Instituto Politécnico Nacional

ESCUELA SUPERIOR DE INGENIERIA MECANICA
Y ELECTRICA
SECCION DE ESTUFDIOS DE POSGRADO E
INVESTIGACION
UNIDAD CULHUACAN

CAMINATAS CUÁNTICAS USANDO ESTADOS MÁXIMAMENTE ENLAZADOS

T E S I S
Que para obtener el grado de

MAESTRO EN CIENCIAS DE INGENIERIA EN
MICROELECTRONICA

P R E S E N T A

Carlos Adolfo Díaz Rodríguez

DIRECTOR DE TESIS:

DR. MIGUEL ANGEL OLIVARES ROBLES

MEXICO, D.F. JULIO 2011

SIP-14

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D. F. siendo las 12:45 horas del día 06 del mes de junio del 2011 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULHUACAN para examinar la tesis titulada:

"Caminatas Cuánticas Usando Estados Máximamente Enlazados"

Presentada por el alumno:

Díaz	**Rodríguez**	**Carlos Adolfo**
Apellido paterno	Apellido materno	Nombre(s)

Con registro: B 0 9 1 7 6 7

aspirante de:

MAESTRÍA EN CIENCIAS DE INGENIERÍA EN MICROELECTRÓNICA

Después de intercambiar opiniones, los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director(a) de tesis

Olivares Robles M.A.

Dr. Miguel Ángel Olivares Robles

Dr. Gonzalo Isaac Duchen Sánchez

Dr. Rubén Vázquez Medina

Dr. Marco Pedro Ramírez Tachiquín

M. en C. Eric Ibarra Olivares

INSTITUTO POLITECNICO NACIONAL ESTADOS UNIDOS MEXICANOS S.E.P. SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION ESIME CULHUACAN

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Gonzalo Isaac Duchen Sánchez

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, D.F. el día 21 del mes Junio del año 2011, el (la) que suscribe Carlos Adolfo Díaz Rodríguez alumno (a) del Programa de Maestría en Ciencias de Ingeniería en Microelectrónica con número de registro B091767, adscrito a SEPI-ESIME-Culhuacán, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección del Dr. Miguel Ángel Olivares Robles y cede los derechos del trabajo intitulado "Caminatas Cuánticas Usando Estados Máximamente Enlazado", al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección cadr.86@gmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Carlos Adolfo Díaz Rodríguez

Nombre y firma

Dedicatorias

Esta tesis la dedico a mis padres, Teresita Rodríguez y Pedrín Díaz, que agradezco su amor incondicional y siempre tener fe en mí, los amo.

Con respeto y cariño para mis asesores,
Dr. Marco Ramiréz mi maestro, amigo y hermano
Dr. Miguel Olivares que me acompaño en este proceso de aprendizaje.
Gracias a ambos por sus consejos y por creer en mí.

A mi amigo Ulises M. Vargas que quiero y estimo.

Agredecimientos

Agradezco al CONACYT por la beca que me otorgó, para que pudiera realizar mis estudios de maestría
Agradezco al IPN que me abrió las puertas y aceptarme como estudiante

Índice general

Índice de figuras

Abstract

Nowdays the classic walks have been used as tools for the development of numerous algorithms. One significant weakness, for the solution of problems is the lack of algorithms that exploit their favor phenomena that nature presents to atomic scales.

In this thesis we study the quantum analogue that has the random walker, known as quantum walk. Since its proposal, the paradigm of quantum walks have attracted considerable interest in its study in recent years because, due to the phenomena of superposition, this group of random walk spread faster than a walk and classical so you can take a space journey fewer iterations classical counterpart. For these reasons, the study of quantum walks superior performance is expected to develop faster algorithms.

We propose as a hypothesis of this work that a change and manipulation in the use of operations and generate initial radical changes in the distributions of the walkers that could be useful in the implementation algorithms. These changes could be observed in the density probability of a walker around a region. Then changes in the distributions could be useful in the implementation algorithms.

Because of this thesis as a central objective analysis of quantum walks, showing the dramatic changes that have the quantum walk in their probability distributions also we provide a basic idea of the possible algorithmic form of implementation of these distributions.

In addition we report new results as far as we investigated in relation to the evolution of quantum walks in higher dimensions coin considering maximally bound states and the Grover operator.

Other objectives set is to give motivation to study the effect of quantum computing. In addition to explaining the phenomena that occur at atomic scales, which are to help strengthen the performance of quantum algorithms and walk.

Resumen

En la actualidad las caminatas aleatorias han sido empleadas como herramientas para el desarrollo de numerosos algoritmos. Sin embargo, una carencia importante para la solución de problemas radica en la falta de algoritmos que exploten a su favor los fenómenos que la naturaleza a escalas atómicas presenta.

En este trabajo de tesis se estudia el análogo cuántico que presenta un caminante al azar, conocido como caminata cuántica. Desde su propuesta, el paradigma de las caminatas cuánticas ha despertado un considerable interés en su estudio durante los últimos años, ya que, debido a los fenómenos de superposición, este grupo de caminata al azar se propagan con mayor rapidez que una caminata clásica y por lo tanto se puede dar un recorrido espacial en un menor número de iteraciones que su contraparte clásica. Por lo anterior, del estudio de caminatas cuánticas se espera un desempeño superior para el desarrollo de algoritmos más veloces.

La hipotesis que en este trabajo se plantea es que a través del cambio y la manipulación en el uso de operadores y los estados iniciales, se generarán cambios radicales en las distribuciones de los caminantes. Se esperan que al realizar estos cambios en la densidad probabilidad de un caminante tengan aplicaciones algoritmica en futuras investigaciones.

Debido a lo anterior esta tesis plantea como objetivo central el análisis de las caminatas cuánticas, mostrando los cambios radicales que presentan las caminata cuánticas en sus distribuciones de probabilidad, además de presentar una idea básica de las posible forma de implementación algorítmica de estas distribuciones.

Además reportamos nuevos resultados, hasta donde hemos investigado, en relación a la evolución de las caminatas cuánticas para monedas en altas dimensiones considerando estados máximamente enlazados y el operador de Grover.

Otros objetivos que se establecen, es dar una motivación para realizar estudios en el sentido de la computación cuántica. Además de explicar los fenomenos que se presentan a escalas atómicas, que son los que ayudan a potencializar el desempeño de los algoritmos y la caminata cuánticas.

Capítulo 1

Introducción

La información es un conjunto organizado de datos procesados, esté conjunto constituye un mensaje que cambia el estado de conocimiento de una persona o sistema que recibe dicho mensaje, la trascendencia e impacto que tiene la información en la vida actual es importante para la toma de decisiones, y por lo tanto mientras mayor sea la cantidad de información que se posea respecto a un tema en particular las decisiones que se deberán tomar tendrán mayor certeza, por lo tanto la necesidad de obtener y manipular cantidades de información cada vez mayor de forma eficiente y precisa crece con el transcurso del tiempo.

Durante el Siglo XX, se llevó generaron las Ciencias de la Computación, y crearon un gran cambio en el paradigma del procesamiento de la información hasta ese momento.

Claramente que las ciencias de la computación se dedican al estudio de una basta área del conocimiento que dentro de su área de estudio, existen dos disiplinas que serán de importancia en el desarrollo de esta tesis

La primera de estas es conocida como el desarrollo de algoritmos, que se definen como un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permiten realizar una actividad mediante pasos sucesivos para la solución de problemásabstractos

La segunda disiplina también tiene gran importancia ya que se encarga del estudio de los recursos informáticos requeridos para la resolución problemásy se denomina Complejidad Computacional, de la que damos una breve explicación en em apéndice B

Por supuesto que el desarrollo de la ciencia no solo se limitó a la informática. En el área de la Física el desarrollo de una de las teorías que revolucionó el conocimiento científico durante el siglo anterior y que actualmente su estudio esta en auge, esta ciencia lleva el nombre de *Mecánica Cuántica*, que es una de las más recientes ciencias, creada a inicios del Siglo XX, con el objetivo de dar una a explicación a fenómenos que se comenzaron a descubrir y que la mecánica Newtoniana no podía, fenómenos que ahora se entiende pasan en un universo de escalas atómicas, que presentan un comportamiento muy distinto a lo que la intuición hace pensar ver apéndice A.

La Mecánica Cuántica y las ciencias de la computación son dos importantes logros del siglo XX. Estas dos áreas de la ciencia no solo han inspirado generaciones de científicos y pensadores, sino que han tenido un impacto significativo en la vida diaria del hombre. La unión entre la física y la computación ha sido usada para el avance en el conocimiento de cada una de estas disciplinas.

La Mecánica Cuántica ha tenido un gran impacto tanto tecnológicamente como socialmente. Para apreciar esto se tomará como ejemplo la invención del transistor, que tal vez sea la aplicación más remarcable que se tiene de la Mecánica Cuántica. A partir del transistor el desarrollo de las computadoras tuvo un gran auge hasta el día de hoy y se puede admirar el enorme impacto de las computadoras en la vida diaria, el impacto es tal que se considera que en la actualidad se vive en la era de la información.

Una de las razón más importantes que motivan este trabajo de investigación, radica en el hecho que en 1965, Gordon Moore, uno de los fundadores de Intel, realizó una observación empírica que se ha mantenido válida durante los últimos 40 años. El afirmo que el número de transistores implementados en un chip, se duplica cada 18 meses.

La observación anterior, mejor conocida como la Ley de Moore [44], es posible que no sea válida por mucho tiempo más, ya que pronto los transistores alcanzarán niveles de miniaturización atómicos y con ello la máxima densidad de transistores posible.

Conforme se van agrupando más y más transistores en un circuito integrado, las longitudes de los chip se torna milimétricas, e incluso nanométricas. En 1988, Robert Keyes usó esta observación para estudiar el número de átomos que se requieren para almacenar un bit. Imitando a Moore, Keyes analizó la variación anual de este número y extrapoló sus resultados para concluir que, en el 2020, se alcanzaría el límite operacional de los chips de silicio en una longitud de cerca de 30 veces las dimensiones de un átomo [7].

Tomando en cuenta las afirmaciones anteriores, en un tiempo relativamente corto se alcanzarán los límites físicos para el procesamiento clásico de la información, y se comenzara a lidiar con un mundo cuántico y sus particularidades, entre las que podemos mencionar la decoherencia, la superposición, o el enlazamiento cuántico, que al ser explotados de manera correcta nos ofrecen ventajas para la eficiencia en el procesamiento de la información.

Una de las más recientes fusiones entre la física y la teoría de la Computación fue propuesta a principios de los años 80, se le denomino *Computación Cuántica.* La Computación Cuántica es definida como el campo de la ciencia que tiene por propósito resolver problemás con procedimientos de tiempo finito, como por ejemplo los algoritmos, al explotan las propiedades de la Mecánica Cuántica de estos sistemás físicos usando la implementación de dichos algoritmos.

La idea que los sistemas cuánticos podrían ser utilizados para procesar la información en forma teóricamente más eficiente que las computadoras clásicas de la época actual fue propuesta hace más de 20 años por el premio Nobel, Richard Feynman (1982) [1], el afirmaba que la naturaleza al no comportarse de forma clásica, si se deseaba una simulación de la naturaleza, esta tendría mejores resultados si se utiliza como heramienta la Mecánica Cuántica.

Propuso que el poder de las computadoras cuánticas radica en los fenómenos que presentan la sistemas cuánticos tales como la *superposición* de estados cuánticos. Estos fenómenos dan un inherente paralelismo cuántico asociado con el principio de superposición, en otras palabras Feynman argumentó que una computadora cuántica puede procesar un gran número de entradas clásicas de un solo proceso algorítmico.

A partir de la propuesta que realizó Feynman las investigaciones, desarrollos e implementaciones realizadas en el área de la Computación Cuántica han ido aumentando de forma asombrosa, así como la propuesta de nuevos protocolos de transferencia de información y de seguridad para la información, como el protocolo de distribución de llaves de criptografía cuántica BB84 [2], además han tomado tal seriedad que las aplicaciones a esta forma de procesar información actualmente son una realidad y cotidianas [3].

Un área fundamental que esta en investigación es el desarrollo de algoritmos que exploten de la mejor forma posible los efectos a niveles cuánticos que se presentan a diario [4], y es precisamente acerca de algoritmos y propuestas para su desarrollo en lo que en esta tesis hace énfasis.

La parte del desarrollo de algoritmos que exploten los fenómenos cuánticos han sido bastante estudiada desde la propuesta de Feynman, a partir de 1985 que David Deutsch propone el primer algoritmo el cual ayuda a la evaluación de funciones, y es el primero en aprovechar la superposición de estados.

El desarrollo de algoritmos cuánticos se aborda de distintas forma, una de las herraminetas utilizadas para el desarrollo de algoritmos se basa en el estudio de *caminatas cuánticas,* que es el tema de estudio principal de esta tesis que además tiene como fundamento el estudio de la Mecánica Cuántica y aspectos importantes de la Computación Cuántica que tendrán especial atención en el entendimiento de los algoritmos de búsqueda que han sido una parte fundamental en el área de la teoría de la computación y que ahora se abordarán desde un punto de vista cuántico .

La estructura de la tesis comienza con el capítulo 2, tiene por objetivo dar una breve introducción a conceptos fundamentales de la Computación Cuántica que va desde el presentación del concepto de el qubit, que el capítulo tratará con detalle, es la unidad básica de información en la Computación Cuántica, se revisará algunas compuerta utilizadas y se examinará con detalle el concepto de paralelismo cúantico, con el fin de presentar el poder de los algoritmos cuánticos, todo este desarrollo aquí presentado es con el proposito de mostrar la ventajas que presenta el Computo Cuántico, al explotar lo fenómenos cuánticos de manera adecuada.

Además se plantea la revisión entre de un algoritmo de búsqueda clásica usado en la actualidad, posteriormente se hace el planteamiento del problema de búsqueda no indexada, para terminar con una revisión detallada acerca del algoritmo de búsqueda cuántica de Gorver.

El capítulo 3 presenta el estudio y analizis de una herramienta actualmente estudiada para la creción de nuevos algoritmos cuánticos, la *caminata cuántica*, en la cual se desarrolla un concepto intuitivo de caminatas cuánticas, así como su formalismo algebraico, además se presten simulaciones de como se desarrollan

las caminatas cuánticas.

La parte de la tesis se presenta en el capítulo 4. La reproducción de resultados y las aportaciones de nuevos resultados de este trabajo, para la modificación en las distribuciones que presentan la caminatas cuánticas por medio de la aplicación de cambios en distinto parametros son presentados. Además se presenta una breve descripción en la noción de la aplicación a algoritmos de búsqueda.

Las conclusiones de nuestro trabajo de investigación las se presenta en el capítulo 5 así como los proyectos futuros.

Capítulo 2

Computación Cuántica

El tema de la Computación Cuántica es un tema vasto y emergente, que abarca desde la teoría de la información clásica hasta la física de partículas, pasando por la informática y la teoría matemática del tratamiento de la información.

Quizá se puede englobar todo en un superconjunto que incluya la Computación Cuántica junto con otras disciplinas de una importancia cada vez mayor para llegar a comprender los fundamentos de la Mecánica Cuántica y el mundo natural. Este superconjunto es a lo que se llama teoría de la información cuántica.

En este capítulo se introducirán los conceptos básicos que tienen que ver con la Computación Cuántica como el bit cuánticos, reversibilidad computacional y paralelismos cuántico, para posteriormente poder trabajar con el tema que compete a este trabajo de tesis que es la revisión de algoritmos cuánticos de búsqueda. Con el proposito de presentar las ventajas que ofrece la computación cuántica frente algunos de los conceptos bien conocido que se tienen en la computación clásica.

2.1. Bits Cuánticos (Qubits)

El *bit* es la unidad básica en la computación y la teoría de la información clásica, el cual puede asumir dos distintos estados que son marcados como 0 y 1. En Computación Cuántica se a creado un concepto análogo, el *bit cuántico*, o *qubit* para abreviar, esta sección introducirá las propiedades de qubits simples y múltiples

Ahora se describiriran los qubits como *objetos matemáticos* con ciertas propiedades específicas.

Justo como los bits clásicos tienen estados perfectamente establecidos. El qubit también tiene dos posibles estados, se denominan estados $|0\rangle$ y $|1\rangle$, que como es lógico corresponden a los estados 0 y 1 para un bit clásico.

La notación '|⟩' se denominna *Notación de Dirac*, es la notación estándar para los estados en la Mecánica Cuántica ver A.1.1, conocido también como *ket*.

Una diferencia que existe entre los bits y los qubits es que un qubit no solo puede estar en los estados $|0\rangle$ o $|1\rangle$, sino que también puede estar en lo que se conoce como estado de *superposición,* es decir que un qubit lo podemos encontrar en ambos estados al mismo tiempo y tienen la posibilidad de formar *combinaciones lineales:*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1.1}$$

Los números α y β son complejos. Dicho de otra manera, el estado de un qubit es un vector en un espacio complejo de dos dimensiones. Los estados $|0\rangle$y $|1\rangle$son conocidos como *estados de base computacional*, y forman una base ortonormal para estos vectores de espacio.

Es bien conocido que es posible examinar un bit para determinar si esta en estado 0 o 1. Por otro lado su contraparte cuántica no se puede examinar, para determinar el estado en que un qubit se encuentre utilizamos los valores de α y β.

La Mecánica Cuántica nos dice que únicamente se puede tener acceso a información mucho más restringida sobre un estado cuántico, esto significa que mientras el qubit puede existir en un estado de superposición, cada vez que se hace una medida, no lo vamos a encontrar como tal.

De hecho, cuando un qubit es medido, se encontrara que esta en el $|0\rangle$ o en $|1\rangle$. Las leyes de la Mecánica Cuántica dicen que del modulo cuadrado de α ,β en 2.1.1, se obtiene la probabilidad de encontrar el qubit en el estado $|0\rangle$ o $|1\rangle$, respectivamente. En otras palabras

$|\alpha|^2$: Dice la probabilidad de encontrar $|\psi\rangle$en estado $|0\rangle$

$|\beta|^2$: Dice la probabilidad de encontrar $|\psi\rangle$en estado $|1\rangle$

Como se sabe de la teoría de probabilidad la suma de toda las probabilidades debe resultar uno. Dado que los cuadrados de estos coeficientes, están relacionados con la probabilidad de obtener un resultado en el momento de una medición entonces α y β se ven limitadas por la exigencia de que

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.1.2}$$

Generalmente se dice, que si un evento tiene N posibles eventos y si la probabilidad de encontrar el $i - esimo$ está dada por p_i, la condición de que las probabilidades sumen uno esta escrita como

$$\sum_{i=1}^{N} p_i = p_1 + p_2 + ... + p_N = 1 \tag{2.1.3}$$

Cuando esta condición es satisfecha por los cuadrados de los coeficientes de un qubit, geométricamente, se puede interpretar esto como la condición de que los estados del qubit están normalizados a la longitud 1.

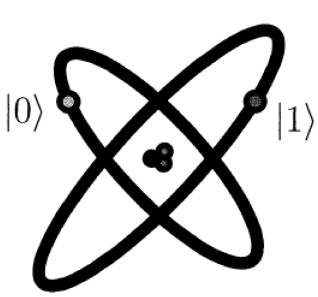


Figura 2.1.1: Representación de un qubit por dos niveles electrónicos en un átomo

La capacidad de un qubit de estar en superposición es un concepto que normalmente escapa del sentido común. Puesto que un bit clásico es como una moneda, ya sea águila o sol lo que caiga. Pero para una moneda imperfecta, debe haber estado intermedios como que se equilibre de un costado. En contraste, un qubit puede estar en un *continuo* de estados entre $|0\rangle$ y $|1\rangle$, hasta que es observado. Hay que enfatizar que cuando un qubit es medido, este resultará en 0 o 1. Por ejemplo se puede presentar un estado,

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2.1.4}$$

Cuando este estado es medido, da como resultado 0 el cincuenta por ciento del tiempo y 1 el otro cincuenta por ciento del tiempo.

Aparentemente este concepto resulta abstracto y teórico, pero en realidad actualmente existen distintas maneras para tener en un qubit en forma física, para poder tener una idea concreta de como un qubit se genera será de ayuda enlistar algunas de las formas en que pueden ocurrir

- Con las distintas polarizaciones de un fotón
- Como una alineación del espín de un electrón
- Dos estados de un electrón orbitando un átomo como se muestra en la figura 2.1.1

En el modelo del átomo el electrón puede existir en dos estados 'tierra' o 'excitado', que podemos identificar como $|0\rangle$ y $|1\rangle$, respectivamente. Por medio de la incidencia de luz en un átomo, durante el apropiado tiempo de exposición y energía, es posible mover el electrón del estado $|0\rangle$ al estado $|1\rangle$. Pero aún más interesante es el hecho que reduciendo el tiempo de incidencia, el electrón inicialmente en el estado $|0\rangle$ puede ser movido a la mitad del camino entre $|0\rangle$ y $|1\rangle$ logrando un estado superposición.

Ahora se desarrollan algunos pasos algebraicos para poder presentar un concepto que resultará de ayuda para la visualización de un qubit.

Se recuerda que $|\alpha|^2 + |\beta|^2 = 1$, entonces la ecuación 2.1.1 se reescribirá en forma de coordenadas polares, utilizando la identidad de Euler y suponiendo un radio r unitario para obtener una ecuación de la siguiente forma

$$|\psi\rangle = r_\alpha e^{i\phi_\alpha}|0\rangle + r_\beta e^{i\phi_\beta}|1\rangle \tag{2.1.5}$$

donde $r_\alpha, \phi_\alpha, r_\beta$ y ϕ_β son cuatro parametro reales.

Se tiene presente que las únicas cantidades medibles son las probabilidades $|\alpha|^2$ y $|\beta|^2$, entonces al multiplicar el qubit por un factor arbitrario $e^{i\gamma}$, denominado como fase global, no tendrá consecuencia observables en el momento de la medición, ya que

$$|e^{i\gamma}\alpha|^2 = (e^{i\gamma}\alpha)^* \cdot (e^{i\gamma}\alpha) = (e^{-i\gamma}\alpha^*) \cdot (e^{i\gamma}\alpha) = \alpha^*\alpha = |\alpha|^2 \tag{2.1.6}$$

lo anterior funciona de igual forma para $|\beta|^2$. Por lo tanto al multiplicar el estado del qubit por $e^{-i\phi_\alpha}$ obtendremos como resultado

$$|\psi'\rangle = r_\alpha e^{-i\phi_\alpha}|0\rangle + r_\beta e^{i\phi_\beta}|1\rangle = r_\alpha|0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)}|1\rangle = r_\alpha|0\rangle + r_\beta e^{i\phi}|1\rangle \tag{2.1.7}$$

donde r_α, r_β son parametros reales y $\phi = \phi_\beta - \phi_\alpha$.

Se toma en cuenta que lo anterior es una representación en coordenadas polares, ahora se presenta la ecuación 2.1.7 en su forma de coordenadas cartesianas

$$|\psi'\rangle = r_\alpha|0\rangle + r_\beta e^{i\phi}|1\rangle = r_\alpha|0\rangle + (x + iy)e^{i\phi}|1\rangle \tag{2.1.8}$$

Además se establece una condición de normalización que indica

$$|r_\alpha|^2 + |x + iy|^2 = r_\alpha^2 + x^2 + y^2 = 1 \tag{2.1.9}$$

en realidad esta representación resulta ser la ecuación de la esfera unitaria con las coordenadas cartesianas (x, y, r_α), esto permite el uso de coordenadas esfericas

$$x = r\sin\theta\cos\phi \tag{2.1.10}$$
$$y = r\sin\theta\sin\phi \tag{2.1.11}$$
$$z = r\cos\theta \tag{2.1.12}$$

y recodando que para estos cálculos $r_\alpha = z$ entonces el estado del qubit tendrá la forma

$$\begin{aligned} |\psi'\rangle &= z|0\rangle + (x + iy)|1\rangle \\ &= \cos\theta|0\rangle + \sin\theta(\cos\phi + i\sin\phi)|1\rangle \\ &= \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle \end{aligned} \tag{2.1.13}$$

Ahora se describe el estado

$$|\psi\rangle = \cos\theta'|0\rangle + e^{i\phi}\sin\theta'|1\rangle \tag{2.1.14}$$

que es un estado que será de ayuda para el último paso algebraico.

Es sencillo notar que para los valores de $\theta' = 0\, entonces\, |\psi\rangle = |0\rangle$ y por otro lado para $\theta' = \frac{\pi}{2}\, entonces\, |\psi\rangle = e^{i\phi}|0\rangle$, esto sugiere que con los valores de $0 \leq \theta' \leq \frac{\pi}{2}$ se puede generar todos los puntos de una esfera.

Ahora se considera un estado $|\psi''\rangle$correspondiente a un punto opuesto dentro de la esfera, el cual tiene las coordenas $(1, \pi - \theta, \phi + \pi)$

$$\begin{aligned} |\psi''\rangle &= \cos(\pi - \theta')|0\rangle + e^{i(\phi+\pi)}\sin(\pi - \theta')|1\rangle \\ &= -\cos(\theta')|0\rangle + e^{i\phi}e^{i\pi}\sin(\theta')|1\rangle \\ &= -\cos(\theta')|0\rangle - e^{i\phi}\sin(\theta')|1\rangle \\ |\psi''\rangle &= -|\psi\rangle \end{aligned}$$

Así que solo es necesario conciderar el hemisferio superior $0 \leq \theta' \leq \frac{\pi}{2}$, como los puntos opuestos en el hemisferio inferior sólo se diferencian por un factor de fase de -1 y así son equivalentes en el ámbito de la representación gráfica que se utiliza para los qubits en el espacio tridimensional denominado esfera de Bloch.

Entonces se pueden asignar puntos en el hemisferio superior en puntos sobre una esfera mediante la definición

$$\theta = 2\theta' \Rightarrow \theta' = \frac{\theta}{2}$$

y es así como se obtiene la siguiente representación

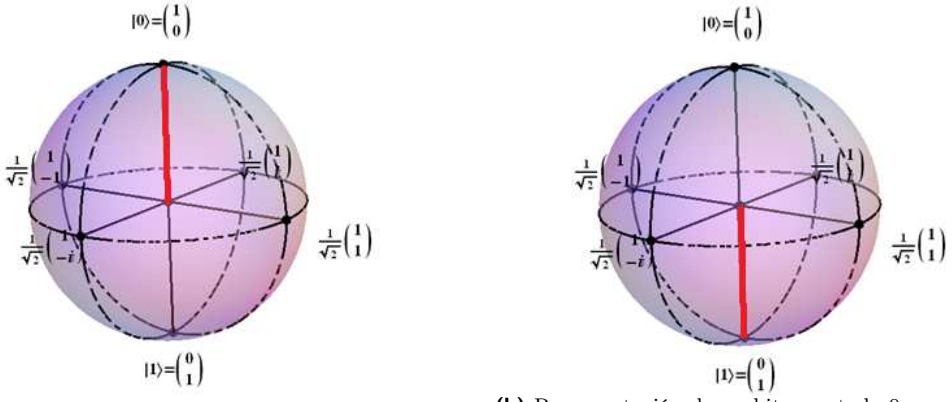
$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{2.1.15}$$

Los números θ y φ definen un punto en la esfera unitaria tridimensional, como se muestra en la figura 2.1.3, y para tener una noción comparativa, los estados que puede adquirir un bit clásicos se presentan en la figura 2.1.2. Esta forma de visualizar al qubit se liga a Felix Bloch, así que esta esfera es comúnmente conocida como la *Esfera de Bloch*

Esta forma de visualización proporciona una forma muy útil para la idealización el estado de un qubit, y a menudo sirve como una excelente banco de pruebas para las ideas acerca de Computación Cuántica. Muchas de las operaciones de qubits individuales, que se describirán más adelante, son descritos dentro de la imagen de la esfera de Bloch. Sin embargo, se debe mantener en mente que esta intuición es limitada por que no hay una generalización simple de la esfera de Bloch conocido para el uso múltiples qubits.

Los puntos en la superficie de la esfera Bloch pueden ser expresados en coordenadas cartesianas como

$$(x, y, z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta) \tag{2.1.16}$$



(a) Representación de un bit en estado 1

(b) Representación de un bit en estado 0

Figura 2.1.2: Representación vectorial de un bit clásico

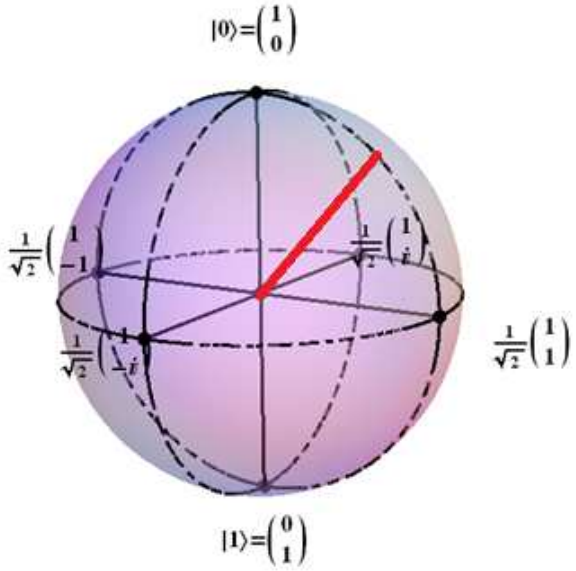


Figura 2.1.3: Representación Vectorial de un qubit en una Esfera de Bloch

Con estas ideas acerca del qubit, paseremos a dar la descripción de los arreglos de qubits.

2.1.1. Multiqubits

La Mecánica Cuántica se basa en cuatro postulado básicos, para la descripción de esta sección nos apoyaremos en el cuarto de estos postulados ver apéndice A.2.

El cuarto postulado de la Mecánica Cuántica habla acerca los estados cuánticos compuestos ver A.2.4. Este postulado indica que se puede construir un espacio de Hilbert[1] más grande a partir de dos o más espacios de Hilbert, para el espacio de dos dimensiones una colección de n qubit se le llama multiqubit de tamaño n y entonces se presenta un arreglo de qubits según lo indica el cuarto postulado de la Mecánica Cuántica,

$$\mid \varphi\rangle = \mid qbit_{N-1}\rangle \otimes \mid qbit_{N-2}\rangle \otimes \cdots \mid qbit_1\rangle \otimes \mid qbit_0\rangle. \tag{2.1.17}$$

Se considera el ejemplo más trivial utilizando dos qubits

$$\mid \varphi_1\rangle = \frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}, \quad \mid \varphi_2\rangle = \frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}} \tag{2.1.18}$$

Cuando se juntan los dos qubits, lleva a un multiqubit de cuatro dimensiones $\mid \varphi\rangle$

$$\mid \varphi\rangle = \mid \varphi_1\rangle \otimes \mid \varphi_2\rangle = \mid \varphi_1, \varphi_2\rangle = \mid \varphi_1\varphi_2\rangle$$

$$= \frac{\mid 0\rangle \otimes \mid 0\rangle + \mid 1\rangle \otimes \mid 0\rangle + \mid 0\rangle \otimes \mid 1\rangle + \mid 1\rangle \otimes \mid 1\rangle}{2} = \frac{\mid 00\rangle + \mid 10\rangle + \mid 01\rangle + \mid 11\rangle}{2} \tag{2.1.19}$$

Los vectores -*00, 01, 10* y *11* - no son otra cosa más que el contenido potencial de un registro de dos bits clásicos. Sin embargo, en el caso cuántico todos ellos son comprimidas en un único multiqubit. Estados que pueden ser producidos a partir de los estados individuales de dimensiones inferiores a través de producto tensorial se llaman estados de producto.

Además se tiene la capacidad de realizar una operación matemática en un solo paso algoritmico sobre todos los números que componen el multiqubit, que es precisamente la definición de paralelismo, y lo que puede considerarse como una extraordinaria capacidad de procesamiento en paralelo.

Desafortunadamente, como veremos más adelante, sólo se puede acceder a uno de los números cuando se realiza una medición sobre el contenido del registro. Por lo tanto, el verdadero reto no es el uso del paralelismo cuántico sino el poder obtener la información deseada en el momento de la medición

[1] Se refiere a un espacio vectorial lineal y normado definido por llos vetores $|\psi_n\rangle$ con el conjunto de funciones de cuadrado integrable $\int \psi_n^* \psi_n dx < \infty$

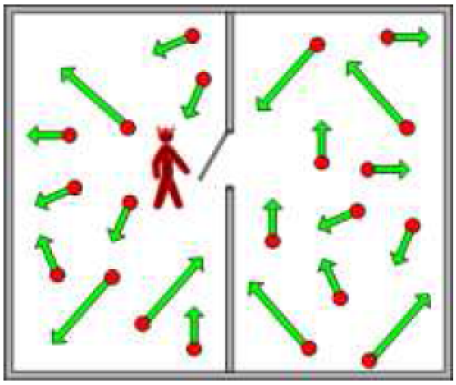


Figura 2.2.1: Demonio de Maxwell

Claro que el diseño de algoritmos capaces de aumentar la amplitud de probabilidad de los resultados deseados lo más cerca posible a 1 garantiza el éxito en el momento de realizar una medición para obtener un resultado.

Una vez expuesta la noción de los qubtis, podemos pasar a la descripción de dos de las grandes ventajas que la Computación Cuántica ofrece, se trata de la reversibilidad computacional y el paralelismo cuántico.

2.2. Reversibilidad Computacional y Compuertas Cuánticas

Se inicia con una breve discusión respecto a la relación que hay entre la energía y la información. Para esto es necesario presentar la paradoja del demonio de Maxwell, propuesta por el físico escocés James Clerk Maxwell en 1867. El imaginó un demonio capaz de monitorear la posición y velocidad de cada una de las moléculas de gas, que esta contenido en una caja inicialmente en equilibrio térmico a una temperatura T.

La caja se divide en dos partes, que están comunicadas a través de una pequeña puerta como lo muestra la figura 2.2.1.

El demonio abre y cierra la puerta para permitir que las moléculas más veloces se muevan de la parte derecha a la izquierda de la caja y las moléculas más lentas se muevan en el sentido contrario, en consecuencia de esta separación la temperatura T_l del gas en la parte izquierda de la caja se hace mayor que la de la parte derecha.

Como se tiene un gas a dos diferentes temperaturas, se puede usar este hecho para producir trabajo. Entonces, el demonio puede generar una diferencia de temperatura sin hacer algún trabajo, en una aparente violación de la segunda ley de la termodinámica. Es claro que el demonio entonces esta introduciendo orden al sistema, por lo tanto la entropía en apariencia se ve reducida.

El demonio de Maxwell generó muchas discusiones y fueron propuestas diferentes soluciones para resolver esta paradoja. En principio se creía que la revolución que produjo la paradoja recaía en el costo de la energía de la *medición* hecha por el demonio.

El resultado de la medición de la partícula debe ser almacenada en la memoria del demonio que es finita, y por lo tanto necesitará *borrar* su memoria para nuevas mediciones. En este proceso de borrado es donde se asocia la disipación de energía. Esto se menciona en el principio de Landauer desarrollado en 1961[8]

El principio de Landauer Cada que un bit de información es borrado, la cantidad de energía disipada en el ambiente es por lo menos de $k_B T ln2$ [8], donde k_B es la constante de Boltzmann y T es la temperatura del ambiente.

Lo anterior significa que cuando la información se pierde en un circuito irreversible esa información es disipada en forma de calor.

En cambio cuando un sistema cuántico aislado evolucióna, este siempre será reversible hasta su momento de ser medido, por lo tanto cualquier tipo de operación aplicado al sistema no requerirá ningun tipo de disipación de energía.

Lo anterior implica que si una computadora cuántica se integrará por medio de componentes similares a las compuertas clásicas, entonces estas desarrollarán operaciones lógicas. Por otro lado si estos componentes siguen el comportamiento que esta de acuerdo a las leyes de la Mecánica Cuántica, entonces todas estas operaciones lógica serán reversibles.

Entonces como se verá en la siguiente sección, la mayoría de los circuitos clásicos son irreversible. Esto significa que pierden información en el proceso de generar resultados por medio de sus entradas como ejemplo, a continuación se dará una breve descripción de las compuertas clásicas que se usan en la computación actual con el proposito de tener una base comparativa para presentar compuertas cuánticas irreversibles.

2.2.1. Compuertas Clásicas

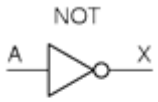
El propósito básico de una compuerta lógica es el manipular o procesar información a nivel de un bit, la información está representada en las computadoras digitales en grupos de bits.

Las compuertas son bloques del hardware que producen señales en binario 1 ó 0 cuando se satisfacen los requisitos de entrada lógica. Las diversas compuertas lógicas se encuentran comúnmente en sistemas de computadoras digitales. Cada compuerta tiene un símbolo gráfico diferente y su operación puede describirse por medio de una función algebraica. La relación de entrada-salida de las variables binarias para cada compuerta pueden representarse en forma tabular en una tabla de verdad.

Compuerta NOT El circuito NOT es un inversor que invierte el nivel lógico de una señal binaria. Esto produce la operación logica NOT, o función complementaria. El símbolo algebraico utilizado para el complemento es una

barra sobre el símbolo de la variable binaria. Si la variable binaria posee un valor 0, la compuerta NOT cambia su estado al valor 1 y viceversa.

El círculo en la figura 2.2.2 muestra la forma gráfica de un inversor que designa un inversor lógico. Es decir cambia los valores binarios 1 a 0 y viceversa.



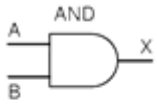
A	X
0	1
1	0

Figura 2.2.2: Compuerta NOT y su tabla de verdad

Compuerta AND La compuerta AND produce una multiplicación lógica, esto es, que la salida es 1 si la entrada A y la entrada B están ambas en el binario 1: de otra manera, la salida es 0. Estas condiciones también son especificadas en la tabla de verdad para la compuerta AND. La tabla muestra que la salida x es 1 solamente cuando ambas entradas A y B están en 1.

Como se muestra en la figura 2.2.3, a la entrada de la compuerta se tienen dos bit y en su salida únicamente se obtiene un solo bit. A esto es lo que se le denomida irreversibilidad.

El símbolo de operación algebraico de la función AND es el mismo que el símbolo de la multiplicación de la aritmética ordinaria (*). La compuerta AND descrita en la figura 2.2.3 pueden tener más de dos entradas y por definición, la salida es 1 si todas las entradas son 1.



A	B	X
0	0	0
0	1	0
1	0	0
1	1	1

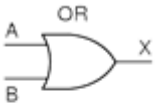
Figura 2.2.3: Compuerta AND y su tabla de verdad

Compuerta OR La compuerta OR produce la función sumadora, esto es, la salida es 1 si la entrada A o la entrada B o ambas entradas son 1; de otra

manera, la salida es 0.

En el uso de esta también se aprecia el fenómeno de la irrversibilidad de las operaciones logicas

El símbolo algebraico de la función OR (+), es igual a la operación de aritmética de suma. La compuertas OR pueden tener más de dos entradas y por definición la salida es 1 si cualquier entrada es 1.



A	B	X
0	0	0
0	1	1
1	0	1
1	1	1

Figura 2.2.4: Compuerta OR y su tabla de verdad

En las compuertas anterior se demostró como es que la pérdida de información es inherente a los cálculos lógicos en los circuitos clásicos, ya que manejan dos bits de entrada y a la salida, en la mayoría de los casos, se obtiene solo uno y es aqui donde se verifica lo que ya se mencionó acerca de la irrversibilidad computación, puesto que el bit pérdido es irrecuperable.

A continuación se pasará a dar la descripción de algunas de las compuertas cuánticas amplimente utilizadas en la literatura con el fin de demostrar que al realizar operaciones lógicas no se perderán qubits en ningún momento.

2.2.2. Compuertas y Circuitos Cuánticos

La ventaja clara del uso de este tipo de compuertas radica en el hecho que en *ningún momento* de la manipulación de los qubits se pierde información, de ahí que se puede decir que son reversibles, toda la información se puede recuperar hasta antes del momento de la medición.

Una característica que poseen todas estas compuertas cuánticas, es la *universalidad*, esto es, que se puede hacer cualquier operación desea, incluso los operaciones lógicas clásicas, estas compuertas ahora se describen.

2.2.2.1. Compuertas de un Qubit

De igual forma que en una computadora clásica, en una computadora cuántica, la información también se procesa utilizando compuertas, pero en este caso las "compuertas" son operaciones unitarias.

Como las compuertas cuánticas son sólo los operadores unitarios, ver apéndice A.1.5 , a menudo se va a hacer referencia entre las palabras compuerta y op-

erador, por lo que hay que tener en cuenta que significan lo mismo en este contexto.

Se define que los operadores cuánticos pueden ser representados por matrices. Entonces una compuerta cuántica con n entradas y salidas pueden ser representados por una matriz de grado 2^n. Para un solo qubit, se requiere un matriz de grado $2^1 = 2$. Esto es, una compuerta cuántica actuando en un sólo qubit será una matriz unitaria de 2×2.

Siguiendo el procedimiento que se utiliza cuando se piensa en compuertas de lógica clásica, hay que comenzar por el examen de la compuerta más simple posible, la puerta cuántica NOT. Resulta que ya se ha encontrado la compuerta cuántica NOT, de hecho ya se han revisado bastante de las compuertas para un solo qubit.

La operación NOT puede llevarse a cabo con la matriz de Pauli X. La matriz de Pauli X, que a menudo se refreirá como el operador NOT, se da en forma de matriz en la base de cálculo estándar o como

$$X = U_{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Entonces ya que las compuertas son operadores unitarios, se puede representar cada uno de los operadores de Pauli, ver A.1.5, que actúan en las bases computacionales, en forma de circuito como sigue

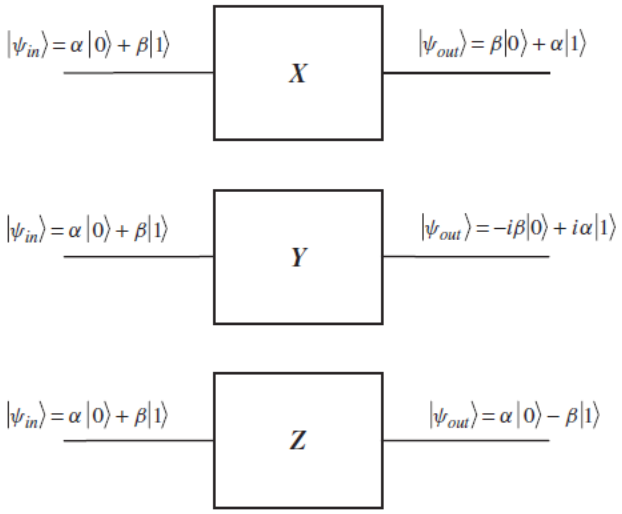


Figura 2.2.5: Compuertas de Pauli

Compuerta de Hadamard Esta es una de las compuertas más utilizadas en Computación Cuántica ya que su forma de actuar sobre las base computacional es

$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{2.2.1}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2.2.2}$$

que como se puede ver, cualquiera que sea su entrada la colocará en un estado de superposición.

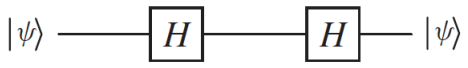


Figura 2.2.6: Compuertas Hadamard en Serie

Una forma de demostrar la reversibilidad de la compuerta de Hadamard se presenta en la figura 2.2.6 y matemáticamente se expresa como

$$H\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}\left(|0\rangle + |1\rangle\right) - \frac{1}{2}\left(|0\rangle - |1\rangle\right) = |1\rangle \tag{2.2.3}$$

$$H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}\left(|0\rangle + |1\rangle\right) + \frac{1}{2}\left(|0\rangle - |1\rangle\right) = |0\rangle \tag{2.2.4}$$

esta superposición de estados es fácilmente generalizada a para *n-qubits*, y cada qubit de forma individual puede ser conectado a una compuerta Hadamard. Comenzando por una entrada de qubits de la siguiente forma $|\varphi\rangle = |0000....,0\rangle$ y la salida tendrá la forma

$$|\psi\rangle = H^{\otimes n}|\varphi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \tag{2.2.5}$$

2.2.2.2. Compuertas multiqubit

Ahora se continúa con el caso de compuertas de dos qubits. En esta sección la noción de una puerta controlada permite aplicar un tipo de *if-else* en la construcción de una puerta cuántica. Se tiene que considerar la posibilidad de una puerta clásica controlada.

Donde se incluye un bit de control C. Entonces si $C = 0$, la puerta no hace nada, pero si $C = 1$, entonces la puerta realiza alguna acción específica. Las compuertas controladas cuánticas, trabajan en forma similar, utilizando un qubit de control para determinar si es o no una acción unitaria especificada se aplica a un qubit objetivo.

CNOT La primera entrada a esta compuerta controlada NOT, actúa como el qubit de control. La acción de una compuerta CNOT puede ser descrita en términos de una operación XOR como sigue:

$$|a, b\rangle \rightarrow |a, b \oplus a\rangle$$

Si el qubit de control es $|0\rangle$, entonces nada pasa el segundo qubit que lleva el rol de objetivo. Por otro lado si el qubit se encuentra en estado $|1\rangle$, entonces la matriz NOT o X es aplicada en el qubit de objetivo.

Las posibles entradas a la compuerta CNOT son $|00\rangle, |01\rangle, |10\rangle$ y $|11\rangle$, y la acción de la compuerta CNOT de estos estados es

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$

El circuito que comúnmente se utiliza para la representación de la compuerta CNOT se muestra en la figura 2.2.7

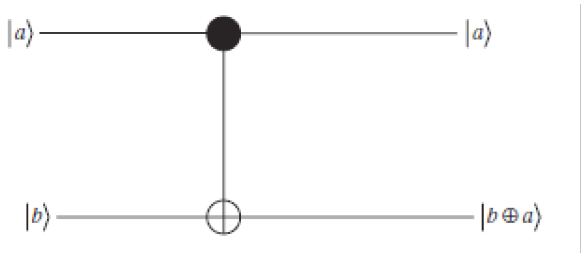


Figura 2.2.7: Compuerta CNOT

La representación matricial de la compuerta NOT controlada, se hace con respecto a los estados $|00\rangle, |01\rangle, |10\rangle$ y $|11\rangle$. La matriz entonces será de 4×4, y la matriz tendrá la siguiente forma

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.2.6}$$

Por supuesto que es lógico, que al ser un operador también tiene una notación en la forma de Dirac

$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \tag{2.2.7}$$

Toffoli Esta compuerta tiene tres qubits en la entrada, *a, b* y *c*. De estos *a* y *b* son conocidos como el *primer y segundo* qubit de control, mientras *c* es el *qubit objetivo*. La compuerta deja los dos qubits de control sin cambio alguno,

pero cambia el qubit objetivo si los dos qubits objetivos están con valor *uno,* en otro caso deja el qubit objetivo sin cambio.

A continuación se presenta la tabla de verdad y su representación en forma de circuito.

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

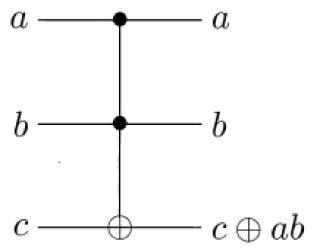


Figura 2.2.8: Compuerta Toffoli y su tabla de Verdad

Ahora que se dio una exploración acerca de compuertas cuánticas, y sus ventajas que se presenta frente a las compuertas clásicas, se presentará una explicacion de otra ventaja que tiene el mundo cuántico frente al clásico. Esto es el *paralelismo cuántico* que se explica con detalle a continuación.

2.3. Paralelismo cuántico

Además de la superposición de estados y la irreversibilidad computacional existe otra ventaja en el uso de la computación cuántica, el *paralelismo cuántico*, que es un concepto de gran importancia en el desarrollo de algoritmos.

El paralelismo cuántico es un fenómeno que se aprovecha para potencializar las operaciones realizadas, ya que un algoritmo posee la capacidad de evaluar la función de $f(x)$ para distintos valores de x simultaneamente, en un solo paso algorítmico.

La primer inspección que se realizará en el desarrollo de algoritmos cuánticos es en realidad simple, pero demuestra el innegable poder de una computadora cuántica. El algoritmo que se va a describir es conocido como el algoritmo de Deutsch.

Se comienza planteando una función considerablemente simple, una que acepta un solo bit como entrada y produce un solo bit a la salida. Esto es, $x \in \{0, 1\}$, entonces solo hay un pequeño número de funciones que pueden actuar en este conjunto de $x \in \{0, 1\}$, y dar un solo bit a la salida. Por ejemplo, se puede tener la función identidad

$$f(x) \begin{cases} 0 & si \quad x = 0 \\ 1 & si \quad x = 1 \end{cases} \tag{2.3.1}$$

también se tiene las funciones constantes

$$f(x) = 0 \tag{2.3.2}$$

$$f(x) = 1 \tag{2.3.3}$$

Finalmente se presenta la función de cambio de bit

$$f(x) \begin{cases} 1 & si \quad x = 0 \\ 0 & si \quad x = 1 \end{cases} \tag{2.3.4}$$

Las funciones de identidad y de cambio son llamadas *balanceadas* por que sus salidas son opuestas para la mitad de las entradas. Entonces una función con un solo bit pueden llamarse *constantes* o *balanceadas*. Que la función sea constante o balanceada es una propiedad global.

El primer paso en el desarrollo de este algoritmo es un operador unitario que se denota como U_f que actúa en dos qubits. Este operador deja el primer qubit solo y producirá una XOR del segundo qubit con la función f evaluada con el primer qubit como argumento. Esto es

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle \tag{2.3.5}$$

Puesto que $|x\rangle$ es un qubit, este puede estar en un estado de superposición. Específicamente se iniciara con un estado $|0\rangle$ y se aplicará una compuerta Hadamard, como se muestra en la siguiente representación del circuito

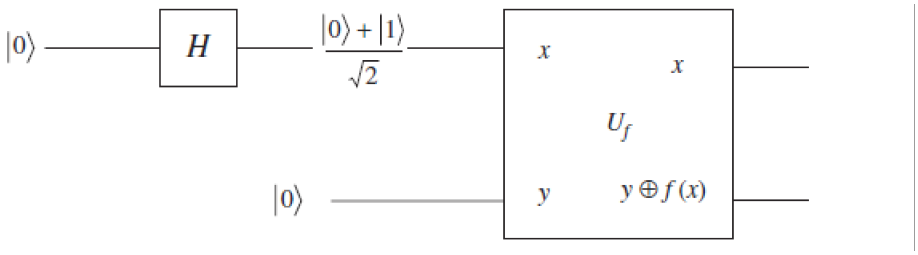


Figura 2.3.1: Circuito de implementación para el operador unitario

Por medio del uso del álgebra, se escribe la acción del circuito mostrado como

$$U_f \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle = \frac{1}{\sqrt{2}} \left(U_f|00\rangle + U_f|10\rangle \right) = \frac{|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle}{\sqrt{2}} \tag{2.3.6}$$

El circuito 2.3.1 ha producido un estado de superposición que tiene información sobre cada posible valor de $f(x)$, en un ***solo paso***.

Si $f(x)$ es una función identidad, entonces el estado resultante será

$$U_f\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle = \frac{|0,0\oplus f(0)\rangle+|1,0\oplus f(1)\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle}{\sqrt{2}} \tag{2.3.7}$$

Lo anterior se ve bastante elegante, se tiene un estado de superposición con todos los posibles pares de x y $f(x)$ representados. Pero hay que recordar que la medición funciona de una forma particular. Esto es, si se mide el estado $\sum|x\rangle|f(x)\rangle$, se obtiene un y solo un valor de x y $f(x)$. Después de una medición el sistema esta en un estado proporcional a $|x\rangle|f(x)\rangle$para ese solo y especifico valor de x.

Por lo tanto, se demuestra como se explotan las características de la Mecánica Cuántica, para un mejor procesamiento de la información.

Es claro que el paralelismo ocupa un papel de gran importancia, lo cual se ilustra mejor en la siguiente sección, donde se explota esta característica para una aplicación más útil, que solo saber una característica de una función, esto es la búsqueda no indexada de un registro.

2.4. Algoritmos de búsqueda

Un algoritmo es un conjunto de instrucciones usadas para realizar alguna tarea bien definida en un computadora. El deseo de desarrollar Computación Cuántica viene a partir de que se descubriera el hecho que algunos algoritmos trabajan mucho mejor en las computadoras cuánticas de lo que podría trabajar en una computadora clásica.

Esto es debido a la naturaleza de los sistemas cuánticos, observados en superposición e interferencia de qubits, permiten desarrollar cálculos en paralelo, lo cual no es posible en computación clásica. Como ejemplo de lo anterior se descubrió que dada una función $f(x)$, un algoritmo cuántico es capaz de evaluar la función a múltiples valores de x simultaneamente.

Como se tratará a lo largo de esta sección, un algoritmo cuántico pone de relieve uno de los conceptos centrales que hay en la teoría cuántica. Un qubit puede existir en una superposición de estados, dando a una computadora cuántica un reino oculto en el cual los cálculos exponenciales son posibles. En otras palabras, el hecho de que un sistema cuántico puede existir en una superposición o combinación lineal de estados, permite hacer cálculos simultáneos en forma paralela que no se puede hacer, en principio, en cualquier computadora clásica. Esta característica permite a una computadora cuántica hacer cálculos en paralelo con un solo circuito que proporcionan una aceleración dramática en muchos casos.

2.4.1. Algoritmo de Grover

En 1996, Lov K. Grover [33] demostró que explotando fenómenos cuánticos se podía resolver un problema de búsqueda no estructurada con una eficiencia

acotada por $O(\sqrt{N})$ evaluaciones, y análogamente a los algoritmos de búsqueda clásicos.

Se parte del hecho que se tiene una base de datos de tamaño N, que se denotan como $x = 1, 2, ..., N$, las cuales todas tiene la misma probabilidad de ser correctas y buscamos de todos estos datos un x_o correcto.

El algoritmo resuelve el problema de búsqueda bajo la suposición que existe un oráculo computacional que es capaz de determinar si un candidato de las N entradas es una solución real. Este oráculo es modelado como una función de caja negra $f(x)$, la acción de esta función es responder si o no para todos los componentes x de la base de datos de la siguiente forma

En el algoritmo de Grover, su poder radica en el hecho que explota un fenómeno denominado paralelismo cuántico esto quiere decir que, el oráculo permite evaluar $f(x)$ simultáneamente sobre todos las posibles entradas de x, con la construcción de un estado cuántico, por medio de la aplicación de una compuerta de Hadamard a las N entradas de la base de datos

$$f(x) = \begin{cases} 1 & si \quad x_0 = x \\ 0 & si \quad x_0 \neq x \end{cases}$$

el cuál es la superposición de las N entradas.

Dado lo anterior se pasa a dar una definición más formal acerca de un oráculo

Definición Un oráculo es una máquina abstracta usada en el estudio de problemas de decisión. Puede ser considerado como una caja negra que es capaz de decidir ciertos problemas de decisión en una sola etapa, es decir, un oráculo tiene la capacidad de *reconocer* las soluciones a ciertos problemas

Con el fin de dar una mejor descripción del algoritmo, el algoritmo es dividido en tres distintas subrutinas.

2.4.1.1. Inicialización y Paralelismo

El éxito del algoritmo consiste en hacer evolucionar los datos a una superposición con la mayor parte de la amplitud de probabilidad concentrada en el objetivo x_0 que se busca de forma que $f(x) = 1$, en otras palabras que el oráculo responda que sí a la función para la x señalada.

Entonces el algoritmo inicia con todos los qubits en el mismo estado inicial $|0\rangle$ y se le aplica una compuerta Hadamard de la siguiente forma

$$|\gamma_1\rangle = \mathbb{H}^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\left[(|0\rangle + |1\rangle) + (|0\rangle + |1\rangle) + \ldots\right] = \frac{1}{\sqrt{N}}\sum_{x=0}^{N}|x\rangle \qquad (2.4.1)$$

donde $\mathbb{H}^{\otimes n}|0\rangle$ representa el producto de la compuerta Hadamard aplicado n veces al estado inicial generando la superposición de las N entradas.

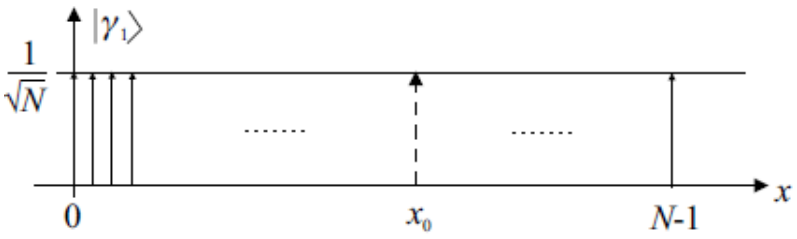


Figura 2.4.1: Superposición de todos los estados con la misma probabilidad

Como se anteriormente acerca de la reversibilidad computacional, es preciso señalar que si se aplica una Hadamard al estado $|\gamma_1\rangle$ entonces se obtendrá

$$\mathbb{H}|\gamma_1\rangle = |0\rangle$$

El estado de superposición de datos 2.4.1, incluye el estado $|x_o\rangle$ de forma que

$$\langle x_0|\gamma_1\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N}\langle x_0|x\rangle = \frac{1}{\sqrt{N}} \tag{2.4.2}$$

Ahora el algoritmo tendndrá éxito cuando se hace evolucionar el estado a una superposición con la mayor parte de la amplitud de probabilidad concentrada en el objetivo x_0, que se busca de forma tal que $f(x) = 1$. En otras palabras, que el oráculo responda sí a la función para la x señalada.

Gráficamente el estado se ve de la forma que muestra la figura 2.4.1

2.4.1.2. Inicio del Oráculo

En esta fase del algoritmos, el operador denominado *oráculo,* se usa para la distinción del objetivo y el resto de los estados

El estado entra al oráculo, en el que se aplica una operación U_f con el fin de realizar un cambio en la amplitud del estado, el cambio que buscamos dar al estado matemáticamente expresado es

$$U_f \,:\, |x\rangle \to (-1)^{f(x)}|x\rangle. \tag{2.4.3}$$

Esta operación tiene por función invertir la fase de $|x\rangle$ en la que $f(x) = 1$, que es cuando la componente del estado es el buscado. Mientras tanto deja sin modificación al resto de las entradas para las que $f(x) = 0$.

Esta función luce contradictoria, por que en apariencia se tiene que saber si una x, conduce a la solución del problema de la búsqueda o no. Si se conoce la solución de antemano, entonces no es necesario buscarla, pero para conocer la solución siempre se tiene que realizar la búsqueda.

La única manera de escapar de este círculo, es decidir que buscar $x = x_0$, no requiere ningún conocimiento a priori sobre x_0. Esto se puede lograr tras evaluar en tiempo real mediante una simple comparación.

El estado anteriormente descrito obtiene por medio de la implementación del operador de inversión de fase

$$O = I - 2|x_0\rangle\langle x_0|. \tag{2.4.4}$$

El efecto de este operador se resume como la función U_f que actúa sobre todos los valores del ket $|x\rangle$ dejando con signo negativo el valor de $|x_0\rangle$, y el resto de los estados permanecen inalterados

$$\begin{aligned} O|x_0\rangle &= -|x_0\rangle \\ O|x\rangle &= |x\rangle \qquad (\forall x \neq x_0) \end{aligned}$$

El estado obtenido al final de esta subrutina se presenta con la forma

$$|\gamma_2\rangle = O|\gamma_1\rangle = (I - 2|x_0\rangle\langle x_0|)\,|\gamma_1\rangle \tag{2.4.5}$$

$$|\gamma_2\rangle = |\gamma_1\rangle - \frac{2}{\sqrt{N}}|x_0\rangle \tag{2.4.6}$$

La figura 2.4.2 muestra en forma gráfica el resultado de la operación sobre nuestro estado.

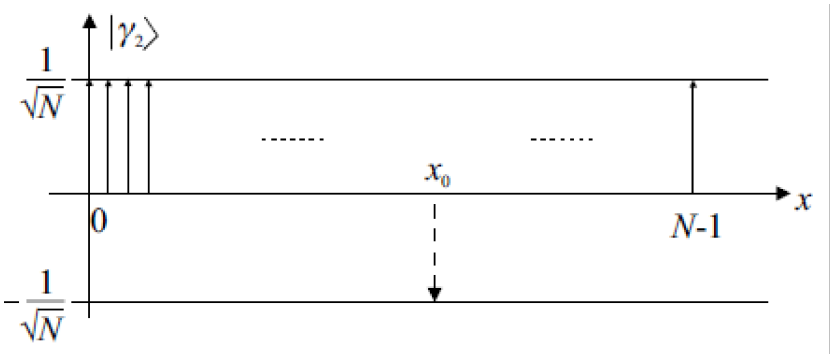


Figura 2.4.2: Cambio de Fase del Objetivo

2.4.1.3. Inversión Sobre el Promedio

Esta parte del algoritmo es la responsable de la amplificación de la probabilidad de amplitud de $|x\rangle$ mientras que se disminuye el resto de las probabilidades. Debe tenerse en cuenta que la transformación no distingue entre bases computacionales según el valor de $f(x)$. Por lo tanto se requiere una compuerta que aplique la misma operación a todo el vector base.

Ahora se explotara la única diferencia que se tiene, que es el signo de las amplitudes de probabilidad. Esta característica se aprovechara con una herramienta matemática denominada *inversión sobre el promedio.* Por el momento se expondrá como funciona, y la formulación matemática exacta se dará después.

Para realizar la inversión sobre el promedio de una computadora cuántica, se debe aplicar una transformación unitaria. Incluso, con el propósito que el algoritmo, en su conjunto resuelva el problema en $O(\sqrt{N})$ iteraciones, la inversión debe ser implementada eficientemente. Como se mostrará a continuación, la inversión puede ser lograda con $O(n) \approx O(log(N))$ compuertas cuánticas

En el algoritmo de Grover [33], se propone el uso del siguiente operador en su forma matricial

$$D_{ij} \begin{cases} \frac{2}{N} & si\ i \neq j \\ \frac{2}{N} - 1 & si\ i = j \end{cases} \tag{2.4.7}$$

que es conocido como el operador de Grover que será un utilizado en el capítulo siguiente.

El operador de Grover en la notación de Dirac tiene la forma,

$$G = 2|\gamma_1\rangle\langle\gamma_1| - I. \tag{2.4.8}$$

Se tiene en cuenta que $|\gamma_1\rangle = H|0\rangle$, $H = H^{\dagger}$y $HIH = I$, entonces el operador anterior toma la siguiente expresión

$$G = 2H|0\rangle\langle 0|H - HIH = H(2|0\rangle\langle 0| - I)H \tag{2.4.9}$$

Al operador $P = 2|0\rangle\langle 0| - I$, se le denomina *cambiador de fase controlada.*

Esta transformación P es simple: todas la amplitudes de probabilidad quedan inalteradas excepto para $|x_0\rangle$ cuyo signo es invertido.

La acción del operador Grover lo desarrollamos a continuación

$$\begin{aligned} |\gamma_3\rangle &= G|\gamma_2\rangle = (2|\gamma_1\rangle\langle\gamma_1| - I)\left(|\gamma_1\rangle - \frac{2}{\sqrt{N}}|x_0\rangle\right) \\ &= 2|\gamma_1\rangle\langle\gamma_1|\gamma_1\rangle - |\gamma_1\rangle - \frac{4}{\sqrt{N}}|\gamma_1\rangle\langle\gamma_1|x_0\rangle + \frac{2}{\sqrt{N}}|x_0\rangle \end{aligned} \tag{2.4.10}$$

Sabemos que usamos bases ortonormales, por lo tanto la ecuación anterior es reducida de la siguiente forma

$$2|\gamma_1\rangle - |\gamma_1\rangle - \frac{4}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}}|\gamma_1\rangle + \frac{2}{\sqrt{N}}|x_0\rangle \tag{2.4.11}$$

$$|\gamma_3\rangle = \frac{N-4}{N}|\gamma_1\rangle + \frac{2}{\sqrt{N}}|x_0\rangle \tag{2.4.12}$$

El estado denotado como $|\gamma_3\rangle$ indica que la probabilidad de $|x_0\rangle$ no solo se invierte nuevamente sino que además se ve aumentada a cada momento que el

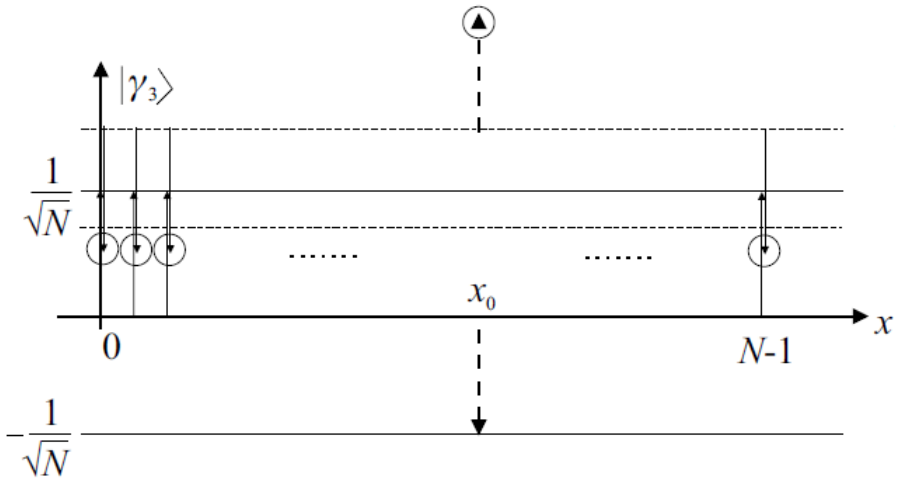


Figura 2.4.3: Inversión Sobre el Promedio

algoritmo se aplica hasta $\sqrt{N}$ veces, y la figura muestra el estado resultante 2.4.3

Con esta subrutina paso del algoritmo se da por concluida la búsqueda del objetivo $|x_0\rangle$, lo que resta es su aplicación durante $\sqrt{N}$ veces.

Ahora se presentan resultados de distintas simulaciones para dar un entendimiento más amplio acerca de este algoritmo es que este algoritmo trabaja.

2.4.2. Simulaciones del Algoritmo de Grover

Con el fin de presentar como es que el algoritmo resuelve un problema búsqueda, se presentan dos casos de simulaciones simples, con una serie de datos pequeña.

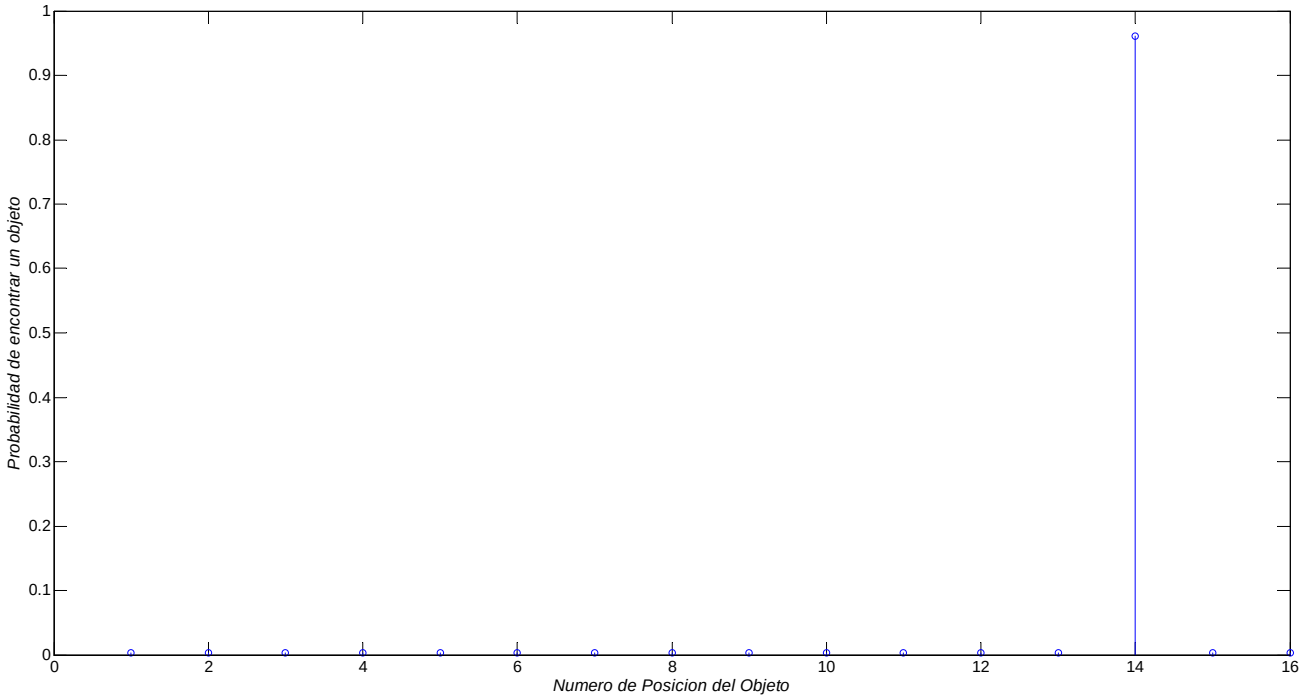
Las simulaciones presentadas a continuación fueron generadas por dos distintos software matemáticos. Es importante señalar que ambas simulaciones se generaron usando una base de datos de 16 elementos, y que en ambos casos se pide encontrar al algoritmo el elemento número 14.

En el primer caso se presenta la simulación con MATLAB© [34].

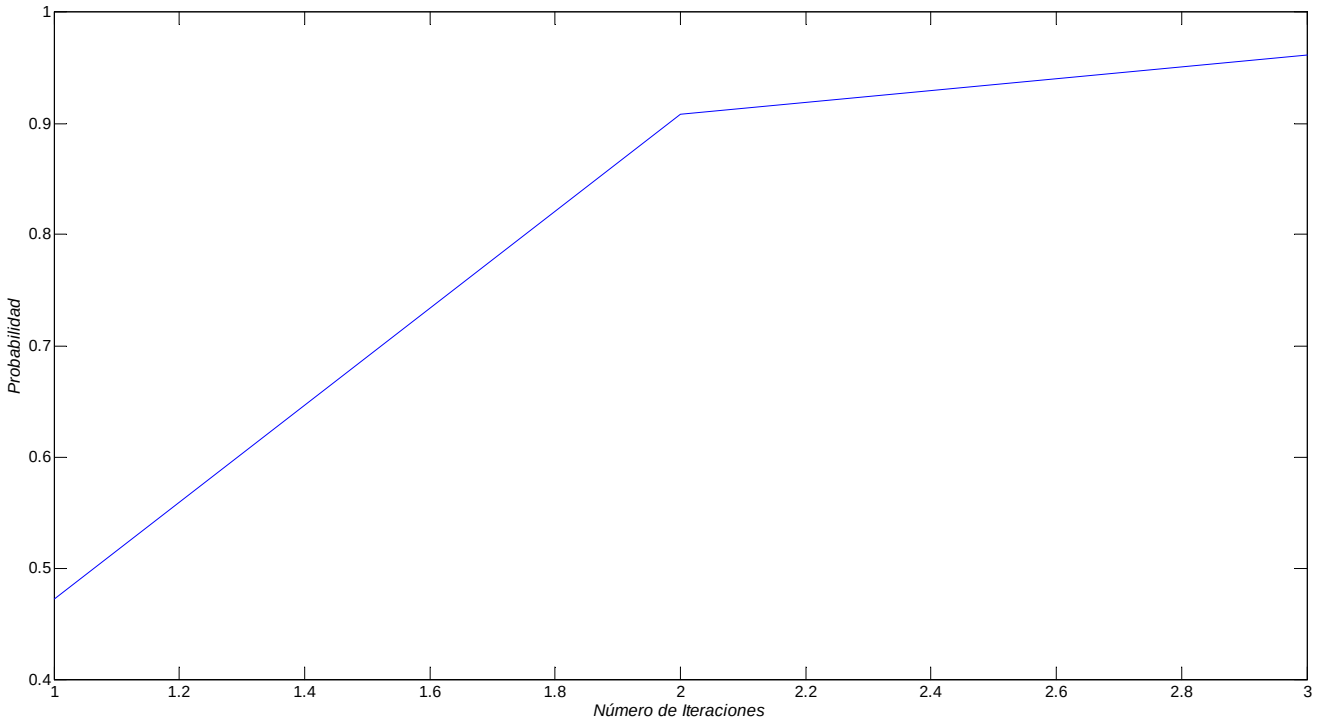
Este simulador genera dos resultados: el primero de ellos muestra la probabilidad con que la se encontró el objetivo $|x_0\rangle$, mientras que, como se espera por la descripción del algoritmo, las probabilidades de los elementos restantes resultan con valores muy cercanos a cero, como se muestra en la figura 2.4.4a.

El segundo resultado de la figura 2.4.4b muestra como la probabilidad de encontrar al objetivo $|x_0\rangle$ crece conforme el número de iteraciones del algoritmo va en aumento. Justamente como indica el algoritmo de Grover esto es $O(\sqrt{N})$ iteraciones, esto se presenta en la imagen 2.4.4.

El segundo software usado es Mathematica©[35].



(a) Objeto encontrado con una probabilidad Maximizada



(b) Presentación del aumento de la probabilidad con las iteración del algoritmo

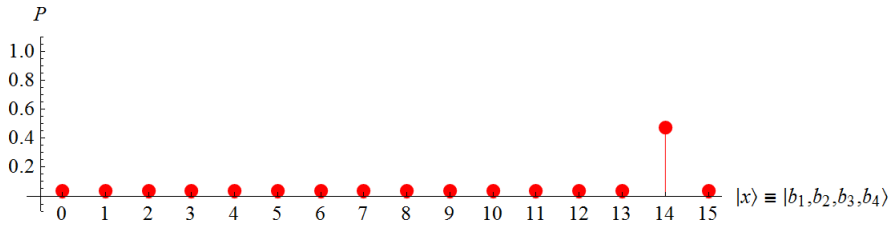
Figura 2.4.4: Resultados de Simulaciones en MATLAB

En el caso de este simulador se presentan cuatro distintas distribuciones, las cuales van presentando el cambio de estas distribuciones, además cabe resaltar que en el momento de aplicarse una iteración extra en el algoritmo la probabilidad del objeto buscado se ve disminuida, lo cual es una cualidad muy importante de observar durante la aplicación de este algoritmo como se presenta en la imagen 2.4.5.

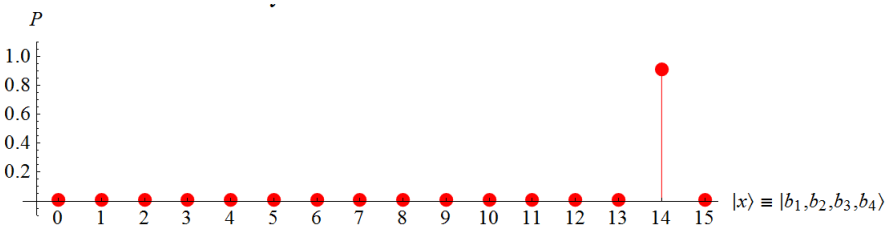
Por lo expuesto en anteriormente se tiene por conclusiones que el algoritmo de Grover es superior que sus contra partes clásicas en el sentido de su capacidad de evaluar diferentes entradas de una base de datos al mismo tiempo, utilizando el fenómeno del paralelismo que está presente en todos procesos de información cuántica[31].

La complejidad computacional que requieren los algoritmos clásicos, es del orden de$log2(n)$ para el primer caso y de un orden que varía de $O(1)$ a $O(n)$, mientras que el caso cuántico tiene una complejidad computacional $O(\sqrt{N})$, lo cual es deseable e indispensable para bases de datos con millones de entradas.

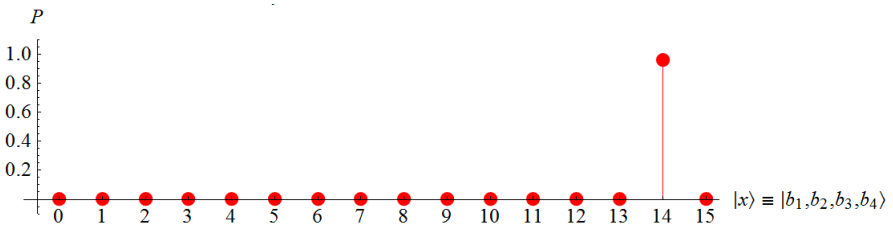
Este algoritmo en la actualidad es objeto de mucho estudio, y obviamente simulación, incluso a nivel laboratorio, pero el desarrollo de nuevos algoritmos que eficienticen las búsquedas explotando las propiedades de los sistemássubatómicos sigue siendo un tema importante, es por eso que en la siguiente parte de este trabajo se mostraran conceptos y los proyectos que se tienen por realizar para el desarrollo de algoritmos de búsqueda usando una herramienta llamada caminatas cuánticas.



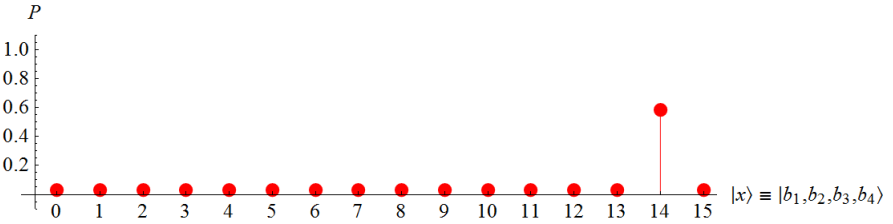
(a) Primera Iteración, que presenta al objeto encontrado con probabilidad $P = 0{,}69$



(b) Segunda Iteración, que presenta al objeto encontrado con probabilidad $P = 0{,}95$



(c) Tercera Iteración, la iteración óptima para este caso, que presenta al objeto encontrado con probabilidad $P = 0{,}98$



(d) Cuarta Iteración, que presente al objeto encontrado con probabilidad $P = 0{,}76$

Figura 2.4.5: Cambio de la Probabilidad a cada Iteración

Capítulo 3

Caminatas Cuánticas

El procedimiento que utiliza Computación Cuántica para hallar una solución se llama algoritmo cuántico, en tanto que un algoritmo convencional (clásico) es un procedimiento programado en una computadora clásica, como las que se utilizan en la vida diaria.

Crear un algoritmo cuántico no es tarea fácil, pues dicho algoritmo debe resolver el problema para el que fue diseñado y, además, debe ser más eficiente que el algoritmo clásico pensado para resolver el mismo problema.

Una herramienta utilizada para el desarrollo de algoritmos son las caminatas aleatorias. A lo largo de este capítulo se estudia un modelo empleado en el desarrollo de algoritmos cuánticos: las caminatas cuánticas (QW).

Para este propósito, primero se explica lo qué es una caminata aleatoria y se hace una comparativa con una caminata cuántica para poder relacionar de forma intuitiva el concepto clásico con su contraparte cuántica.

Después se presenta su formalismo matemático y las ventajas que presenta sobre un camita aleatoria clásica.

3.1. Caminatas Cuánticas

Las caminatas cuánticas son una generalización del modelo clásico, denominado caminata al azar. La idea básica de una caminata consiste en el uso de dos elementos principales, una moneda y un caminante. Este último cambia su posición al azar dependiendo del resultado obtenido del lanzamiento de la moneda.

Suponga que el caminante se desplaza sobre una línea y que su desplazamiento depende del resultado del lanzamiento de la moneda. Si el resultado del lanzamiento es cara, el caminante da un paso a la derecha y si el resultado es cruz, entonces el caminante se mueve a la izquierda.

Después de n lanzamientos de la moneda, surge un pregunta: ¿cuál es la probabilidad de que el caminante esté en el lugar '1000'?.

El modelo matemático que describe el comportamiento del caminante se

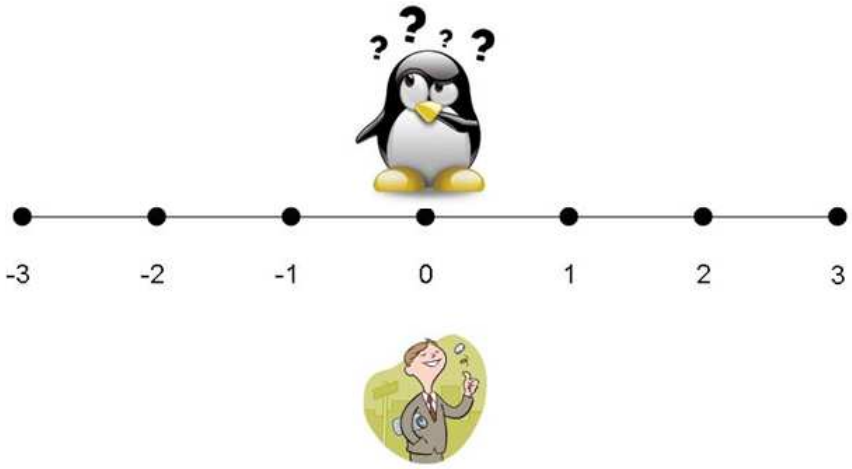


Figura 3.1.1: Cada paso de este pingüino depende que se mueva a la izquierda o derecha. Este movimiento es determinado por el resultado del volado

llama caminata aleatoria y se emplea para calcular la probabilidad de encontrar al caminante en cierta posición o, alternativamente, el tiempo que le tomará ir de un punto a otro.

En una caminata al azar, el lugar en que se encuentra el caminante en una posición $t+1$ depende de la posición t, donde t es una variable discreta. En el caso unidimensional más sencillo, el caminante da pasos iguales (a la derecha o a la izquierda) con probabilidad p y $1-p$, respectivamente, ocupando sitios discretos uniformemente distribuidos en una línea, que indicamos por enteros $x = 0, \pm 1, \pm 2, ..$, como se presenta en la figura 3.1.1.

El desplazamiento es condicional al resultado de una variable aleatoria binaria, la moneda.

En una caminata cuántica (QW), que es el análogo de una caminata al aleatoria, los elementos moneda y caminante son sustituidos por dos elementos cuántizados, *qubits*. Estos dos qubits van a representar el estado de la moneda, asi como el estado del caminante.

El componente estocástico o azaroso en la caminata cuántica, que es el resultado del lanzamiento de la moneda, es reemplazado por una operación aplicada sobre el qubit moneda.

Claro que si el qubit del caminante se mide a cada paso, se destruye la coherencia y el proceso pasa a ser clásico. Por lo tanto el poder del caminante cuántico radicará mientras evoluciona sin que sea afectado por el proceso de medición.

El qubit moneda , a diferencia de su contraparte clásica, puede existir en una superposición de los resultados de la moneda clásica. Esto es, que puede estar en sol y aguíla al mismo tiempo. Por lo tanto en este caso el caminante se desplaza simultáneamente hacia la derecha y a la izquierda.

La evolución resultante es reversible, justo como lo requiere la Mecánica Cuántica, y por lo tanto la caminata cuántica *no es un proceso estocástico*, hasta su momento de medición.

Si bien el desplazamiento condicional es un elemento común a ambos enfoques, el punto de vista cuántico es muy diferente del de un proceso clásico. Al cabo de cierto número de pasos, el caminante cuántico se encuentra en una superposición de varios lugares ocupados en la linea.

Sólo cuando se realiza una medida, se obtiene una posición concreta y se destruye el estado previo en el proceso. Además, la propia evolución va generando correlaciones cuánticas o enlazamientos entre la moneda y la posición ver A.2.4, que es el fenómeno que se aprovecha en el siguiente capítulo, de modo que en una medición de la moneda se afecta drásticamente la distribución de probabilidad de la posición.

3.2. Formalismo Matemático

Como se mencionó en la sección anterior anterior los componentes principales de una caminta cuántica son un caminante, una moneda y además los repsectivos operadores que se palican a la moneda y al caminanta para lograr que el sistema evolucione.

El caminante es un sistema cuántico matemático que éxiste en un espacio de Hilbert, ver A.1.1 , de dimensiones infinitas pero contables que se denotará como $\mathcal{H}_c$. Por costumbre se utilizan los vectores de la base computacional para la representación de la posición. Entonces el caminante se denota como $|posición\rangle$ el espacio de posiciones es generado por un conjunto ortonormal de vectores $|x\rangle$ donde los enteros $x = 0, \pm 1, \pm 2...$, que están asociados a lugares en una línea. Usualmente el estado es inicializado en el 'origen', $|posición\rangle_{in} = |0_c\rangle$.

La moneda es un sistema cuánticos que vive en un espacio de Hilbert de dos dimensiones $\mathcal{H}_m$. La moneda toma las bases canonicas $|0\rangle$ y $|1\rangle$. En resumen se dice que $|moneda\rangle \in \mathcal{H}_m$, en general un estado normalizado de la moneda puede escribirse como $|moneda\rangle_{in} = a|0\rangle + b|1\rangle$.

El espacio de Hilbert total en el que una caminata cuántica (QW) evoluciona tiene la forma $\mathcal{H}_t = \mathcal{H}_c \otimes \mathcal{H}_m$. De forma que el estado inicial del caminante es descrito como

$$|\psi\rangle_{in} = |posición\rangle_{in} \otimes |moneda\rangle_{in}$$

Loso peradores de evolución de una caminata cuántica se dividen en dos partes que son el equivalente al comportamiento de las caminatas clásicas.

Se presenta en primer lugar el equivalente cuántico al lanzamiento de la moneda. Este consiste en aplicar un operador de evolución al estado de la moneda seguido de un operador de desplazamiento condicional al sistema cuántico total.

El objetivo del operador que actúa sobre la moneda es hacer que el estado de este sistema quede en un estado de superposición, mientras que el estado del caminante queda intacto, para que se logré este resultado se aplica un operador que tiene la forma

$$S = H \otimes I = \left[\frac{1}{\sqrt{2}} \left(|0\rangle_m\langle 0| + |0\rangle_m\langle 1| + |1\rangle_m\langle 0| - |1\rangle_m\langle 1| \right) \right] \otimes I \qquad (3.2.1)$$

mientras que la aleatoriedad se introduce mediante la realización de una medición sobre el sistema.

El segundo operador que se aplica realiza el desplazamiento de izquierda o derecha se denomina operador condicional de desplazamiento

$$U = \left(|0\rangle_m\langle 0| \otimes \sum_{i=-\infty}^{\infty} |i+1\rangle_c\langle i| \right) + \left(|1\rangle_m\langle 1| \otimes \sum_{i=-\infty}^{\infty} |i-1\rangle_c\langle i| \right) \qquad (3.2.2)$$

este operador actuará en el sistema inicial de tal forma que si el estado moneda esta en $|1\rangle$ el caminante retrocederá un lugar y si el estado se encuentra en $|0\rangle$ entonces el caminante avanzara un espacio; aquí es donde radica el poder de la caminata cuántica ya que la moneda al estar en superposición hará que el caminante se mueva a dos lugares en el primer paso.

Para tener un mejor entendimiento de lo expuesto anteriormente, a continuación se desarrollan algebraicamente los dos primero pasos que da el caminante.

3.2.1. Desarrollo Algebraico de un Caminante Cuántico

En esta parte del formalismo se presenta con detalle la forma en que los operadores previamente definidos toman acción sobre un estado inicial previamente definido y preparado.

Antes de iniciar con este desarrollo algebraico, es bueno recordar que, el estado al ser cuántico, presentará fenómenos de interferencia y superposición entonces se comienza preparando un sistema inicial arbitrario de la forma

$$|\psi\rangle_0 = |0_m\rangle \otimes |0_c\rangle \qquad (3.2.3)$$

Después se procede a aplicar el operador moneda S al sistema

$$\begin{aligned}
|\psi'\rangle_0 = S|\psi\rangle_0 &= (H \otimes I) \cdot (|0\rangle_m \otimes |0\rangle_c) = \\
&= \left\{ \left[\frac{1}{\sqrt{2}} \left(|0\rangle_m\langle 0| + |0\rangle_m\langle 1| + |1\rangle_m\langle 0| - |1\rangle_m\langle 1| \right) \right] \otimes \left[|0\rangle_c\langle 0| + |1\rangle_c\langle 1| \right] \right\} \cdot \\
&\cdot (|0\rangle_m \otimes |0\rangle_c) = \\
&= \frac{1}{\sqrt{2}} \left[|0\rangle_m\langle 0|0\rangle_m + \cancelto{0}{|0\rangle_m\langle 1|0\rangle_m} + |1\rangle_m\langle 0|0\rangle_m - \cancelto{0}{|1\rangle_m\langle 1|0\rangle_m} \right] \otimes \\
&\otimes |0\rangle_c\langle 0|0\rangle_c + \cancelto{0}{|1\rangle_c\langle 1|0\rangle_c} = \\
&= \frac{|0\rangle_m|0\rangle_c + |1\rangle_m|0\rangle_c}{\sqrt{2}}
\end{aligned}$$

en este punto se puede apreciar la superposición que tiene la moneda. Ahora el operador U actuará en el estado en superposición

$$\begin{aligned}
|\psi\rangle_1 &= U \cdot |\psi'\rangle \\
&= \left\{ \left(|0\rangle_m\langle 0| \otimes \sum_{i=-\infty}^{\infty} |i+1\rangle_c\langle i| \right) + \left(|1\rangle_m\langle 1| \otimes \sum_{i=-\infty}^{\infty} |i-1\rangle_c\langle i| \right) \right\} \cdot \\
&\quad \cdot \left\{ \frac{|0\rangle_m|0\rangle_c + |1\rangle_m|0\rangle_c}{\sqrt{2}} \right\}
\end{aligned}$$

$$= \frac{1}{\sqrt{2}} \left[(|0\rangle_m\langle 0|0\rangle_m \otimes |0+1\rangle_c\langle 0|0\rangle_c) + (|0\rangle_m\langle 0|1\rangle_m \otimes |0+1\rangle_c\langle 0|1\rangle_c) \right] +$$

$$+ \frac{1}{\sqrt{2}} \left[(|1\rangle_m\langle 1|0\rangle_m \otimes |0+1\rangle_c\langle 0|0\rangle_c) + (|1\rangle_m\langle 1|1\rangle_m \otimes |0-1\rangle_c\langle 0|0\rangle_c) \right] =$$

$$= \frac{1}{\sqrt{2}} \left\{ \left(|0\rangle_m\langle 0|0\rangle_m \otimes |0+1\rangle_c\langle 0|0\rangle_c \right) + \left(|1\rangle_m\langle 1|1\rangle_m \otimes |0-1\rangle_c\langle 0|0\rangle_c \right) \right\}$$

Al final de la aplicación de estos operadores, el primer paso del caminante cuántico tiene la siguiente forma

$$|\psi\rangle_1 = \frac{1}{\sqrt{2}} \left[|0\rangle_m \otimes |1\rangle_c + |1\rangle_m \otimes |-1\rangle_c \right] \tag{3.2.4}$$

Es importante señalar que el estado final de este primer paso deja al sistema del caminante en la posición 1 y -1 al mismo tiempo, ahora en la figura 3.2.1 se muestra gráficamente lo que el estado 3.2.4 representa

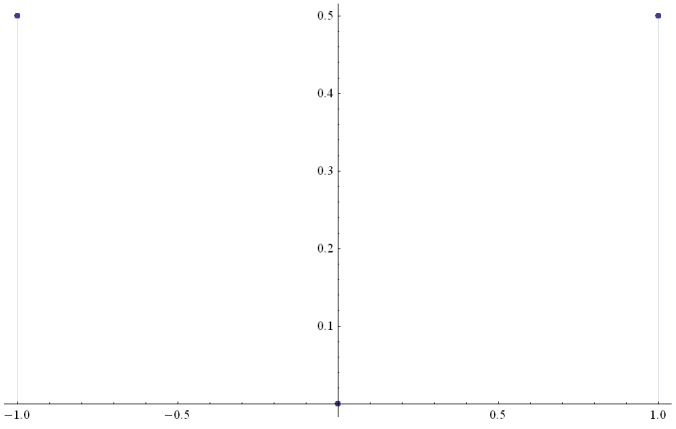


Figura 3.2.1: Primer Paso de la Caminata

El segundo paso de la caminata cuántica se hace de una manera similar, primero se aplica una superposición en el estado de la moneda con el operador S y se procede con emplear el operador de evolución,

$$|\psi\rangle_2 = U \cdot S|\psi\rangle_1 \tag{3.2.5}$$

Entonces los pasos algebraicos son presentados a continuación, es claro que la dificultad va aumentado en función del paso siguiente del caminante.

Primero se aplica la operación Hadamard al estado $|\psi\rangle_1$

$$\begin{aligned}
|\psi'\rangle_1 &= S|\psi\rangle_1 = (H \otimes I) \cdot \frac{1}{\sqrt{2}} \left[|0_m\rangle|1_c\rangle + |1_m\rangle|-1_c\rangle\right] = \\
&= \left\{ \left[\frac{1}{\sqrt{2}} \left(|0\rangle_m\langle 0| + |0\rangle_m\langle 1| + |1\rangle_m\langle 0| - |1\rangle_m\langle 1| \right) \right] \otimes \left[|0\rangle_c\langle 0| + |1\rangle_c\langle 1| \right] \right\} \cdot \\
&\quad \frac{1}{\sqrt{2}} \left[|0_m\rangle|1_c\rangle + |1_m\rangle|-1_c\rangle\right] \\
&= \frac{1}{2} \left[|0\rangle_m\langle 0|0\rangle_m + \cancelto{0}{|0\rangle_m\langle 1|0\rangle_m} + |1\rangle_m\langle 0|0\rangle_m - \cancelto{0}{|1\rangle_m\langle 1|0\rangle_m} \right] \otimes |1\rangle_c + \\
&\quad + \frac{1}{2} \left[\cancelto{0}{|0\rangle_m\langle 0|1\rangle_m} + |0\rangle_m\langle 1|1\rangle_m + \cancelto{0}{|1\rangle_m\langle 0|1\rangle_m} - |1\rangle_m\langle 1|0\rangle_m \right] \otimes \\
&\quad \otimes |-1\rangle_c \\
&= \frac{1}{2} \left[(|0_m, 1_c\rangle + |1_m, 1_c\rangle) + (|0_m, -1_c\rangle - |1_m, -1_c\rangle) \right]
\end{aligned}$$

El operador condicional de cambio actua sobre el estado resultante de la siguiente manera

$$\begin{aligned}
|\psi\rangle_2 &= U \cdot |\psi'\rangle_1 = \\
&= \left\{ \left(|0\rangle_m\langle 0| \otimes \sum_{i=-\infty}^{\infty} |i+1_c\langle i| \right) + \left(|1\rangle_m\langle 1| \otimes \sum_{i=-\infty}^{\infty} |i-1\rangle_c\langle i| \right) \right\} \cdot \\
&\quad \frac{1}{2} \left[(|0_m, 1_c\rangle + |1_m, 1_c\rangle) + (|0_m, -1_c\rangle - |1_m, -1_c\rangle) \right] =
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2} \left(\cancelto{1}{|0\rangle_m\langle 0|0\rangle_m} \otimes |1+1\rangle_c \cancelto{1}{\langle 1|1\rangle_c} \right) + \\
&\quad \frac{1}{2} \left(\cancelto{1}{|1\rangle_m\langle 1|1\rangle_m} \otimes |1-1\rangle_c \cancelto{1}{\langle 1|1\rangle_c} \right) + \\
&+ \frac{1}{2} \left(\cancelto{1}{|0\rangle_m\langle 0|0\rangle_m} \otimes |-1+1\rangle_c \cancelto{1}{\langle -1|-1\rangle_c} \right) + \\
&\quad \frac{1}{2} \left(\cancelto{1}{|1\rangle_m\langle 1|1\rangle_m} \otimes |-1-1\rangle_c \cancelto{1}{\langle -1|-1\rangle_c} \right) =
\end{aligned}$$

Finalmente el estado del paso número dos del caminante tiene la forma

$$|\psi\rangle_2 = \frac{1}{2}|0_m, 2_c\rangle + \frac{1}{2}|1_m, 0_c\rangle + \frac{1}{2}|0_m, 0_c\rangle - \frac{1}{2}|1_m, (-2)_c\rangle \tag{3.2.6}$$

Lo que la ecuación 3.2.6 indica que el sistema se encuentra con una una probabilidad de $\frac{1}{4}$ en las posiciones 2 y -2 mientras que tiene una probabilidad de $\frac{1}{2}$ de hallarse en la posición 0 de la recta

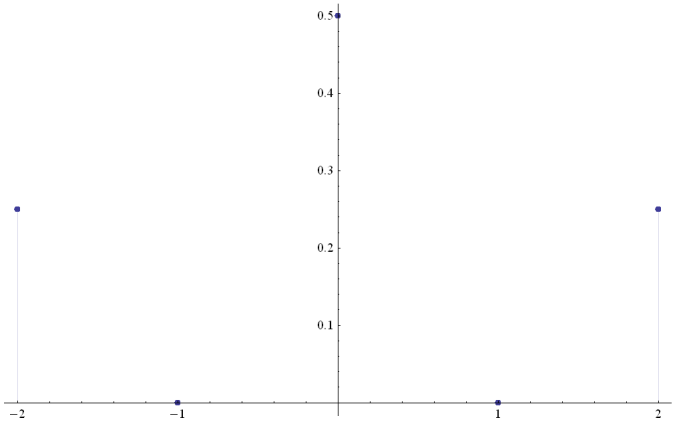


Figura 3.2.2: Distribución en el tercer paso de la caminata cuántica

El desarrollo algebraico para el tercer paso del sistema , se omite, y solo se presenta el resultado final

$$|\psi\rangle_3 = \frac{1}{2\sqrt{2}}|0_m, 3_c\rangle + \frac{1}{\sqrt{2}}|0_m, 1_c\rangle + \frac{1}{2\sqrt{2}}|1_m, 1_c\rangle - \frac{1}{2\sqrt{2}}|0_m, (-1)_c\rangle + \frac{1}{2\sqrt{2}}|1_m, (-3_c)\rangle \tag{3.2.7}$$

La ecuación 3.2.7 advierte que el sistema se encuentra en cuatro distintos puntos de la recta, pero radica una importante diferencia, y es que la distribución de probabilidad esta desbalanceada como se muestra en la figura 3.2.3.

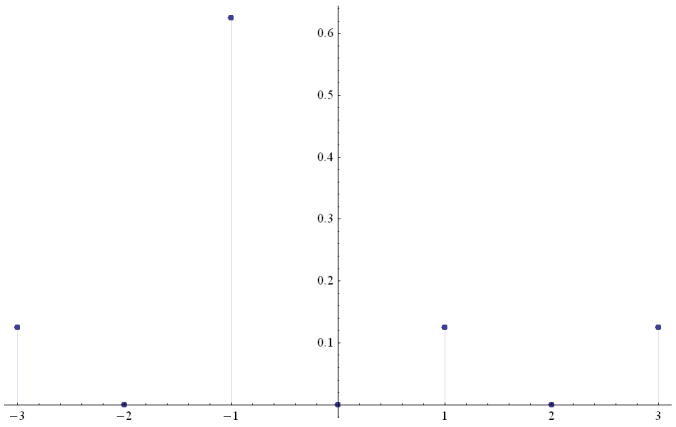


Figura 3.2.3: Distribución para el paso tres del sistema

Como se expuso anteriormente, la evolución de las caminatas cuánticasse puede describir como la aplicación de n veces de los dos operadores partiendo de un estado inicial predefinido, como se indica a continuación

$$|\psi\rangle_n = U^{\otimes n} \cdot S^{\otimes n} \cdot |\psi\rangle_0$$

Una vez expuesto el formalismo que encierran las caminatas cuánticas y entendida la forma en que evolucionan, se continúan mostrando las ventajas que presentan sobre las caminatas clásica, tanto en distribución, como en su velocidad de propagación a lo largo de una línea.

3.3. Manipulación en las Distribuciones de Caminatas Cuánticas

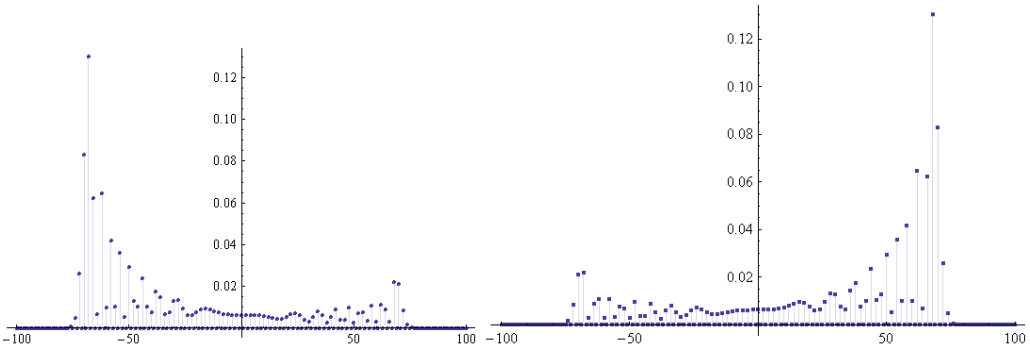
Los resultados en las distribuciones de las caminatas cuánticas son modificados fácilmente según la forma en que se definen nuestros estados iniciales o los operadores de moneda y desplazamiento.

Para el caso particular en que se usa el operador de desplzamiento 3.2.1 y un estado inicial 3.2.3, después de 100 iteraciones la distribucion obtenida tiene la forma de la figura 3.3.1b.

Cuanto se propone un cambio el operador de desplazamiento de la siguiente forma

$$S = \left(|0\rangle_m\langle 0| \otimes \sum_{i=-\infty}^{\infty} |i-1\rangle_c\langle i| \right) + \left(|1\rangle_m\langle 1| \otimes \sum_{i=-\infty}^{\infty} |i+1\rangle_c\langle i| \right) \qquad (3.3.1)$$

esta modificación cambia la forma del desplazamiento del caminante de tal forma que si el estado es $|1\rangle$ el caminante ahora avanzará un paso y si por



(a) Caminata Cuántica Desbalanceada a la izquierda después de 100 pasos

(b) Caminata Cuántica Desbalanceada a la derecha después de 100 pasos

Figura 3.3.1: Caminatas Cuánticas desbalanceadas

el contrario la moneda esta en estado $|0\rangle$ entonces el caminante retrocederá un paso. No obstante de que es una modificación pequeña en el operador, la distribución resultante se modifica notoriamente como se muestra en la figura 3.3.1a.

Por supuesto que las distribuciones anteriores son el resultado de la forma en que se eligió preparar el estado inicial, la distribución de estas probabilidades se vuelve a una balanceada al tener un estado inicial de la forma

$$|\psi\rangle_{in} = \frac{1}{\sqrt{2}} \left(|0_m\rangle + i\,|1_m\rangle\right) \otimes |0_c\rangle$$

La figura 3.3.2 muestra lo que describimos anteriormente exhibiendo un cambio muy dramático en que como se distribuyen la probabilidades de encontrar a nuestro caminante después de 100 pasos.

La clara ventaja del uso de un caminante cuántico se ve reflejada en el hecho de como se menciona en [18], una caminata clásica después de n pasos tiene una varianza $\sigma^2 = n$, por lo tanta la distancia que se espera este del origen es del orden de $\sigma = n^{1/2}$. Por contraste se puede mostrar que la caminatacuántica tiene una varianza de $\sigma \sim n^2$, esto implica que el valor esperado de su distancia al origen es del orden de $\sigma \sim n$. Esto nos indica que la caminata cuántica se propaga cuadraticamnete más rapido.

Lo anterior se ve reflejado en la figura 3.3.3. Donde se presentan la comparación entre las distribuciones de dos caminatas, una clásica y una cuánticase muestra como una caminata cuántica después de 100 pasos ha cubierto un espacio mayor en la recta que su contraparte clásica.

Los resultados obtenido en la figuras 3.3.1a y 3.3.1b muestran distribuciones desbalanceadas, que manifiestan la distribución en las que un caminante cuántico puede estar con mayor probabilidad del lado positivo o negativo de la linea. La capacidad de manipular esta propiedad en que se distribuye el caminante al final de n pasos permite pensar en la implementación de algoritmos de búsqueda

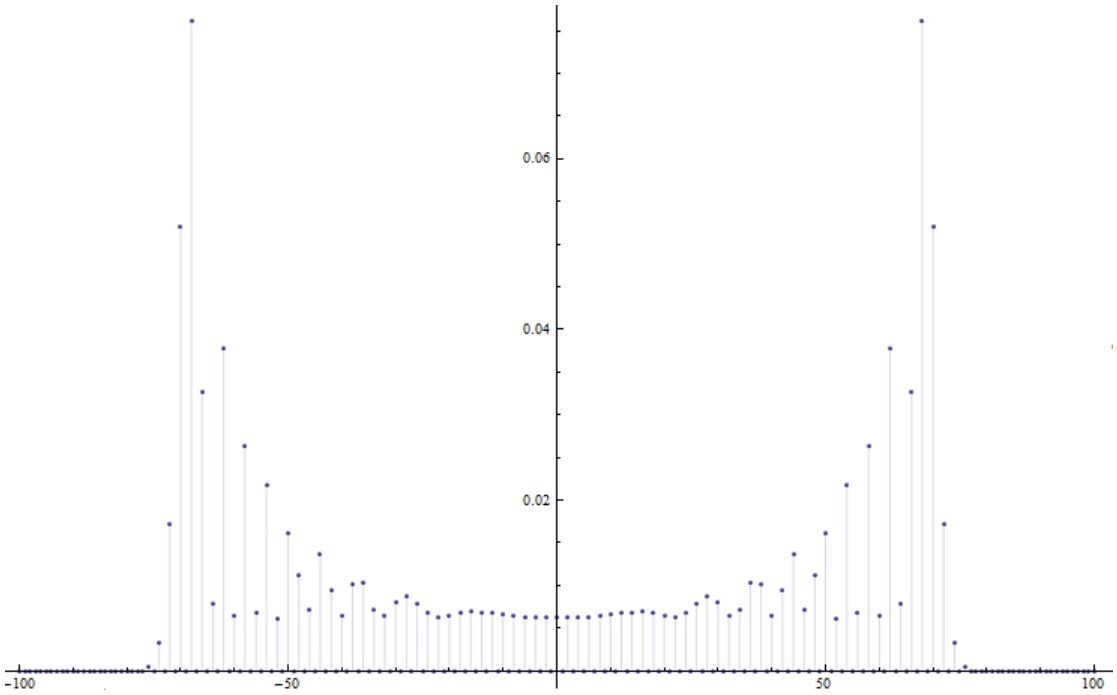


Figura 3.3.2: Caminata Cuántica Balanceada después de 100 pasos

en los cuales se pueda predeterminar el espacio o los punto en los que hay mayor probabilidad de encontrar un dato en especifíco.

Mientras que la que en la figura 3.3.2 se muestra una distribución balanceada. Esto representa una cambio drástico respecto de los dos casos anteriores ya que presenta una distribución que poseé la misma probabilidad de encontrar al caminanta en ambos lados de la linea. Esta característica aporta la venta de aplicar un distribución de este tipo para realizar un búsqueda que no este predeterminada.

Tomando en cuenta que las distribuciones de nuestro caminante en un proceso cuántico en nuestro siguiente capítulo exploramos nuevas distribuciones en la caminatas así como se hacen reproducciones y propuestas de mejoramientos en los procesos de evolución.

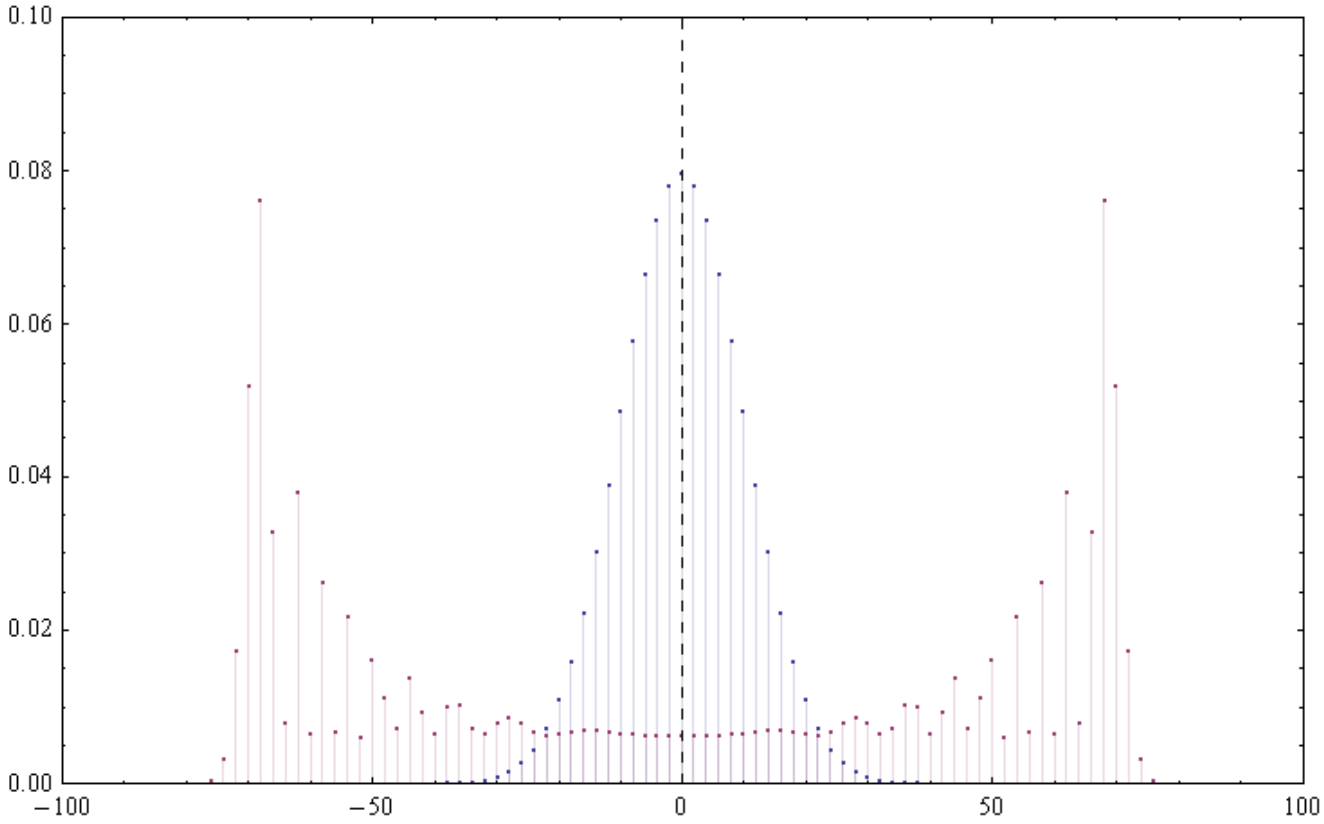


Figura 3.3.3: Comparación de Evolución en una Caminata Clásica contra una Caminata Cuántica

Capítulo 4

Resultados Computacionales de Caminatas Cuánticas con Operadores en Altas Dimensiones

Este capítulo muestra nuestros resultados obtenidos al simular el modelo de caminata cuántica usando monedas en altas dimensiones. Esto se refiere al uso de mas de una moneda en el proceso de la caminata cuántica

El estudio de caminatas cuanticas en altas dimensiones con partículas enlazadas fue propuesto por [43]. Las razones para el desarrollo de caminatas en altas dimensiones es el deseo de explorar cambios en el comportamiento de las distribuciones de las caminatas cuánticas. Aunque el modelo de caminatas cuánticas en altas dimensiones ha sido explorado ampliamente [40, 41, 42]. Sin embargo, el estudio de caminatas cuánticas sometidas a estados inciales con máximo enlazamiento es un campo poco estudiado[36, 43]. Por lo tanto, el deseo de analizar la dimanica de las caminatas cuántica con estados enlazados, presentara resultados en las distribucioens, que podran tener aplicaciones algoritmicas futuras.

Esta sección de resultados es dividida en tres partes importantes, la reproducción de resultados, mejoras en las propuesta de resultados y la más importante la presentación de nuevos resultados.

En la primer parte de nuestros resultados, se plantea por objetivo el verificar nuestros cálculos numéricos por medio de la reproducción de resultados publicados en el 2011 [38] usando monedenas en altas dimensiones. Después cotejamos nuestros cálculos al utilizar estados enlazados, por medio de la reproducción de distribuciones con monedas en altas dimensiones y estados máximamente enlazados publicados en [36].

La segunda parte de este capítulo de resultados ilustra que el comportamien-

to de las caminatas cuánticas con monedas enlazadas es muy diferentes en comparación con la caminata cuántica usual, con una solo moneda. Los resultados que se resaltan en este sección es que además de la reproducción de resultados presentados en [37], nosotros proponemos un cambio en el uso del operador moneda, que no solo despliega la misma distribución sino que además presenta una mejora drástica en los tiempos de ejecución de las simulaciones.

La ultima parte de nuestros resultado proponen una combinación nunca antes explorada para la evolución de caminatas cuánticas, que consiste en el uso de estados iniciales, operadores monedas y de desplazamiento. Con lo anterior se muestran nuevas distribuciones en las caminatas cuánticas, que posiblemente tendran aplicaciones algoritmicas.

4.1. Reproducción de Resultados con Monedas en Altas Dimensiones

En años recientes el interés en la investigación en caminatas cuánticas ha crecido ampliamente, motivado por la importancia de las caminatas clásicas aplicadas a la ciencia de la computación, así también podemos obtener ventajas de las caminatas cuánticas.

Las caminatas clásicas son una herramienta importante para el desarrollo de algoritmos estocásticos. Por lo tanto, las caminatas clásicas son elementos importantes de la informática.

Además, por los recientes desarrollos en la Computación Cuántica se ha puesto de manifiesto que al explotar los sistemas mecánico-cuánticos para fines del mejoramiento en el cálculo, conduce a una serie de ventajas significativas que presentan sobre los sistemas clásicos.

Por lo tanto, es razonable esperar que el estudio de las caminatas aleatorias explotando las características que ofrece la mecánica cuántica puede resultar ventajosas.

Esta sección esta dividiva en dos partes en la primer parte se comienza a desarrollar el concepto de caminatas cuánticas en altas dimensiones y se presenta la primer reproducción de resultados con monedas en altas dimensiones. La segunda parte, comienza abordar el concepto de monedas enlazadas y presenta la reproducción de resultados respecto a este sentido.

4.1.1. Moneda Grover en Dimensiones Superiores

Para el desarrollo de un caminata cuántica en altas dimensiones se hará uso de un concepto importante.

Es el cuarto postulado de la mecánica cuántica, ver A.2.4, el cual habla que dos o más sistema cuánticos pueden unirse para generar un estado cuántico mayor, como se presenta a continuación

$$\mid \psi_T\rangle = \mid \psi_1\rangle \otimes \mid \psi_2\rangle.$$

Una consecuencia crear sistemas compuestos, es que el espacio de Hilbert crece en su dimensión, esto significa que $\mathcal{H}^2 \otimes \mathcal{H}^2 = \mathcal{H}^4$.

Por lo anterior se puede explorar la caminatas cuántica utilizando dos monedas en el sistema inicial, para poder estudiar las dinamicas que presentan, y con estados de la siguiente forma

$$|\psi\rangle = (|m_1\rangle \otimes |m_2\rangle) \otimes |c\rangle$$

Entonces al utilizar dos moneda en el estado inicial, es obvio que los operadores moneda deberan crecer en su dimensión.

Uno de los operadores moneda que actualmente es objeto de estudio en el desarrollo de caminatas cuánticas en dimensiones superiores se conoce como moneda de Grover.

El uso de este operador en camiantas cuánticas se basa en la definición 2.4.7 del algoritmo del mismo nombre. La aplicación del operador de Grover como moneda fue propuesto por Moore and Russell [40]. Recientemente en este año se ha propuesto la implementación física de una caminata cuántica con monedas de altas dimensiones, en la que se emplea el operador de moneda de Grover por Hamilton et. al. Quantum walk with a four dimensional con; New J. Phys. 13 01315 (2011).

El operador moneda de Grover es elegido en su estudio de la caminatas cuánticas, por que resulta en dinámicas interesantes de la evolución del caminante cuántico, dependiendo del estado de entrada del sistema.

Por razones de claridad presentamos al operador de Grover en su forma matricial

$$G = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}. \tag{4.1.1}$$

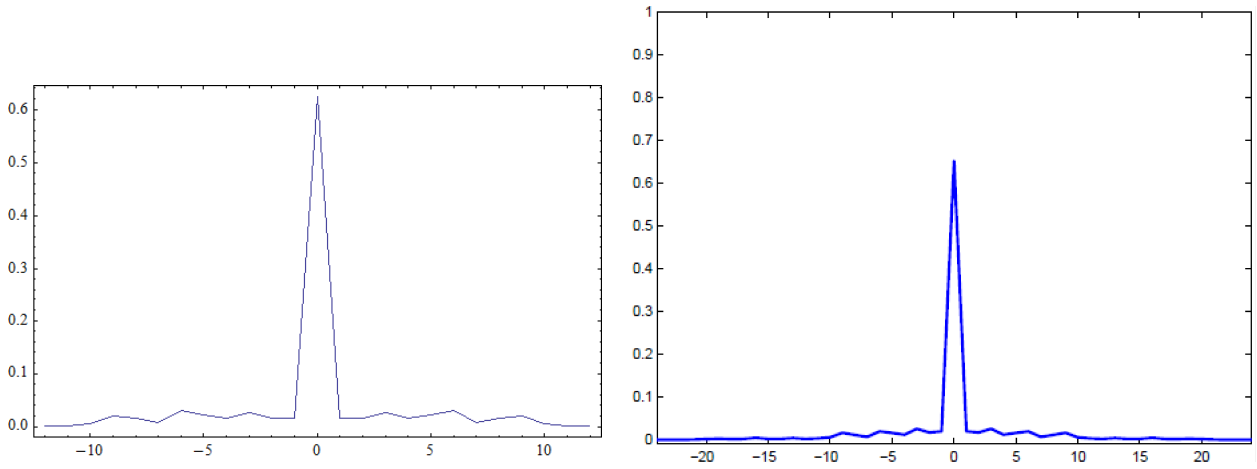
Este operador en su forma de proyector en cuatro dimensiones que se utilizará para la aplicación en el estado moneda, se escribe como

$$\begin{aligned} G_4 = \quad & \tfrac{1}{2}\{-|0_1,0_2\rangle\cdot\langle 0_1,0_2| + |0_1,1_2\rangle\cdot\langle 0_1,0_2| + |1_1,0_2\rangle\cdot\langle 0_1,0_2| \\ & + |1_1,1_2\rangle\cdot\langle 0_1,0_2| + |0_1,0_2\rangle\cdot\langle 0_1,1_2| - |0_1,1_2\rangle\cdot\langle 0_1,1_2| \\ & + |1_1,0_2\rangle\cdot\langle 0_1,1_2| + |1_1,1_2\rangle\cdot\langle 0_1,1_2| + |0_1,0_2\rangle\cdot\langle 1_1,0_2| \\ & + |0_1,1_2\rangle\cdot\langle 1_1,0_2| - |1_1,0_2\rangle\cdot\langle 1_1,0_2| + |1_1,1_2\rangle\cdot\langle 1_1,0_2| \\ & + |0_1,0_2\rangle\cdot\langle 1_1,1_2| + |0_1,1_2\rangle\cdot\langle 1_1,1_2| + |1_1,0_2\rangle\cdot\langle 1_1,1_2| - |1_1,1_2\rangle\cdot\langle 1_1,1_2|\} \end{aligned} \tag{4.1.2}$$

proponiendo un estado inicial de este tipo

$$|\psi\rangle = \frac{1}{2}\left[|00\rangle + |01\rangle - |10\rangle - |11\rangle\right]$$

En esta sección se hizo una reproducción de resultados obtenidos en [38] con el fin de la comparación y verificación de nuestros cálculos.



(a) Gráfica obtenida en simulador **(b)** Gráfica original del artículo,

Figura 4.1.1: Caminata cuántica después de 12 pasos, usando la moneda de Grover y un estado inicial $|\psi\rangle$.

El resultado obtenido por en la figura 4.1.1 y nuestra figura generada 4.1.1a, con este resultado funcionamiento de la aplicación de nuestros calculos, ahora se presentan ambas gráficas en la que se demuestra la exacta similitud entre ambos simulaciones.

En la figura 4.1.1 vemos como la posición de nuestro caminante se mantiene localizada al rededor del origen, esto significa que el caminante casi no se distribuye en el tiempo. Esta distribución muestra un importante cambio en la forma de distribución de las caminatas cuánticas por la libertad de elegir un estado inicial en la moneda.

Expuesto lo anterior demostramos que el uso de nuestros calculos numéricos funcionan de forma correcta ya que logramos una reproducción exacta de resultados recientes.

En la siguiente sección se presentan las propuestas caminatas con el uso del operador de Grover, tanto en la reproducción de resultados conocidos con un mejoramiento de tiempo, como la producción de nuevas distribuciones de probabilidades.

4.1.2. Caminatas Cuánticas usando Monedas Máximamente Enlazadas.

De igual forma

En esta sección obtenemos con nuestros calculos algunos resultados obtenido por Andraca et. al. en su trabajo Quantum Walks with Entangled Coins, New J. Phys. 7 221 (2005). [37, 36].

Los resultados son obtenidos con estados de Bell ver apéndiceA.3.1, como

estados iniciales del sistema, el uso de una moneda de Hadamard para 4 dimensiones tiene la misma finalidad de colocar en estado de superposición el estado inicial y tiene la siguiente forma

$$\begin{aligned} H_4 = \quad & \tfrac{1}{2}\{|0_1,0_2\rangle\cdot\langle 0_1,0_2| + |0_1,1_2\rangle\cdot\langle 0_1,0_2| + |1_1,0_2\rangle\cdot\langle 0_1,0_2| \\ & + |1_1,1_2\rangle\cdot\langle 0_1,0_2| + |0_1,0_2\rangle\cdot\langle 0_1,1_2| - |0_1,1_2\rangle\cdot\langle 0_1,1_2| \\ & + |1_1,0_2\rangle\cdot\langle 0_1,1_2| - |1_1,1_2\rangle\cdot\langle 0_1,1_2| + |0_1,0_2\rangle\cdot\langle 1_1,0_2| \\ & + |0_1,1_2\rangle\cdot\langle 1_1,0_2| - |1_1,0_2\rangle\cdot\langle 1_1,0_2| - |1_1,1_2\rangle\cdot\langle 1_1,0_2| \\ & + |0_1,0_2\rangle\cdot\langle 1_1,1_2| - |0_1,1_2\rangle\cdot\langle 1_1,1_2| - |1_1,0_2\rangle\cdot\langle 1_1,1_2| + |1_1,1_2\rangle\cdot\langle 1_1,1_2|\} \end{aligned} \tag{4.1.3}$$

Puesto que ahora se manejan dos estados enlazados se tendrá la nomenclatura $|E_1,E_2\rangle$ con los subíndices 1 y 2 para denominar los estados de la moneda enlazada mientras que el subíndice para denominar al estado del caminante seguirá conservándose $|E\rangle_c$

Anteriormente mostramos como el estado del caminante al inicio de una caminata es normalmente inicializado en cero $|\textit{posición}\rangle_0 = |0\rangle_p$, que además vive en un espacio de Hilbert infinito, pero contable. Una diferencia que ahora radica en nuestro estado es que la moneda inicial ahora es un estado enlazado de dos qubits, entonces decimos que nuestro estado cuántico vive en un estado de Hilbert de 4 dimensiones.

A continuación se presentan la reproducción de resultados obtenidos, con estados de monedas máximamente enlazados, estas simulaciones fueron realizadas con el propósito de investigar las propiedades de la caminatas cuánticas con estados de monedas enlazados, cuyo estados iniciales se presentaran a continuación, si se desea ampliar la información al respecto se recomiendo revisar el apéndice A.3.1.

La figura 4.1.2 fue generada por un estado inicial de la siguiente forma

$$|\gamma_0^1\rangle = |0\rangle_p \otimes |\phi^+\rangle = |0\rangle_p \otimes \frac{|0_1,0_2\rangle + |1_1,1_2\rangle}{\sqrt{2}}$$

utilizando el primer estado de Bell A.3.8 y con la posición del caminante en cero.

El resultados obtenido de la figura 4.1.3 se genero a partir del estado inicial

$$|\gamma_0^2\rangle = |0\rangle_p \otimes |\phi^-\rangle = |0\rangle_p \otimes \frac{|0_1,0_2\rangle - |1_1,1_2\rangle}{\sqrt{2}}$$

se utilizando el segundo estado máximamente enlazado de BellA.3.9 y con el estado del caminante inicializado en cero.

La ultima gráfica 4.1.4 se generó por el estado inicial con la siguiente forma

$$|\gamma_0^3\rangle = |0\rangle_p \otimes |\psi^+\rangle = |0\rangle_p \otimes \frac{|0_1,1_2\rangle + |1_1,0_2\rangle}{\sqrt{2}}$$

por medio del tercer estado enlazado de Bell A.3.8y la inicialización del estado del caminante en cero.

El cuarto estado de Bell $|\psi^-\rangle = \frac{|0,1\rangle - |1,0\rangle}{\sqrt{2}}$, no lo utilizamos ya que dicho estado permanece sin cambio cuando se aplica el mismo operador unitario a sus qubits constituyentes.

Una de las propiedades mas nobles es que la probabilidad que el caminante se encuentre en el origen es demasiado alta, además es evidente que existen, en los tres casos, dos zonas extremas que tiene mayor posibilidad en que se encuentre el caminante, a estas zonas que el caminante tiene mayor probabilidad de encontrarse es conocida como la "zona de tres picos".

Además, encontramos que al usar diferentes estados moneda como estados iniciales estos mantiene el mismo patrón básico en la distribución de probabilidad como podemos ver en las imágenes 4.1.2, 4.1.3 y 4.1.4, a diferencia de las distribuciones que presentamos en el capitulo anterior que con dar pequeñas modificaciones a los estados monedas nos generaban distribuciones totalmente distintas.

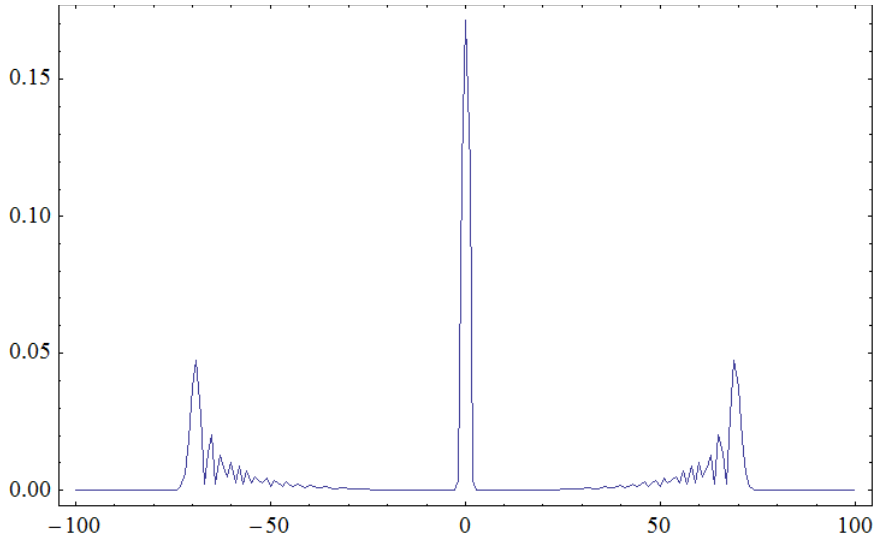


Figura 4.1.2: Caminata con 100 paso con el estado inicial de Bell $|\phi^+\rangle$usando el operador moneda de Hadamard en 4 dimensiones

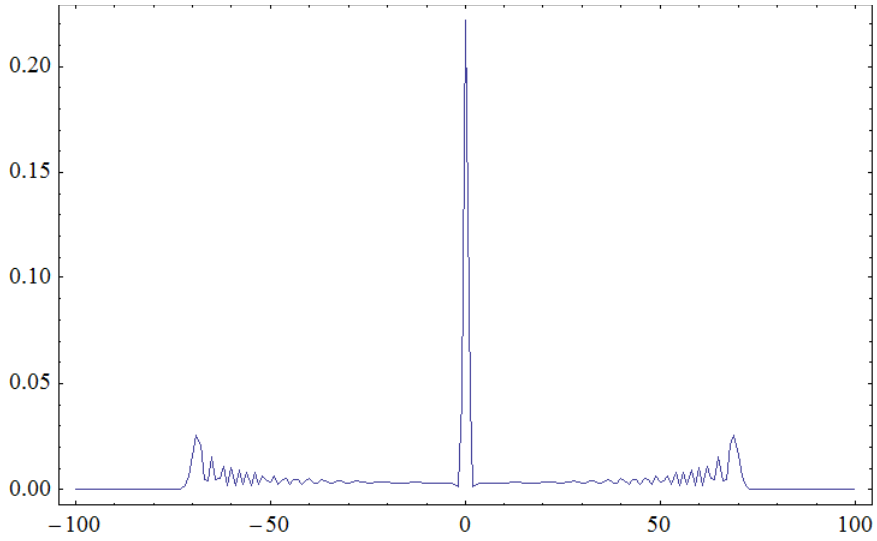


Figura 4.1.3: Caminata con 100 paso con el estado de Bell $|\phi^-\rangle$usando el operador moneda de Hadamard en 4 dimensiones

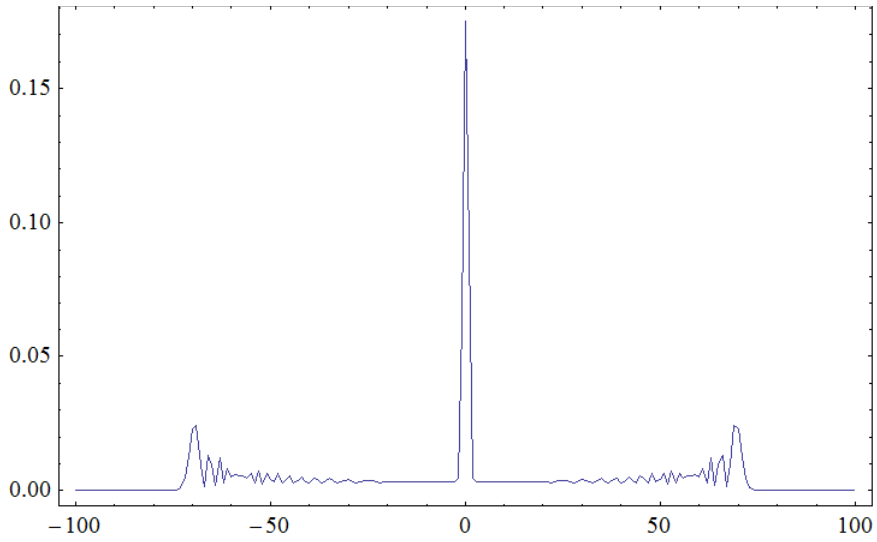


Figura 4.1.4: Caminata con 100 paso con el estado de Bell $|\psi^+\rangle$usando el operador moneda de Hadamard en 4 dimensiones

4.2. Reproducción y Comparación de Caminatas Cuanticas con Operadores Moneda $\hat{Y}$ y Grover

Ahora se reproducen resultados obtenidos en la investigación doctoral del Doctor Salvador Andraca, resultados que se generaron utilizando tres de los estados cuánticos máximamente enlazados llamados estados de Bell y además se usó uno de los operadores de Pauli A.1.5 aplicados al espacio de Moneda y tiene la forma

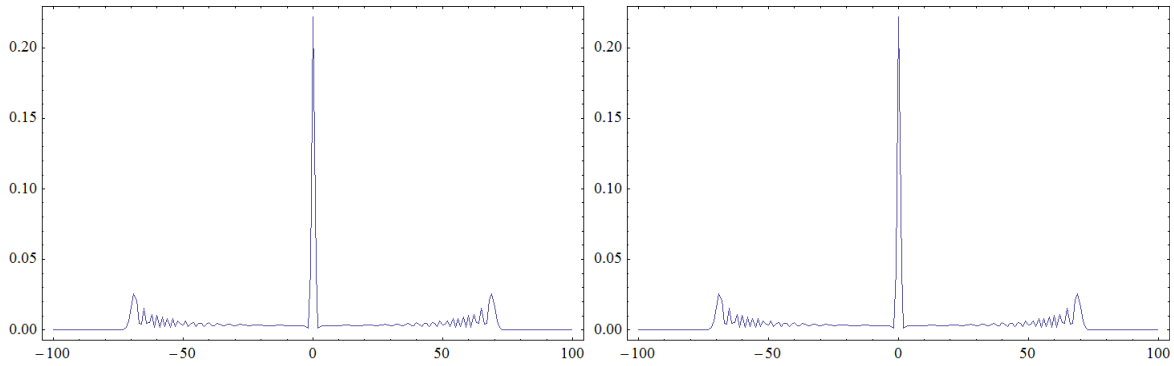
$$\begin{aligned} Y = \quad & \tfrac{1}{2}\{|0_1,0_2\rangle\cdot\langle 0_1,0_2| + i\,|0_1,1_2\rangle\cdot\langle 0_1,0_2| + i\,|1_1,0_2\rangle\cdot\langle 0_1,0_2| \\ & - |1_1,1_2\rangle\cdot\langle 0_1,0_2| + i\,|0_1,0_2\rangle\cdot\langle 0_1,1_2| + |0_1,1_2\rangle\cdot\langle 0_1,1_2| \\ & - |1_1,0_2\rangle\cdot\langle 0_1,1_2| + i\,|1_1,1_2\rangle\cdot\langle 0_1,1_2| + i\,|0_1,0_2\rangle\cdot\langle 1_1,0_2| \\ & - |0_1,1_2\rangle\cdot\langle 1_1,0_2| + |1_1,0_2\rangle\cdot\langle 1_1,0_2| + i\,|1_1,1_2\rangle\cdot\langle 1_1,0_2| \\ & - |0_1,0_2\rangle\cdot\langle 1_1,1_2| + i\,|0_1,1_2\rangle\cdot\langle 1_1,1_2| + i\,|1_1,1_2\rangle\cdot\langle 1_1,0_2| + |1_1,1_2\rangle\cdot\langle 1_1,1_2|\} \end{aligned} \tag{4.2.1}$$

Estos resultados pueden encontrarse en [37], y ahora son reproducidos proponiendo el uso del operador de Grover 4.1.2

Como se puede apreciar en la figuras 4.2.1, 4.2.2 y 4.2.3 las tres presenta las misma característica que las figuras que usan Hadamard, esto esto la distribución de la probabilidad concentrada en tres puntos.

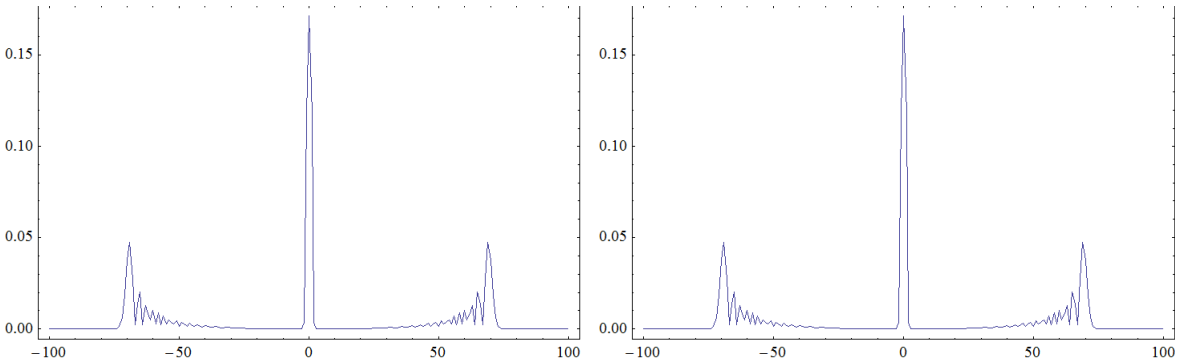
Otro hecho importante que se debe notar el hecho que las seis graficas tienen la misma forma básica, a pesar que 4.2.1a, 4.2.2a y 4.2.3a fueron generadas por medio del uso de la moneda Grover 4.1.2, la cual tiene la clara ventaja sobre la moneda de Pauli4.2.1 que *no usa números imaginarios*, esto hace que los calculos sean mas simples y por tantos mas veloces de realizar como se puede verificar en los tiempos de simulación obtenidos tras generar las graficas.

El mejoramiento en los tiempos de ejecución la cualidad mas importante a resaltar en el momento de utilizar el operador moneda de Grover y compararlo contra el operador $\hat{Y}$.



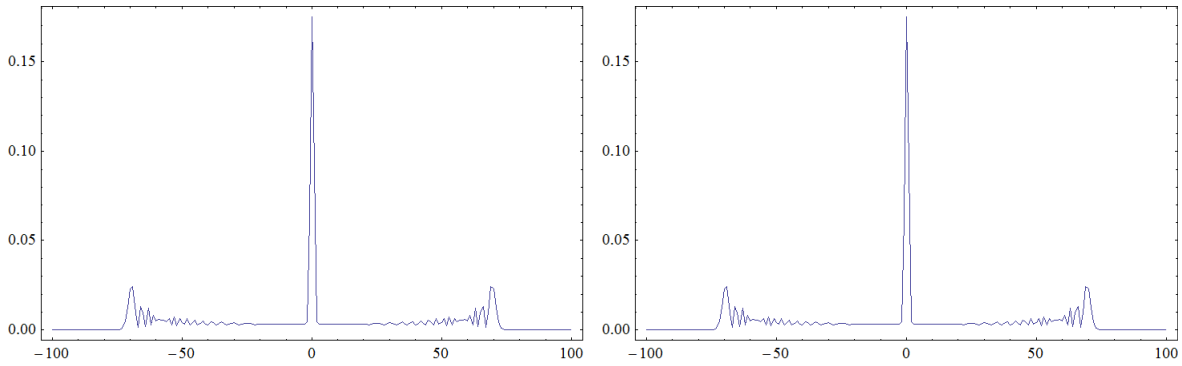
(a) Tiempo de Simulación 598.592 segundos **(b)** Tiempo de Simulación 634.113 segundos

Figura 4.2.1: Ambas Graficas fueron obtenidas utilizando el estado de Bell $|\phi^+\rangle$y 100 pasos de iteración, la figura a) fue obtenida utilizando moneda de Grover ; la figura b) fue obtenida utilizando moneda de Pauli "σ_y"



(a) Tiempo de simulación 699.54 segundos **(b)** Tiempo de Simulación 740.366 segundos

Figura 4.2.2: Ambas Graficas fueron obtenidas utilizando el estado de Bell $|\phi^-\rangle$y 100 pasos de iteración, la figura a) fue obtenida utilizando moneda de Grover; la figura b) fue obtenida utilizando moneda de Pauli "σ_y"



(a) Tiempo de simulación 676.701 segundos **(b)** Tiempo de Simulación 671.865 segundos

Figura 4.2.3: Ambas Graficas fueron obtenidas utilizando el estado de Bell $|\psi^+\rangle$y 100 pasos de iteración, la figura a) fue obtenida utilizando moneda de Grover; la figura b) fue obtenida utilizando moneda de Pauli "σ_y"

4.3. Nuevas Distribuciones Generadas con Estados Enlazados

Como discutimos en el capítulo anterior 3.1 una caminata cuántica se compone por dos sistemas físicos: un caminante y una moneda. Las propiedades de las caminatas cuánticas aplicando múltiples monedas ([41],[38]) sobre un caminante han sido bastante estudiadas así como las características de las caminatas cuánticas utilizando el operador de Grover como operador moneda ([40],[42],[38]) .

Sin embargo, el uso de caminatas cuánticas enlazadas es un campo poco estudiado ([36],[37]), sobretodo aplicando la moneda de Grover

Nuestras motivaciones para el uso de monedas enlazadas es que junto con un cambio en el operador de desplazamiento lleva a nuevas distribuciones del caminante que presentan características únicas, que pueden ser de utilidad para el mejoramiento de tiempos en el recorrido en los diagramas de árbol como discutimos en la siguiente sección

Revisando todos los resultado anteriores una pregunta que seria valida es, ¿Se pueden generar caminata cuya distribución de probabilidad tenga una mayor concentración sobre algún punto en particular?. La respuesta parece ser, si.

Para logra una concentración mayor respecto a la ubicación de la partícula se presenta a continuación una modificación al operador de evolución U ya conocido, esta modificación tiene la forma

$$U_{mod} = \left(|0\rangle_M\langle 0| \otimes \sum_{i=-\infty}^{\infty} |i+1\rangle_C\langle i|\right) + \left(|0\rangle_M\langle 1| \otimes \sum_{i=-\infty}^{\infty} |i+2\rangle_C\langle i|\right) + \left(|1\rangle_M\langle 0| \otimes \sum_{i=-\infty}^{\infty} |i-2\rangle_C\langle i|\right) + \left(|1\rangle_M\langle 1| \otimes \sum_{i=-\infty}^{\infty} |i-1\rangle_C\langle i|\right) \quad (4.3.1)$$

en esta modificación se aprecia una cambio en la combinación de los qubits y que el número de pasos aumenta dependiendo del estado en que la moneda se presenta.

Verificando las distribuciones que exhiben la graficas en la figuras 4.3.1, 4.3.2 y 4.3.3 podemos verificar que tienen un característica muy importante y que la desaparición de la zona de los picos externos es evidente, lo cual indica una mayor concentración de la distribución de probabilidad de encontrar al caminante.

Sin embargo se puede observar que el caminante recorre el resto del espacio con una baja probabilidad. Lo anterior indica que en una aplicación para un algoritmo de búsqueda, se tiene la certeza que el caminante examinará una gran espacio, dando una alta prioridad a una posición especifica.

Una consecuencia de la propiedad anterior de una caminata cuántica mucho más estrecha en su distribución al rededor de la posición $|0\rangle$.

Claro que el hecho de tener una mayor concentración de la distribución alrededor de cero no significa que el caminante no se pueda encontrar otros puntos de la recta, solamente que tiene una menor probabilidad de encontrarse en otros punto, pero verificamos que el caminante a pesar de tener un cambio total en su dinámica aun sigue abarcando un gran espacio en su recorrido.

Estas distribuciones resultan interesantes ya que se puede ver que para la aplicación de algoritmos resultarían de bastante provecho, como en el caso de un algoritmo de búsqueda.

Como uno de los objetivos futuros es que podamos aplicar estas nuevas distribuciones de caminatas cuánticas a un algoritmo de búsqueda cuántico, la relación que se tiene para su implementación como modelos de algoritmos se explica a continuación

4.4. Aplicación de Caminatas Cuánticas y Proyectos Futuros

Como se presenta en la sección anterior algo que caracteriza a las caminatas cuántica es su distribución de probabilidad tan particular que poseen así como su facilidad para cambiar la forma de su distribución. Estas distribuciones tan variadas tienen aplicaciones algorítmicas que serán brevemente descritas a continuación.

Al día de hoy, los algoritmos basados en caminatas cuánticas son un área de amplio estudio ya que resuelven diversas instancias de un problema de búsqueda, que en forma abstracta se plantea así: dado un espacio de estados traducible

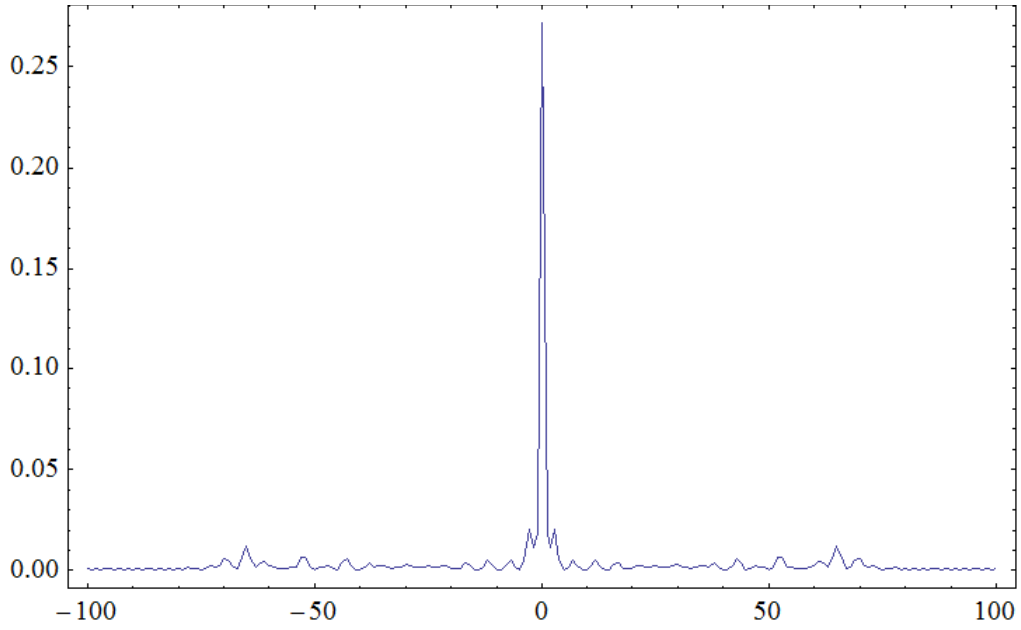


Figura 4.3.1: Caminatas con 100 pasos usando el operador de Grover, un estado inicial $|\gamma_0^1\rangle$ y el operador de desplazamiento modificado

a un grafo$R$, encontrar un estado particular que tiene una marca distintiva, a través de la ejecución de una caminata cuántica en R. El planteamiento se generaliza fácilmente para localizar un conjunto de estados marcados, en vez de uno solo.

Por supuesto, con la lectura del párrafo anterior, una pregunta asalta la mente: ¿es razonable suponer que el nodo buscado tendrá siempre una marca distintiva? La respuesta se puede dar en dos planos distintos:

1. Para aplicaciones concretas de algoritmos de búsqueda, es común estar en posibilidad de distinguir el nodo que buscamos del resto.

2. En algunos problemáscuya solución algorítmica está inspirada en procesos físicos, es posible garantizar que el nodo buscado está marcado por el valor mínimo (o máximo) de la propiedad física incorporada en el algoritmo.

Por supuesto, que una propagación cuadraticamente más veloz en una linea no es un algoritmo, pero para ser un comienzo esta en una buena caracteristica.

Se han estudiado y trabajo con caminatas cuánticas para el desarrollo de algoritmos en este caso en particular para algoritmos de búsqueda.

Como se ha revisado a lo largo de esta tesis el primer algoritmo cuántico para este problema se debe a L. K. Grover (1996), utilizando un método diferente para obtener la misma velocidad cuadrática. Un problema clásico de búsqueda de una base de datos no indexados, por ejemplo, a partir de un número de

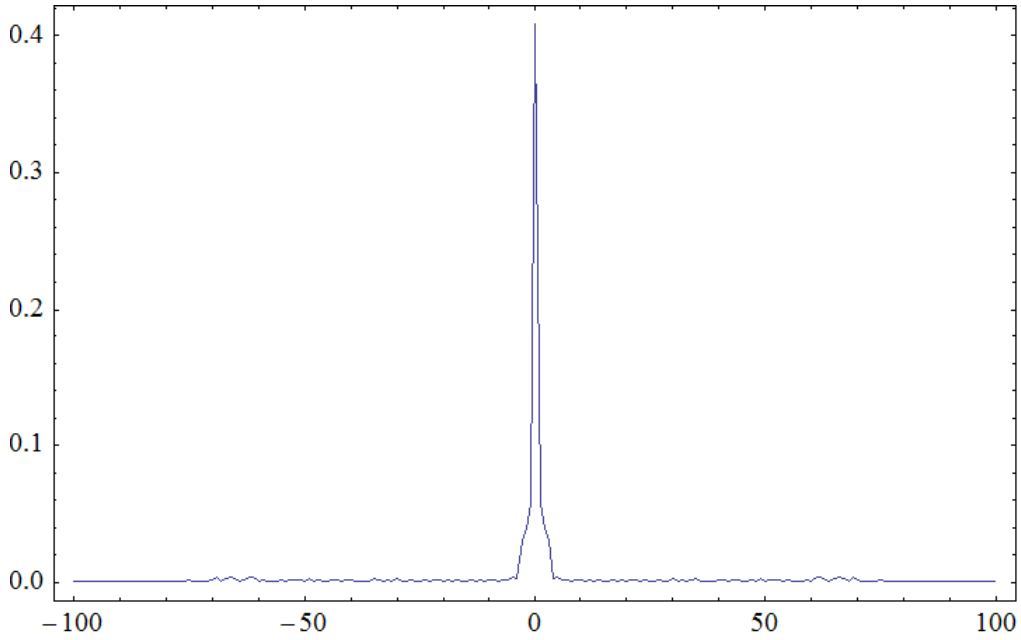


Figura 4.3.2: Caminatas con 100 pasos usando el operador de Grover, un estado inicial $|\gamma_0^2\rangle$ y el operador de desplazamiento modificado

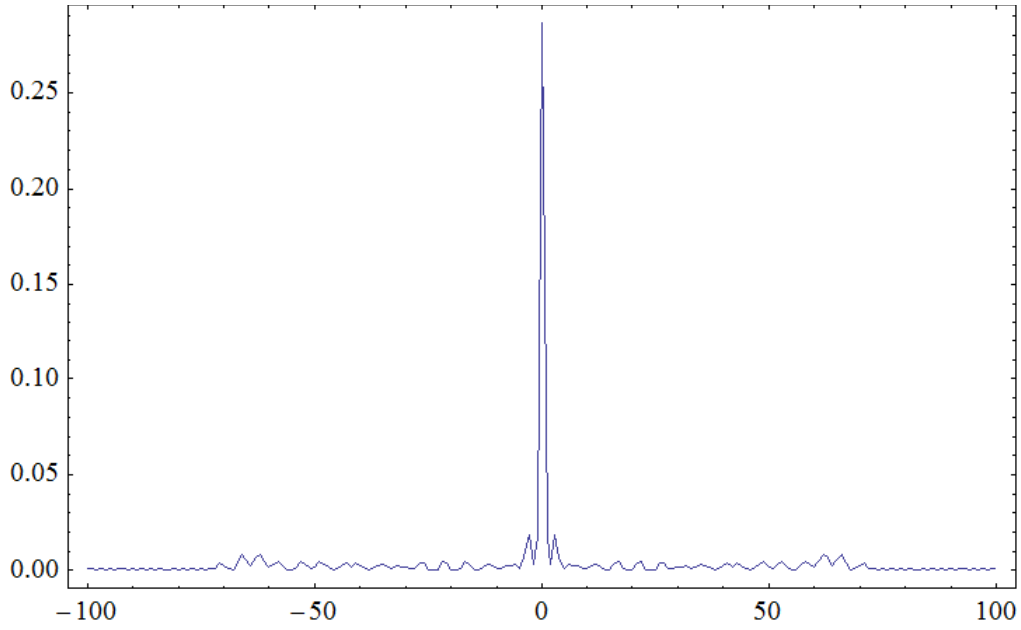


Figura 4.3.3: Caminatas con 100 pasos usando el operador de Grover, un estado inicial $|\gamma_0^3\rangle$ y el operador de desplazamiento modificado

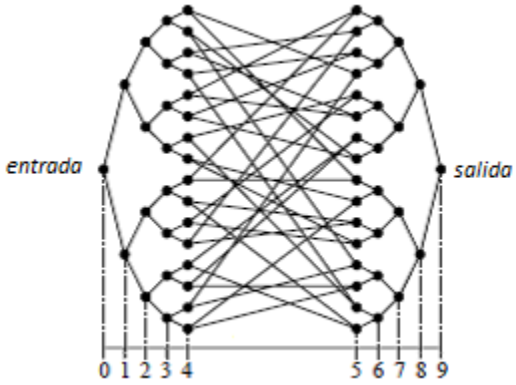


Figura 4.4.1: Ejemplo de la red de Childs et al. (2003). La diferencia entre las columnas 4 y 5 es solo para modelar, la longitud de los caminos es la misma entre todos los nodos.

teléfono y buscar una guía telefónica para encontrar el nombre correspondiente, que potencialmente tiene que comprobar todas las entradas de N en la base de datos, y en promedio tiene que comprobar al menos la mitad. También ya se sabe que este algoritmo tan sólo requiere $\sqrt{N}$ consultas.

En 2003 Childs, demostró que una caminata cuántica podría realizar exponencialmente más rápido que cualquier algoritmo clásico, cuando la búsqueda de una ruta a través de un tipo particular de red. Este es un problema bastante artificial, pero resulta, en principio, que camina cuántica son una poderosa herramienta .

La tarea consiste en encontrar el camino desde el nodo de entrada al nodo de salida, tratando el resto de la red como un laberinto en el que no se puede ver los otros nodos desde donde se está parado, sólo la elección de caminos. Es fácil decir en qué dirección es hacia adelante hasta que que se llega a los puntos aleatorios del centro. Después de esto, cualquier intento en forma clásica de elegir el camino correcto hacia la salida resultará en perdida en la región central y toma una forma exponencial , en promedio, para encontrar la salida.

Una caminata cuántica, en cambio, viaja a través de todos los caminos de superposición, y la interferencia cuántica entre diferentes caminos permite al caminante cuántico de averiguar qué camino es hacia adelante hasta la salida que se encuentra en un tiempo proporcional a la anchura de en la red.

Lo expuesto anteriormente, es lo que motiva este y futuros trabajos sobre la investigación para el desarrollo de nuevos algoritmos de búsqueda que no solo aprovechen los fenómenos cuánticos sino que se basen en el uso de caminatas cuánticas[31], además de buscar una implementación real del algoritmo de Grover, en computación clásica.

Capítulo 5

Conclusiones

En este trabajo de tesis se presentaron argumentos en los que se demuestran las ventajas que ofrece y el estudio de sistemás cuanticos para unprocesamiento máseficiente de la información

Además estudiamos los fenómenos de superposición y enlazamiento que al explotarlos a nuestro favor ayudan al mejoramiento en el procesamiento de información.

La descripción y las simulaciones que se presenta en el capítulo tres nos muestran que en el algoritmo de Grover tiene resultado provechosos para el problema búsqueda no indexada, debido a su capacidad para la evaluación de una gran cantidad entradas en forma paralela, en un solo paso del algoritmo, sin la necesidad de programación en paralelo y sin el requerimiento de grandes cantidades de hardware.

Los resultados discutidos en el cuarto capítulo demostraron que las distribuciones de probabilidad de un caminante cuántico se expanden de forma veloz a lo largo de una recta, además se exhibió que una particularidad que tienen las caminatas cuánticas es su facilidad para manipularlas por medio de sus operadores y la forma en que se cambia su estado inicial.

Los resultados más importantes de este trabajo radican en el uso de caminatas cuánticas en altas dimensiones, que muestran en primer lugar la fiel reproducción de resultados de importantes trabajos de investigaciones de caminatas cuánticas.

También se propuso un cambio en el uso del operador de Pauli contra el operador de Grover, que muestran no solo los mismos resultados en las simulaciones sino que además dan una considerable mejora en los tiempos de simulación de las caminatas cuántica presentadas en la investigación del Doctor Salvar Andraca.

Los resultados centrales de esta tesis muestran nuevas formásen la distribución presentados, cuya concentración un sus distribuciones reflejan una clara concentración en una región especifica, que son de importancia en el desarrollo de algoritmos de búsqueda.

El problema que se trata de resolver en esto momentos es el de generan nuevos algoritmos de búsqueda, basados en las caminatas cuánticas, que por su

fenómeno de superposición que presentan han mostrado tener bastante posibilidades para el desarrollo de algoritmos que resuelvan de forma máseficiente los problemásque los algoritmos usados en la actualidad.

Apéndice A

Mecánica Cuántica

A finales del siglo XIX las evidencias apuntaban a que las física clásica daba predicciones que estaban en total desacuerdo con los resultados del laboratorio. Esto llevo a un cambio profundo en los conceptos básicos del entendimiento de la naturaleza. Una nueva teoría, fue construida, la Mecánica Cuántica es la herramienta para la descripción del comportamiento de la materia y la luz en todos sus detalles, en particular, del comportamiento de la naturaleza a escala atómica.

La forma mástradicional de comenzar el estudio de la Mecánica Cuántica es siguiente el desarrollo historico. Usando este camino se puede apreciar como es que los cientificos durante el primer cuarto del siglo XX fueron forzados a abandonar los tan arraigados conceptos de la física clásica y como es que a pesar de tomar caminos errado lograron formalar la Mecánica Cuántica.

Sin embargo en este trabajo no seguiremos esta forma de estudio, y solo pasaremos a dar una introducción másconcisa de las herramientas necesarias para el desarrollo de este trabajo

Nadie sabe como el mundo físico opera en la realidad. Lo único que se puede hacer es modelarlo. La Mecánica Cuántica se desarrolla por cuatro postulados básicos, los cuales dirán como se representan los sistemásfísicos, como representar las observaciones, como llevar a cabo las mediciones y como evolucionan los sistemáscuando no "son medidos". Ninguna de estas reglas son obvias o naturales. Pero antes de describir las leyes de la Mecánica Cuántica, se explicaran las bases matemáticas, que tiene como propósito principal el familiarizarse con la notación algebraica usada en Mecánica Cuántica.

A.1. Preliminares Matemáticos

A.1.1. Notación de Dirac y Espacios de Hilbert

Los fenómenos que ocurren en la Mecánica Cuántica, por lo tanto de la Computación Cuántica, son caracterizados matemáticamente, en la forma de funciones que pueden ser expresados como espacios vectoriales.

Todos los espacios vectoriales considerados en este trabajo, tendrán la característica de que serán sobre el espacio de los números complejos, y también son de dimensión finita, esto ayudará a la simplificación de las matemáticas necesarias. Estos espacios vectoriales forman parte de una clase denominada espacios de *Hilbert* y usaremos $\mathcal{H}$ para denotar estos espacios.

El concepto de espacio de Hilbert es una generalización del concepto de un espacio euclídeo. Esta generalización permite que las nociones y técnicas algebraicas y geométricas aplicables a espacios de dimensión dos y tres se extiendan a espacios de dimensión arbitraria, incluyendo a espacios de dimensión infinita. Ejemplos de tales nociones y técnicas son la ortogonalidad de vectores, el teorema de Pitagóricas, proyección ortogonal y distancia entre vectores

Es claro que esta noción tiene que ser ampliada, entonces es importante dar una definición clara y formal de lo que se refiere a un Espacio de Hilbert.[5]

El espacio vectorial lineal y normado definido por las funciones ψ_n con el conjunto de funciones de cuadrado integrable

$$\int \psi_n^* \psi_n dx < \infty \tag{A.1.1}$$

el espacio vectorial así constituido se suele denotar como $\mathcal{L}^2$,que de hecho denota la norma del espacio de *Lebesque* de orden 2 [1]; con el producto interno definido como

$$(\psi_n, \psi_m) = \int \psi_n^* \psi_m dx \tag{A.1.2}$$

Generalizando lo anterior a un espacio donde los elementos son funciones que toman el rol de vectores, en Mecánica Cuántica se tendrá la oportunidad de trabajar tanto con vectores discretos en dimensiones finitas, como vectores de dimensiones infinitas. Estos elementos en el espacio de Hilbert pueden ser complejos.

La notación de álgebra lineal utilizada en Computación Cuántica resulta, en el área de la ingeniería, algo con la que se esta poco familiarizado.Nos referimos a la notación de Dirac, que fue introducida por el matemático Pauli Dirac, la cual es una herramienta conveniente usada para la representación de vectores en Mecánica Cuántica. Los estados de los sistemásfísicos son representados por vectores en Mecánica Cuántica.

En libros de matemáticas o física, los vectores son comúnmente representados con una flecha para identificarlos, por ejemplo $\overrightarrow{a}$, en una representación matricial podemos usar este vector presentándolo de la forma

$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_2 \end{pmatrix} \tag{A.1.3}$$

[1] Se refiere a espacios del tipo $\mathcal{L}^p$,son los espacios vectoriales normados más importantes en el contexto de la teoría de la medida

En la Notación de Dirac el símbolo para identificar a un vector se escribe dentro de un *ket* y se representa como, $|a\rangle$.

Es muy importante notar que para construir productos escalares no bastan estos vectores, sino que es necesario introducir el conjunto de vectores duales anteriores, definidos como las correspondientes matrices adjuntas, de tal manera que se tiene que

$$a^\dagger = \begin{pmatrix} a_1 & \cdots & a_2 \end{pmatrix} \tag{A.1.4}$$

Este conjunto de vectores $\{a^\dagger\}$ representa una base en el espacio dual generado por lo vectores columna $\{a\}$.

Por lo tanto se denota al vector dual de a con un *bra* $\langle a|$ que en conjunto forman los *brakets.* Ahorarevisaremos cuidadosamente las definiciones de conceptos de álgebra lineal de interés para la Computación Cuántica, usando la notación de Dirac.

Los kets son presentados por vectores columna. En términos del plano Cartesiano *x-y,* un punto *p=(a,b)* puede representarse como un vector columna a

$$p = \begin{pmatrix} a \\ b \end{pmatrix} \tag{A.1.5}$$

o, como en notación vectorial, como $p = ax + by$, o en la notación de Dirac, como $|p\rangle = a|x\rangle + b|y\rangle$. En el caso de coordenadas Cartesianas, a y b deben ser números reales. En Mecánica Cuántica, los coeficientes a y b tienen la posibilidad de ser complejos. Un estado cuántico puede ser escrito como $\psi = (\alpha, \beta)$ o en notación de Dirac, $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$, donde α y β son números complejos

Ahora pasemos a la definición de un espacio dual, como ya se definió sea $\mathcal{H}$ un espacio de Hilbert. El espacio de Hilbert $\mathcal{H}^*$esta definido como el conjunto de mapeo lineal de $\mathcal{H} \to \mathbb{C}$, entonces lo anterior nos dice que un vector dual $\langle\psi|$ es un operador lineal del espacio vectorial $\mathcal{H}$ a los números complejos del conjunto $\mathbb{C}$. El conjunto de mapeo $\mathcal{H}^*$es un espacio vectorial complejo en si, y es lo que se llama espacio vectorial dual asociado con $\mathcal{H}$

El vector $\langle\psi|$ es llamado el dual de $|\psi\rangle$. En términos de presentación matricial $\langle\psi|$ se obtiene apartir de $|\psi\rangle$ tomando su correspondiente matriz fila y calculamos su complejo conjugado. Si $|\psi\rangle$lo escribimos como un vector columna

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{A.1.6}$$

entonces su dual $\langle\psi|$ es el vector fila

$$\psi^* = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \tag{A.1.7}$$

donde ψ^* es el transpuesto conjugado de ψ. En notación de Dirac $\langle\psi|$ puede ser escrito como

$$\langle\psi| = \alpha^*\langle x| + \beta^*\langle y| \tag{A.1.8}$$

A.1.2. Bases e Independencia Lineal

Un conjunto generador de un espacio vectorial es el grupo de vectores $|v_1\rangle, ..., |v_n\rangle$ de tal manera que cualquier vector $|v\rangle$en el espacio vectorial puede ser escrito como combinación lineal $|v\rangle = \sum_i a_i|v_i\rangle$ de vectores en este grupo. Es decir, se consideraun conjunto generador para el espacio vectorial $\mathbb{C}^2$ que es el grupo

$$|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix};\ |v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{A.1.9}$$

como cualquier vector

$$|v\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \tag{A.1.10}$$

en $\mathbb{C}^2$ puede ser escrita como combinación lineal $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$ de los vectores $|v_1\rangle$ y $|v_2\rangle$. Se dice que los vectores $|v_1\rangle$ y $|v_2\rangle$ generan el espacio vectorial $\mathbb{C}^2$.

Generalmente, un espacio vectorial debe tener diferentes conjuntos generadores. Un segundo conjunto generador para el espacio vectorial $\mathbb{C}^2$ es el conjunto

$$|v_1\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix};\ |v_2\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{A.1.11}$$

como un vector arbitrario $|v\rangle = (\ a_1,\quad a_2\ )$ puede ser escrito como combinación lineal de $|v_1\rangle$ y $|v_2\rangle$

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}}|v_1\rangle + \frac{a_1 - a_2}{\sqrt{2}}|v_2\rangle \tag{A.1.12}$$

Un conjunto de vectores distintos de cero $|v_1\rangle, ..., |v_n\rangle$ se dice que son *linealmente independientes* si existe un conjunto de número complejos $a_1, \ldots, a_n$ con $a_i \neq 0$ para al menos un valor de *i,* de tal manera

$$a_1|v_1\rangle + a_2|v_2\rangle + \cdots + a_n|v_n\rangle = 0 \tag{A.1.13}$$

Otra forma de decir esto es que si un vector del conjunto puede ser escrito como combinación lineal de otros vectores en el conjunto, entonces el conjunto es *linealmente dependiente.*

Esta idea es importante porque los conjuntos de vectores que son linealmente independientes, generan un espacio vectorial y forman una base para dicho espacio. Entre las propiedades de los vectores linealmente dependientes e independientes encontramos:

1. Un conjunto de vectores es linealmente dependiente si y solo si alguno de los vectores es combinación lineal de los demás.

2. Si un conjunto de vectores es linealmente independiente cualquier subconjunto suyo también lo es. Obviamente, si se tiene un conjunto de vectores

tales que ninguno de ellos es combinación de los demás, escogiendo solamente unos cuantos, no podrán ser combinación de los otros.

3. Si un conjunto de vectores es linealmente dependiente también lo es todo conjunto que lo contenga. Ya que un conjunto de vectores es linealmente dependiente si y solo si tiene algún vector que es combinación lineal de los demás, si metemos este conjunto de vectores en otro más grande, seguimos teniendo el vector que es combinación lineal de otros, por tanto, el conjunto más grande sigue siendo linealmente dependiente.

A.1.3. Productos Vectoriales en los Espacios de Hilbert

Existen dos productos entre los vectores que son muy utilizados en los espacios de Hilbert, nos referimos al producto interno y al producto externo pero másadelante estudiaremos un tercero denominado producto tensorial.

Para podamos tener una mejor compresión de ambos conceptos, estos serán presentados con ejemplos de como actúan estos productos.

Producto Interno y Ortonormalidad

El *producto interno* es una función que toma dos vectores $|\psi_i\rangle$ y $|\psi_j\rangle$ de un mismo espacio de Hilbert y produce un número complejo a la salida. El producto interno resulta ser una generalización para el concepto producto punto usado con vectores en espacios Euclidianos.

Comúnmente estamos familiarizados con una notación de producto interno que tiene la siguiente forma

$$(\psi_i, \psi_j) = \int \psi_i^*(x)\psi_j(x)dx \tag{A.1.14}$$

En la notación de Dirac para representar el producto interno entre dos vectores se define como $\langle\psi_i|\psi_j\rangle$ y la notación $\langle\psi|$ es llamado *vector dual* del vector $|\psi\rangle$.

Para calcular el producto interno entre dos vectores, debemos obtener el *vector dual,* que se tiene definido como

$$(|\psi\rangle)^\dagger = \langle\psi| \tag{A.1.15}$$

$$|\psi_i\rangle = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_3 \end{bmatrix} \Rightarrow \langle\psi| = \begin{bmatrix} z_1^* & z_2^* & \cdots & z_3^* \end{bmatrix} \tag{A.1.16}$$

Entonces si el producto interno entre dos vectores resulta ser cero,

$$\langle\psi_i|\psi_j\rangle = 0 \tag{A.1.17}$$

se dice que $|\psi_i\rangle, |\psi_j\rangle$son *ortogonales* el uno del otro.

Cuando la norma del vector es la unidad, se dice que el vector esta normalizado, esto es que

$$\langle\psi|\psi\rangle = 1 \tag{A.1.18}$$

El producto interno es un número complejo. Su conjugado debe satisfacer

$$\langle\psi_i|\psi_j\rangle^* = \langle\psi_j|\psi_i\rangle \tag{A.1.19}$$

El producto interno es útil para definir la norma Euclidiana de $|\psi\rangle$, calculando el producto interno de un vector consigo mismo

$$||\psi|| = \sqrt{\langle\psi|\psi\rangle} \tag{A.1.20}$$

Un vector se dice vector unitario si tiene norma igual a 1. Hay que notar que la norma es un número real; y por lo tanto se puede definir la longitud. Un conjunto de vectores unitarios que son mutuamente ortogonales se les llama base ortonormal.

Por lo expuesto anteriormente se define una función que se usa para la definición de una base ortonormal llamada delta de Kronecker,$\delta_{i,j}$

$$\delta_{i,j} \equiv \begin{cases} 0 & para\, i \neq j \\ 1 & para\, i = j \end{cases} \tag{A.1.21}$$

Para cualquier vector $|\psi\rangle$se tiene que

$$\langle\psi|\psi\rangle \geq 0 \tag{A.1.22}$$

Si un ket es un vector columna, el vector dual o bra sera un vector fila cuyos elementos son los complejos conjugados de los elementos de el vector columna.

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}^\dagger = \begin{pmatrix} a_1^* & a_2^* & \cdots & a_n^* \end{pmatrix} \tag{A.1.23}$$

La discusiones en Mecánica Cuántica a menudo se refieren a *espacios de Hilbert.* En los espacios vectoriales complejos de dimensiones finitas que se presentan en Computación Cuántica, un espacio de Hilbert formalmente definido es un espacio complejo vectorial completo en el que un producto interno esta definido.

Sea $|\psi\rangle$y $|\phi\rangle$ dos vectores pertenecientes a un espacio complejo V y sea α y β números complejos, entonces las siguientes propiedades se mantienen para el producto interno

1. $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$
2. $\langle\psi\,(\alpha|\phi\rangle + \beta|\phi\rangle) = \alpha\langle\psi|\phi\rangle + \beta\langle\psi|\phi\rangle$

3. $(\langle\alpha\psi| + \langle\beta\psi)\,|\phi\rangle = \alpha^*\langle\psi|\phi\rangle + \beta^*\langle\psi|\phi\rangle$

4. $\langle\psi|\psi\rangle \geq 0$

Ejemplo

Se definen dos vectores complejos en un espacio de tres dimensiones como

$$|\psi\rangle = \begin{pmatrix} 2 \\ -7i \\ 1 \end{pmatrix},\ |\phi\rangle = \begin{pmatrix} 1+3i \\ 4 \\ 8 \end{pmatrix}$$

Hallar $\langle\phi|\psi\rangle$y $\langle\psi|\phi\rangle$y la norma de ambos vectores

Solución

Necesitamos el dual de cada uno de los vectores entonces

$$|\psi\rangle = \begin{pmatrix} 2 \\ -7i \\ 1 \end{pmatrix} \Rightarrow \langle\psi| = \begin{pmatrix} 2 & 7i & 1 \end{pmatrix}$$

$$|\phi\rangle = \begin{pmatrix} 1+3i \\ 4 \\ 8 \end{pmatrix} \Rightarrow \langle\phi| = \begin{pmatrix} 1-3i & 4 & 8 \end{pmatrix}$$

Entonces los productos internos de $\langle\phi|\psi\rangle$y $\langle\psi|\phi\rangle$ son

$$\langle\psi|\phi\rangle = \begin{pmatrix} 2 & 7i & 1 \end{pmatrix} \begin{pmatrix} 1+3i \\ 4 \\ 8 \end{pmatrix} = 2(1+3i) + 7i(4) + 1(8) = 10 + 34i$$

$$\langle\phi|\psi\rangle = \begin{pmatrix} 1-3i & 4 & 8 \end{pmatrix} \begin{pmatrix} 2 \\ -7i \\ 1 \end{pmatrix} = (1-3i)2 + 4(-7i) + 1(8) = 10 - 34i$$

Ahora se obtendrá la norma estos vectores

$$\langle\psi|\psi\rangle = \begin{pmatrix} 2 & 7i & 1 \end{pmatrix} \begin{pmatrix} 2 \\ -7i \\ 1 \end{pmatrix} = 2(2) + 7i(-7i) + 1(1) = 54$$

$$\Rightarrow ||\psi|| = \sqrt{\langle\psi|\psi\rangle} = \sqrt{54} = 3\sqrt{6}$$

$$\langle\phi|\phi\rangle = \begin{pmatrix} 1-3i & 4 & 8 \end{pmatrix} \begin{pmatrix} 1+3i \\ 4 \\ 8 \end{pmatrix} = (1-3i)(1+3i) + 4(4) + 8(8) = 90$$

$$\Rightarrow ||\phi|| = \sqrt{\langle\phi|\phi\rangle} = \sqrt{90} = 3\sqrt{10}$$

Producto Externo

Existe una forma útil de representar operadores lineales, los cuales se trataran en las siguientes secciones, esta presentación hace uso de el producto interno, se conoce como la presentación *producto externo.*

Sea $|v\rangle$ un vector en un espacio de producto interno V, y $|w\rangle$un vector en un espacio de producto interno W. Se define $|w\rangle\langle v|$ como un operador lineal que actúa de la siguiente forma sobre un ket arbitrario $|\chi\rangle$

$$(|w\rangle\langle v|)\,|\chi\rangle = |w\rangle\langle v|\chi\rangle = \langle v|\chi\rangle|w\rangle \tag{A.1.24}$$

Se pueden tomar combinaciones lineales del operador de producto externo $|w\rangle\langle v|$ en la forma obvia. Por definición $\sum_i a_i|w_i\rangle\langle v_i|$ es un operador lineal el cual, cuando actúa sobre $|\chi\rangle$, produce $\sum_i a_i|w_i\rangle\langle v_i|\chi\rangle$a la salida

Esta utilidad de la notación del producto externo puede usarse para un importante resultado conocido como *relación completa* para vectores ortonormales. Sea $|i\rangle$cualquier base ortonormal para el espacio vectorial V, así un vector arbitrario $|v\rangle$ puede ser escrito como $|v\rangle = \sum_i v_i|i\rangle$ para algunos conjuntos de números complejo v_i. Se tiene que notar que $\langle i|v\rangle = v_i$ y por lo tanto

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i|i\rangle = |v\rangle \tag{A.1.25}$$

Esto solo puede ser cierto si $\sum_i |i\rangle\langle i| = 1$

Como la ultima ecuación es verdadera para todos $|v\rangle$ sigue que

$$I = \sum_i |i\rangle\langle i| \tag{A.1.26}$$

Esta ecuación es conocida como la relación completa. Una aplicaron que la relación completa es dar un significado para la presentación de cualquier operador en la notación de producto externo.Sea $A{:}V\rightarrow W$ es un operador lineal, $|v_i\rangle$es una bra ortonormal para V, y $|w_j\rangle$ una base ortonormal para W. Usando la relación completa a ambos se obtiene

$$A = I_W A I_V \tag{A.1.27}$$

$$= \sum_{ij} |w_j\rangle\langle w_j|A|v_i\rangle\langle v_i| \tag{A.1.28}$$

$$= \sum_{ij} \langle w_j|A|v_i\rangle|w_j\rangle\langle v_i| \tag{A.1.29}$$

el cual es una presentación de producto externo para A.

Ejemplo

Describir la acción del producto externo, representado de la forma, $A = |0\rangle\langle 0| - |1\rangle\langle 1|$ sobre el vector $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$

Solución

Tomando en cuenta la que nuestro vector es ortonormal, se tiene que

$$A|\psi\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|)\,\alpha|x\rangle + \beta|y\rangle =$$

$$= \alpha\,(|0\rangle\langle 0| - |1\rangle\langle 1|)\,|0\rangle + \beta\,(|0\rangle\langle 0| - |1\rangle\langle 1|)\,|1\rangle =$$

$$= \alpha\,(|0\rangle\langle 0|0\rangle - |1\rangle\langle 1|0\rangle) + \beta\,(|0\rangle\langle 0|1\rangle - |1\rangle\langle 1|1\rangle) =$$

$$= \alpha|x\rangle - \beta|y\rangle$$

Es fácil notar la acción realizada por este productor exterior, la cual consiste en la inversión de la fase del vector, esta forma de actuar se abordara con másdetalle en secciones subsecuentes.

A.1.4. Eigenvectores y Eigenvalores

El problema de los eigenvalores para álgebra lineal juega un papel importante en Mecánica Cuántica. La correspondencia funciona de la siguiente forma, la cual propuesta por Erwin Schrödinger[6] en su trabajo *Quantisierung als Eigenwertproblem.*

Para cada observable física, tal como la energía o el momento, existe un operador, que puede ser representado en forma matricial; los eigenvalores de la matriz son los posible resultados de la medición para ese operador. Como ejemplo se puede conocer el Hamiltoniano-[2] de un sistema físico dado. Se puede formar una matriz que represente este Hamiltoniano, los eigenvalores de esa matriz serán las posibles energías que el sistema puede tener.

El encontrar los Eigenvectores es también importante, porque ellos nos dan una base para el espacio y por lo tanto nos da una forma de representar cualquier estado. En esta sección se revisan brevemente los conceptos y técnicas de álgebra lineal que son necesarios para calcular valores y vectores propios.

Un *Eigenvectores* de un operador lineal A sobre un espacio vectorial, es un vector distinto de cero $|v\rangle$de tal manera que

$$A|v\rangle = k|v\rangle \tag{A.1.30}$$

donde k es un número complejo es conocido como *Eigenvalores* de A correspondiente a $|v\rangle$.Los eigenvalores y Eigenvectores de un operador dado se pueden encontrar examinando el operador en alguna representación matricial. Para hallar los eigenvalores y Eigenvectores de la matriz A se necesita su *ecuación característica* e igualarla a *cero.* La ecuación se encuentra considerando el determinante de la siguiente cantidad

[2]El operador *Hamiltoniano* en Mecánica Cuántica, es el correspondiente al observable de la energía total del sistema. Su espectro es el conjunto de los posibles resultados cuando se mide la energía total de un sistema. Debido a su estrecha relación con el tiempo de evolución de un sistema, es de fundamental importancia en la mayoría de las formulaciones de la teoría cuántica

$$det|A - \lambda I| = 0 \tag{A.1.31}$$

donde λ es una variable desconocida. Por el teorema fundamental del álgebra, se sabe que cada polinomio tiene al menos un raíz compleja, por lo que cada operador A tiene al menos un eigenvalor, y un eigenvector correspondiente. El *eigenespacio* correspondiente a un eigenvalor k es el conjunto de vectores los cuales tienen eigenvalor v.

Un *representación diagonal* para un operador A sobre un espacio vectorial V es una representación $A = \sum_i \lambda_i |i\rangle\langle i|$, donde los vectores $|i\rangle$ forman un conjunto ortonormal de eigenvectores para A, con los correspondientes eigenvalores λ_i. Se dice que un operador es *diagonalizable* si tiene una representación diagonal. Como ejemplo de una representación diagonal, se toma la matriz de Pauli Z que se puede escribir

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{A.1.32}$$

donde la representación matricial es con respecto a los vectores ortonormales $|0\rangle$ y $|1\rangle$, respectivamente. Las representaciones diagonales son conocidas como *descomposición ortonormal.*

Ejemplo

El Hamiltoniano para un sistema de dos estados esta dado por

$$H = \begin{pmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{pmatrix}$$

Una base para este sistema es

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

Encontrar los eigenvalor y eigenvectores de H, expresarlos en términos de $|0\rangle$ y $|1\rangle$

Solución

Se inicia con la obtención de la ecuación característica

$det(H - \lambda I) = det \begin{pmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = det \begin{pmatrix} \omega_1 - \lambda & \omega_2 \\ \omega_2 & \omega_1 - \lambda \end{pmatrix} = 0$

$$\Rightarrow \lambda^2 - 2\omega_1\lambda + (\omega_1^2 - \omega_2^2) = 0$$

Resolviendo la ecuación nos lleva a los eigenvalores

$$\lambda_1 = \omega_1 + \omega_2, \; \lambda_2 = \omega_1 - \omega_2$$

Ahora sea $|A\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ el eigenvector para $\lambda_1 = \omega_1 + \omega_2$. Entonces recordando la definición de eigenvalores y eigenvectores se tiene que

$$H|A\rangle = \lambda|A\rangle$$

$$\begin{pmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = (\omega_1 + \omega_2) \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\omega_1 a + \omega_2 b = (\omega_1 + \omega_2)a \Rightarrow b = a$$

Normalizando se obtiene que

$$1 = \langle A|A\rangle = (a^* \; a^*) \begin{pmatrix} a \\ a \end{pmatrix} = 2|a|^2, \Rightarrow a = \frac{1}{\sqrt{2}}$$

Entonces

$$|A\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Dando este eigenvector en termino de las bases del sistema

$$|A\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Ahora $|B\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ es el eigenvector para $\lambda_2 = \omega_1 - \omega_2$. Se tiene que

$$\begin{pmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = (\omega_1 - \omega_2) \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\omega_1 a + \omega_2 b = (\omega_1 + \omega_2)a \Rightarrow b = -a$$

Normalizando de nuevo

$$1 = \langle B|B\rangle = (a^* \; -a^*) \begin{pmatrix} a \\ -a \end{pmatrix} = 2|a|^2, \Rightarrow a = \frac{1}{\sqrt{2}}$$

Entonces el segundo eigenvector, se escribe también en termino de los estado base

$$|B\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

A.1.5. Operadores Lineales y Matrices

Los operadores juegan un papel importante en Mecánica Cuántica, puesto que los procesos físicos, tales como la medición, la evolución el en tiempo, o la rotación son hechos para el estado cuántico. La forma de realizar algun cambio físico en el estado cuántico es por medio de operaciones matemáticas, es decir, con los operadores.

Como es usual en Mecánica Cuántica, los operadores con los que se *utilizan sean operadorer lineales* A entre espacios vectoriales mapea cada vector $|\psi\rangle \in \mathcal{H}$ a otro vector $|\chi\rangle \in \mathcal{H}$

$$A\left(a|\psi\rangle + b|\chi\rangle\right) = aA|\psi\rangle + bA|\chi\rangle \tag{A.1.33}$$

Decimos que nuestro operador es lineal si para cada vector $|\psi\rangle$y para cualquier número complejo a, mantiene la siguiente condición

$$A\left(a|\psi\rangle\right) = aA\left(|v\rangle\right) \tag{A.1.34}$$

Cuando se dice que un operador lineal A esta definido *sobre* un espacio vectorial $\mathcal{H}$, se refiere que A es un operador lineal de $\mathcal{H}$ a $\mathcal{H}$. Un importante operador lineal, y el mássimple que se puede dar sobre cualquier espacio vectorial $\mathcal{H}$ es el *operador identidad*, I, defino por la ecuación $I|v\rangle \equiv |v\rangle$como podemos notar l deja inalterado el vector. Otra representación que tiene este operador identidad,y se discutirá con mayor detalle másadelante, es la siguiente

$$I = \sum_{i=1}^{n} |v_i\rangle\langle v_i|$$

que como vimos anteriormente la conocemos como relación de completes .

Otro operador lineal importante es el *operador cero,* el cual se denota como 0. El operador cero mapea todos los vectores al vector cero, $0|v\rangle \equiv 0$. Es claro que para A.1.34 una vez que la acción de un operador lineal A sobre una base especificada, la acción de A es completamente determinada sobre todas sus entradas.

Suponer que $\mathcal{H}_1, \mathcal{H}_2\, y\, \mathcal{H}_3$ son espacios vectoriales, y $A : \mathcal{H}_1 \to \mathcal{H}_2$ y $B : \mathcal{H}_2 \to \mathcal{H}_3$ son operadores lineales. Luego se usara la notación $D{=}BA$ *para deno*tar la *composición* de B con A, definida por $(BA)|v\rangle \equiv B(A(|v\rangle))$.

La forma másconveniente de entender operadores lineales es en termino de su *representación matricial*. De hecho, el operador lineal y la matriz resultan se completamente equivalentes. Para ver la conexión, es útil entender que una matriz compleja A de m por n con entradas A_{ij} es de hecho un operador lineal enviando vectores de un espacio vectorial $\mathbb{C}^n$ al espacio vectorial $\mathbb{C}^m$.

Representación Matricial de Operadores

Como ya se vio previamente un ket puede ser representado como un vector columna, al igual que un operador se puede representar como una matriz cuadrada. Lo que significa que la acción de un operador en un vector se reduce a una multiplicación de matrices. Esto hace que los cálculos sean relativamente sencillos. En un espacio vectorial de n-dimensiones, los operadores son representados por matrices de n por n. Si conocemos la acción de un operador A sobre una conjunto de base $|v_i\rangle$entonces podemos definir los elementos de la matriz del operador usando la siguiente relación

$$A = IAI = \left(\sum_j |v_j\rangle\langle v_j|\right) A \left(\sum_i |v_i\rangle\langle v_i|\right) = \sum_{ij} \langle v_i|A|v_j\rangle |v_i\rangle\langle v_j| \quad \text{(A.1.35)}$$

La cantidad $\langle v_i|A|v_j\rangle = A_{ij}$ es un número que representa el elemento de la matriz del operador A localizado en la fila i, columna j en las representaciones matriciales de operadores con respecto a la base $|v_i\rangle$

$$A = \begin{pmatrix} \langle v_1|A|v_1\rangle & \langle v_1|A|v_2\rangle & \cdots & \langle v_1|A|v_n\rangle \\ \langle v_2|A|v_1\rangle & \langle v_2|A|v_2\rangle & & \vdots \\ & & \ddots & \\ \langle v_n|A|v_1\rangle & \cdots & & \langle v_n|A|v_n\rangle \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & & \vdots \\ & & \ddots & \\ A_{n1} & \cdots & & A_{nn} \end{pmatrix} \quad \text{(A.1.36)}$$

En la siguiente sección se presenta operadores de particular interés en el tema de estudio, con las representaciones ya mencionadas.

Lo anterior puede llegar a parecer bastante abstracto y sin sentido pero se puede ejemplificar de la siguiente forma si suponemos que en algunas bases ortonormales $\{|v_1\rangle, |v_2\rangle, |v_3\rangle\}$un operador actúa de la siguiente forma:

$$A|v_1\rangle = 2|v_1\rangle$$

$$A|v_2\rangle = 3|v_1\rangle - i|v_3\rangle$$

$$A|v_3\rangle = -|v_2\rangle$$

y tendremos que escribir la representación matricial de este operador $\langle v_i|v_j\rangle = \delta_{ij}$ y así la representación matricial de A de esta base tiene la forma

$$(A_{ij}) = \begin{pmatrix} \langle v_1|A|v_1\rangle & \langle v_1|A|v_2\rangle & \langle v_1|A|v_3\rangle \\ \langle v_2|A|v_1\rangle & \langle v_2|A|v_2\rangle & \langle v_2|A|v_3\rangle \\ \langle v_3|A|v_1\rangle & \langle v_3|A|v_2\rangle & \langle v_3|A|v_3\rangle \end{pmatrix} = \begin{pmatrix} \langle v_1|\left(2|v_1\rangle\right) & \langle v_1|\left(3|v_1\rangle - i|v_3\rangle\right) & \langle v_1|\left(-|v_2\rangle\right) \\ \langle v_2|\left(2|v_1\rangle\right) & \langle v_2|\left(3|v_1\rangle - i|v_3\rangle\right) & \langle v_2|\left(-|v_2\rangle\right) \\ \langle v_3|\left(2|v_1\rangle\right) & \langle v_3|\left(3|v_1\rangle - i|v_3\rangle\right) & \langle v_3|\left(-|v_2\rangle\right) \end{pmatrix}$$

$$= \begin{pmatrix} 2\langle v_1|v_1\rangle & 3\langle v_1|v_1\rangle - i\langle v_1|v_3\rangle & \langle v_1|v_2\rangle \\ 2\langle v_2|v\rangle & 3\langle v_2|v_1\rangle - i\langle v_1|v_3\rangle & \langle v_2|v_2\rangle \\ 2\langle v_3|v_1\rangle & 3\langle v_3|v_1\rangle - i\langle v_1|v_3\rangle & \langle v_3|v_2\rangle \end{pmatrix}$$

Puesto que la base es ortonormal, será útil recordar la definición de ortonormalidad y por lo tanto se obtiene por resultado

$$A_{ij} = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 0 & -1 \\ 0 & -i & 0 \end{pmatrix}$$

Operadores Adjuntos, Hermitianos y Unitarios

Anteriormente se vio que un operador que actúa en un ket, genera ket, $A|\psi\rangle = |\phi\rangle$. Ahora se considerara la acción de un operado dentro de un producto interno, esto es $\langle\varphi|A|\psi\rangle$. Ahora si se usa el hecho $A|\psi\rangle = |\phi\rangle$, se tiene por resultado

$$\langle\varphi|A|\psi\rangle = \langle\varphi|\phi\rangle \tag{A.1.37}$$

Como el producto interno es solo es la representación de un número complejo, podemos presentar su complejo conjugado el cual esta dado por la relación $\langle\varphi|\phi\rangle = \langle\phi|\varphi\rangle^*$.

Cuando un operador esta presente dentro de un producto interno existe A un operador lineal en un espacio de Hilbert $\mathcal{H}$. Resulta que existe un operador lineal único $A^\dagger$en V tal este se convierte en

$$\langle\varphi|A^\dagger|\phi\rangle = \langle\phi|A|\varphi\rangle^* \tag{A.1.38}$$

Este operador lineal es conocido como *adjunto* o *Hermitiano conjugado* de el operador A. De esta definición se observa que $(AB)^\dagger = B^\dagger A^\dagger$.

Un operador A, cuyo adjunto es A se conoce como operador *Hermitiano* o *auto-adjunto.*

$$A = A^\dagger \tag{A.1.39}$$

Una importante clase de operadores Hermitianos son los *operadores de proyección.* Que serán definidos másadelante en esta misma sección

Un operado se dice que es *normal* si $AA^\dagger = A^\dagger A$. Un operador el cual es Hermitiano es también normal. Esta es un teorema de representación notable para operadores normales conocido como la *descomposición espectral,* que establece que un operador es un operador normal si y solo si es diagonalizable

Es frecuente el uso de operadores que conservan la norma o, másgeneral, el producto escalar de vectores reales. Un operador U ,se dice que es unitario si

$$UU^\dagger = U^\dagger U = I \tag{A.1.40}$$

De esta definición, se tiene que el adjunto de un operador unitario coincide con su inverso $U^\dagger = U^{-1}$

El operador unitario actúa en los vectores de la siguiente forma

$$U|\psi\rangle = |\psi'\rangle \tag{A.1.41}$$

pues a partir de la forma de actuar anterior se nota que

$$\langle\Omega'|\psi'\rangle = \left(\langle\Omega|U^\dagger\right)\left(U|\psi\rangle\right)\langle\Omega|\psi\rangle \tag{A.1.42}$$

Uno de los usos importantes de eso operadores es para la evolución en el tiempo de los sistemáscuánticos, que se detallaran pronto y como se aplican nuestro tema de estudio.

Operadores de Proyección

Para un espacio vectorial V *n-dimensional,* se denotaran un conjunto de vectores base ortonormales como $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle$ donde se retoma la definición de la delta de Kronecker

Un subespacio W de V es un subespacio de V, tal que W es por si mismo un espacio vectorial con respecto a la suma vectorial y al producto interno.

Ahora suponer que un subespacio es *m-dimensional,* donde $m < n$ y es expandida por un conjunto de vectores base ortogonales $|u_1\rangle, |u_2\rangle, ...|u_n\rangle$. Un operador de proyección o proyector P_m esta dado por:

$$P_m = \sum_{i=1}^{m} |u_i\rangle\langle u_i| \tag{A.1.43}$$

Estos tiene dos importantes propiedades

1. Un operador de proyección P es Hermitiano, $P = P^\dagger$.
2. Un operador de proyección P es idempotente, $P = P^2$.

De lo anterior se concluye que todo operador Hermitiano que cumple con la ecuación $P = P^2$ es un proyector

Un operador de Proyección puede ser formado de un base de vectores individual que pertenece a un conjunto ortonormal, $P_i = |u_i\rangle\langle u_i|$ es un operador de proyección valido. Este operador es obviamente Hermitiano, y es igual a su propio cuadrado:

$$P_i^2 = (|u_i\rangle\langle u_i|)\,(|u_i\rangle\langle u_i|) = |u_i\rangle\langle u_i|u_i\rangle\langle u_i| = |u_i\rangle\langle u_i| \tag{A.1.44}$$

Examinando un proyector construido de un base vectorial individual permite considerar la acción fundamental de un operador de proyección. Considerar la aplicación de P_i en un ket arbitrario $|\psi\rangle$:

$$P_i|\psi\rangle = |u_i\rangle\langle u_i|\psi\rangle = (\langle u_i|\psi\rangle)|u_i\rangle \tag{A.1.45}$$

El operador de proyección P_i *proyecta* la componente de $|\psi\rangle$ a lo largo de cualquier vector del espacio de Hilbert en la dirección de $|u_i\rangle$. Esto va de acuerdo con la relación de completes, la cual puede ser expresada de la siguiente forma.

Se representa el operador identidad por la sumatoría de proyectores, formados por productos externos de vectores bases

$$I = \sum_{i=1}^{m} |u_i\rangle\langle u_i| = \sum_{i=1}^{m} P_i \tag{A.1.46}$$

Operadores y Matrices de Pauli y Hadamard

Un conjunto de operadores que resulta de fundamental importancia en Computación Cuántica es conocido como *Operadores de Pauli*. Incluidos el operador identidad y el operador ceso, existen cuatro operadores de Pauli. Desafortunadamente existen diferentes notaciones usadas para estas operadores, los cuales se denotan a continuación como $\sigma_o, \sigma_1, \sigma_2$ y σ_3 o como $\sigma_o, \sigma_x, \sigma_y$ y σ_z o por I,X,Y y Z.

Comenzando con el primero de los Operadores de Pauli, se tiene el operador identidad. El operado actúa en la base computacional como

$$\sigma_o|0\rangle = |0\rangle,\ \sigma_o|1\rangle = |1\rangle \tag{A.1.47}$$

El siguiente operador se denota como $\sigma_1 = \sigma_x = X$ y se forma como sigue

$$\sigma_x|0\rangle = |1\rangle,\ \sigma_x|1\rangle = |0\rangle \tag{A.1.48}$$

Por esta razón X algunas veces es conocido como el *operador NOT*.

Continuando se tiene $\sigma_2 = \sigma_y = Y$, el cual actúa sobre las bases como

$$\sigma_y|0\rangle = i|1\rangle,\ \sigma_y|1\rangle = -i|0\rangle \tag{A.1.49}$$

Cuyo resultado se ve afectado en el intercambio de la probabilidad de amplitud en la base computacional multiplicada por j y $-j$ respectivamente.

Finalmente para completar el conjunto de los operadores de Pauli, se tiene a $\sigma_3 = \sigma_z = Z$, es cual se le conoce como el *operador de cambio de fase,* cuyo efecto sobre la base computacional es de la siguiente forma

$$\sigma_z|0\rangle = |0\rangle,\ \sigma_z|1\rangle = -|1\rangle \tag{A.1.50}$$

Como una simple regla del dedo pulgar puede darse cuenta de que el operador de de cambio de fase multiplica la amplitud de probabilidad del estado base de cálculo $|1\rangle\, por\, -|1\rangle$

Los operadores Pauli tienen su representación con producto externo, la cual nos serán de gran utilidad.

$$\sigma_0 = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{A.1.51}$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{A.1.52}$$

$$\sigma_y = i|0\rangle\langle 1| - i|1\rangle\langle 0| \tag{A.1.53}$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{A.1.54}$$

Alternativamente a estas representaciones, como se vio en la sección anterior, estos operadores se tiene su representación en forma matricial, formadas por matrices de 2X2 y su representación se forma como sigue

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

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

$$\sigma_2 \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

El *Operador de Hadamard* es otro operador lineal ampliamente usado para el desarrollo de los algoritmos, y es definido como un operador que actúa en la base computacional de la siguiente forma

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{A.1.55}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{A.1.56}$$

el cual claramente se verifica un estado de superposición entre las bases computacionales, y además este se representa de la forma matricial y en producto externo como

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

$$H = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0 - |1\rangle\langle 1|\right) \tag{A.1.57}$$

Por la forma de operar sobre las bases computacionales, este operador resulta ser uno de los núcleos en el desarrollo de los algoritmos cuánticos, ya que al generar los estados de superposición, es como se explota una de las ventajas del comportamiento de los algoritmos como se trabajara adelante.

Valor esperado de un Operador

En la Mecánica Cuántica, un valor medio esperado es generalmente referido como un valor esperado. Por lo tanto, el valor esperado es un promedio calculado (en lugar de medir). El término, valor esperado es un poco engañoso, ya que, a pesar de su nombre, no lo hacemos, en general, en realidad esperan obtener el valor esperado en cualquier medición dada.

Por ejemplo, si los dos únicos resultados posibles de una medición son +1 y -1, y si cada resultado es igualmente probable, entonces el valor esperado es cero. Pero, nunca obtendrá este valor esperado en cualquier medición. Las preguntas que se generan a partir de esto son:

Si un estado cuántico $|\psi\rangle$ es preparado varias veces, y se mide un operador dado A en cada momento, ¿Cual es el promedio de los resultados de las mediciones?.Este valor esperado se escribe como.

$$\langle A\rangle = \int_a^b \psi(x)^* A\psi(x)dx \tag{A.1.58}$$

El cual dado en la notación de Dirac tiene la forma de

$$\langle A\rangle = \langle\psi|A|\psi\rangle \tag{A.1.59}$$

A.1.6. Producto Tensorial

El *producto tensorial* es la forma de colocar los espacios vectorial juntos para formar un espacio vectorial másgrande. Sea $\mathcal{H}_1$y $\mathcal{H}_2$ espacios vectoriales de dimensiones m y n respectivamente y que $\mathcal{H}_1$ y $\mathcal{H}_1$ son espacios de Hilbert. Luego $V\otimes W$ *(*se lee V tensor W*)* es un nuevo espacio vectorial de Hilbert de dimensión $m\times n$. Los elementos de $V\otimes W$ son combinaciones lineales del 'producto tensorial' $|v\rangle\otimes|w\rangle$de elementos $|v\rangle$de V y W luego $|i\rangle\otimes|j\rangle$ es una base para $V\otimes W$. A menudo se usan la nataciones abreviadas $|v\rangle|w\rangle$, $|v,w\rangle$ o incluso $|v,w\rangle$ para el producto tensorial $|v\rangle\otimes|w\rangle$.Por definición el producto tensorial satisface las siguientes propiedades de linealidad básicas:

1. Para cualquier $c\epsilon\mathbb{C}$ y elementos $|v\rangle$ V y $|w\rangle$ de W,

$$z\left(|v\rangle\otimes|w\rangle\right) = (z|v\rangle)\otimes|w\rangle = |v\rangle\otimes(z|w\rangle) \tag{A.1.60}$$

2. Para $|v_1\rangle$ y $|v_2\rangle$ arbitrarias en V y $|w\rangle$en W,

$$(|v_1\rangle + |v_2\rangle)\otimes|w\rangle = |v_1\rangle\otimes|w\rangle + |v_2\rangle\otimes|w\rangle \tag{A.1.61}$$

3. Para $|w\rangle$ arbitraria en V y $|w_1\rangle$ y $|w_2\rangle$en W,

$$|v\rangle\otimes(|w_1\rangle + |w_2\rangle) = |v\rangle\otimes|w_1\rangle + |v\rangle\otimes|w_2\rangle \tag{A.1.62}$$

Pero,¿ qué tipo de operadores lineales pueden actuar en el espacio $V\otimes W$*?,* suponer que $|v\rangle$ y $|w\rangle$ son vectores en V y W respectivamente, y que A y B con operadores lineales que actúan sobre V y W. Después se puede definir un operador lineal $A\otimes B$ sobre $V\otimes W$ con la ecuación

$$(A\otimes B)(|v\rangle\otimes|w\rangle) = A|v\rangle\otimes B|w\rangle \tag{A.1.63}$$

La definición de $A\otimes B$ es entonces extendida a todos los elementos de $V\otimes W$ en una forma natural para asegurar la linealidad de , esto es

$$(A\otimes B)\left(\sum a_i|v_i\rangle\otimes|w_i\rangle\right) = \sum a_i A|v_i\rangle\otimes B|w_i\rangle \tag{A.1.64}$$

Toda esta discusión llega a ser bastante abstracta. Claro que se puede ser másconcreto pasando todo esto a una representación matricial másconveniente,

conocida como, *Producto de Kronecker*. Suponer que A es una matriz de $m \times n$, y que B es una matriz de $p \times q$. Entonces como una representación matricial se tiene que

$$A \otimes B = \overbrace{\left.\left[\begin{array}{cccc} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & 1_{m2}B & \dots & A_{mn}B \end{array}\right]\right\} mp}^{nq} \tag{A.1.65}$$

En términos de esta representación como $A_{11}B$ denota las submatrices $p \times q$ cuyas entradas son proporcionales a B, con la proporcionalidad general constante A_{11}. Por ejemplo, el producto tensorial de los $(1, 2)$ y $(2, 3)$es el vector

$$\left[\begin{array}{c} 1 \\ 2 \end{array}\right] \otimes \left[\begin{array}{c} 2 \\ 3 \end{array}\right] = \left[\begin{array}{c} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{array}\right] = \left[\begin{array}{c} 2 \\ 3 \\ 4 \\ 6 \end{array}\right]$$

El producto tensorial de dos matrices de Pauli como X y Y será

$$X \otimes Y = \left[\begin{array}{cc} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{array}\right] = \left[\begin{array}{cccc} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{array}\right]$$

Finalmente, se menciona una notación muy utilizada en el desarrollo de esta tesis

$$|\psi\rangle^{\otimes k} \tag{A.1.66}$$

lo único que significa es que $|\psi\rangle$es tensoriado consigo mismo k veces. Por ejemplo

$$|\psi\rangle^{\otimes 2} = |\psi\rangle \otimes |\psi\rangle \tag{A.1.67}$$

También se tiene una notación análoga que es usada para los operadores operadores en espacios vectoriales con producto tensorial.

Con todo lo expuesto anteriormente se da por terminada la parte de la revisión que da lugar a las matemáticas que usadas como base para la formulación de Mecánica Cuántica, cabe decir que toda esta revisión se hace desde un punto de vista de la mecánica matricial propuesta por Heisengberg, ya que el trata de esta teórica resulta másaccesible para la Computación Cuántica.

Ahora en la siguiente sección se abordara de manera concisa los cuatro postulado de la Mecánica Cuántica, en el cual, entre otras cosas, se dará una definición de los vectores de estados, de la evolución de ellos, y otros postulados que son la base de esta teoría.

A.2. Postulados de Mecánica Cuántica

A través de la historia, el hombre ha intentando dar expoliación del mundo físico real que lo rodea, aun que lo máscercano que se ha logrado es modelarlo. Una teoría propuesta puede ser considerada como una herramienta adecuada para la descripción de acontecimientos a nuestro alrededor si la diferencia o error entre las expectativas provenientes de la teoría y las observaciones se mantienen por debajo de cierto límite. Desde la prehistoria que la reglas las basaban en sus experiencias y observaciones, después la necesidad de tener másprecisión en como se modela el mundo físico, los antiguos griegos generaron aportes másprecisos por medio de observaciones.

mástarde Isaac Newton introdujo además de nociones formulas sofisticadas. Desde entonces durante los inicios del siglo XX, se creía que las leyes de Newton y Maxwell eran leyes correctas y universales de la física. Pero para la década de 1930, las teorías clásica enfrentaron grandes problemásen el intento de explicar los resultados observados de ciertos experimentos. Como resultado, una nueva teoría fue formulada llamada Mecánica Cuántica.

Al igual que todas la teorías, la Mecánica Cuántica se basa en cuatro postulados que forman una base solida para su desarrollo, y estos postulados son los que se presentan a continuación

A.2.1. Estados de un sistemásfísico

Postulado 1.

Para cada sistema físico aislado se asocia un espacio de Hilbert $\mathcal{H}$, el espacio de estados *del sistema. El sistema físico es completamente descrito por su* vector de estado*, el cual es un vector unitario $|\psi\rangle \in \mathcal{H}$. La dimensión de $\mathcal{H}$ depende de los grados de libertad específicos de la propiedad física bajo consideración.*

Este postulado implica que la combinación lineal de los vectores de estado es un vector de estado. Esto es conocido como el *principio de superposición* y es una descripción cuántica de los sistemásfísicos. En particular cada estado $|\psi\rangle$ puede ser descrita con una superposición de estados base $\{|\phi_i\rangle\}$en $\mathcal{H}$.

Entonces si $|\phi_1\rangle, |\phi_2\rangle, ..., |\phi_n\rangle$ son ket que pertenecen al espacio $\mathcal{H}$, la combinación lineal

$$|\psi\rangle = \alpha_{1|}|\phi_1\rangle + \alpha_{2|}|\phi_2\rangle + ... + \alpha_{n|}|\phi_n\rangle \tag{A.2.1}$$

es también un estado valido que pertenece a un espacio $\mathcal{H}$.

Una descripción alternativa del los estados cuánticos esta por el *operador de densidad*. El cual es Hermitiano positivo cuya traza es igual a 1. Un sistema cuántico cuyo estado $|\psi\rangle$es exactamente conocido se dice que es un *estado puro*. El operador de densidad de un estado puro esta dado por $\hat{p} = |\psi\rangle\langle\psi|$. Un operador densidad también describe *los estados cuánticos mezclados.* Un estado mezclado puede ser obtenido de una fuente aleatoria de estados puro. Por ejemplo, suponer que un sistema cuántico tiene un estado elegido de un

conjunto de posibles estados $\{|\psi\rangle_i\}$de acuerdo a la distribución de probabilidad $\{p_i\}$. Su operador de densidad esta dado por

$$\hat{\rho} = \sum_i p_i |\psi\rangle_i \langle\psi| \tag{A.2.2}$$

Los operadores de densidad no solo representan distribuciones sobre estados puros, ya que es posible tener dos conjuntos diferentes estado cuántico que da lugar al operador misma densidad.

A.2.2. Evolución en el Tiempo de un Sistema Cerrado

Postulado 2

Un sistema físico cerrado cambia en el tiempo, la Evolución de un sistema cuántico cerrado con un vector de estado $|\Psi\rangle$ es caracterizado por la transformación unitaria $\hat{U}$.

El estado de un sistema con vector de estado en el tiempo t_2 de acuerdo a su estado en el tiempo t_2 esta dado por

$$|\Psi(t_2)\rangle = \hat{U}|\Psi(t_1)\rangle \tag{A.2.3}$$

Este postulado describe las propiedades matemáticas que un operador de evolución debe de tener. El operador de evolución especifico requerido para describir el comportamiento de sistema cuántico particular depende del sistema en si. En el caso de un qubit simple, cada operador unitario puede ser generado en los sistemásfísicos. Incluso puede ser comparada con la famosa *ecuación de Schrödinger.*

La evolución de un sistema de un sistema cuántico esta descrito por la *ecuación de Schrödinger*

$$i\hbar \frac{d|\psi\rangle}{dt} = \hat{\boldsymbol{H}}|\psi\rangle \tag{A.2.4}$$

donde $\hbar$ es la constante de Planck y $\hat{\boldsymbol{H}}$ es un operador Hermitiano fijo, conocido como *Hamiltoniano* de un sistema cerrado,el cual es un operador Hermitiano que caracteriza la evolución del sistema y representa la función de la energía total del sistema . El Hamiltoniano de un sistema físico particular debe ser determinado y calculado para cada caso. En general, la comprensión del Hamiltoniano de un sistema físico particular es una difícil tarea.

La conexión entre las dos aproximaciones se hace por medio de la siguiente relación

$$\hat{U}|\Psi(t_1)\rangle = e^{\frac{-\imath H(t_2-t_1)}{\hbar}} \tag{A.2.5}$$

A.2.3. Mediciones Cuánticas

Postulado 3

Las mediciones cuánticas son descritas por un conjunto de operadores de medición $\left\{\hat{O}_n\right\}$*, el subíndice* n *marca el diferente resultado de medición, que actúa en el espacio de estado de el sistema que esta siendo medido.El medición de salida corresponde al valor de las* observables*, como son la posición, o el momento, los cuales son operadores Hermitianos que corresponden a las cantidades físicamente medibles.*

Una medición descriptiva esta dada por una *observable* $\hat{M}$, Un operador Hermitiano definido en el estado de espacios de un sistema cuántico. Por medio de la descomposición espectral

$$\hat{M} = \sum_i r_i \hat{P_{r_i}} \tag{A.2.6}$$

donde $\hat{P_{r_i}}$ es un operador proyector para el eigenespacio $E(r_i)$ definido por el eigenvalor r_i. El resultado de la medición corresponde al eigenvalor r_i de la observable $\hat{M}$.

Sea $|\psi\rangle$ el estado de un sistema cuántico inmediatamente antes de una medición. Entonces, la probabilidad que el resultado r_i ocurra esta dado

$$p(r_i) = \langle\psi|\hat{P_{r_i}}|\psi\rangle \tag{A.2.7}$$

y en la medición posterior, el estado cuántico $|\psi\rangle_{pm}$ asociado al resultado r_i esta dado por

$$|\psi\rangle_{pm} = \frac{\hat{P_{r_i}}|\psi\rangle}{\sqrt{p(r_i)}} \tag{A.2.8}$$

además los operadores de mediciones deben satisfacer la relación de completes

$$\sum_m M_m^\dagger M_m = I \tag{A.2.9}$$

puesto que esto garantizara que la suma de la probabilidades dará 1

$$\sum_m \langle\psi \mid M_m^\dagger M_m \mid \psi\rangle = \sum_m p(m) = 1 \tag{A.2.10}$$

En Mecánica Cuántica, la medición es un proceso no trivial y altamente contrario a la intuición por varias razones; primero, por que las mediciones se vuelven inherentemente probabilísticas, puesto que los posible resultados de algunas mediciones son distribuidas de acuerdo a cierta probabilidad de distribución.

Segundo, en cuanto una medición se haya sido realizada, el sistema es inevitablemente alterado debido a la interacción con los instrumentos de medición. Consecuentemente, para un sistema cuántico arbitrario, la medición previa y la posterior de los estados cuánticos por lo general son diferentes.

Tercero, con el propósito de realizar una medición es necesario definir un conjunto de operador de medición. Este conjunto de operadores deben cumplir un cantidad de reglas que permiten calcular la distribución de probabilidad actual, así como los estados cuánticos de la medición posterior.Se puede decir que las mediciones conectan el mundo real con el clásico, olas mediciones son la única herramienta con las cuales se pueden tener una percepción de lo que pasa en el mundo cuántico.

A.2.4. Sistemáscuánticos Compuestos

Hasta el momento se han discutido los postulados para el caso de un solo sistema. Si se necesita saber como un sistema aislado se comporta cuando no se le permite interactuar con otro, esto sería suficiente. Pero si se desea estudiar Computación Cuántica potencialmente útil, se necesitará entender como es que la Mecánica Cuántica funciona para sistemáscompuesto de varias partículas interactuando una con otra. Con el fin de describir el estrado de un sistema cerrado de n partículas, como evolucionan en el tiempo, y que pasa cuando es medido. Tratando grandes sistemáscomo un composición de subsistemas, permite una descripción exponencialmente máseficiente de operaciones actuando en un pequeño número de subsistemas

Postulado 4

Cuando dos sistemás físicos es tratado como un sistema combinado, el espacio de estado de un sistema compuesto físico $\mid \psi_T\rangle$ *puede ser determinado usando el producto tensorial de sistemásindividuales* $\mid \psi_T\rangle = \mid \psi_1\rangle \otimes \mid \psi_2\rangle$.

Después de conocer toda la parte teórica de fundamentos matemáticos y de postulados centrales de la Mecánica Cuántica se pasara a describir el modelo del computó cuántico, así como sus características másimportantes que la hacen tan poderosa.

Una de las consecuencias mas importantes que se deriva del cuarto postulado de la mecánica cuántica es la definición de uno de los fenómenos mas desconsertantes pero interesante asociados a los sistemas cuánticos compuestos denominado *enlazamiento cuántico* el cual será explicado a continuación

A.3. Enlazamiento Cuántico

Una de los aspectos mas inusuales y fascinantes de la mecánica cuántica es el hecho de que las partículas puedan estar *enlazadas*. Para el caso mas simple de dos sistemas cuánticos denotados como A y B. Si estos sistemas estuviese enlazados, significaría que los valores de ciertas propiedades del sistema A están correlacionadas con los valores que esas propiedades serán asumidas para el sistema B. Las propiedades pueden estar correlacionadas incluso cuando dos sistemas están espacialmente separados.

La raíz de esta idea viene del año 1935 cuando Eistein junto con Podolsky y Rosen publicaron un articulo titulados "Can the quantum-mechanical description of reality be considered complete?" [39], en el cual afirman que la teoría cuántica es incompleta y hace predicciones absurdas.

Esta afirmación se base en el hecho de que los sistemas físicos tienen valores definidos, sean o no observados. Esto es que el valor de la propiedad de un sistema esta perfectamente definido previo a que una se realice cualquier medición.

Para explicar esto EPR se enfocaron en las mediciones de posición y momento. La primera observación que se tuvo es que la posición x y el momento$p$ no conmutan

$$[x, p] = i\hbar \tag{A.3.1}$$

Como A.3.1 lo dice, x y p no tienen eigenestados simultáneos. Una consecuencia de este hecho es que si un valor definitivo es asumido para una de las variables, tomando el momento para este caso, entonces la variable posición, para este ejemplo, no puede estar en un eignestado definido.

En esta discusión es común denotar dos sistemas que están en posesión de *Alicia* y *Betty*. Las características medibles de estas partículas están que son posición y momento de denotan para la partícula de Alicia como x_a y p_a y análogamente se hará lo mismo para la partícula de Betty x_b y p_b. El escenario propuesto por EPR es el siguiente

- Las partículas interactúan, después las partículas son espacialmente separadas
- No existe ninguna otra forma de interacción entre las partículas. Se puede decir que estar tan separadas una de otra que ningún tipo de señal la puede conectar, ni siquiera una rayo de luz.

El sistema EPR tiene valores definidos para las siguientes propiedades

- La posición relativa de las dos partículas, que viene dada por $x_a - x_b$
- El momento total de las partículas, el cual es $p_a + p_b$

Sin embargo, previo a la medición, los valores de cada parámetro, x_a, x_b ó p_a, p_b, no están determinados de acuerdo la mecánica cuántica. Si Betty hace alguna medición el puede optar por medir el valor deseado. Si las medidas de momento, el obtiene un valor definido para p_b. Como $p_a + p_b$, Betty conoce el valor exacto de p_a incluso cuando el no haya hecho ninguna observación sobre la partícula que Betty posee.

EPR creían que debido a que Betty puede determinar o conocer los valores de la posición y el momento de la partícula de Alicia, estas propiedades tienen valores definidos, independientemente de son o no medidos. En contraste, la teoría cuántica dice que las funciones de onda de cada partícula existen en superposiciones y cada propiedad no tiene un valor determinado hasta que es

medida. Como la teoría cuántica no puede saber los valores definidos de cada propiedad antes de la medición, el EPR dijo que la teoría es incompleta. Podría haber algunas otras variables físicas que aún no sé nada de eso nos permitiría describir las propiedades definitivas de cada partícula con la teoría. Porque no sabemos lo que esas variables son, se les llama *variables ocultas*.

Esto es lo que EPR predijo y entonces cuando un sistema esta enlazado, significa que los sistemas de componentes individuales están realmente unidos como una sola entidad. Cualquier medida que observe una parte del sistema, en este caso la primera partícula, es en realidad una medición en todo el sistema. La función de onda para el sistema colapsa, y las dos partículas asumen estados definidos. En resumen, si dos sistemas están enlazados, la descripción de cada sistema tiene que ser hecho con referencia al estado del otro sistema, incluso si los sistemas integrantes son espacialmente separados y sin interacción.

Dentro de los estados enlazados no todos tienen el mismo nivel de enlazamiento y dentro de estos existen cuatro sistema de dos partículas que son de particular interés para el estudio de este trabajo, que son lo estados mas altamente enlazados que hay, estos son los estados de Bell.

A.3.1. Sistemas Bipartitos y Estados de Bell

Ahora que se tiene una idea de lo que significa que dos sistemas estén enlazados, se pasará a ver cómo trabajar con la descripción básica y las matemáticas de estos sistemas. Cuando un sistema se compone de dos subsistemas que dicen que es un *sistema bipartito*. Un ejemplo de esto es cuando Betty y Alicia tienen cada uno un miembro de un par enlazado de partículas. Recordando el cuarto postulado de la mecánica cuántica, donde se describen los sistemas compuestos. El espacio de Hilbert del sistema compuesto es el producto tensorial del espacio de Hilbert que describe el sistema de Alicia y el espacio de Hilbert que describe el sistema de Betty. Si representamos estos como H_a y H_b, respectivamente, entonces el espacio de Hilbert del sistema compuesto es

$$H = H_a \otimes H_b \tag{A.3.2}$$

Si se denota los estados base para Betty como $|b_i\rangle$y los estados bases para Alicia como $|a_j\rangle$, entonces los estados base para el sistema compuesto están dados por tomar el producto tensorial de los estados base de Betty y Alicia

$$|\alpha_{ji}\rangle = |a_j\rangle \otimes |b_i\rangle = |a_j\rangle|b_i\rangle = |a_j b_i\rangle \tag{A.3.3}$$

Las bases de Alicia y Betty son ortonormales, así que los estado base para los sistemas compuesto son

$$\langle\alpha_{ji}|\alpha_{kl}\rangle = \langle a_j b_i|a_k b_l\rangle = \langle a_j|a_k\rangle\langle b_i|b_l\rangle = \delta_{jk}\delta_{il} \tag{A.3.4}$$

Ahora se considera el estado cuántico $\psi\rangle$del sistema compuesto. Puede ser extendido en términos de los estados base de A.3.3 como se ve a continuación

$$|\psi\rangle = \sum_{j,i} c_{ji}|\alpha_{ji}\rangle = \sum_{j,i} |a_j b_i\rangle\langle a_j b_i|\psi\rangle \tag{A.3.5}$$

Como un ejemplo de bases para sistemas bipartitos, se pueden consideras las *bases de Bell.* Los miembros de las bases de Bell, algunas veces llamados *estados de Bell* o *Estados EPR,* son

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{A.3.6}$$

$$|\phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{A.3.7}$$

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{A.3.8}$$

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{A.3.9}$$

Apéndice B

Complejidad *Computacional*

Esta sección es escrita con el fin de aclarar ciertas dudas que pudieran surgir respecto a la de algoritmos, en la cual se introducen los conceptos de problemáspolinomiales, clases de problemásque son importantes considerar para la propuesta y desarrollo de algoritmos.

B.1. ¿Que es un algoritmo eficiente?

Para resolver cualquier problema, es necesario un cierta cantidad de recursos. Por ejemplo, el correr un algoritmo en una computadora es necesario *memoria, tiempo* y *energía.*

Para medir la eficiencia de un algoritmo dado, se intentará establecer una relación entre la duración de ejecución de dicho algoritmo, expresado en términos del número de operaciones elementales y el tamaño, expresado en términos del número de caracteres necesarios para codificar los datos del ejemplo tratado, lo que se conoce como *complejidad computacional.* Sin embargo, cuando se menciona que un algoritmo es el máseficiente, se entiende como el más rápido. Pero los requerimientos de tiempo de un algoritmo se expresan convencionalmente en términos de una sola variable, el tamaño del problema, que es el número de datos necesarios para describirlo. Expresando la eficiencia como una relación entre el tamaño (normalmente representado por n) y el número de operaciones necesarias, el análisis de la complejidad ilustra, como una cambio en n, afecta al tiempo de cómputo requerido.

Por lo anterior automáticamente estomáticamente surgen tres preguntas obligadas

- ¿Cuáles son las operaciones elementales que se van a tomar en cuenta?
- ¿Qué codificación de los datos permitirá medir el tamaño del ejemplo tratado?
- ¿Cuáles son las funciones que uniendo el tamaño al número de operaciones elementales permitirán decir que un algoritmo en eficaz?

Afortunadamente, la respuesta a la tercer pregunta, permita responder a las dos primeras.

El que la complejidad computacional considere el tamaño del problema no debería causar mayor problema. En general, se espera que problemásmás grandes requerirán más tiempo para resolverse que los máspequeños. Como ejemplo se puede determinar el mínimo de 1000 números, que supuestamente tomará más tiempo que el problema equivalente para 100 números supuestamente tomará más tiempo que el problema equivalente para 100 números, ¿pero qué tanto más?.

En este contexto, contar el número de operaciones consiste precisamente en contar el número de instrucciones ejecutadas. Desgraciadamente esto resultará en una medida de complejidad que variará de máquina a máquina. Alternativamente, se puede adoptar la definición más informal de una operación como un simple paso conceptual.

Para muchos algoritmos , el número de operaciones efectuadas es altamente dependiente de los datos y puede variar ampliamente de un caso a otro. Esto es muy útil al estimar el comportamiento del algoritmo. Normalmente, interesa más estimar el comportamiento en:

- El caso promedio, que proporciona una idea sobre el comportamiento típico del algoritmo.
- El peor caso posible que proporciona una cota superior para el tiempo requerido

Esta cota se denota como $O(\cdot)$.

Se define un algoritmo *polinomial*, si el número de operaciones elementales necesarios para resolver un problema de tamaño n esta acotado por una función polinomial en n. Entonces un algoritmo se considerará *eficiente* sí y solo sí, es polinomial.

Para entender el significado de algoritmos polinomiales como una clase, se consideran los algoritmos que violan las cotas polinomiales, para ejemplo suficientemente grandes. Normalmente se les conoce como *algoritmos exponenciales,* porque 2^n es el modelo de tasas de crecimiento no polinomiales, otros modelos son $k^n\,(k>1), n!, 2^{n^2}$,etc.

Es claro que cuando el tamaño de los datos crece, cualquier algoritmos polinomial, será más eficiente que cualquiera del tipo exponencial como se muestra en la tabla B.1, en la que se aprecia lo descrito anteriormente.

Función	Valores Aproximados		
n	10	100	1000
$n \log n$	33	664	9966
n^3	1000	1000000	10^9
$10^6 n^8$	10^{14}	10^{22}	10^{30}
2^n	1024	$1{,}27 \times 10^{30}$	$1{,}05 \times 10^{301}$
$n^{\log n}$	2099	$1{,}93 \times 10^{13}$	$7{,}89 \times 10^{29}$
$n!$	3628800	10^{158}	4×10^{256}

Cuadro B.1: Complejidad

Finalmente, los algoritmos polinomiales tienen propiedades muy atractivas; éstos pueden ser combinados para resolver casos especiales del mismo problema. Un algoritmo polinomial puede llamar a otro algoritmo como una subrutina y el algoritmos resultante también es polinomial.

B.2. Clases P y NP

La teoría de complejidad computacional es el tema de la clasificación de la dificultad de los diversos problemásde cálculo, tanto clásica y cuántica, y comprender el poder de los ordenadores cuánticos se examinará en primer lugar algunas ideas generales de la complejidad computacional. La idea más básica es la de una clase de complejidad.

Una clase de complejidad se puede considerar como una colección de problemásde cálculo, todos los que comparten algún rasgo común con respecto a los recursos computacionales necesarios para resolver esos problemas.

Dos de la clases másimportante en las clases de complejidad se definen por los nombres **P** y **NP** . En términos generales, P es la clase de problemáscomputacionales que se puede resolver rápidamente en un ordenador clásico. NP es la clase de problemásque tienen soluciones que pueden ser rápidamente controlada en una computadora clásica.

B.2.1. La clase P

Se define a la clase P como el conjunto de todos los problemáspara los cuales existe un algoritmo polinomial para resolverlos; se dice que los problemásde la clase P son "fáciles". Algunos ejemplos de Problemásque pertenecen a esta clase son: la búsqueda del mínimo de n números; encontrar el camino más corto en una red; problema de corte mínimo. Acoplamiento en graneas bipartitas , etc.

B.2.2. La clase NP

El símbolo NP que caracteriza a la clase de problemásque se va a presentar es engañoso, no se trata de problemás"no polinomiales" como podría pensarse a primera impresión. Las letras NP denotan "*polinomial no determinista*".

NPes la clase de problemásde decisión que se pueden resolver por algoritmos no deterministas en tiempo polinomial"

Un algoritmo no determinista es uno que, además de las características usuales de los algoritmos, debe hacer una selección arbitraria entre varias opciones de una ramificación.

Otra forma de caracterizar la clase NP (que se refiere implícitamente a los algoritmos no deterministas) consiste en decir que son los problemásque se pueden resolver por una exploración arborescente tal que la profundidad de la arborescencia esté acotada por un polinomio (el número de nodos de dicha arborescencia puede no ser polinomial).

Cuando un problema pertenece a P, su complemento también pertenece a P. Se cree que esto no es cierto para problemásen NP. Por definición si un problema pertenece a la clase P, también pertenece a la clase NP, es decir $P \subset NP$. La pregunta ¿Es $P = NP$? no se ha contestado.

Para demostrar que $P = NP$ se tiene que probar que todos los problemásen NP pueden ser resueltos por algoritmos deterministas en tiempo polinomial. Lo cual no se ha logrado determinar. Para probar que $P \neq NP$ se debe mostrar si un problema en NP que no puede resolverse en forma determinista en tiempo polinomial. Tampoco se ha hecho. Se cree que $P \neq NP$, y que se necesitan nuevas técnicas matemáticas para responder a estas preguntas.

Bibliografía

[1] Feynman, R. P. 1982 Simulating physics with computers. Int. J. Theor. Phys. 21, 467.

[2] C.H. Bennett and G. Brassard (1984), "Quantum cryptography: public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, IEEE press., pp. 175-179.

[3] Díaz-Rodríguez C. A. , Olivares-Robles M.A, A. Juarez, An Overview of Quantum Cryptography: Simulation, IEEE, Conielicomp

[4] Shor, P. W. 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Statist. Comput. 26, 1484.

[5] de la Peña Luis, Introduccion a la Mecánica Cuantica, FCE; UNAM, 3ra . Ed., 2006

[6] E.Schrödinger, Quantisierung als Eigenwertproblem (Erste Mitteilung.), Ann. Phys., 79, p. 361-376, (1926)1924 & 1926

[7] Keyes R.W.; Miniaturization of Electronics and its Limits, IBM Journal of Research and Development, 32, 24-28; January, 1988.

[8] Rolf Landauer: "Irreversibility and heat generation in the computing process," IBM Journal of Research and Development, vol. 5, pp. 183-191, 1961.

[9] Ramírez R. J., López Bracho J. y Gutiérrez Andrade M.;Complejidad computacional de Algoritmos; UAMAzcapotzalco; pags. 19-22

[10] Venegas Andraca S.;Caminatas cuánticas: definiciones y algoritmos; Apuntes- CINVESTAV, Enero-Marzo 2008; pags. 64-71.

[11] V.B. Balakirsky; Hashing of Data Bases Based on Indirect Observations of Hamming Distances; http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.49.3686; 1995

[12] McMahon, David. 2008 Quantum Computing Explained. WILEY-INTERSCIENCE

[13] Sándor Imre and Ferenc Balázs. 2005 Quantum Computing and Communications An Engineering Approach.. John Wiley & Sons

[14] Nielsen, M. A. & Chuang, I. J. 2000 Quantum computation and quantum information. Cambridge, UK: Cambridge University Press.

[15] D. Deutsch, Proceedings of the Royal Society of London A425, 73 (1989).

[16] Vivien M. Kendon. 2006 A random walk approach to quantum algorithms. Phil. Trans. R. Soc. A 2006 364, 3407-3422

[17] Chandrashekar C.M. 2009 Discrete-Time Quantum Walk -Dynamics and Applications. A thesis presented to the University of Waterloo for the degree of Doctor of Philosophy in Physics

[18] J. Kempe. Quantum random walks: an introductory overview. Contemporary Physics, volume 44, number 4, July – August 2003

[19] Y. Aharonov, L. Davidovich and N. Zagury. 1992 Quantum Random Walks. Physical Review A, 48, 1687-1690

[20] Farhi, E. & Gutmann, S. 1998 Quantum computation and decision trees. Phys. Rev. A 58, 915–928.

[21] Aharanov, D., Ambainis, A., Kempe, J. & Vazirani, U. 2001 Quantum walks on graphs. In Proc. 33rd Annual ACM STOC, pp. 50–59. ACM: New York, NY.

[22] Childs, A. M., Cleve, R., Deotto, E., Farhi, E., Gutmann, S. & Spielman, D. A. 2003 Exponential algorithmic speedup by a quantum walk. In Proc. 35th Annual ACM STOC, pp. 59–68. ACM

[23] Shenvi, N., Kempe, J. & Birgitta Whaley, K. 2003 A quantum random walk search algorithm. Phys. Rev. A 67, 052307.

[24] Ambainis, A. 2003 Quantum walks and their algorithmic applications. Int. J. Quantum Inf. 1, 507–518.

[25] Hartmut Neven,Vasil S. Denchev. 2009 Training a Large Scale Classifier with the Quantum Adiabatic Algorithm

[26] Lectures on Quantum Computation by David Deutsch

[27] Díaz-Rodríguez C. A. , Carrión V. M. ,Olivares-Robles M.A. 2010 Algoritmo Clásicos Cuánticos. CP-44 IEEE Sección México

[28] A. Auyuanet Larrieu, CAMINATA CUÁNTICA EN LA LÍNEA EN TIEMPO DISCRETO, Tesis Universidad de la Republica Facultad de Ciencias, 2006

[29] Ramírez Rodríguez J., López Bracho R.; Complejidad Complutacional de Algoritmos, Universidad Autonoma Metropolitana, 1996

[30] Aharonov Y., Davidovich L., Zagury N., Quantum Random Walks, Physical Review A. 48, 1687, 1993

[31] Díaz-Rodríguez C. A. , Olivares-Robles M.A, A. Juarez, ALGORITMOS DE búsqueda Y CAMINATAS CUÁNTICAS. Presentación Poster, LIII Congreso Nacional de Física

[32] R Sridhar, A. Amudha, S. Karthiga, Geetha T V; Comparison of modified dual ternary indexing and multi-key hashing algorithms for music information retrieval; International Journal of Artificial Intellience & Applications (IJAOA), Vol. 1, No. 2, Julio de 2010

[33] L.K. Grover, A fast quantum mechanical algorithm for database search. e-print quant-ph/9605046.

[34] E. V. Makarov; Simulador del Algoritmo de Grover ; http://www.mathworks.com/matlabcentral/fileexchange/4711-gsa-m

[35] A. Prokopenya; Simulador de Circuito de Grover ; http://demonstrations.wolfram.com/ QuantumCircuitImplementing-GroversSearchAlgorithm/

[36] Quantum Walks with Entangled Coins S.E. Venegas- Andraca, J.L. Ball, K. Burnett and S. Bose New J. Phys. 7 221 (2005).

[37] Venegas Andraca S. E.; "Discrete Quantum Walks and Quantum Image Processing", Tesis Doctoral, Center for Quantum Computation Keble College University of Oxford 2005

[38] Craig S. Hamilton, Aurél Gábris, Igor Jex and Stephen M. Barnett; "Quantum walk with a four dimensional coin"; New J. Phys. 13 01315 (2011).

[39] A. Einstein, B. Podolsky, and N. Rosen ; Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?; Phys. Rev. 47, 777–780 (1935)

[40] C. Moore and A. Russell, in Proc. 6th Intl. Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM '02), edited by J. D. P. Rolim and S. Vadhan (Springer, 2002), pp. 164–178, quant-ph/0104137.

[41] T.A. Brun, H.A. Carteret, and A. Ambainis. Quantum walks driven by many coins. Phys. Rev. A, 67:052317, 2003.

[42] B. Tregenna,W. Flanagan, R. Maile and V. Kendon. Controlling discrete quantum walks: coins and intitial states. 2003 New J. Phys. 5 83

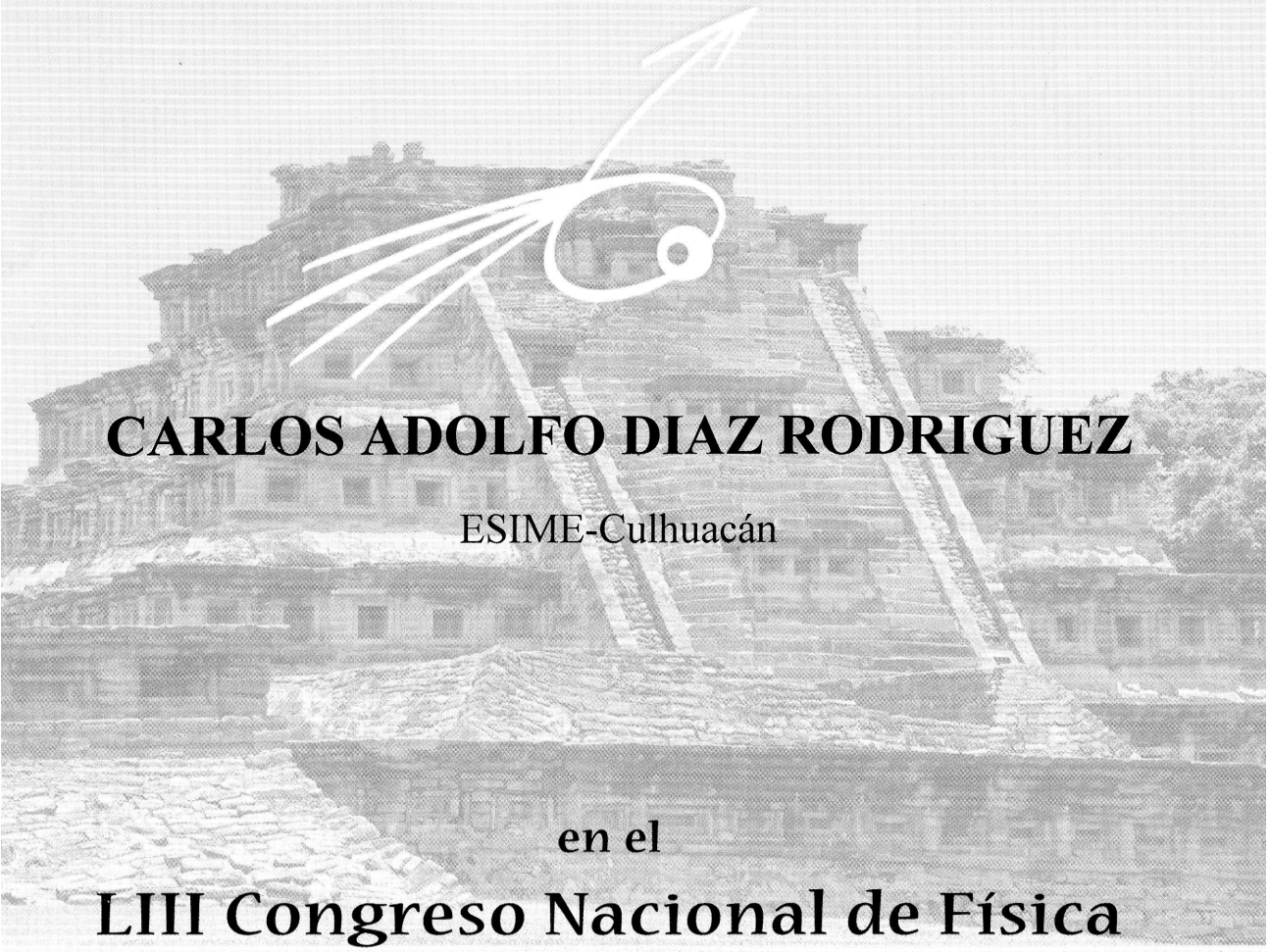
[43] Y. Omar, N. Paunkovi´c, L. Sheridan, and S. Bose. Quantum walk on a line with two entangled particles. quant-ph/0411065.

[44] G. Moore. Cramming more components onto integrated circuits. IBM, Electronics, Volume 38, Number 8, April 19, 1965

Índice alfabético

La Sociedad Mexicana de Física

Agradece la asistencia y participación de:



CARLOS ADOLFO DIAZ RODRIGUEZ

ESIME-Culhuacán

en el

LIII Congreso Nacional de Física

del 25 al 29 de octubre de 2010

World Trade Center y Hotel Galería Plaza, Boca del Río, Veracruz

Dr. Luis Felipe Rodríguez Jorge

Presidente de la SMF

IEEE
SECCION MEXICO

OTORGA EL PRESENTE

RECONOCIMIENTO

AL

Ing. Carlos A. Díaz Rodríguez

POR SU AMABILISIMA PARTICIPACION EN LA:

Vigésimaprimera Reunión de Otoño de Comunicaciones, Computación, Electrónica y Exposición Industrial

LA INFORMATICA, TELECOMUNICACIONES Y CONTROL, EN APOYO DE LAS REDES Y SISTEMAS INTELIGENTES

CON LA PONENCIA:

ALGORITMOS CLASICOS Y CUANTICOS

ING. ROMAN RAMIREZ RODRIGUEZ
PRESIDENTE ROC&C 2010
IEEE SECCION MEXICO

28 de Noviembre al 4 de Diciembre del 2010, Acapulco, Gro.

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

CONIELECOMP 2011

21th International

Conference on electronics communications and computers

CERTIFICATE OF APPRECIATION

Presented for his/her outstanding contribution as Technical Speaker with the lecture entitled:

An overview of Quantum Crystography: Simulation

TO

C. A. Díaz Rodríguez

Dr. Rubén Alejos Palomares
General Chairman

Dr. José Alfredo Sánchez Huitrón
Technical Program Chair

Dr. Jorge Rodriguez Asomoza
Head of CEM Department

Cholula, Puebla, México, February 28th to March 2nd, 2011

UDLAP UNIVERSIDAD DE LAS AMÉRICAS PUEBLA

IEEE SECCION PUEBLA

CENGAGE Learning™ El conocimiento nos compromete

PEARSON

ProSoft® TECHNOLOGY