi_n\rangle + \mid E_n\rangle + V_n \mid E_{n-1}\rangle + \\ + V_nV_{n-1} \mid E_{n-2}\rangle + \ldots + V_nV_{n-1}\ldots V_2 \mid E_1\rangle. \end{aligned}$$

En el peor de los casos los errores son lineales con respecto a la longitud del cómputo cuántico. Esto permite obtener, como consecuencia de la desigualdad del triángulo, que

$$\| \mid \widetilde{\psi}_n\rangle - \mid \psi_n\rangle \| \leq \sum_{k=1}^{n} \| \mid E_k\rangle \| .$$

Donde ademas hemos utilizado el hecho de que la evolución es unitaria

$$\| V_i \mid E_{i-1}\rangle \| = \| \mid E_{i-1}\rangle \| .$$

Podemos acotar la norma Euclideana del vector de error $\mid E_i\rangle$ de la siguiente manera

$$\| \mid E_i\rangle \| = \| (V_i - U_i) \mid \psi_{i-1}\rangle \| \leq \| V_i - U_i \|_{sup}, \tag{2.8.4}$$

donde $\| V_i - U_i \|_{sup}$ denota la norma superior del operador $V_i - U_i$, es decir, el eigenvalor de módulo máximo. Suponiendo que el error está acotado uniformemente en cada paso:

$$\| V_i - U_i \|_{sup} < \epsilon, \tag{2.8.5}$$

se obtiene después de la aplicación de n operadores imperfectos

$$\| \mid \widetilde{\psi}_n\rangle - \mid \psi_n\rangle \| < n\epsilon. \tag{2.8.6}$$

Por lo tanto los errores unitarios se acumulan en el peor de los casos en forma lineal con respecto a la longitud de cómputo. Este error toma lugar en los errores sistemáticos que se alinean en la misma dirección, mientras que errores estocásticos están aleatoriamente direccionados y tienen un crecimiento del orden de $\sqrt{n}$.

Es importante destacar que cualquier cómputo cuántico termina con una medición proyectiva sobre la base computacional, dando como salida i con probabilidad $p_i = \mid \langle i \mid \psi_n\rangle \mid^2$. En la presencia de errores unitarios, la probabilidad real se vuelve $\tilde{p}_i = \mid \langle i \mid \widetilde{\psi}_n\rangle \mid^2$. De esta forma se relaciona la precisión de la función de onda del cómputo cuántico con la precisión del resultado de la computación cuántica.

2.9. Algoritmos Cuánticos

La compuerta de Hadamard (ver 2.4.1) es una herramienta importante para el desarrollo de algoritmos cuánticos; recordemos que esta compuerta ayuda a crear una superposición de estados. Una caracteristica interesante de dicha compuerta es que si la aplicamos en serie actúa de manera reversible, regresándonos el estado original ($\mathrm{H}^2 = I$).

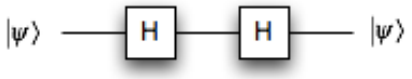


Figure 2.9.1: Dos compuertas de Hadamard aplicadas en serie

Ahora, si aplicamos dicha compuerta de manera paralela (actuando sobre cada qubit) obtenemos el producto de dos estados superpuestos

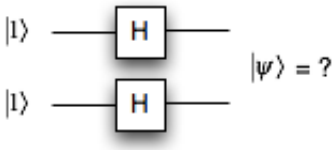


Figure 2.9.2: Dos compuertas de Hadamard aplicadas de manera paralela

Por ejemplo, suponiendo el estado inicial $\mid 1\rangle \mid 1\rangle$, y aplicamos estas compuertas paralelamente obtenemos

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

$$= \frac{1}{2}\left(\mid 00\rangle - \mid 01\rangle - \mid 10\rangle + \mid 11\rangle\right) \tag{2.9.1}$$

Se llama *transformada de Hadamard* a la aplicación de n compuertas de Hadamard en paralelo sobre n qubits: $\mathrm{H}^{\otimes n}$. Entonces la operación (2.9.1) la podríamos escribir en forma abreviada como $\mathrm{H}^{\otimes 2}$.
Si aplicamos $\mathrm{H}^{\otimes 3}$ al estado $\mid 0\rangle \mid 0\rangle \mid 0\rangle$ obtenemos,

$$\begin{aligned}(H \otimes H \otimes H) \quad \mid 000\rangle &= (H \mid 0\rangle)(H \mid 0\rangle)(H \mid 0\rangle) \\ &= \left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right).\end{aligned}$$

$$= \frac{1}{\sqrt{2^3}}\left(\mid 000\rangle + \mid 001\rangle + \mid 010\rangle + \mid 011\rangle + \mid 100\rangle + \mid 101\rangle + \mid 110\rangle + \mid 111\rangle\right).$$

Los resultados anteriores se pueden escribir de forma más compacta. Sea $\mid x\rangle$ un estado general donde $x = 0, ..., 2^n - 1$, es decir, $\mid x\rangle$ es alguno de los estados de dos qubits: $\mid 0\rangle = \mid 00\rangle, \mid 1\rangle = \mid 01\rangle, \mid 2\rangle = \mid 10\rangle, \mid 3\rangle = \mid 11\rangle$. De la misma manera si escribimos $x \in \{0,1\}^3$ entonces $\mid x\rangle$ es alguno de los estados: $\mid 000\rangle, \mid 001\rangle, \mid 010\rangle, \mid 011\rangle, \mid 100\rangle, \mid 101\rangle, \mid 110\rangle, \mid 111\rangle$. Por lo tanto si sumamos sobre la variable $\mid x\rangle$, se obtiene

$$(H \otimes H) \mid 0\rangle \mid 0\rangle = H^{\otimes 2} \mid 0\rangle^{\otimes 2} = \frac{1}{\sqrt{2^2}} \sum_{x=0}^{3} \mid x\rangle. \tag{2.9.2}$$

$$(H \otimes H \otimes H)) \mid 0\rangle \mid 0\rangle \mid 0\rangle \; = H^{\otimes 3} \mid 0\rangle^{\otimes 3} \; = \frac{1}{\sqrt{2^3}} \sum_{x=0}^{7} \mid x\rangle.$$

De esta manera la aplicación $\mathrm{H}^{\otimes n}$ a un estado con n copias de $\mid 0\rangle$ puede escibirse como

$$H^{\otimes n} \mid 0\rangle^{\otimes n} \; = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \mid x\rangle. \tag{2.9.3}$$

De igual manera si aplicamos H⊗H al producto de estados $\mid 0\rangle \mid 1\rangle$ obtendremos

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

$$= \frac{1}{2}\left(\mid 00\rangle - \mid 01\rangle + \mid 10\rangle - \mid 11\rangle\right). \tag{2.9.4}$$

Si $x \equiv 1, 2\, y\, 3$ para denotar los estados respectivamente. Entonces se puede escribir la ecuación de manera más compacta:

$$H^{\otimes 2} \mid 01\rangle \; = \frac{1}{2} \sum_{x=0}^{3} (-1)^x \mid x\rangle.$$

Es directo escribir la acción de la compuerta de Hadamard en la base computacional para el i-ésimo qubit

$$H \mid x_i\rangle = \frac{1}{\sqrt{2}} \sum_{y_i=1}^{i} (-1)^{x_i y_i} \mid y_i\rangle.$$

Entonces la acción en paralelo de n compuertas de Hadamard sobre un estado de n qubits

$$\mid x\rangle = \mid x_{n-1} x_{n-2}, \ldots, x_0\rangle,$$

puede escribirse como

$$\begin{aligned} H^{\otimes n} \mid x\rangle \quad &= \prod_{i=0}^{n-1} \left\{ \frac{1}{\sqrt{2}} \sum_{y_i=0}^{1} (-1)^{x_i y_i} \mid y_i\rangle \right\} \\ &= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} \mid y\rangle, \end{aligned} \tag{2.9.5}$$

donde $x \cdot y = (x_{n-1} y_{n-1} \oplus x_{n-2} y_{n-2} \oplus \cdots \oplus x_0 y_0)$ denota el producto escalar de x y y en base 2. Es inmediato probar que (2.9.5) es una generalización de los resultados obtenidos en las expresiones (2.9.2), (2.9.3) y (2.9.4).

2.9.1. Interferencia Cuántica

La aplicación de una compuerta de Hadamard a un qubit arbitrario es un buen ejemplo para ilustrar el fenómeno de interferencia cuántica. Si calculamos $H \mid \psi\rangle$ para $\mid \psi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle$ obtenemos

$$H \mid \psi\rangle = \left(\frac{\alpha+\beta}{\sqrt{2}}\right) \mid 0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right) \mid 1\rangle. \tag{2.9.6}$$

Notemos que la amplitud de probabilidad de obtener $\mid 0\rangle$ después de una medición ha cambiado como sigue:

$$\alpha \longrightarrow \frac{\alpha+\beta}{\sqrt{2}},$$

y la amplitud de probabilidad de obtener $\mid 1\rangle$ sufre la transformación:

$$\beta \longrightarrow \frac{\alpha-\beta}{\sqrt{2}}.$$

Existen 2 tipos de interferencia: *interferencia positiva,* en donde las amplitudes de las probabilidades se suman constructivamente para aumentarse o *interferencia negativa* donde las amplitudes de las probabilidades decrecen.
Por ejemplo si aplicamos H a $\mid \psi\rangle = (\mid 0\rangle + (-1)^x \mid 1 >)/\sqrt{2}$, donde $x\epsilon\{0,1\}$ obtenemos

$$H \mid \psi\rangle = \left(\frac{1+(-1)^x}{2}\right) \mid 0\rangle + \left(\frac{1-(-1)^x}{2}\right) \mid 1\rangle.$$

Por lo tanto se concluye que

$$H \mid \psi\rangle = \mid 0\rangle \qquad \text{si } x = 0,$$

$$H \mid \psi\rangle = \mid 1\rangle \qquad \text{si } x = 1.$$

Entonces observamos lo siguiente en (2.9.6) para $x = 0$:

- *Interferencia positiva* sobre el estado $\mid 0\rangle$, las dos amplitudes se suman para aumentar la probabilidad de encontrar el estado $\mid 0\rangle$ durante la medición. En este caso la probabilidad se vuelve unitaria.

- *Interferencia negativa* sobre $\mid 1\rangle$, vamos de un estado donde teníamos 50% de probabilidad de encontrar el estado $\mid 1\rangle$ a otro donde la probabilidad de encontrar el estado $\mid 1\rangle$ es nula.

La interferencia cuántica como veremos permite obtener información sobre las propiedades globales de una función *f(x)*, donde $f(x)$ es una función lógica binaria que tiene una entrada de n-qubits (x) y una salida de un qubit, $\{0,1\}$.

2.9.2. Algoritmo de Deutsch

Permite determinar si una función lógica de 2 qubits es constante o balanceada.
Una función básica de una computadora clásica es la evaluación de una función lógica con n bits de entrada y un bit de salida, esto es

$$f : \{0,1\}^n \longrightarrow \{0,1\}\,.$$

Definimos una *función balanceada* como aquella cuyos valores de salida pueden ser opuestas para la mitad de sus entradas. Como ejemplo se tiene la *función swap y la función identidad.*
Una función de un solo bit la definimos como *función constante,* si ocurre que *f(x) = 0 o f(x) = 1*.
Si una función es balanceada o constante es una propiedad global. El algoritmo de Deustsch ayudará a saber si una función de un qubit es una función constante o una función balanceada.

El primer paso es denotar un operador unitario U_f que actúe sobre dos qubits, con la propiedad de que es la función identidad en el primer qubit y produzca una compuerta OR exclusiva del segundo qubit con una función f que usa al primer qubit como argumento,

$$U_f \mid x_i, y_i\rangle = \mid x_i\ ,\ y_i \oplus f(x_i)\rangle, \quad x_i, y_i \epsilon \{0,1\}\,. \tag{2.9.7}$$

Como $\mid x_i\rangle$ es un qubit, entonces puede estar en un estado superpuesto.

El algoritmo de Deutsch utiliza los resultados anteriores para explotar el que un estado se encuentre en una superposición para obtener información sobre la propiedad global de una función. El procedimiento es el siguiente:

$$\mid \psi\rangle_{salida} = (H \otimes I)\, U_f\, (H \otimes H) \mid 0\rangle \mid 1\rangle.$$

Descripción del algoritmo de Deutsch

1. Aplicar las compuertas Hadamard al estado inicial $\mid 0\rangle \mid 1\rangle$ para producir el producto de estados de dos superposiciones.
2. Aplicar U_f al estado obtenido.
3. Aplicar una compuerta Hadamard al primer qubit dejando libre el segundo qubit.

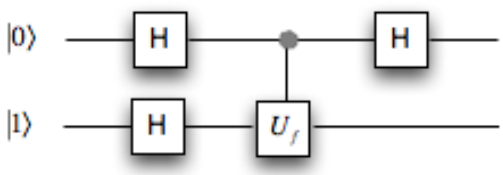


Figure 2.9.3: Circuito Cuántico del Algoritmo de Deutsch

Usando (2.9.4) sabemos el resultado del paso 1

$$(H \otimes H) \mid 0\rangle \mid 1\rangle = \frac{1}{2}\left(\mid 00\rangle - \mid 01\rangle + \mid 10\rangle - \mid 11\rangle\right),$$

obteniéndose entonces una superposición de estados.
Ahora apliquemos U_f a cada término del resultado obtenido en el paso 1.

Para el primer término tenemos

$$U_f \mid 00\rangle = \mid 0,\ 0 \oplus f(0)\rangle = (1 - f(0)) \mid 00\rangle + f(0) \mid 01\rangle.$$

Este resultado toma en cuenta las posibilidades $0 \oplus f(0) = 0$ y $0 \oplus f(0) = 1$. Notemos que si f(0) = 0, entonces $0 \oplus f(0) = 0 + 0 = 0$.
Por otro lado, si f(0)=1, entonces $0 \oplus f(0) = 0 + 1 = 1$.
Similarmente para el resto de los términos, se obtiene

$$U_f \mid 01\rangle = \mid 0,\ 1 \oplus f(0)\rangle = f(0) \mid 00\rangle + (1 - f(0)) \mid 01\rangle,$$

$$U_f \mid 10\rangle = \mid 1,\ 0 \oplus f(1)\rangle = (1 - f(1)) \mid 10\rangle + f(1) \mid 11\rangle,$$

$$U_f \mid 11\rangle = \mid 1,\ 1 \oplus f(1)\rangle = f(1) \mid 10\rangle + (1 - f(1)) \mid 11\rangle.$$

Utilizando los resultados anteriores se tiene que

$$\begin{aligned} \mid \psi' \rangle &= U_f(H \otimes H) \mid 0\rangle \mid 1\rangle \\ &= \frac{1}{\sqrt{2}} \left\{ \left(\frac{1}{2} - f(0) \right) \mid 0\rangle + \left(\frac{1}{2} - f(1) \right) \mid 1\rangle \right\} \left\{ \frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right\}. \end{aligned}$$

Para obtener la salida final del algoritmo de Deutsch aplicamos $H \otimes I$ a $\mid \psi' \rangle$, esto es la compuerta de Hadamard es aplicada al primer qubit, y el segundo qubit es dejado libre.
Por lo tanto aplicando $H \otimes I$ a los términos de $\mid \psi' \rangle$ obtenemos el estado final del algoritmo de Deutsch:

$$\begin{aligned} \mid \psi_{salida}\rangle = (1 - f(0) - f(1)) \mid 0\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right) \\ + (f(1) - f(0)) \mid 1\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right) \end{aligned} \tag{2.9.8}$$

Ahora, suponiendo que la función es constante, tal que f(0) = f(1). Entonces usando (2.9.8) obtenemos dos posibilidades para el estado final de salida

$$\mid \psi_{salida}\rangle = \pm \mid 0\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right).$$

Ahora, si f(0) $\neq$ f(1) se tiene que $(1 - f(0) - f(1)) = 0$ y el estado final está dado por las expresiones

$$\mid \psi_{salida}\rangle = \pm \mid 1\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right).$$

Podemos observar cómo la aplicación de interferencia cuántica nos ayuda a distinguir entre los dos casos de salidas de la función. De tal manera que si se mide el primer qubit y obtenemos 0 se tiene una función constante y si se obtiene 1 es una función balanceada.

2.9.3. Algoritmo Deutsch-Jozsa

El algoritmo de Deutsch-Jozsa es una generalización del algoritmo de Deutsch. Nos permite deducir si una función es constante o balanceada pero para una función con múltiples valores de entrada, esto es una función de n qubits. Si f(x) es constante entonces los valores de salida son los mismos para todas las x. Si f(x) es balanceada entonces f(x)= 0 para la mitad de las entradas y f(x) = 1 para la otra mitad de las entradas.

Fase de reinicio

Consideremos la compuerta U_f de 2 qubits que definimos en el algoritmo de Deutsch (2.9.7) :

$$U_f \mid x, y\rangle = \mid x\ ,\ y \oplus f(x)\rangle, \quad x, y \epsilon \{0, 1\}\,.$$

Cambiemos nuestro registro blanco $\mid y\rangle$ por $\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$, y analicemos la acción de nuestro operador sobre un estado base en el qubit control:

$$\begin{aligned} U_f \mid x\rangle \quad \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= \left(\frac{\mid x\rangle \mid 0 \oplus f(x)\rangle - \mid x\rangle \mid 1 \oplus f(x)\rangle}{\sqrt{2}} \right), \\ &= \mid x\rangle \left(\frac{\mid 0 \oplus f(x)\rangle - \mid 1 \oplus f(x)\rangle}{\sqrt{2}} \right). \end{aligned} \tag{2.9.9}$$

Evaluemos la expresión $\left(\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}\right)$ en los casos donde $f(x) = 0$ y $f(x) = 1$:

$f(x) = 0$: $\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$,

$f(x) = 1$: $\left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right) = (-1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$.

Estos dos resultados difieren por un factor (-1) que depende únicamente por el valor de $f(x)$. Tenemos entonces

$$\left(\frac{\mid 0\oplus f(x)\rangle - \mid 1\oplus f(x)\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right).$$

Asociando el factor $(-1)^{f(x)}$ con el primer qubit el estado (2.9.9) puede reescribirse como

$$U_f \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)} \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right).$$

Cuando el qubit de control se encuentra en una superposición de $\mid 0\rangle$ y $\mid 1\rangle$ tenemos

$$\begin{aligned} U_f(\alpha_0 \mid 0\rangle + \alpha_1 \mid 1\rangle)\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) &= ((-1)^{f(0)}\alpha_0 \mid 0\rangle + (-1)^{f(1)}\alpha_1 \mid 1\rangle)\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) \\ &= \sum_{x=0}^{1}(-1)^{f(x)}\alpha_x \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right). \end{aligned}$$

De la misma manera, si tenemos una superposición de estados dada por $H^{\otimes n} \mid 0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} \mid x\rangle$ obtenemos

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1}(-1)^{f(x)} \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right).$$

Algoritmo

Iniciamos con un estado inicial con n qubits en el estado $\mid 0\rangle$ y un solo qubit en el estado $\mid 1\rangle$. Aplicamos las n compuertas de Hadamard a todos los qubits.

$$\mid \psi\acute{}\rangle = H^{\otimes n} \mid 0\rangle^{\otimes n} \otimes (H \mid 1\rangle).$$

De (2.9.3) sabemos que

$$\mid \psi\acute{}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\epsilon\{0,1\}^n} \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right).$$

Ahora aplicamos U_f para evaluar la función. Los primeros n qubits son los valores de x y el último qubit es el valor de y. La salida de de la compuerta U_f nos da

$$\mid \psi\acute{}\acute{}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x}(-1)^{f(x)} \mid x\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right).$$

Aplicando la compuerta de Hadamard en un estado de n qubits se obtiene el resultado

(2.9.5):

$$H^{\otimes n} \mid x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x.y} \mid y\rangle,$$

donde $x \cdot y$ denota el producto interno de x y de y *mod* 2 i.e., $x \cdot y = x_{n-1}y_{n-1} + \ldots + x_0 y_0$. El estado final da

$$\mid \psi_{salida}\rangle = \frac{1}{2^n} \sum_y \sum_x (-1)^{x.y+f(x)} \mid y\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right).$$

Finalmente se miden las n entradas y existen dos posibles resultados de mediciones sobre $\mid y >$, que es el estado de n entradas en este momento. Los posibles resultados son los siguientes:

- Si la medición de los primeros n qubits da el estado $\mid 000\ldots0\rangle$ con probabilidad uno, entonces la función es constante mientras que si la probabilidad es cero se tiene una función balanceada.
- Lo anterior se debe a que $\sum_{x=0}^{2^n-1} (-1)^{f(x)} = \pm 1$ si f es constante y 0 si f es balanceada.

  Sea $\mid \psi_{inicial}\rangle = \mid 001\rangle$ y apliquemos directamente la función de salida obtenida, entonces:

$$\begin{aligned}
\mid \psi_s\rangle &= \frac{1}{2^2} \sum_y \left((-1)^{f(0)} + (-1)^{f(1)+y_0} + (-1)^{f(2)+y_1} + (-1)^{f(3)+y_1+y_0} \right) \mid y\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{4} \{ ((-1)^{f(0)} (\mid 0\rangle + \mid 1\rangle + \mid 2\rangle + \mid 3\rangle) + (-1)^{f(1)} (\mid 0\rangle - \mid 1\rangle + \mid 2\rangle - \mid 3\rangle) \\
&\quad + (-1)^{f(2)} (\mid 0\rangle + \mid 1\rangle - \mid 2\rangle - \mid 3\rangle) + (-1)^{f(3)} (\mid 0\rangle - \mid 1\rangle - \mid 2\rangle + \mid 3\rangle)) \\
&\quad \cdot \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right) \} \\
&= \{ \frac{1}{4} \left[(-1)^{f(0)} + (-1)^{f(1)} + (-1)^{f(2)} + (-1)^{f(3)} \right] \mid 0\rangle \\
&\quad + \frac{1}{4} \left[(-1)^{f(0)} - (-1)^{f(1)} + (-1)^{f(2)} - (-1)^{f(3)} \right] \mid 1\rangle \\
&\quad + \frac{1}{4} \left[(-1)^{f(0)} + (-1)^{f(1)} - (-1)^{f(2)} - (-1)^{f(3)} \right] \mid 2\rangle \\
&\quad + \frac{1}{4} \left[(-1)^{f(0)} - (-1)^{f(1)} - (-1)^{f(2)} + (-1)^{f(3)} \right] \mid 3\rangle \} \frac{1}{\sqrt{2}} (\mid 0\rangle - \mid 1\rangle).
\end{aligned}$$

  Si f es constante entonces se obtiene $\mid 0\rangle$; si no es constante, uno de los qubits restantes da el valor 1.

  Ejemplo: Sea f(x) = 1 y $\mid \psi_{inicial}\rangle = \mid 001\rangle$ demostraremos directamente como se utiliza el algortimo de Deutsch.Jozsa.

Aplicamos a cada uno de los qubits del estado inicial la compuerta Hadamard, obteniendo

$$\mid \psi' \rangle = \frac{1}{2\sqrt{2}}(\mid 000\rangle - \mid 001\rangle + \mid 010\rangle - \mid 011\rangle + \mid 100\rangle - \mid 101\rangle + \mid 110\rangle - \mid 111\rangle).$$

Aplicamos U_f :

$$\mid \psi'' \rangle = \frac{1}{2\sqrt{2}}(\mid 001\rangle - \mid 000\rangle + \mid 011\rangle - \mid 010\rangle + \mid 101\rangle - \mid 100\rangle + \mid 111\rangle - \mid 110\rangle).$$

Finalmente aplicamos H^2 a los primeros 2 qubits:

$$\begin{aligned}
\mid \psi_{salida}\rangle &= \frac{1}{2\sqrt{2}}(\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right) \mid 1\rangle \\
&\quad - \left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right) \mid 0\rangle \\
&+ \left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) \mid 1\rangle - \left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) \mid 0\rangle \\
&+ \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right) \mid 1\rangle - \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}\right) \mid 0\rangle \\
&+ \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) \mid 1\rangle - \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right)\left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}\right) \mid 0\rangle).
\end{aligned}$$

Expandiendo los términos obtenemos

$$\begin{aligned}
\mid \psi_{salida}\rangle &= \frac{1}{4\sqrt{2}}((\mid 00\rangle + \mid 01\rangle + \mid 10\rangle + \mid 11\rangle) \mid 1\rangle \\
&\quad - (\mid 00\rangle + \mid 01\rangle + \mid 10\rangle + \mid 11\rangle) \mid 0\rangle \\
&+ (\mid 00\rangle - \mid 01\rangle + \mid 10\rangle - \mid 11\rangle) \mid 1\rangle - (\mid 00\rangle - \mid 01\rangle + \mid 10\rangle - \mid 11\rangle) \mid 0\rangle \\
&+ (\mid 00\rangle + \mid 01\rangle - \mid 10\rangle - \mid 11\rangle) \mid 1\rangle - (\mid 00\rangle + \mid 01\rangle - \mid 10\rangle - \mid 11\rangle) \mid 0\rangle \\
&+ (\mid 00\rangle - \mid 01\rangle - \mid 10\rangle + \mid 11\rangle) \mid 1\rangle - (\mid 00\rangle - \mid 01\rangle - \mid 10\rangle + \mid 11\rangle) \mid 0\rangle).
\end{aligned}$$

Factorizamos estas funciones para ponerlas en la forma del tercer qubit $(\mid 0\rangle - \mid 1\rangle)\ /\sqrt{2}$

$$\begin{aligned}
\mid \psi_{salida}\rangle = \frac{1}{4}&(-(\mid 00\rangle + \mid 01\rangle + \mid 10\rangle + \mid 11\rangle)(\mid 0\rangle - \mid 1\rangle)\ /\sqrt{2} \\
&-(\mid 00\rangle - \mid 01\rangle + \mid 10\rangle - \mid 11\rangle)(\mid 0\rangle - \mid 1\rangle)\ /\sqrt{2} \\
&-(\mid 00\rangle + \mid 01\rangle - \mid 10\rangle - \mid 11\rangle)(\mid 0\rangle - \mid 1\rangle)\ /\sqrt{2} \\
&-(\mid 00\rangle - \mid 01\rangle - \mid 10\rangle + \mid 11\rangle)(\mid 0\rangle - \mid 1\rangle)\ /\sqrt{2}
\end{aligned}$$

Por lo tanto

$$\mid \psi_{salida}\rangle = - \mid 00\rangle \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right).$$

La medida sobre los primeros dos qubits nos da el estado $\mid 00\rangle$ con probabilidad uno, confirmando que nuestra función es una función constante.

2.9.4. Transformada Cuántica de Fourier

La Transformada Discreta de Fourier (TDF) es un caso particular de la Transformada de Fourier para secuencias de longitud finita en que se evalúa el espectro[3] solamente en unas frecuencias concretas, obteniendo un espectro discreto. La TDF tiene aplicaciones en la física, la teoría de los números, la combinatoria, el procesamiento de señales (electrónica), la teoría de la probabilidad, la estadística, la óptica, la propagación de ondas y otras áreas.

La Transformada Discreta de Fourier de una función discreta $f_0, \ldots, f_{N-1}$ está dada por

$$\tilde{f}_k \equiv \frac{1}{\sqrt{N}} \sum_{j'=0}^{N-1} e^{2\pi i j' k/N} f_j.$$

La transformada inversa

$$f_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i j k/N} \tilde{f}_j.$$

Se puede verficar que substituyendo la expresión anterior en $\tilde{f}_k$ se obtiene una identidad, esto es $\tilde{f}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} f_j \equiv \tilde{f}_k$. Demostración:

$$\begin{aligned} \tilde{f}_k &\equiv \frac{1}{\sqrt{N}} \sum_{j'=0}^{N-1} e^{\frac{2\pi i}{N} j' k} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-\frac{2\pi i}{N} j j'} \tilde{f}_j \right) \\ &= \frac{1}{N} \sum_{j,j'}^{N-1} e^{\frac{2\pi i}{N} j'(k-j)} \tilde{f}_j, \end{aligned}$$

donde del resultado $\sum_{j'} e^{\frac{2\pi i}{N} j'(k-j)} = N\delta_{kj}$, se obtiene

$$\tilde{f}_k = \frac{1}{N} \left(N \sum_{j=0}^{N-1} \delta_{kj} \tilde{f}_j \right) = \tilde{f}_k,$$

que es lo que se quería demostrar.
Puede definirse la TDF cuántica como un operador lineal que actúa sobre las amplitudes

[3]Un espectro de frecuencias es el gráfico que muestra cómo es la descomposición de una señal ondulatoria (sonora, luminosa, electromagnética,...) en el dominio frecuencial.

del sistema cúantico, esto es,

$$\sum_j \alpha_j \mid j > \rightarrow \sum_k \tilde{\alpha_k} \mid k\rangle,$$

donde

$$\tilde{\alpha_k} \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} \, \alpha_j.$$

Denotando la TDF por el operador $\hat{F}$, tenemos que el estado cuántico transformado está dado por:

$$\mid \tilde{\psi}\rangle = \hat{F} \mid \psi\rangle.$$

Observamos que las amplitudes $\tilde{\alpha_j}$ son lineales en el α_j original. Por lo tanto existe un operador lineal $\hat{F}$, que implementa la transformada, y podemos escribirla

$$\hat{F} \equiv \sum_{j,k=0}^{N-1} \frac{e}{\sqrt{N}}^{2\pi ijk/N} \mid k\rangle\langle j \mid .$$

A continuación mostramos que

$$\mid \psi\rangle \rightarrow \mid \tilde{\psi}\rangle,$$

$$\begin{aligned} F \mid \psi\rangle &= \sum_{j,k=0}^{N-1} e^{2\pi ijk/N} \mid k\rangle\langle j \mid \left(\sum_{j'=0}^{N-1} \alpha_{ji}{}' \mid j' \rangle \right) \\ &= \sum_{k=0}^{N-1} \left(\sum_{j=0}^{N-1} e^{2\pi ijk/N} \, \alpha_j \right) \mid k\rangle \\ &= \sum_{k=0}^{N-1} \tilde{\alpha}_k \mid k\rangle = \mid \tilde{\psi}\rangle. \end{aligned}$$

Falta checar que $\hat{F}$ es unitaria. Tomando el hermiteano conjugado de $\hat{I}$ se tiene

$$\hat{F}^\dagger \equiv \sum_{j,k=0}^{N-1} \frac{e^{-2\pi ijk/N}}{\sqrt{N}} \mid j\rangle\langle k \mid,$$

y ahora efectuando el producto con $\hat{I}$ se tiene

$$\begin{aligned}\hat{F}^{\dagger}\hat{F} &= \frac{1}{N}\sum_{j,kj^{\prime}} e^{2\pi i(j^{\prime}-j)k/N} \mid j\rangle\langle j^{\prime} \mid, \\ &= \frac{1}{N}\sum_{j,j} \mid j\rangle\langle j^{\prime} \mid \delta_{jj^{\prime}}N, \\ &= \sum_{j} \mid j\rangle\langle j \mid = \hat{I}.\end{aligned}$$

De la misma forma puede probarse que $\hat{F}\hat{F}^{\dagger} = I$. Esta transformación es unitaria, por lo tanto, puede ser implementada por una computadora cuántica.
Se puede construir ahora el circuito cuántico de la Transformada de Fourier Cuántica, por medio de productos de estados.

Se ha encontrado que al actuar la transformada de Fourier sobre un estado de n qubits da

$$\hat{F}(\mid j\rangle) = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{\frac{2\pi i}{2^n}jk} \mid k\rangle.$$

Substituyendo en la expresión anterior $k = k_{n-1}\ldots k_0 = k_{n-1}2^{n-1} + \ldots + k_0 2^0$ donde $k_l \in \{0,1\}$ con $l = 0,1,\ldots,n-1$, se obtiene que

$$\hat{F}(\mid j\rangle) = \frac{1}{\sqrt{2^n}}\sum_{k_{n-1}=0}^{1}\cdots\sum_{k_0=0}^{1} e^{2\pi ij\sum_{l=1}^{n}\frac{k_{n-l}}{2^l}} \mid k_{n-l}\rangle.$$

Utilizando que la exponencial de una suma es el producto de las exponenciales resulta

$$\begin{aligned}\hat{F}(\mid j\rangle) &= \frac{1}{\sqrt{2^n}}\sum_{k_{n-1}=0}^{1}\cdots\sum_{k_0=0}^{1}\prod_{l=1}^{n} e^{2\pi ij\frac{k_{n-l}}{2^l}} \mid k_{n-l}\rangle \\ &= \frac{1}{\sqrt{2^n}}\prod_{l=1}^{n}\left[\sum_{k_{n-l}=0}^{1} e^{2\pi ij\frac{k_{n-l}}{2^l}} \mid k_{n-l}\rangle\right].\end{aligned}$$

donde usamos que $\sum_{k_{n-1}}\sum_{k_0}\prod_{l=1}^{n} \to \prod_{l=1}^{n}\sum_{k_{n-l=0}}^{1}$.

Finalmente se define la representación de una fracción binaria, esto es,

$$0.j_l j_{l+1}\ldots j_m = \frac{1}{2}j_l + \frac{1}{4}j_{l+1} + \cdots + \frac{1}{2^{m-l+1}}j_m.$$

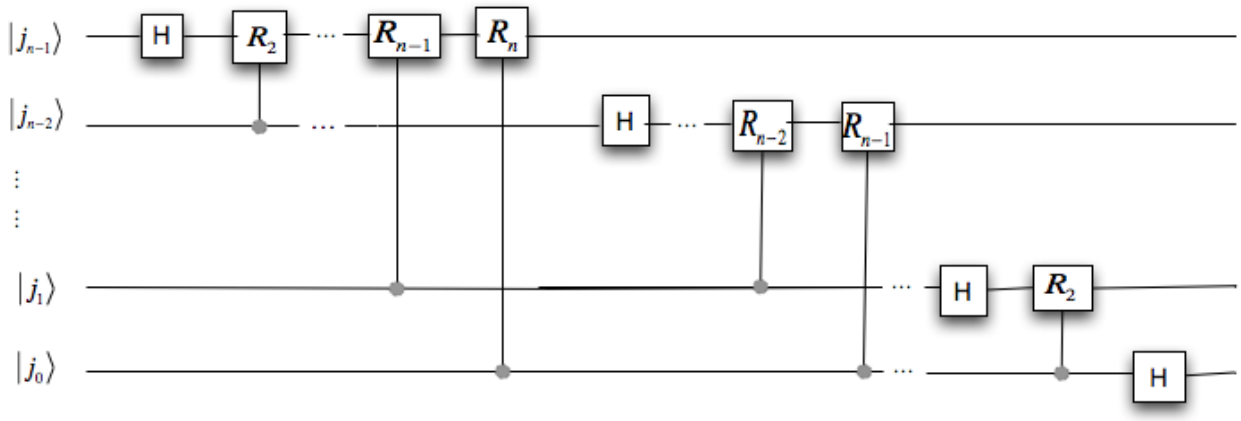


Figure 2.9.4: Circuito de la Transformada Cuántica de Fourier

obteniéndose

$$F(\mid j\rangle) = \frac{1}{\sqrt{2^n}}\left(\mid 0\rangle + e^{2\pi i 0.j_0} \mid 1\rangle\right)\left(\mid 0\rangle + e^{2\pi i 0.j_1 j_0} \mid 1\rangle\right)\cdots \cdots \left(\mid 0\rangle + e^{2\pi i 0.j_{n-1} j_{n-2}\ldots j_0} \mid 1\rangle\right). \quad (2.9.10)$$

Se puede notar que la representación que se obtuvo se encuentra factorizada, esto demuestra que el estado cuántico no está entrelazado. Esta representación permite construir un circuito cuántico para la transformada cuántica de Fourier de forma más eficiente (Ver Figura 2.9.4). En la figura el operador está definido por la expresión

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{bmatrix}.$$

Se actúa con la compuerta de Hadamard sobre el qubit más significativo, esto es,

$$H \mid j\rangle = (H \mid j_{n-1}\rangle) \mid j_{n-2} j_{n-3}\cdots j_0\rangle$$

$$Si\ j_{n-1} = 0 \text{ entonces } H \mid j_{n-1}\rangle = \frac{1}{\sqrt{2}}\left\{\mid 0\rangle + \mid 1\rangle\right\},$$

$$Si\ j_{n-1} = 1 \text{ entonces } H \mid j_{n-1}\rangle = \frac{1}{\sqrt{2}}\left\{\mid 0\rangle - \mid 1\rangle\right\}.$$

Obsevamos que los resultados anteriores pueden escribirse en una sola expresión como

$$H \mid j_{n-1}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i 0.j_{n-1}} \mid 1\rangle\right),$$

donde $0.j_{n-1} = \frac{1}{2} j_{n-1}$, de tal manera que si $j_{n-1} = 0$ vale cero, y si $j_{n-1} = 1$ vale $\frac{1}{2}$; por lo tanto $e^{2\pi i 0.j_{n-1}} = -1$.

Por lo tanto la primer compuerta de Hadamard actúa en el qubit más significativo y genera

el estado

$$\frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i 0\cdot j_{n-1}} \mid 1\rangle\right) \mid j_{n-2}\ldots j_0\rangle.$$

Las subsecuentes $n-1$ compuertas de fase de rotación, $R_2-controlada$ hasta $R_n-controlada$ agregan fases desde $\frac{\pi}{2}$ hasta $\frac{\pi}{2^{n-1}}$ si el correspondiente qubit de control es uno. Después de estas n-1 compuertas la función se encuentra en el estado

$$\frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i 0\cdot j_{n-1}j_{n-2}\ldots j_0} \mid 1\rangle\right) \mid j_{n-2}\ldots j_0\rangle.$$

De manera similar se realizan las subsecuentes $n-2$, $n-1$, ..., 1 rotaciones controladas con su correspondiente transformación de Hadamard para el resto de los qubits obteniendo así el estado de salida

$$\frac{1}{\sqrt{2}}\left(\mid 0\rangle + e^{2\pi i 0\cdot j_{n-1}j_{n-2}\ldots j_0} \mid 1\rangle\right)\left(\mid 0\rangle + e^{2\pi i 0\cdot j_{n-2}\ldots j_0} \mid 1\rangle\right)\cdots \\ \cdots\left(\mid 0\rangle + e^{2\pi i 0\cdot j_0} \mid 1\rangle\right)$$

Comparando el resultado con (2.9.10), lo único que queda por realizar son n SWAPS al estado de salida para obtener el orden correcto del estado transformado.

Estados periódicos

Suponiendo que estamos en N dimensiones y tenemos un estado de la forma

$$\mid \Theta\rangle = \sum_{n=0}^{N/r-1} c \mid a_0 + nr\rangle,$$

donde $c = \sqrt{r/N}$. Este es un estado periódico con periodo r y un elemento compensatorio a_0 .
Aplicando la TDF cuántica al estado $\mid \Theta\rangle$ se obtiene

$$\begin{aligned} \mid \tilde{\Theta}\rangle &= \hat{F} \mid \hat{\Theta}\rangle \\ &= \sum_{n=0}^{N/r-1} c \sum_{k=0}^{N-1} \frac{1}{\sqrt{n}} e^{2\pi i \frac{(a_0+nr)}{N}} \mid k\rangle, \end{aligned}$$

donde utilizamos $\langle j \mid a_0 + nr\rangle = \delta_{j,a_0+nr}$. Intercambiando las sumas tenemos

$$\mid \tilde{\Theta}\rangle = \frac{c}{\sqrt{n}} \sum_{k=0}^{N-1} e^{2\pi i \frac{a_o k}{N}} \left(\sum_{n=0}^{N/r-1} e^{2\pi i \frac{nrk}{N}} \right) \mid k\rangle.$$

La suma entre los paréntesis redondos puede simplificarse utilizando la progresión geométrica

$$\sum_{n=0}^{N/r-1} a^n = \begin{cases} N/r & \text{si } a = 1, \\ \frac{1-a^{N/r}}{1-a} & \text{si } a \neq 1, \end{cases}$$

con $a = \exp\left\{\frac{2\pi i\, kr}{N}\right\}$. Como $a^{N/r} = \exp\{2\pi ik\} = 1$ entonces se concluye que para tener un resultado diferente de cero debe de ocurrir que $a = 1$ y entonces k es un múltiplo entero de N/r. Sea por lo tanto $k = m\frac{N}{r}$ y tenemos finalmente

$$\mid \tilde{\Theta}\rangle = \sum_{m=0}^{r-1} \alpha_m \mid m\frac{N}{r}\rangle,$$

donde $\alpha_m = c\frac{N}{r}\frac{1}{\sqrt{N}} exp^{2\pi i a_0 m/r} = \frac{exp^{2\pi i a_0 m/r}}{\sqrt{r}}$ y $\mid \alpha_m \mid = \sqrt{1/r}$ para toda m.

Este estado también es periódico y nuestro elemento compensatorio es ahora cero. Podemos explotar este hecho para encontrar el periodo del estado. Si medimos en este momento nuestro registro obtendremos un valor mN/r para alguna m entre 0 y r-1. Esto por si solo no nos dice mucho de quien es N/r y por lo tanto r. Pero si corremos nuestro algortimo d veces obtendremos una secuencia de enteros $m_1 N/r, \ldots, m_d N/r$ que son todos múltiplos de N/r . Con un número de iteraciones d que crece moderadamente sobre N, podemos decir con alta probabilidad que N/r es el único factor común de todos los números obteniendo así r.

2.9.5. Algoritmo de Factorización de Shor

En 1994 Peter Shor publicó el artículo "Algorithms for quantum computation, discrete logarithms and factorig" en donde mostró un nuevo enfoque al algoritmo de factorización, combinando principios de la mecánica cuántica con la teoría de números. Este algoritmo ha creado gran interés en computación cuántica debido a que los sistemas criptográficos basan su seguridad en la dificultad de factorizar números muy grandes.

El problema consiste en escribir un número entero positivo impar-no primo como un producto de números primos, N = fac1 $\cdot$ fac2 .
(Ej. 154,729 = 359 x 431).

Por el Teorema Fundamental de la Aritmética sabemos que todo entero positivo puede representarse de forma única como producto de factores primos.
No es complicado resolver este problema para factores primos pequeños, pero si nos encontramos con números enteros más grandes no existe clásicamente un algoritmo que pueda de manera rápida factorizar dicho número. El mejor algoritmo clásico de factorización (Criba Numérica de Campo) requiere $exp(O(n^{1/3}(log\, n)^{2/3}))$ de operaciones donde n es el tamaño de entrada.

Algortimo Clásico de Factorización

Dado un número N impar - no primo, que sea producto de dos primos, describiremos el algoritmo de la siguiente manera:

1. Seleccionar un número $y < N$, tal que y sea coprimo de N, i.e., $mcd(y, N) = 1$.
2. Calcular el orden r de $y\ mod\, N$. El orden se define como el periódo de repetición de la congruencia $y^r \equiv 1\ mod\ N$.

3. Si r es par y $y^{r/2} \not\equiv -1 \, mod \, N$, entonces $x = y^{r/2}$, caso contrario volver a (1).

4. Calcular los dos factores primos: fac1 = $mcd(x+1,\, N)$, fac2 = $mcd(x-1,\, N)$.

Ejemplo: Sea N = 55.
Notemos que N es impar y no primo.

1. Los valores de y coprimos a N son: $\{1, 2, 3, 4, 6, 7, 8, 9, 12, 13, \ldots, 54\}$ y tomamos uno al azar, sea este número el 9.

2. Debemos de hallar el orden r de $9 \, mod \, 55$,

   Por Teoría de Números sabemos que : "Suponiendo que el $mcd(y,\, N) = 1$, entonces el orden r de $y mod N$ es la menor potencia de y congruente a $1 mod N$, i.e., $y^r \equiv 1 mod \, N$."
   Como $y = 9$ sus potencias son: $\{9, 81, 729, 6561, \ldots, 3486784401, \ldots, \}$
   Sus valores de congruencia están dadas por
   $y^i \ mod \ 55\,;\, i = 1, 2, 3, \ldots$: $\{9, 26, 14, 16, 34, 31, 4, 36, 49, 1, 9, 26, \ldots\}$, podemos notar que el orden es r =10.

3. Dado que r es par y $9^{10/2}$ no es congrente con $-1 \ mod \, 55$, $x = 9^{10/2} = 59094$.

   $$x \quad = \quad 59049$$

4. $$fac1 \quad = \quad mcd(59050,\, 55) = 5,$$

   $$fac2 \quad = \quad mcd(59048,\, 55) = 11.$$

   De donde obtenemos que 5 y 11 son los dos factores primos de 55.

Algoritmo Cúantico de Shor

Shor usa elementos del algoritmo clásico (teoría de números) para resolver el problema de factorización de manera cuántica. Halla el orden r de $y \ mod \ N$ en tiempo polinomial, descomponiendo en factores un número N en tiempo O($(log \, N)^3$).

Hacemos uso de 2 registros, uno de L qubits que permitirá determinar el orden r de $y \ mod \ N$ y otro de L´ qubits de longitud que servirá como auxiliar:

$$\psi = \mid L\rangle \mid L'\rangle.$$

1. Determinar L y L´.

   Elegimos q= 2^L tal que $N^2 \leq q < 2N^2$. L´ la obtenemos para garantizar que forman un número de longitud de N-1 en forma binaria.

2. Una vez obtenidos L y L´pondremos nuestra máquina en una superposición de estados cuánticos.

Entonces preparamos nuestros registros L y L´en el estado $\mid 0\rangle$ y le aplicamos la transformada discreta de Fourier al primer registro, obteniendo

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \mid a\rangle \mid 0\rangle, \tag{2.9.11}$$

donde a representa los números binarios de 0 a $q-1$, es decir, de 0 a 2^L-1. La acción de la transformada discreta de Fourier y la transformación de Hadamard son iguales al actuar sobre un estado $\mid 0\rangle$ de q qubits.

3. Calcular la función $y^a \ mod \ N$ para cada valor de a entre 0 y $q-1$. Almacenamos el resultado en el segundo registro.

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \mid a\rangle \mid y^a \ mod \ N\rangle. \tag{2.9.12}$$

Cabe destacar que este mismo paso lo realizamos en el algoritmo clásico pero de manera secuencial, el algortimo de Shor aprovecha las propiedades del cómputo cuántico para realizar los cálculos en una misma iteración.
Los valores obtenidos en el segundo registro son los mismos que obtuvimos en el paso 2 del algoritmo clásico. Ahora, sabemos que por los principios de la mecánica cuántica si realizamos en este momento una observación del estado, el estado colapsará en un nuevo estado donde la información del orden r se encontrará dentro de él.

4. Se realiza una medición en la base computacional para determinar los valores de los bits en el segundo registro, suponiendo que el resultado es $k = y^{a_0} mod \ N$ para algún valor mínimo a a_0. Si r es el orden de $y \ mod \ N$, entonces $y^{a_0} \equiv y^{dr+a_0} \ mod \ N$ para todas las d. Entonces una medición selecciona n valores de $a = a_0, \ a_0 + r, \ a_0 + 2r, \ldots, \ a_0 + (A\, r)$ donde A es el entero más grande menor que $\frac{q-a_0}{r}$ y $a_0 \leq r$. Notemos que $A \approx \frac{q}{r}$.

Por lo tanto el nuevo estado colapsado está dado por [31]

$$\mid \psi\rangle = \frac{1}{\sqrt{A+1}} \sum_{d=0}^{A} \mid a_0 + dr, \ k\rangle. \tag{2.9.13}$$

Sea M = A + 1:

$$\mid \Phi\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} \mid a_0 + dr, \ k\rangle. \tag{2.9.14}$$

5. Aplicaremos la TDF al estado (2.9.14) para determinar, en general, el orden r:

$$\text{TDF} : \mid \Phi\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} e^{2\pi i (a_0+dr)c/q} \mid c, k\rangle$$

$$\mid \Phi\rangle = \sum_{c=0}^{q-1} e^{2\pi i a_0 \frac{c}{q}} \tilde{f}(c) \mid c, k\rangle,$$

donde

$$\tilde{f}(c) = \frac{1}{\sqrt{qM}} \sum_{d=0}^{M-1} \exp\left\{2\pi i d\left(rc/q\right)\right\}.$$

De acuerdo al resultado anterior para una función períodica, su TDF cuántica será diferente de cero si c es un múltiplo de q/r. En este caso es aproximadamente periódica, y entonces $M \approx q/r$.

6. El nuevo estado obtenido estará gobernado por una distribución de probabilidades, la cual está dada por [31]

$$P(c) = \frac{1}{qM} \left| \sum_{d=0}^{M-1} e^{(2\pi i d(rc \bmod q))/q} \right|^2,$$

donde P(c) es la probabilidad de obtener cualquier valor de c entre 0 y $q-1$.
Como existen ciertos valores de c que tienen mayor probabilidad de ser observados, estos son los cercanos a los múltiplos de $\frac{q}{r}$ y cumplen con la relación [32]

$$-\frac{r}{2} \leq rc \, mod \, q \leq \frac{r}{2}. \tag{2.9.15}$$

Existen precisamente r valores de $c \; mod \; q$ que satisfacen la ecuación y la probabilidad de ver un estado c será de al menos $\frac{1}{3}\, r^2$ [32].

7. Una vez obtenidos los valores de c, se escoge uno aleatoriamente, sea d su valor que debe satisfacer la relación:

$$-\frac{1}{2q} \leq \frac{c}{q} - \frac{d}{r} \leq \frac{1}{2q},$$

para algún valor entre $0 \leq d \leq r-1$.
La fracción $\frac{d}{r}$ puede ser hallada mediante la expansión de fracciones continuas de $\frac{c}{q}$, donde uno de los convergentes del desarrollo nos dará $\frac{d}{r}$. Los convergentes son las aproximaciones racionales generadas por la expansión de fracciones continuas.
Obteniendo así el orden r el cual nos permitirá obtener los dos factores primos de N.

Ejemplo del algoritmo Cuántico de Shor

Consideremos N= 55 y $y = 9$.
Para obtener L, tomemos $q = 2^{12} = 4096$ donde $55^2 \leq q < 2 \cdot 55^2$. Dado que $q = 2^{12}$, L = 12 . El valor de L´debe ser capaz de almacenar de 0 a 54 en binario, entonces como 54 =

110110, L´ = 6.[4]
Consideremos un registro con 2 qubits en el estado $\mid 0^2\rangle$. Recordando la acción de la transformada de Hadamard.

$$H \mid 0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(\mid 0\rangle + \mid 1\rangle\right).$$

Entonces si aplicamos Hadamard a los dos qubits obtenemos

$$H \mid 0^2\rangle = \frac{1}{\sqrt{2^2}} \sum_{a=0}^{2^2-1} \mid a\rangle,$$

donde 00 es el binario de 0, 01 el binario de 1, 10 de 2 y 11 de 3 (para el ejemplo usaremos numeros enteros).
De la misma manera, si aplicamos H a los 12 qubits del primer registro del ejemplo 1:

$$\psi = \mid 000000000000\rangle \mid 000000\rangle,$$

donde L = 12 qubits y L´= 6 qubits. Obtenemos entonces la superposicón deseada con $2^{12} - 1$ términos, esto es

$$\frac{1}{\sqrt{2^{12}}}\left(\mid 0,0\rangle + \mid 1,0\rangle + \mid 2,0\rangle + \ldots + \mid 4095,0\rangle\right)$$

$$= \frac{1}{\sqrt{2^{12}}} \sum_{a=0}^{2^{12}-1} \mid a\rangle \mid 0\rangle \equiv \mid \chi\rangle.$$

Ahora calculamos la función $9^a \ mod\ 55$ para cada valor de a desde 0 hasta ,

$$\mid \chi\rangle = \frac{1}{\sqrt{2^{12}}}\left(\mid 0,\ 9^0 mod\, 55\rangle + \mid 1,\ 9^1 mod\, 55\rangle + \ldots + \mid 4095,\ 9^{4095} mod\, 55\rangle\right),$$

que al evaluar las expresiones del segundo registro toma la forma

$$\mid \chi\rangle = \frac{1}{\sqrt{4096}}\left(\mid 0,1\rangle + \mid 1,9\rangle + \mid 2,26\rangle + \ldots + \mid 4,16\rangle + \ldots + \mid 10,1\rangle + \ldots + \mid 4095,34\rangle\right).$$

Suponiendo que al efectuar una medición se obtiene $k = 16$, que implica un valor de $a_0 = 4$. Entonces el estado después de la medición está determinado por la expresión $\mid \psi\rangle$ con M = 410,

$$\begin{aligned} \mid \Phi\rangle &= \frac{1}{\sqrt{410}}\left(\mid 4,16\rangle + \mid 14,16\rangle + \mid 24,16\rangle + \ldots + \mid 104,16\rangle + \ldots \mid 4094,16\rangle\right) \\ &= \frac{1}{\sqrt{410}} \sum_{d=0}^{410-1} \mid 4 + d \cdot 10,\ 16\rangle. \end{aligned}$$

Para verificar que $r = 10$ y $M = 410$, hay que demostrar que $y^{a_0} \equiv y^{a_0 + d \cdot r}\ mod\ N$. i.e

[4]Para fines prácticos obtenemos L de la relación: L = $\frac{ln(2N^2)}{ln2}$, considerando el rango al que pertenece q.

verificar que para un r dado se cumple
$mod(y^{a_0},\ N) = mod(y^{a_0+d\cdot r},\ N)$ para todo d entre $0\ y\ M-1$.
En nuestro caso tenemos

$$mod(9^4, 55) = 16.$$

Entonces debemos comprobar que para un r dado se cumple: $mod(9^4, 55) = mod(9^{4+d\cdot r}, 55)$.
En la tabla se observa la igualdad para todo valor de d. Por lo que el valor de r es 10.

$mod(9^(4 + (d \cdot r)), 55)$	d=1	d=2	d=3	d=4	d=5	$\cdots$	d=409
r=1	34	31	4	36	49	-	14
r=2	31	36	1	26	16	-	25
$\cdots$	-	-	-	-	-	-	-
r=8	26	1	36	31	16	-	31
r=9	14	26	9	1	49	-	34
r=10	16	16	16	16	16	-	16
r=11	34	31	4	36	49	-	14
$\cdots$	-	-	-	-	-	-	-

Entonces, puede calcularse inmediatamente el valor de M, esto es,

$$M = \frac{q}{r} = \frac{4096}{10} \approx 410.$$

Consideremos la aplicación de la TDF al estado obtenido:

$$\mid \Phi\rangle = \frac{1}{\sqrt{410}} \sum_{d=0}^{410-1} \mid 4 + d\cdot 10,\ 16\rangle,$$

de tal manera que

$$\text{TDF} \mid \Phi\rangle\ = \sum_{c=0}^{4095} \frac{e^{2\pi i(4)c/4096}}{\sqrt{4096\cdot 410}} (\sum_{d=0}^{409} \zeta^d) \mid c, 1\rangle,$$

con $\varsigma = e^{2\pi i(10)c/4096}$.

A continuación se calcula la distribución de probabilidades para el caso $N = 55$ con $q = 4096$ y $r = 10$, y los valores de c siguientes:
$\{0, 410, 819, 1229, 1638, 2048, 2458, 2867, 3277, 3686\}$, obteniéndose
$P(c) = \{.100, .057, .087, .087, .057, .100, .057, .087, .087, .057\}$, respectivamente.

Podemos checar la desigualdad (2.9.15) para c=2458:

$$-\frac{10}{2} \leq 10 \cdot 2458\ mod\ 4096 \leq \frac{10}{2}$$

$$-5 \leq 4 \leq 5$$

Entonces para $c = 2458$, hallaremos $\frac{d}{r}$ mediante la expansión la fracción continua siguiente

$$\frac{c}{q} = \frac{2458}{4096} = \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{409}}}}$$

cuyos convergentes son

$$\frac{1}{1} = 1$$

$$\frac{1}{1+\frac{1}{1}} = \frac{1}{2}$$

$$\frac{1}{1+\frac{1}{1+\frac{1}{1}}} = \frac{2}{3}$$

$$\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}} = \frac{3}{5}$$

$$\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{409}}}} = \frac{1229}{2048}$$

De aqui obtenemos que $\frac{d}{r} = \frac{6}{10} = \frac{3}{5}$, ya que el denominador no excede a 55 (N=55).

El orden r de mod N es un múltiplo de r =5.
La siguiente tabla muestra la función $y^a \equiv 1$,

a	$y^a mod\, N \;= 9^a mod\, 55$
5	34
10	1
15	34

donde a es un múltiplo de 55. Obteniendo así el orden $r = 10$. Una vez obtenido el período se continuán los pasos del algoritmo clásico de factorización para obtener los dos factores primos de 55, esto es

$$x = y^{\frac{r}{2}} = 9^{\frac{10}{2}} = 59094,$$

$$\text{fac1} = mcd(59050, 55) = 5,$$
$$\text{fac2} = mcd(59048, 55) = 11.$$

2.9.6. Algoritmo de Grover

Un algoritmo de búsqueda es aquel que está diseñado para encontrar un elemento x en un conjunto posible de soluciones (estructura de datos) tal que $P(x)$ sea verdadero. Una gran clase de problemas dentro de las Ciencias de la Computación implican un proceso de búsqueda.

Como ejemplo podríamos ver la búsqueda de un elemento en una base de datos, el ordenamiento de una lista o el coloreado de una gráfica. El coloreado de una grafica puede ser vista como una busqueda para encontrar y asignar el color correcto a los vertices de la gráfica tal que el enunciado "todos los vértices adyacentes tienen diferentes colores" sea verdadero. El problema de coloreado es uno de los probemas más conocidos de la teoría de gráficas, el problema consiste en asignar colores diferentes a los vértices de una gráfica de modo que ningún par de vértices adyacentes tengan el mismo color (Figura 2.9.5).

Un problema de búsqueda sobre una base de datos estructurada es aquella donde la información de nuestro espacio de busqueda y nuestro enunciado P puede ser explotado para construir un algoritmo eficiente. Realizar una búsqueda sobre una lista ordenada alfabeticamente puede ser explotada para encontrar una solución eficiente.
Un problema de búsqueda sobre una base de datos no estrucuturada es aquella donde no "sabemos" nada acerca de la estructura del espacio de soluciones y de nuestro enunciado P. De manera general en un problena de búsqueda no estructurada, probando aleatoriemente la veracidad de $P(x_i)$ elemento por elemento es lo mejor que podemos hacer clásicamente. Para un problema de busqueda sobre un espacio no estructurado de tamaño N requiere $O(N)$ evaluaciones de P. En una computadora cuántica Grover demostró que este mismo problema puede ser resuelto con una probabilidad acotada en $O(\sqrt{N})$. Cabe destacar que el algoritmo de Grover hace la búsqueda *más eficiente* que un algoritmo clásico, no la hace más sencilla.

El algoritmo de Grover busca en una lista no estructurada de tamaño N alguna x tal que $P(x)$ sea verdadero. Sea n tal que $2^n \geq N$ y sea U_p la compuerta cuántica que implementa la función clásica $P(x)$ que prueba la veracidad del enunciado, donde denotaremos que el enunciado es verdadero con un 1. Recordemos que $P(x)$ es una función binaria de $\{0,1\}^n \rightarrow \{0,1\}$ tal que $P(x) = 1$ si $x = x_0$ y $P(x) = 0$ de otra manera.

$$U_p : \mid x,\ 0\rangle \longrightarrow \mid x,\ P(x)\rangle.$$

El primer paso es calcular P para todas las posibles entradas x_i, aplicando U_p a un registro

que contiene la superposición $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} \mid x\rangle$ de todas las 2^n posibles entradas x junto con un registro $P(x)$ iniciado en 0 , obteniendo el registro

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} \mid x\rangle \mid P(x)\rangle. \tag{2.9.16}$$

Es difícil obtener un resultado útil a partir de esta superposición.
Para cualquier x_0 tal que $P(x_0)$ es verdadero, $\mid x_0, 1\rangle$ formará parte de la superposición descrita en (2.9.16). Como la amplitud de dicho estado es $\frac{1}{\sqrt{2^n}}$, la probabilidad de que una medición aleatoria produzca x_0 es solo 2^{-n}. El truco reside en lograr incrementar las amplitudes de los vectores $\mid x_0, 1\rangle$ para los cuales P es verdadero y disminuir las amplitudes de los vectores $\mid x_0, 0\rangle$ donde P sea falso en la ecuación (2.9.16).
Una vez que dicha transformación fue realizada sobre el estado cuántico, solo se requiere medir el utlimo qubit del estado cuántico que representa $P(x)$. Debido al cambio de amplitudes que se realizó, existe una alta probabiidad de que el resultado sea 1. En este caso la medición proyecta el estado (2.9.16) sobre el subespacio $\frac{1}{\sqrt{2^k}} \sum_{i=1}^{k} \mid x_i, 1\rangle$ donde k es el número de soluciones. Si la medición da 0 entonces el proceso debe iniciarse de nuevo y la superposición de la ecuación (2.9.16) deberá calcularse nuevamente.

Descripción del Algoritmo de Grover

1. Preparar la función de onda de la computadora en el estado $\mid 00\ldots0\rangle \mid 1\rangle$ donde utilizamos un qubit auxiliar
2. Preparar un registro que contenga una superposicón de todos los posibles valores $x_i \in [0, \ldots, 2^n - 1]$ y el estado $\frac{1}{\sqrt{2}} \{\mid 0\rangle - \mid 1\rangle\}$ del qubit auxiliar. Esto se realiza mediante la acción de $n + 1$ compuertas de Hadamard.
3. Calcular $P(x_i)$ sobre el registro.
4. Cambiar las amplitudes α_j a $-\alpha_j$ para x_j tal que $P(x_j) = 1$ (ver subsección sobre cambio de Signo).
5. Aplicar inversión sobre el promedio (ver Inversión sobre el promedio) para incrementar las amplitudes de x_j con $P(x_j) = 1$. Las amplitudes resultantes donde $P(x_i) = 0$ han disminuido en forma considerable.
6. Repetir $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$ veces los pasos del 2 al 4.
7. Leer el resultado.

Cambio de signo
El objetivo es implementar la transformación:

$$U \mid x\rangle = (-1)^{f(x)} \mid x\rangle$$

que no modifica los $\mid x\rangle$ si ocurre que $f(x) = 0$ y le agrega un coeficiente -1 en los que verifica que $f(x) = 1$.

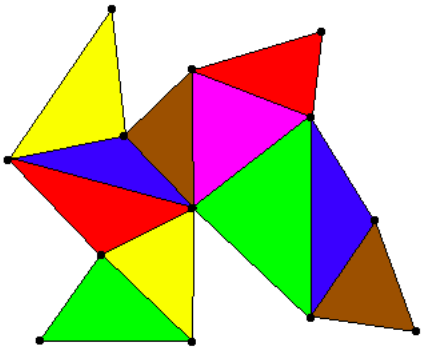


Figure 2.9.5: Problema de coloreado de gráficas.

La transformación U_f (2.9.7) implementa la evaluación de la función booleana f. Cuando sólo queremos evaluar f sobre un estado $\mid x\rangle$ se aplica U_f con $b = 0$, en este caso se escoge $\mid b\rangle = \frac{1}{\sqrt{2}}(\mid 0\rangle - \mid 1\rangle)$. Nótese que si $f(x) = 0$, entonces $\mid b \oplus f(x)\rangle = b$, mientras que si $f(x) = 1$ es $\mid b \oplus f(x)\rangle = \frac{1}{\sqrt{2}}(\mid 1\rangle - \mid 0\rangle) = - \mid b\rangle$. Luego

$$U_f(\mid x, b\rangle) = (-1)^{f(x)} \mid x, b\rangle.$$

Con esta transformación realizamos la evaluación de f y el cambio de signo de las amplitudes $\mid x_j\rangle$ que satisfacen la propiedad.
Al aplicar U_f sobre un estado cualquiera $\mid \phi\rangle = \sum_{j=0}^{N-1} a_j \mid x_j\rangle$.

Sea $X_0 = \{x \mid f(x) = 0\}$ y $X_1 = \{x \mid f(x) = 1\}$

$$U_f(\mid \phi, b\rangle) = U_f\left(\sum_{x_j \in X_0} a_j \mid x_j, b\rangle + \sum_{x_j \in X_1} a_j \mid x_j, b\rangle\right)$$

$$= \sum_{x_j \in X_0} a_j \mid x_j, b\rangle - \sum_{x_j \in X_1} a_j \mid x_j, b\rangle$$

$$= \left(\sum_{x_j \in X_0} a_j \mid x_j\rangle - \sum_{x_j \in X_1} a_j \mid x_j\rangle\right) \otimes \mid b\rangle.$$

Inversión sobre el promedio

Para realizar la operación de inversión sobre el promedio en una computadora cuántica tiene que usarse una transformación unitaria. Se puede observar que la transformación

$$\sum_{i=0}^{N-1} a_i \mid x_i\rangle \rightarrow \sum_{i=0}^{N-1} (2A - a_i) \mid x_i\rangle,$$

donde A denota el promedio de las a_i, es realizada por la matriz de N x N, de la forma $D_{ij} = -\delta_{ij} + \frac{2}{N}$, esto es

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix}.$$

Como $DD^* = I$, D es unitaria y entonces puede ser implementada por una computadora cuántica.[5]

Ejemplo Algortimo de Grover

Consideremos la búsqueda de una cosa de 4 objetos que pueden ser representados por dos qubits. Inicialmente los dos qubits se preparan en el estado $\mid 00\rangle$ y el qubit auxiliar se encuentra en el estado $\mid y\rangle = \mid 1\rangle$. Cada uno de ellos sufre una transformación de Hadarmard obteniéndose

$$\begin{aligned} \mid \psi\rangle = H^3 \mid 001\rangle &= \frac{1}{\sqrt{2^2}} \sum_{x=0}^{2^2-1} \mid x\rangle \frac{1}{\sqrt{2}} (\mid 0\rangle - \mid 1\rangle) \\ &= \{\mid 000\rangle + \mid 010\rangle + \mid 100\rangle + \mid 110\rangle \\ &\quad - \mid 001\rangle - \mid 011\rangle - \mid 101\rangle - \mid 111\rangle\}, \end{aligned}$$

donde en el primer renglón usamos la base computacional.
Ahora se evalúa la función f(x), las preguntas o pregunta se hacen por medio de un operador unitario que para hacer el proceso reversible utiliza un qubit auxiliar y produce el resultado

$$\mid x\rangle \mid y\rangle \underrightarrow{O} \mid x\rangle \mid y \oplus f(x)\rangle$$

Como $\mid y\rangle = \frac{1}{\sqrt{2}} (\mid 0\rangle - \mid 1\rangle)$ por discusiones anteriores se tiene que

$$\mid y \oplus f(x)\rangle = \begin{cases} + \mid y\rangle & f(x) = 0 \\ - \mid y\rangle & f(x) = 1 \end{cases}$$

Sea f(10) = 1 y $f(x) = 0$ para $x = 00$, 01, y 11, entonces después de la indagación el estado queda

$$\frac{1}{2} \{\mid 00\rangle + \mid 01\rangle - \mid 10\rangle + \mid 11\rangle\} \frac{1}{\sqrt{2}} \{\mid 0\rangle - \mid 1\rangle\}$$

que difiere del anterior en el signo del coeficiente del estado favorable. Como el registro auxiliar no ha cambiado ya no se considera. El paso siguiente es transformar la diferencia

[5]Grover propuso una implementación eficiente de esta transformación con $O(log(N))$ puertas elementales $D = H\,\sigma_x^2\,(I \otimes H)\,CNOT\,(I \otimes H)\,\sigma_x^2$ donde $(I \otimes H)\,CNOT\,(I \otimes H)\,\sigma_x^2 = CPHASE\,(\pi)$. Grover,L (1996) "A fast quantum mechanical algortihm for database search".

de fase que aparece en $\mid 10 >$ en una diferencia de amplitud. Esto se logra mediante la tansformación unitaria D con $N = 2$ que toma la forma

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

de tal manera que

$$\frac{1}{2}\, D \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Por lo tanto una medición estándar de los dos qubits da el resultado $\mid 10\rangle$ con certeza. Concluyéndose que el problema ha sido resuelto con una sola indagación de la función f, mientras que la computadora clásica requiere en promedio $N_I = \frac{1}{4} * 1 + \frac{1}{4} * 2 + \frac{1}{2} * 3 = 2.25$ indagaciones. Para una búsqueda de un objeto entre 8 posibles en la primera iteración se tiene una probabilidad de $\frac{25}{32}$ de obtener el item buscado. Para aumentar éste se tiene que repetir el procedimiento indicado del algoritmo de Grover.

2.10. Máquina Universal de Turing Cuántica

La teoría de la computación ha tenido un gran avance durante los últimos años, ha ayudado a estudiar, definir y entender el cómputo de mejor manera. Nos ayuda a comprender la importancia de la teoría matemática en el cómputo, a definir lo computable y lo no computable (i.e posibilidades y limitaciones del cómputo) y a realizar una clasificación de los problemas computacionales, de manera más general la Teoría de la Computación son los cimientos de las ciencias de la computación. En 1985 Deutsch [26] definió una computadora como cualquier sistema físico cuya evolución dinámica lo lleva de uno de un conjunto de estados de entrada a uno de un conjunto de estados de salida. Los estados están etiquetados en alguna forma canónica, la máquina es preparada en un estado con una etiqueta inicial dada y después, seguida por unos movimientos (cada movimiento es un paso en el programa), el estado de salida es medido. Para un sistema clásico determinístico la medición de la etiqueta de salida es una función definida f de la etiqueta de entrada; además el valor de esa etiqueta de salida en principio puede ser medida por un observador externo (el usuario) y entonces se puede decir que la máquina calcula la función f.

En este sentido dos computadoras son computacionalmente equivalentes, sobre etiquetas dadas, si en cualquier posible experimento o secuencia de experimentos en donde sus etiquetas fueron preparadas equivalentemente sobre sus etiquetas de entradas y los observables correspondientes a cada una de las etiquetas de entrada fueron medidos, los valores de medición de estos observables para estas dos máquinas serán estadísticamente indistinguibles. Es decir las funciones de distribución de probabilidad para las salidas de las dos máquinas serán idénticas.

En 1936 Alan Turing describió un modelo abstracto de una máquina conocida como máquina de Turing que sigue un conjunto finito de reglas bien definidas que actúan sobre cadenas finitas de entrada y las convierte en cadenas finitas de salida. La máquina de Turing es un dispositivo que corre sobre una cinta infinita bidireccional dividida en celdas discretas donde en cada celda está contenido el simbolo 0,1 o blanco. Además de un conjunto finito de posibles estados internos y un cabezal que puede leer los contenidos de las celdas de las cintas que están inmediatamente sobre ella. El cabezal en cada paso puede escribir un símbolo sobre la celda en la que se encuentre. Existen dos estados internos especiales: un estado inicial q_0 y un estado de detención q_H. Una Máquina de Turing (MT) contiene una lista de reglas de transición describiendo su operación, existe a lo más una regla de transición para cada probable contenido de la celda y el estado interno. Si el estado interno es q_i y el cabezal se encuentra sobre la celda con contenido S_j entonces la máquina busca la regla de transición (q_i, S_j). Si ninguna regla es encontrada la máquina entra a un estado de detención inmediatamente. Un cómputo consiste en inicializar la MT con el cabezal sobre la primer celda no vacía del lado izquierdo de la cinta y la máquina en el estado interno q_0. Posteriormente las reglas de transición son simplemente aplicadas hasta que la máquina llega al estado de detención q_H, en este momento el contenido de la celda será la salida del cómputo.

Una máquina[6] M cómputa a lo más una función. No debe de haber una diferencia fundamental entre alterar el estado de entrada en la que M es preparada y alterar sistematicamente la constitución de M para que se convierta en una máquina diferente $M´$, que compute una función diferente. Para realizar estas operaciones es necesario considerar una computadora con dos entradas y la preparación de un programa que detemine cual de las funciónes será computada. A cada máquina M le corresponde un conjunto $C(M)$ de M funciones computables. Una función f es $M - computable$ si M puede computar f con un programa preparado. Dadas dos máquinas M y $M´$es posible construir una nueva máquina cuyo conjunto de funciones computables contenga la unión de $C(M)$ y $C(M´)$ y así consecutivamente. Una computadora es un autómata gobernado por un programa, tal que diferentes programas harán trabajar a la computadora de manera distinta.

En 1936 Church y Turing estabecen que *"toda función que es intuitivamente computable puede ser computada por la máquina universal de Turing*". Esta tesis nos indica que todas las máquinas de cómputo finitas pueden ser simuladas por una sola máquina llamada Máquina Universal de Turing.

Definimos $C(T)$ como el conjunto de las funciones recursivas que es menor al total de las funciones que van de $\mathbb{Z}$ a $\mathbb{Z}$ donde T es la máquina universal de Turing. Las entradas de estas funciones pueden ser números naturales, números binarios, hexadecimales o cadenas de algún lenguaje formal . Para las funciones que van de $\mathbb{Z}$ a $\mathbb{Z}$ el conjunto $C(M)$ siempre está contenido en $C(T)$. Esto quiere decir que existen problemas que las computadoras clásicas pueden no resolver (problemas no decidibles) y otros tantos que son difícil de resolver, es decir que el tiempo requerido para encontrar su solución es demasiado grande (problemas intratables). Un ejemplo de un problema no decidible es el probema de detención. Dado

[6]El modelo matemático para una máquina de estado finita es conocido como autómata. El modelo más sencillo de un autómata puede considerarse como la computadora más simple.

la descripción de un programa y una entrada finita, el problema consiste en decidir si el programa llega a un estado de detención o nunca se detiene. Un problema intratable es el problema de factorización de números primos (Sec. 2.7.5).

La tesis de Church Turing acota el espacio de funciones computables mediante la descripción de un subconjunto de las matemáticas que puede ser calculado . Si no existe algoritmo que solucione el problema la función no será computable, permitiendo como ya se mencionó que existan sistemas físicos finitos que no puedan ser simulados por una máquina de Turing.

Deutsch reinterpreta esta tesis de Church-Turing. Define una *función naturalmente computable* como las funciones que en principio pueden ser computadas por algún sistema físico real en un número finito de pasos. Introduce el concepto de simulación perfecta. Una máquina o computadora M es capaz de simular pefectamente un sistema físico S sobre un etiquetado dado en sus entradas y en su salida si existe un programa $\pi(s)$ para M que exprese a un programa M computacionalmente equivalente a S sobre estas etiquetas. En otras palabras $\pi(s)$ convierte a M en una caja negra funcional e indistinguible de S. La versión física del principio de Church-Turing descrito por Deutsch dice que *todo sistema físico realizable puede ser simulado perfectamente por un modelo universal de máquina operando por medios finitos* [26]. *Todo sistema fisico realizable* se refiere a cualquier objeto físico donde la experimentación sea posible.

Esta definición de Deutsch es más fuerte que la tesis de Chusrch-Turing. Dada la continuidad de la dinámica clásica, los posibles estados de un sistema clásico necesariamente forman un continuo. Por otro lado sólo hay una cantidad contable de maneras de preparar una entrada finita en T. Entonces T no puede simular perfectamente un sistema dinámico, T puede simular un sistema continuo únicamente mediante aproximaciones discretas sucesivas. La Teoría Cuántica si es compatible con la reinterpretación de Deutsch de la tesis de Church-Turing [26].

Deutsch afirma que no existe razón alguna para pensar que las leyes de la física deben respetar las limitaciones de la hipótesis de Church-Turing y de los procesos matemáticos llamados algoritmos, aunque existan funciones fuera del conjunto de funciones computables de cada máquina físicamente posible, es decir no existe alguna inconsistencia en postular sistemas físicos que computen funciones fuera de *C(T)*, afirmando que la razón por la que podemos construir computadoras aritméticas es gracias a que las leyes de la física permiten la existencia de modelos para los operadores de la aritmética tales como la suma, la resta y la diferencia. Deutsch propuso un modelo de una Máquina Universal de Turing Cuántica (MUTC) para la cual siempre existe una Máquina de Turing Cuántica (MTC) con un programa como parte del estado de entrada que realiza una transformación unitaria sobre un número arbitrario de qubits arbitrariamente cercanos a cualesquiera qubits deseados.

La MUTC de Deutsch no es el único modelo universal de una computadora cuántica. Nielsen y Chuang [33] propusieron un arreglo de compuertas cúanticas programables. Bernstein y Vazirani [35] se basaron en el modelo de Deutsch y propusieron un dispositivo cuántico y demostraron que existe una máquina de Turing U capaz de simular otra MT M con precisión ε.

Máquina de Turing Cuántica

A partir de la generalización de una máquina de Turing clásica, una MTC consiste en un procesador finito de N qubits $n = \{n_1\}\,(i = 0, \cdots, N-1)$ y una cinta infinita consistente de una secuencia de qubits $m = \{m_1\}\,(i = \cdots, -1, 0, 1, \cdots)$, en donde sólo una porción finita de la cinta es usada. El cómputo es realizado en pasos fijos con duración T y durante cada paso solo el procesador y una parte finita de la memoria interactúan, el resto de la memoria se mantiene estática. La dirección actual de la cinta , es decir la posición de la cabeza esta descrita por el observable x, la cual contiene a todo $\mathbb{Z}$ como su espectro. Se define el estado de una MTC como un vector unitario en el espacio de Hilbert desarrollada sobre los estados base

$$\mid x\rangle \mid n\rangle \mid m\rangle,$$

donde $\mid n\rangle \equiv\mid n_0, n_1, \cdots, n_{N-1}\rangle$, $\mid m\rangle \equiv\mid \cdots, m_{-1}, m_0, m_1, \cdots\rangle$.

Si U es el operador unitario que describe una aplicación de la regla de transición de la máquina, los elementos no ceros de la matriz están determinados por

$$\langle x \pm 1; n^{'}; m_x^{'}, m_{y\neq x} \mid U \mid x; n; m_x, m_{y\neq x}\rangle,$$

donde cada elección de U se define una MTC diferente. La evolución de la máquina durante s pasos se encuentra descrita por

$$\mid \Psi\,(sT)\rangle = U^s \mid \Psi\,(0)\rangle$$

donde $\mid \Psi\,(0)\rangle$ es el estado incial y T es el tiempo de duración de cada paso. Si la medición ocurre después de n_1 pasos, y la medición es descrita por un operador J_1 entonces la evolución de la máquina para los primeros $n_1 + j$ pasos se encuentra descrita por $U^j J_1 U^{n_1}$, la cual ha dejado de ser unitaria dado que el operador J_1 es una medición sobre la base computacional. La salida de la máquina se encuentra en la cinta como una superposición de los estados base y deberá ser leída después de haber realizado la medición del contenido del qubit de detención y haberla encontrado en el estado uno. El operador podrá medir en cualquier momento el bit de detención en orden para decidir cuando leer el contenido de la cinta (y colapsar el estado de la máquina). La intención del bit de detención es dar al operador de la máquina una indicación de cuando la salida deberá de ser leída de la cinta sin interferir excesivamente en el cómputo. La salida de una máquina de Turing cuántica para alguna entrada x, que puede ser una superposición de las estados clásicos de entrada, es una distribución de probabilidad P_x sobre todos los posibles contenidos de la cinta en el momento de observar el bit de detención que ha sido activado. Dada la unitariedad, la dinámica de la MTC, asi como la de cualquier sistema cuántico cerrado, es necesariamente reversible.

Máquina Universal de Turing Cuántica

Deutsch afirmó que existe una MUTC (basada en la MTQ y la MUT con 8 operaciones adicionales[26]) para la cual existe un programa que realiza una transformación unitaria, arbitrariamente cercana a cualquier transformación unitaria sobre un número finito de qubits.

Para la MUTC escribimos su estado como

$$\mid Q_x, n\rangle \mid n_h\rangle \mid D\rangle \mid P\rangle \mid \Sigma\rangle,$$

donde $\mid Q_x, n\rangle$ es el estado del procesador, incluyendo la posición de la cabeza, $\mid n_h\rangle$ es el qubit de detención, $\mid D\rangle$ es el estado de los datos de registro y $\mid P\rangle$ es el estado del programa. $\mid D\rangle$ y $\mid P\rangle$ son ambos parte de la cinta y $\mid \Sigma\rangle$ es el resto de la cinta, no afectada durante el cómputo.
Deutsch afirmó que para una U, con alguna transformación arbitraria $\mathcal{U}$ y una precisión arbitraria ε, existe siempre un estado de programa $\mid P\left(D,\mathcal{U},\varepsilon\right)\rangle$ y un número entero $s\left(D,\mathcal{U},\varepsilon\right)$, tal que

$$\begin{aligned} &U^{s(D,\mathcal{U},\varepsilon)} \mid Q_x, n\rangle \mid D\rangle \mid P\left(D,\mathcal{U},\varepsilon\right)\rangle \mid \Sigma\rangle \\ =&\mid Q_x^{'}, n\rangle \mid D^{'}\rangle \mid P^{'}\left(D,\mathcal{U},\varepsilon\right)\rangle \mid \Sigma\rangle, \end{aligned}$$

donde $\| D^{'}\rangle - \mid UD\rangle|^2 < \varepsilon$, $P^{'}$ es el estado de programa después de s pasos, Q y $Q^{'}$ son los estados del procesador en el tiempo inicial y después de s pasos respectivamente.

Deutsch realiza la demostración de la MUTC mediante un esquema de concatenación. La concatenación de dos programas es un programa cuyo efecto es el seguimiento del segundo programa inmediatamente después del primero. Se dio por sentado que si estos dos programas eran válidos entonces su concatenación existe pero la validez de esta no fue probada[22] por Deutsch. Entonces la MUTC de Deutsch fue definida más no realmente probada. Por otro lado el concepto de universabilidad en las MTC no es la misma que tenemos para las máquinas de turing clásicas donde las simulaciones son exactas, la simulación es claramente solo una *aproximación* [25].

La MUT nos ha dado los instrumentos necesarios para encontrar en un número finíto de pasos soluciones a problemas en distintas áreas de las ciencias, pudiendo ejecutar todo tipo de cálculo que sea realizable. No podríamos entender el concepto de la computadora digital sin la MUT. Grandes avances en la ciencia se han dado gracias al desarrollo y las capacidades logradas por las computadoras, una MUT es el modelo abstracto de nuestras computadoras hoy en día.
De la misma manera el lograr la construcción de una MUTC ampliaría las capacidades ya logradas por los algoritmos cuánticos, pudiendo calcular cualquier función cuánticamente computable que le sea introducida.

Capítulo 3

Comunicación Cuántica

La necesidad de la comunicación humana ha existido desde los inicios de la civilización. A través de gestos, sonidos y señales el hombre empezó a comunicarse. La evolución y la complejidad de la sociedad generó nuevas maneras de transmitir información de manera oculta o mediante sistemas que impidieran descubrir el significado de la misma. El objetivo de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación. La criptografía es la ciencia que usa las matemáticas para codificar y decodificar la información. El mensaje original que comunicamos en un lenguaje que comúnmente es entendido por un largo grupo de personas es llamado texto claro y el mensaje oculto texto cifrado. Llamaremos al emisor del mensaje cifrado como Alice, Bob será el receptor y Eve el observador que desea interceptar el mensaje.
Se mostrarán en este capítulo las propiedades elementales del proceso de información y comunicación clásica, la contribución de la mecánica cuántica en la criptografía, el codificado denso y la teleportación cuántica.

3.1. Criptografía Clásica

Es importante mencionar el papel vital que jugaron los anagramas en el desarrollo de la criptografía. Un anagrama consiste en tomar las letras de una palabra y colocarlas en diferente orden, para formar otra palabra. A este procedimiento se le llama transposición, aunque cuando el mensaje es muy corto no es muy aconsejable utilizarlo. Como ejemplo mencionamos la carátula de los dos volumenes sobre Principios de la Computación Cuántica e Información que escribieron G. Benenti, G. Casati y G. Strini, este es el cuadrado latino o la fórmula de Sartor. Éste está costituido por una serie de palabras de 5 letras como sigue:

$$\begin{array}{ccccc} R & O & T & A & S \\ O & P & E & R & A \\ T & E & N & E & T \\ A & R & E & P & O \\ S & A & T & O & R \end{array}$$

En este cuadrado se leen palabras en latín que significan “Él, que guía el arado, planta la semilla”. Lo primero que llama la atención es que se trata de un palíndrome: se lee igual de derecha a izquierda que de izquierda a derecha. Sin embargo es absolutamente simétrica,

se lee igual en todas las direcciones. Este mensaje, se cree, esconde el siguiente significado después de reordenar la palabras Pater Noster, repetido dos veces, formando una cruz la cual tiene significado cristiano. Finalmente, las letras A y O restantes representan la alfa y omega, la primera y la última letra del alfabeto griego, el principio y el fin, también con significado cristiano.

Se cree que el cuadrante latino se ponía en las casas que ofrecían refugio a los cristianos, perseguidos durante el Imperio Romano, quienes eran las únicas personas que sabían cómo trasponer las letras para obtener el significado real del cuadrado. Estos cuadrados han sido encontrados en las paredes de algunas residencias romanas en Pompeya.

Uno de los primeros sistemas criptográficos fue usado durante la guerra de las Galias entre los años 50 a 51 A.C., con el propósito de la expansión de la República Romana sobre territorio galo, dicho sistema conocido como cifrado de César, en referencia al emperador Julio César[1], utiliza un alfabeto al cual le es aplicado un corrimiento de un número fijo $k\epsilon\{0,1,\ldots,n-1\}$ (donde n es el tamaño del alfabeto) de pasos sobre cada letra del alfabeto en el que el mensaje es escrito, obteniendo una correspondencia entre los símbolos del mensaje original y el cifrado. Sea i el i-esimo símbolo del alfabeto tal que al cifrar el mensaje se substituye i donde $i\,\epsilon\{0,1,\ldots,n-1\}$ por el j-esimo símbolo mediante un corrimiento de k lugares a su derecha, entonces podemos escribir $j=\{i+k\}\,(mod\,n)$. Este código era difícil de romper en el siglo I A.C pero en la actualidad es realmente fácil de descifrar.

Los cifrados por substitución como el del Cesár dejó de ser una manera segura de comunicación secreta desde que el análisis de frecuencias traspasó las fronteras del mundo árabe. Esto cambió cuando en lugar de utilizar una substitución monoalfabética se consideró una entrada polialfabética, éste fue uno de los mayores adelantos de la criptografía y su culminación fue el llamado cifrado de Vignere. Este cifrado utliza una tabla de 27 alfabetos (26 si es en inglés) donde cada fila se construye desplazando la anterior un espacio hacia la izquierda. Esta tabla se bautizó como tabula recta. Adicionalmente se utiliza una palabra clave que se repite tantas veces como el texto claro que se quiere mandar de mensaje. Entonces para cifrar cada letra del texto claro se busca la letra en la intersección con la línea de la tabula recta que comienza con la letra de la clave. A este cifrado se le consideró indescifrable, sin embargo fue Charles Babbage quién descubrió en 1854 como descifrarlo al darse cuenta que repeticiones en el mensaje cifrado indicaban repeticiones en el texto claro y estableció un procedimiento para hacerlo. Esto no se supo sino hasta el siglo XX, ya que nunca hizo públicos sus descubrimientos.

Notemos que en este caso Alice deberá comunicarle inicialmente a Bob la llave, en este caso k, a través de una línea segura para que Eve no tenga acceso a ella. Después de esto Alice manda el mensaje cifrado a Bob a través de una línea insegura.
Otro método de cifrado es el cifrado de Polybios que consiste en colocar las letras del alfabeto en una matriz de 5x5. El sistema consiste en hacer corresponder a cada letra del alfabeto un par de letras o de números que indican la fila y la columna en la cual se encuentran.

[1]En particular Julio César utilizó una k=3 en sus mensajes cifrados a los generales romanos.

3.1.1. Cifrado de Vernam

El cifrado de Vernam es el primer sistema de cifrado matemático perfectamente seguro. Inventado por Gilbert Vernam en 1917 y su seguridad fue demostrada por Claude Shannon 30 años más tarde. Para realizar el cifrado se siguen los siguientes pasos:

1. El texto claro se escribe como una secuencia binaria de 0´s y 1´s.
2. La llave secreta es una secuencia binaria completamente aleatoria de la misma longitud que el texto claro.
3. El texto cifrado se obtiene sumando en módulo 2 la llave secreta al texto claro.

Si $\{p_1,p_2,\ldots,p_n\}$ denota el texto claro en binario y $\{k_1,k_2,\ldots,k_n\}$ la llave privada, entonces el texto cifrado $\{c_1,c_2,\ldots,c_n\}$ puede ser obtenido mediante

$$c_i = p_i \oplus k_i \qquad (i = 1, 2, \ldots, n)\,.$$

La seguridad de este método descansa en que la llave es completamente aleatoria y por lo tanto el texto cifrado será también completamente aleatorio. Además no da información alguna del texto claro. Como la llave secreta es compartida por Alice y Bob, éste puede reconstruir el mensaje de una manera sencilla realizando la siguiente operación

$$p_i = c_i \oplus k_i \qquad (i = 1, 2, \ldots, n)\,.$$

Si el cifrado de Vernam se usa más de una vez se vuelve inseguro. Si Eve intercepta dos textos cifrados con la misma llave entonces la adición módulo 2 de sus correspondientes textos claros será igual. Como en el texto claro siempre se encontrará redundancia entonces se vuelve descifrable. Por lo tanto la llave privada de este método debe de ser usada solo una vez. (El cifrado de Vernam también es conocida como "one-time-pad", es decir para cada mensaje se tiene que generar una nueva llave completamente aleatoria). De tal manera que el problema en criptografía no consiste en la transmisión del mensaje cifrado sino en la distribución de la llave privada a través de algún canal seguro. Eve podría interceptar la llave sin dejar rastro alguno. Si esto sucede Alice y Bob nunca podrán estar seguros de la seguridad de la llave. Gran parte de la seguridad del cifrado de Vernam reside en la generación de una cadena aleatoria binaria al menos tan larga como el mensaje que se quiere transmitir. El deseo de romper la seguridad de sistemas criptográficos sofisticados estimuló la construcción de las computadoras electrónicas.

3.1.2. Criptosistema de llave pública

En 1970 Diffie y Hellman propusieron el sistema criptográfico de llave pública. Dicho método surgió con el fin de evitar el problema de la distribución de la llave en los sistemas de cifrado tradicionales. Las diferencias fundamentales entre los criptosistemas de llave privada y los criptosistemas de llave pública reside en:

1. En los criptosistemas de llave privada la seguridad del mensaje se basa en la secrecia de la llave. Alice hace uso de esta llave para encriptar el mensaje. Bob con la misma llave secreta desencripta el mensaje. En algún momento Alice debe de transmitirle a Bob la llave secreta, es por esto que siempre existe el riesgo de que la llave sea interceptada.

2. En los criptosistemas de llave pública Alice y Bob nunca intercambian una llave secreta. Bob hace pública una llave (conocida como llave pública) usada por Alice para encriptar el mensaje. El mensaje no puede ser desencriptado por esta llave sino por otra llave (llave privada) que solo Bob posee. Evitando de esta manera el problema de la distribución de la llave que teníamos en el sistema anterior. De esta manera cualquiera puede encriptar un mensaje pero solo Bob podrá desencriptarlo.

Este sistema requiere de una función matemática f que sea fácil de calcular pero que su inversa f^{-1} sea difícil de computar, es decir que no exista algoritmo que en tiempo polinomial encuentre una solución de $f(x)$ cuando x es escogida al azar. (Su inversa puede ser fácil de computar si se tiene la información correcta). Cualquier problema que cumpla con estas características puede ser usado en principio por la criptografía. Estos problemas caen en la clase computacional NP, que son problemas que pueden ser resueltos en tiempo polinomial por una máquina no determinista. Entonces dos llaves son usadas: una llave pública f usada por Alice para encriptar el mensaje y una llave secreta f^{-1} que sólo Bob tiene y la usa para desencriptar el mensaje.

3.1.3. Protocolo RSA

Los criptógrafos buscaron una función matemática que hiciera realidad la criptografía de clave o llave pública y en 1977 Ronald Rivest, Adi Shamir y Leonard Adleman se dieron cuenta de que los números primos constituían la base ideal para la criptografía de clave pública. Los tres desarrollaron un algoritmo cifrado, conocido actualmente como protocolo RSA, que se convirtío en la piedra angular de la criptografía moderna ya que es la base de la seguridad en Internet.

Supongamos que Alice desea mandar un mensaje encriptado a Bob.

- Generación de la llave:
  Bob selecciona 2 grandes números primos p y q aleatorios y distintos.
  Calcula $pq = N$ y $\Phi = (p-1)(q-1)$.
  Posteriormente Bob selecciona un número aleatorio e coprimo a Φ , donde $1 < e < \Phi$, y calcula d, la inversa $mod\ \Phi$ de e.[2]
  La llave privada de Bob será $k \equiv (d, N)$ y la llave pública la denotamos por $\pi \equiv (e, N)$.
- Encriptación: Alice escribe el mensaje como una secuencia de bloques donde cada bloque puede ser escrito como un número P tal que $P \leq N$, Alice encripta cada P como

$$C = \hat{E}_\pi(P) = P^e mod\, N \tag{3.1.1}$$

  y manda el mensaje encriptado a Bob. Donde $\hat{E}$ denota la operación de encriptación y P el mensaje a codificar con la llave π.
- Desencriptación: Bob recibe el criptograma C y lo desencripta calculando

$$\hat{D}_k(C) = C^d mod\, N = P \tag{3.1.2}$$

[2]Dados dos enteros e y Φ que sean coprimos existe un entero único $d \in \{0, 1, \ldots, N-1\}$ tal que $ed = 1\ mod\ \Phi$. El entero d es el inverso modulo Φ de e

donde $\hat{D}$ denota la operación de desencriptación, k la llave privada y C el mensaje a desencriptar.

Demostración: Por demostrar que el criptograma C es desencriptado por $P^{ed}\ mod\, N$.
En (3.1.1) se definió $C = P^e mod\, N$, por lo tanto vale para $C^d = P^{ed} mod\, N$. Como $ed = 1\ mod\, \Phi$, esto implica la existencia de un entero k tal que $ed = k\Phi + 1 = k(p-1)(q-1)+1$.

Por Teoría de Números sabemos que si un primo p y un entero positivo a son coprimos, entonces

$$a^{p-1} = 1\ mod\, p, \tag{3.1.3}$$

este resultado es conocido como Pequeño Teorema de Fermat.

Si $P \neq 0\ mod\, p$ entonces

$$P^{ed}\ mod\, N = \left(P^{p-1}\right)^{k(q-1)} P\ mod\, p = P\ mod\, p. \tag{3.1.4}$$

Porque $P^{p-1} = 1 \,\mathrm{mod} p$ por 3.1.3 $\therefore \left(P^{p-1}\right)^{k(q-1)} = 1 \mathrm{mod} p$.
Como $N = pq$ entonces por (3.1.4) tenemos que $P^{ed}\ mod\, N = P\ mod\, p = P\ mod\, q$,

$$\therefore P^{ed}\ mod\, N = P, \tag{3.1.5}$$

el criptograma C es entonces desencriptado por $P^{ed}\ mod\, N$.

A diferencia del cifrado de Vernam el protocolo RSA no necesita distribuir una llave privada sobre algún canal supuestamente seguro, la llave privada es sólo conocida por Bob. La llave pública puede ser usada por cualquier sujeto que desee transmitirle un mensaje a Bob y puede ser usada cualquier cantidad de veces que se necesite.
Si uno encuentra los factores p y q de N el cifrado RSA puede ser desencriptado. Como e es conocida entonces d podrá ser calculado. La eficiencia de este algoritmo radica en la complejidad para obtener los factores de un entero N.
En la actualidad es recomendado usar una llave de tamaño de 1024 bits como mínimo para el uso del protocolo RSA[43]. La siguiente tabla nos muestra el tiempo estimado de computo requerido para la factorización de enteros con la Criba Numérica de Campo (Ver 2.7.5). Un año MIPS (Millones de Instrucciones por Segundo) es equivalente al poder computacional de una computadora que realiza 1 MIPS durante un año.

tamaño n (bits)	Años MIPS
512	$3 \cdot 10^4$
768	$2 \cdot 10^8$
1024	$3 \cdot 10^{11}$
1280	$1 \cdot 10^{14}$
1536	$3 \cdot 10^{16}$
2048	$3 \cdot 10^{20}$

Esta tabla muestra la dificultad que resulta encontrar la solución del problema de factorización mediante una computadora clásica. La posibilidad de que sea descubierto un algoritmo de tiempo polinomial para la resolución de este problema no ha quedado excluida. En *2.7.5* observamos que existe un algoritmo que en tiempo polinomial puede resolver el problema de factorización en una computadora cuántica demostrando que los criptosistemas de llaves públicas no son garantía de seguridad para guardar información indefinidamente.

Ejemplo: Bob elige los números primos $p = 773$ y $q = 739$ de tal manera que $N = 571,247$. Posteriormente Bob determina $\Phi = (p-1)(q-1) = 569736$ y elige aleatoriamente $e = 179$. De tal manera que se tiene la llave pública $k = (179, 541247)$.
A continuación Bob determina d pidiendo

$$179d \equiv 1 \; mod \, 569736,$$

que significa que existe un entero n tal que

$$d = \frac{1}{179}\left(569736\, n + 1\right).$$

Esto puede hacerse mediante la construcción de una tabla y determinar el número entero que cumple con la expresión anterior, el resultado es $d = 515627$.
Alice encripta el mensaje estableciendo una correspondencia entre las 27 (26) letras del alfabeto en español (inglés) y números, todos del mismo número de dígitos que N. Si el mensaje tiene l números, $M = \{M_1, \ldots, M_l\}$ de N digitos estos se mezclan mediante la función

$$\left(M_{0k}\right)^e \equiv mod\left(N\right),$$

con $k = 1, 2, \ldots, l$.

Sea el mensaje original

$$M_0 = \{180700, 100413, 261314, 192618, 190817, 170403\} \tag{3.1.6}$$

y el mensaje encriptado

$$M_e = \{141072, 253510, 459477, 266170, 286371, 87175\}$$

El mensaje M_l se envía a Bob quien conoce la clave secreta y puede desencriptar el mensaje, esto es

$$\left(M_{ek}\right)^d \equiv mod\left(N\right)$$

de tal manera que Bon recupera (3.1.6).

3.2. Teorema de No-Clonación

Una propiedad del cómputo clásico es la capacidad de poder copiar un bit. Mientras que el estado genérico de un qubit no puede ser clonado. El teorema de no clonación introducido en 1982 por Dieks, Wooters y Zurek es un resultado de la linealidad de las ecuaciones de movimiento de la mecánica cuántica.
Suponiendo que exista una máquina capaz de clonar estados de qubits. Entonces se puede

hacer una gran cantidad de copias del estado genérico

$$\mid \psi\rangle = \cos\ \beta\ \mid 0\rangle + \sin\ \beta\ \mid 1\rangle. \tag{3.2.1}$$

Por lo tanto sería posible medir todos los estados clonados y obtener con cualquier exactitud deseada el ángulo β. Esta máquina de clonado puede pensarse como parte del aparato de medición contradiciendo el postulado de medición. Este postulado implica que mediante la medición del estado de polarización de un único fotón solo se puede obtener un bit de información. Se obtiene 0 con probabilidad $p_0 = cos^2\beta$ y 1 con probabilidad $p_1 = sin^2\beta$. Sin embargo si esta máquina existiera podríamos determinar con esta medición, y con cualquier exactitud, el parámetro β. Con la simple medición del estado de polarización de un solo fotón podríamos extraer una cantidad arbitraria de información. Por el postulado de medición de la mecánica cuántica podemos deducir que esta máquina de clonación no puede existir.

Demostración matemática del teorema de no clonación

Supongamos que tenemos un sistema compuesto por el qubit a clonar, un segundo qubit y la máquina de copiado(o clonación). El primer qubit se encuentra en el estado genérico

$$\mid \psi\rangle = \alpha\ |\uparrow\rangle + \beta\ |\downarrow\rangle, \tag{3.2.2}$$

donde $\alpha, \beta \in \mathbb{C}$ se encuentran restringidos por la constante de normalización $|\alpha|^2 + |\beta|^2 = 1$. El segundo qubit se encuentra en el estado de referencia $\mid \phi\rangle$ y la maquina de copiado se encuentra en el estado inicial $\mid A_i\rangle$. Suponemos que la máquina de copiado es capaz de realizar la transformación unitaria

$$U\left(\mid \psi\rangle \mid \phi\rangle \mid A_i\rangle\right) = \mid \psi\rangle \mid \psi\rangle \mid A_{f\psi}\rangle = \left(\alpha\ |\uparrow\rangle + \beta\ |\downarrow\rangle\right)\left(\alpha\ |\uparrow\rangle + \beta\ |\downarrow\rangle\right) \mid A_{f\psi}\rangle, \tag{3.2.3}$$

donde el estado final de la máquina $\mid A_{f\psi}\rangle$ depende de estado a clonar $\mid \psi\rangle$.
De la misma manera, si el primer qubit se encuentra en el estado $|\uparrow>$, la máquina de copiado hará la siguiente transformación

$$U\left(|\uparrow\rangle \mid \phi\rangle \mid A_i\rangle\right) = |\uparrow\rangle\ |\uparrow\rangle \mid A_{f\uparrow}\rangle. \tag{3.2.4}$$

Análogamente, si el estado se encuentra en el estado $|\downarrow\rangle$

$$U\left(|\downarrow\rangle \mid \phi\rangle \mid A_i\rangle\right) = |\downarrow\rangle\ |\downarrow\rangle \mid A_{f\downarrow}\rangle. \tag{3.2.5}$$

Por la linealidad de las transformaciones unitarias , y definiendo $|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$,

$$|\rightarrow\rangle \mid \phi\rangle \mid A_i\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \otimes \mid \phi\rangle \mid A_i\rangle \tag{3.2.6}$$

$$\longrightarrow \frac{1}{\sqrt{2}}\left(|\uparrow\rangle\ |\uparrow\rangle \mid A_{f\uparrow}\rangle + |\downarrow\rangle\ |\downarrow\rangle \mid A_{f\downarrow}\rangle\right) \tag{3.2.7}$$

lo cual difiere con la copia ideal obtenida en (3.2.3) para el caso $\alpha = \beta = \frac{1}{\sqrt{2}}$, por lo tanto dicha transformación unitaria no puede existir.

Gran parte de la seguridad de la criptografía cuántica radica en este teorema. Eve no podrá realizar una copia del mensaje transmitido entre Alice y Bob, por lo que la información

del mensaje se mantiene segura, lo que si puede suceder en criptografía clásica. Por otro lado, en computación clásica existen técnicas que ayudan a detectar errores en la transmisión de la información para asegurarnos que la información es transmitida sin errores. Uno de estos métodos se basa en generar respaldos de los estados en medio de un cómputo para posteriormente ser utilizados si hubo un error en el cálculo. Como en el cómputo cuántico no puedo copiar un estado, el teorema de no clonación obliga a buscar nuevas herramientas de detección de errores para la computación cuántica.

3.3. Criptografía Cuántica

Como se ha visto el principal objetivo de la criptografía es ocultar el significado de los mensajes transmitidos a cualquier intruso que desee interceptar la información, en nuestro caso Eve. En información clásica Eve puede interceptar esta información sin que Alice y Bob se den cuenta de esta intrusión y puede realizar, en principio, una cópia de esta información sin modificar el mensaje original. Por otro lado si medimos el estado de un sistema cuántico dicho estado se perturbará (ver Cap. 1) permitiendo así poder detectar si hay un intruso en la comunicación. Esto puede ser aprovechado para crear una llave secreta entre Alice y Bob. Contrario a la criptografía clásica que utiliza algoritmos numéricos la criptografía cuántica utiliza elementos de la mecánica cuántica para elaborar llaves secretas.

3.3.1. Protocolo BB84

El protocolo BB84 es un protocolo creado en 1984 por Charles Bennett y Gilles Brassard [44] que utiliza propiedades cuánticas para realizar una distribución segura de llaves cuánticas. Este protocolo hace uso de 4 estados y dos alfabetos, cada uno de dos estados.

- Alfabeto - z: $\mid 0\rangle, \mid 1\rangle$. Este alfabeto está asociado con los vectores propios de la matriz de Pauli σ_z.
- Alfabeto - x: $\mid +\rangle \equiv \mid 0\rangle_x = \frac{1}{\sqrt{2}}(\mid 0\rangle + \mid 1\rangle)$, $\mid -\rangle \equiv \mid 1\rangle_x = \frac{1}{\sqrt{2}}(\mid 0\rangle - \mid 1\rangle)$. Asociado con los vectores propios de la matriz de Pauli σ_x.

La descripción del protocolo BB84 viene dado de la siguiente manera

1. Alice genera una cadena aleatoria de ceros y unos.
2. Por cada bit generado Alice realiza la siguiente acción: Si el bit es cero, Alice lo codifica escogiendo aleatoriamente entre $\mid 0\rangle$ (alfabeto-z) y $\mid +\rangle$ (alfabeto-x) . Si el bit es uno, lo codifica escogiendo aleatoriamente entre $\mid 1\rangle$ (alfabeto-z) y $\mid -\rangle$ (alfabeto-x).
3. La cadena resultante es enviada a Bob.
4. Para cada qubit, Bob decide aleatoriamente que eje o alfabeto usar para la medición (z o x). Si escoge x entonces mide la polarización del espín a lo largo del eje x, si escoge z medirá a lo largo del eje z. Cabe destacar que en promedio en la mitad de los casos Bob escogerá el mismo eje que Alice escogió, entonces Alice y Bob compartirán el mismo bit. En la otra mitad de los casos Alice y Bob tendrán bits diferentes. A partir de este momento Alice y Bob sólo intercambian información sobre canales públicos.

5. Bob le comunica a Alice que alfabeto uso (z o x) durante la medición sin comunicar los resultados de está.

6. De la misma manera, Alice le comunica a Bob el alfabeto usado para la codificación de cada qubit.

7. Alice y Bob descartan todos los bits donde los alfabetos utilizados sean distintos. Ahora, Alice y Bob comparten la misma llave (conocida como llave preliminar o raw key). Claramente esto sucede en la ausencia de Eve y de ruido como la preparación o la detección de un estado imperfecto o la interacción de un qubit con el medio, etc.

8. Sobre un canal público, Alice y Bob anuncian y comparan su *llave preliminar.* A partir de esta comparación podrán estimar una tasa de error R debido a algún tipo de ruido o a la intrusión de algún espía como Eve. Si la tasa R es demasiado alta deberán de comenzar nuevamente el protocolo, si la tasa es baja realizan reconciliación de información y amplificación de privacidad para derivar una clave secreta común.

9. Reconciliación de información: Alice y Bob dividen la cadena restante de bits de la llave en subconjuntos de longitud l tal que $R \cdot l \ll 1$, es decir se escoge l tal que no se tenga más de un error por subconjunto. La paridad P de una cadena binaria $\{b_1, b_2, \ldots, b_l\}$ está definida por $P = b_1 \oplus b_2 \oplus \cdots \oplus b_l$. Para cada subconjunto Alice y Bob realiza un chequeo de paridad, eliminando en cada ocasión el ultimo bit. Si la paridad de un subconjunto dado es diferente entre Alice y Bob, se localiza y se elimina el bit incorrecto. Como en cada ocasión se elimina el último bit de los subconjuntos de esta manera se evita que Eve obtenga información de sus chequeos de paridad. Al final, con alta probabilidad, Alice Bob compartirán la misma llave.

10. Amplificación de privacidad: Después de calcular R Alice y Bob estiman que el máximo número de bits que Eve puede tener es k. Se define s como un parámetro de seguridad. Alice y Bob escogen de manera aleatoria $n - k - s$ subconjuntos de su llave, donde n es la longitud de la llave. Las paridades de estos subconjuntos se vuelven la llave final. Esta llave es más segura que la anterior ya que Eve necesita información acerca de cada bit de los subconjuntos para poder obtener información acerca de su paridad.

Finalmente, una vez que fue creada la llave por medio del protocolo BB84, Alice puede hacer uso de esta llave para encriptar su mensaje y Bob con la misma llave compartida puede desencriptar el mensaje. Se puede garantizar la seguridad del uso de esta llave debido a que su creación y transmisión fue realizada de manera absolutamente segura, de acuerdo a los fundamentos de la mecánica cuántica.

Ejemplo

Se puede comunicar un mensaje de manera segura haciendo uso de la criptografia clásica y de la criptografia cuántica. La parte de codificación y decodificación del mensaje es realizada por el cifrado de Vernam y la parte de creación segura de la llave es realizada mediante el protocolo BB84. Este último basa su seguridad en que utiliza dos alfabetos asociados a los eigenestados de σ_z y σ_x que no conmutan. Por lo tanto Eve no puede medir tanto la polarización sobre x y sobre z para el mismo qubit.

Se escogío como mensaje original o texto claro la palabra: *Feynman.*

Incialmente, se escribe el texto claro como una secuencia binaria de 0´s y 1´s, con ayuda del codigo ASCII (cualquier otra forma de escribir el texto claro en texto binario puede ser utilizada) se obtiene

$$\overbrace{F}^{\overbrace{01000110}}\ \overbrace{e}^{\overbrace{01100101}}\ \overbrace{y}^{\overbrace{01111001}}\ \overbrace{n}^{\overbrace{01101110}}\ \overbrace{m}^{\overbrace{01101101}}\ \overbrace{a}^{\overbrace{01100001}}\ \overbrace{n}^{\overbrace{01101110}}. \tag{3.3.1}$$

Por comodidad escribimos la secuencia binaria obtenida en una matriz p de $8x7$, donde cada renglón representa una letra del texto claro.

$$p_{i,j} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \tag{3.3.2}$$

Ahora, Alice y Bob necesitan crear una llave compartida secreta y utilizan el protoclo BB84, recordemos que esta llave tiene que ser de la misma longitud que el texto claro.
Alice genera la siguiente cadena aleatoria de ceros unos, sea la cadena generada por 10 columnas y 8 renglones (la cadena generada por Alice tiene que ser necesariamente mayor o igual a la longitud del texto claro)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}. \tag{3.3.3}$$

Una vez generada su cadena, Alice escoge aleatoriamente que alfabeto usará para la codificación

$$\begin{pmatrix} z & x & z & x & z & z & z & x & x & z \\ x & x & z & x & z & z & x & z & z & x \\ z & z & z & x & x & z & x & z & x & x \\ z & x & z & x & z & x & x & x & z & z \\ z & z & x & z & x & z & x & x & z & z \\ x & z & x & z & x & x & z & x & x & z \\ z & x & x & z & x & z & x & z & x & x \\ x & z & x & z & x & x & x & z & z & x \end{pmatrix}. \tag{3.3.4}$$

De acuerdo al alfabeto seleccionado Alice codifica su cadena de bits y la cadena resultante le es enviada a Bob

$$\begin{pmatrix} |0\rangle & |1\rangle_x & |1\rangle & |1\rangle_x & |0\rangle & |0\rangle & |1\rangle & |0\rangle_x & |1\rangle_x & |0> \\ |1\rangle_x & |0\rangle_x & |0\rangle & |1\rangle_x & |0\rangle & |0\rangle & |1\rangle_x & |0\rangle & |1\rangle & |1>_x \\ |0\rangle & |0\rangle & |1\rangle & |1\rangle_x & |1\rangle_x & |0\rangle & |1\rangle_x & |0\rangle & |1\rangle_x & |1>_x \\ |1\rangle & |1\rangle_x & |0\rangle & |0\rangle_x & |0\rangle & |1\rangle_x & |0\rangle_x & |0\rangle_x & |0\rangle & |1> \\ |0\rangle & |1\rangle & |0\rangle_x & |1\rangle & |1\rangle_x & |1\rangle & |0\rangle_x & |1\rangle_x & |0\rangle & |0> \\ |0\rangle_x & |1\rangle & |0\rangle_x & |1\rangle & |0\rangle_x & |1\rangle_x & |1\rangle & |0\rangle_x & |1\rangle_x & |1> \\ |1\rangle & |0\rangle_x & |0\rangle_x & |0\rangle & |1\rangle_x & |0\rangle & |1\rangle_x & |0\rangle & |1\rangle_x & |0>_x \\ |0\rangle_x & |0\rangle & |1\rangle_x & |0\rangle & |1\rangle_x & |0\rangle_x & |1\rangle_x & |1\rangle & |0\rangle & |0>_x \end{pmatrix}. \tag{3.3.5}$$

Para cada qubit recibido Bob decide aleatoriamente que alfabeto usar para la medición, notemos que debido a la aleatoriedad la probabilidad de que Alice y Bob escogan el alfabeto z es igual a la probabilidad de que escojan el alfabeto x.

$$\begin{pmatrix} z & x & z & z & x & z & x & z & x & x \\ x & x & z & z & z & x & x & z & z & x \\ x & x & z & x & x & z & x & z & x & z \\ z & x & z & x & z & z & x & z & z & z \\ z & z & x & x & z & x & z & z & z & z \\ x & z & x & z & z & z & z & x & x & z \\ x & x & x & z & x & z & x & z & z & z \\ x & z & x & x & x & z & x & z & z & x \end{pmatrix}. \tag{3.3.6}$$

Bob realiza una medición para cada uno de los qubits de acuerdo a su alfabeto seleccionado, obtieniendo como resultado

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}. \tag{3.3.7}$$

Bob y Alice se comunican el alfabeto usado para la medición descartando todos los bits donde el alfabeto seleccionado sea distinto, la llave queda entonces como:

$$\begin{pmatrix} 0 & 1 & 1 & - & - & 0 & - & - & 1 & - \\ 1 & 0 & 0 & - & 0 & - & 1 & 0 & 1 & 1 \\ - & - & 1 & 1 & 1 & 0 & 1 & 0 & 1 & - \\ 1 & 1 & 0 & 0 & 0 & - & 0 & - & 0 & 1 \\ 0 & 1 & 0 & - & - & - & - & - & 0 & 0 \\ 0 & 1 & 0 & 1 & - & - & 1 & 0 & 1 & 1 \\ - & 0 & 0 & 0 & 1 & 0 & 1 & 0 & - & - \\ 0 & 0 & 1 & - & 1 & - & 1 & 1 & 0 & 0 \end{pmatrix}. \tag{3.3.8}$$

Finalmente eliminando los espacios en blanco y escribiendo los bits obtenidos en una matriz k de 8 columnas por 7 renglones la llave queda de la siguiente manera

$$k_{i,j} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}. \tag{3.3.9}$$

Una vez creada la llave[3] el texto cifrado $c_{i,j}$ se obtiene de realizar la suma binaria de la llave secreta y el texto claro, entonces $c_{i,j} = p_{i,j} \oplus k_{i,j}$

$$c_{i,j} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.3.10}$$

En este momento Alice es capaz de enviarle el texto cifrado a Bob. Una vez que Bob recibe el texto cifrado puede recuperar (desencriptar) el mensaje original mediante la siguiente suma binaria

$$p_i = c_i \oplus k_i \tag{3.3.11}$$

3.3.2. Protocolo de Brassard (B92)

En 1992 Benett descubrío que para la comunicación cuántica únicamente se necesitan dos estados no-ortogonales. Así surge el protocolo B92 que es una generalización del protocolo BB84, que mantiene sus características, pero trabaja con bases diferentes de codificación y también estados diferentes. Se puede describir el procedimiento del protocolo B92 de la siguiente manera

1. Alice crea una cadena de bits aleatorios a_i, $i = 1, 2, \ldots, n$ y de acuerdo a los valores obtenidos los codifica de acuerdo a

$$|\psi\rangle = \begin{cases} |0\rangle & si \quad a_i = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & si \quad a_i = 1 \end{cases} \tag{3.3.12}$$

2. Alice le envía a Bob la cadena de qubits resultante de la codificación.

3. Bob genera una cadena de bits aleatorios $a_i{}'$ y mide los qubits recibidos en la base computacional $\{|0\rangle, |1\rangle\}$ si $a_i{}' = 0$ o en la base $\{|+\rangle, |-\rangle\}$ si $a_i{}' = 1$, el resultado de las mediciones hecho por Bob se le denomina b_i.

[3]Cabe destacar que Alice y Bob pueden mejorar la seguridad de su llave aplicando reconciliación de información y amplificación de privacidad.

4. Bob le comunica el resultado de las mediciones a Alice.

5. Bob y Alice se comunican para conservar solamente aquellos pares a_i, $a_i{}'$ para los cuales $b_i = 1$. Unicamente cuando $a_i{}' = 1 - a_i$ ocurre que $b_i = 1$. Si $a = a'$ entonces $b = 0$, estos dos eventos ocurren con probabilidad $\frac{1}{2}$.

La clave final es la concatenación de los valores de bits conservados por Alice y Bob: a_i para Alice y $a_i{}' - 1$ para Bob. Posteriormente, Alice y Bob pueden aplicar reconciliación de la información y amplificación de privacidad para hacer su llave más segura.

3.3.3. Protocolo de Ekert (E91)

En 1991 Artur Ekert [46] propuso una implementación para la distribución de llaves cuánticas usando estados cuánticos entrelazados observados por EPR. En este protocolo se tiene un emisor central que crea partículas entrelazadas, en particular pares de partículas de espín $\frac{1}{2}$ en estados singuletes, ϕ (estados de Bell), y las envía a Alice y Bob respectivamente,

$$\mid \phi\rangle = \frac{1}{\sqrt{2}} \left(\mid 01\rangle + \mid 10\rangle \right). \tag{3.3.13}$$

Alice y Bob deben de escoger aleatoriamente uno de los tres ejes coplanares donde realizarán la medición de las partículas recibidas, denotadas por vectores unitarios a_i y b_j $(i, j = 1, 2, 3)$ para Alice y Bob respectivamente. Las partículas emitidas se encuentran sobre el eje z, y los vectores a_i y b_j se encuentran sobre el plano $x - y$ (perpendicular a la trayectoria de las partículas), caracterizadas por los ángulos (medidos desde el eje x): $\phi_1^a = 0^o$; $\phi_2^a = 45^o$; $\phi_3^a = 90^o$; $\phi_1^b = 45^o$; $\phi_2^b = 90$; $\phi_3^b = 135^o$. Los superíndices a y b denotan los analizadores de Alice y Bob respectivamente. Cada medición puede dar como resultado $+1$ (espín para arriba) ó -1 (espín para abajo) y potencialmente revelar un bit de información. Se denota $p_{\pm\pm}(a_i, b_j)$ como la probabilidad de que el resultado ± 1 sea obtenido sobre a_i y ± 1 sobre b_j. Se define entonces el coeficiente de correlación

$$E(a_i, b_j) = p_{++}(a_i, b_j) + p_{--}(a_i, b_j) - p_{+-}(a_i, b_j) - p_{-+}(a_i, b_j) \tag{3.3.14}$$

Para los dos pares de analizadores con la misma orientación (a_2, b_1 y a_3, b_2) la mecánica cuántica predice una anticorrelación total de los resultados obtenidos por Alice y Bob: $E(a_2, b_1) = E(a_3, b_2) = -1$.
Por los resultados obtenidos en la sección 1.7 sabemos que

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) = 2\sqrt{2}. \tag{3.3.15}$$

Una vez realizada la transmisión, Alice y Bob anuncian sobre un canal público los ejes escogidos para cada medición. Posteriormente hacen públicas las salidas de su medición en los casos en los que sus ejes de polarización no coinciden. Esto le permite establecer el valor de S, el cual si las partículas no fueron directamente (Eve) o indirectamente (ruido) perturbadas entonces el valor de S será igual a $2\sqrt{2}$. Esto asegura que los estados están totalmente anti correlacionados y pueden ser convertidos en una cadena secreta de bits (la llave), como el valor de $S = 2\sqrt{2}$ está nueva llave será segura. Posteriormente esta llave secreta puede ser usada en un canal convencional de criptografía cuántica entre Alice y Bob. Alice y Bob pueden aplicar reconciliación de la información y amplificación de privacidad.

Figure 3.3.1: Diagrama de transmisión de partículas en E91

Cabe destacar que durante la transmisión de las partículas, Emisor $\longrightarrow$ Alice, Bob, Eve no podrá robar información alguna de las partículas ya que durante este proceso ninguna información codificada se encuentra sobre las partículas. Está información aparece únicamente después de que Alice y Bob realizan sus mediciones. Eve podría intentar engañar a Alice y Bob, sustituyendo las partículas enviadas por el emisor por sus propias partículas, pero al no conocer de antemano que aparatos de medición usaran Alice y Bob esta estrategia no le será de mucha utilidad.

El funcionamiento de estos protocolos demuestra que en general Alice y Bob no pueden conocer a priori la clave que el algoritmo proporcionará, demostrando por que en algunas ocasiones son conocidos como protocolos de generación de llaves y no como protocolos de transmisión de llaves.

3.3.4. Pruebas de seguridad de mecanismo cuánticos de distribución de llaves

Desde la creación del primer protocolo de distribución de claves en 1984 por Benett y Brassard[44] distintos investigadores (Mayers, 1991 [49] ; Lo y Chau, 1999 [50] ; Biham, 1997 [47] y 2001 [48]; Shor y Preskill, 2000 [51]) han realizado diferentes demostraciones acerca de la seguridad de estos protocolos, una medida de la seguridad de estos protocolos es la cantidad de información que Eve puede obtener de la llave final obtenida. En el año 1999 Biham *et al.* [47] presentó una prueba de seguridad de los mecanismos cuánticos de distribución de llaves simulando los ataques más genéricos que Eve puede aplicar permitidos por la leyes de la física (clásica y cuántica) , suponiendo que este tiene acceso a los canales de comunicación, una capacidad tecnológica ilimitada (memoria cuántica, computadora cuántica).

El ataque más general que Eve puede realizar puede dividirse en dos pasos. El primero de ellos es interceptar y almacenar (memoria cuántica) los qubits que se encuentren en el canal de comunicación entre Alice y Bob en un dispositivo que trate de comprobar el estado de los qubits. El objetivo de Eve es aprender la máxima cantidad de información posible sobre la llave final sin que Alice y Bob aborten el protocolo.

Basándose en los estándares de la distribución cuántica de llaves [52] (Alice y Bob comparten un canal clásico, Eve no puede atacar los laboratorios de Alice y Bob y Alice envía a Bob bits cuánticos) Biham, trabajando sobre el protocolo BB84, demostró que la potencia del mecanismo de distribución de cuántica de llaves queda determinada por la aleatoriedad de la elección de las bases utilizadas para las mediciones y la capacidad de selección aleatoria de los bits de verificación.

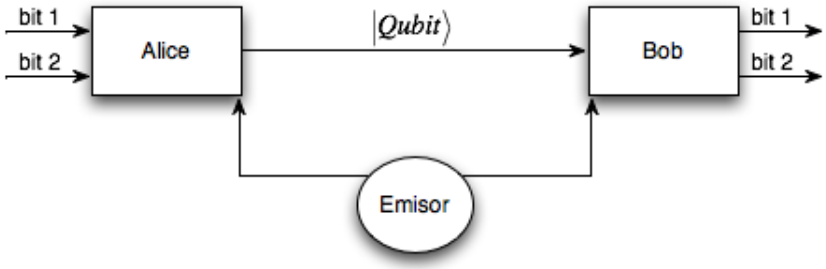


Figure 3.4.1: Descripción del protocolo de codificado denso

3.4. Codificado Denso

Clásicamente el envío de más de un bit de información requiere la manipulación de más de un estado clásico, en comunicación cuántica se tiene la capacidad de poder codificar y transmitir 2 bits de información intercambiando un único qubit físico, con el único requerimiento de que los transmisores y receptores (Alice y Bob) compartan dos partículas entrelazadas, cada una de ellas individualmene puede cargar solo un bit de información.
El codificado denso es la forma más sencilla de aplicación del entrelazamiento cuántico en las comunicaciones.

Inicialmente un emisor S genera un par EPR compartido por Alice y Bob, este par puede ser generado por medio del cicuito visto en *2.5.2*, a partir de una compuerta de Hadamard y una compuerta U_{CNOT}.

$$|\,\phi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|\,00\rangle + |\,11\rangle\right), \tag{3.4.1}$$

$$|\,\phi^{-}\rangle = \frac{1}{\sqrt{2}}\left(|\,00\rangle - |\,11\rangle\right), \tag{3.4.2}$$

$$|\,\psi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|\,01\rangle + |\,10\rangle\right), \tag{3.4.3}$$

$$|\,\psi^{-}\rangle = \frac{1}{\sqrt{2}}\left(|\,01\rangle - |\,10\rangle\right), \tag{3.4.4}$$

el primer qubit le pertenece a Alice y el segundo qubit le pertenece a Bob.

Alice desea enviar un mensaje de dos bits a Bob, clásicamente exisen 4 posibles combinaciones para un par de estas partículas: 00, 01, 10 y 11. Alice escoge una de estas posibles combinaciones de información para enviarsela a Bob y realiza una operación unitaria, con el consentimiento de Bob, de un solo qubit sobre su parte del par EPR de acuerdo a la siguiente tabla

- Si Alice desea enviar los bits 00, Alice aplica I.
- Si Alice desea enviar los bits 01, Alice aplica X.
- Si Alice desea enviar los bits 10, Alice aplica Z.

- Si Alice desea enviar los bits 11, Alice aplica iY (XZ).

Después de aplicar la transformación deseada sobre el estado de Bell, en este caso veremos el par EPR $\mid \phi^+\rangle$, se obtiene uno de los cuatro estados de Bell respectivamente

- 00: $I \otimes I \mid \phi^+\rangle = \frac{1}{\sqrt{2}} (\mid 00\rangle + \mid 11\rangle) = \mid \phi^+\rangle$.
- 01: $I \otimes X \mid \phi^+\rangle = \frac{1}{\sqrt{2}} (\mid 01\rangle + \mid 10\rangle) = \mid \psi^+\rangle$.
- 10: $I \otimes Z \mid \phi^+\rangle = \frac{1}{\sqrt{2}} (\mid 00\rangle - \mid 11\rangle) = \mid \phi^-\rangle$.
- 11: $I \otimes iY \mid \phi^+\rangle = \frac{1}{\sqrt{2}} (\mid 01\rangle - \mid 10\rangle) = \mid \psi^-\rangle$.

En este momento, Alice envía su mitad del par EPR a Bob, esto es Alice le envía dos bits de información clásica a Bob.
Para recuperar la información enviada por Alice, Bob necesita transformar los estados de Bell en estados de la base computacional. Esto se puede lograr mediante la inversa de $U_{CNOT}(H \otimes I)$ que es el circuito que nos permitió obtener el par EPR

$$(U_{CNOT} (H \otimes I))^{-1} = (H \otimes I) U_{CNOT}. \tag{3.4.5}$$

Una vez realizada la operación unitaria apropiada sobre el par EPR, Bob mide los dos qubits y obtiene con probabilidad unidad los dos bits de información clásica enviados originalmente por Alice.
Entonces

- $$\begin{aligned} \mid \psi_{00}\rangle = \; & (H \otimes I) U_{CNOT} \left(\tfrac{1}{\sqrt{2}} (\mid 00\rangle + \mid 11\rangle) \right) = (H \otimes I) \tfrac{1}{\sqrt{2}} (\mid 00\rangle + \mid 10\rangle) = \\ & = \tfrac{1}{\sqrt{2}} \tfrac{1}{\sqrt{2}} ((\mid 0\rangle + \mid 1\rangle) \mid 0\rangle + (\mid 0\rangle - \mid 1\rangle) \mid 0\rangle) = \mid 00\rangle, \end{aligned}$$
- $$\begin{aligned} \mid \psi_{01}\rangle = \; & (H \otimes I) U_{CNOT} \left(\tfrac{1}{\sqrt{2}} (\mid 10\rangle + \mid 01\rangle) \right) = (H \otimes I) \tfrac{1}{\sqrt{2}} (\mid 11\rangle + \mid 01\rangle) = \\ & = \tfrac{1}{\sqrt{2}} \tfrac{1}{\sqrt{2}} ((\mid 0\rangle - \mid 1\rangle) \mid 1\rangle + (\mid 0\rangle + \mid 1\rangle) \mid 1\rangle) = \mid 01\rangle, \end{aligned}$$
- $$\begin{aligned} \mid \psi_{10}\rangle = \; & (H \otimes I) U_{CNOT} \left(\tfrac{1}{\sqrt{2}} (\mid 00\rangle - \mid 11\rangle) \right) = (H \otimes I) \tfrac{1}{\sqrt{2}} (\mid 00\rangle - \mid 10\rangle) = \\ & = \tfrac{1}{\sqrt{2}} \tfrac{1}{\sqrt{2}} ((\mid 0\rangle + \mid 1\rangle) \mid 0\rangle + (\mid 1\rangle - \mid 0\rangle) \mid 0\rangle) = \mid 10\rangle, \end{aligned}$$
- $$\begin{aligned} \mid \psi_{11}\rangle = \; & (H \otimes I) U_{CNOT} \left(\tfrac{1}{\sqrt{2}} (\mid 01\rangle - \mid 10\rangle) \right) = (H \otimes I) \tfrac{1}{\sqrt{2}} (\mid 01\rangle - \mid 11\rangle) = \\ & \tfrac{1}{\sqrt{2}} \tfrac{1}{\sqrt{2}} ((\mid 0\rangle + \mid 1\rangle) \mid 1\rangle + (\mid 1\rangle - \mid 0\rangle) \mid 1\rangle) = \mid 11\rangle. \end{aligned}$$

Cabe destacar que este protocolo garantiza la seguridad en la transmisión de información, ya que aunque Eve intercepte el qubit emitido por Alice nunca podrá acceder a información alguna del sistema, ya que ésta se encuentra codificada en las correlaciones existentes entre los dos qubits entrelazados, por lo tanto, la única manera de obtener esta información es realizando una medición conjunta en el par EPR colapsando el sistema y por consiguiente advirtiendo a Alice y Bob del intruso.

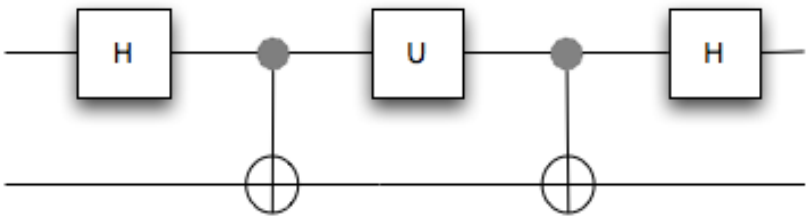


Figure 3.4.2: Circuito Cuántico del Protocolo de Codificado Denso

3.5. Teletransportación Cuántica

Un principio fundamental de la mecánica cuántica es el principio de superposición, aunque en sí mismo este principio puede entenderse en la física clásica. Sin embargo entre los sistemas mecánico cuánticos da lugar a una propiedad llamada enredamiento. Clásicamente las partículas pueden estar correlacionadas sobre distancias grandes simplemente porque pueden prepararse en el mismo estado. Estas correlaciones pueden entenderse perfectamente usando distribuciones de probabilidad clásica y la intuición clásica, la situación es completamente diferente para las correlaciones cuánticas.

El interés en el enredamiento cuántico se ha incrementado en forma notable por el descubrimiento de la teletransportación cuántica. En este proceso un estado cuántico desconocido de una partícula que está descrita por un sistema de dos niveles se teletransporta a otra partícula distante. Es inmediato entonces, ya que la partícula misma no es transportada, que el proceso representa un método de transferencia segura de información entre un remitente (Alice) y un destinatario (Bob). En el proceso, como veremos, el ingrediente clave es que Alice y Bob comparten públicamente un estado maximalmente enredado.

La idea intuitiva de la teletransportación es que queremos que un cuerpo que se encuentre localizado en A, al tiempo t, se desmaterialice y aparece en B al tiempo $t + T$. El proceso cuántico es un poco diferente ya que se está teletransportando el estado de la partícula localizada en B, como las partículas cuánticas son indistinguibles, de cualquier manera el resultado es equivalente.

Una manera posible de realizar la teletransportación es estudiar al objeto en forma exhaustiva posiblemente destruyéndolo, enviar cada una de sus partes a B y reconstruirlo allí. Este procedimiento presenta problemas ya que tenemos un estado cuántico individual que no podemos conocer, ya que se necesita un ensamble de sistemas igualmente preparadas para determinar su estado cuántico. Por lo tanto esa descripción no es posible; es la propiedad del enredamiento cuántico la que permite establecer el protocolo de teletransportación, sin conocer el estado cuántico individual. Adicionalmente se requerirá enviar información clásica de A a B. Es importante señalar que el estado desconocido de la partícula localizada en A es destruida aunque la partícula misma permanece intacta.

Alice y Bob quienes están lejos uno de otro desean realizar el protocolo de la teletransportación. Inicialmente necesitan compartir un estado maximalmente enredado de dos qubits que se llame estado de Bell. Posteriormente Alice recibe un estado desconocido $|\Psi\rangle$ de dos niveles que quiere transportarlo a Bob. Si el estado fuera conocido bastaría con llamar a Bob y darle los detalles del estado y éste podría recrearlo en la partícula que posee.

Entonces recurre al estado de Bell que comparte con Bob y tienen un estado total de tres qubits, que Alice puede reconstruir en términos de la base de Bell y el qubit que pertenece a Bob, notando que a cada estado de Alice le corresponde un estado a Bob.

En 1993 Charles Benett propuso el esquema mencionado arriba que permite transmitir o teletransportar un estado cuántico (información cuántica) entre dos usuarios (Alice y Bob), inclusive en la ausencia de un canal cuántico de comunicación entre Alice y Bob, enviando únicamente dos bits de información, inclusive si estos se encuentran espacialmente separados. Este fenómeno de teletransportación es una de las aplicaciones mas importantes del entrelazamiento cuántico.
El protocolo de teletransportación en detalle se describe de la siguiente manera:
Inicialmente Alice desea transmitir (teletransportar) el estado

$$\mid \varphi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle, \tag{3.5.1}$$

cabe destacar que Alice no conoce el contenido de α y β, recordemos que α y β puede describir una cantidad infinita de información clásica ya que el estado cuántico se encuentra sobre un espacio continuo. Lo único que se sabe es que el estado se encuentra normalizado por $|\alpha|^2 + |\beta|^2 = 1$.

1. Alice y Bob comparten un estado enredado generado por el circuito cuántico visto en la sección 2.5.2 generando uno de los siguientes estados de Bell: $\mid \phi^+\rangle, \mid \phi^-\rangle, \mid \psi^+\rangle, \mid \psi^-\rangle$. Cualesquiera de estos estados enredados pueden ser utilizados en el protocolo de teltransportación, sin modificar el funcionamiento del protocolo. En este caso se aplicará el protocolo de teletransportación para el par EPR $\mid \phi^+\rangle$

$$\mid \phi^+\rangle = \frac{1}{\sqrt{2}} \left(\mid 00\rangle + \mid 11\rangle\right), \tag{3.5.2}$$

   donde el primer qubit corresponde a Alice y el segundo qubit corresponde a Bob. Una vez creado $\mid \phi^+\rangle$ Alice y Bob se separan físicamente. Este estado se obtiene de aplicar $U_{CNOT}\,(H \otimes I)$ al estado de la base computacional $\mid 000\rangle$. (Ver Fig. 3.5.1)

2. Se define $\mid \psi\rangle$ como el estado total del sistema formado por el producto tensorial de (3.5.1) y (3.5.2)

$$\begin{array}{l} \mid \psi\rangle = \mid \varphi\rangle \otimes \mid \phi^+\rangle = (\alpha \mid 0\rangle + \beta \mid 1\rangle) \frac{(|00\rangle + |11\rangle)}{\sqrt{2}} \\ = \frac{\alpha}{\sqrt{2}} \left(\mid 000\rangle + \mid 011\rangle\right) + \frac{\beta}{\sqrt{2}} \left(\mid 100\rangle + \mid 111\rangle\right). \end{array} \tag{3.5.3}$$

   Los primeros dos qubits de este estado le pertenecen a Alice, el tercer qubit pertenece a Bob.
   Si en este momento Alice realiza una medición sobre la base computacional el estado $\mid \psi\rangle$ colapsaria en $\mid 0\rangle$ o en $\mid 1\rangle$ por lo que Alice ya no contaría con la información suficiente para reconstruir el estado. Para evitar esto Alice permite la interacción de su miembro del par EPR con $\mid \psi\rangle$ aplicando una compuerta U_{CNOT}, donde $\mid \varphi\rangle$ funciona como el qubit control y su miembro del par EPR funciona como el qubit blanco. Cabe recordar que al aplicar la compuerta U_{CNOT} si el qubit control es 0 nada se modifica, si el qubit control es 1, entonces el qubit blanco es intercambiado (Ver sección 2.5.1). Por linealidad la compuerta pueda operar en cada uno de los estados, entonces

$$\mid \psi\,'\rangle = U_{CNOT} \mid \psi\rangle = \frac{\alpha \left(\mid 000\rangle + \mid 011\rangle\right) + \beta \left(\mid 110\rangle + \mid 101\rangle\right)}{\sqrt{2}}. \tag{3.5.4}$$

Podemos reescribir (3.5.4) como

$$| \psi' \rangle = \frac{\alpha \mid 0\rangle (\mid 00\rangle + \mid 11\rangle)}{\sqrt{2}} + \frac{\beta \mid 1\rangle (\mid 10\rangle + \mid 01\rangle)}{\sqrt{2}}. \tag{3.5.5}$$

3. Poteriormente Alice aplica una compuerta Hadamard sobre el primer qubit, esta compuerta convierte nuestra base computacional en una superoposición de nuestra base (Ver 2.4.1). Por linealidad la compuerta Hadamard opera sobre la mitad izquierda y derecha de $| \psi' \rangle$:

$$\begin{aligned} | \psi'' \rangle &= H \mid \psi' \rangle = \alpha \left(\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}} \right) \frac{(\mid 00\rangle + \mid 11\rangle)}{\sqrt{2}} \\ &= +\beta \left(\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \right) \frac{(\mid 10\rangle + \mid 01\rangle)}{\sqrt{2}}. \end{aligned} \tag{3.5.6}$$

Desarrollando la ecuación (3.5.6) podemos reescribir el estado $| \psi'' \rangle$ en términos de los posibles resultados de la medición sobre los dos primeros qubits.

$$\begin{aligned} | \psi'' \rangle = \tfrac{1}{2}[&\mid 00\rangle (\alpha \mid 0\rangle + \beta \mid 1\rangle) + \mid 01\rangle (\alpha \mid 1\rangle + \beta \mid 0\rangle) + \\ &\mid 10\rangle (\alpha \mid 0\rangle - \beta \mid 1\rangle) + \mid 11\rangle (\alpha \mid 1\rangle - \beta \mid 0\rangle)]. \end{aligned} \tag{3.5.7}$$

4. En este momento Alice realiza una medición sobre los qubits que se encuentren en su posesión.
De esta manera si Alice mide $\mid 00\rangle$ el estado se colapsa y Bob obtiene $\alpha \mid 0\rangle + \beta \mid 1\rangle$ que es el estado $\mid \varphi\rangle$ enviado por Alice.
Si Alice mide $\mid 01\rangle$ entonces Bob obtiene $(\alpha \mid 1\rangle + \beta \mid 0\rangle)$, aplicando la compuerta X sobre este estado, Bob es capaz de recuperar el estado enviado por Alice $\mid \varphi\rangle$

$$X (\alpha \mid 1\rangle + \beta \mid 0\rangle) = \alpha X \mid 1\rangle + \beta X \mid 0\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle. \tag{3.5.8}$$

Si Alice mide $\mid 10\rangle$ entonces Bob obtiene $(\alpha \mid 0\rangle - \beta \mid 1\rangle)$, si aplica la compuerta Z sobre el estado, Bob recupera $\mid \varphi\rangle$

$$Z (\alpha \mid 0\rangle - \beta \mid 1\rangle) = \alpha Z \mid 0\rangle - \beta Z \mid 1\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle. \tag{3.5.9}$$

Finalmente, si Alice mide $\mid 11\rangle$ Bob obtiene $(\alpha \mid 1\rangle - \beta \mid 0\rangle)$. En esta ocasión Bob aplica las compuertas XZ y entonces recupera $\mid \varphi\rangle$

$$ZX (\alpha \mid 1\rangle - \beta \mid 0\rangle) = \alpha ZX \mid 1\rangle - \beta ZX \mid 0\rangle = \alpha Z \mid 0\rangle - \beta Z \mid 1\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle. \tag{3.5.10}$$

5. Alice le envía a Bob, por medio de cualquier canal clásico de comunicación, los dos bits clásicos de la medición a Bob. Una vez recibido los bits de información de Alice, Bob puede recuperar el estado originalmente enviado por Alice: $\mid \psi\rangle$, realizando la operación unitaria correspondiente.

En la figura 3.5.1 podemos observar el circuito cuántico correspondiente al protocolo de teletranportación. Aqui $\mid a\rangle, \mid b\rangle$ puede tomar cualquier valor de nuestra base computacional, recordemos que el protocolo de teleportación puede ser aplicado a cualquier estado entrelazado de Bell. D_1 y D_2 corresponde a los detectores utilizados para realizar la medición

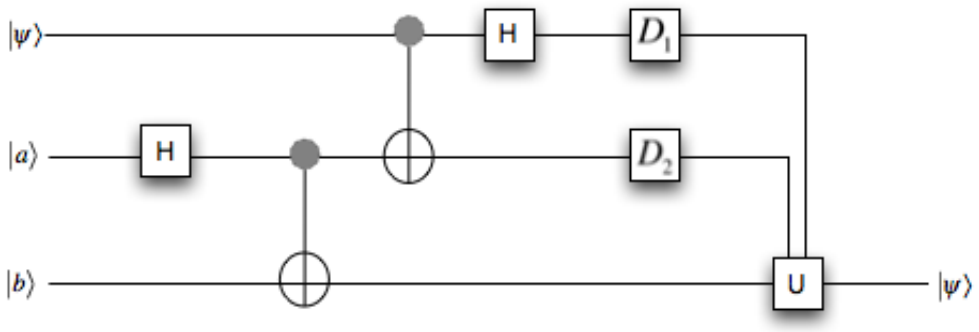


Figure 3.5.1: Circuito cuántico del protocolo de teletransportación.

correspondiente y U la compuerta unitaria correspondiente para recuperar el estado inicial $|\varphi\rangle$.

Alice únicamente le envía a Bob información clásica, por cada qubit teletransportado Alice necesita enviarle a Bob dos bits de información clásica, estos bits no cargan información completa del qubit teletrasportado por lo tanto si Eve intercepta estos bits de información no tendrá la información suficiente para reconstruir el qubit teletransportado. Gracias al estado de Bell compartido entre ellos Alice puede transmitirle a Bob información cuántica. Cabe destacar que en ningún momento se realiza una copia de información por lo que nunca se viola el principio de no clonación. Igualmente el protocolo de teletransportación nunca permite la transmisión de la información más rapido que la luz ya que el protocolo depende totalmente de la transmisión de los resultados de medición obtenidos por Alice mediante un canal de información clásico, y este canal de transmisión está limitado por la velocidad de a luz.
En recientes trabajos [52] se ha usado la teletransportación para transmitir estado cuánticos entre nodos distantes en una red de comunicación cuántica.

La criptografía cuántica ofrece grandes ventajas sobre los métodos clásicos de la criptografía, basa su estructura y seguridad en la combinación de conceptos mecánico cuánticos y de teoría de la información. Es una de las áreas de mayor crecimiento en la computación e información cuántica, su progreso teórico y experimetal en los años recientes ha dado lugar a nuevas áreas de investigación, como la amplificación de privacidad y la búsqueda de nuevos canales de comunicación. Todavía existen retos tecnológicos que permitan a la criptografía cuántica la posibilidad de poder transmitir de manera segura información entre dos actores (Alice y Bob) ilimitadamente distantes pero sin duda es una de las áreas con mayor futuro en la Computación e Información Cuántica.

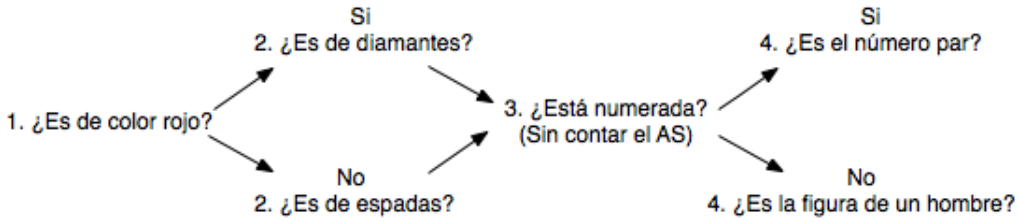
Capítulo 4

Teoría Cuántica de la Información

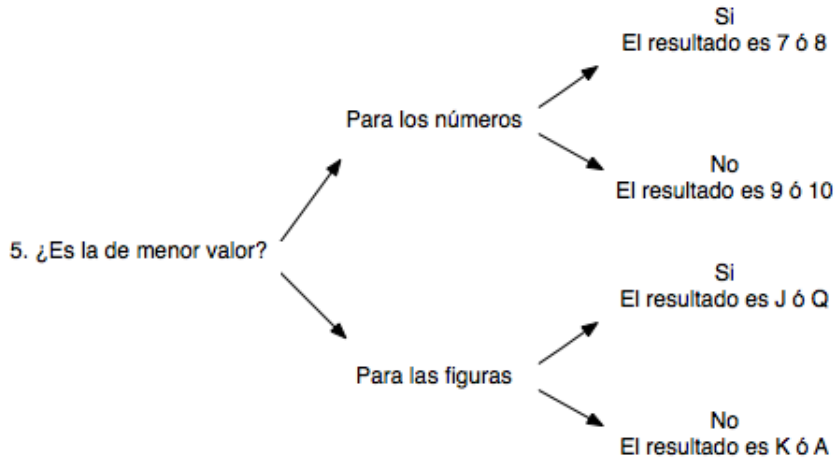
Primero explicaremos el significado del concepto de infomación, que indica la cantidad de detalle contenida en una señal o mensaje. Por lo tanto es un concepto cuantitativo que puede sumarse, almacenarse y transmitirse.

Un ejemplo muy conocido de información lo constituyen los resultados de un experimento de arrojar una moneda muchas veces que son registradas en una computadora, se utiliza un bit por cada tiro. Ocho bits llenan un byte, 1024 bytes se encuentran en un kilobyte, 1024 kb es un megabyte, 1024 Mb en un gigabyte y así sucesivamente.

Otro ejemplo proviene de la teoría de probabilidad y está relacionado con juegos de 32 cartas (7, 8, 9, 10, J, Q, K, A) con dos colores y cuatro trajes (corazones, diamantes, tréboles y espadas). En estos juegos es posible conocer la identidad de una carta mediante las respuestas sí/no de 5 preguntas:



Hasta el momeno de acuerdo a las respuestas se tiene dos posibilidades
7 & 9 *ó* 8 & 10,
si son números mientras que
J & K *ó* Q & A,
si son figuras. Entonces la quinta pregunta podria ser



Lo anterior no es de sorprender si utilizamos el sistema binario e identificamos cada carta por un número de 5 bits y las 5 preguntas se refieren a cada uno de los 5 bits individuales.

En el ejemplo encontramos que con dos bits de información distinguimos los 4 colores, mientras que con tres distinguimos entre 8 casos. Entonces con 5 bits obtenemos el número total de casos 32, de ta manera que relacionar el número de casos con la cantidad de información se necesita una función logarítmica, esto es

$$log_2 32 = 5.$$

En general tendremos que para almacenar un mensaje de m estados se necesitan n bits,

$$n = log_2 m.$$

Cuanta información obtenemos de un mensaje, si éste tiene una alta probabilidad se gana poca información, si es baja se obtiene más información. Por ejemplo: En 1812 ocurrió un temblor en una población, hecho que ocurre muy rara vez entonces si se anuncia mañana no habrá un temblor en la población, este mensaje dará muy poca información.

Entonces para cuantificar la cantidad de información se utiliza el concepto de entropía, que es una cantidad que mide el desorden en la naturaleza.

La información es el opuesto del desorden de tal manera que se mostrará en este capítulo como se utiliza el concepto de entropía para caracterizar el contenido de información en una señal o mensaje, así como indicar cuantos bits se necesitan para transmitir la señal en forma confiable.

Veremos en este capítulo que para cuantificar el contenido de información de un mensaje se utiliza la entropía de Shannon mientras que para el caso análogo del contenido de información cuántica de un mensaje será usada la entropía de Von Neumann. Por lo que se hará también una revisión del formalismo de matriz densidad de la mecánica cuántica.

Una vez que se es capaz de transmitir información clásica o cuántica entre dos entidades (Alice y Bob) la siguiente pregunta a responder es que tanto Bob aprendió de esta información recibida, en la Teoría de la información clásica el Teorema de codificación sin ruido de Shannon responde a esta pregunta. Resulta que se puede extender este teorema a la versión cuántica y medir la cantidad de información transmitida en un canal cuántico (Teorema de Von Neumann). Estos resultados nos ayudan a saber qué tanto podemos comprimir

un mensaje (clásico o cuántico) sin perder información de una manera segura. Antes de llegar a estos resultados se ven las herramientas necesarias para construir estos teoremas, tanto en su versión clásica como en su versión cuántica y se da una breve discusión de la máquina copiadora cuántica que es una máquina de clonado imperfecto propuesta por Buzek y Hillery.

4.1. Formalismo de la matriz densidad

En ciertas ocasiones el estado de un sistema no puede ser descrito por un vector de estado (estado puro) bien definido y lo único que podemos decir del sistema es que el qubit se encuentra descrito por un vector perteneciente a un conjunto de vectores de estado, cada uno con probabilidad p_i. La suma de las probabilidade de los elementos del conjunto es igual a uno. El estado descrito por esta distribución de probabilidad es llamado estado mixto. Podemos tener estados mixtos formados por un ensamble de l estados, esto es

$$\{\mid \psi_1\rangle, \mid \psi_2\rangle, \ldots, \mid \psi_l\rangle\}, \tag{4.1.1}$$

con la distribución de probabilidades $\{p_1, p_2, \ldots, p_l\}$.
La probabilidad p_i de que una medición de la observable A de el resultado a_i está dada por

$$p_i = \sum_{k=1}^{l} p_k \langle \psi_k \mid P_i \mid \psi_k \rangle, \tag{4.1.2}$$

donde las $\mid \psi_k >$ ´s no son necesariamente ortogonles y P_i es el proyector asociado al valor propio a_i. Si lo fueran la expresión será una identidad.
En la expresión anterior $< \psi_k \mid P_i \mid \psi_k >$ denota la probabilidad de medir el eigenvalor a_i de A en el estado puro $\mid \psi_k >$.
El valor esperado de cualquier observable A está determinado por la expresión

$$\begin{aligned} \langle A \rangle &= \sum_{i=1}^{n} a_i p_i, \\ &= \sum_{k=1}^{l} p_k \sum_{i=1}^{n} a_i \langle \psi_k \mid P_i \mid \psi_k \rangle, \\ &= \sum_{k=1}^{l} p_k \langle \psi_k \mid A \mid \psi_k \rangle, \end{aligned} \tag{4.1.3}$$

donde se usó que $A = \sum_{i=1}^{n} a_i p_i$ y en (4.1.3) la probabilidad p_k aparece por la falta de información sobre el sistema mientras que $\langle \psi_k \mid P_i \mid \psi_k \rangle$ está asociado a la probabilidad debida al proceso de medición[1] del eigenvalor a_i.
Los estados mixtos también se pueden representar en términos de operadores sobre el espacio de Hilbert H. Estos operadores son llamados operadores densidad y se definen como

$$\rho = \sum_{k=1}^{l} p_k \mid \psi_k \rangle \langle \psi_k \mid . \tag{4.1.4}$$

[1]Esta probabilidad es intrínsicamente mecánico cuántica.

Dada una base $\{\mid i\rangle\}$ con $\{i = 1, 2, \ldots, n\}$, donde n es la dimensión del espacio de Hilbert H asociado con el sistema, se puede asociar ρ con una representación matricial

$$\rho_{i,j} \equiv \langle i \mid \rho \mid j\rangle. \tag{4.1.5}$$

Los valores de los elementos de la diagonal ρ_{ii} son las probabilidades de encontrar el sistema en sus respectivos estados y la suma de sus elementos es igual a uno. Los elementos fuera de la diagonal ρ_{ij} con $i \neq j$ son conocidos como coherencias. Estos estados fuera de la diagonal representan interferencias entre los estados $\mid i\rangle$ y $\mid j\rangle$. Dichas interferencias se encuentran presentes para cualquier estado $\mid \psi_k\rangle$ del ensamble que contenga una superposición lineal de $\mid i\rangle$ y $\mid j\rangle$.

El valor esperado de cualquier observable puede ser escrito en términos del operador densidad

$$\langle A\rangle = Tr\left(\rho A\right), \tag{4.1.6}$$
$$p(i) = Tr(\rho P_i). \tag{4.1.7}$$

Por lo tanto el operador densidad caracteriza en forma completa el estado, de donde podemos predecir las probabilidades de los posibles resultados de cualquier experimento realizado sobre el sistema.
En el Capítulo 1, Sección 1.2 (Postulados de la Mecánica Cuántica) se vio que si un sistema se encuentra descrito por el vector de estado $\mid \psi_k\rangle$ y se mide la observable A, obteníendose el resultado a_i, el estado del sistema inmediatamente después de la medición es la proyección normalizada

$$\mid \psi\acute{}_k\rangle = \frac{P_i \mid \psi_k\rangle}{\sqrt{\langle\psi_k \mid P_i \mid \psi_k\rangle}}, \tag{4.1.8}$$

donde P_i es el proyector asociado al valor propio a_i.
Por lo tanto, si el sistema se encuentra en un estado mixto descrito por (4.1.4) y se obtiene el resultado a_i, entonces la nueva matriz densidad después de la medición está dada por

$$\rho\acute{} = \sum_{k=1}^{l} p\left(k \mid i\right) \mid \psi\acute{}_k\rangle\langle\psi\acute{}_k \mid, \tag{4.1.9}$$

donde $p\left(k \mid i\right)$ es la probabilidad condicional de que el sistema se encuentre descrito por el vector de estado $\mid \psi\acute{}_k\rangle$ dado que se midió a_i para la observable A.
Recordando un poco teoría de la probabilidad, dado un ensamble estadístico en el que ocurre dos eventos que denotamos por A y B. Si se miden las frecuencias relativas, entonces se obtienen las probabilidades $p\left(A\right)$ y $p\left(B\right)$. La probabilidad conjunta $p\left(A \cap B\right) = p\left(B \cap A\right)$ y está determinada por la frecuencia relativa de ambos eventos. En un ensamble estadístico dado se cumple

$$\begin{aligned} p\left(A \cap B\right) &= p\left(A \mid B\right) p\left(B\right), \\ &= p\left(B \mid A\right) p\left(A\right). \end{aligned} \tag{4.1.10}$$

De estas expresiones se puede obtener el teorema de Bayes que establece

$$p\left(A \mid B\right) = p\left(B \mid A\right) \frac{p\left(A\right)}{p\left(B\right)}. \tag{4.1.11}$$

Usando estos resultados para nuestro sistema físico se tiene que la probabilidad conjunta

$$p(k,i) = p_i p\left(k \mid i\right) = p_k p\left(i \mid k\right). \tag{4.1.12}$$

Si se sustituye (4.1.8) en (4.1.9) se obtiene

$$\rho^{'} = \sum_{k=1}^{l} p\left(k,i\right) \frac{P_i \mid \psi_k\rangle\langle\psi_k \mid P_i}{\langle\psi_k \mid P_i \mid \psi_k\rangle}, \tag{4.1.13}$$

usando el resultado (4.1.12) tenemos que

$$\begin{aligned} p\left(k \mid i\right) &= p\left(B \mid A\right) \frac{p_k}{p_i} \\ &= \frac{p_k}{p_i}\langle\psi_k \mid P_i \mid \psi_k\rangle, \end{aligned} \tag{4.1.14}$$

donde recordamos de los postulados de la mecánica cuántica $p\left(i \mid k\right) = \langle\psi_k \mid P_i \mid \psi_k\rangle$.
Por lo tanto

$$\begin{aligned} \rho^{'} &= \sum_{k=1}^{l} p_k \frac{P_i \mid \psi_k\rangle\langle\psi_k \mid P_i}{p_i}, \\ &= \frac{P_i \rho P_i}{Tr\left(\rho P_i\right)}, \end{aligned} \tag{4.1.15}$$

donde en la ultima igualdad utilizamos la definición de la matriz densidad (4.1.4) y la probabilidad de medir e eigenvalor $a_i$en el sistema (4.1.2).

La evolución temporal del operador densidad puede ser encontrada fácilmente usando la ecuación 1.28 (ecuación de Schrödinger)

$$i\hbar \frac{d}{dt} \mid \psi(t)\rangle = H(t) \mid \psi(t)\rangle. \tag{4.1.16}$$

Como $H = H^{\dagger}$ se puede escribir

$$-i\hbar \frac{d}{dt} \langle\psi(t) \mid = \langle\psi(t) \mid H(t). \tag{4.1.17}$$

La derivada del operador densidad con respecto al tiempo definida en (4.1.4) se escribe

$$\frac{d}{dt}\rho(t) = \sum_{k=1}^{l} p_k \left[\left(\frac{d}{dt} \mid \psi_k(t)\rangle\right) \langle\psi_k \mid (t)+ \mid \psi_k(t)\rangle \left(\frac{d}{dt}\langle\psi_k(t) \mid\right)\right]. \tag{4.1.18}$$

Sustituyendo las derivadas temporales que aparecen en la ecuación de Schrödinger se tiene que

$$\frac{d}{dt}\rho(t) = \frac{1}{ih}\left(H\rho(t) - \rho(t)H\right) = \frac{1}{ih}\left[H, \rho(t)\right], \tag{4.1.19}$$

que se conoce como ecuación de von Neumann.

4.1.1. Propiedades del operador densidad

Un operador ρ es un operador densidad si y sólo si satisface las siguientes propiedades:

- El operador densidad es Hermitiano, esto es $\rho = \rho^\dagger$.
  Si se desarrolla en serie un estado puro $\mid \psi_k\rangle$ sobre una base ortonormal $\{\mid i\rangle\}$, se tiene que

$$\mid \psi_k\rangle = \sum_{i=1}^{n} c_i^{(k)} \mid i\rangle, \tag{4.1.20}$$

  entonces

$$\rho_{i,j} = \sum_{k=1}^{l} p_k \langle i \mid \psi_k\rangle \langle \psi_k \mid j\rangle = \sum_{k=1}^{l} p_k \sum_{l,m=1}^{n} c_l^{(k)} c_m^{(k)*} \langle i \mid l\rangle \langle m \mid j\rangle \tag{4.1.21}$$

  usando la propiedad de ortonormalidad se tiene que

$$= \sum_{k=1}^{l} p_k c_i^{(k)} c_j^{(k)*} = \sum_{k=1}^{l} p_k c_j^{(k)*} c_i^{(k)} = \rho_{ji}^*. \tag{4.1.22}$$

- $Tr(\rho) = 1$.

$$Tr(\rho) = \sum_{i=1}^{n} \rho_{ii} = \sum_{k=i}^{l} p_k \sum_{i=1}^{n} \left| c_l^{(k)} \right|^2 = \sum_{k=i}^{l} p_k = 1. \tag{4.1.23}$$

- ρ es un operador positivo definido, esto es $\langle u \mid \rho \mid u\rangle \geq 0$, para cualquier vector estado $\mid u >$.

$$\langle u \mid \rho \mid u\rangle = \langle u \mid \left(\sum_{k=1}^{l} p_k \mid \psi_k\rangle\langle\psi_k \mid \right) \mid u\rangle = \sum_{k=1}^{l} p_k \left|\langle u \mid \psi_k\rangle\right|^2 \geq 0. \tag{4.1.24}$$

4.1.2. Matriz densidad de un qubit

Como se vio en la sección 2.2.1 el estado puro de un qubit puede ser representado como un punto (θ, ϕ) en la esfera de Bloch

$$\mid \psi(\theta,\phi)\rangle = \cos\frac{\theta}{2} \mid 0\rangle + e^{i\phi} \sin\frac{\theta}{2} \mid 1\rangle. \tag{4.1.25}$$

El operador densidad correspondiente es

$$\rho\,(\theta,\phi) = \mid \psi(\theta,\phi)\rangle\langle\psi(\theta,\phi) \mid, \tag{4.1.26}$$

y su representación matricial en la base $\{\mid 0\rangle, \mid 1\rangle\}$ se define como

$$\rho\,(\theta,\phi) = \begin{bmatrix} cos^2\frac{\theta}{2} & sin\frac{\theta}{2}cos\frac{\theta}{2}e^{-i\phi} \\ sin\frac{\theta}{2}cos\frac{\theta}{2}e^{i\phi} & sin^2\frac{\theta}{2} \end{bmatrix}. \tag{4.1.27}$$

Si elevamos ρ al cuadrado identificamos que es un estado puro, ya que $\rho^2 = \rho$.
Como se vió en la *sección 2.4.3* cualquier operador de un solo qubit puede ser escrito como

una combinación lineal de los operadores $I, \sigma_x, \sigma_y, \sigma_z$. Los operadores $\sigma_x, \sigma_y.\sigma_z$ tienen traza 0 y la traza de I es 1, entonces podemos escribir el operador densidad de un solo qubit como

$$\rho = \frac{1}{2}\left(I + x\sigma_x + y\sigma_y + z\sigma_z\right), \tag{4.1.28}$$

donde $x, y, z \in \mathbb{R}$. El vector $\bar{r} = (x, y, z)$ nos indica las coordenadas del punto en la esfera de Bloch correspondiente al estado ρ, y comunmente se le llama vector de polarización ó vector de Bloch.

La representación matricial para el estado de un qubit toma la forma

$$\rho = \frac{1}{2}\begin{bmatrix} 1+z & x-iy \\ x+iy & 1-z \end{bmatrix}. \tag{4.1.29}$$

La matriz densidad es no negativa por lo tanto debe ocurrir que sus eigenvalores, los denotamos por λ_1 y λ_2 , deben de ser mayores o iguales a cero. Entonces es inmediato

$$det\,\rho = \frac{1}{4}\left(1 - |\bar{r}|^2\right) \geq 0,$$

de tal manera que $0 \leq \bar{r} \leq 1$. Por lo tanto hay una correspondencia uno a uno entre las matrices densidad para un qubit y los puntos sobre la bola unidad o bola de Bloch.
Para un estado puro

$$\begin{aligned} x &= \sin\theta\cos\phi, \\ y &= \sin\theta\sin\phi, \\ z &= \cos\theta, \end{aligned}$$

y entonces $\mid \bar{r} \mid = 1$y $det\rho = 0$. Por lo tanto los estados de Bloch se encuentran en la superficie o frontera de la bola de Bloch. Como un ejemplo de un estado mixto tenemos el estado no polarizado con vector de Bloch $\bar{r} = 0$, obteniéndose

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

4.1.3. Sistemas compuestos

El estado puro de un sistema bipartito reside en el espacio de Hilbert $H = H_1 \otimes H_2$, que es el producto tensorial de los espacios de Hilbert asociados con los subsistemas uno y dos *(Sección 1.1)*. Se puede entonces expresar un estado genérico $\mid \psi\rangle \in H$ normalizado como

$$\mid \psi\rangle = \sum_{i,\alpha} c_{i,\alpha} \mid i\rangle_1 \mid \alpha\rangle_2, \tag{4.1.30}$$

donde $\{\mid i\rangle_1\}$ y $\{\mid \alpha\rangle_2\}$ son bases de H_1 y H_2, respectivamente. Su operador densidad se define como

$$\begin{aligned} \rho =& \mid \psi\rangle\langle\psi \mid = \sum_{i,\alpha}\sum_{j,\beta} c_{i,\alpha}c^*_{j,\beta} \mid i\rangle_1 \mid \alpha\rangle_2 \langle j \mid_1 \langle\beta \mid_2, \\ &= \sum_{i,\alpha}\sum_{j,\beta} \rho_{i\alpha;j\beta} \mid i\rangle_1 \mid \alpha\rangle_2\, {}_1\langle j \mid {}_2\langle\beta \mid, \end{aligned} \tag{4.1.31}$$

con los elementos de matriz de ρ definidos por

$$\rho_{i\alpha;j\beta} =_1 \langle i \mid {}_2\langle \alpha \mid \rho \mid j \rangle_1 \mid \beta \rangle_2. \tag{4.1.32}$$

Suponiendo que la totalidad del sistema se encuentra descrito por la matriz densidad ρ y se desea calcular el valor medio de un operador A_1 actuando únicamente sobre el primer subsistema. Se extiende el operador A_1 sobre todo el espacio de Hilbert H definiendo el operador

$$\tilde{A} = A_1 \otimes I_2, \tag{4.1.33}$$

con I_2 el operador identidad en H_2. Entonces el valor esperado de A_1 está determinado por

$$\langle A_1 \rangle = Tr(\rho \tilde{A}) = \sum_{i,j,\alpha} \rho_{i\alpha;j\alpha}\, {}_1\langle j \mid A_1 \mid i \rangle_1 . \tag{4.1.34}$$

Se define la matriz de densidad reducida para el primer subsistema como

$$\rho_1 = Tr_2 \rho, \tag{4.1.35}$$

donde $Tr_2 =$ denota la traza parcial sobre el subsistema 2

$$Tr_2 \rho = \sum_{\alpha} {}_2\langle \alpha \mid \rho \mid \alpha \rangle_2 . \tag{4.1.36}$$

De la misma manera se puede definir a matriz reducida para el subsistema 2

$$\rho_2 = Tr_1 \rho = \sum_{i} {}_1\langle i \mid \rho \mid i \rangle_1 . \tag{4.1.37}$$

Los elementos de matriz de ρ_1 en la base $\{\mid i\rangle\}$ están dados por

$$(\rho_1)_{ij} = {}_1\langle i \mid \rho_1 \mid j \rangle_1 = \sum_{\alpha} \rho_{i\alpha;j\alpha}. \tag{4.1.38}$$

Sustituyendo (4.1.38) en (4.1.34) se obtiene

$$\langle A_1 \rangle = \sum_{i,j} {}_1\langle i \mid \rho_1 \mid j \rangle_1 \; {}_1\langle j \mid A_1 \mid i \rangle_1 = \sum_{i} {}_1\langle i \mid \rho_1 A_1 \mid i \rangle_1 = Tr(\rho_1 A_1). \tag{4.1.39}$$

Por lo tanto es posible encontrar el valor esperado de un operador actuando únicamente sobre el subsistema uno como si el sistema se encontrara aislado y descrito por la matriz densidad reducida ρ_1. Entonces ρ_1 describe el estado del primer subsistema.
Cabe destacar que aunque ρ denote un estado puro no necesariamente ρ_1 y ρ_2 describirán un estado puro.
La matriz densidad ρ que describe a todo el sistema no es igual al producto tensorial $\rho_1 \otimes \rho_2$ de las matrices de densidad reducidas, esto quiere decir que al mayor conocimiento posible de un todo no necesariamente incluye el mayor conocimiento posible de sus partes.

4.1.4. Matriz densidad de dos qubits

En el siguiente ejemplo se verá como encontrar la matriz densidad de dos qubits dados $\mid A\rangle$ y $\mid B\rangle$

$$\mid A\rangle = \frac{\mid 0\rangle - i \mid 1\rangle}{\sqrt{2}} \tag{4.1.40}$$

$$\mid B\rangle = \sqrt{\frac{2}{3}} \mid 0\rangle + \frac{1}{\sqrt{3}} \mid 1\rangle \tag{4.1.41}$$

Calculamos el producto $\mid A\rangle \otimes \mid B\rangle$

$$\begin{aligned} \mid A\rangle \otimes \mid B\rangle &= \left(\frac{\mid 0\rangle - i \mid 1\rangle}{\sqrt{2}}\right) \otimes \left(\sqrt{\frac{2}{3}} \mid 0\rangle + \frac{1}{\sqrt{3}} \mid 1\rangle\right) \\ &= \frac{1}{\sqrt{3}} \mid 00\rangle + \frac{1}{\sqrt{6}} \mid 01\rangle - \frac{i}{\sqrt{3}} \mid 10\rangle - \frac{i}{\sqrt{6}} \mid 11\rangle \end{aligned}$$

El operador densidad está determinado por la expresión

$$\begin{aligned} \rho = &\left(\frac{1}{\sqrt{3}} \mid 00\rangle + \frac{1}{\sqrt{6}} \mid 01\rangle - \frac{i}{\sqrt{3}} \mid 10\rangle - \frac{i}{\sqrt{6}} \mid 11\rangle\right) \\ &\cdot \left(\frac{1}{\sqrt{3}}\langle 00 \mid + \frac{1}{\sqrt{6}}\langle 01 \mid + \frac{i}{\sqrt{3}}\langle 10 \mid + \frac{i}{\sqrt{6}}\langle 11 \mid\right), \\ &= \frac{1}{3} \mid 00\rangle\langle 00 \mid + \frac{1}{\sqrt{18}} \mid 00\rangle\langle 01 \mid + \frac{i}{3} \mid 00\rangle\langle 10 \mid + \frac{i}{\sqrt{18}} \mid 00\rangle\langle 11 \mid \\ &+ \frac{1}{\sqrt{18}} \mid 01\rangle\langle 00 \mid + \frac{1}{6} \mid 01\rangle\langle 01 \mid + \frac{i}{\sqrt{18}} \mid 01\rangle\langle 10 \mid + \frac{i}{6} \mid 01\rangle\langle 11 \mid \\ &- \frac{i}{3} \mid 10\rangle\langle 00 \mid - \frac{i}{\sqrt{18}} \mid 10\rangle\langle 10 \mid + \frac{1}{3} \mid 10\rangle\langle 10 \mid + \frac{1}{\sqrt{18}} \mid 10\rangle\langle 11 \mid \\ &- \frac{i}{\sqrt{18}} \mid 11\rangle\langle 00 \mid - \frac{i}{6} \mid 11\rangle\langle 11 \mid + \frac{1}{\sqrt{18}} \mid 11\rangle\langle 10 \mid + \frac{1}{6} \mid 11\rangle\langle 11 \mid . \end{aligned}$$

Su representación matricial en la base computacional está dada por

$$\rho = \begin{pmatrix} \frac{1}{3} & \frac{1}{\sqrt{18}} & \frac{i}{3} & \frac{i}{\sqrt{18}} \\ \frac{1}{\sqrt{18}} & \frac{1}{6} & \frac{i}{\sqrt{18}} & \frac{i}{6} \\ -\frac{i}{3} & -\frac{i}{\sqrt{18}} & \frac{1}{3} & \frac{1}{\sqrt{18}} \\ -\frac{i}{\sqrt{18}} & -\frac{i}{6} & \frac{1}{\sqrt{18}} & \frac{1}{6} \end{pmatrix}. \tag{4.1.42}$$

Es inmediato mostrar que $Tr(\rho) = 1$, y se puede decir que $\rho^2 = \rho$, por lo que la matriz densidad describe un estado puro, entonces también ocurre que $\rho = \rho_A \otimes \rho_B$.

4.1.5. Máquina copiadora cuántica

Como se observó anteriormente una máquina clonadora perfecta y determinística de estados cuánticos arbitrarios queda excluida por el principio de no clonación. Pero este principio

aplica únicamente para clonaciones perfectas (Buzek y Hillery, 1996). Buzek y Hillery sugirieron la posibilidad de un clonado imperfecto, especialmente sugirieron una operación unitaria U capaz de realizar un clonado optimo con una calidad de 5/6, tal que el estado de salida toma la forma

$$\mid \phi\rangle^{salida} = \mid A_0\rangle \mid 0\rangle + \mid A_1\rangle \mid 1\rangle, \tag{4.1.43}$$

donde

$$\mid A_0\rangle = \alpha\sqrt{\frac{2}{3}} \mid 00\rangle + \beta\sqrt{\frac{1}{6}} \left(\mid 10\rangle + \mid 01\rangle\right),$$
$$\mid A_1\rangle = \beta\sqrt{\frac{2}{3}} \mid 11\rangle + \alpha\sqrt{\frac{1}{6}} \left(\mid 10\rangle + \mid 01\rangle\right).$$

La calidad de las copias obtenidas se encuentran especificadas por la medida de la fidelidad F definida como

$$F = \langle \psi \mid \rho \mid \psi\rangle, \tag{4.1.44}$$

donde $\mid \psi\rangle$ es el estado puro arbitrario que se desea clonar y ρ es la matriz densidad de salida del estado clonado.
El circuito de la máquina copiadora descrita se muestra en la Figura 1. Este circuito puede descomponerse en dos partes: la parte de preparación del estado y el estado de copiado. En la etapa de preparación $\mid \phi^{prep}\rangle$ el qubit a copiar $\mid \psi\rangle$ no es operado y los qubits auxiliares $\mid 0\rangle \mid aux\rangle$ son rotados y entrelazados por compuertas R_y y U_{CNOT} respectivamente. Es decir no hay flujo de información entre el qubit $\mid \psi\rangle$ y los qubits auxiliares. Posteriormente en la parte de clonación la información cuántica en $\mid \psi\rangle$ es redistribuida en los tres qubits $\mid \psi\rangle, \mid 0\rangle\, y \;\mid 0\rangle$ por una secuencia de cuatro compuertas U_{CNOT}.

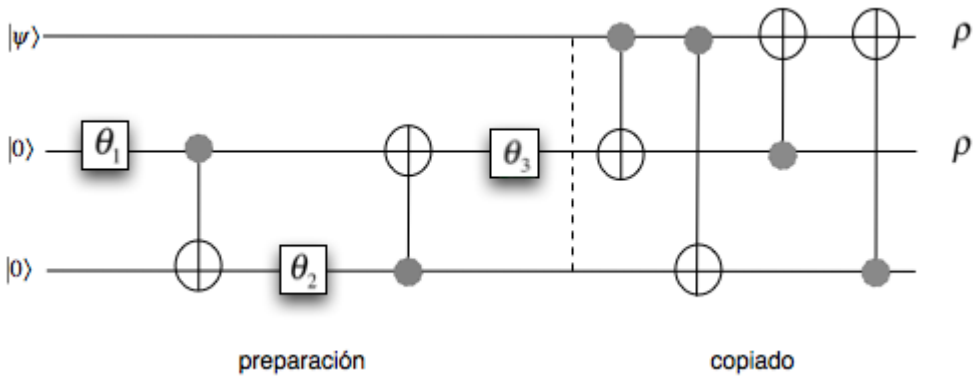


Figure 4.1.1: Máquina Copiadora de Buzek y Hillery

El operador de rotación se encuentra definido como

$$R_y\left(-2\theta\right) = \begin{pmatrix} cos\theta_i & sin\theta_i \\ -sin\theta_i & cos\theta_i \end{pmatrix}. \tag{4.1.45}$$

Denotamos $cos\theta_i = C_i$ y $sin\theta_i = S_i$.

Etapa de Preparación

A continuación describiremos la etapa de preparación del protocolo de la máquina copiadora. Entonces siguiendo el criterio mostrado en la Fig. 4.1.1 se tiene que vamos a efectuar la rotación θ_1 del primer qubit auxiliar, esto es

$$\begin{aligned} R_1 \mid 00\rangle =& (C_1 \mid 0\rangle - S_1 \mid 1\rangle) \mid 0\rangle, \\ =& C_1 \mid 00\rangle - S_1 \mid 10\rangle. \end{aligned} \tag{4.1.46}$$

Ahora al estado resultante lo actuamos con la compuerta U_{CNOT} con el primer qubit auxiliar como control

$$U^1_{CNOT} R_1 \mid 00\rangle = C_1 \mid 00\rangle - S_1 \mid 11\rangle. \tag{4.1.47}$$

La acción de una segunda rotación sobre el segundo qubit

$$\begin{aligned} R_2 U^1_{CNOT} R_1 \mid 00\rangle &= C_1 \mid 0\rangle (C_2 \mid 0\rangle - S_2 \mid 1\rangle) - S_1 \mid 1\rangle (S_2 \mid 0\rangle + C_2 \mid 1\rangle), \\ &= C_1 C_2 \mid 00\rangle - C_1 S_2 \mid 01\rangle - S_1 S_2 \mid 10\rangle - S_1 C_2 \mid 11\rangle. \end{aligned} \tag{4.1.48}$$

Actuamos con la segunda compuerta U_{CNOT} pero ahora con el segundo qubit como control, i.e,

$$C_1 C_2 \mid 00\rangle - C_1 S_2 \mid 11\rangle - S_1 S_2 \mid 10\rangle - S_1 C_2 \mid 01\rangle \tag{4.1.49}$$

Se termina la etapa de preparación mediante una tercera rotación sobre el primer qubit auxiliar, de tal manera que se obtiene

$$\begin{aligned} R_3 U^2_{CNOT} R_2 U^1_{CNOT} R_1 \mid 00 >= \quad & C_1 C_2 (C_3 \mid 0\rangle - S_3 \mid 1\rangle) \mid 0\rangle \\ & -C_1 S_2 (S_3 \mid 0\rangle + C_3 \mid 1\rangle) \mid 1\rangle \\ & -S_1 S_2 (S_3 \mid 0\rangle + C_3 \mid 1\rangle) \mid 0\rangle \\ & -S_1 C_2 (C_3 \mid 0\rangle - S_3 \mid 1\rangle) \mid 1\rangle, \end{aligned} \tag{4.1.50}$$

que denotamos por

$$\mid \phi^{prep}\rangle = D_1 \mid 00\rangle + D_2 \mid 01\rangle + D_3 \mid 10\rangle + D_4 \mid 11\rangle \tag{4.1.51}$$

donde

$$\begin{aligned} C_1 C_2 C_3 - S_1 S_2 S_3 &= D_1, \\ -C_1 S_2 S_3 - S_1 C_2 C_3 &= D_2, \\ -C_1 C_2 S_3 - S_1 S_2 C_3 &= D_3, \\ -C_1 S_2 C_3 + S_1 C_2 S_3 &= D_4, \end{aligned} \tag{4.1.52}$$

Etapa de Clonación

En la segunda parte de la máquina de copiado el qubit $\mid \psi >$ es mezclado con el estado de preparación $\mid \phi^{prep} >$

$$\mid \phi^{clonacion}\rangle = \mid \psi\rangle \mid \phi^{prep}\rangle = D_1 \mid \psi 00\rangle + D_2 \mid \psi 01\rangle + D_3 \mid \psi 10\rangle + D_4 \mid \psi 11\rangle. \tag{4.1.53}$$

En esta etapa se utilizan cuatro compuertas U_{CNOT}: La primera de ellas que denotamos U^3_{CNOT} tiene como bit de control el estado que se quiere clonar y el qubit blanco es el primer qubit auxiliar

$$\begin{aligned}
U^3_{CNOT} \mid \psi 00\rangle &= \alpha \mid 000\rangle + \beta \mid 110\rangle, \\
U^3_{CNOT} \mid \psi 01\rangle &= \alpha \mid 001\rangle + \beta \mid 111\rangle, \\
U^3_{CNOT} \mid \psi 10\rangle &= \alpha \mid 010\rangle + \beta \mid 100\rangle, \\
U^3_{CNOT} \mid \psi 11\rangle &= \alpha \mid 011\rangle + \beta \mid 101\rangle.
\end{aligned}$$

La segunda compuerta la denotamos U^4_{CNOT} y utiliza como qubit de control al estado que se quiere clonar y el blanco es el segundo qubit auxiliar

$$\begin{aligned}
U^4_{CNOT}U^3_{CNOT} \mid \psi 00\rangle &= \alpha \mid 000\rangle + \beta \mid 111\rangle, \\
U^4_{CNOT}U^3_{CNOT} \mid \psi 01\rangle &= \alpha \mid 001\rangle + \beta \mid 110\rangle, \\
U^4_{CNOT}U^3_{CNOT} \mid \psi 10\rangle &= \alpha \mid 010\rangle + \beta \mid 101\rangle, \\
U^4_{CNOT}U^3_{CNOT} \mid \psi 11\rangle &= \alpha \mid 011\rangle + \beta \mid 100\rangle.
\end{aligned}$$

La tercera se denota U^5_{CNOT} y utiliza como qubit de control el primer qubit de control el primer qubit auxiliar y el blanco es el estado a copiar, entonces

$$\begin{aligned}
U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 00\rangle &= \alpha \mid 000\rangle + \beta \mid 011\rangle, \\
U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 01\rangle &= \alpha \mid 001\rangle + \beta \mid 010\rangle, \\
U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 10\rangle &= \alpha \mid 110\rangle + \beta \mid 101\rangle, \\
U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 11\rangle &= \alpha \mid 111\rangle + \beta \mid 100\rangle,
\end{aligned}$$

La última compuerta U^6_{CNOT} tiene como qubit de control al segundo qubit auxiliar y el estado a clonar como qubit blanco

$$\begin{aligned}
U^6_{CNOT}U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 00\rangle &= \alpha \mid 000\rangle + \beta \mid 011\rangle, \\
U^6_{CNOT}U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 01\rangle &= \alpha \mid 101\rangle + \beta \mid 010\rangle, \\
U^6_{CNOT}U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 10\rangle &= \alpha \mid 110\rangle + \beta \mid 001\rangle, \\
U^6_{CNOT}U^5_{CNOT}U^4_{CNOT}U^3_{CNOT} \mid \psi 11\rangle &= \alpha \mid 011\rangle + \beta \mid 100\rangle.
\end{aligned}$$

Por lo tanto el estado de salida está dado por

$$\begin{aligned}
\mid \phi^{salida} > = \alpha &\left(D_1 \mid 000\rangle + D_2 \mid 101\rangle + D_3 \mid 110\rangle + D_4 \mid 011\rangle\right) \\
&+ \alpha \left(D_1 \mid 111\rangle + D_2 \mid 010\rangle + D_3 \mid 001\rangle + D_4 \mid 100\rangle\right),
\end{aligned}$$

que puede reescribirse en la forma

$$\begin{aligned}
\mid \phi^{salida} > &= \mid A_0\rangle \mid 0\rangle + \mid A_1\rangle \mid 1\rangle, \\
&= \left\{\alpha \left(D_1 \mid 00\rangle + D_3 \mid 11\rangle\right) + \beta \left(D_2 \mid 01\rangle + D_4 \mid 10\rangle\right)\right\} \mid 0\rangle \\
&\quad + \left\{\alpha \left(D_2 \mid 10\rangle + D_4 \mid 01\rangle\right) + \beta \left(D_1 \mid 11\rangle + D_3 \mid 00\rangle\right)\right\} \mid 1\rangle
\end{aligned} \tag{4.1.54}$$

Por medio de éstas pueden determinarse fácilmente los estados $\mid A_0\rangle$ y $\mid A_1\rangle$.

Cálculo de la Fidelidad

A continuación se van a comparar las matrices densidad del primero y segundo qubits con la matriz densidad del estado que se quiere copiar a través del concepto de Fidelidad. El procedimiento es el siguiente:

Se establece la matriz densidad reducida, ρ_{12}, trazando sobre el qubit menos significante y el resultado es

$$\rho_{12} =\mid A_0\rangle\langle A_0 \mid + \mid A_1\rangle\langle A_1 \mid,$$

donde definimos

$$\begin{aligned}\mid A_0\rangle &= \alpha\left(D_1 \mid 00\rangle + D_3 \mid 11\rangle\right) + \beta\left(D_2 \mid 01\rangle + D_4 \mid 10\rangle\right),\\ \mid A_1\rangle &= \alpha\left(D_2 \mid 10\rangle + D_4 \mid 01\rangle\right) + \beta\left(D_1 \mid 11\rangle + D_3 \mid 00\rangle\right).\end{aligned}$$

Entonces tenemos

$$\rho_1 = Tr_2\rho_{12} \qquad , \qquad \rho_2 = Tr_1\rho_{12},$$

que explicitamente toman la forma

$$\rho_1 = B_1 \mid 0\rangle\langle 0 \mid + B_2 \mid 1\rangle\langle 1 \mid + B_3 \mid 0\rangle\langle 1 \mid + B_3^* \mid 1\rangle\langle 0 \mid,$$

con

$$\begin{aligned}B_1 &= |\alpha|^2\left(D_1^2 + D_4^2\right) + |\beta|^2\left(D_2^2 + D_3^2\right),\\ B_2 &= |\alpha|^2\left(D_2^2 + D_3^2\right) + |\beta|^2\left(D_1^2 + D_4^2\right),\\ B_3 &= 2\alpha\beta^* D_1 D_4 + 2\alpha^*\beta D_2 + D_3.\end{aligned}$$

La expresión de ρ_2 se obtiene de la anterior reemplazando $D_2 \longrightarrow D_4$ y $D_4 \longrightarrow D_2$.
La fidelidad está determindada por

$$\begin{aligned}F &= |\alpha|^2\langle 0 \mid \rho_1 \mid 0\rangle + \alpha^*\beta B_3 + \alpha\beta^*\langle 1 \mid \rho_1 \mid 0\rangle + |\beta|^2\langle 1 \mid \rho_1 \mid 1\rangle,\\ &= |\alpha|^2 B_1 + \alpha^*\beta\langle 0 \mid \rho_1 \mid 1\rangle + \alpha\beta^* B_3^* + |\beta|^2 B_2.\end{aligned}$$

Substituyendo las expresiones de las $B\acute{}s$ en la relación anterior se obtiene

$$\begin{aligned}F &= D_1^2 + D_4^2 + 2|\alpha|^2|\beta|^2\left[D_2^2 + D_3^2 - (D_1 - D_4)^2\right]\\ &\quad + 2\left(\alpha^{*2}\beta^2 + \alpha^2\beta^{*2}\right)D_2 D_3.\end{aligned}$$

Para obtener una fidelidad independiente del estado a copiar pedimos que los coeficientes

$$\begin{aligned}D_2 D_3 &= 0,\\ D_2^2 + D_3^2 &= (D_1 - D_4)^2.\end{aligned}$$

Se obtiene el mismo resultado para el segundo qubit, obteniéndose las condiciones para los ángulos

$$\cos 2\Theta_1 = \frac{1}{\sqrt{5}}, \qquad \cos 2\Theta_2 = \frac{\sqrt{5}}{3}, \qquad \cos 2\Theta_3 = \frac{2}{\sqrt{5}}. \tag{4.1.55}$$

podemos calcular numéricamente la fidelidad de la máquina copiadora. En el apéndice A se efectúa el cáculo de los ángulos y la fidelidad $F = \frac{5}{6}$.

Para una máquina copiadora cuántica universal de M estados de entrada y dos de salida $(M \longrightarrow N)$ ha sido demostrado [60] que la fidelidad óptima o máxima es $F^{opt}(M,N) = (MN+N+M)/N(M+2)$, de esta ecuación se puede observar que para el caso de la máquina de Buzek y Hillery $(1 \longrightarrow 2)$ su máxima fidelidad es de $5/6$.

Una máquina copiadora cuántica puede ser usada para mejorar el rendimiento de algunas tareas computacionales, mejorar el proceso de información cuántica y su entendimiento. También se podría mejorar el rendimiento de la medición sobre los observables realizando mediciones sobre las copias del sistema cuántico original.

4.1.6. Descomposición de Schmidt

Dado un estado puro $\mid \psi > \in H = H_1 \otimes H_2$ de un sistema cuántico bipartito existen estados ortonormales $\{\mid i >\}$ y $\{\mid i^{\prime} >\}$ para H_1 y H_2, respectivamente tales que

$$\mid \psi >= \sum_{i=1}^{k} \sqrt{p_i} \mid i >_1 \mid i^{\prime} >_2, \tag{4.1.56}$$

con p_i un número real positivo tal que $\sum_{i=1}^{k} p_i = 1$ ($\sqrt{p_i}$ son llamados coeficientes de Schmidt). Los estados $\{\mid i >\}$ y $\{\mid i^{\prime} >\}$ son conocidos como bases de Schmidt para los sistemas H_1 y H_2. Los coeficientes de Schmidt pueden ser calculados de la matriz reducida del sistema, ya sea ρ_A o ρ_B, esto es

$$Tr_B \left(\mid \psi >< \psi \mid \right), \tag{4.1.57}$$

esta matriz tiene como valores propios a p_i. El número de Schmidt es el número de valores propios p_i diferentes de cero y puede ser usado como un criterio de entrelazamiento:

- Si el estado es separable entonces el número de Schmidt es 1.
- Si el estado se encuentra enredado, el número de Schmidt es mayor a uno.

4.1.7. Criterio de Separabilidad de Peres

Dado un estado puro $\mid \psi_{AB} \rangle$ de un sistema bipartito $A+B$ se dice que es separable si y sólo si puede escribirse como un producto de estados $\mid \psi_{AB} \rangle = \mid \alpha \rangle_A \otimes \mid \beta \rangle_B$, donde los estados $\mid \alpha \rangle_A$ y $\mid \beta \rangle_B$ describen las componentes de los dos sistemas. Un estado mixtose dice que es separable si puede ser preparado por dos entidades (Alice y Bob) de alguna manera clásica, esto es por medio de operaciones LOCC. Esto significa que Alice y Bob se ponen de acuerdo sobre canales clásicos de comunicación (teléfono, internet, mensajería, etc.) en la preparación local de los dos subsistemas A y B. Por lo tanto un estado mixto es separable si y sólo si puede ser escrito como,

$$\rho_{AB} = \sum_{k} p_k \rho_{Ak} \otimes \rho_{Bk}, \tag{4.1.58}$$

donde $p_k \geq 0$, $\sum_k p_k = 1$ y ρ_{Ak}, ρ_{Bk} son las matrices densidad de los dos subsistemas. Un sistema separable siempre satisface las desigualdades de Bell *(Ver 1.7)*, esto es, sólo contiene correlaciones clásicas.

Dada una matriz densidad ρ_{AB} no es nada sencillo demostrar si dicha descomposición dada en (4.1.58) existe o no. Existen varios criterios de separabilidad más fáciles de probar. En este caso se verá el criterio de separabilidad de Peres.

El criterio de Peres encuentra una condición necesaria para la existencia de la descomposición dada en (4.1.58), esto quiere decir que una violación de dicho criterio es una condición suficiente para definir entrelazamiento. Dada una base ortonormal $\{\mid i\rangle_A \mid \alpha\rangle_B\}$ sobre el espacio de Hilbert H_{AB} asociada con el sistema bipartito $A+B$, la matriz densidad ρ_{AB} tiene elementos de matriz $(\rho_{AB})_{i\alpha;j\beta} =_A \langle i \mid {}_B\langle\alpha \mid \rho_{AB} \mid j\rangle_A \mid \beta\rangle_B$. Se toma la transpuesta parcial de la matriz densidad (que es construida tomando únicamente la transpuesta sobre los indices latinos, Alice, o los índices griegos, Bob). Por lo tanto, la transpuesta parcial con respecto a Alice está dada por

$$\left(\rho_{AB}^{T_A}\right)_{i\alpha;j\beta} = (\rho_{AB})_{j\alpha;i\beta}\,. \tag{4.1.59}$$

Como un estado separable ρ_{AB} puede ser siempre escrito de la forma 4.1.58 y las matrices densidad ρ_{Ak} y ρ_{Bk} tienen valores propios no negativos, entonces la matriz densidad ρ_{AB} también tiene valores propios no negativos. La transpuesta parcial de estados separables se define como

$$\rho_{AB}^{T} = \sum_k p_k \rho_{Ak}^{T} \otimes \rho_{Bk}. \tag{4.1.60}$$

Como las matrices transpuestas $\rho_{Ak}^{T} = \rho_{Ak}^{*}$ son matrices hermitianas no negativas con traza unitaria, entonces son también matrices de densidad legítimas para Alice. Por lo tanto, ninguno de los valores propios de $\rho_{AB}^{T_A}$ son no negativos. Esta es una condición necesaria para que se cumpla la descomposición 4.1.58. Es entonces suficiente encontrar por lo menos un valor propio negativo para ρ_{AB}^{T} para concluir que el estado ρ_{AB} se encuentra entrelazado.

Ejemplo

El estado de Werner se encuentra descrito por

$$(\rho w)_{AB} = \frac{1}{4}(1-p)\,I + p \mid\mid \psi^-\rangle\langle\psi^- \mid, \tag{4.1.61}$$

donde $0 \leq p \leq 1$, I es la matriz densidad en el espacio de Hilbert H_{AB} y $\mid \psi^-\rangle = \frac{1}{\sqrt{2}}(\mid 01\rangle - \mid 10\rangle)$ es un estado de las bases de Bell. Sobre las bases $\{\mid 00\rangle, \mid 01\rangle, \mid 10\rangle, \mid 11\rangle\}$ la matriz densidad $(\rho w)_{AB}$ se puede escribir como

$$(\rho w)_{AB} = \begin{bmatrix} \frac{1-p}{4} & 0 & 0 & 0 \\ 0 & \frac{1+p}{4} & \frac{-p}{2} & 0 \\ 0 & \frac{-p}{2} & \frac{1+p}{4} & 0 \\ 0 & 0 & 0 & \frac{1-p}{4} \end{bmatrix}. \tag{4.1.62}$$

Si se toma la transpuesta parcial se obtiene

$$(\rho w)_{AB}^{T_A} = \begin{bmatrix} \frac{1-p}{4} & 0 & 0 & \frac{-p}{2} \\ 0 & \frac{1+p}{4} & 0 & 0 \\ 0 & 0 & \frac{1+p}{4} & 0 \\ \frac{-p}{2} & 0 & 0 & \frac{1-p}{4} \end{bmatrix}. \tag{4.1.63}$$

Esta matriz tiene como valores propios $\lambda_1 = \lambda_2 = \lambda_3 = \frac{1+p}{4}$ y $\lambda_4 = \frac{1-3p}{4}$. Como $\lambda_4 < 0$ para $\frac{1}{3} < p \leq 1$ entonces el estado de Werner se encuentra entrelazado para estos valores de p.

En 1996 M. Horodecki [20] demostró que para estados compuestos de dimensión 2×2 y 2×3 el criterio de Peres provee una condición suficiente y necesaria de separabilidad, esto es, el estado ρ_{AB} es separable si y sólo si $\rho_{AB}^{T_A}$ es no negativa. Sin embargo, para sistemas de mayor dimensión existen estados donde todos los valores propios de su transpuesta parcial son no negativos pero no son estados separables.

4.1.8. Medición de la matriz densidad para un qubit

En la sección 2.2 se observó que las coordenadas (x, y, z) del vector de Bloch de un estado puro pueden ser medidas si se tienen disponibles una gran cantidad de estados preparados de la misma manera. Igualmente se puede obtener una medición para estados mixtos. Dada la matriz densidad de un qubit descrita por la ecuación (4.1.29), el procedimiento de medición se realiza a través de una transformación unitaria U que convierte a la matriz densidad ρ de la ecuación (4.1.29) en una nueva matriz $\rho' = U\rho U^\dagger$ y un detector D realiza la medición de σ_z (Ver Figura 4.1.2).

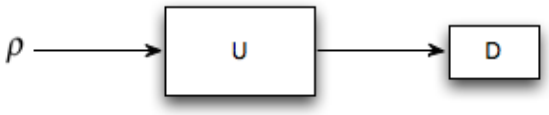


Figure 4.1.2: Medición de la matriz densidad

Las posibles salidas de esta medición son $\sigma_z = \pm 1$ con probabilidad

$$p_i = Tr\left(\rho' P_i\right) = Tr\left(U\rho U^\dagger P_i\right) = Tr\left(\rho U^\dagger P_i U\right) = Tr\left(\rho Q_i\right), \tag{4.1.64}$$

donde los operadores P_i están descritos por

$$P_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad P_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \tag{4.1.65}$$

y $Q_i = U^+ P_i U$.
Para realizar una medición de la coordenada z se toma $U = I$, tal que $Q_0 = P_0$ y $Q_i = P_i$. De esta manera se puede calcular p_0 y p_1 y checar que

$$p_0 - p_1 = z \tag{4.1.66}$$

Para calcular la coordenada x se toma U como una rotación (el sentido positivo de una rotación es la dirección del movimiento de las manecillas del reloj) de $\frac{\pi}{2}$ en la esfera de Bloch sobre el eje y, es decir $U = R_y\left(-\frac{\pi}{2}\right)$. De esta manera el eje x es transformado en el eje z y entonces x podrá ser calculado realizando la medición de σ_z y $p_0 - p_1 = x$
De la misma manera se puede realizar una rotación sobre el eje x para calcular y con$U = R_y\left(-\frac{\pi}{2}\right)$ y entonces $p_1 - p_0 = y$.
Para obtener un buen estimado de las coordenadas se puede realizar el mismo proceso un número considerable de veces. Este mismo método se puede generalizar para medir matrices densidad de mayores dimensiones.

4.1.9. Mediciones Generalizadas, mediciones débiles y POVM

Una medición generalizada se encuentra descrita por un conjunto de operadores de medición $\{M_i\}$, no necesariamente auto-adjuntos, que satisfacen la relación de completez

$$\sum_i M_i^\dagger M_i = I. \tag{4.1.67}$$

Si el estado del sistema antes de la medición es $\mid \psi >$, entonces la probabilidad de una medición i esta dada por

$$p_i = \langle \psi \mid M_i^\dagger M_i \mid \psi \rangle. \tag{4.1.68}$$

El estado del sistema después de la medición viene descrito por

$$\mid \psi' >= \frac{M_i \mid \psi \rangle}{\sqrt{\langle \psi \mid M_i^\dagger M_i \mid \psi \rangle}}. \tag{4.1.69}$$

La relación de completez dada en (4.1.67) nos asegura que las sumas de las probabilidades sea unitaria: $\sum_i p_i = \sum_i \langle \psi \mid M_i^\dagger M_i \mid \psi \rangle = 1$. Las mediciones de proyección descritas en la sección 1.2 junto con operaciones unitarias son equivalentes a las mediciones generalizadas (con ayuda de qubits auxiliares). Esto quiere decir que las mediciones generalizadas son equivalentes a las mediciones de proyección en espacios de Hilbert mayores, este enunciado es conocido como Teorema de Neumark.
Este resultado no es válido para subsistemas de un mismo sistema, una medición de proyección realizado sobre el sistema no puede ser descrita como una medición de proyección sobre el subsistema.

Un tipo especial de mediciones generalizadas son las mediciones débiles, mediciones que casi no distorsionan el estado de sistema. La cantidad de información que puede ser extraída por una medición débil es pequeña, aunque si una medición débil es repetida un gran número de ocasiones su efecto puede ser igual al de las mediciones fuertes.

En ciertas ocasiones el estado de un sistema puede ser medido una sola vez y no se tiene interés en el estado del sistema después de la medición. A este tipo de mediciones se les conoce como mediciones POVM (Positive Operator Valued Measurements). Una medición POVM está descrita por un conjunto de operadores no negativos F_i (elementos POVM[2]), tales que

$$\sum_i F_i = I. \tag{4.1.70}$$

Si la medición es realizada en un sistema descrito por el vector estado $\mid \psi \rangle$, la probabilidad de obtener i es

$$p_i = \langle \psi \mid F_i \mid \psi \rangle. \tag{4.1.71}$$

Las mediciones POVM pueden ser vistas como mediciones generalizadas si definimos $F_i = M_i^\dagger M_i$. Las mediciones de proyección también pueden ser vistas como POVM, si adicionalmente tenemos $M_i^\dagger M_i = M_i$, con M_i como proyectores y $\sum_i F_i = \sum_i M_i = I$.

[2]Elementos de una medición POVM no son necesariamente ortogonales, por lo que el número de elementos en POVM puede ser mayor que la dimensión del espacio de Hilbert en donde se está actuando

Se pueden encontrar estados de medición POVM que puedan distinguir entre dos estados cuánticos no ortogonales.

4.2. Entropía de Shannon

En el capítulo 3 se ha visto como se puede comunicar un mensaje m codificando su información como una secuencia binaria de ceros y unos. Una herramienta básica de la Teoría de la Información Clásica es cuantificar la información que es enviada en un mensaje m. Claude E. Shannon demostró en 1948 que se puede realizar una correcta aproximación de la información contenida en un mensaje dado. El método de Shannon nos permite caracterizar cuanta información ganamos de una señal recibida. Si un mensaje tiene una alta probabilidad de ocurrencia, entonces cuando el mensaje es recibido no se gana mucha información nueva. Por otro lado, cuando la probabilidad de ocurrencia del mensaje es baja se gana una cantidad significantiva de información al recibir el mensaje. Shannon cuantificó esto tomando el logaritmo en base 2 de la probabilidad de que un mensaje dado ocurra. Esto es, si denotamos la información contenida en un mensaje como I, y la probabilidad de su ocurrencia como p, entonces:

$$I = -log_2\, p. \tag{4.2.1}$$

El signo negativo nos asegura que la cantidad de información contenida en el mensaje será positiva, ya que $0 \leq p \leq 1$; además se garantiza que un mensaje con mayor probabilidad de ocurrencia tendrá menor información contenida y un mensaje con menor probabilidad tendrá mayor información

Ejemplo: Supongamos que la probabilidad de que no ocurra un sismo en la ciudad de Durango es de 0.995, entonces la información contenida en este mensaje será

$$I = -log_2\,(0.995) = 0.0072. \tag{4.2.2}$$

Y la probabilidad de que si ocurra un sismo en la ciudad de Durango es de 0.005, entonces

$$I\,' = -log_2\,(0.005) = 7.6439 \tag{4.2.3}$$

Sea X una variable aleatoria caracterizada por una distribución de probabilidad, y supongamos que X puede tomar los valores $x_1, x_2, \ldots, x_n$ con probabilidades $p_1, p_2, \ldots, p_n$. Donde las probabilidades satisfacen que $0 \leq p_i \leq 1$ y $\sum_i p_i = 1$.
Entonces, la entropía de Shannon de X esta definida como

$$H\,(X) = -\sum_i p_i log_2\, p_i. \tag{4.2.4}$$

La mayor cantidad de información $H\,(X)$ que puede obtenerse ocurre cuando la distribución de probabilidad de los n elementos de X es la misma. La probabilidad de encontrar cada elemento de X, si su distribución de probabilidad es uniforme, es $\frac{1}{n}$. Entonces la entropía de X está dada por $-\sum \frac{1}{n} log\, \frac{1}{n} = \sum \frac{1}{n} log\, n = log\, n$. Por lo tanto la entropía de Shannon está acotada por

$$0 \leq H\,(X) \leq log\, n. \tag{4.2.5}$$

De esta manera se puede ver como la entropía de Shannon ayuda a determinar la cantidad de información contenida en un mensaje (también puede verse como una medida de la

incertidumbre o de la aleatoriedad de un mensaje, mientras menor sea su incertidumbre será mayor su entropía) .

4.2.1. Compresión de datos clásicos

La entropía de Shannon además de ayudarnos a medir la cantidad de información contenida en un mensaje, puede ayudar a responder ¿qué tanto se puede comprimir un mensaje sin perder información?.
Supongamos que se requieren l_i bits para representar cada x_i en X. Entonces la tasa media de bits requerida para codificar X está dada por

$$R_X = \sum_{i=1}^{n} l_i p_i, \tag{4.2.6}$$

donde l_i es la longitud en bits de la letra codificada.
La entropía de Shannon es la cota inferior de la tasa media de bits

$$H(X) \leq R_X \tag{4.2.7}$$

Ej. Consideremos un mensaje escrito usando el siguiente alfabeto de 4 letras: $A = \{a_1, a_2, a_3, a_4\}$. Supongamos que estas letras ocurren con probabilidad $p_1 = \frac{1}{2}$, $p_2 = \frac{1}{4}, p_3 = p_4 = \frac{1}{8}$. Para poder especificar una letra dentro del alfabeto se necesitan 2 bits de información.
Podemos codificar las letras de la siguiente forma

$$a_1 \to c_1 = 00,\ a_2 \to c_2 = 01,\ a_3 \to c_3 = 10,\ a_4 \to c_4 = 11,$$

para la cual $R_x = \frac{1}{2}2 + \frac{1}{4}2 + \frac{1}{8}2 + \frac{1}{8}2 = 2$, por lo que no se obtiene compresión alguna.
Si las letras se codifican de la siguiente manera

$$a_1 \to c_1 = 0,\ a_2 \to c_2 = 10,\ a_3 \to c_3 = 110,\ a_4 \to c_4 = 111, \tag{4.2.8}$$

se obtiene $R_x = \frac{7}{4} < 2$ por lo tanto la información puede ser comprimida correctamente. Cabe destacar que una buena estrategia de compresión de datos es codificar las cadenas con mayor probabilidad de aparición con las secuencias de menor tamaño y las cadenas con menor probabilidad con secuencias mayores.

Shannon demostró que la tasa de compresión óptima de datos está dada por la entropía de Shannon.

4.2.2. Teorema de codificación sin ruido de Shannon

Dado un mensaje cuyas letras han sido seleccionadas de un ensamble $A = \{a_1, a_2, \ldots, a_k\}$ con probabilidades de aparición $\{p_1, p_2, \ldots, p_k\}$, existe una compresión óptima y confiable del mensaje con $H(p_1, p_2, \ldots, p_k)$ bits por letra.

Esto es, si Alice le envía a Bob una cadena de n bits de información tomada del ensamble A, entonces Alice podrá enviar el mensaje de una manera óptima y confiable enviando únicamente $nH(p_1, p_2, \ldots, p_k)$ bits de información.

Mensaje	Codigo de Huffman
0000	10
0001	000
0010	001
0011	11000
0100	010
0101	11001
0110	11010
0111	1111000
1000	011
1001	11011
1010	11100
1011	111111
1100	11101
1101	111110
1110	111101
1111	1111001

Figure 4.2.1: Código de Huffman con $p_0 = \frac{3}{4}$ y $p_1 = \frac{1}{4}$

Ejemplo:

Usando el codificado visto en (4.2.8) a un alfabeto de 4 letras con $p_1 = 0.9$, $p_2 = 0.05$, $p_3 = p_4 = 0.025$. La compresión óptima está determinada por $H(p_1, p_2, p_3, p_4) \approx 0.62$, mientras que $R_X = 1.15$. Por lo tanto, en este caso aunque es útil, la codificación no es óptima. Si ahora las probabilidades son equiprobables, $p_i = \frac{1}{4}$ para $i = 1, 2, 3, 4$, en este caso se obtiene $H = 2$, por lo tanto no es posible compresión alguna y se envían exactamente 2 bits de información por letra. Por otro lado, si calculamos $R_X = 2.25 > 2$, por lo tanto en es este caso el código no mejora la eficiencia de la transmisión de los datos.
Si consideramos el código de Huffman (el código de Huffman se basa en la probabilidad de aparición de cada letra que un mensaje contenga) dado en la figura 4.2.1 y un alfabeto binario $\{0, 1\}$ y el procedimiento de codificación está aplicado a cadenas de 4 bits de longitud. Hay entonces en total $2^4 = 16$ cadenas posibles formadas con el alfabeto binario. Sea P_i la probabilidad de que la cadena i ocurra, con $i = 0, 1, \ldots, 15$. Se tiene que $P_0 = p_0^4$, $P_1 = p_0^3 p_1, \ldots,\ P_{15} = p_1^4$. Supongamos que $p_0 = \frac{3}{4}$ y $p_1 = \frac{1}{4}$, entonces $4H(p_0, p_1) \approx 3.25$, mientras que el código de Huffman da $R_X \approx 3.27$, por lo que la compresión lograda es muy cercana a la óptima.
La relevancia de la compresión de datos en telecomunicaciones es muy amplia, permite incrementar la tasa de transmisión de datos en una señal así como la capacidad de almacenamiento en un dispositivo digital, así como en teleportación y criptografía. El teorema de Shannon dice que mientras las probabilidades de aparición de las letras de un mensaje no sean equiprobables una compresión de datos es posible.

4.3. Entropía de Von Neumann

El análogo cuántico de la entropía de Shannon es la entropía de Von Nuemann, en lugar de utilizar elementos de una distribución de probabilidad utilizamos operadores densidad. La entropía de un estado cuántico con un operador ρ , llamada entropía de Von Neumann, está dada por

$$S(\rho) = -Tr\left(\rho \log \rho\right). \tag{4.3.1}$$

Se puede observar la analogía con la entropía de Shannon en el siguiente ejemplo: Alice tiene a su disposición un alfabeto $A = \{\rho_i, \rho_2, \ldots, \rho_k\}$, donde cada ρ_i corresponde a matrices densidad que describen un estado cuántico. Estas letras o matrices son escogidas aleatoriamente con probabilidad p_i tal que $\sum_{i=1}^{k} p_i = 1$. Supongamos que Alice envía una letra (un estado cuántico) a Bob y lo único que sabe Bob es que dicha letra fue tomada del ensamble $\{\rho_i, p_i\}$. Por lo tanto Bob describe el sistema cuántico en términos de la matriz densidad

$$\rho = \sum_{i=1}^{k} p_i \rho_i. \tag{4.3.2}$$

Entonces

$$S(\rho) = -Tr\left(\rho \log \rho\right) = -\sum_{i=1}^{k} \lambda_i log \lambda_i = H\left(\lambda_i, \ldots, \lambda_k\right), \tag{4.3.3}$$

donde λ_i son los valores propios de la matriz densidad ρ y $H\left(\lambda_i, \ldots, \lambda_k\right)$ es la entropía de Shannon asociada al ensamble $\{\lambda_i\}$.
La entropía de Von Neumann satisface las siguientes propiedades:

1. Para un estado puro, $S\left(\rho\right) = 0$. Si ρ es un estado puro, únicamente un valor propio de ρ es diferente de cero, sea $\lambda_1 = 1$, entonces $-\sum_i \lambda_i log \lambda_i = -\lambda_1 log \lambda_1 = 0$.

2. La entropía S no es afectada si un cambio de base unitario es aplicado, es decir $S\left(U\rho U^{\dagger}\right) = S\left(\rho\right)$. La entropía S únicamente depende de los valores propios de ρ, esto es: la entropía de Von Neumann es invariante sobre una evolución temporal unitaria.

3. Si el operador densidad ρ actúa sobre un espacio de Hilbert de dimensión N, entonces $0 \leq S\left(\rho\right) \leq log\, N$. Esto puede observarse si igualamos $S\left(\rho\right) = H\left(\lambda_i, \ldots, \lambda_N\right)$ en la ecuación (4.2.5).

A continuación se presenta un ejemplo en el que se muestran las semejanzas y diferencias entre las entropías de Von Neumann y Shannon.

En el caso más simple, Alice tiene a su disposición una fuente que produce un qubit a partir de dos estados puros ortogonales. Estos estados constituyen una base para el espacio de Hilbert de un solo qubit llamada $\mid 0\rangle$y $\mid 1\rangle$. Las matrices densidad correspondientes son $\rho_0 = \mid 0\rangle\langle 0 \mid$ y $\rho_1 = \mid 1\rangle\langle 1 \mid$. Suponemos que la fuente genera el estado $\mid 0 >$ o el estado $\mid 1 >$ con probabilidades $p_0 = p$ y $p_1 = 1 - p$ respectivamente. Entonces se define la matriz densidad ρ como:

$$\rho = p_0 \mid 0\rangle\langle 0 \mid + p_1 \mid 1\rangle\langle 1 \mid = \begin{bmatrix} p_0 & 0 \\ 0 & p_1 \end{bmatrix}. \tag{4.3.4}$$

La entropía de Von Neumann está dada por

$$S(\rho) = -Tr\left(\left[\begin{array}{cc} p_0 & 0 \\ 0 & p_1 \end{array}\right]\left[\begin{array}{cc} log\, p_0 & 0 \\ 0 & log\, p_1 \end{array}\right]\right) = -p_0 log\, p_0 + -p_1 log\, p_1 = H(p_0, p_1). \quad (4.3.5)$$

Cabe destacar que en este caso en donde las letras del alfabeto corresponden a estados puros ortogonales la entropía de Von Neumann coincide con la entropía de Shannon. Esto se debe a que los estados ortogonales son perfectamente distinguibles.

Un caso más complejo es cuando se tiene una fuente de estados puros no ortogonales $\left(\mid \tilde{0}\rangle\ y\ \mid \tilde{1}\rangle\right)$. Se puede siempre escoger una base apropiada $\left\{\mid \tilde{0}\rangle, \mid \tilde{1}\rangle\right\}$ tal que

$$\mid \tilde{0}\rangle = \cos\theta \mid 0\rangle + \sin\theta \mid 1\rangle = \left[\begin{array}{c} C \\ S \end{array}\right], \quad (4.3.6)$$

$$\mid \tilde{1} > = \sin\theta \mid 0\rangle + \cos\theta \mid 1\rangle = \left[\begin{array}{c} S \\ C \end{array}\right], \quad (4.3.7)$$

donde definimos $C = \cos\theta$ y $S = \sin\theta$. Sin pérdida de generalidad se puede considerar $0 \leq \theta \leq \frac{\pi}{4}$. El producto interior de estos estados es en general distinto de cero y está dado por

$$< \tilde{0} \mid \widetilde{1} >= \sin 2\theta. \quad (4.3.8)$$

Las matrices densidad correspondientes a los estados $\mid \tilde{0}\rangle\ y\ \mid \tilde{1}\rangle$ son

$$\rho_0 = \mid \tilde{0}\rangle\langle\tilde{0} \mid = \left[\begin{array}{cc} C^2 & CS \\ CS & S^2 \end{array}\right], \quad (4.3.9)$$

$$\rho_1 = \mid \tilde{1}\rangle\langle\tilde{1} \mid = \left[\begin{array}{cc} C^2 & CS \\ CS & S^2 \end{array}\right]. \quad (4.3.10)$$

Si la fuente genera el estado $\mid \tilde{0} >$ con probabilidad p y el estado $\mid \tilde{1} >$ con probabilidad $1-p$, entonces la matriz densidad correspondiente es

$$\rho = p\rho_0 + (1-p)\rho_1 = \left[\begin{array}{cc} S^2 + p\, cos 2\theta & CS \\ CS & C^2 - p\, cos 2\theta \end{array}\right]. \quad (4.3.11)$$

Los valores propios de la matriz densidad están definidos por

$$\lambda_{\pm} = \frac{1}{2}\left(1 \pm \sqrt{1 + 4p(p-1)\, cos^2 2\theta}\right). \quad (4.3.12)$$

Entonces la entropía de Von Neumann se puede calcular como

$$S(\rho) = -\lambda_+ log\lambda_+ - \lambda_- log\lambda_-. \quad (4.3.13)$$

Para $\theta = 0$ los estados son ortogonales y los valores propios de la matriz densidad se definen por p y $1-p$, recuperando el caso anterior, por lo que $S(\rho) = H(p)$. Si $\theta = \frac{\pi}{4}$, entonces $S(\rho) = 0$. En este caso como los estados son idénticos no existe transmisión de información alguna. Para otros valores de θ los valores propios se repelen los unos a los otros.
Entonces, en el caso de tener una fuente de estados no ortogonales $S(\rho) \leq H(\rho)$. Si los estados son no ortogonales su similitud aumenta con el producto interior $< \tilde{0} \mid \widetilde{1} >= sin\, 2\theta$.

Por lo tanto, la ignorancia inicial de Bob del sistema es menor, y entonces obtiene menos información al recibir un mensaje tomado del ensamble $\left\{|\,\tilde{0}\rangle, |\,\tilde{1}\rangle\right\}$. En el caso límite donde $\theta = \frac{\pi}{4}$, la superposición de los estados tomados de $\left\{|\,\tilde{0}\rangle, |\,\tilde{1}\rangle\right\}$ es unitaria, esto significa que los estados son idénticos y por lo tanto no existe una ignorancia inicial acerca del sistema y entonces ninguna información es transmitida en este caso.

4.3.1. Compresión de datos cuánticos

Se puede realizar un extensión del teorema de codificación sin ruido de Shannon al caso cuántico. Suponiendo que Alice le envía a Bob un mensaje de n letras, donde cada letra fue seleccionada de manera aleatoria del ensamble $A = \{|\,\psi_1\rangle, |\,\psi_2\rangle, \ldots, |\,\psi_k\rangle\}$. El estado $|\,\psi_i\rangle$ es extraído con probabilidad p_i y $\sum_i p_i = 1$. Por lo tanto cada letra del mensaje esta descrita por la matriz densidad

$$\rho = \sum_{i=1}^{k} p_i \mid \psi_i\rangle\langle\psi_i \mid, \tag{4.3.14}$$

mientras que la matriz densidad de todo el mensaje está dada por

$$\rho^n = \rho^{\otimes n}, \tag{4.3.15}$$

donde $\rho^{\otimes n}$ denota el producto tensorial $\rho \otimes \rho \otimes \cdots \otimes \rho$. Por lo tanto todas las letras en este mensaje son estadísticamente independientes y descritas por la misma matriz densidad ρ. La extensión del teorema de Shannon (teorema cuántico de compresión sin ruido de Schumacher) dice que es posible comprimir un mensaje con una tasa de compresión óptima dada por la entropía de Von Neumann.

4.3.2. Teorema cuántico de compresión sin ruido de Schumacher

Dado un mensaje cuyas letras están compuestas por estado cuánticos puros tomados del ensamble $A = \{|\,\psi_1\rangle, |\,\psi_2\rangle, \ldots, |\,\psi_k\rangle\}$ con probabilidades de aparición $\{p_1, p_2, \ldots, p_k\}$, *existe una compresión optima y confiable* del mensaje con $S(\rho)$ qubits por letra, donde $\rho = \sum_{i=1}^{k} p_i \mid \psi_i\rangle\langle\psi_i \mid$.

Se puede describir la descomposición espectral de ρ como

$$\rho = \sum_{i=1}^{k} \lambda_i \mid a_i\rangle\langle a_i \mid . \tag{4.3.16}$$

En este caso $H(\lambda_1, \ldots, \lambda_k) = S(\rho)$. El ensamble $A' = \{|\,a_i\rangle, \ldots, |\,a_k\rangle\}$ constiyuye el alfabeto de estados cuánticos puros ortogonales.
Se define un estado $|\,x_1\rangle \otimes \cdots \otimes |\,x_n\rangle \in A$ como $\epsilon - \textit{típico}$ si:

$$\left| -\frac{1}{n} log\left[\lambda(x_i) \ldots \lambda(x_n) - S(\rho)\right] \right| < \epsilon, \tag{4.3.17}$$

donde $\lambda(x_i) = \lambda_j$ si $|\,x_i\rangle$ es la letra $|\,a_j\rangle$. Un subespacio $\varepsilon - \textit{típico}$ es el subespacio generado por los estados $\epsilon - \textit{típicos}$. La dimensión de este subespacio es aproximadamente $2^{nS(\rho)}$.

Si P_{tip} denota el proyector de este subespacio, entonces para cualquier $\delta > 0$ se tiene que $Tr\left(P_{tip}\rho^n\right) > 1-\delta$ con una n muy grande. Por lo tanto cuando n tiende a infinito la matriz densidad ρ^n recae en el subespacio típico de dimensión $2^{nS(\rho)}$. Un mensaje típico de n estados puede ser entonces codificado usando solo $nS\left(\rho\right)$ qubits.

4.3.3. Compresión de un mensaje de n qubits

Sea un alfabeto binario $A = \{\mid \psi_0\rangle, \mid \psi_1\rangle\}$, donde $\mid \psi_0\rangle = \mid \tilde{0}\rangle$ y $\mid \psi_1\rangle = \mid \tilde{1}\rangle$ son los qubits en las expresiones (4.3.6) y (4.3.7), respectivamente.
Suponiendo que Alice desea enviar un mensaje de n qubit a Bob

$$\mid \Psi_K\rangle = \mid \psi_{k_1}\rangle \otimes \mid \psi_{k_2}\rangle \otimes \cdots \otimes \mid \psi_{k_n}\rangle, \tag{4.3.18}$$

donde $K = \{k_1, k_2, \ldots, k_n\}$. Los estados $\mid \tilde{0}\rangle$ y $\mid \tilde{1}\rangle$ son tomados del alfabeto A con probabilidades p y $1-p$, respectivamente. Cualquier letra del mensaje $\mid \Psi_K\rangle$ pertenece al espacio de Hilbert

$$H^n = H^{\otimes n}, \tag{4.3.19}$$

donde H es el espacio de Hilbert para un solo qubit. Por lo tanto, H^n es de dimensión 2^n. Para cada qubit, se puede diagonalizar la matriz densidad

$$\rho = p \mid \tilde{0}\rangle\langle\tilde{0} \mid + (1-p) \mid \tilde{1}\rangle\langle\tilde{1} \mid \tag{4.3.20}$$

y a partir de esta diagonalización construir el subespacio típico. Un mensaje genérico $\mid \Psi_K\rangle$ puede ser descompuesto en una componente del subespacio típico (H_{tip}) y otra componente perteneciente al subespacio atípico (H_{atip}). Esto se puede escribir como

$$\mid \Psi_K\rangle = \alpha_K \mid \tau_K\rangle + \beta_K \mid \tau_K^{\perp}\rangle, \tag{4.3.21}$$

donde $\mid \tau_K\rangle \in (H_{tip})$ y $\mid \tau_K^{\perp}\rangle \in (H_{atip})$.
Para determinar si $\mid \Psi_K\rangle$ pertenece al subespacio típico o atípico Alice realiza una medición. Si pertenece al subespacio típico el mensaje es codificado y enviado a Bob. Entonces de acuerdo al teorema de Schumacher el subespacio típico tiene dimensión $2^{nS(\rho)}$, y solamente se necesitan $nS\left(\rho\right)$ qubits para codificarlo. Por otro lado, si $\mid \Psi_K\rangle$ pertenece al subespacio atípico, éste se sustituye por un estado de referencia $\mid R\rangle$ perteneciente al subespacio típico. Finalmente, Bob decodifica los $nS\left(\rho\right)$ recibidos y obtiene un estado descrito por la matriz densidad

$$\tilde{\rho}_K = \left|\alpha_K\right|^2 \mid \tau_K\rangle\langle\tau_K \mid + \left|\beta_K\right|^2 \mid R\rangle\langle R \mid . \tag{4.3.22}$$

Para determinar que tan confiable es la transmisión de información se puede medir la fidelidad F de la transmisión mediante la expresión

$$F = \langle\Psi_K \mid \tilde{\rho}_K \mid \Psi_K\rangle, \tag{4.3.23}$$

donde $0 \leq F \leq 1$. La máxima fidelidad ($F = 1$) es obtenida cuando el estado inicial y el estado final coinciden ($\tilde{\rho}_K = \mid \Psi_K\rangle\langle\Psi_K \mid$), mientras que F=0 cuando el estado inicial y el final son ortogonales. La fidelidad promedio $\overline{F}$ es obtenida después de promediar todos los posibles mensajes $\mid \Psi_K\rangle$, cada uno con probabilidad p_k:

$$\begin{aligned} \overline{F} &= \sum_k p_k \langle\Psi_K \mid \tilde{\rho}_K \mid \Psi_K\rangle, \\ &= \sum_k p_k \langle\Psi_K \mid \left(\left|\alpha_K\right|^2 \mid \tau_K\rangle\langle\tau_K \mid + \left|\beta_K\right|^2 \mid R\rangle\langle R \mid\right) \mid \Psi_K\rangle, \\ &= \sum_k p_k \left|\alpha_K\right|^4 + \sum_k p_k \left|\beta_K\right|^2 \left|\langle\Psi_k \mid R>\right|^2 . \end{aligned} \tag{4.3.24}$$

Schumacher demuestra que la fidelidad tiende a uno si $n \to \infty$. Esto significa que en este límite, los mensajes tienen un traslape unitario con el subespacio típico, por lo tanto podemos codificar únicamente el subespacio tipico y obtener de todas maneras una buena fidelidad.

Ejemplo: Compresión de un mensaje de dos qubits.

Sea A el alfabeto definido en la sección *4.3.3*. Donde los estados $\mid \tilde{0}\rangle$ y $\mid \tilde{1}\rangle$ son tomados del alfabeto A con probabilidades p y $1-p$ respectivamente. Alice genera un mensaje de dos qubits pero únicamente puede enviarle un qubit. Bob recibe este qubit y adivina que la segunda letra del mensaje es algún estado de referencia, en este caso será $\mid \tilde{0}\rangle$. Si se calcula en este momento las fidelidades $F_k = \left|\langle\psi_2 \mid \tilde{0}\rangle\right|^2$ de los 4 posibles mensajes donde $\mid \psi_2\rangle$ es el estado actual del segundo qubit, entonces

K	Mensaje	p_k	Opción de Bob	F_k
0	$\mid \tilde{0}\tilde{0}\rangle$	p^2	$\mid \tilde{0}\tilde{0}\rangle$	1
1	$\mid \tilde{0}\tilde{1}\rangle$	$p\,(1-p)$	$\mid \tilde{0}\tilde{0}\rangle$	$\sin^2 2\theta$
2	$\mid \tilde{1}\tilde{0}\rangle$	$p\,(1-p)$	$\mid \tilde{1}\tilde{0}\rangle$	1
3	$\mid \tilde{1}\tilde{1}\rangle$	$(1-p)^2$	$\mid \tilde{1}\tilde{0}\rangle$	$\sin^2 2\theta$

La fidelidad promedio se obtiene de

$$\overline{F} = \sum_k p_k F_k = p\cos^2 2\theta + \sin^2 2\theta, \tag{4.3.25}$$

para varios valores de θ. Cabe destacar que cuando $\theta = 0$ se obtiene el caso clásico (transmisión de estados ortogonales[3]). Se puede definir una fidelidad clásica $f_{c,k}$ que es igual a uno si el mensaje es transmitido correctamente (en la tabla dada se obtiene este resultado cuando $K = 0$ y $K = 2$) y es igual a cero en cualquier otro caso (en la tabla $K = 1$ y $K = 3$). Resulta que la fidelidad clásica promedio $\overline{f_c} = \sum_k p_k\, f_{c,k} = p$ es igual a la fidelidad cuántica para $\theta = 0$. Para el caso de $\theta \neq 0$ los estados no son ortogonales y por lo tanto la fidelidad es mayor (en este caso $F_1 = F_3 = sin^2 2\theta > 0$). En el caso límite $\theta = \frac{\pi}{4}$ los estados $\mid \tilde{0}\rangle$ y $\mid \tilde{1}\rangle$ coinciden y entonces $F = 1$ para cualquier valor de p. En este caso no se puede transmitir información, y los estados no pueden ser distinguidos.

[3]Desde el punto de vista de la teoría de la información la situación es clásica cuando la entropía de Von Neumann es igual a la entropía de Shannon.

Ejemplo: Compresión de un mensaje de tres qubits

Supongamos que ahora se quiere mandar un mensaje de tres qubits tomado del ensamble $\left\{\mid \tilde{0}\rangle, \mid \tilde{1}\rangle\right\}$ con probabilidades $\{p, 1-p\}$, donde $\mid \tilde{0}\rangle$ es generado con probabilidad $p \geq \frac{1}{2}$. En esta ocasión Alice solo puede enviar dos de los tres qubit del mensaje.
Cada letra del mensaje esta descrita por la matriz densidad $\rho = p \mid \tilde{0}\rangle\langle\tilde{0} \mid + (1-p) \mid \tilde{1}\rangle\langle\tilde{0}\tilde{1} \mid$ con valores propios dados por $\lambda_{\pm} = \frac{1}{2}\left(1 \pm \sqrt{1 + 4p\,(p-1)\,cos^2 2\theta}\right)$. Sus vectores propios están definidos por:

$$\mid \pm\rangle = \frac{1}{\sqrt{\left(\lambda_{\pm} + p\,cos2\theta - C^2\right)^2 + C^2 S^2}} \begin{bmatrix} \lambda_{\pm} p\,cos2\theta - C^2 \\ CS \end{bmatrix}, \tag{4.3.26}$$

donde $C = cos\theta$ y $S = sin\theta$. Para propósitos posteriores, como veremos más adelante, se escriben los productos internos

$$\langle\tilde{0} \mid \pm\rangle = \frac{C\left[\lambda_{\pm} + p\,cos2\theta - C^2\right] + CS^2}{\sqrt{N_{\pm}}}, \tag{4.3.27}$$

$$\langle\tilde{1} \mid \pm\rangle = \frac{S\left[\lambda_{\pm} + p\,cos2\theta - C^2\right] + CS^2}{\sqrt{N_{\pm}}}, \tag{4.3.28}$$

donde $N_{\pm} \equiv \left(\lambda_{\pm} + p\,cos2\theta - C^2\right)^2 + C^2 S^2$.
Sea el conjunto los kets $\{\mid \Psi_K > \; con\; k = 0, 1, 2, \ldots, 8\}$ los posibles mensajes que puede formar Alice

$$\begin{aligned} &\mid \Psi_0\rangle = \mid \tilde{0}\tilde{0}\tilde{0}\rangle, \mid \Psi_1\rangle = \mid \tilde{0}\tilde{0}\tilde{1}\rangle, \mid \Psi_2\rangle = \mid \tilde{0}\tilde{1}\tilde{0}\rangle, \mid \Psi_3\rangle = \mid \tilde{0}\tilde{1}\tilde{1}\rangle, \\ &\mid \Psi_4\rangle = \mid \tilde{1}\tilde{0}\tilde{0}\rangle, \mid \Psi_5\rangle = \mid \tilde{1}\tilde{0}\tilde{1}\rangle, \mid \Psi_6\rangle = \mid \tilde{1}\tilde{1}\tilde{0}\rangle, \mid \Psi_7\rangle = \mid \tilde{1}\tilde{1}\tilde{1}\rangle, \end{aligned} \tag{4.3.29}$$

que están caracterizadas por la distribución de probabilidades
$\left\{p^3, p^2\,(1-p), p^2\,(1-p), p\,(1-p)^2, p^2\,(1-p), p\,(1-p)^2, p\,(1-p)^2, (1-p)^3\right\}$.
Denotemos por el conjunto de kets $\{\mid X_J > \; con$ j=1,2,...,8$\}$ los vectores propios del sistema de tres qubits, i.e., de $p^{\otimes 3}$

$$\begin{aligned} &\mid X_0\rangle = \mid +++\rangle, \mid X_1\rangle = \mid ++-\rangle, \mid X_2\rangle = \mid +-+\rangle, \mid X_3\rangle = \mid +--\rangle, \\ &\mid X_4\rangle = \mid -++\rangle, \mid X_5\rangle = \mid -+-\rangle, \mid X_6\rangle = \mid --+\rangle, \mid X_7\rangle = \mid ---\rangle, \end{aligned} \tag{4.3.30}$$

donde $\mid +\rangle$ y $\mid -\rangle$ son los vectores propios de ρ.
Los estados $\{\mid X_J\rangle\}$ forman una base en el espacio de Hilbert formado por los tres qubits y entonces se puede descomponer cada uno de los mensajes posibles como

$$\mid \Psi_K\rangle = \sum_J c_{KJ} \mid X_J\rangle, \tag{4.3.31}$$

donde $c_{KJ} = \langle X_J \mid \Psi_k\rangle$.
Como $p > \frac{1}{2}$ entonces el peso λ_+ del vector propio $\mid +\rangle$ es mayor que el peso λ_- del vector propio $\mid -\rangle$, i.e, $\lambda_+ > \lambda_-$. Entonces el subespacio con mayor probabilidad está dado por los estados con mayor probabilidad

$$\mid X_0\rangle = \mid +++\rangle, \mid X_1\rangle = \mid ++-\rangle, \mid X_2\rangle = \mid +-+\rangle, \mid X_4\rangle = \mid -++\rangle. \tag{4.3.32}$$

Mientras que el subespacio menos probable está dado por

$$\mid X_3\rangle =\mid +--\rangle, \mid X_5\rangle =\mid -+-\rangle, \mid X_6\rangle =\mid --+\rangle, \mid X_7\rangle =\mid ---\rangle. \tag{4.3.33}$$

Como se vio anteriormente en 4.3.3 los estados $\mid \Psi_K\rangle$ pueden ser descompuestos en una componente típica $\mid \tau_K\rangle$ y en otra componente atípica $\mid \tau_K^{\perp}\rangle$, donde $\mid \Psi_K\rangle = \alpha_K \mid \tau_K\rangle + \beta_K \mid \tau_K^{\perp}\rangle$. Por medio de (4.3.31) es directo encontrar que los coeficientes α_K y β_K están dados por

$$\alpha_K = \sqrt{|c_{k0}|^2 + |c_{k1}|^2 + |c_{k2}|^2 + |c_{k4}|^2}, \tag{4.3.34}$$

$$\beta_K = \sqrt{|c_{k3}|^2 + |c_{k5}|^2 + |c_{k6}|^2 + |c_{k7}|^2}. \tag{4.3.35}$$

Para decodificar el mensaje, Alice realiza la estrategia siguiente. Primero aplica una transformación unitaria U que rota los estados base del subespacio típico o más probable a los estados $\mid i_1\rangle \mid i_2\rangle \mid 0\rangle$, con $i = 0, 1$. Mientras que los elementos del subespacio atípico son rotados a $\mid i_1\rangle \mid i_2\rangle \mid 1\rangle$. Posteriormente realiza una medición sobre el tercer qubit: si obtiene cero, entonces el estado $\mid \Psi_K\rangle$ ha sido proyectado en el subespacio típico. En este caso, Alice le envía los dos primeros qubits a Bob. Si de la medición Alice obtiene un uno, entonces el estado ha sido proyectado sobre el subespacio atípico y Alice le envia a Bob los dos primeros qubits de $U \mid R\rangle$, donde $\mid R\rangle$ es algún estado de referencia perteneciente al subespacio típico. Alice le da el valor del estado $\mid X_J\rangle$ más probable a $\mid R\rangle$, en este caso $\mid X_0\rangle$. A los dos qubits recibidos, Bob le agrega un qubit auxiliar preparado en el estado $\mid 0\rangle$. Posteriormente aplica U^{-1} a estos tres qubits y obtiene la matriz densidad (descrita en 4.3.3): $\tilde{\rho}_K = |\alpha_K|^2 \mid \tau_K\rangle\langle\tau_K \mid + |\beta_K|^2 \mid R\rangle\langle R \mid$. La fidelidad promedio viene dada por

$$\overline{F} = \sum_{k=0}^{7} p_k \langle \Psi_K \mid \tilde{\rho}_K \mid \Psi_K\rangle = \sum_{k=0}^{7} p_k \left(|\alpha_K|^4 + |\beta_K|^2 \left\{ |\langle \Psi_k \mid R\rangle|^2 \right\} \right), \tag{4.3.36}$$

donde p_k es la probabilidad de que el mensaje $\mid \Psi_K\rangle$ sea generado. Para $\theta = 0$, $\mid \tilde{0}\rangle =\mid 0\rangle$ y $\mid \tilde{1}\rangle =\mid 1\rangle$ que corresponde al caso clásico, el promedio de las fidelidades $\overline{f_c}$ es obtenido de realizar la suma de las probabilidades de todos los mensajes correctamente transmitidos

$$\overline{f_c} = p^3 + 3p^2 (1 - p) = 3p^2 - 2p^3. \tag{4.3.37}$$

Para $p = \frac{1}{2}$ se tiene que $\overline{f_c} = \frac{1}{2}$. En este caso todos los mensajes ocurren con la misma probabilidad y sólo 4 son correctamente transmitidos. La fidelidad promedio es entonces mayor a $\frac{1}{2}$ cuando $\theta > 0$. Esto se debe a que la ignorancia a priori de estados no ortogonales es menor que la de estados ortogonales. En el caso límite de $\theta = \frac{\pi}{4}$ los estados $\mid 0\rangle$ y $\mid 1\rangle$ coinciden , por lo que $\overline{F}\left(\frac{\pi}{4}\right)$=1, y no existe transmisión de información.

4.4. Información Accesible

Una vez que Alice es capaz de enviarle información codificada a Bob, ¿Qué tanta información puede ganar Bob del mensaje realizando mediciones sobre el estado cuántico recibido?. La dificultad de este problema radica en que estados cuánticos no ortogonales no pueden ser perfectamente distinguibles. Es necesario introducir nuevas definiciones para definir la

información accesible.

Se define la entropía conjunta de un par de variables aleatorias X y Y, con probabilidades $p(x)$ y $p(y)$, respectivamente, como

$$H(X,Y) = -\sum_{x,y} p(x,y) log\, p(x,y), \tag{4.4.1}$$

donde $p(x,y)$ es la probabilidad de que $X = x$ y $Y = y$.

La entropía condicional se define como

$$H(Y \mid X) = -\sum_{x,y} p(x,y)\, log\, p(y \mid x), \tag{4.4.2}$$

donde $p(y \mid x)$ denota la probabilidad de que la variable aleatoria Y tenga el valor y dado que la X resultó x. Recordando que la probabilidad condicional está dada por la relación

$$p(y \mid x) = \frac{p(x,y)}{p(x)},$$

puede demostrarse fácilmente que

$$H(Y \mid X) = H(X,Y) - H(X).$$

En forma semejante se obtiene

$$H(X \mid Y) = H(X,Y) - H(Y).$$

Entonces las entropías condicionales dadas en las expresiones anteriores dan una medida de la ignorancia de la variable Y (X) dado que sabemos el valor de X (Y).

La información mutua $I(X:Y)$ ayuda a medir cuánta información es compartida por X y Y, y está definida por

$$I(X:Y) \equiv H(X) + H(Y) - H(X,Y) = -\sum_{x,y} p(x,y)\, log \frac{p(x)p(y)}{p(x,y)}. \tag{4.4.3}$$

Si X y Y son independientes, esto es $p(x,y) = p(x)p(y)$, entonces $I(X:Y) = 0$. La información mutua está relacionada con la entropía condicional de la siguiente manera

$$I(X:Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X). \tag{4.4.4}$$

Se puede ver de (4.4.3) que la información mutua es simétrica

$$I(Y:X) = I(X:Y). \tag{4.4.5}$$

Si X y Y denotan variables aleatorias asociadas con las letras generadas por Alice y por las salidas de las mediciones realizadas por Bob, respectivamente, entonces la información accesible se encuentra definida como el máximo valor de $I(X:Y)$ sobre todos los posibles esquemas de medición.

4.4.1. Cota de Holevo

La cota de Holevo establece una cota superior para la cantidad de información accesible.

Si Alice prepara un estado mixto ρ_X tomado de un ensamble $A = \{\rho_1, \ldots, \rho_k\}$ con probabilidades a priori $\{p_1, \ldots, p_k\}$y Bob realiza una medición POVM sobre el estado, con elementos POVM $\{F_1, \ldots, F_l\}$y las salidas de las mediciones están escritas por la variable aleatoria Y, entonces la información mutua $I(X:Y)$ está acotada por

$$I(X:Y) \leq S(\rho) - \sum p_i S(\rho_i) \equiv \chi(\mathcal{E}), \tag{4.4.6}$$

donde $\rho = \sum_{i=1}^{k} p_i \rho_i$ y $\chi(\mathcal{E})$ es conocida como la información de Holevo del ensamble $\mathcal{E} \equiv \{\rho_1, \ldots, \rho_k; p1, \ldots, p_k\}$.

Ejemplo

Suponiendo que Alice le envía a Bob estados puros cuánticos ortogonales tomados del ensamble $\{\mid \psi_1\rangle, \ldots, \mid \psi_k\rangle\}$, entonces Bob podrá distinguir estos estados por medio de mediciones proyectivas descritas por elementos POVM $\{F_1 = \mid \psi_1\rangle\langle\psi_1 \mid, \ldots, F_k = \mid \psi_k\rangle\langle\psi_k \mid\}$. En este caso como los estados son puros ortogonales $I(X:Y) = H(X)$ ya que $H(X \mid Y) = 0$, por lo tanto este caso no es diferente al de transmisión de información clásica sobre un canal sin ruido. Esto significa que si se envía la letra a_x se recupera la misma letra , esto es $a_y = a_x$.
El ejemplo más simple que no puede reducirse a su caso clásico es cuando Alice le envía a Bob estados puros cuánticos no ortogonales. Sean $\mid \tilde{0} >$ y $\mid \tilde{1}\rangle$ como en la sección *4.3.3* generados con probabilidades $p_0 = p$ y $p_1 = 1 - p$ respectivamente. Como las letras son representadas en este caso por estados puros, la entropía de Von Neumann es $S(\rho_0) = S\left(\mid \tilde{0}\rangle\langle\tilde{0} \mid\right) = 0$ y $S(\rho_1) = S\left(\mid \tilde{1}\rangle\langle\tilde{1} \mid\right) = 0$. Por lo tanto la información de Holevo es reducida a

$$\mathcal{X}(\mathcal{E}) = S(\rho), \tag{4.4.7}$$

donde $\rho = p\rho_0 + (1-p)\rho_1$. Por lo tanto, la cota de Holevo nos da

$$I(X:Y) \leq S(\rho). \tag{4.4.8}$$

Suponiendo que Bob realiza una medición proyectiva sobre los qubits recibidos a lo largo de la dirección $\hat{n}$, esto significa que Bob mide $\hat{n} \cdot \sigma$, en ete caso la cota de Holevo es satisfecha. La medición de Bob a lo largo de la dirección $\hat{n}$ está descrita por los elementos o proyectores POVM

$$F_0 = \frac{1}{2}(I + \hat{n} \cdot \sigma) \qquad F_0 = \frac{1}{2}(I - \hat{n} \cdot \sigma). \tag{4.4.9}$$

Si $\hat{n} = (0,0,1)$,entonces $F_0 = \mid 0\rangle\langle 0 \mid$ y $F_0 = \mid 1\rangle\langle 1 \mid$. Se calcula la probabilidad condicional

$$p(y \mid x) = Tr(\rho_x F_y), \qquad (x, y = 0, 1), \tag{4.4.10}$$

que es la probabilidad de que Bob mida y dado el estado ρ_x enviado por Alice. Se puede escribir la representación de Bloch de las matrices densidad asociadas con los estados $\mid \tilde{0}\rangle$ y

$\mid \tilde{1}\rangle$ (*Ver 4.1.2*)

$$\rho_0 = \mid \tilde{0}\rangle\langle\tilde{0} \mid = \frac{1}{2}\left(I + \hat{r}_0 \cdot \bar{\sigma}\right), \tag{4.4.11}$$

$$\rho_1 = \mid \tilde{1}\rangle\langle\tilde{1} \mid = \frac{1}{2}\left(I + \hat{r}_1 \cdot \bar{\sigma}\right), \tag{4.4.12}$$

donde las componentes cartesianas del vector de Bloch $\hat{r}_0$ y $\hat{r}_1$ están dadas por

$$\hat{r}_0 = \left(\sin 2\theta, 0, \cos 2\theta\right), \tag{4.4.13}$$

$$\hat{r}_1 = \left(\sin 2\theta, 0, -\cos 2\theta\right). \tag{4.4.14}$$

Recordando que $Tr\left(\sigma_i\right) = 0$ y $Tr\left(\sigma_i\sigma_j\right) = 2\delta_{i,j}$ para $i, j = x, y, z$. Se pueden ahora calcular las probabilidades condicionales

$$p\left(0 \mid 0\right) = Tr\left(\rho_0 F_0\right) = \frac{1}{2}\left(I + \hat{r}_0 \cdot \hat{n}\right), \tag{4.4.15}$$

$$p\left(1 \mid 0\right) = Tr\left(\rho_0 F_1\right) = \frac{1}{2}\left(I - \hat{r}_0 \cdot \hat{n}\right), \tag{4.4.16}$$

$$p\left(0 \mid 1\right) = Tr\left(\rho_1 F_0\right) = \frac{1}{2}\left(I + \hat{r}_1 \cdot \hat{n}\right), \tag{4.4.17}$$

$$p\left(1 \mid 1\right) = Tr\left(\rho_1 F_1\right) = \frac{1}{2}\left(I - \hat{r}_1 \cdot \hat{n}\right). \tag{4.4.18}$$

Supongamos que la dirección de la medición cae en el plano (x, z) de la esfera de Bloch, entonces $\hat{n} = \left(sin\overline{\theta}, 0, cos\overline{\theta}\right)$ y se tiene

$$p\left(0 \mid 0\right) = \frac{1}{2}\left[1 + \cos\left(\overline{\theta} - 2\theta\right)\right], \tag{4.4.19}$$

$$p\left(1 \mid 0\right) = \frac{1}{2}\left[1 - \cos\left(\overline{\theta} - 2\theta\right)\right], \tag{4.4.20}$$

$$p\left(0 \mid 1\right) = \frac{1}{2}\left[1 - \cos\left(\overline{\theta} + 2\theta\right)\right], \tag{4.4.21}$$

$$p\left(1 \mid 1\right) = \frac{1}{2}\left[1 + \cos\left(\overline{\theta} + 2\theta\right)\right]. \tag{4.4.22}$$

Se puede ahora calcular $p\left(x, y\right) = p\left(x\right)p\left(y \mid x\right)$ donde como se vio al inicio del ejemplo $p\left(X = 0\right) = p$ y $p\left(X = 1\right) = 1 - p$. Por lo tanto

$$p\left(0, 0\right) = \frac{1}{2}p\left[1 + \cos\left(\overline{\theta} - 2\theta\right)\right], \tag{4.4.23}$$

$$p\left(0, 1\right) = \frac{1}{2}p\left[1 - \cos\left(\overline{\theta} - 2\theta\right)\right], \tag{4.4.24}$$

$$p\left(1, 0\right) = \frac{1}{2}\left(1 - p\right)\left[1 - \cos\left(\overline{\theta} + 2\theta\right)\right], \tag{4.4.25}$$

$$p\left(1, 1\right) = \frac{1}{2}\left(1 - p\right)\left[1 + \cos\left(\overline{\theta} + 2\theta\right)\right]. \tag{4.4.26}$$

De la misma manera podemos calcular $p(y) = \sum_x p(x, y)$

$$p(Y = 0) = \frac{1}{2}\left[1 + p\cos\left(\overline{\theta} - 2\theta\right) - (1 - p)\cos\left(\overline{\theta} + 2\theta\right)\right], \tag{4.4.27}$$

$$p(Y = 1) = \frac{1}{2}\left[1 - p\cos\left(\overline{\theta} - 2\theta\right) + (1 - p)\cos\left(\overline{\theta} + 2\theta\right)\right] \tag{4.4.28}$$

Se pueden insertar ahora las expresiones $p(x)$, $p(y)$ y $p(x, y)$ en la ecuación 4.4.3 y obtener la información mutua $I(X : Y)$. Si fijamos $\theta = \frac{\pi}{10}$ y $p = 0.8$ podemos obtener la información mutua $I(X : Y)$. El parámetro a variar en este caso para maximizar I es $\overline{\theta}$. Se puede ver en la figura **??** que el valor máximo $I_{max} = max_{\overline{\theta}} I(\theta) = 0.4$. Este valor se encuentra por debajo de la cota de Holevo $\mathcal{X} = S(\rho) \approx 0.526$. En el apéndice B se encuentra un programa en Mathematica que efectúa los calculos mencionados y permite hacer la gráfica mencionada.

El costo de la codificación de información cuántica por un factor $S < H$ radica en la capacidad de Bob de reconstruir el estado cuántico enviado por Alice, pero debido a que este estado es tomado de una fuente de estados no ortogonales, no existe una confiabilidad perfecta en la reconstrucción del estado. Aún así la compresión de información cuántica podría ser usada en la memoria de una computadora cuántica o en la transferencia comprimida de información cuántica entre procesadores cuánticos.

Conclusiones

La teoría de la información cuántica introduce nuevas formas de procesar y comunicar información a tráves de herramientas cuánticas. Para empezar a trabajar en la teoría de la información cuántica es necesario entender sus bases. Estas bases son fundamentalmente la mecánica cuántica y la computación clásica.
En el primer capítulo se vieron las herramientas matemáticas necesarias (espacios de Hilbert, operadores, productos tensoriales, etc.) para empezar a trabajar con la mecánica cuántica. Una vez que se conocen estas herramientas es conveniente también entender los postulados que rigen los comportamientos de la naturaleza. Una de las características con las que se trabaja en la teoría de la información cuántica es el entrelazamiento, una propiedad única del formalismo cuántico que permite correlacionar las propiedades de un sistema A con las de un sistema B, inclusive si se encuentran espacialmente separados. Existen maneras de cuantificar la cantidad de entrelazamiento entre dos sistemas, una pequeña introducción de estas cuantificaciones es vista en el capítulo 1. Esta característica es aprovechada por Ekert en la teoría de la información ya que podemos conocer la correlación entre dos estados y realizar comunicación cuántica.
Al igual que en la computación clásica la computación cuántica sugiere una unidad mínima y elemental de información llamada bit cuántico o qubit, para conocer el valor de un qubit es necesario realizar una medición sobre el estado del qubit que cumple con los postulados vistos en el capítulo 1. Un qubit puede ser representado en la esfera de Bloch, donde cada punto de la esfera representa un estado del espacio de Hilbert. En computación clásica para realizar algún cálculo o cómputo es necesario un estado inicial, un estado final y un conjunto de operaciones que actúen sobre el estado inicial. Similarmente en computación cuántica es necesario definir un estado inicial, operar el estado inicial a través de transformaciones unitarias y finalmente realizar una medición sobre una base apropiada. Estas transformaciones unitarias son conocidas computacionalmente como compuertas cuánticas y operan sobre uno o más qubits, al contrario que en la mayoría de las compuertas clásicas, estas compuertas son reversibles. Las compuertas básicas en computación cuántica son: compuerta de Hadamard, compuerta de corrimiento de fase, rotación, CNOT, CPHASE, Toffoli y $C^k - U$ (las 3 primeras son compuertas de un qubit). De manera general se demostró que cualquier transformación unitaria puede descomponerse en una secuencia de compuertas de 1-qubit y de CNOT´s. De manera conjunta estas compuertas cuánticas (junto con otras herramientas matemáticas) puede ayudarnos a construir algoritmos cuánticos.
El algoritmo de Deutsch, un algoritmo de decisión que ayuda a determinar si una función lógica de dos qubits se encuentra balanceada o no. La generalización del algoritmo de Deutsch resuelve la misma interrogante para una función con múltiples valores de entrada.

El algoritmo de Shor resuelve el problema de factorización, utilizando teoría de números, la superposición de estados cuánticos y la transformada cuántica de Fourier, Shor utiliza elementos del algoritmo clásico y lo complementa con elementos cuánticos para descomponer un número N en sus factores primos. Cabe destacar que Shor resuelve el problema de factorización en un tiempo mucho menor que el mejor algoritmo clásico conocido para resolver este problema por lo que pone en entredicho a todos los sistemas que basan su seguridad en el principio de factorización de números muy grandes.
El algoritmo de Grover es un algoritmo cuántico de búsqueda que encuentra un elemento dado en una lista no estructurada de tamaño N utilizando compuertas cuánticas y técnicas de aumento de amplitudes de probabilidad para poder realizar la medición correcta. Al igual que Shor, Grover resuelve este problema de manera más rápida que su contraparte clásica.
Existen además otros algoritmos cuánticos que no fueron considerados en el presente trabajo como: Algoritmos para la estimación de valores propios cuánticos, algoritmos para encontrar logaritmos discretos (M. Mosca, "Quantum Computer Algorithms"), algoritmos para estimar la media de un conjunto de valores (Grover 1998), algoritmos para resolver sistemas de ecuaciones lineales (Seth Lloyd et al, "Quantum algorithm for linear systems of equations") y algoritmos más avanzados que sirven para encontrar subgrupos específicos en un grupo dado.

La complejidad de los algoritmos presentados en el trabajo se pueden resumir en la siguiente tabla:

Problemas	Complejidad Clásica	Complejidad Cuántica
Factorización	$O\left(e^{(logN)^{1/3}(log\,logN)^{2/3}}\right)$	$O\left((log\,N)^3\right)$
Búsqueda	$O\left(N\right)$	$O\left(\sqrt{N}\right)$
Decisión	$\Theta\left(N\right)$	$\Theta\left(\sqrt{N}\right)$

Esto demuestra que un mismo problema puede tener distintos grados de complejidad en la computación cuántica y en la computación clásica. Dando lugar a nuevas clases de complejidad, por ejemplo, la clase BQP (Bounded error, Quantum, Polinomial Time) es el conjunto de todos los lenguajes aceptados por una máquina de Turing Cuántica en tiempo polinomial con una probabilidad de error acotada. Varios de los problemas computacionales más interesantes en las ciencias de la computación, como la factorización y la búsqueda algorítmica, pertenecen a BQP (y probablemente estén fuera de la complejidad polinomial P). Al finalizar el capítulo 2 se dio una pequeña discusión acerca de la universalidad de la Máquina de Turing Cuántica propuesta por Deutsch en 1985. La máquina propuesta por Deutsch es una reinterpretación de la Máquina Universal de Turing clásica para sistemas físicos, en este caso un sistema cuántico. Resulta que la máquina universal cuántica propuesta por Deutsch no es realmente universal. Es importante resaltar que la definición de universalidad es diferente para máquinas cuánticas que para máquinas clásicas.
Un sistema de procesamiento de información cuántica no solamente puede realizar cálculos numéricos de manera más eficiente que una computadora clásica sino que también permite el establecimiento de protocolos de comunicación cuántica. La comunicación cuántica es

quizá el área con mayor interés y avances desarrollados en los últimos años (Capítulo 3). Este interés se ha dado gracias a una de las propiedades más interesantes de la mecánica cuántica, el teorema de la no clonación, que garantiza que ningún estado cuántico puede ser copiado en su totalidad. En base a este resultado surgen varios protocolos de criptografía que garantizan la seguridad de transmisión de información cuántica. Es el caso del protocolo BB84 que realiza una distribución segura de llaves cuánticas con ayuda de 4 estados y dos alfabetos (bases) entre un receptor (Bob) y un transmisor (Alice), la mecánica cuántica garantiza la seguridad de esta llave. La generalización del protocolo BB84 está dada por el protocolo B92 que trabaja con diferentes bases de codificación y diferentes estados. Otro protocolo importante en la criptografía cuántica es el protocolo de Ekert que es capaz de generar una llave cuántica secreta aprovechando el entrelazamiento de estados cuánticos para saber si el mensaje fue interceptado o perturbado por ruido externo.
Otro tipo de transmisión de información cuántica es el codificado denso, este proceso tiene la capacidad de poder enviar dos bits de información clásica en un solo bit cuántico. Este proceso se basa de igual manera en el entrelazamiento de estados cuánticos, su seguridad radica en que si un intruso accede a la información del sistema, la única manera de acceder a ella sería midiendo el par EPR, colapsando el sistema y advirtiendo a Alice y Bob del intruso.
El proceso que más llama la atención en la comunicación cuántica es el fenómeno de teleportación. Este proceso es capaz de transmitir información cuántica entre dos entidades inclusive si estas se encuentran separadas espacialmente, algo inimaginable en la comunicación clásica. Este fenómeno aprovecha estados entrelazados compartidos por Alice y Bob. El mensaje a transmitir junto con la mitad del estado compartido perteneciente a Alice es operado (por una transformación unitaria) y medido: obteniéndose dos bits clásicos, en este momento debido al fenómeno de entrelazamiento Bob comparte la información del mensaje que Alice le deseaba compartir. En ningún momento se realiza una copia del qubit transmitido por lo que ningún resultado de la mecánica cuántica es violado. Por lo tanto la codificación y la transmisión segura de datos cuánticos a través de canales cuánticos es posible. Además, resulta que esta información transmitida puede ser comprimida de manera óptima y confiable (Capítulo 4). Para entender el proceso de compresión cuántica fue necesario definir una nueva forma de representación de los estados cuánticos (en este caso estados mixtos). Estos estados mixtos, descritos por una distribución de probabilidad, pueden representarse en términos de operadores (operadores densidad) y ser asociados a una representación matricial conocida como matriz densidad. La ventaja de el operador densidad es que puede describir estados puros y mixtos. La matriz densidad puede ayudarnos a realizar una aproximación de un copiado cuántico. Buzek y Hillery propusieron una transformación unitaria que realiza un clonado imperfecto de un estado dado. Se encontró que la fidelidad de esta máquina de copiado puede llegar a ser de hasta 0.833333 que es la máxima fidelidad posible de una máquina copiadora cuántica, para ese número de entradas y salidas. Este resultado nos sugiere que puede ser mejorado el rendimiento de las mediciones , si estas mediciones son realizadas sobre las copias del sistema cuántico original. La compresión de información clásica viene dada por el teorema de codificación sin ruido de Shannon que encuentra una compresión óptima y fiable de un mensaje dado con una tasa de compresión dada por la entropía de Shannon. La versión cuántica de este teorema está dada por el teorema de codificación sin ruido de Schumacher, que define una

tasa de compresión óptima (dada por la entropía de Von Neuman) de un mensaje cuántico. Resulta que si dos estados cuánticos son ortogonales (estos estados forman un bit cuántico de información) la entropía de Von Neuman es idéntica a la entropía de Shannon debido a que los estados ortogonales son perfectamente distinguibles. Esto no es cierto si los estados con los que genero el qubit no son ortogonales. Para este caso la entropía de Von Neumann es menor o igual a la entropía de Shannon.

¿Qué falta por realizar? Atacar los problemas como la decoherencia y la corrección de errores para poder lograr un modelo de procesamiento de información cuántica robusto y seguro.
La teoría nos indica que en principio se puede construir un dispositivo capaz de realzar operaciones cuánticas, utilizando inclusive una cantidad polinomial de recursos, con una cota de error dada por cada operación utilizada o por ruido encontrado en el canal cuántico. Además, desafortunadamente cuando un sistema cuántico interactúa con el medio ambiente las superposiciones pueden ser perdidas y entonces la pérdida de información es posible; este fenómeno se conoce como decoherencia. Existen métodos que se enfocan específicamente en la corrección de errores cuánticos, tales como los códigos CSS (Calderbak-Shor-Stean) [76, 77, 78] , los códigos de Hamming, el código de intercambio de bits (o de fase) de 3 qubits [80], el código de 9 qubits de Shor [79], que nos ayudan a disminuir el valor de esta cota.
Estas técnicas de corrección de errores cuánticos también ayudan a entender los requerimientos necesarios para construir computadoras cuánticas. Modelos como el de Resonancia Magnética Nuclear (RMN) donde se pueden controlar operaciones cuánticas lógicas sobre sistemas de qubits (espín-nuclear $1/2$) de moléculas en solución utilizando campos magnéticos estáticos y oscilantes simultáneamente. Esta técnica a permitido demostrar experimentalmente algoritmos cuánticos de hasta 7-qubits y un número de compuertas cuánticas de hasta $O\left(10^2\right)$. Existen además otros métodos como el de cavidades cuánticas electromagnéticas que permiten la interacción entre átomos y fotones individuales dentro de una cavidad de resonancia o el modelo de la trampa de iones que permite tener una cadena de iones en una posición controlada y cada uno de los iones en una dirección dada por pulsos de láser; este método tiene la ventaja de tomar el progreso experimental realizado en la óptica cuántica.

La teoría de la información cuántica es un nuevo paradigma computacional, que cambia nuestra forma trabajar en las ciencias de la computación (Análisis de Algoritmos, Teoría de la Computación, Complejidad Computacional, Criptografía, etc.) y requiere de un trabajo interdisciplinario de la mano de físicos y matemáticos. Además de la eficiencia y rapidez de los algoritmos descritos en el presente trabajo aún existe la interrogante del límite real de una computadora cuántica. El principal reto radica en crear nuevas técnicas (algoritmos, procesos y hardware) capaces de adaptarse a la teoría de la información cuántica.
Se debe de entender a una computadora como cualquier sistema físico capaz de procesar y almacenar información, este sistema no necesariamente tiene que hacerlo como una computadora clásica, esto incluye átomos y moléculas.

> "Casi cualquier cosa se convierte en un ordenador si se le alumbra con el tipo correcto de luz[4]".

[4] Seth Lloyd en "The Computational Universe".

Apéndice A

Cálculo de la fidelidad para la máquina copiadora

```
D1[θ1_,θ2_,θ3_] := Cos[θ1] Cos[θ2]Cos[θ3] - Sin[θ1] Sin[θ2]Sin[θ3]

D2[θ1_,θ2_,θ3_] := -Cos[θ1] Sin[θ2]Sin[θ3] - Sin[θ1] Cos[θ2]Cos[θ3]

D3[θ1_,θ2_,θ3_] :=- Cos[θ1] Cos[θ2]Sin[θ3] - Sin[θ1] Sin[θ2]Cos[θ3]

D4[θ1_,θ2_,θ3_] := -Cos[θ1] Sin[θ2]Cos[θ3] + Sin[θ1] Cos[θ2]Sin[θ3]

Fidelity[α_,β_,θ1_,θ2_,θ3_] :=( 1- 2 Abs[α]^2 Abs[β]^2) ( D1[θ1,θ2,θ3]^2+ D4[θ1,θ2,θ3]^2)
+  2 Abs[α]^2 Abs[β]^2 (D2[θ1,θ2,θ3]^2 + D3[θ1,θ2,θ3]^2 + 2 D4[θ1,θ2,θ3] D1[θ1,θ2,θ3])
 + 2( α^2 Conjugate[β]^2 + β^2 Conjugate[α]^2) D3[θ1,θ2,θ3] D2[θ1,θ2,θ3]
```

In[6]:=
```
s1=Solve[Cos[2 θ1]== 1/Sqrt[5],θ1];

s2=Solve[Cos[2 θ2]== Sqrt[5]/3,θ2];

s3=Solve[Cos[2 θ3]== 2/Sqrt[5],θ3];
```

In[9]:=
```
Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[1,1,2]],θ2→ s2[[1,1,2]],θ3→s3[[1,1,2]]};
N[FullSimplify[%]]
```

Out[10]=
```
0.833333
```

Si realizamos los cálculos con el resto de todas las posibles soluciones $s1$, $s2$ y $s3$ se obtiene:

```
In[12]:= Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[2,1,2]],θ2→ s2[[2,1,2]],θ3→s3[[2,1,2]]};
         N[FullSimplify[%]]
         Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[1,1,2]],θ2→ s2[[1,1,2]],θ3→s3[[2,1,2]]};
         N[FullSimplify[%]]
         Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[1,1,2]],θ2→ s2[[2,1,2]],θ3→s3[[1,1,2]]};
         N[FullSimplify[%]]
         Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[2,1,2]],θ2→ s2[[1,1,2]],θ3→s3[[1,1,2]]};
         N[FullSimplify[%]]
         Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[2,1,2]],θ2→ s2[[2,1,2]],θ3→s3[[1,1,2]]};
         N[FullSimplify[%]]
         Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[2,1,2]],θ2→ s2[[1,1,2]],θ3→s3[[2,1,2]]};
         N[FullSimplify[%]]
         Fidelity[α,β,θ1,θ2,θ3]  /. {θ1→ s1[[1,1,2]],θ2→ s2[[2,1,2]],θ3→s3[[2,1,2]]};
         N[FullSimplify[%]]

Out[13]= 0.0333333 (17. + 12. (β Conjugate[α] - 1. α Conjugate[β])^2)

Out[15]= 0.0333333 (17. - 12. β^2 Conjugate[α]^2 + 8. α β Conjugate[α] Conjugate[β] - 12. α^2 Conjugate[β]^2)

Out[17]= 0.0333333 (17. + 12. (β Conjugate[α] - 1. α Conjugate[β])^2)

Out[19]= 0.0333333 (17. - 12. β^2 Conjugate[α]^2 + 8. α β Conjugate[α] Conjugate[β] - 12. α^2 Conjugate[β]^2)

Out[21]= 0.833333 - 2.66667 α β Conjugate[α] Conjugate[β]

Out[23]= 0.833333

Out[25]= 0.833333 - 2.66667 α β Conjugate[α] Conjugate[β]
```

Resumiendo, entonces notamos que en dos combinaciones se puede obtiene la máxima fidelidad esperada de la máquina copiadora $(0.833333) = \frac{5}{6}$.

Apéndice B

Cálculo de la Información Mutua

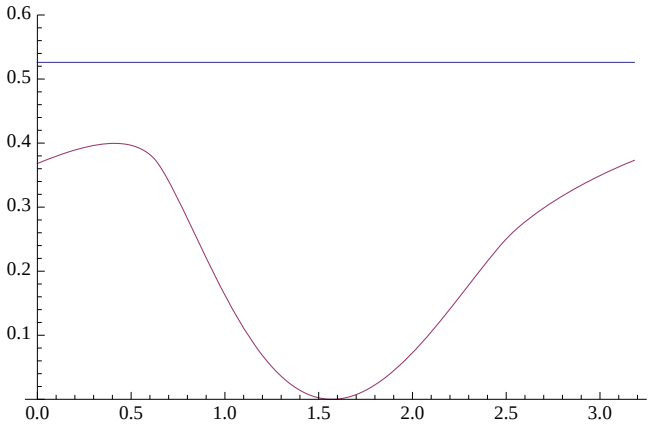
```
(*Se definen los vectores r0, r1 y n0*)

r0[θ_] := {Sin[2 θ], 0, Cos[2 θ]}
r1[θ_] := {Sin[2 θ], 0, -Cos[2 θ]}
n0[θb_] := {Sin[θb], 0, Cos[θb]}
sigma = {σx, σy, σz};
```

```
{r0[x].sigma, r1[x].sigma, n0[x].sigma}
```

```
{σz Cos[2 x] + σx Sin[2 x], -σz Cos[2 x] + σx Sin[2 x], σz Cos[x] + σx Sin[x]}
```

```
(*Se describen las coordenadas obtenidas en {r0[x].sigma,r1[x].sigma,n0[x].sigma}*)

R00[x_] := {{Cos[2 x], Sin[2 x]}, {Sin[2 x], -Cos[2 x]}}
R11[x_] := {{-Cos[2 x], Sin[2 x]}, {Sin[2 x], Cos[2 x]}}
nn[x_] := {{Cos[x], Sin[ x]}, {Sin[ x], -Cos[x]}}

(*Cá lculode las matrices densidad asociadas a los estados 0 y 1*)
ϱ0[x_] := 1/2 (IdentityMatrix[2] + R00[x])

ϱ1[x_] := 1/2 (IdentityMatrix[2] + R11[x])
(*Cá lculode los proyectores F0 y F1*)
F0[x_] := 1/2 (IdentityMatrix[2] + nn[x])

F1[x_] := 1/2 (IdentityMatrix[2] - nn[x])

(* Se obtienen las probabilidades condicionales
  y se deinen las probabilidades de que X=0 y X=1 *)

p[0, 0] = FullSimplify[Tr[ϱ0[x] . F0[y]]];
p[0, 1] = FullSimplify[Tr[ϱ1[x] . F0[y]]];
p[1, 0] = FullSimplify[Tr[ϱ0[x] . F1[y]]];
p[1, 1] = FullSimplify[Tr[ϱ1[x] . F1[y]]];
pX[0] = p;
pX[1] = 1 - p;
```

```
(*Se pueden obtener entonces las probabilidades p(x,y)=p(x)p(y|x)*)

pnew[0, 0] = pX[0] p[0, 0];
pnew[0, 1] = pX[0] p[1, 0];
pnew[1, 0] = pX[1] p[0, 1];
pnew[1, 1] = pX[1] p[1, 1];

(* De la misma manera se puede obtener p(y)=∑□x=□p(x,y)*)

pY[0] = Sum[pnew[k, 0], {k, 0, 1}];
pY[1] = Sum[pnew[k, 1], {k, 0, 1}];

(* Obtenemos entonces I(X:Y)=-∑□x,y=□log (p(x)p(y)/p(x,y)))*)
InfM[θb_] := N[-Sum[
     pnew[k1, k2] Log[2, pX[k1] pY[k2] / pnew[k1, k2]] /. {p → 0.8, x → π/10, y → θb}, {k1, 0, 1}, {k2, 0, 1}]]

FindMaximum[InfM[z], z]

{0.399555, {z → 0.411088}}

Plot[{0.526, InfM[z]}, {z, 0, 10/π}, PlotRange → {0, 0.6}]
```



Bibliografía

[1] http://qubit.nist.gov/

[2] http://www.iontrap.umd.edu/

[3] http://www.eng.yale.edu/rslab/

[4] Sansone, G. "*Elementary Notions of Hilbert Space.*" §1.3 in Orthogonal Functions, rev. English ed. New York: Dover, pp. 5-10, 1991.

[5] C. Cohen-Tannoudji, B. Liu and F. Laloe, *"Quantum Mechanics"*, Vol I, 1977.

[6] G. Abal, R. Siri, *"Introducción al procesamiento cuántico de la información"*, Instituto de Física, Facultad de Ingeniería Universidad de la República.

[7] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight Optics Section, ,"*Quantifying Entanglement"*, American Physical Society, p. 2275–2279, 1997.

[8] D. Yang, M. Horodecki, R. Horodecki and B. Synak-Radtke, Phys. Rev. Lett. 95, 190501 (2005).

[9] E. Geva. *"The Postulates of Quantum Mechanics"*, Univesrity of Michigan, Lecture Notes.

[10] N. David Mermin, *"Quantum Computer Science, An Introduction"*, Cabridge University Press, 2007.

[11] D. McMahon, *"Quantum Computer Explained"*, Wiley-InterScience. 2008.

[12] B. Giulio Casati, G Strini., *"Principles of Quantum Computation and Information Vol. 1"*, World Scientific, 2004.

[13] D. Cohen, *"Lecture Notes in Quantum Mechanics"*, quant-ph/0605180v3, 2006.

[14] P Kaye, R. Laflamme, M. Mosca, *"An Introduction to Quantum Computing"*, Oxford Univesrity Pres, 2007.

[15] V. K. Thankappan, *"Quantum Mechanics"* , Wiley Eastern Ltd, 1996.

[16] M. Nielsen, I. Chuang, *"Quantum Computation and Quantum Information"*, Cabridge University Press, 2000.

[17] Y. Peleg, R. Pnini, E. Zaarur, *"Theory and problems of Quantum Mechanics"*, Shaum´s Outline Series, 1998.

[18] H. Levitt, *"Spin Dynmaics"*, Wiley and Sons Ltd., 2008.

[19] Young, Thomas, *"Experiments and Calculations Relative to Physical Optics"*, Abstracts of the Papers Printed in the Philosophical Transactions of the Royal Society of London, Volume 1, pp. 131-132.

[20] M. Horodecki, P. Horodecki, R. Horodecki, *"Separability of Mixed States: Necessary and Sufficient Conditions"*, Physics Letters A 223, 1-8 (1996)

[21] J. F. Clauser, M.A. Horne, A. Shimony and R. A. Holt, *"Proposed experiment to test local hidden-variable theories"*, Phys. Rev. Lett. 23, 880-884 (1969).

[22] Eleanor G Rieffel, Wolfgang Polak, *"An Introduction to Quantum Computing for Non-Physicists",* FX Palo Alto Labratory, *arXiv:quant-ph/9809016v2* .

[23] P. Kaye, R. Laflame, M. Mosca, *"An Introduction to Quantum Computing",* Oxford University Press (2007).

[24] E. E. Rosinger, *"Basics of Quantum Computation (Part 1)",* University of Pretoria, arXiv:quant-ph/0407064v1.

[25] W. Fouché, J. Heidema, G. Jones, *"Deutsch´s Universal Quantum Turing Machine (Revisted)",* arXiv:quant-ph/0701108v1.

[26] D. Deutsch, *"Quantum Theory, The Church-Turing principle and the universal quantum computing",* Proceeds of the Royal Society of London, 400, pp. 97-117 (1985).

[27] Feymann, R. P, *"The Feymann Lectures on Computation",* Addison-Wesley. (1996).

[28] N. David Mermin, *"From Cbits to Qbits: Teaching computer scientists quantum mechanics",* Cornell Univesity, arXIv:quant-ph/0207118v1.

[29] G. Abal, R. Siri, *"Introducción al procesamiento cuántico de la información".* Universidad de la República (2005).

[30] C. Zalka, *"Introduction to Quantum Computers and Quantum Algortihms",* University of Waterloo, arXiv:quant-ph/0305053v1.

[31] A.Ekert,R. Jozsa. *"Quantum Computation and Shor´s Factorithm Algorithm, Review of Modern Phiscs*", 68, (1996) 733-753.

[32] P.W. Shor, *"Algorithms for quantum computation: discrete logarithms and factoring". Proc 35th Ann. Sym. on found of Comp. Sci.*, (1994) 124-134.

[33] M. A. Nielsen y I. L. Chuang, Physics Review Letters 79, 321 (1997).

[34] Yu Shi, *"Remarks on Universal Quantum Computers"* , Physics Letters A Volume 293, Issues 5-6, 4 February 2002, Pages 277-282

[35] Berstein, Vazirani. *"Quantum Complexity Theory",* Proceedings of the 25th Annual ACM Symposium on Theory of Computing.

[36] M. Ozawa, *"Quantum Turing Machines: Local Transition, Preparation, Measurement, and Halting",* Nagoya University, quant-ph/9809038v1, 1998.

[37] N. David Nermin, *"Lecture Notes on Quantum Computation"*, Cornell University, Physics 481-681; CS 483, 2005 & 2006.

[38] Valerio Scarani, *"Quantum Computing",* Institut de Physique Expérimentale, Ecole Polytechnique Fédérale, quant-ph/9804044v2, 1998.

[39] N. David Nermin, *"Quantum Computer Science, An Introduction"*, Cabridge University Press, 2007.

[40] D. McMahon, *"Quantum Computer Explained"*, Wiley-InterScience. 2008.

[41] B. Giulio Casati, G. Strini., *"Principles of Quantum Computation and Information Vol. 1"*, World Scientific, 2004.

[42] R. Feynman, *"The Feynman Lectures on Computation"*, edited by A. J. G. Hey and R. W. Allen (Reading, MA: Addison-Wesley), 1996.

[43] Burt Kaliski, *TWIRL and RSA Key Size*, RSA Laboratories, May 6, 2003

[44] C. H. Bennet and G. Brassard, *"Quantum Cryptography: Public key distribution and coin tossing"*, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)

[45] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *"Quantum cryptography"*, Rev. Mod. Phys. 74, 145 - 195 (2002).

[46] Artur K. Ekert, *"Quantum cryptography based on Bell's theorem"*, Phys. Rev. Lett. 67, 661 - 663 (1991)

[47] Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, Vwani Roychowdhury, *"A Proof of the Security of Quantum Key Distribution"*, arXiv.org:quant-ph/9912053 (1999).

[48] Eli Biham, Michel Boyer, Gilles Brassard, Jeroen van de Graaf, Tal Mor, *"Security of Quantum Key Distribution Against All Collective Attacks"*, 2001.

[49] D. Mayers, *"Unconditional security in quantum cryptography"*, LANL e-print, quant-ph/9802025.

[50] H. K. Lo and H. F. Chau, *"Unconditional security of quantum key distribution over arbitrarily long distances"*, Science, vol.283 (1999), p2050-6.

[51] Peter W. Shor and John Preskill, *"Simple Proof of Security of the BB84 Quantum Key Distribution Protocol"*, Phys. Rev. Lett. 85, 441 - 444 (2000).

[52] Song Ke-Hui et al. *"Scheme for teleporting an unknown atomic state to any node in a quantum communication network"*, Chinese Phys. (2002).

[53] Sergio Nesmachnow, *"Criptografa cuantica"*, Noviembre, 2004.

[54] Kenneth H. Rosen, Ph.D., *"An Introduction to Cryptography"*, Second Edition, Series Editor Kenneth H. Rosen,2007.

[55] Artur Ekert, Patrick Hayden and Hitoshi Inamori, *"Basic concepts in quantum computation"*, Centre for Quantum Computation, University of Oxford, quant-ph/0011013v1 (2008).

[56] V. Scarani, S. Iblisdir, N. Gisin, *"Quantum cloning"*, Group of Applied Physics, University of Geneva, quant-ph/0511088v1 (2005).

[57] Nicolas Gisin, Rob Thew, *"Quantum Communication"*, Group of Applied Physics, University of Geneva, quant-ph/0703255v1 (2007).

[58] Nikolina Ilic, *"The Ekert Protocol"*, Department of Physics, University of Waterloo, J. Phy334 1, NUMBER (2007).

[59] B. Giulio Casati, G. Strini., *"Principles of Quantum Computation and Information Vol. 2"*, World Scientific, 2004.

[60] D. Bruss, A. Ekert, and C. Macchiavello, *"Optimal Universal Quantum Cloning and State Estimation"*, Phys. Rev. Lett. 81, 2598 (1998).

[61] Dagmar Bruß, *"Optimal universal and state-dependent quantum cloning"*, Phys. Rev. A 57, 2368 - 2378 (1998).

[62] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin y Antonio Acin, *"Quantum cloning"*, quant-ph/0511088.

[63] V.N.Dumachev, S.V.Orlov Voronezh, *"Cloning of Qubits of a Quantum Computer"*, Militia Institute, Ministry of Internal Affairs of the Russia, arXiv:quant-ph/0212029v1 (2002).

[64] V. Buzek y M. Hillery, *"Quantum copying: Beyond the no-cloning theorem"*,Phys. Rev. A 54, 1844 (1996).

[65] H. Barnum, C.M. Caves, C.A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. 76, 2818 (1996).

[66] V. Buzek y M. Hillery, *"Universal optimal cloning of qubits and quantum registers"*, quant-ph/9801009.

[67] V. Scarani, S. Iblisdir, N. Gisin, *"Quantum cloning"*, Group of Applied Physics, University of Geneva, quant-ph/0511088v1 (2005).

[68] B. Schumacher, (1995), *"Quantum coding"*, Phys. Rev. A 51, 2738.

[69] R.F. Werner, *"Optimal Cloning of Pure States"*, Inst. f. Mathematische Physik, TU Braunschweig, arXiv:quant-ph/9804001v1

[70] J. Preskill, *"Lecture Notes, Course Information for Physics"*, Lauritsen Laboratory Caltech, 1998.

[71] Shannon, C. E. , *"A mathematical theory of communication"*, Bell System Tech. J. 27, 379; 623, (1948).

[72] Tzvetan S, Metodi, F. Chong, *"Qantum computers for computer Architects"*, Morgan and Claypool, 2006

[73] N. David Nermin, *"Quantum Computer Science, An Introduction"*, Cabridge University Press, 2007.

[74] D. McMahon, *"Quantum Computer Explained"*, Wiley-InterScience. 2008.

[75] B. Giulio Casati, G. Strini., *"Principles of Quantum Computation and Information Vol. 2"*, World Scientific, 2004.

[76] A. M. Steane, *"Error correcting codes in quantum theory"*, Phys. Rev. Lett., vol. 77, pp. 793-767, July 1996

[77] A. R. Calderbank and P. W. Shor, *"Good quantum error-correcting codes ex- ist"*, Phys. Rev. A, vol. 54, pp. 1098-1105, Aug. 1996

[78] A. M. Steane, *"Multiple particle interference and quantum error correction"*, Proc. Roy. Soc. Lond. A, vol. 452, pp. 2551-2577, Nov. 1996.

[79] P. W. Shor, *"Scheme for reducing decoherence in quantum computer memory"*, Phys. Rev. A 52, R2493–R2496

[80] Samuel L. Braunstein, *"Quantum error correction of dephasing in 3 qubits"*, arXiv:quant-ph/9603024v1.