





**INSTITUTO POLITÉCNICO NACIONAL**

---

---

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA  
SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN  
UNIDAD CULHUACÁN

# **SIMULACIÓN DE CAMINATAS EN COMPUTACIÓN CUÁNTICA**

**TÉISIS**

Que para obtener el grado de:  
Maestro en Ciencias de Ingeniería en  
Microelectrónica

Presenta:

Lic. Arturo Juárez García

Asesor:

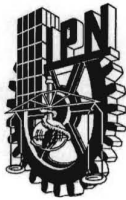
Dr. Miguel Ángel Olivares Robles



México D.F.

Junio 2011

26 de julio de 2011



# INSTITUTO POLITÉCNICO NACIONAL SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

## ACTA DE REVISIÓN DE TESIS

En la Ciudad de México D. F., siendo las 11:00 horas del día 29 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-CULH. para examinar la tesis titulada:

"Simulación de Caminatas en Computación Cuántica"

Presentada por el alumno:

<u>Juárez</u>	<u>García</u>	<u>Arturo</u>
Apellido paterno	Apellido materno	Nombre(s)

Con registro: 

B	0	9	1	7	6	9
---	---	---	---	---	---	---

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 de tesis

Dr. Miguel Ángel Olivares Robles

Dr. Juan Carlos Sánchez García

Dr. Gabriel Sánchez Pérez

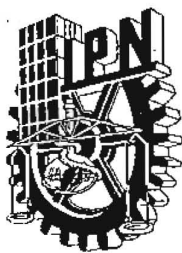
M. en C. Víctor Manuel Carreón Calderón

M. en C. José Luis Olivares Robles

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Gonzalo Isaac Duchén Sánchez





**INSTITUTO POLITÉCNICO NACIONAL**  
**SECRETARÍA DE INVESTIGACIÓN Y POSGRADO**

*CARTA CESIÓN DE DERECHOS*

En la Ciudad de México D.F. el día 25 del mes Julio del año 2011, el (la) que suscribe Arturo Juárez García alumno (a) del Programa de Maestría en Ciencias de Ingeniería en Microelectrónica con número de registro B091769, 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 "Simulación de Caminatas en computación cuántica", 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 hodicchino@hotmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Arturo Juárez García

Nombre y firma

# Resumen

Los componentes del último de los procesadores de intel (i7,i9), poseen el tamaño de alrededor de 45 y 32 nm. respectivamente , entonces cabe la pregunta del Físico Richard Feynman,

¿Hasta dónde es posible, en teoría, seguir haciendo máquinas más pequeñas según las leyes de la naturaleza?

El párrafo anterior nos muestra que estamos llegando a las fronteras de lo subatómico (debido a la miniaturización), en donde sólo las leyes de la mecánica cuántica nos pueden predecir el comportamiento de la materia.

Por lo cual el presente trabajo tiene por objetivo mostrar cómo se ha ido aprovechando esas leyes, desde el marco de la computación, para dar lugar a una nueva rama de la investigación científica, llamada, **computación cuántica**.

Centrado en las caminatas cuánticas, método utilizado para el diseño de los algoritmos cuánticos, y apoyado en el software de simulación cuántica, genero las gráficas que me permiten comparar las caminatas clásicas con las cuánticas y con base a sus distribuciones probabilísticas mostrar las ventajas de los algoritmos cuánticos en algunas aplicaciones, como el manejo cuántico de la información. Realizaré una simulación de las caminatas cuánticas sobre una partícula, para terminar presentando algunas nociones de complejidad algorítmica, considerando la perspectiva de cómo manejar a nivel de los algoritmos cuánticos algunos de los problemas considerados duros (NP-completos) para los cuales no se conocen algoritmos eficientes.

# Abstract

The components of the latest Intel processors (i7, i9), have the size of about 45 to 32 nm. respectively, then there is the question of the physicist Richard Feynman, How far is it possible, in theory, continue to make smaller machines under the laws of nature?

The previous paragraph shows that we are approaching the borders of the subatomic, where only the laws of quantum mechanics we can predict the behavior of matter.

Therefore this paper aims to show how it has been building on these laws, from the context of computing, giving rise to a new branch of research called, quantum computing.

Focused on quantum walks, the method used for the design of quantum algorithms, and supported by quantum simulation software, generate graphs that allow me to compare classical with quantum walks and based on their probability distributions show the advantages of quantum algorithms in some applications, such as quantum information management.

I begin with a simulation of quantum walks on a particle, and finally presenting some notions of algorithmic complexity, considering the perspective of how to handle level of quantum algorithms some of the problems considered hard (NP-complete) for which there are algorithms efficient

# Agradecimientos

- » Gracias a Dios por haberme dado la oportunidad de vislumbrar un poco de sus maravillas que tiene escondida en los rincones de lo que llamamos ciencia, porque lo invisible de él su eterno poder y divinidad se manifiestan en la creación, que nosotros también descubrimos poco a poco.
- » Muy en especial a mi hermosísima y muy amada Araceli, muchas gracias por todo el amor y paciencia que has mostrado no sólo a lo largo del desarrollo de éste trabajo, sino de siempre, te amo, Dios te siga bendiciendo mucho.
- » A mis queridísimos hijos Hans, Fernando, y Abraham, por quién tengo motivos suficientes para seguir luchando en ésta vida, los amo.
- » A mi pequeño nieto Emiliano Zaid y a mi muy estimada nuera Madai, gracias por su apoyo.
- » A mi incansable madre, con quién estaré agradecido, por toda la vida, la bendigo mucho
- » A mis hermanos Luis, Gabriel y Sergio, de quienes estoy orgulloso y a quienes siempre llevaré en mi corazón.
- » Retomando sus palabras, a Charlie , mi compañero científico, gracias brother.
- Por supuesto a mi asesor el Dr. Miguel Ángel Olivares Robles, y a todos aquellos que he conocido en la SEPI, el doc (Carlos), Alex, Juanjo, Erick etc.

## *CON TODO MI CORAZÓN GRACIAS*

- Agradezco el apoyo económico que me brindó CONACYT para la realización de este trabajo
- Y el apoyo brindado por la SEPI-IPN del Programa Institucional de formación de investigadores



# Índice general

<b>1. ESTADO DEL ARTE</b>	<b>13</b>
1.1. Introducción . . . . .	13
1.2. El principio . . . . .	14
1.3. Década de los 90. . . . .	14
1.4. Década 2000 . . . . .	15
1.5. En la actualidad . . . . .	16
1.5.1. Artículos (papers) claves . . . . .	17
<b>2. Fundamentos</b>	<b>20</b>
2.1. Qubit. . . . .	20
2.2. Superposición cuántica . . . . .	23
2.3. Enlazamiento cuántico . . . . .	24
2.4. Paralelismo cuántico . . . . .	25
2.5. Postulados de la Mecánica cuántica . . . . .	25
2.5.1. Postulado 1: Estados de un sistema físico . . . . .	26
2.5.2. Postulado 2: Evolución del sistema en el tiempo . . . . .	26
2.5.3. Postulado 3: Mediciones cuánticas . . . . .	27
2.5.4. Postulado 4: Sistemas cuánticos compuestos . . . . .	28
<b>3. Caminatas clásicas discretas</b>	<b>29</b>
3.1. Definición . . . . .	29
3.1.1. Caso unidimensional . . . . .	30
3.2. Modelos computacionales determinísticos y no determinísticos . . . . .	31
3.2.1. Máquina de Turing . . . . .	33
3.3. Algoritmos estocásticos . . . . .	34
3.4. Conclusiones de la caminata aleatoria clásica . . . . .	34
<b>4. Caminatas Cuánticas Discretas</b>	<b>37</b>
4.1. Modelo de Caminatas cuánticas (QW) . . . . .	37
4.2. Estructura del modelo de una caminata cuántica (QW) . . . . .	38
4.3. Características del Simulador de Mathematica . . . . .	40
4.3.1. Ejemplo con los tres primeros pasos detallados . . . . .	41
4.4. Mis resultados . . . . .	48
4.4.1. Reproducción . . . . .	48

<i>ÍNDICE GENERAL</i>	7
4.4.2. Mis resultados . . . . .	51
4.4.3. Propuesta de moneda M. . . . .	53
4.5. Congreso Nacional de Física . . . . .	55
4.6. Conclusiones . . . . .	56
4.7. Trabajos futuros . . . . .	56
<b>5. Apéndice A</b>	<b>58</b>
<b>6. Apéndice B</b>	<b>73</b>

# Índice de figuras

2.1.	Representación de un qubit por dos niveles electrónicos en un átomo . . . . .	21
2.2.	Esfera de Bloch . . . . .	22
2.3.	Como muestra la figura el electrón tiene un spin hacia arriba y hacia abajo, pero en la superposición posee los dos valores a la vez. . . . .	24
2.5.	Una función $f(x)$ se puede evaluar en múltiples valores de $x$ simultáneamente, apoyados en la superposición . . . . .	25
2.4.	Ilustración de dos memorias cuánticas. Cada memoria consiste en una celda de vidrio lleno de átomos de cesio, que se muestran en color azul y pequeñas bolas rojas. El haz de luz se envía a través de los átomos y la información cuántica se transfiere desde la luz a los átomos. (Imágenes: Quantop) . . . . .	25
3.1.	Cada paso de la caminata aleatoria consiste en que Froggy se mueve a la izquierda o derecha.El sentido de éste movimiento depende del resultado del volado. . . . .	30
3.2.	La Distribución para una caminata aleatoria clásica es del tipo Binomial, tendiendo pra el número de pasos muy grandes a una normal. . . . .	31
3.3.	Cómputo determinístico y no determinístico . . . . .	32
3.4.	Las caminatas aleatorias clásicas generan una distribución normal o gaussiana, para un número de pasos bastante grande. . . . .	35
3.5.	Los 5 primeros (t) lanzamientos de una caminata aleatoria clásica se pueden observar, así como las posiciones (n) en la recta que van avanzando con sus respectivas probabilidades de tales posiciones. . . . .	36
4.1.	En su versión básica unidimensional, un caminante al azar da un paso a la derecha con probabilidad $p$ o (excluyente) a la izquierda con probabilidad $1 - p$ . . . . .	38
4.2.	En ésta gráfica podemos observar el comportamiento del caminante en el primer paso, vemos el principio de superposición en acción. . . . .	42

4.3. En ésta gráfica podemos observar el comportamiento del caminante en el segundo paso, vemos más enfáticamente el principio de superposición en acción. . . . .	44
4.4. En ésta gráfica podemos observar el comportamiento del caminante en el tercer paso, vemos el principio de superposición nuevamente en acción. . . . .	45
4.5. Distribución de caminata cuántica con 100 iteraciones, caminante y moneda en el origen . . . . .	46
4.7. Distribuciones comparadas para la iteración t=100. La distribución fuertemente oscilante corresponde al caminante cuántico que muestra mayor probabilidad de estar lejos del origen que el caminante clásico. . . . .	46
4.6. Comparación estadística entre caminatas clásicas y cuánticas . . . . .	47
4.8. La gráfica es presentada en su tesis doctoral en [3] . . . . .	48
4.9. Reproducción de la gráfica de caminata cuántica con moneda en superposición . . . . .	49
4.10. Gráfica con desbalance a la derecha . . . . .	50
4.11. Gráfica con desbalance a la izquierda . . . . .	51
4.12. Gráfica desbalanceada a la izquierda, con caminante en superposición . . . . .	52
4.13. Gráficas con caminante en superposición desbalanceada a la derecha y a la izquierda . . . . .	53
4.14. Gráfica balanceada con caminante en superposición . . . . .	53
4.15. Gráfico con moneda $M = \frac{1}{\sqrt{2}}( 0\rangle\langle 0  - i 0\rangle\langle 1  - i 1\rangle\langle 0  +  1\rangle\langle 1 )$ . . . . .	54
4.16. El caminante esta en superposición y la moneda es M . . . . .	55
4.17. Distribución uniforme de una caminata cuántica . . . . .	56
6.1. Representaciones de los diagramas de los circuitos de Pauli y su acción sobre un sólo qubit . . . . .	74
6.2. Diagrama de Hadamard aplicada dos veces . . . . .	75
6.3. Dos compuertas Humarada en paralelo aplicadas al estado $ 1\rangle 1\rangle$ . . . . .	76
6.4. Representación del diagrama de un circuito de una compuerta NOT controlada o CNOT . . . . .	78
6.5. Diagrama y tabla de verdad de compuerta Toffoli . . . . .	79
6.6. Diagrama del circuito para $U_f  x, y\rangle =  x, y \oplus f(x)\rangle$ . . . . .	80

# PROLOGO

En nuestro mundo moderno las computadoras se han convertido en el instrumento de todos los días, diversas áreas del ser humano se han beneficiado con el desarrollo de este invento, por ejemplo podemos mencionar, el ámbito laboral, la educación, el entretenimiento, la diversión, las comunicaciones, etc. Pero detrás de estos dispositivos se encuentra el trabajo de científicos con diferentes especialidades, tales como físicos, ingenieros, matemáticos etc. No bastó con haberlas inventado, su evolución ha continuado a través de los años permitiendo incrementar su velocidad y reducir su tamaño en proporciones sorprendentes, del tamaño de una habitación al tamaño de la palma de la mano.

Ahora se plantea un nuevo escalón en esta evolución que promete revolucionar por completo el funcionamiento de las computadoras, y surge precisamente de la física, de una rama relativamente nueva que vio la luz a principios del siglo XX y que ha cambiado la visión del mundo microscópico que hasta entonces había tenido la humanidad, se trata de: *La mecánica cuántica*.

La *mecánica cuántica* es la más extraña de las disciplinas científicas. Desde la perspectiva de nuestra vida cotidiana, nada tiene sentido en la teoría cuántica, teoría acerca de las leyes de la naturaleza que rigen el dominio de lo muy pequeño (así como de algunos sistemas grandes, como los superconductores ). En el dominio cuántico todo es borroso; existe un aspecto aleatorio común a todas las entidades con las que tratamos, sean éstas luz o electrones o átomos o quarks. Un principio de *incertidumbre* reina en la mecánica cuántica, donde la mayoría de las cosas no pueden verse, sentirse o conocerse con precisión, sino sólo a través de *una neblina de probabilidad y azar*.

Las predicciones científicas sobre resultados (medidas) son de naturaleza estadística y se dan en términos de probabilidades; podemos predecir la localización más probable de una partícula y no su posición exacta. Y en ningún caso podemos determinar la posición y el momento de una partícula con gran precisión simultáneamente.

Simplemente, la incertidumbre, la borrosidad, la probabilidad, la dispersión no puede desaparecer; estos misteriosos, ambiguos y velados elementos son parte íntegra de éste mundo de maravillas.

Aún mas inexplicable es la misteriosa *superposición de estados de sistemas cuánticos*. Un electrón (partícula elemental cargada negativamente) o un fotón (cuanto de luz) pueden hallarse en una superposición de dos o más estados.

Ya no hablamos de aquí o allí; en el mundo cuántico se habla de aquí y allí.

Es decir, en cierto sentido, un fotón, una parte de un flujo de luz que ilumina una pantalla con dos agujeros, puede pasar a través de los dos agujeros a la vez, y no, como cabría esperar, a través de uno u otro. En ese sentido también un electrón en órbita alrededor del núcleo (atómico) se halla potencialmente en muchos sitios a la vez.

Pero sin duda el fenómeno más asombroso en el extraño mundo del cuanto es el efecto llamado *entrelazamiento* (<<entanglement>>).

Dos partículas que pueden estar muy alejadas entre sí, millones o billones de kilómetros (en teoría)<sup>1</sup>, están misteriosamente ligadas la una con la otra. Es decir cualquier cosa que le ocurra a una de ellas causa de inmediato un cambio a la otra. Mediante el entrelazamiento, puede también <<teleportarse>> el estado de una partícula hasta un destino lejano, como sucede con el capitán Kirk en la serie televisiva Star Trek cuando pide ser proyectado de vuelta al Enterprise. Para ser preciso, nadie ha sido todavía capaz de teleportar a una persona. Pero el estado de un sistema cuántico ha sido teleportado en laboratorio.[1]

***Serán estos fenómenos los que se utilicen para introducir nuevas formas de procesar la información en una computadora.***

Las expectativas que han surgido con la introducción de la física cuántica al campo del manejo de la información son enormes. En resumen se pretende:

1. Reducir el número de pasos requeridos (y por consiguiente el tiempo) para encontrar la información en una base de datos, en una forma mucho más drástica que lo que podía conseguirse incrementando la velocidad del procesador de una computadora. Por ejemplo pasando de 10000 pasos a 100 solamente.
2. Realizar operaciones sobre una gran cantidad de datos en forma simultánea (cómputo en paralelo), sin tener que incrementar sustancialmente ni la memoria, ni el equipo de procesamiento en la computadora como se requiere en las computadoras clásicas.
3. Realizar, en forma eficiente, simulaciones de sistemas complejos, como los sistemas cuánticos.
4. Proponer métodos, que permitan atacar los problemas que clásicamente han sido clasificados como intratables. Tal es el caso de la factorización de números muy grandes (digamos, con unos 400 dígitos) en sus factores primos. Precisamente es en esta dificultad en la que se basan los sistemas de seguridad por encriptación más confiables hasta la fecha, pero que podrían ser violados de existir una computadora cuántica.

---

<sup>1</sup>Por primera vez en la historia se ha conseguido la teletransportación de un fotón a larga distancia, lo que constituye un fuerte impulso para el desarrollo de la criptografía y los ordenadores cuánticos, así como para nuevos sistemas de telecomunicaciones capaces de obtener la transmisión instantánea de datos. De esta forma, la teletransportación no sólo se consolida como fenómeno físico controlable, sino como un nuevo desafío a la concepción del mundo basada en el tiempo y el espacio. En realidad, los dos laboratorios, y por ende las partículas del experimento, estaban separadas entre sí 55 metros, pero el cable que separó a los dos fotones gemelos tenía una extensión mayor para simular una distancia de dos kilómetros y verificar que a esta distancia la teletransportación también es factible.

5. Proveer de un sistema de alta seguridad para el envío de información confidencial.[4]

La estructura del trabajo se desarrolla bajo las siguientes consideraciones:

En el capítulo 1, a través de una introducción histórica breve, muestro la manera en que fueron tomadas en cuenta las propuestas de dos físicos de los ochenta, así cómo se ha desarrollado la computación cuántica hasta nuestros días, indicando artículos claves que me permitan justificar mi trabajo.

Prosiguiendo en el capítulo 2, explicamos los fundamentos físicos (y matemáticos en el apéndice A) de ciertos fenómenos de la mecánica cuántica

Continuando con el capítulo 3, brevemente describimos a las caminatas aleatorias clásicas.

El capítulo 4, lo dedicamos a definir las características de la caminatas cuánticas, finalizando el capítulo con mis resultados y conclusiones.

El apéndice B, hago referencia a una parte de compuertas cuánticas para señalar aspectos del algoritmo de Deutsch, que nos ayuda a comprender un poco más el paralelismo cuántico.

# Capítulo 1

## ESTADO DEL ARTE

A partir de una breve introducción histórica, que abarca de los 80s. hasta el día de hoy, señalo en forma básica el desarrollo de la computación cuántica, finalizado el capítulo con algunos artículos que mostrarán cómo el modelo de caminatas cuánticas es un tema de actualización.

### 1.1. Introducción

Cuarenta años después del bombardeo atómico de Nagasaki, Feynman, veterano del Proyecto Manhattan, pronuncia una conferencia en Japón.

Pero ahora se trata de un tema pacífico que sigue ocupando a nuestras mentes más perspicaces: *el futuro de los computadores*, incluido el tema que hizo de Feynman un Nostradamus de la ciencia de la computación: *el límite teórico inferior para el tamaño de un computador*.<sup>[9]</sup>

En dicha conferencia trata tres temas que hoy en día se han desarrollado de manera espectacular, y que ha permitido a la ciencia de la computación ampliar sus horizontes, tales temas referidos por Feynman son:

1. Computadores en paralelo.
2. Reducción de la pérdida de energía en un computador.
3. La reducción del tamaño.

Los tres temas se han abordado desde los ochenta, los primeros en proponer tales sistemas fueron Poul Benioff y Richard Feynman.

En cuanto al tercer tema de la conferencia de Feynman, él argumentaba: *¿Hasta dónde es posible, en teoría, seguir haciendo máquinas más pequeñas según las leyes de la naturaleza?* <sup>[9]</sup>. En la actualidad entendemos lo siguiente:

*A medida que evoluciona la tecnología, aumenta la escala de integración y caben más transistores en un espacio, así se fabrican micro-chips cada vez más pequeños, ya que, cuanto más pequeño es un micro-chip, mayor velocidad de proceso alcanza.* <sup>1</sup>

---

<sup>1</sup>Por ejemplo los últimos componentes de los microprocesadores de intel, *i7* e *i9*, fueron



*Sin embargo, no podemos hacer los chips infinitamente pequeños. Hay un límite en el cual dejan de funcionar correctamente. Cuando se llega a la escala de nanómetros, los electrones se escapan de los canales por donde deben circular. A esto se le llama **efecto túnel**.*

*Una partícula, si se encuentra con un obstáculo, no puede atravesarlo y rebota. Pero con los electrones, que son **partículas cuánticas** y se comportan como **ondas**, existe la posibilidad de que una parte de ellos pueda atravesar las paredes si son demasiado finas; de esta manera la señal puede pasar por canales donde no debería circular. Por ello, el chip deja de funcionar correctamente. En consecuencia, la computación digital tradicional no tardaría en llegar a su límite, puesto que ya se han llegado a escalas de sólo algunas decenas de nanómetros. Y a estas escalas se empiezan a manifestar los efectos cuánticos de la materia, por ello las conjeturas de Feynman. Para poder resolver dicho problema o aprovechar tales efectos, se propone un nuevo paradigma para tratar el procesamiento de la información, tal paradigma es una de las últimas aventuras de la ciencia, en particular entre la ciencia de la computación y la mecánica cuántica.*

## 1.2. El principio

La idea de computación cuántica surge en 1981, cuando **Paul Benioff** en [10] propone un modelo teórico de la máquina de Turing operando con algunos principios de la mecánica cuántica. Posteriormente en 1982 **Richard Feynman** propone en [18] el uso de fenómenos cuánticos para realizar cálculos computacionales y exponía que dada su naturaleza algunos cálculos de gran complejidad se realizarían más rápidamente en un ordenador cuántico, en particular mencionaba que la simulación de fenómenos cuánticos sería muy difícil de reproducir en un ordenador clásico, por ello propone la posibilidad de la construcción de una **computadora cuántica**.

Posteriormente en 1985, el científico **David Deutsch** en [11] realiza la descripción del primer computador cuántico universal, es decir, capaz de simular cualquier otro computador cuántico (principio de Church-Turing ampliado). También es autor de la descripción teórica del paralelismo cuántico, mediante su algoritmo que es capaz de evaluar una función en varios valores simultáneamente. De este modo surgió la idea de que si es posible la construcción de un computador cuántico y por ende de los algoritmos cuánticos.

## 1.3. Década de los 90.

Para la década de los 90, la teoría empezó a plasmarse en la práctica: aparecieron los primeros algoritmos cuánticos, las primeras aplicaciones cuánticas y las primeras máquinas capaces de realizar cálculos cuánticos.

---

*elaborados en espacios de 45 y 32nm respectivamente*

En 1993 *Dan Simon* en [12] comparó el modelo de probabilidad clásica con el modelo cuántico observando las ventajas del modelo cuántico, y además sus ideas sirvieron de base para el desarrollo de algunos algoritmos futuros (como el de Shor). En el mismo año *Charles H. Bennett* en [27] descubrió y publicó los principios del teletransporte cuántico y esto abrió una nueva vía de investigación hacia el desarrollo de comunicaciones cuánticas.

El mayor impulso para la realización del cómputo cuántico o el resultado hito, es sin duda el resultado en 1995 de *Peter Shor*, cuando en [28] desarrolla, el algoritmo que lleva su nombre y que permite calcular los factores primos de números a una velocidad mucho mayor que en cualquier computador tradicional. Además su algoritmo permitiría romper muchos de los sistemas de criptografía utilizados actualmente. *Su algoritmo sirvió para demostrar a una gran parte de la comunidad científica que observaba incrédula las posibilidades de la computación cuántica, que se trataba de un campo de investigación con un gran potencial.* Además, un año más tarde, propuso un sistema de corrección de errores en el cálculo cuántico.

Otro resultado de gran peso para el impulso del cómputo cuántico es el presentado en [29] por Lov Grover en 1996, sorprendiendo a la comunidad con su algoritmo de búsqueda.

La década de los 90 termina con, el primer experimento de comunicación segura, usando criptografía cuántica, el cual se realiza con éxito a una distancia de 23 Km. Además se realiza el primer teletransporte cuántico de un fotón, además investigadores de Los Álamos y el Instituto Tecnológico de Massachusetes consiguen propagar el primer Qubit a través de una solución de aminoácidos, lo cual prepara el primer paso para analizar la información que transporta un Qubit. Durante ese mismo año, nació la primera máquina de 2-Qbit, que fue presentada en la Universidad de Berkeley, California (EE.UU.) Un año más tarde, en 1999, en los laboratorios de IBM-Almaden, se creó la primera máquina de 3-Qbit y además fue capaz de ejecutar por primera vez el algoritmo de búsqueda de Grover.

## 1.4. Década 2000

Continuando ésta aventura, en los inicios del año 2000 Isaac Chuang implementa el algoritmo de Shor, logrando que este algoritmo se ejecute en un simple paso, haciendo uso de la resonancia magnética como lo indica en [30], cuando en un computador tradicional requeriría de numerosas iteraciones, además desarrolla para IBM un computador cuántico de 5-Qubit. Para el 2001, IBM y la Universidad de Stanford, consiguen ejecutar por primera vez el algoritmo de Shor en el primer computador cuántico de 7-Qbit desarrollado en Los Álamos. En el experimento se calcularon los factores primos de 15, dando el resultado correcto de 3 y 5 utilizando para ello 1018 moléculas, cada una de ellas con 7 átomos. Así en 2005 el Instituto de “Quantum Optics and Quantum Information” en la universidad de Innsbruck (Austria) anunció que sus científicos habían creado el primer Qbyte, una serie de 8 Qbits utilizando *trampas de iones*.

En 2006 Científicos en Waterloo y Massachusetts diseñan métodos para mejorar el control del cuanto y consiguen desarrollar un sistema de 12-Qbits. El control del cuanto se hace cada vez más complejo a medida que aumenta el número de Qbits empleados por los computadores. Continuando con ésta escalada de sorprendentes avances en 2007, la compañía canadiense D-Wave presenta públicamente su primer computador cuántico de 16 Qbit. Entre las aplicaciones que presenta para su sistema, se encuentra un sistema gestor de bases de datos y un algoritmo que soluciona Sudokus. Todo ello a través de una interface gráfica similar a la utilizada en los computadores actuales, tratándose del primer acercamiento de la computación cuántica al mundo comercial y no tan científico. En septiembre del mismo 2007 dos equipos de investigación estadounidenses, el National Institute of Standards (NIST) de Boulder y la Universidad de Yale en New Haven consiguieron unir componentes cuánticos a través de superconductores. De este modo aparece el primer bus cuántico, y este dispositivo además puede ser utilizado como memoria cuántica, reteniendo la información cuántica durante un corto espacio de tiempo antes de ser transferido al siguiente dispositivo.

Sorprendentemente en 2008 un equipo de científicos consiguió almacenar por primera vez un Qubit (el equivalente a un “bit” del “mundo clásico”, pero en el “mundo cuántico”) en el interior del núcleo de un átomo de fósforo, y pudieron hacer que la información permaneciera intacta durante 1.75 segundos. Este periodo puede ser expandible mediante métodos de corrección de errores, por lo que es un gran avance en el almacenamiento de información. Para 2009, el equipo de investigadores estadounidense dirigido por el profesor Robert Schoelkopf, de la universidad de Yale, que ya en 2007 desarrollaron el Bus cuántico, crean el primer procesador cuántico de estado sólido, mecanismo que se asemeja y funciona de forma similar a un microprocesador convencional, aunque con la capacidad de realizar sólo unas pocas tareas muy simples, como operaciones aritméticas o búsqueda de datos. Para la comunicación en el dispositivo, esta se realiza mediante fotones que se desplazan sobre el bus cuántico, circuito electrónico que almacena y mide fotones de microondas, aumentando el tamaño de un átomo artificialmente.

## 1.5. En la actualidad

Actualmente existen dos modelos equivalentes predominantes [13] para “pensar” la computación cuántica:

1. Máquinas de Turing Cuánticas [14][15]
2. Circuitos cuánticos [16]

Las Máquinas de Turing Cuánticas proveen un modelo para definir la universalidad de la Computación Cuántica, pero razonar sobre ellas es un proceso bastante complicado. Por ese motivo los circuitos cuánticos son más populares: proveen una visión gráfica y *composición de los algoritmos* y pueden ser manipulados algebraicamente.

Parte fundamental en el desarrollo computacional, incluso en la computación cuántica son los **algoritmos**, en cómputo cuántico no es nada sencillo construir los algoritmos cuánticos, aunque en los últimos años se ha desarrollado una técnica llamada **caminatas cuánticas** que ha inyectado cierto dinamismo en el diseño de los algoritmos.

De hecho, podemos introducir algunas definiciones de computación cuántica, que se consideran en la actualidad de la siguiente manera:

1. *Computación cuántica se puede definir como el campo científico, cuyo propósito es resolver los problemas con los procedimientos de tiempo finito, es decir. **algoritmos** que aprovechan las propiedades de la mecánica cuántica de los sistemas físicos que se utilizan para implementar este tipo de algoritmos.[2]*
2. *Es un nuevo paradigma de la computación, que surge de la combinación entre la computación y la mecánica cuántica.[3]*

De acuerdo a[2]: *Entre los descubrimientos teóricos y conjeturas prometedoras que han posicionado a la computación cuántica como elemento clave en la ciencia moderna, encontramos:*

1. *El desarrollo de nuevos y potentes métodos de cálculo que nos permitirá aumentar significativamente nuestra capacidad de procesamiento para resolver ciertos problemas.[2][17]*
2. *Y la **simulación** de sistemas físicos complejos que ningún ordenador clásico podría, incluso, en principio, para simular de manera eficiente.*

A propósito, he enfatizado, en párrafos previos, dos palabras claves en el presente trabajo, **ALGORITMOS** y **SIMULACIÓN**, tales son el centro o los ejes sobre los que gira la presente tesis. A continuación menciono algunos artículos, recientes, en donde se muestra que los *temas están vigentes*, y que son temas de investigación a diferentes niveles.

### 1.5.1. Artículos (papers) claves

A continuación menciono algunos de los papers claves, que hacen referencia al modelo de caminatas cuánticas y que me sirvieron como guías para el presente trabajo:

1. **Quantum Walks**: En este artículo se ofrece un estudio introductorio sobre caminatas cuánticas. A partir de un efecto físico (analizando una partícula, y los efectos de un operador unitario) se ilustra las principales ideas que permiten introducir las caminatas cuánticas, se revisan algunas de sus propiedades y resumen las notables diferencias con respecto a las caminatas clásicas (caminatas aleatorias).[24]
2. **Using Quantum Computers for Quantum Simulation**: El artículo señala la importancia de la simulación para la comprensión de los fenómenos naturales. Muchos sistemas de gran interés e importancia, en áreas tales como los materiales superconductores y la química cuántica, se cree que son descritos

por los modelos que no podemos resolver con suficiente precisión, ni analítica ni numéricamente con los ordenadores clásicos. [31]

3. **Recent Progress in Quantum Algorithms:** Mostrando las diferencias de cómo operan los algoritmos clásicos y los cuánticos, los autores plantean la importancia a nivel criptográfico del algoritmo de Shor.[33]

4. **The QWalk Simulator of Quantum Walks:** El artículo señala como una serie de investigadores han comenzado a poner sus ojos en la investigaciones de las caminatas cuánticas, mediante las simulaciones numéricas.[34]

5. **A random walk approach to quantum algorithms:** Analiza las caminatas aleatorias clásicas mediante el modelo cuántico.[26]

Algunos de las publicaciones anteriores son de 2011. La revisión de todo lo anterior muestra la importancia de la computación cuántica.

A continuación comento desde diferentes enfoques científicos, ¿por qué hacer un estudio de la computación cuántica?:

### 1. Desde la tecnología y su comercialización

†La miniaturización a alcanzado en los últimos años escalas atómicas (por ejemplo, microprocesadores cuyos componentes alcanzan el tamaño de 45 nm fabricados por Intel). En consecuencia, *es necesario aprender a controlar sistemas cuánticos* individuales, para así poder usarles en el procesamiento de información.

†Para que México sea productor, y no un simple consumidor, de tecnología computacional y de comunicaciones.

### 2. Como científicos de la computación

†Diseñar computadoras y algoritmos que aprovechen las propiedades cuánticas de la materia, ya es una necesidad.

†Como se busca aumentar la capacidad de las computadoras para resolver problemas y procesar información, es necesario conocer esta implementación tecnológica.

### 3. Como físicos

†Desarrollar de manera continua herramientas que permitan aguzar (y simplificar) nuestra intuición en el estudio de la mecánica cuántica.

### 4. Para cualquier científico

†En nuestro intento por controlar sistemas cuánticos individuales, es inevitable relacionarlo con el resto del universo, por lo cual éste estudio nos lleve a aprender más sobre dicha estructura, y posiblemente generar nuevas conjeturas y mayor profundidad en nuestro propio conocimiento.

### 5. Para el desarrollo de la industria del cómputo y comunicaciones

†Ya empieza (sino es que ya lo es) a ser una necesidad imperiosa, comprender y aprovechar los efectos de la miniaturización a escala atómica/sub-atómica.

### 6. Desde la ciencia

†Conocer las leyes que la naturaleza impone, invita a nuestra capacidad, para hacer un mejor cómputo.

‡Aumentar nuestro entendimiento sobre la naturaleza y sus leyes (en particular, la mecánica cuántica) ha sido un desafío para la mente humana.

**7. Desde el punto de vista empresarial**

‡Contar con grupos de expertos (Mexicanos) que puedan orientar a las empresas, para implementar sistemas de seguridad cuántica, que es uno de los intereses que existe en el cómputo cuántico.

## Capítulo 2

# Fundamentos

En el presente capítulo definiré los siguientes conceptos: Qubit, superposición de estados, enlazamiento y paralelismo cuántico que son las propiedades cuánticas que se aprovechan en el desarrollo de la computación cuántica.

### 2.1. Qubit.

La Computación clásica almacena la información en la unidad básica denominado, *bit*, los cuales pueden tomar los valores lógicos de 0 ó 1. De manera análoga con su contraparte clásica, la computación cuántica almacena la información en la unidad básica que llamaremos *quantum bit*, o en forma corta *qubits*. Estos son estados mecánico cuánticos de partículas tales como, fotones, átomos o núcleos.

Los qubits los podemos ver como:

*Un qubit es , una entidad física descrita por las leyes de mecánica cuántica.*

*Un qubit es , un sistema cuántico de dos niveles, el cual es equivalente a un espacio vectorial de dos dimensiones sobre el campo de los números complejos.*

En la siguiente lista mostramos algunos de los más importantes sistemas que han sido considerados para éste contexto:

Sistema cuántico	Propiedad física	$ 0\rangle$	$ 1\rangle$
Fotón	Polarización lineal	Horizontal	Vertical
Fotón	Polarización circular	Izquierda	Derecha
Núcleo	Spin	Arriba	Abajo
Electrón	Spin	Arriba	Abajo
Dos niveles del átomo	Estado de excitación	Estado base	Estado excitado

La diferencia entre el bit clásico y nuestro nuevo qubit, radica en que ambos pueden tomar los valores de 0 ó 1, pero el qubit existe en un estado llamado de *superposición*, el cual es una *combinación lineal* del 0 y 1.

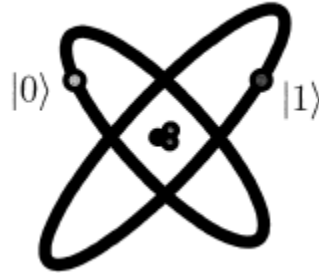


Figura 2.1: Representación de un qubit por dos niveles electrónicos en un átomo

Algo que inmediatamente comenzamos a percibir cuando nos acercamos al mundo cuántico, es que debemos abandonar todas las concepciones previas acerca del mundo derivadas de nuestra experiencia y nuestros sentidos y **dejar que las matemáticas nos dirijan**. El electrón mora en un espacio distinto del que vivimos nosotros. Reside en lo que los matemáticos llaman un **<<espacio de Hilbert>>**, como también lo hacen las otras partículas microscópicas y los fotones.[1]. Por ello la bella teoría matemática del espacio de Hilbert, el álgebra abstracta y la teoría de la probabilidad (serán nuestra herramienta matemática para tratar los fenómenos cuánticos) nos permiten predecir los resultados de experimentos con una precisión asombrosa, pero no nos proporcionan una comprensión de los procesos subyacentes. Tomando en cuenta esto y retomando la segunda parte de la última definición, un qubit matemáticamente<sup>1</sup> lo definimos de la siguiente manera:

Un qubit es un vector de dos dimensiones, que para nuestra conveniencia lo expresaremos en forma de vector columna  $\begin{pmatrix} a \\ b \end{pmatrix}$  con  $a, b \in \mathbb{C}$ .

Por razones que de momento parecerán obscuras denotaremos a los estados cero y uno como  $|0\rangle$  y  $|1\rangle$  respectivamente, entonces la superposición de un estado  $|\psi\rangle$  de esos valores es:

$$|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \quad (2.1)$$

ésta sería la representación de un qubit en superposición con notación de Dirac que a continuación explicaré. Algo importante, es que las leyes de la mecánica cuántica nos dicen la probabilidad de que el qubit se encuentre en el estado  $|0\rangle$  o en el estado  $|1\rangle$  mediante los módulos cuadráticos de  $\alpha$  y  $\beta$  de la siguiente manera:

$|\alpha|^2$  Nos determina la probabilidad de encontrar al estado  $|\psi\rangle$  en el estado  $|0\rangle$  y

<sup>1</sup>La ventaja de manejar a los qubits matemáticamente, es que no dependen de ningún sistema



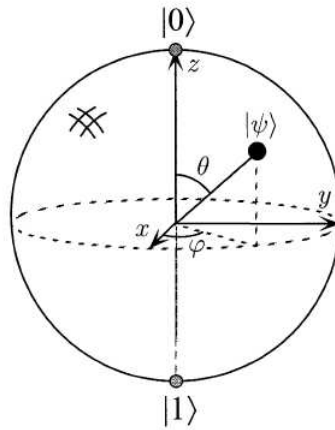


Figura 2.2: Esfera de Bloch

$|\beta|^2$  Nos determina la probabilidad de encontrar al estado  $|\psi\rangle$  en el estado  $|1\rangle$   
Además:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2.2)$$

$|\alpha|^2 = (\alpha)(\alpha)^*$  donde  $(\alpha)^*$  es el complejo conjugado de  $(\alpha)$  y de manera análoga para  $|\beta|^2$ .

En física cuántica los estados se representan por medio de la notación de Dirac<sup>2</sup>, y en cómputo cuántico se utiliza la misma notación.

Como  $|\alpha|^2 + |\beta|^2 = 1$ , la ecuación 2.1 la podemos reescribir mediante coordenadas polares, para lo cual utilizamos la identidad de Euler y suponiendo un radio  $r$  unitario, dándonos la siguiente ecuación:

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

Con los números  $\theta$  y  $\varphi$  se define un punto en una esfera unitaria tridimensional, conocida como esfera de Bloch.

La esfera de Bloch, nos proporciona una forma muy útil para la idealización de un qubit, y a menudo sirve como banco de pruebas para expresar las ideas de computación cuántica.

<sup>2</sup>Ver apéndice, donde se describe detalladamente la nomenclatura y el fundamento matemático, con dicha notación

## 2.2. Superposición cuántica

Ocurre cuando un objeto "posee simultáneamente" dos o más valores de una cantidad observable ver fig. 2.3 (ejem. la posición o la energía de una partícula). Más específicamente, en mecánica cuántica, cualquier cantidad observable corresponde a un autovector de un operador lineal hermítico. *La combinación lineal de dos o más autovectores da lugar a la superposición cuántica de dos o más valores de la cantidad, como se muestra en la ecuación 2.1.* Si se mide la cantidad, el postulado de proyección establece que el estado colapsa aleatoriamente sobre uno de los valores de la superposición (con una probabilidad proporcional al cuadrado de la amplitud de ese autovector en la combinación lineal).

De acuerdo a esto a partir de la ecuación 2.1  $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ , podemos concluir que:

$|\alpha|^2$  Nos determina la probabilidad de encontrar al estado  $|\psi\rangle$  en el estado  $|0\rangle$  y

$|\beta|^2$  Nos determina la probabilidad de encontrar al estado  $|\psi\rangle$  en el estado  $|1\rangle$

Inmediatamente después de la medida, el estado del sistema será el autovector que corresponde con el autovalor medido, es decir al medir el qubit  $|\psi\rangle$  colapsa a uno de los dos estados  $|0\rangle$  ó  $|1\rangle$ .

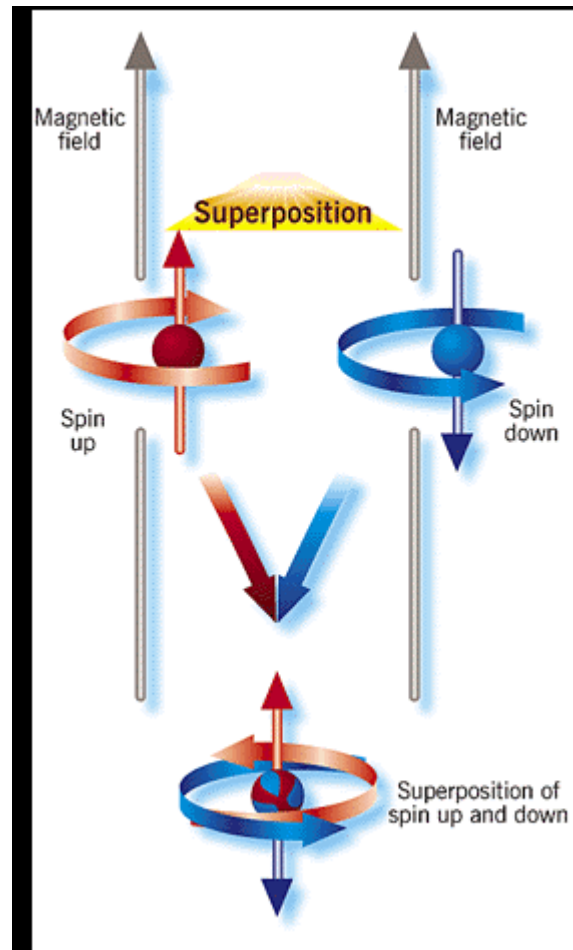


Figura 2.3: Como muestra la figura el electrón tiene un spin hacia arriba y hacia abajo, pero en la superposición posee los dos valores a la vez.

### 2.3. Enlazamiento cuántico

Básicamente, las partículas enlazadas comparten todas sus propiedades cuánticas, incluso si están separados por distancias enormes en el espacio. La parte realmente extraña es que los cambios realizados a las propiedades de una partícula al instante se producirán en la otra partícula, ver pie de figura 2.4.

En otras palabras, el enlazamiento cuántico formalmente afirma que es posible *correlacionar* dos partículas en un *solo estado cuántico*.

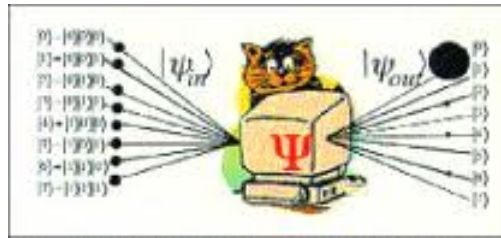


Figura 2.5: Una función  $f(x)$  se puede evaluar en múltiples valores de  $x$  simultáneamente, apoyados en la superposición

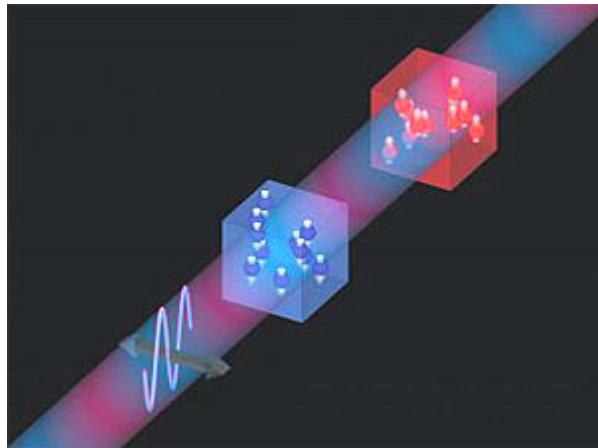


Figura 2.4: Ilustración de dos memorias cuánticas. Cada memoria consiste en una celda de vidrio lleno de átomos de cesio, que se muestran en color azul y pequeñas bolas rojas. El haz de luz se envía a través de los átomos y la información cuántica se transfiere desde la luz a los átomos. (Imágenes: Quantop)

## 2.4. Paralelismo cuántico

Heurística-mente, y aun a riesgo de simplificar en exceso, el paralelismo cuántico permite a los ordenadores cuánticos evaluar una función  $f(x)$  para muchos valores diferentes de  $x$  de *forma simultánea*, en un sólo paso algorítmico. Para lo cual recomendamos ver como opera el algoritmo de Deutsch, en el punto del apéndice B.4 .

## 2.5. Postulados de la Mecánica cuántica

El ser humano en su intento de explicar el mundo físico real que le rodea, ha desarrollado modelos que son lo más cercano a su búsqueda y que le han

permitido explicar algunos de los fenómenos físicos con los que se ha encontrado, claro, algunos lo han dejado atónito y perplejo. Entre éstas se encuentra la mecánica cuántica, y que ha desarrollado una teoría o modelo que le permite explicarse .

Habiendo examinado los estados cuánticos (qubits) y observables (operadores), cerramos el capítulo con una mirada a cómo poner esto junto, en el marco de una teoría física viable. Esto se hace mediante una lista de los "postulados" de la mecánica cuántica. Estos postulados son un conjunto de axiomas que definen cómo funciona la teoría .

### 2.5.1. Postulado 1: Estados de un sistema físico

Para cada sistema físico aislado, asociamos un espacio vectorial complejo con producto interno (es decir un espacio de Hilbert  $\mathcal{H}$ ), el cual es denominado *el espacio de estados del sistema*. El sistema físico está completamente descrito por su vector de estado, el cual es un vector unitario (*i.e.*  $\|\psi\| = 1 \in \mathcal{H}$ ) en el espacio de estados del sistema. La dimensión de  $\mathcal{H}$  depende de los grados de libertad específicos de la propiedad física bajo consideración.

Matemáticamente lo que nos deja éste postulado, es que la combinación lineal de los vectores de estado es un vector de estado, lo cual es llamado el principio de superposición la cual describe cuánticamente los sistemas físicos. Eso implica que cada estado  $|\psi\rangle$  puede ser descrito con una superposición de estados base  $\{|\phi_i\rangle\} \in \mathcal{H}$ .

De ésta manera  $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, \dots, |\phi_n\rangle$  son ket que pertenecen al espacio  $\mathcal{H}$ , la combinación lineal

$$|\psi\rangle = \alpha_1 |\phi_1\rangle + \alpha_2 |\phi_2\rangle + \alpha_3 |\phi_3\rangle + \dots + \alpha_n |\phi_n\rangle$$

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

El estado de un sistema cuántico es un vector  $|\psi\rangle$  en un espacio de Hilbert (hacemos hincapié en que puede cambiar con el tiempo). El estado  $|\psi\rangle$  *contiene toda la información* que podemos obtener sobre el sistema. Trabajamos con los estados normalizados, es decir  $\langle\psi|\psi\rangle = 1$ , lo que llamamos vectores de estado. *Un qubit es un vector de estado en un espacio vectorial complejo bidimensional* 2.1 normalizado de tal manera que 2.2.

### 2.5.2. Postulado 2: Evolución del sistema en el tiempo

Un sistema físico cerrado cambia en el tiempo, dicha evolución 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  $t_1$  está dado por

$$|\Psi(t_2)\rangle = \hat{U}|\Psi(t_1)\rangle \quad (2.3)$$

El postulado nos describe las propiedades del operador a saber; El operador depende del sistema, para el caso de un qubit simple, cada operador unitario puede ser generado en los sistemas físicos, incluso puede ser comparado con la famosa ecuación de Schrödinger, es decir la evolución del sistema está descrito por la ecuación de Schrödinger:

$$i\hbar \frac{d|\psi\rangle}{dt} = \hat{H}|\psi\rangle \quad (2.4)$$

donde  $\hbar$  es la constante de Planck y  $\hat{H}$  es un operador Hermitiano fijo, conocido como Hamiltoniano de un sistema cerrado, y que representa la función de la energía total del sistema, y cuyo cálculo no es tarea fácil.

La conexión entre ambas aproximaciones es :

$$\hat{U}|\Psi(t_1)\rangle = e^{-\frac{iH(t_2-t_1)}{\hbar}} \quad (2.5)$$

### 2.5.3. Postulado 3: Mediciones cuánticas

Al conjunto  $\{\hat{O}_n\}$  se le denomina como, operadores de medición, el subíndice  $n$  marca el resultado diferente de la medición, que actúa en el espacio de estado del sistema que está siendo medido. La medición de salida corresponde al valor de los observables, como pueden ser, la posición o el momento, los cuales son operadores Hermitianos que corresponde a las cantidades físicas medibles.

Supongamos que una medición esta dada por el observable  $\hat{M}$  el cual puede ser representado por medio de su descomposición es espectral

$$\hat{M} = \sum_i r_i \hat{P}_{r_i}$$

donde  $\hat{P}_{r_i}$  es un operador proyector para el eigenspacio  $E(r_i)$  definido por el eigenvalor  $r_i$ .

Sea  $|\psi\rangle$  el estado de un sistema cuántico inmediatamente antes de la medición, entonces la probabilidad de que el resultado  $r_i$  ocurra es dado por

$$p(r_i) = \langle \psi | \hat{P}_{r_i} | \psi \rangle$$

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

$$|\psi\rangle_{pm} = \frac{\hat{P}_{r_i} |\psi\rangle}{\sqrt{p(r_i)}}$$

además los operadores de medición deben de satisfacer la relación de completos

$$\sum_m M_m^\dagger M_m = I$$

ya que esto garantiza que la suma de las probabilidades sea 1.

$$\sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle = \sum_m p(m) = 1$$

En mecánica cuántica la medición es un proceso no trivial y altamente contrario a la intuición por las siguientes razones:

1. Las mediciones se vuelven inherentemente probabilísticas, ya que los posibles resultados de algunas mediciones son distribuidas de acuerdo a ciertas distribuciones de probabilidad.

2. Hecha una medición el sistema colapsa, es decir es inevitablemente alterado, debido a la interacción con el medio ambiente y los aparatos de medición. Por lo tanto la medición hechas antes y después son diferentes.

3. Se deben de definir un conjunto de operadores de medición que deben de cumplir, una cantidad de reglas que permitan calcular la distribución de probabilidad actual, así como los estado cuánticos de la medición posterior.

Se puede decir que las mediciones conectan al mundo real con el clásico, o bien las mediciones son la única herramienta con las cuales se puede tener una percepción de lo que pasa en el mundo cuántico.

#### 2.5.4. Postulado 4: Sistemas cuánticos compuestos

Cuando dos sistemas físicos son tratados como un sistema combinado, el espacio de estados total  $|\psi_T\rangle$  puede ser determinado usando el producto tensorial de sistemas individuales  $|\psi_T\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

Los tres primeros postulados nos remiten a sistemas individuales, lo cual es suficiente, si sólo queremos ver algunas de las propiedades cuánticas y comprobar cómo actúa la teoría, con un sistema simple basta.

Pero lo potencialmente útil a nivel cuántico, son los sistemas compuestos, es decir sistemas compuestos de uno o más subsistemas, lo cual incluye varias partículas interactuando entre si. La operación que nos permitirá analizar un sistema de n-partículas en un sistema cerrado, su evolución en el tiempo, y qué pasa cuando lo medimos, es el producto tensorial, el cual mediante un grupo de subsistemas creamos un sistema más grande, lo cual se muestra en el postulado 4.

## Capítulo 3

# Caminatas clásicas discretas

La caminata aleatoria o paseo aleatorio, abreviado en inglés como RW (Random Walks), es una formalización matemática de la trayectoria que resulta de hacer sucesivos pasos aleatorios. Los resultados del análisis de paseo aleatorio han sido aplicados a la computación, la física, la ecología o la economía. En física, el modelo ha servido, por ejemplo, para modelar el camino seguido por una molécula que viaja a través de un líquido o un gas (movimiento browniano). En ecología, se emplea para modelar los movimientos de un animal de pastoreo, etc.

### 3.1. Definición

En su forma más general, los paseos aleatorios son cualquier proceso aleatorio donde la posición de una partícula en cierto instante depende sólo de su posición en algún instante previo y alguna variable aleatoria que determina su subsecuente dirección y la longitud de paso. Casos específicos o límites de los paseos aleatorios incluyen la caminata de un borracho, el vuelo de Lévy y el movimiento browniano. Los paseos aleatorios están relacionados con los modelos de difusión y son un tema fundamental en la discusión de los procesos de Márkov. Varias propiedades de los paseos aleatorios incluyen distribuciones dispersas, tiempos del primer cruce y rutas de encuentro.

Formalmente digamos que  $X(t)$  define una trayectoria que empieza en la posición  $X_0 = X(0)$ .

Un paseo aleatorio se modela mediante la siguiente expresión:

$$X(t + \tau) = X(t) + \Phi(t)$$

donde  $\Phi$  es la variable aleatoria que describe la ley de probabilidad para tomar el siguiente paso y  $\tau = 1$  es el intervalo de tiempo entre pasos subsecuentes. A medida que la longitud y dirección de un paso dado depende solo de la posición  $X(t)$  y no de alguna posición previa, se dice que el paseo aleatorio posee la Propiedad de Márkov. Comúnmente la distribución del paso será



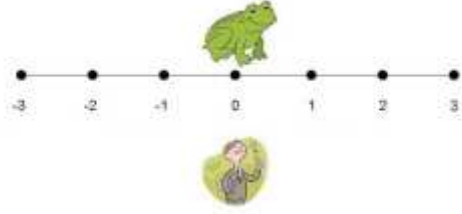


Figura 3.1: Cada paso de la caminata aleatoria consiste en que Froggy se mueve a la izquierda o derecha. El sentido de éste movimiento depende del resultado del volado.

independiente de la posición o del tiempo transcurrido, una propiedad llamada homogeneidad. De cualquier modo, la formulación es extremadamente general. Los paseos aleatorios pueden ocurrir en cualquier número de dimensiones, ser parciales o imparciales, discretos o continuos en el tiempo y/o espacio, y pueden violar lo homogeneidad en algún número de formas.

### 3.1.1. Caso unidimensional

Con la notación anterior una caminata simple, discreta y unidimensional en la recta numérica tiene un intervalo  $\tau = 1$  y  $\Phi$  son variables aleatorias independientes con una distribución de Bernoulli que toma valor  $+1$  con probabilidad  $p$  y  $-1$  con probabilidad  $1-p$  en cada paso. Una caminata simple, discreta, unidimensional y sin sesgo tiene la misma probabilidad de ir a la derecha que a la izquierda, es decir  $p = 0.5$ .

Es decir el modelo básico de las caminatas aleatorias es el movimiento de una partícula llamado **caminate** sobre puntos discretos distribuidos sobre una línea sin restricciones. El sentido del movimiento del caminante, **izquierda o derecha**, dependen de un sistema bivaluado, como por ejemplo el de **una moneda**, cuyos valores, para cada paso, depende de la probabilidad.

Para ejemplificar de manera graciosa lo anterior, suponga que tenemos a la rana Froggy y una moneda, como se muestra en la figura 4.1. Froggy se desplazará sobre una línea y su movimiento dependerá del resultado de tirar volados. Si el resultado del volado es sol entonces Froggy da un brinco a la derecha, y si el resultado del volado es águila Froggy se moverá a la izquierda, suponemos que Froggy se encuentra al inicio en el origen o posición cero de la recta.

Después de muchos volados (digamos, un millón), uno puede hacer varias preguntas interesantes, por ejemplo: ¿Cuál es la probabilidad de que Froggy se encuentre en la posición 100?

La ecuación que nos permite calcular la probabilidad de encontrar a nuestra rana en el lugar  $k$ , suponiendo que el movimiento comenzó en la posición 0 y que Froggy se ha movido  $n$ -veces ( esto es, que se han tirado  $n$ -volados) están dada por la distribución binomial

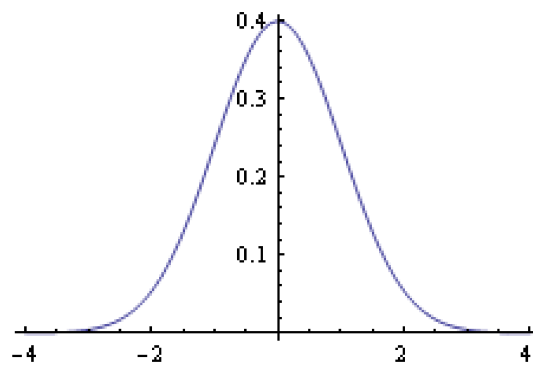


Figura 3.2: La Distribución para una caminata aleatoria clásica es del tipo Binomial, tendiendo para el número de pasos muy grandes a una normal.

$$P_{0k}^n = \binom{n}{\frac{1}{2}(k+n)} p^{\frac{1}{2}(k+n)} q^{\frac{1}{2}(k-n)}$$

cuya gráfica se muestra en la figura 3.2:

Dos propiedades importantes de las caminatas aleatorias sobre una línea son:

1. La varianza de la distribución es proporcional al número de pasos ejecutados, es decir  $\sigma^2 = \mathcal{O}(n)$ .

2 La forma de la distribución binomial no depende del punto de partida, lo que implica que si cambiamos a Froggy al punto 10 en vez de cero, la gráfica sólo se desplaza a la derecha o a la izquierda según sea el caso.

En resumen, una caminata aleatoria, la podemos describir de manera general como un proceso aleatorio con:

1. Un caminante, que se moverá de acuerdo a un sistema probabilístico ( en éste caso la moneda).

2. La moneda que determina hacia donde se mueve el caminante, como resultado de haberla arrojado.

### 3.2. Modelos computacionales determinísticos y no determinísticos

La teoría de la computación se divide en tres áreas de estudio, a saber:

1. **Teoría de autómatas**, cuyo objetivo es la creación de modelos matemáticos de computadora. Un ejemplo de estos modelos es la máquina de Turing.

2. **Teoría de la computabilidad**. Dado un problema P y el modelo matemático M de una computadora, esta disciplina estudia si dicho problema P puede

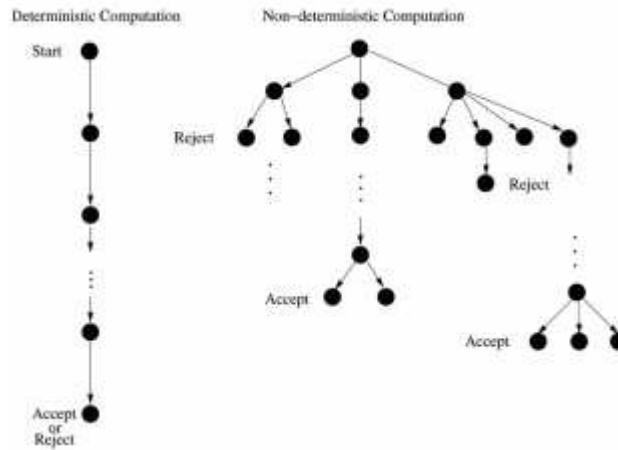


Figura 3.3: Cómputo determinístico y no determinístico

ser resuelto, en principio, con el modelo  $M$ , siendo válido suponer que se cuenta con una cantidad ilimitada de recursos (por ejemplo, tiempo o memoria).

3. **Teoría de la complejidad.** Suponga que tenemos un modelo computacional  $M$  y un problema  $P$  que se puede resolver con un algoritmo  $A$  implantado en el modelo  $M$ . La pregunta que debe responder esta rama de la computación es: ¿cuántos recursos hay que invertir para ejecutar  $A$  en  $M$ ? En otras palabras, la teoría de la complejidad cuantifica el costo (tiempo o energía, por ejemplo) de ejecutar **un algoritmo**.

Respecto a los algoritmos, existen varias formas de ejecutar algoritmos en modelos computacionales.

Uno de estos métodos llamado **cómputo determinístico**, consiste en crear algoritmos que obedezcan la siguiente regla: para cualquier paso  $s_i$  de un algoritmo  $A$ , siempre es posible determinar, con toda certeza, el paso  $s_{i+1}$ . En otras palabras, un algoritmo determinístico tiene un comportamiento **predecible y exacto** (visto desde las matemáticas, la relación entre un nodo y sus hojas es siempre una función, pues sólo hay una hoja por nodo).

Otro método, llamado **cómputo no-determinístico**, consiste en obedecer la siguiente regla: para un paso arbitrario  $s_i$  del algoritmo  $A$ , existen varios pasos siguientes  $s_{i+1}^j$ , donde  $j \in \{1, 2, \dots, m\}$  es un índice que corre sobre el conjunto de los  $m$  pasos que siguen a  $s_i$ . En este caso, el nodo tiene una relación no funcional con sus hojas, pues en general hay más de una hoja por nodo.

Estos tipos de cómputo se pueden visualizar como árboles al estilo de la figura 3.3, en la que el método determinístico se representa con un árbol con una sola derivación, en tanto que los procedimientos no-determinísticos permiten que, de un nodo dado, aparezcan varias ramificaciones. Cada ramificación representa un proceso computacional que se ejecuta al mismo tiempo que todos los demás.

De los dos métodos presentados, el cómputo determinístico se ajusta perfec-

tamente a la noción de disponibilidad de recursos, en tanto que en este mismo rubro, el cómputo no-determinístico se antoja irreal. Luego, ¿por qué es este método un tema de estudio en la ciencia computacional? La respuesta es que el cómputo no-determinístico no escatima la cantidad de recursos disponibles pues su objetivo es averiguar si es posible, al menos en principio, ejecutar un algoritmo dado aunque ello implique suponer el uso de una cantidad infinita de recursos. *No es lo mismo no poder resolver un problema que sólo tener que invertir muchos recursos en lograrlo.*

### 3.2.1. Máquina de Turing

Entre los diversos modelos computacionales sobresalen las *máquinas de Turing*, consideradas como el modelo computacional más poderoso creado a la fecha por las siguientes razones:

1. Cualquier problema resuelto por un modelo computacional distinto de la máquina de Turing (como los autómatas finitos) puede ser también resuelto por una máquina de Turing.
2. En consecuencia, cualquier problema resuelto con una computadora construida al día de hoy también puede ser resuelto por una máquina de Turing.

La capacidad de ejecutar algoritmos entre las máquinas de Turing, sea en su versión determinística o no determinística, difieren en el tiempo que tardan en hacerlo, como mostramos en las siguientes:

1. Aquellos algoritmos que al ejecutarse en una máquina determinística de Turing efectúen una cantidad de pasos acotada superiormente por una función  $f(n)$  polinomial en el número de datos de entrada, i. e.  $f(n) = \sum_i \alpha_i n^i$ , donde  $n$  es el número de datos de entrada del algoritmo, reciben el nombre de algoritmos P (un problema es P si encuentra solución en un algoritmo P).

2. Los algoritmos que al ejecutarse en una máquina no-determinística de Turing consumen una cantidad de pasos acotada por una función polinomial  $g(n)$  en el número de datos de entrada, i.e.  $g(n) = \sum_k \beta_k n^k$ , donde  $n$  es el número de datos de entrada del algoritmo, reciben el nombre de problemas NP (un problema es NP si encuentra solución en un algoritmo NP).

3. Por último, un algoritmo L es NP-completo si y sólo si L es NP y se cumple que, para todo problema L en NP, es posible transformar al algoritmo L en el algoritmo L usando solamente una cantidad polinomial de pasos (un problema es NP-completo si encuentra solución en un algoritmo NP-completo).

Los algoritmos P son vistos con muy buenos ojos por la comunidad de científicos computacionales, pues utilizan una cantidad aceptable de tiempo en su ejecución. Para comprender mejor este concepto analicemos el caso contrario, el de los algoritmos NP. Dada la disparidad de recursos disponibles entre los modelos determinístico y no-determinístico, la ejecución de un algoritmo NP en

una máquina determinística de Turing requiere una cantidad de recursos que crece exponencialmente (o factorialmente) en el número de datos de entrada.

La explicación de este fenómeno radica en el hecho de que, para un problema NP y un NP-completo, el espacio de soluciones posibles es muy grande, y explorarlo exhaustivamente requiere muchos recursos.

### 3.3. Algoritmos estocásticos

Se han propuesto diversos caminos para hacer del cómputo no-determinístico algo más cercano a lo que es posible hacer con una computadora real. En uno de ellos, la computadora escoge aleatoriamente (i. e. usando una distribución de probabilidad) una de las ramas del árbol no-determinístico y la ejecuta. Esto es, si el algoritmo está en el paso  $s_i$ , entonces el siguiente y **único paso**  $s_{i+1}$  se escoge (usando una distribución de probabilidad) del conjunto de pasos  $\{s_{i+1}^j \mid j \in \{1, 2, 3, \dots, m\}\}$ . Este proceso se conoce con el nombre de **cómputo probabilístico** y, aunque no es precisamente equivalente al cómputo no-determinístico, su gran ventaja es que es posible implantarlo en una computadora convencional (el único problema práctico es que no es posible generar números totalmente aleatorios en una computadora convencional, mas los números pseudo-aleatorios son, en general, suficientemente buenos para muchas aplicaciones).

Un **algoritmo estocástico** es un algoritmo cuya sucesión de pasos (i. e. cuya evolución en el tiempo) se produce usando una distribución de probabilidad.

Dicho de otra forma, un algoritmo estocástico es un procedimiento ejecutado en una máquina capaz de hacer cómputo probabilístico.

Los algoritmos estocásticos juegan un papel central en el estudio de los problemas NP-completos pues, gracias a ellos, es posible encontrar soluciones para dichos problemas, que consumen menos pasos que los que requeriría un algoritmo de fuerza bruta, i. e. un algoritmo que explorase, exhaustivamente, el espacio completo de posibles soluciones.

### 3.4. Conclusiones de la caminata aleatoria clásica

De acuerdo al ejemplo de una dimensión y que posteriormente compararemos estadísticamente con la caminata cuántica, de la caminata al azar clásica tenemos:

1. Cada paso, se elige al azar la dirección, la cual depende del resultado de la moneda.

2.  $P(x, t)$  es una distribución binomial:

$$P(x, t) = \frac{t!}{\left(\left(\frac{t+x}{2}\right)!\right)\left(\left(\frac{t-x}{2}\right)!\right)} p^{\frac{t+x}{2}} (1-p)^{\frac{t-x}{2}}$$

con media  $\bar{x} = (2p - 1)t$ ; varianza  $\sigma^2 = 4tp((1 - p))$ .

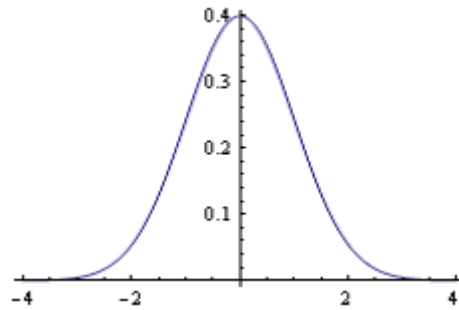


Figura 3.4: Las caminatas aleatorias clásicas generan una distribución normal o gaussiana, para un número de pasos bastante grande.

Pero si  $p = q = \frac{1}{2}$  es decir una caminata equilibrada tendríamos

$$P(x, t) = \frac{t!}{\left(\left(\frac{t+x}{2}\right)!\right)\left(\left(\frac{t-x}{2}\right)!\right)} \left(\frac{1}{2^t}\right)$$

con media  $\bar{x} = 0$  ; varianza  $\sigma^2 = t$

3. La distribución  $P(x)$ , luego de muchos pasos ( $t \gg 1$ ), es aproximadamente gaussiana como en fig 3.4:

4. El ancho característico  $\sigma(t)$  crece linealmente con  $t$  (proceso difusivo)

5. El desarrollo que va generando en cada paso (hasta el paso 5, en nuestra figura) la caminata aleatoria clásica se muestra en la fig 3.5

$t \setminus n$	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					$\frac{1}{2}$		$\frac{1}{2}$				
2				$\frac{1}{4}$		$\frac{2}{4}$		$\frac{1}{4}$			
3			$\frac{1}{8}$		$\frac{3}{8}$		$\frac{3}{8}$		$\frac{1}{8}$		
4		$\frac{1}{16}$		$\frac{4}{16}$		$\frac{6}{16}$		$\frac{4}{16}$		$\frac{1}{16}$	
5	$\frac{1}{32}$		$\frac{5}{32}$		$\frac{10}{32}$		$\frac{10}{32}$		$\frac{5}{32}$		$\frac{1}{32}$

Figura 3.5: Los 5 primeros (t) lanzamientos de una caminata aleatoria clásica se pueden observar, así como las posiciones (n) en la recta que van avanzando con sus respectivas probabilidades de tales posiciones.

## Capítulo 4

# Caminatas Cuánticas Discretas

En éste capítulo revisaremos la contraparte de las caminatas aleatorias clásicas, las caminatas cuánticas, las cuales nos permitirán abordar los mismos problemas que en las caminatas aleatorias clásicas y ver ventajas y desventajas entre ellas.

### 4.1. Modelo de Caminatas cuánticas (QW)

Las caminatas cuánticas son la contraparte cuántica de las caminatas aleatorias clásicas.

La caminata cuántica (QW) de acuerdo a [24], es un análogo de una cadena de Markov, en el cual el componente estocástico (un bit de información obtenido, digamos, como resultado de arrojar una moneda) se reemplaza por una operación unitaria aplicada sobre un qubit. Si este qubit se mide a cada paso, se destruye la coherencia y el proceso es markoviano. Pero si se le deja evolucionar en forma unitaria, y se realiza el desplazamiento condicional se obtiene un proceso coherente con características propias.

En una cadena de Markov o caminata al azar, la posición del caminante en un instante dado  $t$  queda determinada por su posición anterior, en  $t - 1$ , donde  $t$  es una variable discreta no negativa. 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. Ocupa sitios discretos uniformemente distribuidos en una línea, que indicamos por enteros  $x = 0, \pm 1, \pm 2, \dots$  (vea la Fig. 4.1).

El desplazamiento es condicional al valor de una variable aleatoria binaria. La caminata al azar es un paradigma para procesos difusivos en general y como tal encuentra múltiples aplicaciones en Ciencia y Tecnología. En particular, las cadenas de Markov han servido de base para diversos algoritmos de optimización que requieren la exploración de espacios multidimensionales.



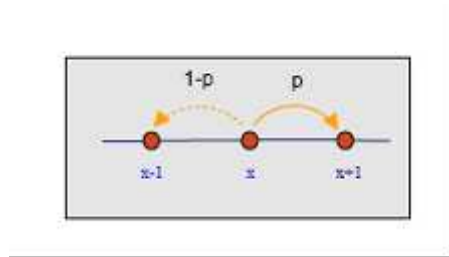


Figura 4.1: En su versión básica unidimensional, un caminante al azar da un paso a la derecha con probabilidad  $p$  o (excluyente) a la izquierda con probabilidad  $1 - p$ .

Por ejemplo, algunos de los mejores algoritmos para resolver problemas NP-completos son estocásticos y se basan en la caminata al azar.

Una caminata aleatoria clásica unidimensional se define en términos de las probabilidades de una partícula a dar un paso de una longitud dada a la izquierda o a la derecha. La caminata aleatoria cuántica se describen en cambio, en términos de las amplitudes de probabilidad.

Existen dos modelos de caminatas cuánticas, las discretas (DQRW) y las continuas (CQRW), en el presente trabajo nos enfocaremos en las discretas (En su versión a tiempo discreto, el QW fue propuesto originalmente por [25]).

## 4.2. Estructura del modelo de una caminata cuántica (QW)

Los actores principales de una caminata cuántica sobre una línea (DQWL) son: *Un caminante, una moneda y un operador de evolución para ambos, además de un conjunto de observables.*

### *El caminante*

El caminante es un sistema cuántico que viven en un espacio de Hilbert de dimensión infinita, pero numerable  $\mathcal{H}_p$ . Es una costumbre usar vectores de la base canónica computacional de  $\mathcal{H}_p$  como posiciones del caminante. De ésta manera denotaremos al caminante como  $|posición\rangle \in \mathcal{H}_p$  y afirmamos que los estados de la base canónica  $|i\rangle_p$  genera  $\mathcal{H}_p$ , tan bien como la superposición de la forma  $\sum_i \alpha_i |i\rangle_p$ , sujeta a que  $\sum_i |\alpha_i|^2 = 1$ , son válidos para los estados  $|posición\rangle$ . El caminante es usualmente inicializado en el origen, es decir  $|posición\rangle_{inicial} = |0\rangle_p$ .

### *La moneda*

La moneda es un sistema cuántico viviendo en un espacio de Hilbert de dos dimensiones  $\mathcal{H}_c$ . La moneda puede tomar los estados de la base canónica  $|0\rangle$  y  $|1\rangle$  tan bien como cualquier superposición de esa base de estados. Por lo tanto

la  $|moneda\rangle \in \mathcal{H}_c$ , y en general los estados normalizados de la moneda pueden ser escritos como  $|moneda\rangle = a|0\rangle_c + b|1\rangle_c$ , con  $|a|^2 + |b|^2 = 1$ .

El espacio total de la caminata cuántica reside en  $\mathcal{H}_t = \mathcal{H}_p \otimes \mathcal{H}_c$ . Hasta aquí, únicamente los estados de  $\mathcal{H}_t$  se han utilizado como estados iniciales, esto es,  $|\psi\rangle_{inicial} = |posición\rangle_{inicial} \otimes |moneda\rangle_{inicial}$ .

### Operador de evolución

La evolución del caminante cuántico está dividido en dos partes que se parecen mucho al comportamiento de una caminata clásica. En el caso clásico, el azar juega un rol clave en la evolución del sistema.

Lo cual será evidente en el siguiente ejemplo: en primer lugar se lanza una moneda (ya sea parcial o imparcialmente) y, a continuación, dependiendo del resultado de la moneda, el caminante se mueve un paso hacia la derecha o hacia la izquierda. En el caso cuántico, el equivalente del proceso anterior consiste en aplicar un operador de evolución al estado de la moneda, seguido de un operador de cambio condicional al sistema cuántico total. El objetivo del operador de la moneda es hacer que ella se encuentre en una superposición, y la aleatoriedad se introduce mediante la realización de una medición sobre el sistema después de que ambos operadores de evolución se han aplicado al total del sistema cuántico varias veces.

Dentro de los operadores monedas ( $\hat{C}$ ) comúnmente usados en caminatas cuánticas tenemos al operador Hadamard, el cual se identifica por  $\hat{H}$ , para lo cual retomamos la representación de su producto externo dado en la subsección 2.4.5

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle_{cc} \langle 0| + |0\rangle_{cc} \langle 1| + |1\rangle_{cc} \langle 0| - |1\rangle_{cc} \langle 1|) \quad (4.1)$$

Para el operador de cambio condicional se hace uso de un operador unitario, que permita al caminante un paso hacia adelante, si el estado de la moneda esta acompañado de un de los dos estados base (por ejemplo  $|0\rangle$ ), o un paso hacia atrás, si el estado de la moneda está acompañado del otro de los estados base (es decir  $|1\rangle$ ). Una condición adecuada del operador de cambio condicional es el que tiene la forma:

$$\hat{S} = |0\rangle_{cc} \langle 0| \otimes \sum_i |i+1\rangle_{pp} \langle i| + |1\rangle_{cc} \langle 1| \otimes \sum_i |i-1\rangle_{pp} \langle i| \quad (4.2)$$

Por consecuencia, el operador total del espacio de Hilbert es,  $\hat{U} = \hat{S} \cdot (\hat{C} \otimes \hat{I}_p)$ , y una representación matemática de una caminata cuántica después de  $t$ -pasos es :

$$|\psi\rangle_t = (\hat{U})^t |\psi\rangle_{inicial} \quad (4.3)$$

donde  $|\psi\rangle_{inicial} = |posición\rangle_{inicial} \otimes |moneda\rangle_{inicial}$

### Observables

La ventaja de las caminatas cuánticas sobre las clásicas, son las consecuencias de los efectos de interferencia entre la moneda y el caminante después de varias aplicaciones de  $\hat{U}$ . Sin embargo, debemos desarrollar una medida en algún punto, con el fin de conocer el resultado de nuestro caminante. Para hacerlo, definimos un conjunto de observables de acuerdo a los estado base, que se han utilizado para definir la moneda y el caminante. Hay varias formas de extraer la información del sistema cuántico compuesto. Por ejemplo, en primer lugar realizamos una medición sobre la moneda usando el observable

$$\hat{M}_c = \alpha_0 |0\rangle_{cc} \langle 0| + \alpha_1 |1\rangle_{cc} \langle 1| \quad (4.4)$$

Entonces una medida debe de efectuarse sobre el estado de posición de el caminante, mediante el uso del operador:

$$\hat{M}_p = \sum_i a_i |i\rangle_{pp} \langle i| \quad (4.5)$$

### 4.3. Características del Simulador de Mathematica

Con base en [25] que es considerado el primer artículo de caminatas cuánticas, [35] desarrolla el simulador de cómputo cuántico, del cual tomamos la parte de caminatas cuánticas para generar los resultados que a continuación presentamos. Pasemos a describir brevemente como funciona el simulador de Mathematica.

1. La moneda  $C$  puede tener únicamente dos estados, el estado 0 y el estado 1 (águila o sol (cara o cruz en ingles)), mientras que el caminante  $P$  puede estar en cualquier posición (entera). Tanto la moneda como el caminante están inicializados en el origen, es decir en cero, todo lo cual se denota por:

$$|w[0]\rangle = |0\rangle_{\hat{c}} \otimes |0\rangle_{\hat{p}}$$

2. Definimos el operador para lanzar la moneda, para nuestro caso es el operador Hadamard, aunque puede ser cualquier otro operador unitario que actué solamente sobre la moneda  $C$ .

$$\hat{H} = \frac{1}{\sqrt{2}} (|0_{\hat{c}}\rangle \langle 0_{\hat{c}}| + |1_{\hat{c}}\rangle \langle 0_{\hat{c}}| + |0_{\hat{c}}\rangle \langle 1_{\hat{c}}| - |1_{\hat{c}}\rangle \langle 1_{\hat{c}}|)$$

3. Definimos el operador para el movimiento del caminante

$$s = |0_{\hat{c}}\rangle \langle 0_{\hat{c}}| \otimes \sum_{j=-\infty}^{\infty} (|(j-1)_{\hat{p}}\rangle \cdot \langle j_{\hat{p}}|) + |1_{\hat{c}}\rangle \langle 1_{\hat{c}}| \otimes \sum_{j=-\infty}^{\infty} (|(j+1)_{\hat{p}}\rangle \cdot \langle j_{\hat{p}}|)$$

4. Aquí se define la posición del proyector para cada posición del caminante:

$$pp[j] := |0_{\hat{c}}, j_{\hat{p}}\rangle \cdot \langle 0_{\hat{c}}, j_{\hat{p}}| + |1_{\hat{c}}, j_{\hat{p}}\rangle \cdot \langle 1_{\hat{c}}, j_{\hat{p}}|$$

5. El programa calculan en automático las probabilidades y genera la gráfica correspondiente.

### 4.3.1. Ejemplo con los tres primeros pasos detallados

1. Preparamos el sistema, para lo cual definimos el estado inicial, de manera que la moneda estará en reposo o sin lanzar, mientras que nuestro caminante se encuentra en el origen, es decir en posición cero.

Para ello definimos  $|\psi\rangle_0$  nuestro estado inicial,  $|0\rangle_m$  nuestro estado inicial o cero de la moneda,  $|0\rangle_c$  el estado inicial o cero del caminante, por supuesto que la moneda habita en  $\mathcal{H}_m$  espacio de Hilbert, y el caminante en  $\mathcal{H}_c$  espacio de Hilbert totalmente distinto al de la moneda, así nuestro estado  $|\psi\rangle_0$  habita en el espacio de Hilbert total [ver A.5]  $\mathcal{H}_t = \mathcal{H}_m \otimes \mathcal{H}_c$ , de lo cual tenemos:

$$|\psi\rangle_0 = |0\rangle_m \otimes |0\rangle_c$$

2. Ahora el producto tensorial, entre un operador de Hadamard y el operador identidad (que no tiene ningún efecto, pero que juega un papel importante), nos permite construir o definir el operador (cuyo propósito es poner en superposición a la moneda) que lanzará el volado de la moneda y por ende el avance del caminante, es decir:

$$\hat{S} = \hat{H} \otimes \mathbf{I}$$

3. Ahora se establece el operador unitario  $U$ , a través del cual podemos ver la evolución del sistema, además de indicarnos a donde se moverá el caminante de acuerdo al estado de la moneda, es decir, si la moneda se encuentra en  $|1\rangle$  el caminante se moverá a la derecha, si la moneda se encuentra en  $|0\rangle$  el caminante se moverá a la izquierda, *y es aquí donde se puede observar las ventajas de la superposición, ya que el caminante se encontrará moviéndose en dos lugares en el primer paso.*

$$U = \left( |0\rangle_{mm} \langle 0| \otimes \sum_{j=-\infty}^{\infty} |j+1\rangle_{cc} \langle j| \right) + \left( |1\rangle_{mm} \langle 1| \otimes \sum_{j=-\infty}^{\infty} |j-1\rangle_{cc} \langle j| \right)$$

4. De ésta manera, primeramente aplicamos el operador  $S$  a nuestro estado  $|\psi\rangle_0$ , para obtener un estado  $|\psi'\rangle_0$ , de la siguiente manera:

$$|\psi'\rangle_0 = \hat{S} |\psi\rangle_0 = (\hat{H} \otimes \mathbf{I}) \cdot (|0\rangle_m \otimes |0\rangle_c) = (\mathbf{H} |\hat{0}\rangle_m) \otimes (\mathbf{I} |0\rangle_c) = \frac{|0\rangle_m |0\rangle_c + |1\rangle_m |0\rangle_c}{\sqrt{2}}$$

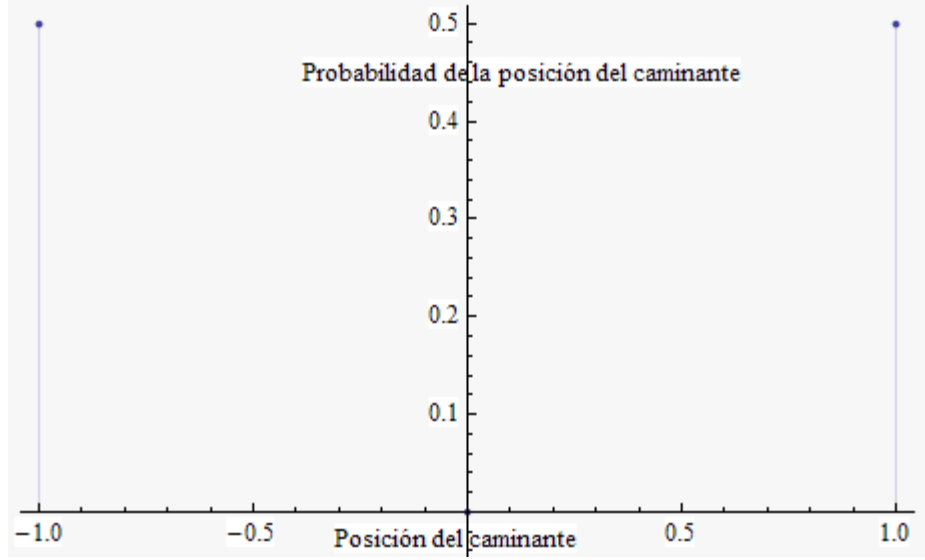


Figura 4.2: En ésta gráfica podemos observar el comportamiento del caminante en el primer paso, vemos el principio de superposición en acción.

5. Ahora hacemos que actúe el operador  $U$  sobre el sistema:

$$\begin{aligned}
 |\psi\rangle_1 &= U |\psi'\rangle_0 = \left\{ \left( |0\rangle_{mm} \langle 0| \otimes \sum_{j=-\infty}^{\infty} |j+1\rangle_{cc} |j\rangle \right) + \left( |1\rangle_{mm} \langle 1| \otimes \sum_{j=-\infty}^{\infty} |j-1\rangle_{cc} |j\rangle \right) \right\} \\
 &\cdot \left\{ \frac{|0\rangle_m |0\rangle_c + |1\rangle_m |0\rangle_c}{\sqrt{2}} \right\} = \\
 &= \frac{1}{\sqrt{2}} [(|0\rangle_m \langle 0|_0 \otimes |0+1\rangle_c \langle 0|_0) + (|0\rangle_m \langle 0|_1 \otimes |0+1\rangle_c \langle 0|_0)] + \\
 &+ \frac{1}{\sqrt{2}} [(|1\rangle_m \langle 1|_0 \otimes |0+1\rangle_c \langle 0|_0) + (|1\rangle_m \langle 1|_1 \otimes |0-1\rangle_c \langle 0|_0)] \\
 &= \frac{1}{\sqrt{2}} \{ (|0\rangle_m \langle 0|_0 \otimes |0+1\rangle_c \langle 0|_0) + (|1\rangle_m \langle 1|_1 \otimes |0-1\rangle_c \langle 0|_0) \}
 \end{aligned}$$

De ésta manera el caminante, después del primer paso adquiere la siguiente forma:

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

Veamos ésto gráficamente:

Como vemos en la figura 4.2 el caminante queda posicionado en 1 y  $-1$  al mismo tiempo, debido al principio de superposición, en el eje horizontal se parametriza la posición del caminante  $|p\rangle_c$ .

Para el segundo paso, actuamos de manera muy similar al primero, es decir, aplicamos una superposición en el estado de la moneda, que en éste momento es  $|\psi\rangle_1$ , e inmediatamente después se aplica el operador de evolución, lo cual nos presenta las siguientes situaciones:

$$|\psi\rangle_2 = U \cdot S|\psi\rangle_1$$

Aplicamos el operador Hadamard al estado  $|\psi\rangle_1$ :

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

El operador de evolución actuará de la siguiente manera:

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

$$\begin{aligned} |\psi\rangle_2 &= \frac{1}{2} [(|0\rangle_m \langle 0| 0\rangle_m \otimes |1+1\rangle_c \langle 1| 1\rangle_c) + (|1\rangle_m \langle 1| 0\rangle_m \otimes |1-1\rangle_c \langle 1| 1\rangle_c)] + \\ &\frac{1}{2} [(|0\rangle_m \langle 0| 1\rangle_m \otimes |1+1\rangle_c \langle 1| 1\rangle_c) + (|1\rangle_m \langle 1| 1\rangle_m \otimes |1-1\rangle_c \langle 1| 1\rangle_c)] + \\ &\frac{1}{2} [(|0\rangle_m \langle 0| 0\rangle_m \otimes |-1+1\rangle_c \langle -1| -1\rangle_c) + (|1\rangle_m \langle 1| 0\rangle_m \otimes |-1-1\rangle_c \langle -1| -1\rangle_c)] + \\ &\frac{1}{2} [(|0\rangle_m \langle 0| 1\rangle_m \otimes |-1+1\rangle_c \langle -1| -1\rangle_c) + (|1\rangle_m \langle 1| 1\rangle_m \otimes |-1-1\rangle_c \langle -1| -1\rangle_c)] = \\ &= \frac{1}{2} [(|0\rangle_m \langle 0| 0\rangle_m \otimes |1+1\rangle_c \langle 1| 1\rangle_c) + (|1\rangle_m \langle 1| 1\rangle_m \otimes |1-1\rangle_c \langle 1| 1\rangle_c)] + \\ &\frac{1}{2} [(|0\rangle_m \langle 0| 0\rangle_m \otimes |-1+1\rangle_c \langle -1| -1\rangle_c) + (|1\rangle_m \langle 1| 1\rangle_m \otimes |-1-1\rangle_c \langle -1| -1\rangle_c)] \end{aligned}$$

Lo que al final nos arroja:

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

Lo que la ecuación final de  $|\psi\rangle_2$  nos indica es que el sistema del caminante, se encuentra con 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, lo cual se vislumbra en la gráfica 4.3

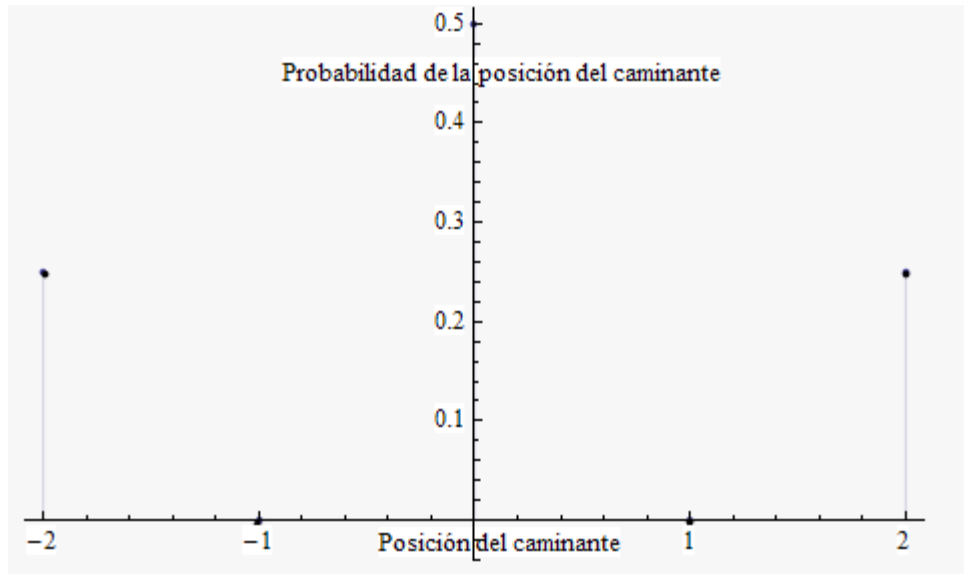


Figura 4.3: En ésta gráfica podemos observar el comportamiento del caminante en el segundo paso, vemos más enfáticamente el principio de superposición en acción.

A continuación presentamos la gráfica del paso 3, que comienza a mostrar un ligero desbalance a la izquierda, además como vemos el sistema se puede encontrar en cuatro putos distintos del eje horizontal, nuevamente debido al principio de superposición.

El desarrollo algebraico del paso tres nos conduce a:

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

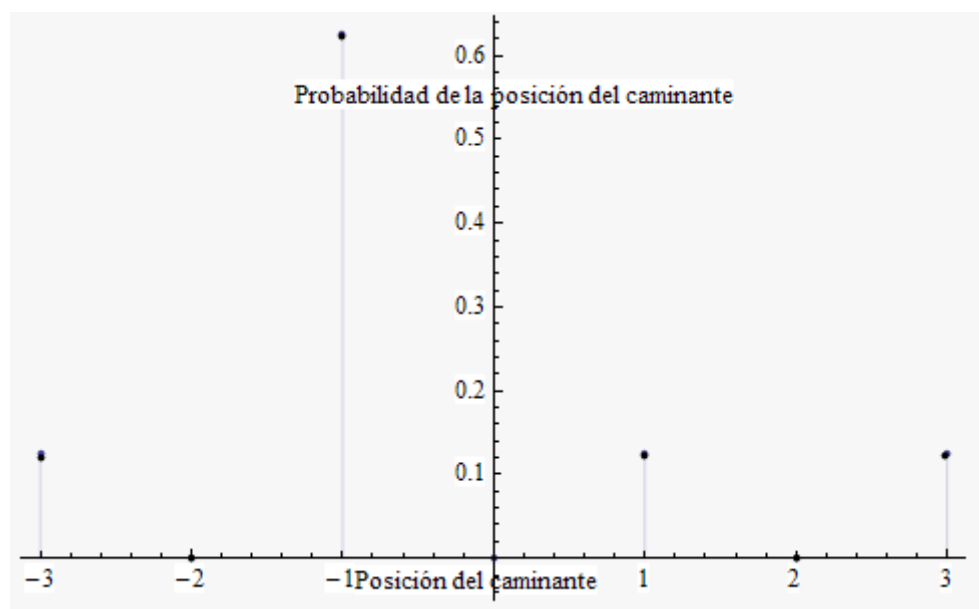


Figura 4.4: En ésta gráfica podemos observar el comportamiento del caminante en el tercer paso, vemos el principio de superposición nuevamente en acción.

Ahora veamos en la gráfica de la fig. 4.5 , la distribución después de 100 pasos:



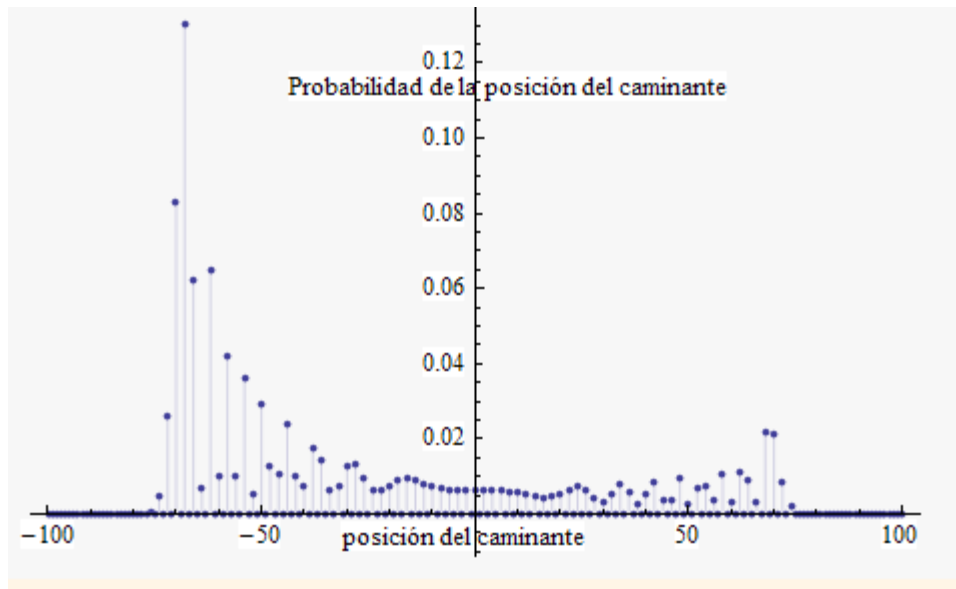


Figura 4.5: Distribución de caminata cuántica con 100 iteraciones, caminante y moneda en el origen

Lo primero que percibimos al ver el gráfico es la forma de la distribución, totalmente diferente de una caminata clásica, tales diferencias las podemos resumir en la fig. 4.6 , donde comparamos las caminatas clásicas discretas (DRW) y las caminatas cuánticas discretas (DQW):

Las características mencionadas en fig.4.6 las podemos apreciar Gráficamente en la fig. 4.7

Ahora presentamos una gráfica que nos muestra tanto la caminata clásica como la cuántica en 100 pasos, podemos ver sus respectivas distribuciones:

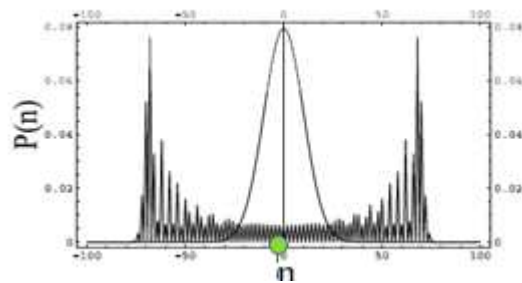


Figura 4.7: Distribuciones comparadas para la iteración  $t=100$ . La distribución fuertemente oscilante corresponde al caminante cuántico que muestra mayor probabilidad de estar lejos del origen que el caminante clásico.

Caminata clásica (RW)	Caminata Cuántica (QW)
<p>1. La varianza de la distribución binomial es proporcional al número de pasos ejecutados,</p> <p>2. La forma de la distribución no depende del punto de partida</p> <p>3. La ecuación que nos permite calcular la probabilidad es una distribución binomial.</p>	<p>1. Las caminatas cuánticas discretas tiene una varianza que crece proporcionalmente al cuadrado del número de pasos</p> <p>1.1 Se puede aumentar la velocidad ejecución de un algoritmo basado en QW.</p> <p>2. La forma de la distribución depende del punto de partida</p> <p>2.1 El estado del caminante o de la moneda puede ser usado como parámetro computacional.</p>

Figura 4.6: Comparación estadística entre caminatas clásicas y cuánticas

## 4.4. Mis resultados

### 4.4.1. Reproducción

Con base a todo lo que hemos analizado, lo primero que podemos hacer es reproducir los resultados que se muestran en los Artículos (papers) que divulgan las caminatas cuánticas, por ejemplo:

En la figuras 4.8, se muestra la gráfica que se presenta en [26], [24], [25], [3] todas manejadas a 100 iteraciones y balanceada.

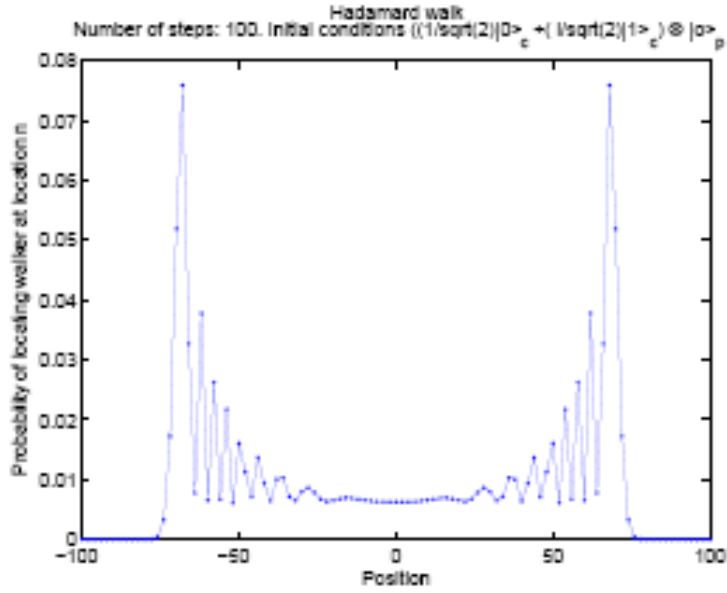


Figura 4.8: La gráfica es presentada en su tesis doctoral en [3]

Tal gráfica la reproduzco en fig.4.9 ahora entiendo que:

1. Se genera preparando el sistema, de tal manera que la moneda este en superposición, el estado inicial tiene la siguiente estructura:

$$|w[0]\rangle = \left(\frac{1}{\sqrt{2}}(|0_c\rangle + I|1_c\rangle)\right) \otimes |0_p\rangle$$

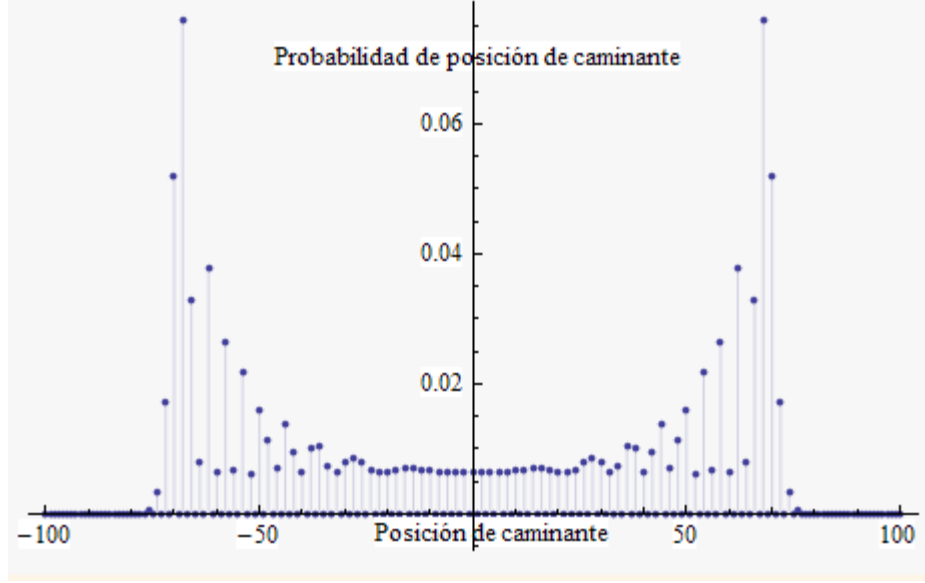


Figura 4.9: Reproducción de la gráfica de caminata cuántica con moneda en superposición

2. Ahora bien hasta este momento el simulador de Mathematica ha trabajado con el operador unitario

$$U = \left( |0\rangle_{mm} \langle 0| \otimes \sum_{j=-\infty}^{\infty} |i+1\rangle_{cc} \langle i| \right) + \left( |1\rangle_{mm} \langle 1| \otimes \sum_{j=-\infty}^{\infty} |i-1\rangle_{cc} \langle i| \right)$$

y podemos ver que los resultados en las distribuciones de las caminatas cuánticas son fácilmente alterables, de acuerdo a cómo están definidos nuestros estados iniciales y nuestro operador moneda y de desplazamiento. Un ligero cambio en nuestro operador unitario cambiando el orden de tal manera que si el estado esta  $|1\rangle$  el caminante ahora avanzará un espacio y si por el contrario la moneda esta en estado  $|0\rangle$ , entonces el caminante retrocederá un espacio, es decir:

$$U = \left( |0\rangle_{mm} \langle 0| \otimes \sum_{j=-\infty}^{\infty} |i-1\rangle_{cc} \langle i| \right) + \left( |1\rangle_{mm} \langle 1| \otimes \sum_{j=-\infty}^{\infty} |i+1\rangle_{cc} \langle i| \right)$$

a pesar de ser una modificación pequeña se nota en la distribución son muy notorios, y a partir de ello puedo generar las que son denominadas gráficas desbalanceadas en las figuras 4.10, 4.11

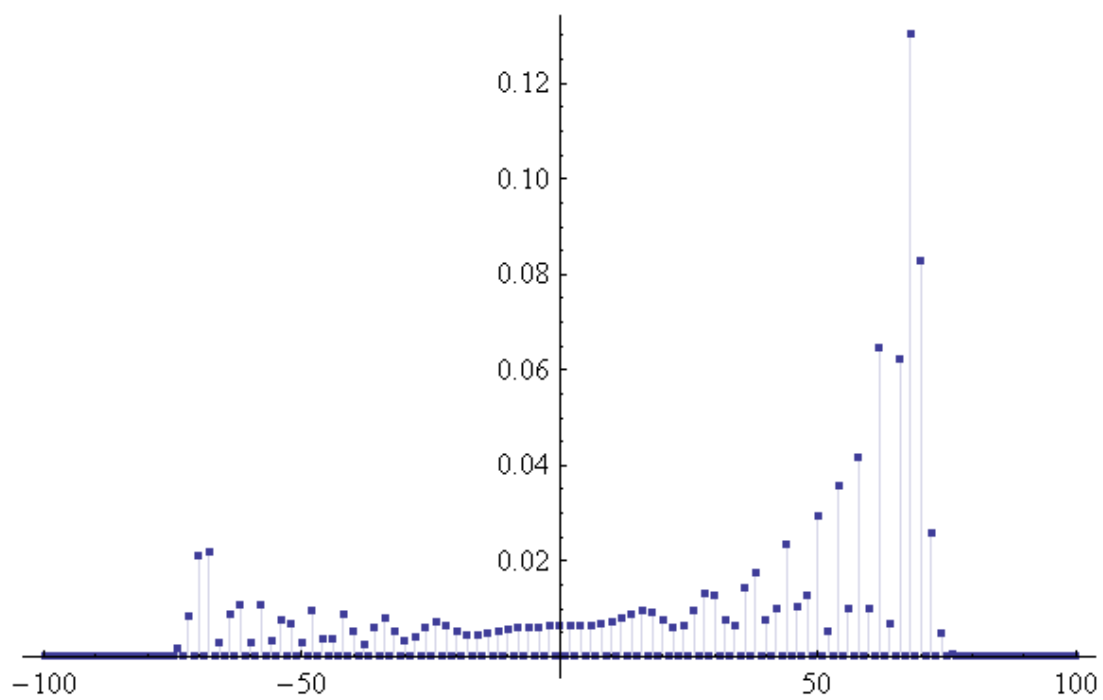


Figura 4.10: Gráfica con desbalance a la derecha

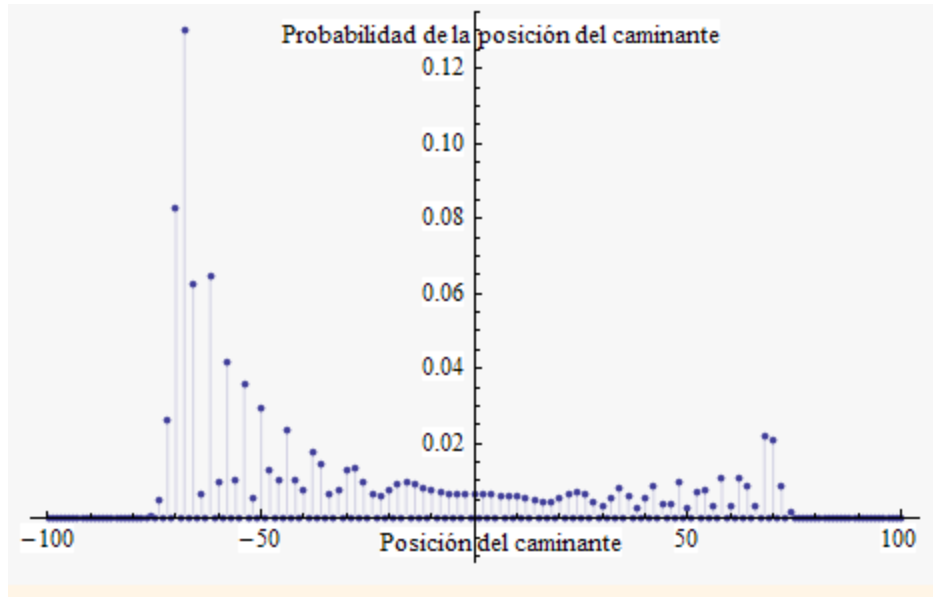


Figura 4.11: Gráfica con desbalance a la izquierda

#### 4.4.2. Mis resultados

En ésta simulación propongo poner en superposición al caminante, es decir:

$$|w[0]\rangle = |0_{\hat{c}}\rangle \otimes \left( \frac{1}{\sqrt{2}}(|0_{\hat{p}}\rangle + |1_{\hat{p}}\rangle) \right)$$

Lo cual me genera una gráfica donde podemos ver que ahora, la distribución se lleva a cabo por pares como podemos observar en fig.4.12

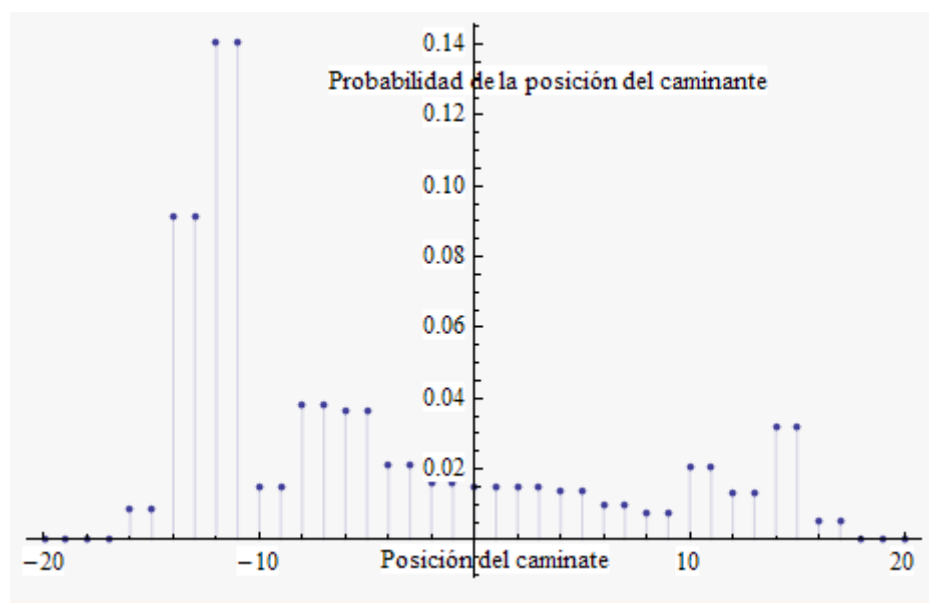


Figura 4.12: Gráfica desbalanceada a la izquierda, con caminante en superposición

También podemos generar el desbalance a la derecha y la forma balanceada como mostramos en las gráficas 4.13 y 4.14

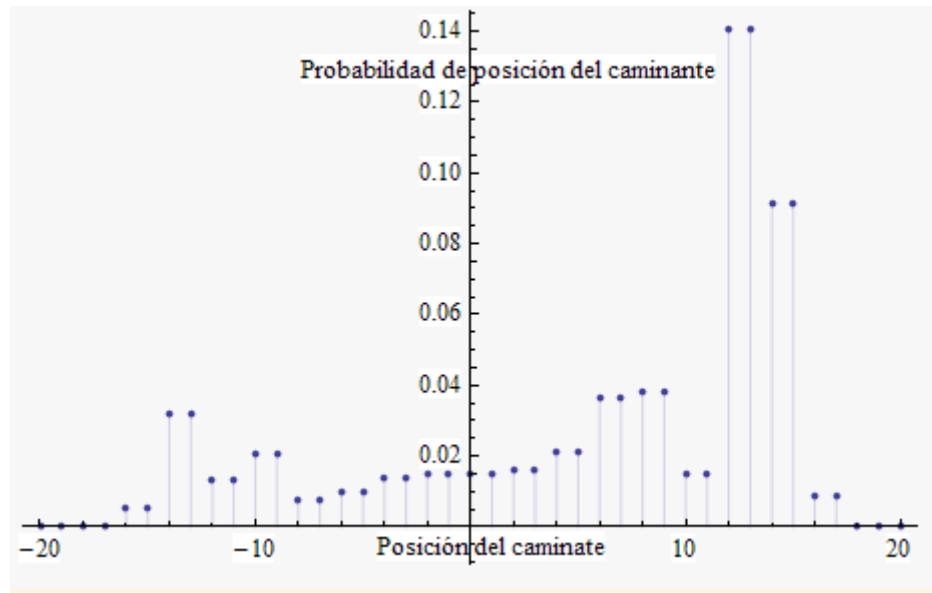


Figura 4.13: Gráficas con caminante en superposición desbalanceada a la derecha y a la izquierda

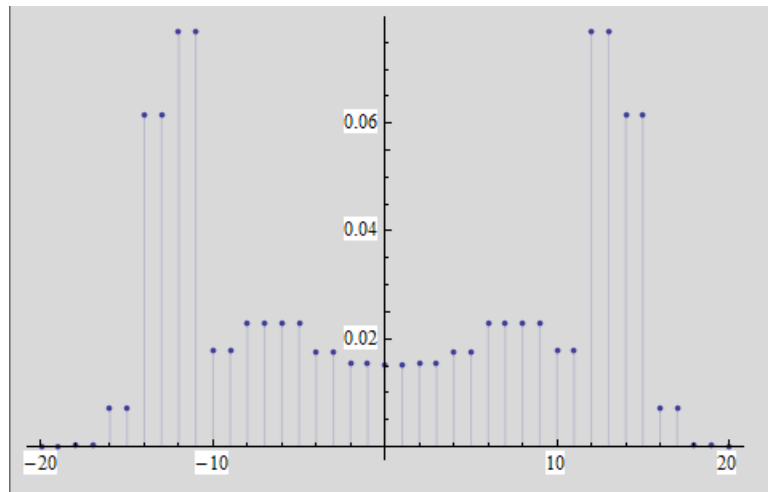


Figura 4.14: Gráfica balanceada con caminante en superposición

#### 4.4.3. Propuesta de moneda $M$ .

De acuerdo a las características que he observado que debe de cumplir el operador moneda, en el caso del simulador y en los artículos, es el operador



Hadamard, encuentre un operador distinto que puede fungir como moneda, al que denomine  $M$ , y que se define así:

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

Que en forma de productos externos obtenemos:

$$M = \frac{1}{\sqrt{2}} (|0\rangle \langle 0| - i |0\rangle \langle 1| - i |1\rangle \langle 0| + |1\rangle \langle 1|)$$

La distribución para éste operador es:

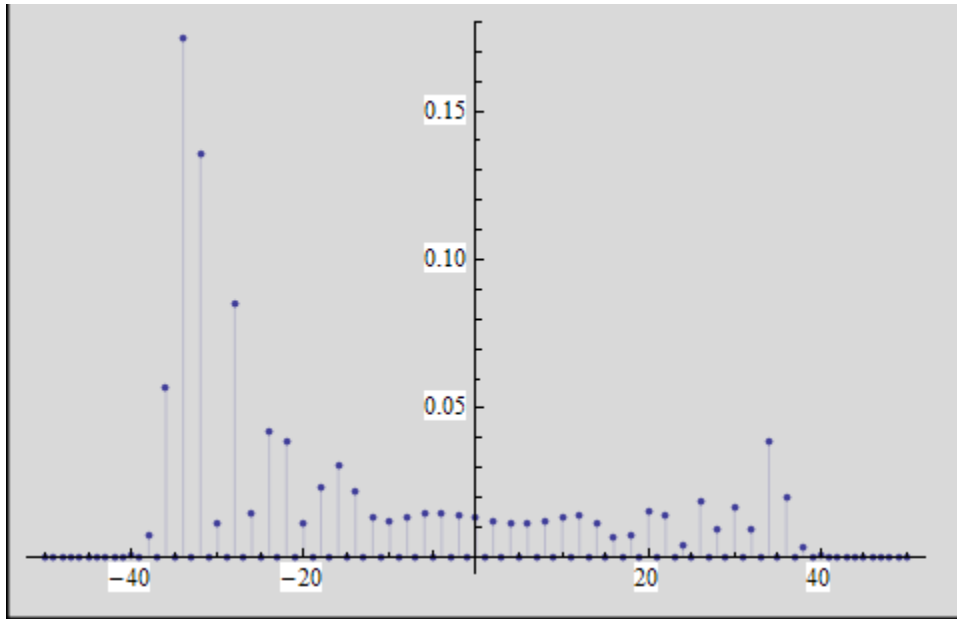


Figura 4.15: Gráfico con moneda  $M = \frac{1}{\sqrt{2}} (|0\rangle \langle 0| - i |0\rangle \langle 1| - i |1\rangle \langle 0| + |1\rangle \langle 1|)$

Como se puede observar generamos el mismo tipo de gráficos que en los diferentes artículos (papers), e incluso se pueden generar las gráficas desbalanceadas y la balanceada.

Este mismo operador con caminante en superposición nos genera un gráfico muy similar:

La ventaja del operador Hadamard es que éste actúa como compuerta también, y mi operador  $M$  tendríamos que diseñarle la compuerta correspondiente para implementación física, para fines de desarrollo matemático y simulación todo operador que cumple con las propiedades de Hadamard es candidato a ser moneda es decir siempre que sea unitario [ver A.3.5 y A.4.3]

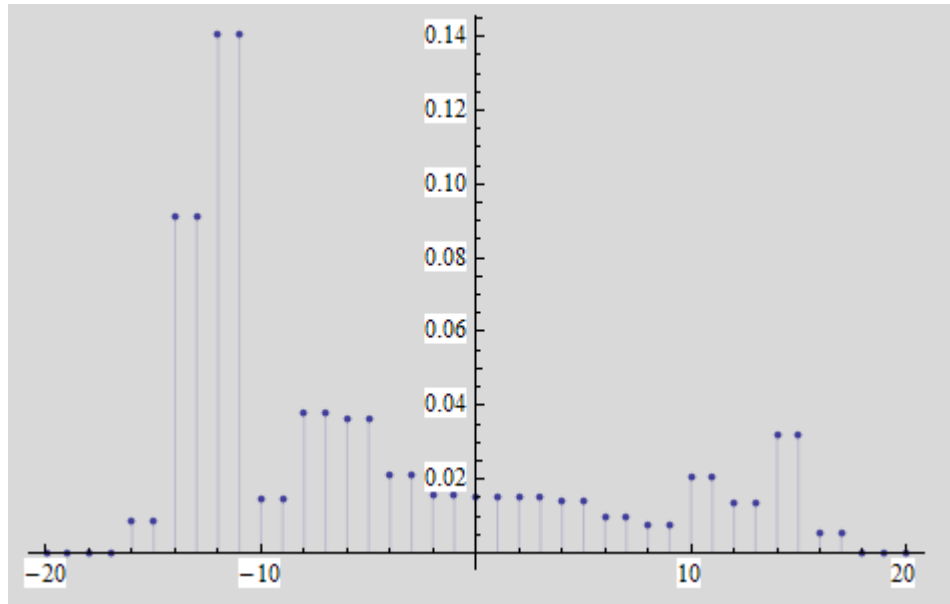


Figura 4.16: El caminante esta en superposición y la moneda es M

## 4.5. Congreso Nacional de Física

Con base en lo ya explicado, en el congreso nacional de física, se presentó un análisis comparativo entre las caminatas clásicas y las cuánticas, dicho artículo lo resumo de la siguiente manera:

1. El objetivo era describir el uso de las caminatas cuánticas en el diseño de algoritmos cuánticos.

2. Mostrar algunos resultados mediante la aplicación del simulador de caminatas cuánticas de Mathematica.

3. La aplicación de las dos operaciones cuánticas (la del operador Hadamard y el operador de traslación condicional) es equivalente a un paso algorítmico.

4. Las caminatas cuánticas discretas tienen una varianza que crece proporcionalmente al cuadrado del número de pasos, i. e.  $\sigma_q^2(n) = \mathcal{O}(n)$

5. La forma de la distribución de probabilidad generada con una caminata cuántica depende del estado inicial. *Una vez establecido el estado de partida se aplica un operador de Hadamard y un operador de traslación condicional. Al cabo de varias iteraciones del proceso, se obtienen distribuciones que no aproximan a una Gaussiana y que pueden ser incluso no simétricas para algunas condiciones iniciales. Esta propiedad podría ser muy útil en un algoritmo de búsqueda.* Este hecho es importante pues el estado inicial del caminante y la moneda puede ser utilizado como un parámetro computacional. De hecho, la interacción de la moneda con el medio ambiente puede generar la distribución top-hat, una gráfica cuasi uniforme, muy agradable a la vista de un científico computacional.

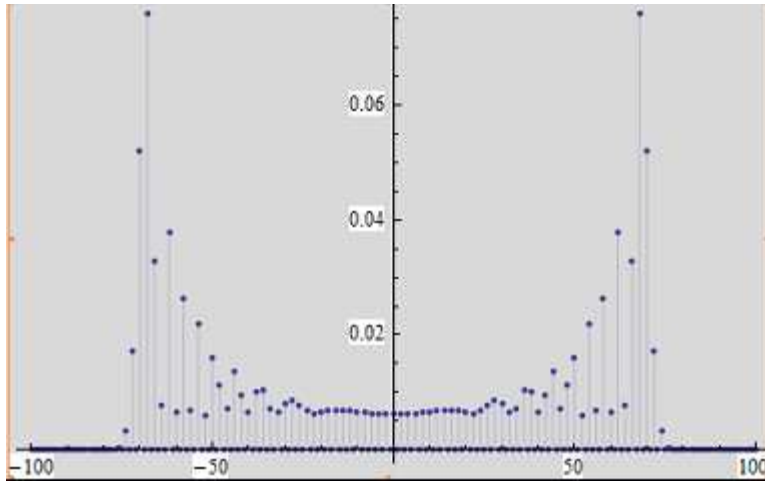


Figura 4.17: Distribución uniforme de una caminata cuántica

Como se muestra en la figura 5.15

## 4.6. Conclusiones

Las podemos resumir en:

1. Los argumentos que discutimos indican que la computación cuántica presenta ventajas frente a la computación clásica, debido a las propiedades cuánticas de superposición, paralelismo y entrelazamiento.
2. Las distribuciones de probabilidad de un caminante cuántico se expanden de forma más rápida, con una distribución de las probabilidades, generando una curva agradable para propósitos computacionales.
3. Debido a que las caminatas cuánticas discretas tienen una varianza que crece proporcionalmente al cuadrado del número de pasos, podemos incrementar la velocidad de ejecución de un algoritmo, aplicando QW.
4. Como la forma de la distribución depende del punto de partida, podemos usar el estado del caminante o el estado de la moneda como parámetro computacional.
5. Mostramos que podemos obtener resultados similares, para diferentes operadores Hermitianos y unitarios que actúen como moneda,.

## 4.7. Trabajos futuros

Sin duda hay una fuente importante en la aplicación de los principios cuánticos a la computación, entre los trabajos a futuro podríamos mencionar:

- Generación de nuevos algoritmos

- Aumentar el número de monedas ( Caminatas cuánticas en altas dimensiones)
- Criptografía cuántica
- Diseño de circuitos cuánticos.

# Capítulo 5

## Apéndice A

### A.1 Notación de Dirac

La notación bra-ket, también conocida como notación de Dirac por su inventor Paul Dirac, es la notación estándar para describir los estados cuánticos en la teoría de la mecánica cuántica. Esta notación nos permitirá representar vectores de la siguiente manera:

El símbolo  $\langle\psi|$  representa un vector en notación de Dirac, que se le conoce como **bra**.

Y el símbolo  $|\psi\rangle$  representa un vector en notación de Dirac conocido como **ket**.

Ambos símbolos aplicados, forman un bracket  $\langle\varphi|\psi\rangle$ , el cual representará el *producto interno* de dos vectores como veremos más adelante.

Y como ya habíamos mencionado los *bra y ket* son representaciones de vectores por lo tanto podemos representarlos por medio de vectores columnas, por ejemplo: Sea  $p = (a, b) \in \mathbb{R}^2$ , entonces  $p$  puede representarse como vector columna de la siguiente manera:

$$p = \begin{pmatrix} a \\ b \end{pmatrix} \tag{5.1}$$

Pero en notación vectorial tendríamos:  $p = ax + by$ , en notación de Dirac  $|p\rangle = a|x\rangle + b|y\rangle$ . Recordemos que en mecánica cuántica  $a, b$  son complejos.

Un bra representa el complejo conjugado transpuesto de un ket, es decir: si el ket  $|\psi\rangle$  está representado como vector columna

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{5.2}$$

con  $\alpha, \beta$  complejos, entonces el bra de  $|\psi\rangle$  es el vector fila

$$\psi^\dagger = ( \alpha^* \quad \beta^* ) \tag{5.3}$$

Donde  $\psi^\dagger$  es el transpuesto conjugado de  $\psi$ , y  $\alpha^*, \beta^*$  son los conjugados de  $\alpha, \beta$  respectivamente.

En mecánica cuántica un estado cuántico puede ser representado por  $\psi = (\alpha, \beta)$  con  $\alpha, \beta$  números complejos, y en notación de Dirac,  $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$ , entonces para un bra tendríamos:

$$\langle\psi| = \alpha^*\langle x| + \beta^*\langle y| \quad (5.4)$$

Como vemos los qubits tratados matemáticamente forman un espacio vectorial, en palabras de [5] *"Mientras que la unidad básica de información en computación cuántica es el qubit, la arena en el que se lleva a cabo la computación cuántica es una abstracción matemática llamada espacio vectorial."* En particular nos interesa el espacio de n-tuplas de números complejos  $\mathbb{C}^n$ , es decir ya con notación de Dirac, tomemos el vector  $a \in \mathbb{C}^n$  entonces

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad (5.5)$$

con los  $a_i$  complejos.

De ésta manera podemos ver las leyes de un espacio vectorial de la siguiente manera:

1. La adición de vectores

$$|a\rangle + |b\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad (5.6)$$

2. La multiplicación por escalar

$$\alpha|a\rangle = \begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ \vdots \\ \alpha a_n \end{pmatrix} \quad (5.7)$$

3. Existe un elemento llamado vector cero tal que se cumple lo siguiente:

$$|a\rangle = |0\rangle + |a\rangle = |a\rangle + |0\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad (5.8)$$

4. La asociatividad de la suma

$$|a\rangle + [|b\rangle + |c\rangle] = [|a\rangle + |b\rangle] + |c\rangle \quad (5.9)$$

5. Para cada  $a \in V$  existe el inverso aditivo de  $a$  tal que:

$$|a\rangle + (-|a\rangle) = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} -a_1 \\ -a_2 \\ \vdots \\ -a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (5.10)$$

6. La conmutatividad de la suma.

$$|a\rangle + |b\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix} = \begin{pmatrix} b_1 + a_1 \\ b_2 + a_2 \\ \vdots \\ b_n + a_n \end{pmatrix} = |b\rangle + |a\rangle \quad (5.11)$$

Sabemos que hay más propiedades pero por el momento son las que nos servirán para el desarrollo del tema.

De manera general un qubit puede ser representado como un vector unitario en un espacio de Hilbert de dos dimensiones  $|\psi\rangle \in \mathcal{H}^2$ .

$$|\psi\rangle = \alpha|p\rangle + \beta|q\rangle \quad (5.12)$$

Donde  $\alpha$  y  $\beta \in \mathbb{C}$ ,  $|\alpha|^2 + |\beta|^2 = 1$ , y  $\{|p\rangle, |q\rangle\}$  es una base arbitraria que genera  $\mathcal{H}^2$  aunque generalmente se trata de escoger la base más simple, en éste caso elegimos  $\{|0\rangle, |1\rangle\}$  la cual llamaremos **base computacional** la cual forma una base ortonormal para  $\mathcal{H}^2$ .

## A.2 Base e independencia Lineal

Sea  $\alpha_1, \dots, \alpha_n$  un conjunto de números complejos y  $|v_1\rangle, \dots, |v_n\rangle$  un conjunto de vectores, definimos una combinación lineal de éstos vectores por:  $\alpha_1|v_1\rangle + \dots + \alpha_n|v_n\rangle = \sum_{i=1}^n \alpha_i|v_i\rangle$ . Si para cualquier vector  $|v\rangle$  de un espacio vectorial  $V$  existe un conjunto de vectores  $\{|v_i\rangle\}$  de tal manera que  $|v\rangle = \sum_{i=1}^n \alpha_i|v_i\rangle$ , entonces a los  $\{|v_i\rangle\}$  se le llama conjunto generador del espacio vectorial  $V$ .

Por ejemplo el espacio vectorial  $\mathbb{C}^2$  posee a los vectores generadores:

$$|v_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}; |v_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (5.13)$$

Es decir para cualquier vector  $|v\rangle$  de  $\mathbb{C}^2$ , éste vector se puede representar como una combinación lineal de los vectores  $|v_1\rangle, |v_2\rangle$  establecidos en la ecuación 5.13,

de la siguiente manera:  $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$ , al conjunto generador de un espacio vectorial se le llama base del espacio, ésta no es única.

Por ejemplo  $\mathbb{C}^2$  puede ser generado por los vectores:

$$|v'_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \quad |v'_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Es decir éstos nuevos vectores son una base de  $\mathbb{C}^2$ . Y si tomamos un vector arbitrario en  $\mathbb{C}^2$ , por ejemplo  $|v\rangle = (a_1, a_2)$ , entonces  $|v\rangle$ , puede representarse como combinación lineal de  $|v'_1\rangle, |v'_2\rangle$  como a continuación mostramos:

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}} |v'_1\rangle + \frac{a_1 - a_2}{\sqrt{2}} |v'_2\rangle$$

Al número de elementos que componen la base de un espacio vectorial se le llama dimensión del espacio.

Decimos que el conjunto de vectores  $|v_i\rangle \neq 0, (\forall i = 1, \dots, n)$  son linealmente independientes si existe un conjunto de números complejos  $\alpha_1 \dots \alpha_n$  con  $\alpha_i \neq 0$  para al menos un  $i$  tal que:

$$\alpha_1 |v_1\rangle + \alpha_2 |v_2\rangle + \dots + \alpha_n |v_n\rangle = 0 \quad (5.14)$$

De lo contrario se dice que son linealmente dependientes, es decir si un vector del conjunto puede representarse como combinación lineal de los otros, éstos son linealmente dependientes.

### A.3 Operadores lineales y matrices

Un operador es una regla matemática que se aplica a una función para obtener otra función, por ejemplo el operador de la derivada, aplicado a una función la transforma en otra función. En especial extendemos éste concepto a los espacios vectoriales así que un operador transformará un vector en otro vector, en particular a un ket en otro ket, un bra en otro bra.

Denotemos a los operadores por  $\hat{A}$  o simplemente por  $A$  aunque haciendo la aclaración que es un operador.

Podemos aplicar el operador a un ket o a un bra de la siguiente manera:  $\hat{A}|\psi\rangle$  y por  $\langle\psi|\hat{A}$  respectivamente.

Así  $\hat{A}|\psi\rangle = |\phi\rangle$  y  $\langle\psi|\hat{A} = \langle\phi|$ , es decir un operador manda un ket a otro ket y un bra a otro bra.

Sean  $V$  y  $W$  espacios vectoriales, definimos el operador  $\hat{A}$  como la función  $\hat{A}: V \rightarrow W$  decimos que  $\hat{A}$  es un operador lineal si cumple las dos propiedades siguientes:

$$\hat{A}(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha(\hat{A}|\psi_1\rangle) + \beta(\hat{A}|\psi_2\rangle) \quad (5.15)$$



$$\hat{A}\left(\sum_{i=1}^n \alpha_i |u_i\rangle\right) = \sum_{i=1}^n \alpha_i (\hat{A} |u_i\rangle) \quad (5.16)$$

### A.3.1 Observables

En la teoría cuántica, las variables dinámicas como la posición, momentum, momentum angular y la energía son llamados observables. Esto se debe a que los observables son fenómenos que se pueden medir con el fin de caracterizar los estados cuánticos de las partículas.

Resulta que un importante postulado de la teoría cuántica nos dice “*que existe un operador que corresponde a cada observable físico*”.

### A.3.2 Operador identidad y el operador cero

Dos importantes operadores que necesitamos considerar son: *El operador lineal identidad* que se define como  $I |v\rangle = |v\rangle$ . Una representación importante del operador lineal identidad es:

$$I = \sum_{i=1}^n |v_i\rangle\langle v_i| \quad (5.17)$$

El otro es el *operador lineal cero* el cual se denota como 0, y es el que mapea cualquier vector al vector cero;  $0 |v\rangle = 0$ .

### A.3.3 Composición de operadores

Podemos definir la composición entre dos operadores de la siguiente manera: Sean  $V, W$  y  $X$  espacios vectoriales y  $\hat{A} : V \rightarrow X$  y  $\hat{B} : W \rightarrow X$  los operadores lineales definidos sobre los espacios vectoriales dados, definimos la composición como:

$$(\hat{B}\hat{A})|v\rangle \equiv \hat{B}(\hat{A}(|v\rangle)) \quad (5.18)$$

aquí entendemos que  $\hat{B}\hat{A}$  denota la composición de  $B$  con  $A$ .

Una manera *muy práctica* de usar los operadores lineales es a través de su *representación matricial*. De hecho la representación matricial y el uso de los operadores lineales son equivalentes. Para ver dicha conexión, es necesario entender que una matriz  $A$  de tamaño  $m \times n$  con entradas  $A_{ij}$ , actúa como operador lineal enviando vectores de un espacio vectorial  $\mathbb{C}^n$  al espacio vectorial  $\mathbb{C}^m$ .

### A.3.4 Operadores de Pauli

Un conjunto de operadores que resulta de fundamental importancia en computación e información cuántica son los cuatro operadores denominados *Operadores de Pauli*. Desafortunadamente existen diferentes notaciones para estos

operadores, pero para el fin del presente trabajo usaremos  $I, X, Y, Z$ , a continuación mostramos cómo se definen y su representación matricial:

1. *Operador identidad, denotado por  $\sigma_0$ , ó  $I$ :*

$$\left. \begin{aligned} \sigma_0|0\rangle &= |0\rangle, \sigma_0|1\rangle = |1\rangle \\ \sigma_0 &= I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \right\} \quad (5.19)$$

2. *Operador 1, denotado por  $\sigma_x$ , ó  $\sigma_1$ , ó  $X$ ; por la manera en que está definido éste operador se le indentifica como el operador NOT*

$$\left. \begin{aligned} \sigma_1|0\rangle &= |1\rangle, \sigma_1|1\rangle = |0\rangle \\ \sigma_x &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{aligned} \right\} \quad (5.20)$$

3. *Operador 2, denotado por  $\sigma_y$ , ó  $\sigma_2$ , ó  $Y$*

$$\left. \begin{aligned} \sigma_2|0\rangle &= i|1\rangle, \sigma_2|1\rangle = -i|0\rangle \\ \sigma_y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \end{aligned} \right\} \quad (5.21)$$

4. *Operador 3, denotado por  $\sigma_z$ , ó  $\sigma_3$ , ó  $Z$*

$$\left. \begin{aligned} \sigma_3|0\rangle &= |0\rangle, \sigma_3|1\rangle = |-1\rangle \\ \sigma_z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned} \right\} \quad (5.22)$$

### A.3.5 Operador Hadamard

Otro de los operadores muy utilizados en; compuertas y caminatas cuánticas, es el operador hadamard  $\hat{H}$ , cuya representación matricial y representación en producto externo es:

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

$$\hat{H} = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

## A.4 Representación matricial de los operadores

Ya establecimos que un *ket* puede ser representado como vector columna, de la misma manera un operador se podrá representar matricialmente, esto significa que la acción de un operador en un vector se reduce a una *multiplicación de matrices*, ayudándonos a que nuestros cálculos sean más sencillos.

En un espacio vectorial de n-dimensiones, los operadores son representados por matrices de tamaño nxn. Si conocemos la acción de un operador  $\hat{A}$  sobre un conjunto  $|v_i\rangle$ ; entonces podemos encontrar los elementos de la matriz que representa al operador  $\hat{A}$ , mediante la siguiente relación:

$$A = IAI = \left( \sum_j |v_j\rangle\langle v_j| \right) A \left( \sum_i |v_i\rangle\langle v_i| \right) = \sum_{ij} \langle v_i|A|v_j\rangle |v_i\rangle\langle v_j| \quad (5.23)$$

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

$$A = \begin{pmatrix} \langle v_1|A|v_1\rangle & \langle v_1|A|v_2\rangle & \cdots & \langle v_1|A|v_n\rangle \\ \langle v_2|A|v_1\rangle & \langle v_2|A|v_2\rangle & & \vdots \\ \vdots & \vdots & \ddots & \\ \langle v_n|A|v_1\rangle & \cdots & & \langle v_n|A|v_n\rangle \end{pmatrix} \quad (5.24)$$

### A.4.1 Producto exterior

Examinemos el producto externo mediante matrices, para ello tomemos los siguientes qubits, en forma de vectores columnas:

$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$  y  $|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$  el producto exterior ( el cual es un operador) es denotado por  $|\psi\rangle\langle\phi|$  y recordemos que  $\langle\phi| = (|\phi\rangle)^\dagger$  entonces tenemos lo siguiente:

$$|\psi\rangle\langle\phi| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c^* & d^* \end{pmatrix} = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix} \quad (5.25)$$

### A.4.2 Matrices de Operadores en dos dimensiones

A nosotros nos interesa los espacios de Hilbert en dos dimensiones, ya que es en ellos donde viven los qubits, para esos operadores que representan qubits necesitamos matrices de 2x2:

$$\hat{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (5.26)$$

Para escribir o encontrar la matriz que representa un operador en la base computacional aplicamos 5.24 de la siguiente manera:

$$\hat{A} = \begin{pmatrix} \langle 0|\hat{A}|0\rangle & \langle 0|\hat{A}|1\rangle \\ \langle 1|\hat{A}|0\rangle & \langle 1|\hat{A}|1\rangle \end{pmatrix} \quad (5.27)$$

Aplicando 5.27 podemos encontrar las expresiones de las matrices de los operadores de Pauli como aparecen en 5.19, 5.20, 5.21 y 5.22.

### A.4.3 Operadores Hermitianos, Unitarios y Normal

Dos tipos especiales de operadores que juegan un rol fundamental en la teoría cuántica y aquí en computación cuántica son, el operador Hermitiano y los operadores unitarios.

#### A.4.3.1 El operador Hermitiano adjunto

El operador Hermitiano adjunto de un operador  $\hat{A}$  es denotado por  $\hat{A}^\dagger$  y se define de la siguiente manera:

$$\langle a|\hat{A}^\dagger|b\rangle = \langle b|\hat{A}|a\rangle^* \quad (5.28)$$

El cálculo del Hermitiano adjunto de cualquier expresión, tomamos los conjugados de las constantes, y cambiamos los bra por ket y los ket por bra, y al operador por su adjunto. A continuación enlisto algunas de las propiedades del hermitiano adjunto:

$$\left(\alpha\hat{A}\right)^\dagger = \alpha^*\hat{A}^\dagger \quad (5.29)$$

$$\left(|\psi\rangle\right)^\dagger = \langle\psi| \quad (5.30)$$

$$\left(\langle\psi|\right)^\dagger = |\psi\rangle \quad (5.31)$$

$$\left(\hat{A}\hat{B}\right)^\dagger = \hat{B}^\dagger\hat{A}^\dagger \quad (5.32)$$

$$\left(\hat{A}|\psi\rangle\right)^\dagger = \langle\psi|\hat{A}^\dagger \quad (5.33)$$

$$\left(\hat{A}\hat{B}|\psi\rangle\right)^\dagger = \langle\psi|\hat{B}^\dagger\hat{A}^\dagger \quad (5.34)$$

$$\left(\hat{A} + \hat{B} + \hat{C}\right)^\dagger = \hat{A}^\dagger + \hat{B}^\dagger + \hat{C}^\dagger \quad (5.35)$$

De ésta manera si un operador se escribe en la notación de producto externo, usamos 5.30, 5.31 y 5.32 para obtener:

$$\hat{A}^\dagger = |\psi\rangle\langle\phi| \quad (5.36)$$

#### A.4.3.2 Operador Hermitiano

Un operador se dice que es Hermitiano si:

$$\hat{A} = \hat{A}^\dagger \quad (5.37)$$

#### A.4.3.3 Operador Unitario

El inverso de un operador es denotado por  $A^{-1}$ , éste operador satisface  $AA^{-1} = A^{-1}A = I$ , donde  $I$  es el operador identidad. El operador se dice que es unitario si su adjunto es igual a la inversa. Los operadores unitarios son denotados por  $U$ , y por lo tanto tenemos:

$$UU^\dagger = U^\dagger U = I \quad (5.38)$$

Los operadores unitarios son importantes porque ellos describen el tiempo de evolución de un estado cuántico.

Los operadores de Pauli son tanto Hermitianos como Unitarios.

#### A.4.3.4 Operadores Normales

Un operador  $\hat{A}$  se dice que es normal si se cumple:

$$\hat{A}\hat{A}^\dagger = \hat{A}^\dagger\hat{A} \quad (5.39)$$

### A.4.3.5 Producto interno

Para calcular la longitud de un vector, aún si es en un sentido abstracto, necesitamos definir una manera de calcular el *producto interno*. Este es una generalización del *producto punto* usado con espacios vectoriales Euclidianos. Pero la diferencia estriba en que el producto punto toma dos vectores y los mapea a un número real y el producto interno los mapea a un número complejo.

La notación estándar en mecánica cuántica para el producto interno es  $\langle u | w \rangle$  como ya habíamos mencionado en 2.1.1 cuando definimos a los vectores *bra* y *ket*.

Si el producto interno entre dos vectores es cero es decir  $\langle u | v \rangle = 0$  decimos que  $|u\rangle$  y  $|v\rangle$  son ortogonales uno respecto del otro.

Como el producto interno es un complejo, podemos tomar su conjugado, éste cumple la siguiente regla:

$$\langle u | v \rangle^* = \langle v | u \rangle \quad (5.40)$$

También podemos usar el producto interno para definir la norma, de la siguiente manera:

$$\|u\| = \sqrt{\langle u | u \rangle} \quad (5.41)$$

Notemos que a norma es un número real, y así podemos definir una longitud, de ésta manera para cualquier vector  $|u\rangle$  tenemos:

$$\langle u | u \rangle \geq 0 \quad (5.42)$$

La igualdad se da si y solo si  $|u\rangle = 0$ .

Para calcular el producto interno entre dos vectores, necesitamos calcular la conjugada Hermitiano de un vector:

$$(|u\rangle)^\dagger = \langle u| \quad (5.43)$$

En física cuántica el símbolo  $\langle v|$  es llamado el *vector dual o bra correspondiente a  $|v\rangle$* . Esto lo que significa que si un ket es un vector columna, el vector dual o bra es un vector renglón cuyos elementos son los conjugados complejos de los elementos del vector columna. En otras palabras, cuando trabajamos con vectores columnas, el Hermitiano conjugado es calculado en dos pasos:

1. Escribimos las componentes del vector como un renglón de números.
2. Tomamos los complejos conjugados de cada elemento y los arreglamos a ellos en un vector renglón.

Es decir, lo que la ecuación 5.19 nos da entender es:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}^\dagger = ( a_1^* \quad a_2^* \quad \dots \quad a_n^* ) \quad (5.44)$$

## NOTA

Los debates de la mecánica cuántica a menudo se refieren al *espacio de Hilbert*. En los espacios vectoriales complejos de dimensión finita que surgen en la computación cuántica e información cuántica, *un espacio de Hilbert es un espacio con producto interno*. A partir de ahora utilizaremos los dos términos indistintamente, prefiriendo el término *espacio de Hilbert*. Por los espacios de Hilbert de dimensión infinita no debemos preocuparnos por el momento, debido a que el cómputo cuántico se lleva a cabo en espacios de Hilbert de dimensión dos.

### A.4.3.6 Ortonormalidad

Cuando la norma de un vector es uno, decimos que está normalizado. Esto es:

$$\langle u | u \rangle = 1 \quad (5.45)$$

Si un vector no está normalizado, podemos generar un vector normalizado a través de la norma, de la siguiente manera:

$$|\tilde{v}\rangle = \frac{|v\rangle}{\|v\|} \quad (5.46)$$

Donde  $|\tilde{v}\rangle$  representa el vector normalizado.

Si cada elemento de un conjunto de vectores es normalizado y los elementos son ortogonales entre sí, decimos que el conjunto es *ortonormal*.

### A.4.3.7 Eigenvectores y eigenvalores

Un vector es denominado un eigenvector de un operador  $\hat{A}$  si la siguiente ecuación es satisfecha:

$$\hat{A} |\psi\rangle = \lambda |\psi\rangle \quad (5.47)$$

donde  $\lambda$  es un número complejo.  $\lambda$  es llamado el eigenvalor de del operador  $\hat{A}$ .

Un problema común en mecánica cuántica es el siguiente: *Dado un operador, encontrar los eigenvalores y eigenvectores.* El primer paso en éste proceso es encontrar los eigenvalores usando lo que conocemos como ecuación característica.

$$\det |\hat{A} - \lambda I| = 0 \quad (5.48)$$

#### A.4.3.8 Traza de un operador

Si un operador esta en su representación matricial, la traza del operador es la suma de los elementos de la diagonal.

Ejemplos:

$$\hat{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ entonces la traza de } \hat{A} \text{ es } Tr(\hat{A}) = a + d$$

$$\hat{A} = \begin{pmatrix} a & b & c \\ d & e & i \\ f & g & h \end{pmatrix}, \text{ entonces la traza de } \hat{A} \text{ es } Tr(\hat{A}) = a + e + h$$

Si un operador se escribe como un producto externo, tomamos la traza mediante la suma de los productos internos con los vectores base.

$$Tr(\hat{A}) = \sum_{i=1}^n \langle u_i | \hat{A} | u_i \rangle \quad (5.49)$$

### A.5 Producto Tensorial

En mecánica cuántica no siempre trabajaremos con partículas individuales aisladas. En muchos casos, alguno de los cuales veremos en el contexto del procesamiento de la información cuántica, para lo cual es necesario trabajar con estados de multipartículas. Matemáticamente, es necesario construir espacios de Hilbert más grandes, compuestos de espacios de Hilbert más pequeños, los cuales están asociados a sistemas de partículas individuales. La maquinaria que se requiere para hacer esto nos conduce al nombre de Kronecker o **producto tensorial**. Consideremos el caso de dos partículas.

Supongamos que  $H_1$  y  $H_2$  son dos espacios de Hilbert de dimensión  $N_1$  y  $N_2$  respectivamente. Podemos poner estos dos espacios de Hilbert juntos para construir un espacio de Hilbert más grande, denotemos a dicho espacio por  $H$  y usemos el producto tensorial el cual denotaremos por  $\otimes$ .

De ésta manera tenemos:

$$H = H_1 \otimes H_2 \quad (5.50)$$



La dimensión del espacio más grande, es el producto de las dimensiones de  $H_1$  y  $H_2$ , es decir, supongamos que  $\dim(H_1) = N_1$  y que  $\dim(H_2) = N_2$ , entonces;

$$\dim(H) = N_1 N_2$$

Sean  $|\phi\rangle \in H_1$  y  $|\chi\rangle \in H_2$  dos vectores pertenecientes a los espacios vectoriales que se usan para formar el espacio vectorial  $H$ , podemos mediante estos vectores formar un vector  $|\psi\rangle \in H$  de la siguiente manera:

$$|\psi\rangle = |\phi\rangle \otimes |\chi\rangle \quad (5.51)$$

El producto tensorial de dos vectores es lineal, es decir;

$$|\phi\rangle \otimes [|\chi_1\rangle + |\chi_2\rangle] = |\phi\rangle \otimes |\chi_1\rangle + |\phi\rangle \otimes |\chi_2\rangle \quad (5.52)$$

$$[|\phi_1\rangle + |\phi_2\rangle] \otimes |\chi\rangle = |\phi_1\rangle \otimes |\chi\rangle + |\phi_2\rangle \otimes |\chi\rangle \quad (5.53)$$

Además es lineal con respecto al producto de escalares:

$$|\phi\rangle \otimes [\alpha |\chi\rangle] = \alpha [|\phi\rangle \otimes |\chi\rangle] \quad (5.54)$$

Para formar la base del espacio de Hilbert más grande  $H$ , simplemente formamos el producto tensorial de los vectores base de los espacios  $H_1$  y  $H_2$ . Para lo cual denotamos por  $|u_i\rangle$  base de  $H_1$ , y  $|v_i\rangle$  base de  $H_2$ , entonces podemos construir  $|w_i\rangle$  base de  $H = H_1 \otimes H_2$  usando:

$$|w_i\rangle = |u_i\rangle \otimes |v_i\rangle \quad (5.55)$$

### A.5.1 Cálculo de producto interno mediante producto tensorial

Supongamos que  $|\psi_1\rangle \in H_1$  y  $|\psi_2\rangle \in H_2$ , además  $|\psi_1\rangle = |\phi_1\rangle \otimes |\chi_1\rangle$  y  $|\psi_2\rangle = |\phi_2\rangle \otimes |\chi_2\rangle$ , entonces definimos el producto interno de la siguiente manera:

$$\langle \psi_1 | \psi_2 \rangle = (\langle \phi_1 | \otimes \langle \chi_1 |) (|\phi_2\rangle \otimes |\chi_2\rangle) = \langle \phi_1 | \phi_2 \rangle \langle \chi_1 | \chi_2 \rangle \quad (5.56)$$

### A.5.2 Producto tensorial mediante vectores

Cuando los vectores de estado son representados mediante vectores columnas, el producto tensorial se calcula de la siguiente manera:

Sean  $|\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$  y  $|\chi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ , entonces definimos el producto tensorial de la siguiente forma:

$$|\phi\rangle \otimes |\chi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \quad (5.57)$$

### A.5.3 Producto tensorial y operadores

Sean  $|\phi\rangle \in H_1$  y  $|\chi\rangle \in H_2$  vectores pertenecientes a los espacios vectoriales que permiten construir  $H$ . Ahora tomemos a  $A$  un operador que actúa sobre  $|\phi\rangle \in H_1$  y  $B$  un operador que actúa sobre  $|\chi\rangle \in H_2$ , podemos crear un operador  $A \otimes B$  que actúe en los vectores  $|\psi\rangle \in H$  como sigue:

$$(A \otimes B) |\psi\rangle = (A \otimes B)(|\phi\rangle \otimes |\chi\rangle) = (A|\phi\rangle) \otimes (B|\chi\rangle) \quad (5.58)$$

El producto tensorial de dos operadores  $A \otimes B$ , satisface las siguientes propiedades:

1. Si  $A$  y  $B$  son Hermitianos, entonces  $A \otimes B$  es Hermitiano
2. Si  $A$  y  $B$  son operadores de proyección, entonces  $A \otimes B$  es un operador de proyección
3. Si  $A$  y  $B$  son unitarios, entonces  $A \otimes B$  es unitario
4. Si  $A$  y  $B$  son positivos, entonces  $A \otimes B$  es positivo

### A.5.4 Producto tensorial de matrices

Vamos a mantener las cosas simples y centrarse en la consideración de productos tensoriales de los operadores en los espacios de Hilbert en dos dimensiones para producir un operador que actúa en un espacio de Hilbert de cuatro dimensiones.

Sean  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$  y  $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ , las representaciones matriciales de los operadores  $A$  y  $B$  respectivamente, entonces el producto tensorial  $A \otimes B$  está dado por:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix} \quad (5.59)$$

## Capítulo 6

# Apéndice B

### Compuertas Cuánticas

Las computadoras cuánticas hacen una importante parte de su magia a través de *operaciones reversibles*, las cuales transforman el estado inicial de un qubit en un estado final usando únicamente procesos cuya acción puede ser invertida, de hecho la única parte irreversible en cómputo cuántico, es la medición, la cual es la única manera o forma de extraer información de los qubits, después de haber adquirido su forma final. Estas operaciones reversibles serán llevadas a cabo por las compuertas cuánticas, cuya acción es comprada con las compuertas clásicas, es decir nos ayudan a procesar la información, recordemos que en cómputo clásico utilizamos las compuertas (not, and, or, nand, etc) para procesar la información. Veamos ,entonces las características de las compuertas cuánticas.

#### B.1 Compuerta de un Qubit

En una computadora cuántica, la información también es procesada usando compuertas, pero en este caso las compuertas son *operaciones unitarias*.

Como las compuertas cuánticas son justamente los *operadores unitarios*, hay que tener en cuenta que hablar de compuertas cuánticas o de operadores unitarios será lo mismo en este contexto.

Recordemos que un operador unitario  $U$  es uno donde su adjunto, es igual a la inversa, es decir  $U = U^\dagger$  , además estos operadores cuánticos se pueden representar por matrices. Entonces una compuerta cuántica con  $n$  entradas y salidas puede ser representado por matrices de grado  $2^n$ . Para un solo qubit, se requiere de una matriz de grado  $2^1 = 2$ , es decir una compuerta cuántica actuando en un sólo qubit será una matriz unitaria de  $2 \times 2$ .

De manera análoga que en las compuertas lógicas clásicas, comencemos por examinar la compuerta más simple posible, la compuerta cuántica *NOT* . Ya se ha encontrado la compuerta cuántica NOT, de hecho se ha revisado exhaustivamente las compuertas de un sólo qubit.

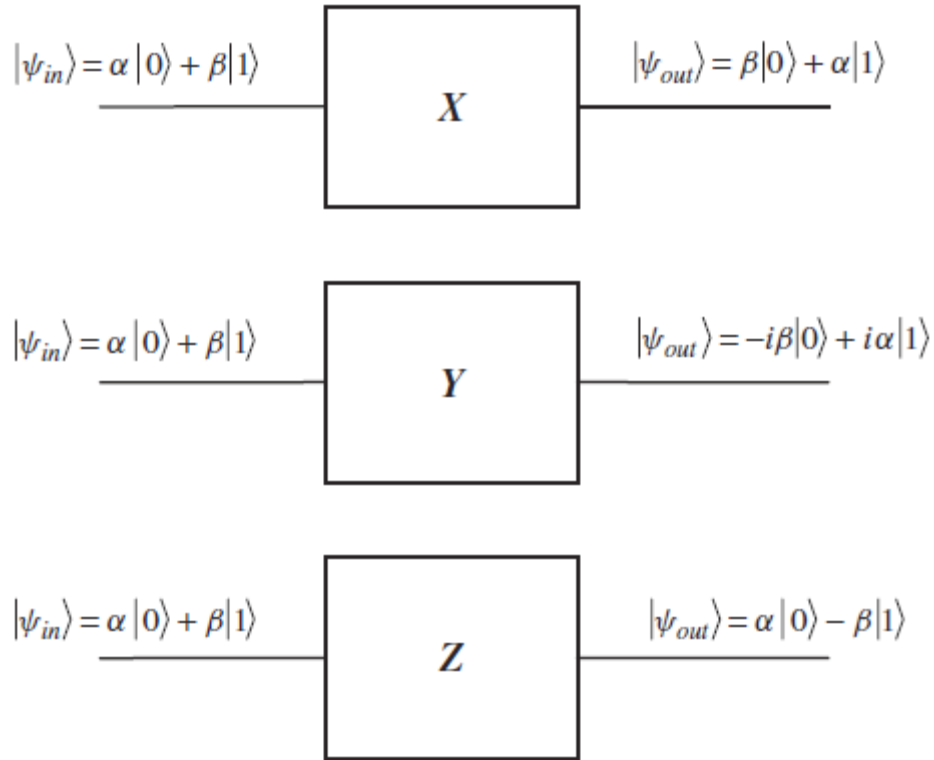


Figura 6.1: Representaciones de los diagramas de los circuitos de Pauli y su acción sobre un sólo qubit

La operación se puede llevar a cabo con la matriz de Pauli  $X$ , que bajo este contexto se verá como el operador NOT o compuerta NOT, recordemos que se representa por :

$$X = U_{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (6.1)$$

Podemos representar la acción de una compuerta cuántica dibujando un diagrama del circuito. Cada operador unitario o compuerta es representado por bloques con líneas ( o cables) usados para representar la entrada y la salida, por ejemplo la representación de los operadores de Pauli  $X, Y, y Z$  y su acción sobre un qubit individual como se muestra en la figura

## B.2 Compuerta Hadamard

Una compuerta de gran importancia en el procesamiento cuántico y un paso importante en los algoritmos cuánticos es la denominada compuerta Hadamard,

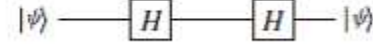


Figura 6.2: Diagrama de Hadamard aplicada dos veces

con la cual se *crea superposición de estados*. Recordemos que la compuerta Hadamard  $H$  actúa sobre la base computacional de estados de la siguiente manera:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (6.2)$$

Dos características singulares de la compuerta Hadamard ocurren cuando, dos compuertas Hadamard actúan en serie o en paralelo como veremos a continuación.

### B.2.1 Compuerta Hadamard en serie

Consideremos la aplicación de la compuerta Hadamard dos veces, primeramente sobre el qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , y posteriormente sobre el resultado de la primera aplicación:

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

Volvamos a aplicar Hadamard sobre este resultado:

$$\begin{aligned} H\left[\left(\frac{\alpha + \beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|1\rangle\right] &= \left(\frac{\alpha + \beta}{\sqrt{2}}\right)H|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)H|1\rangle = \left(\frac{\alpha + \beta}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \\ &\left(\frac{\alpha - \beta}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \\ &= \left(\frac{\alpha + \alpha + \beta - \beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha - \alpha + \beta + \beta}{\sqrt{2}}\right)|1\rangle = \alpha|0\rangle + \beta|1\rangle \end{aligned}$$

Lo que implica que el estado regresa a su estado original, es decir que la compuerta Hadamard presenta la propiedad de reversibilidad, su diagrama se representa en la figura 3.2

### B.2.2 Hadamard en paralelo

Ahora veamos que pasa cuando aplicamos dos compuertas Hadamard en paralelo. Para ello aplicamos Hadamard en paralelo al estado  $|1\rangle|1\rangle$ , ver la figura 3.3

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

Cuando  $n$  compuertas actúan en paralelo sobre  $n$  qubits, a dicha acción se le denomina *Transformada Hadamard*. Podemos simplificar la notación de la transformada Hadamard de la siguiente manera; escribimos  $H^{\otimes n}$ , de esta manera dos compuertas Hadamard en paralelo, lo denotaríamos por  $H^{\otimes 2}$ , para

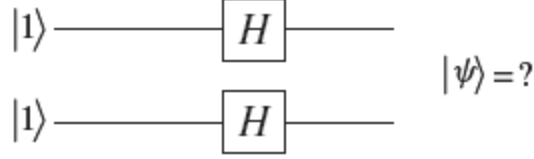


Figura 6.3: Dos compuertas Humarada en paralelo aplicadas al estado  $|1\rangle |1\rangle$

una aplicación sobre un estado  $|0\rangle |0\rangle |0\rangle$ , se denotaría por  $H^{\otimes 3}$ , cuyo efecto matemáticamente es:

$$\begin{aligned} (H \otimes H \otimes H)(|0\rangle |0\rangle |0\rangle) &= (H |0\rangle)(H |0\rangle)(H |0\rangle) = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = \\ &= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \end{aligned}$$

Podemos escribir una suma como  $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$  en forma compacta, de la siguiente manera: Sea  $|x\rangle$  un estado general con  $x \in \{0, 1\}^2$ ; es decir  $|x\rangle$  es cualquiera de los siguientes  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ ; si  $x \in \{0, 1\}^3$ , entonces  $|x\rangle$  es uno de los qubits  $|000\rangle, |001\rangle, |010\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$ ; en resumen tendremos para  $n = 2$ :

$$(H \otimes H)(|0\rangle |0\rangle) = H^{\otimes 2} |0\rangle^{\otimes 2} = \frac{1}{\sqrt{2^2}} \sum_{x \in \{0,1\}^2} |x\rangle$$

En general, la aplicación de  $H^{\otimes n}$  al producto de estado de  $n$  copias de  $|0\rangle$ ,H es:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \tag{6.3}$$

Si pensamos que  $x$  corre sobre los números 00,01,10,11 (es decir 0,1,2,3), entonces podemos escribir en forma compacta de la siguiente manera:

$$(H \otimes H)(|0\rangle |1\rangle) = \frac{1}{2} \sum_{x \in \{0,1\}} (-1)^x |x\rangle$$

Mientras que

$$(H \otimes H)(|1\rangle |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = \frac{1}{2} \sum_{x \in \{0,1\}^2} (-1)^{x_0 \oplus x_1} |x\rangle$$

donde  $x_0 \oplus x_1$  es or-exclusiva de dos qubits, y decimos que  $|x\rangle$  es un qubit de dos estados de la forma  $|x_0 x_1\rangle$ , donde  $x_0, x_1$  son 0 ó 1.

### B.3 Compuertas multiqubits

Ahora hay que avanzar con el caso de compuertas de dos qubits. En ésta sección, la noción de compuerta controlada nos permitirá aplicar un tipo *if – else* en la construcción de una compuerta cuántica. Se tiene que considerar la posibilidad de una compuerta clásica controlada. Donde se incluye un bit de control  $C$ . Si  $C = 0$ , entonces la compuerta no hace nada, pero si  $C = 1$ , entonces la compuerta realiza alguna acción específica. Las compuertas controladas cuánticas( o controlada unitaria) trabaja en forma similar, utilizando un qubit de control para determinar, si o no una acción unitaria especificada es aplicada a un qubit objetivo.

Cuando se trabaja con compuertas de dos qubits, consideramos su acción con respecto a los estados de dos qubits. Estos estados son de la forma  $|a\rangle \otimes |b\rangle$ , los cuales se pueden escribir también por  $|a\rangle |b\rangle$  o bien por  $|ab\rangle$ . De ésta manera si conocemos la acción de un operador sobre un estado  $|a\rangle \otimes |b\rangle$ , entonces podemos encontrar su matriz de representación. La matriz de representación de dos qubits se puede encontrar usando:

$$U \doteq \begin{pmatrix} \langle 00|U|00\rangle & \langle 00|U|01\rangle & \langle 00|U|10\rangle & \langle 00|U|11\rangle \\ \langle 01|U|00\rangle & \langle 01|U|01\rangle & \langle 01|U|10\rangle & \langle 01|U|11\rangle \\ \langle 10|U|00\rangle & \langle 10|U|01\rangle & \langle 10|U|10\rangle & \langle 10|U|11\rangle \\ \langle 11|U|00\rangle & \langle 11|U|01\rangle & \langle 11|U|10\rangle & \langle 11|U|11\rangle \end{pmatrix}$$

#### B.3.1 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:

$$|a, b\rangle \rightarrow |a, b \oplus a\rangle \quad (6.4)$$

Si el qubit de control es  $|0\rangle$ , entonces nada pasa al qubit objetivo o blanco. Si el qubit de control es  $|1\rangle$ , entonces la matriz NOT o la matriz X es aplicada al qubit objetivo. Las posibles estados de entrada de la compuerta CNOT son;  $|00\rangle |01\rangle |10\rangle |11\rangle$ , y la acción de la compuerta CNOT de esos 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 3.4



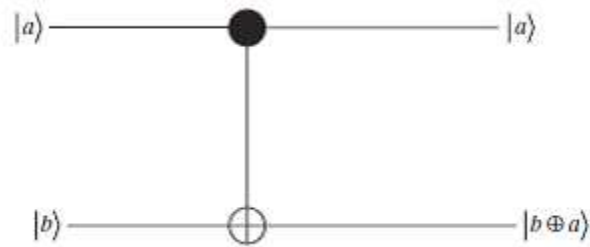


Figura 6.4: Representación del diagrama de un circuito de una compuerta NOT controlada o CNOT

Para escribir la representación matricial de la compuerta CNOT, tenemos que hacerlo con respecto a los estados  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  and  $|11\rangle$ . La cual es una matriz  $4 \times 4$ . La representación matricial de esta compuerta esta dada por:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (6.5)$$

Si usamos notación de Dirac, la representación por el producto externo de la CNOT es :

$$CNOT = |00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10|$$

### B.3.2 TOFFOLI

La compuerta Toffoli tiene tres qubits de entrada y tres de salida, como se observa en la figura 3.5. Dos de los qubits son de control, los cuales no son afectados por la acción de la compuerta Toffoli. El tercer qubit es el qubit objetivo que es cambiado si ambos qubits de control son 1, de otra manera se queda solo. Notemos que si aplicamos la compuerta Toffoli dos veces al conjunto de qubits tiene el efecto:  $(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$ , mostrándonos que la compuerta Toffoli es una compuerta reversible, ya que en sí misma tiene una inversa.

Ya hemos observado ciertas propiedades de las compuertas cuánticas, y sus ventajas pero hay una característica fundamental en el desarrollo de los algoritmos cuánticos, que es la que revisaremos a continuación, hablaremos es la de *paralelismo cuántico*.

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

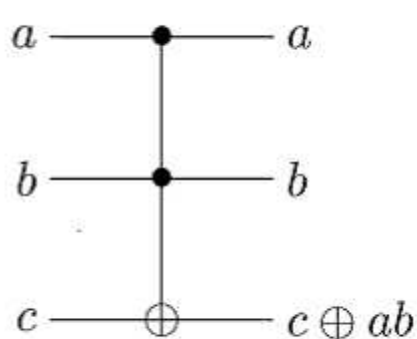


Figura 6.5: Diagrama y tabla de verdad de compuerta Toffoli

## B.4 Paralelismo cuántico

Heurística-mente, y aun a riesgo de simplificar en exceso, el paralelismo cuántico permite a los ordenadores cuánticos evaluar una función  $f(x)$  para muchos valores diferentes de  $x$  de *forma simultánea*, en un sólo paso algorítmico[5]. Para ello describiremos el trabajo del llamado algoritmo de Deutsch. Así que veamos cómo funciona el paralelismo cuántico.

Comencemos considerando una función muy simple, una que acepte un bit de entrada y obtenga un bit a la salida. Esto es,  $x \in \{0, 1\}$ . Para lo cual hay un número pequeño de funciones que pueden actuar sobre el conjunto  $x \in \{0, 1\}$ .

Por ejemplo tenemos:

1. La función identidad

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

2. La función constante

$$f(x) = 0 \quad f(x) = 1$$

3. Finalmente la función de cambio de bit

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

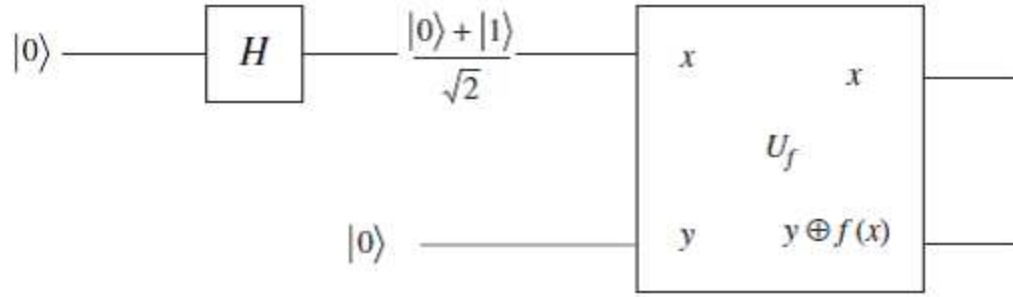


Figura 6.6: Diagrama del circuito para  $U_f |x, y\rangle = |x, y \oplus f(x)\rangle$

Las funciones identidad y de cambio de bit son llamadas balanceadas, porque sus salidas son opuestas para la mitad de las entradas. Así una función con un sólo bit puede llamarse constante o balanceada. 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 denotaremos por  $U_f$  que actúa en dos qubits. Este operador deja el primer qubit sólo y producirá una *XOR* del segundo qubit con la función  $f$  evaluada con el primer qubit como argumento. Esto significa

$$U_f |x, y\rangle = |x, y \oplus f(x)\rangle \quad (6.6)$$

Puesto que  $|x\rangle$  es un qubit, puede estar en un estado de superposición. Específicamente se iniciará con un estado  $|0\rangle$  y se le aplicará una compuerta Hadamard, como se muestra en la figura 3.6:

Algebráicamente éste circuito trabaja de la siguiente manera:

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

Así el circuito de la figura 3.6 ha producido un estado de superposición que tiene información sobre cada valor de  $f(x)$ , **en un sólo paso**.

Si  $f(x)$  es la función identidad, entonces el estado resultante es:

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

Recordemos que  $0 \oplus 0 = 1 \oplus 1 = 0$ ;  $0 \oplus 1 = 1 \oplus 0 = 1$ , por lo que en general la salida de este circuito es:

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

Esto se ve muy elegante, tenemos un estado de superposición con todos los pares de  $x, f(x)$  representados. Pero recordemos como trabaja la medición cuántica. Si medimos el estado  $\sum |x\rangle |f(x)\rangle$  obtenemos uno y sólo un valor de  $x$  y de  $f(x)$ . Después de la medición el sistema está en un estado proporcional a  $|x\rangle |f(x)\rangle$  para ese solo y específico valor de  $x$ . Además, el valor de  $x$  que obtenemos es completamente al azar. Algoritmo de Deutsch toma lo que hemos hecho hasta ahora para aprovechar el hecho de que el sistema está en un estado de superposición  $\sum |x\rangle |f(x)\rangle$  para obtener información acerca de las propiedades globales de la función, si es o no constante  $f(0) = f(1)$  o balanceada  $f(0) \neq f(1)$ . Esto lo hace mediante el cálculo

$$|\psi\rangle_{out} = (H \otimes I) U_f (H \otimes H) |0\rangle |1\rangle$$

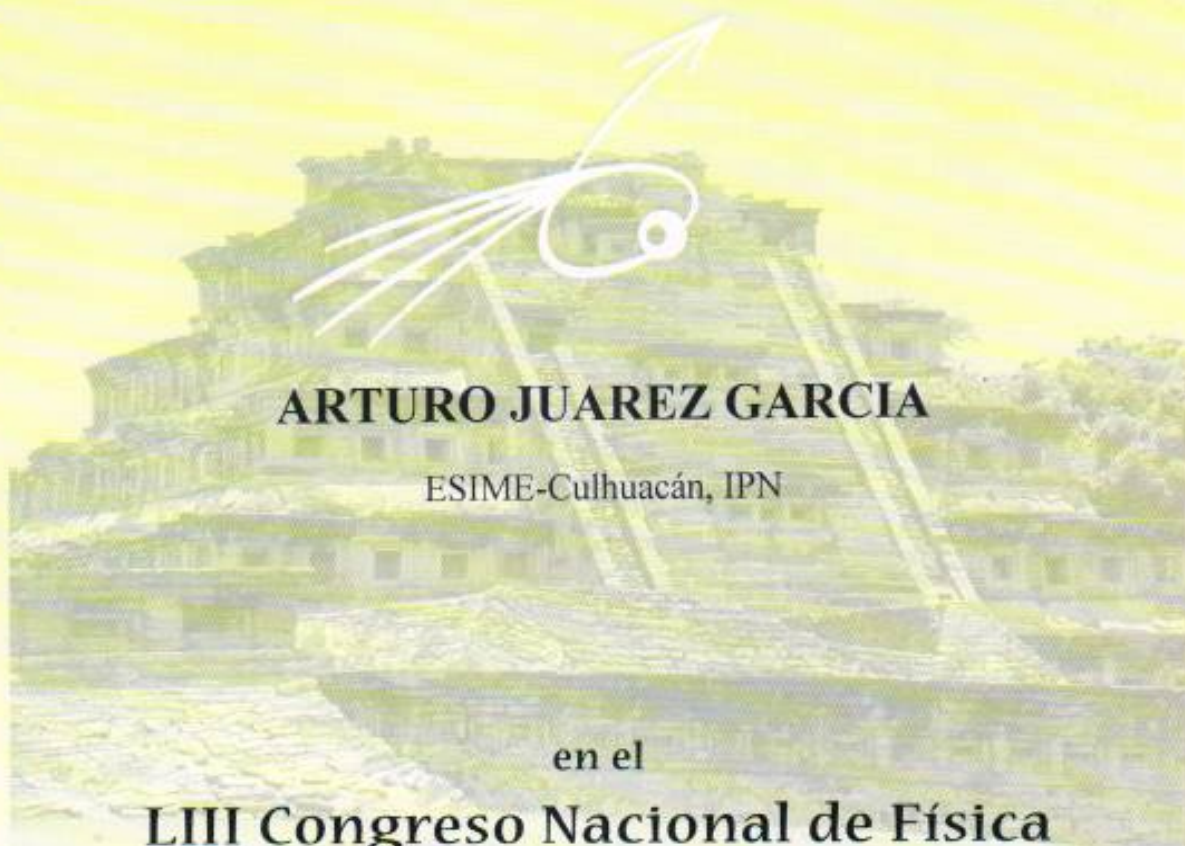
En palabras, el algoritmo de Deutsch es implementado por los siguientes pasos:

1. Aplicamos compuerta Hadamard a la entrada de los estados  $|0\rangle |1\rangle$  para producir un producto de estados en dos superposiciones.
2. Aplicamos  $U_f$  al estado producto
3. Aplicamos compuerta Hadamard al primer qubit dejando al segundo qubit sólo.

A partir de ello explotan las características de la mecánica cuántica, para mejor procesamiento de la información.

# La Sociedad Mexicana de Física

Agradece la asistencia y participación de:



**ARTURO JUAREZ GARCIA**

ESIME-Culhuacán, IPN

en el  
**LIII Congreso Nacional de Física**

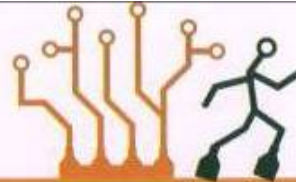
del 25 al 29 de octubre de 2010

World Trade Center y Hotel Galería Plaza, Boca del Río, Veracruz

Dr. Luis Felipe Rodríguez Jorge

Presidente de la SMF

# 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 Cryptography: Simulation

TO

**Arturo Juárez**

Handwritten signature of Dr. Rubén Alejos Palomares in black ink.

**Dr. Rubén Alejos Palomares**  
General Chairman

Handwritten signature of Dr. José Alfredo Sánchez Huitrón in black ink.

**Dr. José Alfredo Sánchez Huitrón**  
Technical Program Chair

Handwritten signature of Dr. Jorge Rodríguez Asomoza in black ink.

**Dr. Jorge Rodríguez Asomoza**  
Head of CEM Department

Cholula, Puebla, México, February 28th to March 2nd, 2011

**UDLAP**  
UNIVERSIDAD DE LAS  
AMÉRICAS PUEBLA

**IEEE**  
SECCION PUEBLA  
©2011 IEEE

**CENGAGE**  
Learning  
El conocimiento no compromete

**PEARSON**

**ProSoft**  
TECNOLOGÍA

# Bibliografía

- [1] Amir D. Aczel, *Entrelazamiento*. Editorial drakontos 2002.
- [2] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Information*. 2000. Cambridge Univ.Press.
- [3] Salvador E. Andraca. *Quantum Walks for computer scientists*. 2008. Morgan&Claypool Publishers series.
- [4] Verónica Arriola. *Computación Cuántica*. 2004. Facultad de ciencias de la UNAM
- [5] David Macmahon. *Quantum Computing explained*. 2008. John Wiley & Sons
- [6] Cohen-Tannoudji. *Quantum Mechanics*. vol1 y vol2.
- [7] B. Lovett Cline. *Los creadores de la nueva física*. Fondo de Cultura Económica
- [8] J. Sánchez Ron. *Historia de la física cuántica*. Editorial Drakontos 2005.
- [9] Richard P. Feynman. *El placer de descubrir*. editorial drakontos 2004.
- [10] Paul Benioff. *Quantum Mechanical Hamiltonian Models of Turing Machines*. Journal of Statistical Physics, FoL 29, No. 3, 1982
- [11] David Deutsch. *Quantum theory, the church-turing principle and the universal quantum computer*. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 400(1818):97–117, 1985.
- [12] D. R. Simon. *On the power of quantum computation*. Society for Industrial and Applied Mathematics Juournal on Computing 26, 5, 1474-1483
- [13] Andrew Yao. *Quantum circuit complexity*. In Proceedings of the 34th Annual Symposium on Foundations of Computer Science, pages 352–361, Los Alamitos, CA, 1993. Institute of Electrical and Electronic Engineers Computer Society Press.



- [14] David Deutsch. *Quantum theory, the church-turing principle and the universal quantum computer*. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 400(1818):97–117, 1985.
- [15] Charles H. Bennet. *Logical reversibility of computation*. IBM Journal of Research and Development, 17(525532), 1973
- [16] David Deutsch. *Quantum computational networks*. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 425(1868):73–90, 1989.
- [17] A.Y. Kitaev, A. H. Shen. *Classical and quantum computation*. American Mathematical Society, 1999.
- [18] R.P.Feynman. *Simulating physics with computers*. Int.J. Theor.Phys.,Vol.21(6/7), pp.467-488,1982.
- [19] C.M. Grinstead and J.L. Snell. *Introduction to probability*. American Mathematical Society, 1997.
- [20] O. L´opez-Acevedo and T. Gobron. *Quantum walks on cayley graphs*. quant-ph/0503078, 2005.
- [21] C.H. Papadimitriou. *On selecting a satisfying truth assignment*. Proceedings 32nd IEEE Symposium on the Foundations of Computer Science, pages 163 – 169, 1991.
- [22] C.H. Papadimitriou. *Computational Complexity*. Addison Wesley Publishing Co., 1995.
- [23] H. Rantanen. *Analyzing the random-walk algorithm for SAT*. Master’s thesis, Helsinki University of Technology, 2004.
- [24] J. Kempe. *Quantum random walks - an introductory overview*. Contemp. Phys., 44:307, 2003, preprint quant-ph/0303081.
- [25] Y. Aharonov, L. Davidovich, and N. Zagury *"Quantum Random Walks"* Phys. Rev. A 48, 1687 - 1690 (1993)
- [26] V.M.Kendon, *A random walk approach to quantum algorithms*, Phil.Trans.R.S. A 2006
- [27] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, *"Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels"*
- [28] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Computing 26, pp. 1484-1509 (1997).



- [29] *Rapid sampling through quantum computing*. Proceedings of 32th Annual ACM Symposium on Theory of Computing (STOC), 2000, pages 618-626. [quant-ph/9912001](#).
- [30] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. Sherwood, and I. L. Chuang.. *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*. Nature, 414 pp. 883, 2001.
- [31] *Katherine L. Brown 1, William J. Munro 2,3 and Vivien M. Kendon 1* *Entropy* 2010, 12, 2268-2307; [doi:10.3390/e12112268](#).
- [33] *Recent Progress in Quantum Algorithms What quantum algorithms outperform classical computation and how do they do it? Dave Bacon, Wim van Dam* *Communications of the ACM* Vol. 53 No. 2, Pages 84-93 [10.1145/1646353.1646375](#)
- [34] *The QWalk Simulator of Quantum Walks* F.L. Marquezino ; R. Portugal ,LNCC, Laboratório Nacional de Computac̃ao Cientca Av. Getulio Vargas 333, CEP 25651-075, Petropolis, RJ, Brazil
- [35] *Mathematica* Wolfram.org