Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Generación de estados cuánticos para computadoras cuánticas

Tesis presentada al

Posgrado en Física Aplicada

como requisito parcial para la obtención del grado de

Maestro en Ciencias (Física Aplicada)

por

Uriel Leonardo Casco Domínguez

Asesorado por

Dr. Luis Manuel Arévalo Aguilar

Puebla Pue.
Agosto de 2025

Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

Generación de estados cuánticos para computadoras cuánticas

Tesis presentada al

Posgrado en Física Aplicada

como requisito parcial para la obtención del grado de

Maestro en Ciencias (Física Aplicada)

por

Uriel Leonardo Casco Domínguez

Asesorado por

Dr. Luis Manuel Arévalo Aguilar

Puebla Pue.
Agosto de 2025

Título: Generación de estados cuánticos para computadoras cuánticas
Estudiante: Uriel Leonardo Casco Domínguez

COMITÉ

Dra. Marcela Maribel Mendez Otero
Presidente

Dr. Martín Rodolfo Palomino Merino
Secretario

Dr. Eduardo Jonathan Torres Herrera
Vocal

Dra. María del Rosario Pastrana Sánchez
Suplente

Dr. Luis Manuel Arévalo Aguilar
Asesor

Agradecimientos

Este trabajo fue hecho con mucho entusiasmo y dedicación de mi parte, sin embargo, sería egoísta no reconocer el apoyo de quienes me apoyaron en esta etapa de mi vida.

Quiero agradecer a mis padres, las personas más importantes de mi vida y el pilar de esta, José Federico Casco Vásquez (papá Fede) y María Teresa Domínguez Aguayo (la peque), por todo su apoyo, su amor incondicional, por estar siempre al pendiente de mi... Por todo lo que hacen y han hecho por mi, por todo eso y más, gracias, los amo. También agradezco a mis hermanos, Alejandro, Iván y Marco, mis compañeros de vida, que a pesar de cualquier posible diferencia que tengamos o lleguemos a tener, sé que siempre puedo contar con ellos.

De igual forma quiero agradecer al Dr. Luis Manuel Arévalo Aguilar, quien fue de mucho apoyo para la realización de este trabajo, me guió y siempre fue comprensivo conmigo en todo este proceso.

Finalmente, agradezco a todas las personas que estuvieron presentes en esta etapa de mi vida y al Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), hoy conocido como la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI), por el apoyo brindado a través de una beca para la realización de mis estudios de posgrado.

Índice general

Resumen

La computación cuántica ha tomado gran importancia y relevancia en la investigación científica desde el siglo XX, esto gracias a la ventaja computacional que aparenta ofrecer este tipo de máquinas en contraste con su contraparte clásica. Entre las áreas de estudio de la computación cuántica se encuentran la generación de estados cuánticos para su uso en computadoras cuánticas, el diseño e implementación de algoritmos cuánticos, entre otras.

La generación de estados cuánticos, a pesar de ser tomada por muchos autores como una subrutina de los famosos algoritmos cuánticos, a la cual no se le presta demasiada atención, es un área de investigación que hoy en día forma parte de uno de los problemas a solucionar al momento de diseñar algoritmos cuánticos.

En este trabajo de tesis se analizará y realizará el proceso de generación de estados cuánticos mediante el cálculo de los ángulos que generen ciertas rotaciones en los estados para que, de esta manera, se pueda generar un estado cuántico particular con el uso de diversas compuertas lógico-cuánticas. Todo esto mediante el uso de dos algoritmos con los cuales se generarán M estados consecutivos en superposición uniforme para después eliminar los estados de la superposición, haciendo que queden en una superposición cuántica de estados únicamente los estados deseados.

Introducción

La computación cuántica es una consecuencia de la revolución científica que causó la mecánica cuántica, luego de que en los años 80's, uno de los grandes precursores de esta área de estudio de la física y la computación, Richard Feynman, en su artículo *"Simulating Physics with Computers"* [10], propusiera el uso de máquinas que pudieran simular cualquier sistema cuántico y llamara a estas como computadoras cuánticas. A partir de esto la comunidad científica entre el final de la década de los 80's y los comienzos de los 90's formalizaron la forma en la que se describían las computadoras cuánticas [12] y se comenzó a mostrar interés en esta área de estudio que en las últimas décadas ha tomado una gran relevancia debido a la superioridad que demuestra tener sobre su contraparte clásica en el procesamiento de información, la realización de algunas operaciones y a su gran potencial de aplicabilidad. Como en su nombre se indica, la computación cuántica obedece las leyes de la mecánica cuántica y basa su funcionamiento en el aprovechamiento de los fenómenos físicos que estudia esta rama de la física.

La forma en la que una computadora cuántica puede realizar una tarea o procesar información es por medio de una serie de transformaciones unitarias, también conocidas como compuertas lógico-cuánticas, que son aplicadas a uno o varios qubits (estos son la unidad básica de información para las computadoras cuánticas, cuyo estado puede ser representado por medio de la esfera de bloch) de forma continua, modificando el estado de estos hasta obtener el estado deseado; a este proceso se le conoce como algoritmos cuánticos.

Usualmente los algoritmos cuánticos se inician teniendo al conjunto de qubits (o también conocido como *"registro"*) a manipular en el estado $|0\rangle$, sin embargo, en algunos casos se necesita construir un estado particular para llevar a cabo el algoritmo; a este proceso se le conoce como generación de estados cuánticos, el cual es considerado muchas veces en la literatura, e incluso en algunos artículos científicos como una subrutina de los algoritmos cuánticos que no siempre es tratada a profundidad o que simplemente es realizada por medio de *"cajas negras"*, que de una forma inexplicable consiguen generar el estado a utilizar. Sin embargo, esta tarea es de suma importancia, dado que para poder implementar cualquier algoritmo cuántico, se requiere conocer el proceso de generación del estado a ocupar, dado que en la implementación no existen las *"cajas negras"*, así sin este proceso no sería posible la implementación de cualquier algoritmo cuántico.

En el primer capítulo de este trabajo, se presentan conceptos fundamentales sobre la computación cuántica, como lo son los postulados de la mecánica cuántica, los cuales rigen el funcionamiento de estas máquinas. En el segundo capítulo se exponen los algoritmos cuánticos que resultan relevantes para este trabajo de tesis, desarrollando y explicando a detalle como funcionan estos, para después exponer el algoritmo propuesto para este proyecto de tesis, el cual genera un estado

cuántico compuesto por la superposición de diferentes estados cuánticos arbitrarios pertenecientes a la base de estados computacionales, finalmente en el tercer y cuarto capítulo se muestran los resultados y conclusiones de la ejecución del algoritmo cuántico propuesto en este trabajo con el uso de la biblioteca qiskit [14], desarrollada por la empresa IBM.

Capítulo 1

Conceptos Fundamentales

En este capítulo se pretende hacer una revisión de los conceptos fundamentales de la computación cuántica y por ende, también de la mecánica cuántica, pues es la rama de la física que rige el funcionamiento de una computadora cuántica y nos permite entender la computación cuántica.

1.1. Mecánica Cuántica

La mecánica cuántica es un área de estudio de la física moderna que se encarga de describir fenómenos físicos que ocurren a una escala muy pequeña, esta ha funcionado muy bien desde su desarrollo a finales del siglo XIX y principios del siglo XX. A través de los años la comunidad científica a partir de hechos experimentales y conocimiento matemático a propuesto los que se conocen como los postulados de la mecánica cuántica, los cuales rigen esta área de la física y que, dependiendo de la literatura que se revise se pueden tener 4,5 o más postulados diferentes e incluso el orden de en que estos son presentados puede variar. Para este trabajo se presenta una sintetización de algunos de los postulados, los cuales se consideran son los más esenciales para estudiar la computación cuántica.

1.1.1. Primer postulado

El estado de un sistema físico aislado es representado por un vector de estado (también conocido como ket de estado) normalizado $|\psi\rangle$, es decir $\langle\psi|\psi\rangle = 1$, el cual pertenece a un espacio vectorial complejo llamado espacio de estados, también conocido como espacio de Hilbert $\mathcal{H}$. Además, para un conjunto de n sistemas cuánticos tratados como un sistema combinado el espacio de estados está dado por el producto tensorial entre los espacios de Hilbert asociados a cada sistema, $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \cdots \otimes \mathcal{H}_n$. De esta forma el estado del sistema es representado de igual forma como el producto tensorial entre los estados de cada sistema

$$|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \cdots \otimes |\psi\rangle_n \tag{1.1}$$

1.1.2. Segundo Postulado

La evolución de un sistema físico cerrado está descrita por un operador unitario U, donde se tiene que para que el operador U sea unitario se debe cumplir que

$$UU^\dagger = U^\dagger U = I \tag{1.2}$$

donde I es el operador identidad, el cual deja invariante a cualquier estado al que se le sea aplicado y además, dado que U es unitario, se cumple que $U^\dagger = U^{-1}$, donde U^{-1} es el inverso del operador U.

De esta forma, si el estado inicial del sistema es $|\psi_1\rangle$, al aplicar el operador de evolución U se tiene que

$$U|\psi_1\rangle = |\psi_2\rangle \tag{1.3}$$

Además, dicho operador es lineal, lo que implica que al ser aplicado a una combinación lineal de estados este se distribuye linealmente en cada estado de la combinación

$$\begin{aligned} U\,|\psi\rangle &= U[\alpha_1\,|\psi_1\rangle + \alpha_2\,|\psi_2\rangle + \cdots + \alpha_n\,|\psi_n\rangle] \\ &= U\alpha_1\,|\psi_1\rangle + U\alpha_2\,|\psi_2\rangle + \cdots + U\alpha_n\,|\psi_n\rangle \\ &= \alpha_1 U\,|\psi_1\rangle + \alpha_2 U\,|\psi_2\rangle + \cdots + \alpha_n U\,|\psi_n\rangle \end{aligned} \tag{1.4}$$

1.1.3. Tercer Postulado

Toda cantidad física $\mathcal{A}$ que sea medible es descrita por un operador A llamado observable [8], la cual cumple con la condición de ser un operador hermítico, es decir $A = A^\dagger$; donde $A^\dagger$ es el operador adjunto de A.

Lo que quiere decir que la observable A es un operador autoadjunto y, por ende, permite una descomposición espectral de la observable en términos de sus eigenvalores y sus operadores de proyección

$$A = \sum_n a_n |a_n\rangle\langle a_n| = \sum_n a_n P_n \tag{1.5}$$

donde los vectores $|a_n\rangle$ corresponden a los eigenvectores de la observable A; que además forman un conjunto ortonormal, es decir, $\langle a_n|a_m\rangle = \delta_{n,m}$ y también cumplen con la relación de completitud $\sum_n |a_n\rangle\langle a_n| = \mathbb{I}$, formando de esta forma una base ortonormal.

De esta forma, el único resultado que se puede obtener al realizar una medición de la cantidad física $\mathcal{A}$ es uno de los eigenvalores correspondientes a la observable A, el cual comple con la condición de siempre ser un valor perteneciente al conjunto de los números reales $\mathbb{R}$.

1.1.4. Cuarto Postulado

Cuando una cantidad física $\mathcal{A}$ es medida en un sistema que se encuentra en el estado normalizado $|\psi\rangle$, la probabilidad $\mathcal{P}(a_n)$ de obtener el eigenvalor a_n de la observable correspondiente A esta dada por

$$\mathcal{P}(a_n) = |\,\langle a_n|\psi\rangle\,|^2 \tag{1.6}$$

donde $|a_n\rangle$ es el eigenvector de A, asociado con el eigenvalor a_n.

Si la cantidad física $\mathcal{A}$ al ser medida da como resultado el valor a_n, el estado del sistema inmediatamente después de la medición es la proyección normalizada del estado $|\psi\rangle$ en el espacio vectorial generado por los eigenvectores de la observable

$$|\psi\rangle \xrightarrow{Medición} |\psi'\rangle = \frac{P_n |\psi\rangle}{\sqrt{\langle\psi| P_n |\psi\rangle}} \tag{1.7}$$

1.2. Computación Cuántica

La computación cuántica es el estudio del procesamiento de información utilizando sistemas cuánticos, de los cuales son aprovechados fenómenos que ocurren en esta área de la física para poder realizar tareas de una forma más rápida en comparación con su contraparte clásica.

Para comprender y poder estudiar alguna de las distintas áreas de investigación de la computación cuántica es necesario conocer ciertos conceptos básicos, los cuales son presentados a continuación.

1.2.1. Qubits

Los qubits (quantum bits) son la unidad básica de información de la computación cuántica, estos son generados a partir de distintos sistemas cuánticos que por lo general son de dos niveles y son representados por los estados cuánticos de estos.

Las leyes que rigen el comportamiento de los qubits y la forma en la que estos cambian son las mismas que las de la mecánica cuántica. De esta forma, así como los conocidos bits, que pueden tomar alguno de los valores entre 0 y 1, los qubits pueden tomar algún valor entre los estados $|0\rangle, |1\rangle$ o una combinación entre estos dos valores, lo cual es conocido como una combinación lineal de estados también llamado como superposición de estados.

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1.8}$$

donde las cantidades α y β son números complejos .

Considerando el primer postulado de la mecánica cuántica (1.1.1), el estado de un qubit puede ser visto como un vector de estado asociado a un espacio vectorial complejo de dos dimensiones conformado por los vectores base $|0\rangle$ y $|1\rangle$, los cuales son conocidos como los estados base computacionales y forman una base ortonormal. Otra forma de representar los estados $|0\rangle$ y $|1\rangle$ es con la notación vectorial en la que se tiene que

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad y \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.9}$$

de tal forma que la ecuación 1.8 queda expresada como

$$\begin{aligned} |\psi\rangle &= \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} \\ &= \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \end{aligned} \tag{1.10}$$

El estado de un bit puede ser examinado para determinar si este es 0 o 1, esto lo hacen las computadoras al consultar el contenido de su memoria, sin embargo, con un qubit esto es algo diferente, dado que no es posible examinar un qubit para determinar el estado en el que se encuentra, esto debido al tercer y cuarto postulado de la mecánica cuántica (1.1.3 y 1.1.4), dado que cuando un qubit es medido se puede obtener como resultado un 0 con una probabilidad $|\alpha|^2$ o se puede obtener como resultado un 1 con una probabilidad $|\beta|^2$, de tal forma que al sumar estas probabilidades el resultado de la suma es 1, es decir

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.11}$$

esto quiere decir que el vector de estado de un qubit está normalizado (es unitario) y además que un qubit puede encontrarse en ambos estados $|0\rangle\, y\, |1\rangle$ a la vez, con el importante hecho de que al ser medido este colapsa su estado a alguno de los dos estados 0 o 1.

Considerando una fase global $e^{i\gamma}$ tal que esta se multiplique por el estado $|\psi\rangle$ de un qubit se tiene

$$e^{i\gamma}\,|\psi\rangle = e^{i\gamma}\alpha\,|0\rangle + e^{i\gamma}\beta\,|1\rangle \tag{1.12}$$

donde la probabilidad de medir 0 estará dada por

$$\begin{aligned} |\,\langle 0|\psi\rangle\,|^2 &= |e^{i\gamma}\alpha\,\langle 0|0\rangle + e^{i\gamma}\beta\,\langle 0|1\rangle\,|^2 \\ &= |e^{i\gamma}\alpha(1) + e^{i\gamma}\beta(0)|^2 \\ &= |e^{i\gamma}\alpha|^2 \\ &= |e^{i\gamma}|^2|\alpha|^2 \\ &= (e^{i\gamma}e^{-i\gamma})|\alpha|^2 \\ &= (e^{i\gamma-i\gamma})|\alpha|^2 \\ &= |\alpha|^2 \end{aligned} \tag{1.13}$$

y la probabilidad de medir 1

$$\begin{aligned} |\langle 1|\psi\rangle|^2 &= |e^{i\gamma}\alpha\langle 1|0\rangle + e^{i\gamma}\beta\langle 1|1\rangle|^2 \\ &= |e^{i\gamma}\alpha(0) + e^{i\gamma}\beta(1)|^2 \\ &= |e^{i\gamma}\beta|^2 \\ &= |e^{i\gamma}|^2|\beta|^2 \\ &= (e^{i\gamma}e^{-i\gamma})|\beta|^2 \\ &= (e^{i\gamma-i\gamma})|\beta|^2 \\ &= |\beta|^2 \end{aligned} \tag{1.14}$$

Por lo que el añadir una fase global al estado de un qubit no tiene impacto alguno al momento de realizar una medición; así, los estados $|\psi\rangle$ *y* $e^{i\gamma}|\psi\rangle$ son equivalentes.

1.2.1.1. Esfera de Bloch

Una forma muy útil de entender el comportamiento del estado de un qubit es de forma gráfica con el uso de la Esfera de Bloch.

Primero se debe considerar la ecuación 1.8, de la cual los valores α *y* β al ser complejos pueden ser expresados en su forma polar

$$\alpha = r_\alpha e^{i\phi_\alpha} \tag{1.15}$$

$$\beta = r_\beta e^{i\phi_\beta} \tag{1.16}$$

de esta forma la ecuación 1.8 puede ser expresada como

$$|\psi\rangle = r_\alpha e^{i\phi_\alpha}|0\rangle + r_\beta e^{i\phi_\beta}|1\rangle \tag{1.17}$$

y dado que al multiplicar el estado $|\psi\rangle$ por una fase global $e^{-i\phi_\alpha}$ esta no tiene ningún efecto al momento de realizar una medición, así la ecuación 1.17 queda expresada como

$$\begin{aligned} e^{-i\phi_\alpha}|\psi\rangle &= r_\alpha e^{i(\phi_\alpha-\phi_\alpha)}|0\rangle + r_\beta e^{i(\phi_\beta-\phi_\alpha)}|1\rangle \\ &= r_\alpha|0\rangle + r_\beta e^{i(\phi_\beta-\phi_\alpha)}|1\rangle \\ &= r_\alpha|0\rangle + r_\beta e^{i\phi}|1\rangle \\ &= |\psi\rangle \end{aligned} \tag{1.18}$$

donde $\phi_\beta - \phi_\alpha = \phi$. Además, por 1.11 se tiene que

$$\begin{aligned} |r_\alpha|^2 + |r_\beta e^{i\phi}|^2 &= r_\alpha r_\alpha^* + (r_\beta e^{i\phi})(r_\beta e^{i\phi})^* \\ &= r_\alpha^2 + (r_\beta e^{i\phi})(r_\beta e^{-i\phi}) \\ &= r_\alpha^2 + r_\beta^2 e^{i(\phi-\phi)} \\ &= r_\alpha^2 + r_\beta^2 \\ &= 1 \end{aligned} \tag{1.19}$$

Así, las cantidades r_α^2 y r_β^2 puden ser expresadas como

$$\begin{aligned} r_\alpha^2 = \cos^2(\frac{\theta}{2}) \longrightarrow r_\alpha = \cos\left(\frac{\theta}{2}\right) \\ r_\beta^2 = \sin^2(\frac{\theta}{2}) \longrightarrow r_\beta = \sin\left(\frac{\theta}{2}\right) \end{aligned} \tag{1.20}$$

para un ángulo $0 \leq \theta \leq 2\pi$. De esta forma 1.8 puede ser escrita como

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{1.21}$$

con $0 \leq \phi \leq 2\pi$. Donde con los ángulos θ y ϕ se puede representar cualquier estado $|\psi\rangle$ de un qubit ya sea en superposición o no, el cual estaría representado gráficamente por un punto sobre la superficie de una esfera unitaria, como se puede ver en la figura 1.1.

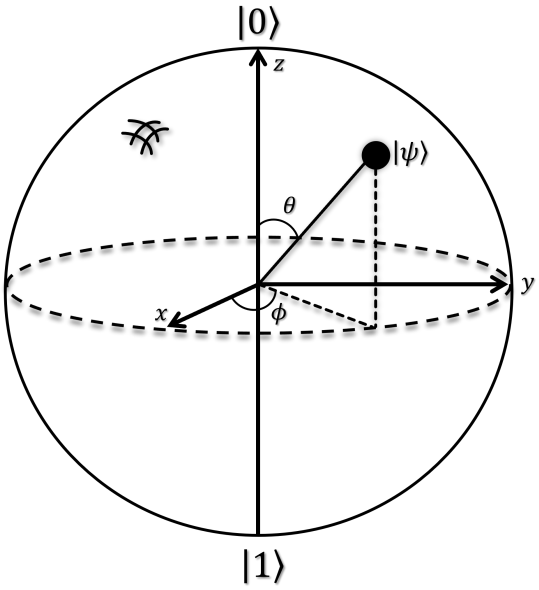

Figura 1.1: Representación del estado general de un qubit en la esfera de Bloch.

Es así como gracias a la esfera de Bloch es posible visualizar el estado de un qubit y el como este cambia en función de dos parámetros (θ y ϕ) que no son más que los ángulos correspondientes a las coordenadas esféricas en las que el parámetro r es igual a 1.

1.2.1.2. Multiples qubits

Para el caso en el que se esté trabajando con 2 o más qubits se tendrían varios subsistemas cuánticos que representen a estos, formando un solo sistema cuántico, por lo que se tiene que el estado de los subsistemas conjuntos estaría dado por lo que nos dice el primer postulado de la mecánica cuántica (1.1.1) que es la ecuación 1.1, donde cada vector de estado $|\psi\rangle_i$ (con $i = 0, 1, 2, ..., n$) representa al estado en superposición de cada qubit

$$|\psi\rangle_i = \alpha_i |0\rangle_i + \beta_i |1\rangle_i \tag{1.22}$$

Tomando como ejemplo el caso para dos qubits, los posibles estados en los que podría encontrarse el sistema serían

$$|0\rangle_0 \otimes |0\rangle_1 , \ |0\rangle_0 \otimes |1\rangle_1 , \ |1\rangle_0 \otimes |0\rangle_1 , \ |1\rangle_0 \otimes |1\rangle_1 \tag{1.23}$$

que también pueden ser expresados como $|00\rangle, |01\rangle, |10\rangle, |11\rangle$; los cuales forman una base a la cual se le conoce como la base computacional y esta no está restringida solamente a 2 qubits, sino que es una base general para n cantidad de qubits. Además, el estado del sistema conjunto también puede encontrarse en una superposición de estos estados

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \tag{1.24}$$

Para sistemas de múltiples qubits la probabilidad de que al medir, se obtenga alguno de los estados en superposición esta dada por $|\alpha_x|^2$ (con $x = \{00, 01, 10, 11\}$), y además se debe cumplir la regla de normalización, de tal forma que

$$\sum_{x \in \{0,1\}^2} |\alpha_x|^2 = 1 \tag{1.25}$$

donde $\{0, 1\}^2$ representa dos conjuntos de estados que pueden tomar como valor 0 ó 1 [17].

Además, para un sistema de varios qubits también es posible medir solamente un subconjunto de qubits pertenecientes a este, de tal forma que solamente se colapsaría el sistema que representa a cada qubit al valor que se obtenga de la medición haciendo que el estado del conjunto completo de qubits cambie en base al resultado de la medición.

Tomando como ejemplo el caso de un sistema de dos qubits, en el cual el estado del sistema completo está dado por la ecuación 1.24 y se mide al primer qubit, se tiene que la probabilidad de obtener 0 al realizar la medición es de $|\alpha_{00}|^2 + |\alpha_{01}|^2$ y la probabilidad de obtener 1 es $|\alpha_{10}|^2 + |\alpha_{11}|^2$; de tal forma que si se obtiene 0 al realizar la medición, el estado resultante después de la medición está dado por

$$|\psi'\rangle = \frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{1.26}$$

donde $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ es la cantidad que normaliza al estado haciendo que se cumpla la condición de normalización.

Para un conjunto de n qubits el estado general de estos estaría dado por

$$\begin{aligned} |\psi\rangle &= \alpha_{00\cdots0} |00\cdots0\rangle + \alpha_{00\cdots1} |00\cdots1\rangle + \cdots + \alpha_{11\cdots1} |11\cdots1\rangle \\ &= \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \end{aligned} \tag{1.27}$$

A veces, los estados conformados por los valores binarios que pueden tomar los qubits también son representados como números decimales [25]. Tomando esto en cuenta, podemos tomar al qubit más a la izquierda como el qubit cero, al qubit a su derecha inmediata como el qubit 1 y así sucesivamente hasta llegar al qubit más a la derecha, el cual sería el qubit n, de tal forma que la representación de cualquier número decimal estaría dada como

$$|M\rangle = |q\rangle_{n-1} |q\rangle_{n-2} \cdots |q\rangle_2 |q\rangle_1 |q\rangle_0 = |q_{n-1} q_{n-2} \cdots q_2 q_1 q_0\rangle \tag{1.28}$$

donde la forma de convertir un número del sistema decimal al sistema binario puede revisarse en el apéndice A.1.

1.2.2. Compuertas Cuánticas y Circuitos Cuánticos

Los cambios que pueda experimentar un estado cuántico pueden ser descritos con la computación cuántica [17] y, de forma análoga a la computación clásica, donde se construyen circuitos eléctricos con compuertas lógicas, en la computación cuántica también se construyen circuitos cuánticos conformados por cables y compuertas cuánticas que cambian el estado de uno o más qubits.

1.2.2.1. Compuertas cuánticas de un solo qubit

Las compuertas de un solo qubit pueden ser vistas como un operador unitario actuando sobre un sistema cuántico asociado a un espacio vectorial complejo de dos dimensiones, que no es más que el espacio vectorial que se utiliza para representar el estado de un solo qubit.

Existen una variedad infinita de compuertas cuánticas de un solo qubit, que, en la práctica pueden ser compuestas por una cantidad determinada de compuertas estándar, un ejemplo de estas compuertas es la compuerta NOT (también conocida como la compuerta X de Pauli) la cual cambia el estado $|0\rangle$ al estado $|1\rangle$, y viceversa. De esta forma se puede ver que para el estado en superposición $|\psi\rangle$ y por la ecuación 1.4, la aplicación de esta compuerta al estado $|\psi\rangle$ da como resultado

$$\begin{aligned} X|\psi\rangle &= X[\alpha|0\rangle + \beta|1\rangle] \\ &= \alpha X|0\rangle + \beta X|1\rangle \\ &= \alpha|1\rangle + \beta|0\rangle \end{aligned} \tag{1.29}$$

por lo que para el estado en superposición $|\psi\rangle$ la aplicación de la compuerta NOT invierte las amplitudes α y β.

Existe una forma de representar a las compuertas cuánticas, la cual es por medio de matrices. Tomando como ejemplo a la compuerta X, su representación matricial está dada por

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.30}$$

de tal forma que al tomar la representación vectorial del estado $|\psi\rangle$ (ecuación 1.10) y aplicarle la

compuerta X en su representación matricial se tiene un producto matricial cuyo resultado es

$$\begin{aligned} X|\psi\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \\ &= \begin{bmatrix} 0 \times \alpha + 1 \times \beta \\ 1 \times \alpha + 0 \times \beta \end{bmatrix} \\ &= \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \end{aligned} \tag{1.31}$$

Así, las compuertas cuánticas de un solo qubit pueden ser descritas como matrices de 2×2.

Otra compuerta cuántica muy importante en la computación cuántica es la compuerta de Hadamard, la cual genera un estado en superposición uniforme entre el $|0\rangle$ y $|1\rangle$, su representación matricial está dada por

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1.32}$$

y la forma en la que actúa sobre los estados $|0\rangle$ y $|1\rangle$ es

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \end{aligned} \tag{1.33}$$

1.2.2.2. Compuertas cuánticas para múltiples qubits

Generalizando las compuertas cuánticas de un solo qubit para múltiples se tienen las compuertas cuánticas para múltiples qubits, siendo la compuerta Control-Not o también conocida como $C-NOT$ la compuerta de múltiples qubits más conocida y más empleada en la computación cuántica. Esta compuerta toma como entrada 2 qubits, de los cuales uno es considerado como el qubit de control mientras que el otro es considerado como el qubit objetivo.

A partir del primer postulado de la mecánica cuántica (1.1.1), al tener que las compuertas cuánticas son operadores y que estos están actuando cada uno en su respectivo espacio de Hilbert, si se tienen compuertas A y B la forma en la que estos operadores se aplican a un estado $|\psi\rangle$ conformado por los qubits $|q_0\rangle$ y $|q_1\rangle$, cada uno perteneciente a su respectivo espacio de Hiblert al cual pertenecen A y B, es

$$(A \otimes B)|\psi\rangle = (A \otimes B)(|q_0\rangle \otimes |q_1\rangle) = A|q_0\rangle \otimes B|q_1\rangle = A|q_0\rangle\, B|q_1\rangle = A_0 B_1 |q_0 q_1\rangle \tag{1.34}$$

La forma en la que la compuerta $C-NOT$ actúa sobre un sistema de dos qubits es la siguiente: Si el qubit de control se encuentra en el estado 0, entonces el estado del qubit objetivo no cambia. Mientras que si el qubit de control se encuentra en el estado 1, entonces el estado del qubit objetivo cambia. La siguiente ecuación muestra la forma en la que la compuerta $C-NOT$ actúa sobre un sistema de dos qubits en sus diferentes estados

$$|00\rangle \xrightarrow{C-NOT} |00\rangle\,;\ |01\rangle \xrightarrow{C-NOT} |01\rangle\,;\ |10\rangle \xrightarrow{C-NOT} |11\rangle\,;\ |11\rangle \xrightarrow{C-NOT} |10\rangle \tag{1.35}$$

La representación matricial de esta compuerta es la siguiente

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.36}$$

que también es un operador unitario, dado que $(CNOT)(CNOT^{\dagger}) = (CNOT^{\dagger})(CNOT) = I$

Otra forma de describir la forma en la que actúa la compuerta C-NOT es mediante el uso de la suma módulo 2 (ver apéndice A.2), de tal forma que al aplicar esta a un sistema de dos qubits se tiene que

$$I \otimes CNOT\left[|q_c\rangle\,|q_o\rangle\right] = I\,|q_c\rangle\,CNOT\,|q_o\rangle = |q_c\rangle\,|q_o \oplus q_c\rangle \tag{1.37}$$

donde $|q_c\rangle$ y $|q_o\rangle$ representan a los qubits de control y objetivo, respectivamente.

Otra compuerta de múltiples qubits muy popular es la compuerta de Toffoli, que es similar a la comperta $C-NOT$. En esta compuerta se tienen dos qubits de control y un qubit objetivo, del cual es modificado su estado si ambos qubits de control se encuentran en el estado $|1\rangle$

Un hecho importante que se obtiene a partir de que las compuertas cuánticas sean operadores unitarios es que estas son siempre revertibles, dado que la inversa de una matriz unitaria es otra matriz unitaria [17]; de esta forma siempre es posible regresar al estado inicial de cualquier sistema de múltiples o de un solo qubit.

1.2.2.3. Circuitos Cuánticos

La forma en la que son representadas todas las operaciones realizadas en una computadora cuántica es a través de circuitos cuánticos, los cuales son diagramas que permiten visualizar gráficamente la forma en la que se realiza cualquier tarea, son expresados por medio de cables (no son necesariamente cables físicos o reales) que se asocian individualmente con cada qubit del sistema con el que se trabaje, se leen de izquierda a derecha o también puede considerarse que la forma en la que evoluciona el sistema va de izquierda a derecha. La figura 1.2 muestra al circuito cuántico que representa un sistema de 5 qubits.

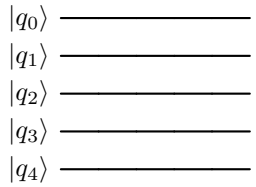

Figura 1.2: Circuito cuántico que representa un sistema de 5 qubits

A la colección de qubits que son utilizados para realizar cualquier tarea en un circuito cuántico se le conoce como registro cuántico y todos los qubits pertenecientes a un registro cuántico se inicializan en el estado $|0\rangle$ [21].

La forma en la que se representan las compuertas cuánticas en los circuitos cuánticos se puede observar en la figura 1.3, donde se tienen tres qubits, en los cuales están actuando las compuertas X, H, $C-NOT$, la compuerta de Toffoli y por último, en el tercer qubit se realiza una medición.

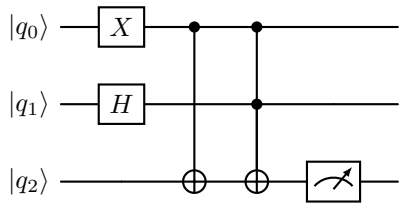

Figura 1.3: Representación de un circuito cuántico con compuertas

1.2.3. Algoritmos Cuánticos

Un algoritmo puede ser definido como una secuencia de pasos u operaciones [6]. De esta forma los algoritmos cuánticos son el conjunto de operaciones realizadas en una computadora cuántica, que como fue mencionado en la sección anterior (1.2.2.3), estos son representados gráficamente por circuitos cuánticos.

Entre los algoritmos cuánticos más conocidos se encuentran el algoritmo de Deutsch y su generalización conocida como el algoritmo de Deutsch-Jozsa que aprovechan y hacen uso del paralelismo cuántico para evaluar una función en todos sus valores de entrada con una sola consulta, también se tienen algoritmos más complejos como lo son el algoritmo de búsqueda de Grover, el algoritmo de estimación de fase, entre otros.

Es con el diseño y la implementación de los algoritmos cuánticos con lo que se obtiene, o se busca obtener una ventaja sobre la computación cuántica, siendo parte importante la generación de estados cuánticos

1.2.4. Complejidad computacional

El realizar cualquier tarea requiere del uso de recursos, por lo que es necesario tener una forma de cuantizar este requerimiento para llevar a cabo cualquier proceso o algoritmo. Una herramienta que se desarrollo para esto es la notación asintótica, la cual puede ser utilizada para resumir el comportamiento más esencial de una función [17]. La notación asintótica más utilizada en esta área es la notación big O (O) la cual sirve para establecer límites superiores en el comportamiento de una función. De tal forma que para las funciones $f(n)$ y $g(n)$ que se encuentren en el dominio de los enteros positivos, se dice que $f(n)$ es una función perteneciente a la clase $O(g(n))$ si existen las constantes c y n_0 tal que para todos los valores n mayores a n_0 se tiene que $f(n) \leq cg(n)$ [17].

Capítulo 2

Generación de estados cuánticos

Como ya fue mencionado en el capítulo anterior, la generación de estados cuánticos es una tarea importante en la implementación de cualquier algoritmo cuántico y en el procesamiento de información cuántica [20] , siendo la generación de estados otro algoritmo cuántico (también considerada como subrutina) que debe diseñarse y construirse como primer paso; es por esto que en este capítulo se presenta un algoritmo capaz de generar cualquier estado en superposición de uniforme de una cantidad arbitraria de estados.

2.1. Generación de M estados consecutivos en superposición uniforme

La generación de M estados en superposición uniforme utilizando todo el conjunto de estados de la base computacional (de tal forma que $M = 2^n$) es un problema que se resuelve aplicando n compuertas de Hadamard a n qubits en el estado $|0\rangle$ que conformen el registro cuántico con el que se esté trabajando, de tal forma que el estado resultante está dado por

$$|\psi\rangle = (H \otimes H \cdots \otimes H)(|0\rangle \otimes |0\rangle \cdots |0\rangle) = H^{\otimes n} |00\cdots 0\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \quad (2.1)$$

Sin embargo, cuando no se requiere utilizar todo el conjunto de estados base, el aplicar únicamente compuertas de Hadamard a todos los qubits del registro cuántico no funciona, es por eso que Shulka y Vedula propusieron el siguiente algoritmo [20] que pretende generar un estado $|\Theta\rangle$ en superposición uniforme de M estados, donde $2 < M < 2^n$. Este algoritmo hace uso de compuertas NOT, $Hadamard$, $Control - Hadamard$ y compuertas de rotación.

El funcionamiento del algoritmo es el siguiente:

1. Calcular $l_0, l_1, \ldots, l_k$. Donde $M = \sum_{j=0}^{k} 2^{l_j}$ con $0 \leq l_0 < l_1 < \ldots < l_{k-1} < l_k \leq n-1$ (convertir M de sistema decimal al sistema binario).

2. Iniciar $|\Theta_0\rangle = |q\rangle_{n-1} |q\rangle_{n-2} \cdots |q\rangle_2 |q\rangle_1 |q\rangle_0 = |q_{n-1} q_{n-2} \cdots q_2 q_1 q_0\rangle = |0\rangle^{\otimes n}$.

3. Aplicar la compuerta X en los qubits $|q\rangle_i$ para $i = l_1, l_2, \ldots, l_k$ (aplicar Compuertas NOT en los qubits con posición $l_1, l_2, \ldots, l_k$).

4. Establecer $M_0 = 2^{l_0}$.

5. Si $l_0 > 0$ entonces aplicar la compuerta de Hadamard en los qubits $|q\rangle_i$ para $i = 0, 1, \ldots l_0 - 1$ (si M es par, entonces aplicar compuertas Hadamard en los l_0 qubits más a la derecha).

6. Aplicar la compuerta de rotación $R_Y(\theta_0)$ en el qubit $|q\rangle_{l_1}$ con $\theta_0 = -2 \arccos\left(\sqrt{\frac{M_0}{M}}\right)$; donde esta compuerta es una compuerta de un solo qubit y está definida de forma matricial como

$$R_Y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \tag{2.2}$$

   además, la forma en la que esta compuerta actúa sobre los estados $|0\rangle$ y $|1\rangle$ es

$$\begin{aligned} R_Y(\theta)\,|1\rangle &= -\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle = a\,|0\rangle + b\,|1\rangle \\ R_Y(\theta)\,|0\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle = b\,|0\rangle - a\,|1\rangle \end{aligned} \tag{2.3}$$

7. Aplicar una compuerta $Control - Hadamard$ en los qubits $|q\rangle_i$ para $i = l_0, l_0 + 1, \ldots l_1 - 1$ con $|q\rangle_{l_1}$ siendo que el qubit de control debe estar en el estado $|0\rangle$ para aplicar la compuerta Hadamard al qubit objetivo.

8. Para $m = 1$ a $k - 1$:

   a) Aplicar una compuerta $Control - Rotación$ $CR_Y(\theta_m)$ en el qubit $|q\rangle_{l_{m+1}}$ condicionado a que el qubit de control $|q\rangle_{l_m}$ se encuentre en el estado $|0\rangle$.

   Donde $\theta_m = -2 \arccos\left(\sqrt{\frac{2^{l_m}}{M - M_{m-1}}}\right)$.

   b) Aplicar una compuerta Control-Hadamard en los qubits $|q\rangle_i$ para $i = l_m, l_m + 1, \ldots, l_{m+1} - 1$ condicionados a que el qubit de control $|q\rangle_{l_{m+1}}$ se encuentre en el estado $|0\rangle$.

   c) Establecer $M_m = M_{m-1} + 2^{l_m}$.

9. Obtener el estado $|\Theta\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle$.

2.1.1. Desarrollo del algoritmo y deducción del valor de los ángulos de rotación

A partir del paso 1 se puede notar que los valores $l_0, l_1, \ldots, l_k$ son una secuencia ordenada de números que contienen la posición de los 1 en la representación binaria de M, así, una vez que se

han calculado $l_0, l_1, \ldots, l_k$ se inicializa al registro cuántico con el que se va a trabajar en el estado $|0\rangle^{\otimes n}$ (paso 2).

Una vez que se tiene el estado $|\Theta_0\rangle$ a partir del paso 3 se aplican compuertas NOT en los qubits con posición $l_1, l_2, \ldots, l_k$, de tal forma que se tiene como resultado al estado

$$\begin{aligned} |\Theta_1\rangle &= X_i \, |0 \cdots \overbrace{0}^{l_k} \cdots 0 \cdots \overbrace{0}^{l_{k-1}} \cdots 0 \cdots \overbrace{0}^{l_1} \cdots 0 \cdots \overbrace{0}^{l_0} \cdots 0\rangle \\ &= |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{1}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0} \cdots 0\rangle \end{aligned} \tag{2.4}$$

Donde las expresiones $\overbrace{1}^{l_k} \cdots 0 \cdots \overbrace{1}^{l_{k-1}}$ y $0 \cdots \overbrace{1}^{l_k}$ (ya sea que tenga los indices por arriba o por debajo de los estados de cada qubit) indican que todos los qubits entre las posiciones l_k y l_{k-1} se encuentran en el estado 0 y que todos los qubits a la izquierda del qubit l_k se encuentran en el estado 0.

Al tener el estado $|\Theta_1\rangle$ y siguiendo el paso 4 se define $M_0 = 2^{l_0}$ y dependiendo del valor que tenga l_0 el algoritmo se divide en dos posibles casos los cuales son:

Caso 1. $l_0 = 0$. Para este caso, dado que $l_0 = 0$, se tiene que M es impar, de tal forma que el estado $|\Theta_1\rangle$ para este caso quedaría expresado como

$$|\Theta_1\rangle = |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{1}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0}\rangle \tag{2.5}$$

además, por el paso 5 no se debe aplicar ninguna compuerta de Hadamard, sino que se aplica la compuerta de rotación $R_Y(\theta_0)$ en el qubit $|q\rangle_{l_1}$ (paso 6), y de acuerdo con la ecuación 2.3 se tiene

$$\begin{aligned} |\Theta_2\rangle &= R_Y(\theta_0)_{l_1} \, |0 \cdots \overbrace{1}^{l_k} \cdots 0 \cdots \overbrace{1}^{l_{k-1}} \cdots 0 \cdots \overbrace{1}^{l_1} \cdots 0 \cdots \overbrace{0}^{l_0}\rangle \\ &= a_0 \, |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{0}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0}\rangle \\ &+ b_0 \, |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{1}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0}\rangle \end{aligned} \tag{2.6}$$

De acuerdo con el paso 7, se aplica la compuerta $Control - Hadamard$ en los qubits correspondientes dando como resultado al estado

$$\begin{aligned} |\Theta_3\rangle &= a_0 \left(CH_i^{q_{l_1}=0}\right) |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{0}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0}\rangle \\ &+ b_0 \left(CH_i^{q_{l_1}=0}\right) |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{1}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0}\rangle \\ &= a_0 \, |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{0}_{l_1} \cdots + \cdots \underbrace{+}_{l_0}\rangle \\ &+ b_0 \, |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{1}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0}\rangle \end{aligned} \tag{2.7}$$

donde el subíndice de la expresión $CH_i^{q_{l_1}=0}$ representa los qubits objetivo y el superíndice representa al qubit de control y el valor que este debe tomar para que la compuerta realice el cambio de estados. Además, la expresión + dentro de los estados en superposición de la ecuación 2.7 es la representación de uno de los estados resultantes al aplicar la compuerta de Hadamard sobre alguno de los estados $|1\rangle$ o $|0\rangle$, como se puede ver en la ecuación 1.33.

Finalmente, al llegar al paso 8 se debe realizar una secuencia de pasos iterativa, así, para $m = 1$ se tiene para el paso $8a$ el estado

$$
\begin{aligned}
|\Theta_4\rangle &= a_0 \left(CR_Y(\theta_1)_{q_{l_2}}^{q_{l_1}=0}\right) |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_{k-1}}\cdots 0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
&+ b_0 \left(CR_Y(\theta_1)_{q_{l_2}}^{q_{l_1}=0}\right) |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_{k-1}}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle \\
&= a_0(a_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{0}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
&+ b_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle) \\
&+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle \\
&= a_0a_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{0}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
&+ a_0b_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
&+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle
\end{aligned}
\tag{2.8}
$$

ahora para el paso $8b$ se aplica una cumpuerta $Control - Hadamard$ en los qubits $|q\rangle_i$ para $i = l_1, l_1 + 1, \ldots, l_2 - 1$ condicionada a que el qubit de control $|q\rangle_{l_2}$ se encuentre en el estado $|0\rangle$. De esta forma

$$
\begin{aligned}
|\Theta_5\rangle = \left(CH_i^{q_{l_2}=0}\right) [a_0a_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{0}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ a_0b_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle] \\
= a_0a_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{0}_{l_2}\cdots +\cdots\underbrace{+}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ a_0b_1 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots 0\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle
\end{aligned}
\tag{2.9}
$$

Para el paso $8c$ se define $M_1 = M_0 + 2^{l_1}$ y se repite el mismo proceso para $m = 2$ de tal forma que del paso $8a$

$$
\begin{aligned}
|\Theta_6\rangle = \left(CR_Y(\theta_2)_{q_{l_3}}^{q_{l_2}=0}\right) [a_0a_1 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{0}_{l_2}\cdots +\cdots\underbrace{+}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ a_0b_1 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle] \\
= a_0a_1(a_2 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{0}_{l_3}\cdots\underbrace{0}_{l_2}\cdots +\cdots\underbrace{+}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ b_2 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{0}_{l_2}\cdots +\cdots\underbrace{+}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle) \\
+ a_0b_1 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle \\
= a_0a_1a_2 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{0}_{l_3}\cdots\underbrace{0}_{l_2}\cdots +\cdots\underbrace{+}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ a_0a_1b_2 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{0}_{l_2}\cdots +\cdots\underbrace{+}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ a_0b_1 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{0}_{l_1}\cdots +\cdots\underbrace{+}_{l_0}\rangle \\
+ b_0 |0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots 0\cdots\underbrace{1}_{l_1}\cdots 0\cdots\underbrace{0}_{l_0}\rangle
\end{aligned}
\tag{2.10}
$$

a partir del paso $8b$ el estado resultante es

$$
\begin{aligned}
|\Theta_7\rangle = \left(CH_i^{q_{l_3}=0}\right)\,[a_0a_1a_2\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{0}_{l_3}\cdots\underbrace{0}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0a_1b_2\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{0}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0b_1\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,b_0\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots0\cdots\underbrace{1}_{l_1}\cdots0\cdots\underbrace{0}_{l_0}\rangle] \\
=\,a_0a_1a_2\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{0}_{l_3}\cdots+\cdots\underbrace{+}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0a_1b_2\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{0}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0b_1\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,b_0\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots0\cdots\underbrace{1}_{l_1}\cdots0\cdots\underbrace{0}_{l_0}\rangle
\end{aligned}
\tag{2.11}
$$

donde $i = l_2, l_2+1, \ldots, l_{2+1}-1$. Ahora, del paso $8c$ se define $M_2 = M_1 + 2^{l_2}$, y repitiendo el proceso iterativo hasta llegar a $m = k-1$ se tiene el estado

$$
\begin{aligned}
|\Theta\rangle = a_0a_1\ldots a_{k-1}\,|0\cdots\underbrace{0}_{l_k}\cdots+\cdots\underbrace{+}_{l_{k-1}}\cdots+\cdots\underbrace{+}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0a_1\ldots a_{k-2}b_{k-1}\,|0\cdots\underbrace{1}_{l_k}\cdots0\cdots\underbrace{0}_{l_{k-1}}\cdots+\cdots\underbrace{+}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0a_1\ldots a_{k-3}b_{k-2}\,|0\cdots\underbrace{1}_{l_k}\cdots0\cdots\underbrace{1}_{l_{k-1}}\cdots\underbrace{0}_{l_{k-2}}\cdots+\cdots\underbrace{+}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\cdots \\
+\,a_0a_1a_2b_3\,|0\cdots\underbrace{1}_{l_k}\cdots0\cdots\underbrace{1}_{l_{k-1}}\cdots0\cdots\underbrace{0}_{l_3}\cdots+\cdots\underbrace{+}_{l_2}\cdots\underbrace{+}_{l_1}\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0a_1b_2\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{0}_{l_2}\cdots+\cdots\underbrace{+}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,a_0b_1\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots0\cdots\underbrace{0}_{l_1}\cdots+\cdots\underbrace{+}_{l_0}\rangle \\
+\,b_0\,|0\cdots\underbrace{1}_{l_k}\cdots\underbrace{1}_{l_3}\cdots\underbrace{1}_{l_2}\cdots0\cdots\underbrace{1}_{l_1}\cdots0\cdots\underbrace{0}_{l_0}\rangle
\end{aligned}
\tag{2.12}
$$

donde el estado $|\Theta\rangle$ representa la superposición uniforme de M estados consecutivos, y, finalmente se define $M_{k-1} = M_{k-2} + 2^{l_{k-1}}$.

Caso 2. $l_0 > 0$. Este caso implica que M es un número par, por lo que el estado $|\Theta_1\rangle$ es expresado de la misma forma que la ecuación 2.4 de tal forma que al aplicar la compuerta Hadamard que menciona el paso 5 se tiene

$$\begin{aligned} |\Theta_2\rangle &= H_i \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{1}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots 0\rangle \\ &= |0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{1}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle \end{aligned} \tag{2.13}$$

A partir del paso 6 en adelante se realiza lo mismo que en el **Caso 1.** de tal forma que el estado generado por este paso es

$$\begin{aligned} |\Theta_3\rangle &= R_Y(\theta_0)_{l_1} \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{1}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle \\ &= a_0 \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{0}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle \\ &+ b_0 \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{1}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle \end{aligned} \tag{2.14}$$

Para el paso 7 se tiene que

$$\begin{aligned} |\Theta_4\rangle &= \left(CH_i^{q_{l_1}=0}\right)(a_0 \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{0}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle \\ &+ b_0 \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{1}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle) \\ &= a_0 \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{0}_{l_1}\cdots +\cdots \underbrace{+}_{l_0}\cdots +\cdots\rangle \\ &+ b_0 \,|0\cdots \underbrace{1}_{l_k}\cdots 0\cdots \underbrace{1}_{l_{k-1}}\cdots 0\cdots \underbrace{1}_{l_1}\cdots 0\cdots \underbrace{0}_{l_0}\cdots +\cdots\rangle \end{aligned} \tag{2.15}$$

De esta forma el estado final que se obtiene de seguir con la ejecución de los pasos iterativos del paso 8 es similar al estado que se obtiene en el caso anterior con la diferencia de no tener al estado con posición l_0 en la posición más a la derecha, sino que hay más estados a la derecha de este, siendo que el estado $|\Theta\rangle$ para este caso queda expresado como

$$
\begin{aligned}
|\psi\rangle = a_0 a_1 \ldots a_{k-1} |0 \cdots \underbrace{0}_{l_k} \cdots + \cdots \underbrace{+}_{l_{k-1}} \cdots + \cdots \underbrace{+}_{l_2} \cdots + \cdots \underbrace{+}_{l_1} \cdots + \cdots \underbrace{+}_{l_0} \cdots + \cdots \rangle \\
+ a_0 a_1 \ldots a_{k-2} b_{k-1} |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{0}_{l_{k-1}} \cdots + \cdots \underbrace{+}_{l_2} \cdots + \cdots \underbrace{+}_{l_1} \cdots + \cdots \underbrace{+}_{l_0} \cdots + \cdots \rangle \\
+ a_0 a_1 \ldots a_{k-3} b_{k-2} |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots \underbrace{0}_{l_{k-2}} \cdots + \cdots \underbrace{+}_{l_2} \cdots + \cdots \underbrace{+}_{l_1} \cdots + \cdots \underbrace{+}_{l_0} \cdots + \cdots \rangle \\
+ \cdots \\
+ a_0 a_1 a_2 b_3 |0 \cdots \underbrace{1}_{l_k} \cdots 0 \cdots \underbrace{1}_{l_{k-1}} \cdots 0 \cdots \underbrace{0}_{l_3} \cdots + \cdots \underbrace{+}_{l_2} \cdots \underbrace{+}_{l_1} \cdots \underbrace{+}_{l_0} \cdots + \cdots \rangle \\
+ a_0 a_1 b_2 |0 \cdots \underbrace{1}_{l_k} \cdots \underbrace{1}_{l_3} \cdots \underbrace{0}_{l_2} \cdots + \cdots \underbrace{+}_{l_1} \cdots + \cdots \underbrace{+}_{l_0} \cdots + \cdots \rangle \\
+ a_0 b_1 |0 \cdots \underbrace{1}_{l_k} \cdots \underbrace{1}_{l_3} \cdots \underbrace{1}_{l_2} \cdots 0 \cdots \underbrace{0}_{l_1} \cdots + \cdots \underbrace{+}_{l_0} \cdots + \cdots \rangle \\
+ b_0 |0 \cdots \underbrace{1}_{l_k} \cdots \underbrace{1}_{l_3} \cdots \underbrace{1}_{l_2} \cdots 0 \cdots \underbrace{1}_{l_1} \cdots 0 \cdots \underbrace{0}_{l_0} \cdots + \cdots \rangle
\end{aligned}
\tag{2.16}
$$

Además, por la ecuación 1.33 los estados $|+\rangle$ en las ecuaciones 2.12 y 2.16 añaden a la amplitud de cada estado en superposición un factor $\frac{1}{\sqrt{2^{l_j}}}$, con $j = 0, 1, 2, \ldots, k-1, k$, esto debido a las compuertas Hadamard aplicadas en los pasos 5, 7 y 8*b*.

Ahora, para hallar el valor de los ángulos pertenecientes a las compuertas de rotación $R_Y(\theta)$ aplicadas en el algoritmo se debe tomar que todas las amplitudes de los estados en superposición generados y representados por el estado $|\psi\rangle$ deben ser iguales a $\frac{1}{\sqrt{M}}$; de esta forma

$$
\frac{a_0 a_1 \cdots a_{k-2} a_{k-1}}{\sqrt{2^{l_k}}} = \frac{a_0 a_1 \cdots a_{k-2} b_{k-1}}{\sqrt{2^{l_{k-1}}}} = \cdots = \frac{a_0 a_1 b_2}{\sqrt{2^{l_2}}} = \frac{a_0 b_1}{\sqrt{2^{l_1}}} = \frac{b_0}{\sqrt{2^{l_0}}} = \frac{1}{\sqrt{M}} \tag{2.17}
$$

Así, despejando b_0 en la igualdad con $\frac{1}{\sqrt{M}}$ se tiene

$$
b_0 = \sqrt{\frac{2^{l_0}}{M}} \tag{2.18}
$$

y debido a la condición de normalización (ecuación 1.11) y la acción de la compuerta de rotación (ecuación 2.3) se tiene que

$$
|a_0|^2 + |b_0|^2 = 1 \longrightarrow a_0 = \sqrt{1 - |b_0|^2} = \sqrt{1 - {b_0}^2} \tag{2.19a}
$$

de tal forma que

$$
a_0 = \sqrt{1 - \left(\sqrt{\frac{2^{l_0}}{M}}\right)^2} = \sqrt{1 - \frac{2^{l_0}}{M}} = \sqrt{\frac{M - 2^{l_0}}{M}} \tag{2.19b}
$$

Ahora, despejando b_1

$$\frac{a_0 b_1}{\sqrt{2^{l_1}}} = \frac{1}{\sqrt{M}} \longrightarrow b_1 = \frac{\sqrt{2^{l_1}}}{a_0\sqrt{M}} = \frac{\sqrt{2^{l_1}}}{\sqrt{\frac{M-2^{l_0}}{M}}\sqrt{M}} = \frac{\sqrt{2^{l_1}}}{\sqrt{M-2^{l_0}}} = \sqrt{\frac{2^{l_1}}{M-2^{l_0}}} \tag{2.20}$$

y de la misma forma que la ecuación 2.19b, por la condición de normalización, el valor de a_1 resulta ser

$$a_1 = \sqrt{1-{b_1}^2} = \sqrt{1-\frac{2^{l_1}}{M-2^{l_0}}} = \sqrt{\frac{M-2^{l_0}-2^{l_1}}{M-2^{l_0}}} \tag{2.21a}$$

pero a partir del paso 8c se definió $M_m = M_{m-1}+2^{l_m}$ para $m = 1$ a $k-1$, por lo que $M_1 = M_0+2^{l_1}$ y del paso 4 $M_0 = 2^{l_0}$, lo que implica que M_1 esté definido como $M_1 = 2^{l_0}+2^{l_1}$. Así

$$a_1 = \sqrt{\frac{M-2^{l_0}-2^{l_1}}{M-2^{l_0}}} = \sqrt{\frac{M-M_1}{M-M_0}} \tag{2.21b}$$

Si ahora se despeja b_2 se obtiene como resultado

$$b_2 = \frac{\sqrt{2^{l_2}}}{a_0 a_1\sqrt{M}} = \frac{\sqrt{2^{l_2}}}{\sqrt{\frac{M-M_0}{M}}\sqrt{\frac{M-M_1}{M-M_0}}\sqrt{M}} = \frac{\sqrt{2^{l_2}}}{\sqrt{M-M_1}} = \sqrt{\frac{2^{l_2}}{M-M_1}} \tag{2.22}$$

y siguiendo el mismo proceso que se utilizó para hallar a_0 y a_1 se puede calcular a_2 de tal forma que

$$a_2 = \sqrt{1-{b_2}^2} = \sqrt{1-\frac{2^{l_2}}{M-M_1}} = \sqrt{\frac{M-M_1-2^{l_2}}{M-M_1}} \tag{2.23a}$$

y como $M_2 = M_1+2^{l_2}$, entonces

$$a_2 = \sqrt{\frac{M-M_2}{M-M_1}} \tag{2.23b}$$

Es así como se puede ver que existe una forma general de representar el valor de cada a_i y b_i con $0 < i \leq k-1$, de tal forma que las ecuaciones que definen estos términos son

$$a_i = \sqrt{\frac{M-M_i}{M-M_{i-1}}} \tag{2.24a}$$

$$b_i = \sqrt{\frac{2^{l_i}}{M-M_{i-1}}} \tag{2.24b}$$

siendo los términos a_0 y b_0 definidos de forma única como están expresados en las ecuaciones 2.19b y 2.18, respectivamente.

Una vez conociendo el valor de las amplitudes a_i, b_i , a_0 y b_0 se puede proceder a hallar el valor de los ángulos θ_0 y θ_m. Esto a partir del valor que toman a y b en la ecuación 2.3, así, para θ_0 se tiene que

$$\cos\left(\frac{\theta_0}{2}\right) = b_0 = \sqrt{\frac{2^{l_0}}{M}} \longrightarrow \theta_0 = \pm 2 \arccos(b_0) = \pm 2 \arccos\left(\sqrt{\frac{2^{l_0}}{M}}\right) \tag{2.25}$$

sin embargo, para la amplitud a_0 se tiene que $a_0 = -\sin\left(\frac{\theta_0}{2}\right)$ y en este algortimo se debe cumplir que las amplitudes de todos los estados en superposición sean positivas, por lo que $\sin\left(\frac{\theta_0}{2}\right) < 0$ para que se cumpla que $a_0 > 0$, de esta forma se tiene que el ángulo que cumple con esta condición en la ecuación 2.25 es

$$\theta_0 = -2 \arccos\left(\sqrt{\frac{2^{l_0}}{M}}\right) \tag{2.26}$$

Ahora, para el ángulo θ_m se tiene que

$$\cos\left(\frac{\theta_m}{2}\right) = b_m = \sqrt{\frac{2^{l_m}}{M - M_{m-1}}} \longrightarrow \theta_m = \pm 2 \arccos\left(\sqrt{\frac{2^{l_m}}{M - M_{m-1}}}\right) \tag{2.27}$$

y utilizando el mismo argumento para determinar el valor de θ_0 el valor del ángulo θ_m resulta ser

$$\theta_m = -2 \arccos\left(\sqrt{\frac{2^{l_m}}{M - M_{m-1}}}\right) \tag{2.28}$$

2.2. Algoritmo de Amplificación de Amplitudes

El algoritmo de amplificación de amplitudes, es una generalización del muy conocido algoritmo de búsqueda de Grover [12], este último llamado así en honor a Lov K. Grover, quien fue el primero en proponer tal algoritmo.

Brassard, Hoyer y Mosca [3, 4, 5], fueron quienes propusieron por primera vez una generalización al algoritmo de Grover, estableciendo este último como un caso especial de su algoritmo. Sin embargo, es importante familiarizarse primero con el algoritmo de búsqueda de Grover para comprender correctamente la amplificación de amplitudes.

2.2.1. Algoritmo de búsqueda Grover

En su artículo [12], Grover propone un sistema que contiene $N = 2^n$ estados, etiquetados como $S_1, S_2, S_3, \ldots, S_N$, los cuales están representados como n cadenas de bits. Además, toma al estado S_v como el único que cumple con la condición $C(S_v) = 1$, mientras que para todos los demás estados S, se tiene que $C(S) = 0$. El problema a resolver es identificar al estado S_v. Es a partir de esta premisa que Grover propone su algoritmo en una secuencia de 3 pasos, sin embargo, el desarrollo del algoritmo y la deducción de algunos valores importantes de este no son desarrollados de una forma muy clara en el artículo publicado por Grover, hay una gran variedad de artículos y libros que desarrollan y explican de una forma más clara este algoritmo [2, 4, 5, 6, 7, 9, 13, 15, 17, 18, 22, 23, 24, 25], así los pasos del algoritmo de búsqueda de Grover son los siguientes:

I. Generar la superposición de los N estados que conforman al sistema. Esto se logra aplicando n compuertas de Hadamard a los n qubits del registro cuántico con el que se esté trabajando. De esta forma el estado resultate es

$$|\psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle \tag{2.29}$$

II. Aplicar el operador de Grover, definido como G, el cual se divide en los siguientes pasos:

a) Aplicar el operador oráculo, definido como O, el cual se puede comprender como una función $f : \{0,1\}^n \to \{0,1\}$ que cumple con la condición

$$f(x) = \begin{cases} 1 & si \quad x = x_0 \\ 0 & si \quad x \neq x_0 \end{cases} \tag{2.30}$$

esta función toma cualquier estado $|x\rangle$ y cambia su fase de la forma

$$|x\rangle \xrightarrow{O} \begin{cases} |x\rangle & si \quad f(x) = 0 \\ -|x\rangle & si \quad f(x) = 1 \end{cases} \iff |x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle \tag{2.31}$$

de tal forma que el operador oráculo marca al estado que es solución al problema. Además, la forma en la que este sea construido no es universal para cualquier estado solución.

b) Aplicar el operador difusor, también conocido como inversión sobre la media, el cual está definido como

$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi_1\rangle\langle\psi_1| - I \tag{2.32}$$

c) Repetir todo el paso II. $O\left(\sqrt{N}\right)$ veces

III. Medir el registro cuántico y obtener el estado $|x_0\rangle$ con una probabilidad de al menos $\frac{1}{2}$

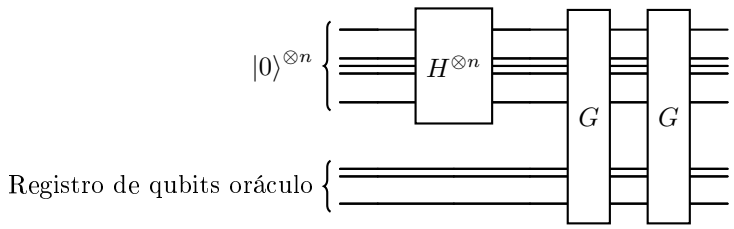

Figura 2.1: Circuito que representa la implementación del algoritmo de Gover

Es de una forma casi directa que el algoritmo de Grover puede ser aplicado para realizar la búsqueda de M elementos que cumplan con la condición de la función $f(x) = 1$ solamente modificando al operador oráculo de tal forma que este "marque"los estados solución, de tal forma que para M elementos solución, el paso II.*c* cambiaría de aplicar el paso II. $O\left(\sqrt{N}\right)$ veces a $O\left(\sqrt{\frac{N}{M}}\right)$ veces.

Una forma de comprender mejor como funciona el algoritmo de Grover es desarrollando este de forma geométrica.

2.2.1.1. Desarrollo del algoritmo de Grover desde el punto de vista geométrico

Para este tipo de enfoque se define al estado $|\psi_1\rangle$ de la ecuación 2.29 como la superposición de dos estados ortonormales, $|\alpha\rangle$ y $|\beta\rangle$, lo que implica que

$$\begin{aligned} \langle\alpha|\alpha\rangle &= 1 \\ \langle\beta|\beta\rangle &= 1 \\ \langle\alpha|\beta\rangle &= 0 = \langle\beta|\alpha\rangle \end{aligned} \tag{2.33}$$

De esta forma estos estados están definidos como

$$\begin{aligned} |\alpha\rangle &= \frac{1}{\sqrt{N-M}} \sum_{x \notin S} |x\rangle \\ |\beta\rangle &= \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle \end{aligned} \tag{2.34}$$

donde $|\alpha\rangle$ es el vector de estado que representa a todos los estados que no son solución y $|\beta\rangle$ representa a los M estados que son solución y pertenecen al subconjunto S, que contiene a todos estos, además N es el número total de estados. De esta forma el estado $|\psi_1\rangle$ queda definido como

$$|\psi_1\rangle = \alpha\,|\alpha\rangle + \beta\,|\beta\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \tag{2.35}$$

de tal forma que las amplitudes α y β toman los valores

$$\begin{aligned} \alpha &= \sqrt{\frac{N-M}{N}} \\ \beta &= \sqrt{\frac{M}{N}} \end{aligned} \tag{2.36}$$

así, el estado $|\psi_1\rangle$ se encuentra en un plano generado a partir de los estados $|\alpha\rangle$ y $|\beta\rangle$, como se puede ver en la figura 2.2 .

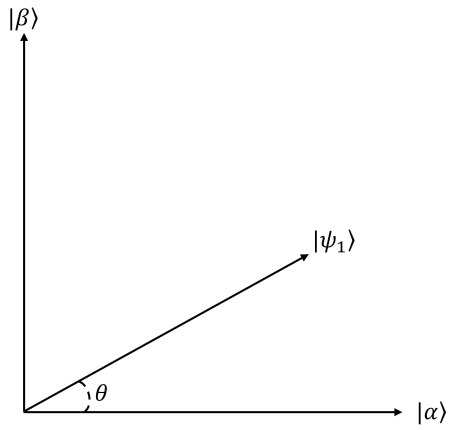

Figura 2.2: Estado $|\psi_1\rangle$ representado en un plano generado por los estados ortonormales $|\alpha\rangle$ y $|\beta\rangle$.

además, a partir de la figura 2.2 se tiene que

$$\begin{aligned} \sin(\theta) &= \sqrt{\frac{M}{N}} \\ \cos(\theta) &= \sqrt{\frac{N-M}{N}} \end{aligned} \tag{2.37}$$

Al aplicar el operador de Grover (que está compuesto por el operador oráculo y el operador de difusión), primero se debe aplicar el oráculo, con el cual se realiza una reflexión sobre el estado $|\alpha\rangle$ en el plano definido por los estados $|\alpha\rangle$ y $|\beta\rangle$, como se puede observar en la figura 2.3.

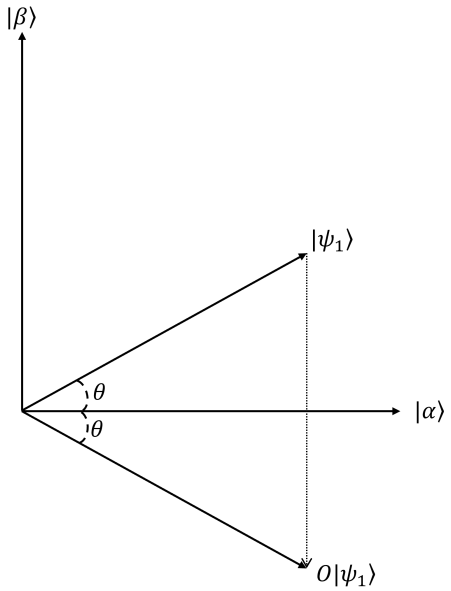

Figura 2.3: Aplicación del oráculo al estado $|\psi_1\rangle$, el cual causa una reflexión sobre el el estado $|\alpha\rangle$, haciendo que los estados solución sufran de un cambio de fase a una negativa.

De esta forma, el estado $|\psi_2\rangle$ queda definido como

$$\begin{aligned} |\psi_2\rangle = O\,|\psi_1\rangle &= O\left(\alpha\,|\alpha\rangle + \beta\,|\beta\rangle\right) \\ &= \alpha\,|\alpha\rangle - \beta\,|\beta\rangle \end{aligned} \tag{2.38}$$

Finalmente, al aplicar el operador difusor D (ecuación 2.32) al estado $|\psi_2\rangle$, de forma similar que al aplicar O, se tiene una reflexión sobre un estado, siendo este el estado $|\psi_1\rangle$, como se puede ver en la figura 2.4; de tal forma que se obtiene como resultado

$$|\psi_3\rangle = D\,|\psi_2\rangle = \left(2\,|\psi_1\rangle\,\langle\psi_1| - \ I\right)|\psi_2\rangle \tag{2.39}$$

pero

$$\begin{aligned} |\psi_1\rangle &= \cos(\theta)\,|\alpha\rangle + \sin(\theta)\,|\beta\rangle \\ |\psi_2\rangle &= \cos(\theta)\,|\alpha\rangle - \sin(\theta)\,|\beta\rangle \end{aligned} \tag{2.40}$$

por lo que el estado $|\psi_3\rangle$ resulta en

$$\begin{aligned}
|\psi_3\rangle &= \left[2\left(\cos(\theta)|\alpha\rangle + \sin(\theta)|\beta\rangle\right)\left(\cos(\theta)\langle\alpha| + \sin(\theta)\langle\beta|\right) - \ I\right]\left[\cos(\theta)|\alpha\rangle - \sin(\theta)|\beta\rangle\right] \\
&= \left[2\left(\cos^2(\theta)|\alpha\rangle\langle\alpha| + \cos(\theta)\sin(\theta)|\alpha\rangle\langle\beta| + \cos(\theta)\sin(\theta)|\beta\rangle\langle\alpha| + \sin^2(\theta)|\beta\rangle\langle\beta|\right) - I\right]\left[\cos(\theta)|\alpha\rangle - \sin(\theta)|\beta\rangle\right] \\
&= 2\left[\cos^3(\theta)|\alpha\rangle\langle\alpha|\alpha\rangle + \cos^2(\theta)\sin(\theta)|\alpha\rangle\langle\beta|\alpha\rangle + \cos^2(\theta)\sin(\theta)|\beta\rangle\langle\alpha|\alpha\rangle + \sin^2(\theta)\cos(\theta)|\beta\rangle\langle\beta|\alpha\rangle\right. \\
&\quad \left. - \cos^2(\theta)\sin(\theta)|\alpha\rangle\langle\alpha|\beta\rangle - \cos(\theta)\sin^2(\theta)|\alpha\rangle\langle\beta|\beta\rangle - \cos(\theta)\sin^2(\theta)|\beta\rangle\langle\alpha|\beta\rangle - \sin^3(\theta)|\beta\rangle\langle\beta|\beta\rangle\right] \\
&\quad - I\left[\cos(\theta)|\alpha\rangle - \sin(\theta)|\beta\rangle\right] \\
&= 2\left[\cos^3(\theta) + \cos^2(\theta)\sin(\theta)|\beta\rangle - \cos(\theta)\sin^2(\theta)|\alpha\rangle - \sin^3(\theta)|\beta\rangle\right] - \cos(\theta)|\alpha\rangle + \sin(\theta)|\beta\rangle \\
&= 2\cos^3(\theta)|\alpha\rangle + 2\cos^2(\theta)\sin(\theta)|\beta\rangle - 2\cos(\theta)\sin^2(\theta)|\alpha\rangle - 2\sin^3(\theta)|\beta\rangle - \cos(\theta)|\alpha\rangle + \sin(\theta)|\beta\rangle \\
&= \underbrace{\left[2\cos^3(\theta) - 2\cos(\theta)\sin^2(\theta) - \cos(\theta)\right]}_{\text{Parte de } \alpha}|\alpha\rangle + \underbrace{\left[2\cos^2(\theta)\sin(\theta) - 2\sin^3(\theta) + \sin(\theta)\right]}_{\text{Parte de } \beta}|\beta\rangle
\end{aligned} \tag{2.41}$$

Haciendo uso de las identidades trigonométricas del seno y coseno para ángulos triples

$$\begin{aligned}
\sin(3\theta) &= 3\sin(\theta) - 4\sin^3(\theta) \\
\cos(3\theta) &= 4\cos^3(\theta) - 3\cos(\theta)
\end{aligned} \tag{2.42}$$

la parte de α de la ecuación 2.41 puede ser expresada como

$$\begin{aligned}
2\cos^3(\theta) - 2\cos(\theta)\sin^2(\theta) - \cos(\theta) &= 2\cos^3(\theta) - 2\cos(\theta)\left[1 - \cos^2(\theta)\right] - \cos(\theta) \\
&= 2\cos^3(\theta) - 2\cos(\theta) + 2\cos^3(\theta) - \cos(\theta) \\
&= 4\cos^3(\theta) - 3\cos(\theta) \\
&= \cos(3\theta)
\end{aligned} \tag{2.43}$$

y de la misma forma, la parte de β es expresada como

$$\begin{aligned}
2\cos^2(\theta)\sin(\theta) - 2\sin^3(\theta) + \sin(\theta) &= 2\left[1 - \sin^2(\theta)\right]\sin(\theta) - 2\sin^3(\theta) + \sin(\theta) \\
&= 2\sin(\theta) - 2\sin^3(\theta) - 2\sin^3(\theta) + \sin(\theta) \\
&= 3\sin(\theta) - 4\sin^3(\theta) \\
&= \sin(3\theta)
\end{aligned} \tag{2.44}$$

Así, el estado $|\psi_3\rangle$ resulta ser

$$|\psi_3\rangle = \cos(3\theta)|\alpha\rangle + \sin(3\theta)|\beta\rangle \tag{2.45}$$

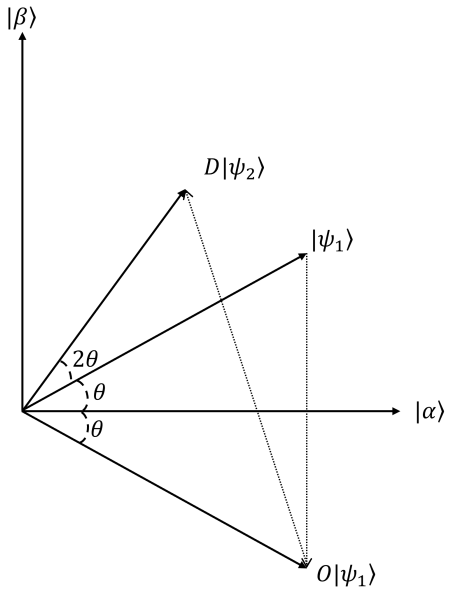

Figura 2.4: Aplicación del operador difusor al estado $|\psi_2\rangle$, el cual causa una rotación que acerca al estado $|\psi_3\rangle$ al eje representado por los estados solución $|\beta\rangle$.

Repitiendo la aplicación del operador oráculo se tiene una reflexión del estado $|\psi_3\rangle$ sobre el estado $|\alpha\rangle$, como se puede ver en la figura 2.5.

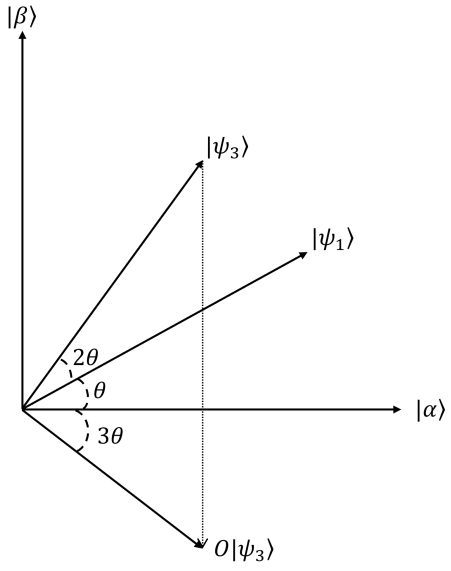

Figura 2.5: Aplicación del oráculo al estado $|\psi_3\rangle$.

El estado resultante $|\psi_4\rangle$ está dado por

$$|\psi_4\rangle = O\,|\psi_3\rangle = \cos(3\theta)\,|\alpha\rangle - \sin(3\theta)\,|\beta\rangle \tag{2.46}$$

La aplicación del operador difusor da como resultado

$$\begin{aligned} |\psi_5\rangle &= D\,|\psi_4\rangle = (2\,|\psi_1\rangle\,\langle\psi_1| - \ I)\,|\psi_4\rangle \\ &= \cos(5\theta)\,|\alpha\rangle + \sin(5\theta)\,|\beta\rangle \end{aligned} \tag{2.47}$$

que puede verse en la figura 2.6

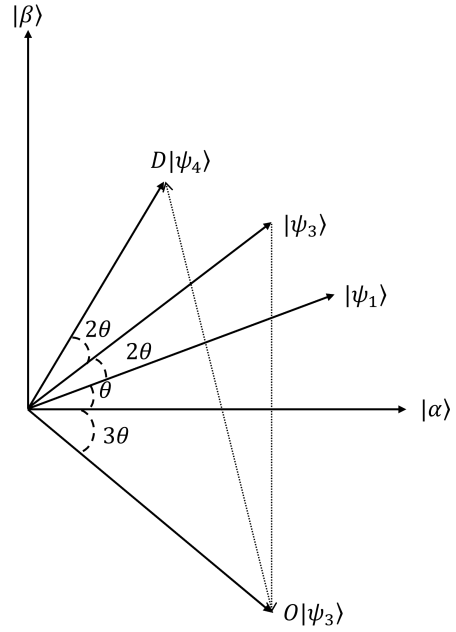

Figura 2.6: Aplicación del operador difusor al estado $|\psi_4\rangle$.

Es a partir de la aplicación del operador de Grover una cantidad t de veces que se tiene

$$G^t\,|\psi_1\rangle = \cos((2t+1)\theta)\,|\alpha\rangle + \sin((2t+1)\theta)\,|\beta\rangle \tag{2.48}$$

De esta forma se puede definir al operador G como una rotación de 2θ en el plano generado por los estados $|\alpha\rangle$ y $|\beta\rangle$, haciendo que el estado resultante de la aplicación de G se encuentre cerca del estado $|\beta\rangle$ con cada aplicación.

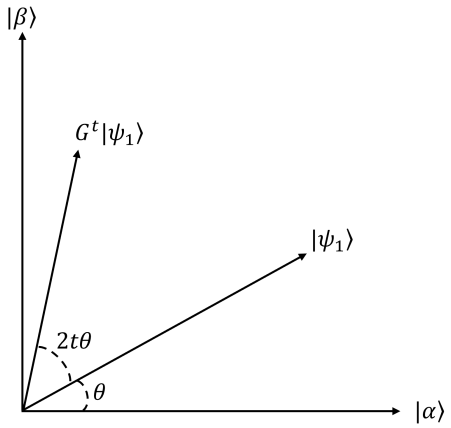

Figura 2.7: Aplicación del operador de Grover G, t veces al estado $|\psi_1\rangle$, de tal forma que este se aproxime al estado $|\beta\rangle$.

Conociendo como es que funciona el algoritmo de Grover solamente hace falta saber cuántas veces se debe aplicar G para que al realizar las mediciones correspondientes se obtenga al estado $|\beta\rangle$ con una probabilidad alta, y siguiendo el desarrollo geométrico del algortimo puede notarse que para obtener $|\beta\rangle$ se debe tener que

$$(2t+1)\theta \approx \frac{\pi}{2} \longrightarrow t \approx \frac{\pi}{4\theta} - \frac{1}{2} \tag{2.49}$$

y como t debe tomar como valor un número entero dado que representa la cantidad de veces que debe aplicarse G, lo que se puede hacer es suponer que $\frac{\pi}{4\theta}$ toma un valor entero y tomar que $t \approx \frac{\pi}{4\theta}$, siendo así que se toma el valor entero más cercano a t.

Además, considerando de la ecuación 2.37 el valor de θ es igual a

$$\theta = \arcsin\left(\sqrt{\frac{M}{N}}\right) \tag{2.50}$$

y tomando el caso en el que $N \gg M$, lo cual implica que $\frac{M}{N} \to 0$, así haciendo uso de la aproximación cuando $x \to 0$

$$\arcsin(x) \approx x \tag{2.51}$$

se tiene entonces que

$$\theta \approx \sqrt{\frac{M}{N}} \longrightarrow t \approx \frac{\pi}{4\sqrt{\frac{M}{N}}} = \frac{\pi}{4}\sqrt{\frac{N}{M}} \leq \sqrt{\frac{N}{M}} \tag{2.52}$$

Lo que indica que el operador de Grover debe aplicarse $O\left(\sqrt{\frac{N}{M}}\right)$ veces para el caso de M estados solución, mientras que para el caso de una sola solución $M = 1$, lo cual implica que G debe aplicarse $O\left(\sqrt{N}\right)$ veces.

2.2.2. Amplificación de Amplitudes

Una vez conociendo como funciona el algoritmo de Grover es muy sencillo entender el algoritmo de amplificación de amplitudes, el cual define al operador de Grover como

$$G = G(A, \chi) = -AS_0^{\phi}A^{-1}S_{\chi}^{\varphi} \tag{2.53}$$

donde el operador A, que es unitario, representa a un algoritmo cuántico cualquiera, que no utiliza mediciones y que genera un estado cualquiera en superposición que contiene todos los estados en los que se evalúa una función $\chi(x)$ sin importar si estos cumplen con la condición que vuelve una solución o no a cada estado en la que es evaluada. Este operador (algoritmo cuántico) se supone tiene una inversa A^{-1} y además es aplicado al estado $|0\rangle^{\otimes n}$ (con n la cantidad de qubits con la que se trabaje) generando a un estado $|\Psi\rangle$.

El operador S_{χ}^{φ} está definido como aquel que cambia de forma condicional la fase de los estados que componen $|\Psi\rangle$ por un factor φ de acuerdo con

$$|x\rangle \rightarrow \begin{cases} \varphi\,|x\rangle & si \quad \chi(x) = 1 \\ |x\rangle & si \quad \chi(x) = 0 \end{cases} \tag{2.54}$$

Finalmente, el operador S_0^{ϕ} cambia la fase de un estado que compone a $|\Psi\rangle$ por un factor de ϕ, si y sólo si el estado es el estado $|0\rangle$.

Es de esta forma que se tiene una generalización del algoritmo de Grover; que dependiendo del problema a tratar se asignan los valores de φ y ϕ. Para este trabajo de tesis se toman como valores aquellos que coincidan con la forma en la que son aplicados el operador oráculo y el operador difusor del algoritmo de Grover. Así, el valor que toman ambos parámetros es -1, siendo que A es la parte fundamental que construye al estado $|\Psi\rangle$ con el cual se planea amplificar la amplitud de aquellos estados solución que cumplan con la condición de la ecuación 2.54. De esta forma G es definido como

$$G = G_{AA} = -AS_0^{-1}A^{-1}S_{\chi}^{-1} = -AS_0A^{-1}S_{\chi} \tag{2.55}$$

donde G_{AA} es el operador de Grover definido para el objetivo de este trabajo de tesis, y los términos $-AS_0A^{-1}$ pueden ser vistos como el operador difusor del algoritmo de Grover, ya que la aplicación conjunta de estos hace lo que dicho operador.

2.3. Generación de K estados arbitrarios en superposición uniforme

A partir de los algoritmos presentados en las secciones 2.1 y 2.2 es posible generar un estado $|\Psi\rangle$ compuesto por la superposición uniforme de K estados arbitrarios, siendo este tipo de estados conocidos como estados cuánticos dispersos (sparse quantum states, en inglés) [11].

La generación de los K estados en superposición se puede lograr eliminando los estados no deseados pertenecientes a la superposición uniforme de M estados consecutivos, donde se debe cumplir que $M = 4K$, de tal forma que con la ayuda del algoritmo de amplificación de amplitudes se puedan eliminar los estados no deseados.

Definiendo al algoritmo para la generación de M estados consecutivos en superposición uniforme como el operador A del algoritmo de amplificación de amplitudes y aplicando el operador de

Grover una sola vez es posible generar una superposición de K estados arbitrarios en superposición uniforme. Así, los pasos para generar dicho estado son los siguientes:

1. Determinar el valor de M sabiendo que

$$M = 4K \tag{2.56}$$

2. Iniciar el registro cuántico con el que se trabaje en el estado

$$|\Psi_0\rangle = |0\rangle^{\otimes n} \tag{2.57}$$

   donde n es la cantidad de qubits del registro cuántico, la cual se calcula a partir del valor M, convirtiendo este número del sistema numérico decimal al sistema numérico binario (ver A.1), además, dependiendo de la forma en la que se implemente S_χ, añadir la cantidad de qubits auxiliares necesarios, si es que se requieren.

3. Aplicar el operador A, definido como el algoritmo revisado en la sección 2.1, con el cual se genera la superposición de M estados consecutivos en superposición uniforme, de tal forma que se tiene como resultado al estado

$$|\Psi_1\rangle = A\,|\Psi_0\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle \tag{2.58}$$

4. Aplicar el operador de Grover G_{AA} una sola vez (ecuación 2.55) al estado $|\Psi_1\rangle$

$$G_{AA}\,|\Psi_1\rangle = -AS_0A^{-1}S_\chi\,|\Psi_1\rangle \tag{2.59}$$

   La forma en la que los operadores que componen G_{AA} actúan puede separarse en dos pasos:

   a) Primero, el operador S_χ actúa sobre el estado $|\psi_1\rangle$, cambiando la fase de los estados que cumplen con la condición de la ecuación 2.54 por un factor de -1. Esto es lo mismo que ocurre en el paso II.*a* del algoritmo de búsqueda de Grover, por lo que se puede considerar al operador S_χ como aquel encargado de marcar los estados arbitrarios deseados, los cuales van a estar en superposición uniforme. Así, S_χ es equivalente al operador oráculo del algoritmo de Grover. De tal forma que se tiene como resultado al estado

$$|\Psi_2\rangle = S_\chi\,|\Psi_1\rangle = \frac{1}{\sqrt{M}} \left[\sum_{j \notin D} |j\rangle - \sum_{j \in D} |j\rangle \right] \tag{2.60}$$

   donde D es el conjunto en el que se encuentran los estados deseados.

   b) Una vez marcados los estados deseados se proceden a aplicar en conjunto los operadores $-AS_0A^{-1}$, los cuales pueden ser considerados en conjunto como el operador difusor del algoritmo de Grover, esto debido a que el operador S_0, al ser el encargado de cambiar la fase del estado 0 por un factor de -1, puede ser expresado de la siguiente forma

$$S_0 = I - 2\,|0\rangle\,\langle 0| \tag{2.61}$$

con I siendo la matriz identidad.

Esto se puede vefiricar y argumentar como correcto debido a la ortonormalidad de los estados base computacionales, de tal forma que al aplicar el operador S_0 a un estado culaquiera distinto de 0 el resultado es el mismo estado, dado que

$$\begin{aligned} S_0 |x\rangle &= [I - 2|0\rangle\langle 0|]|x\rangle = I|x\rangle - 2|0\rangle\langle 0|x\rangle \\ &= |x\rangle - 2\delta_{0,x}|x\rangle \\ &= \begin{cases} |x\rangle; & si \quad |x\rangle \neq |0\rangle, \quad dado\ que \quad \delta_{0,x} = 0 \\ |0\rangle - 2|0\rangle = -|0\rangle; & si \quad |x\rangle = |0\rangle, \quad dado\ que \quad \delta_{0,x} = 1 \end{cases} \end{aligned} \tag{2.62}$$

donde $\delta_{0,x}$ es la conocida delta de Kronecker [1]; además

$$\begin{aligned} A|\Psi_0\rangle &= |\Psi_1\rangle \\ \langle 0|A^{-1} &= \langle 0|A^\dagger = \langle \Psi_1| \end{aligned} \tag{2.63}$$

Al sustituir S_0 en la expresión $-AS_0A^{-1}$ se tiene que

$$\begin{aligned} -AS_0A^{-1} &= -A(I - 2|0\rangle\langle 0|)A^{-1} = -AIA^{-1} + 2A|0\rangle\langle 0|A^{-1} \\ &= 2A|0\rangle\langle 0|A^{-1} - AA^{-1} = 2|\Psi_1\rangle\langle\Psi_1| - I \end{aligned} \tag{2.64}$$

lo cual es equivalente al operador de difusión expuesto en el algoritmo de Grover (ecuación 2.32), con la diferencia de que en este caso el estado $|\Psi_1\rangle$ no es generado por medio de la aplicación de compuertas de Hadamard, sino que es generado a partir del operador A, definido para este trabajo como el algoritmo de la sección 2.1.

5. Obtener el estado $|\Psi\rangle$.

De esta forma, la aplicación de G_{AA} es equivalente a la aplicación de G, con la diferencia del estado generado al comienzo de cada algoritmo, dado que mientras en el algoritmo de búsqueda de Grover se genera dicho estado con compuertas Hadamard, las cuales generan la superposición de todos los estados base computaciones, para este trabajo se generan únicamente M estados en superposición uniforme sin ser necesariamente todos los estados base computacionales.

2.3.1. Deducción de la condición que satisface una sola aplicación del operador G_{AA} para la generación del estado $|\Psi\rangle$

Como ya fue mencionado en 2.3, la aplicación de G_{AA} es equivalente a la aplicación del operador G del algoritmo de búsqueda de Grover, por lo que, del análisis realizado en 2.2.1.1 se tiene que la cantidad de veces que G_{AA} debe ser aplicado está dada por la ecuación 2.49, sin embargo, para este caso esto no debe ser un valor aproximado, sino una igualdad, y además, como t está definida como la cantidad de veces que debe ser aplicado G_{AA}, esta debe tomar como valor 1, así

$$(2t+1)\theta = \frac{\pi}{2} \xrightarrow{t=1} (2(1)+1)\theta = 3\theta = \frac{\pi}{2} \rightarrow \theta = \frac{\pi}{6} \tag{2.65}$$

pero de la ecuación 2.50, que para este caso se sustituyen los valores $N \to M$ y $M \to K$, se tiene que

$$\theta = \arcsin\left(\sqrt{\frac{K}{M}}\right) \tag{2.66}$$

Sustituyendo θ en la ecuación 2.65 se obtiene como resultado

$$\arcsin\left(\sqrt{\frac{K}{M}}\right) = \frac{\pi}{6} \to \sin\left(\arcsin\left(\sqrt{\frac{K}{M}}\right)\right) = \sin\left(\frac{\pi}{6}\right) \to \sqrt{\frac{K}{M}} = \frac{1}{2} \tag{2.67}$$

de tal forma que para aplicar una sola vez el operador G_{AA} (se cumple que $t = 1$), se debe satisfacer que

$$\frac{K}{M} = \frac{1}{4} \longrightarrow M = 4K \tag{2.68}$$

Así, el valor que debe tomar M para realizar una sola aplicación de G_{AA} debe ser 4 veces la cantidad de estados en superposición que se deseen generar.

Capítulo 3

Simulación y resultados

A partir del algoritmo propuesto en la sección 2.3 se genera un estado en superposición de 21 estados, los cuales son el estado $|0\rangle$ y los estados que representan a los primeros 20 números pares, los cuales van del 2 al 40 en su representación decimal,sin embargo, este algoritmo funciona para una cantidad arbitraria de estados K. Además se implementa el circuito cuántico que representa este caso con ayuda de la librería qiskit, desarrollada por la empresa IBM [14].

3.1. Desarrollo y simulación de la generación de 21 estados arbitrarios en superposición

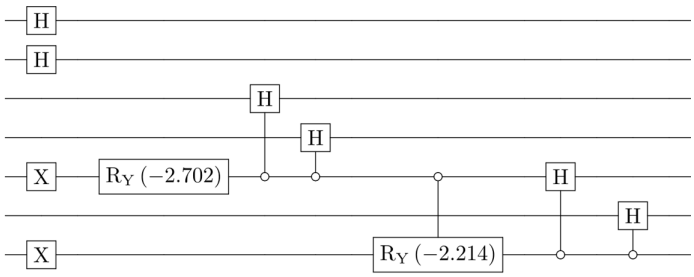

Figura 3.1: Circuito cuántico para la generación del estado $|\psi_1\rangle$.

Siguiendo los pasos del algoritmo propuesto para la generación de K estados arbitrarios en superposición, primero se debe calcular el valor de M el cual para este caso está determinado como

$$M = 4K = 4(21) = 84 \tag{3.1}$$

de esta forma, una vez conociendo el valor de M, se puede realizar su expansión binaria tal que

$$M = 84 = (1)2^6 + (0)2^5 + (1)2^4 + (0)2^3 + (1)2^2 + (0)2^1 + (0)2^0 = 2^6 + 2^4 + 2^2 = 64 + 16 + 4 \tag{3.2}$$

que en binario se expresa como

$$M = 1010100 \tag{3.3}$$

Una vez conocido M y la cantidad de qubits requeridos para representarlo (en este caso son 7), se tiene como estado inicial

$$|\Psi_0\rangle = |0\rangle^{\otimes 7} \tag{3.4}$$

De esta forma al aplicar el operador A, definido como el algoritmo de la sección 2.1, se tiene al estado $|\Psi_1\rangle$, cuyo circuito cuántico para su generación se puede observar en la figura 3.1, y que además, sus estados en superposición, al ser parte de los estados base computacionales, pueden ser representados en el sistema decimal. Así

$$|\Psi_1\rangle = \frac{1}{\sqrt{84}} \sum_{i=0}^{84-1=83} |i\rangle = \frac{1}{\sqrt{84}} \left(|0000000\rangle + |0000001\rangle + |0000010\rangle + \cdots |1010011\rangle + |1010100\rangle\right) \tag{3.5}$$

De tal forma que el estado resultante puede verse en la figura 3.2

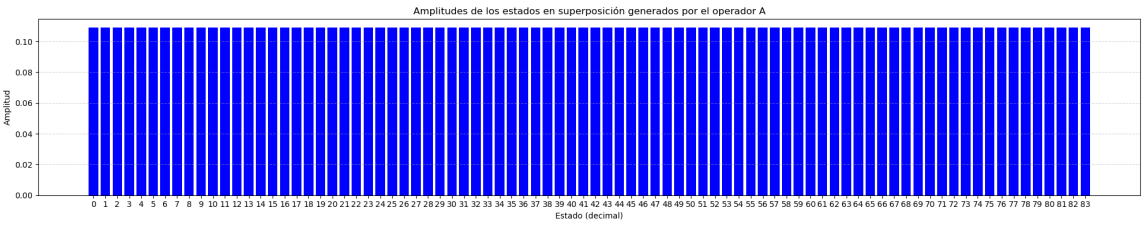

Figura 3.2: Gráfica que representa al estado $|\psi_1\rangle$

Una vez teniendo al estado $|\Psi_1\rangle$ (revisar A.3 para el desarrollo del algoritmo para la generación de $|\Psi_1\rangle$,) se procede a aplicar el operador S_χ el cual, para este caso, fue diseñado de tal forma que se requiere de un qubit en un registro auxiliar para que al construir el circuito cuántico de este operador se apliquen compuertas $Multi - CONTROL - NOT$ en las que los qubits de control sean todos los qubits del registro con el que se está trabajando y el qubit objetivo sea el qubit del registro auxiliar, así, el operador S_χ queda definido como se ve en la figura 3.3.

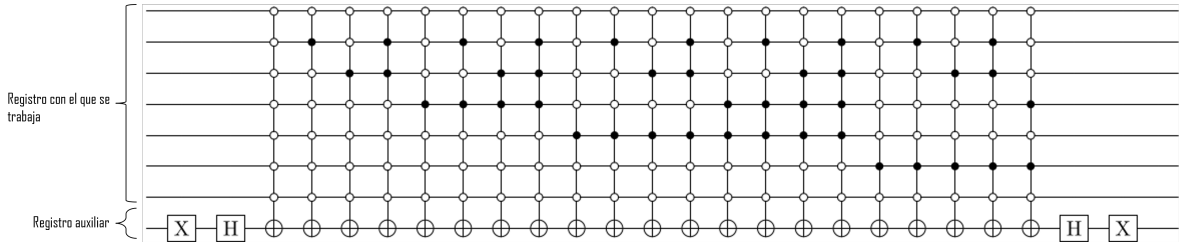

Figura 3.3: Circuito que representa al operador S_χ

Donde las compuertas $Multi - CONTROL - NOT$ que se ven con un circulo blanco requieren que el estado de ese qubit de control se encuentre en el estado $|0\rangle$ y los circulos negros requieren que

el qubit de control esté en el estado $|1\rangle$. De esta forma el estado resultante al aplicar el operador S_χ va a ser la superposición de los M estados consecutivos con los estados seleccionados para generar el estado de K estados en superposición, este estado resultante es el estado $|\Psi_2\rangle$, el cual puede verse representado en la figura 3.4.

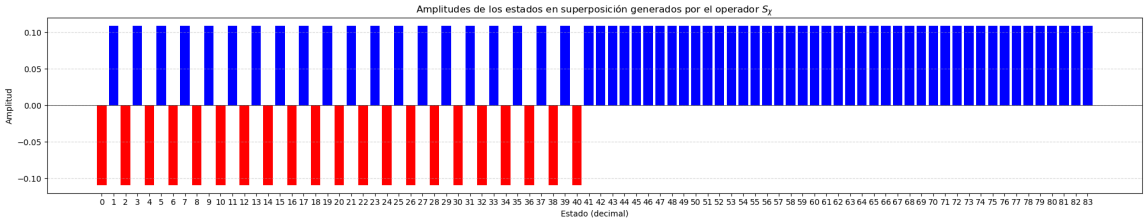

Figura 3.4: Gráfica que representa al estado $|\Psi_2\rangle$.

Finalmente, se aplican los operadores $-AS_0A^{-1}$ al estado $|\Psi_2\rangle$ y se obtiene el estado deseado $|\Psi\rangle$, el cual es la superposición de los 21 estados selecionados al inicio de esta sección. La figura 3.5 representa al circuito cuántico completo para la generación del estado $|\Psi\rangle$

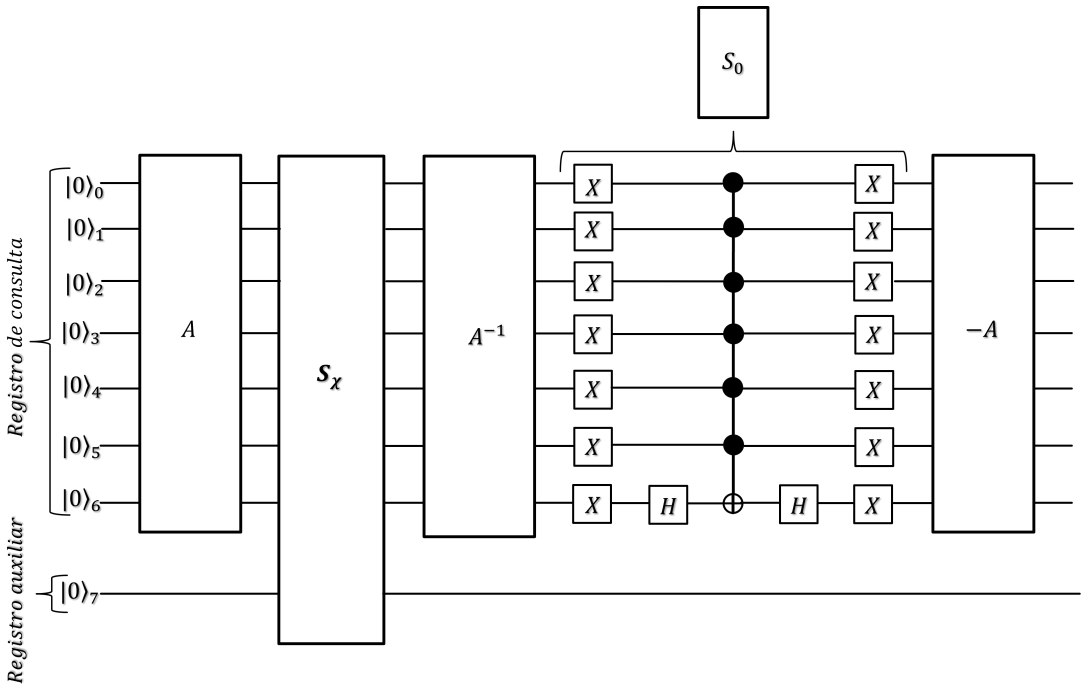

Figura 3.5: Circuito que representa la aplicación del operador A junto con el operador G_{AA}.

Finalmente, si se analiza la gráfica que representa al vector de estado resultante se puede observar que se tienen a los estados deseados, en superposición uniforme.

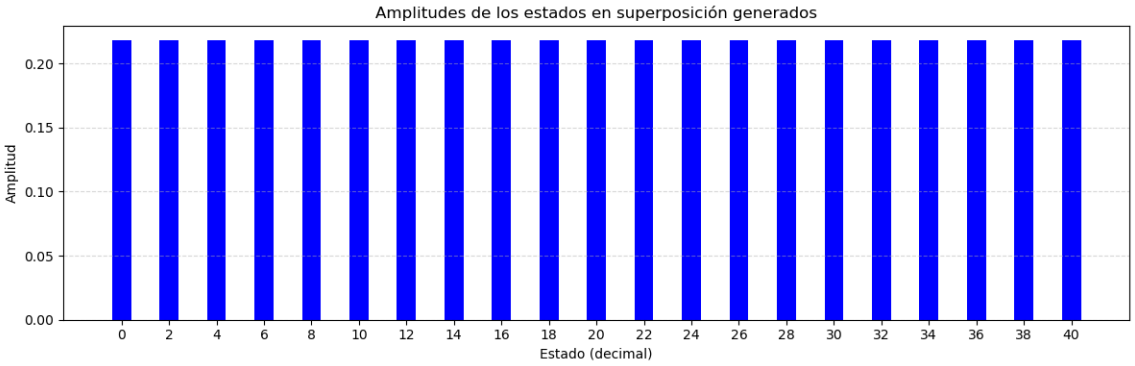

Figura 3.6: Gráfica que representa al estado $|\Psi\rangle$

A continuación se muestra el código utilizado para la implementación del algoritmo utilizando el paquete qiskit en su versión más reciente.

```
from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
import numpy as np
from qiskit.circuit.library import C3XGate ,XGate, MCXGate, RYGate, HGate,
    RZGate, GlobalPhaseGate
from qiskit.visualization import circuit_drawer
from qiskit.quantum_info import Statevector
from matplotlib import pyplot as plt

ch= HGate().control(ctrl_state="0")
x= - 2* np.arccos(np.sqrt(2**(4)/(84-4)))
CRYG = RYGate(x).control(ctrl_state="0")

sup_reg = QuantumRegister(7, 'sup_q')
superpo = QuantumCircuit(sup_reg)
superpo.x(sup_reg[4])
superpo.x(sup_reg[6])
superpo.h(sup_reg[0])
superpo.h(sup_reg[1])
superpo.append(RYGate(-2* np.arccos(np.sqrt(4/84))), [4])
superpo.append(ch, [4, 2])
superpo.append(ch, [4, 3])
superpo.append(CRYG,[4,6])
superpo.append(ch, [6, 4])
superpo.append(ch, [6, 5])

S = superpo.to_gate(label='Superposicion')
S_dagger = superpo.inverse().to_gate(label='Superposicion Inversa')
#-----------------------------------------------------------------------
orac_reg = QuantumRegister(8, 'orac_q')
Oracle = QuantumCircuit(orac_reg)
Oracle.x(orac_reg[7])
```

```
Oracle.h(orac_reg[7])
Oracle.append(MCXGate(7, ctrl_state="0000000"), [0, 1, 2, 3,4,5,6,7]) #1-0
Oracle.append(MCXGate(7, ctrl_state="0000010"), [0, 1, 2, 3,4,5,6,7]) #2-2
Oracle.append(MCXGate(7, ctrl_state="0000100"), [0, 1, 2, 3,4,5,6,7]) #3-4
Oracle.append(MCXGate(7, ctrl_state="0000110"), [0, 1, 2, 3,4,5,6,7]) #4-6
Oracle.append(MCXGate(7, ctrl_state="0001000"), [0, 1, 2, 3,4,5,6,7]) #5-8
Oracle.append(MCXGate(7, ctrl_state="0001010"), [0, 1, 2, 3,4,5,6,7]) #6-10
Oracle.append(MCXGate(7, ctrl_state="0001100"), [0, 1, 2, 3,4,5,6,7]) #7-12
Oracle.append(MCXGate(7, ctrl_state="0001110"), [0, 1, 2, 3,4,5,6,7]) #8-14
Oracle.append(MCXGate(7, ctrl_state="0010000"), [0, 1, 2, 3,4,5,6,7]) #9-16
Oracle.append(MCXGate(7, ctrl_state="0010010"), [0, 1, 2, 3,4,5,6,7]) #
    10-18
Oracle.append(MCXGate(7, ctrl_state="0010100"), [0, 1, 2, 3,4,5,6,7]) #
    11-20
Oracle.append(MCXGate(7, ctrl_state="0010110"), [0, 1, 2, 3,4,5,6,7]) #
    12-22
Oracle.append(MCXGate(7, ctrl_state="0011000"), [0, 1, 2, 3,4,5,6,7]) #
    13-24
Oracle.append(MCXGate(7, ctrl_state="0011010"), [0, 1, 2, 3,4,5,6,7]) #
    14-26
Oracle.append(MCXGate(7, ctrl_state="0011100"), [0, 1, 2, 3,4,5,6,7]) #
    15-28
Oracle.append(MCXGate(7, ctrl_state="0011110"), [0, 1, 2, 3,4,5,6,7]) #
    16-30
Oracle.append(MCXGate(7, ctrl_state="0100000"), [0, 1, 2, 3,4,5,6,7]) #
    17-32
Oracle.append(MCXGate(7, ctrl_state="0100010"), [0, 1, 2, 3,4,5,6,7]) #
    18-34
Oracle.append(MCXGate(7, ctrl_state="0100100"), [0, 1, 2, 3,4,5,6,7]) #
    19-36
Oracle.append(MCXGate(7, ctrl_state="0100110"), [0, 1, 2, 3,4,5,6,7]) #
    20-38
Oracle.append(MCXGate(7, ctrl_state="0101000"), [0, 1, 2, 3,4,5,6,7]) #
    21-40
Oracle.h(orac_reg[7])
Oracle.x(orac_reg[7])
O = Oracle.to_gate(label='Oracle')
#-----------------------------------------------------------------
qreg_q = QuantumRegister(8, 'q')
creg_c = ClassicalRegister(8, 'c')
Amplitude = QuantumCircuit(qreg_q,creg_c)

Amplitude.append(S,[0,1,2,3,4,5,6])

Amplitude.append(O,[0,1,2,3,4,5,6,7])

Amplitude.append(S_dagger,[0,1,2,3,4,5,6])

Amplitude.x(qreg_q[0])
Amplitude.x(qreg_q[1])
```

```
Amplitude.x(qreg_q[2])
Amplitude.x(qreg_q[3])
Amplitude.x(qreg_q[4])
Amplitude.x(qreg_q[5])
Amplitude.x(qreg_q[6])
Amplitude.h(qreg_q[6])
Amplitude.append(MCXGate(6), [0, 1, 2, 3,4,5,6])
Amplitude.h(qreg_q[6])
Amplitude.barrier()
Amplitude.x(qreg_q[0])
Amplitude.x(qreg_q[1])
Amplitude.x(qreg_q[2])
Amplitude.x(qreg_q[3])
Amplitude.x(qreg_q[4])
Amplitude.x(qreg_q[5])
Amplitude.x(qreg_q[6])

Amplitude.append(S,[0,1,2,3,4,5,6])
Amplitude.append(GlobalPhaseGate(np.pi))
sv = Statevector.from_instruction(Amplitude)

# Extraer amplitudes
states = sv.to_dict()

# Filtro: eliminar amplitudes ~0 y convertir etiquetas binarios a decimales
threshold = 1e-10
filtered = [(int(b, 2), np.real(a)) for b, a in states.items() if abs(a) >
    threshold]

# Separar en etiquetas y amplitudes
labels, amps = zip(*filtered)

# Graficar
plt.figure(figsize=(20, 4))
plt.bar(labels, amps, color=['blue' if a >= 0 else 'red' for a in amps])
plt.axhline(0, color='black', linewidth=0.5)
plt.ylabel('Amplitud')
plt.xlabel('Estado (decimal)')
plt.title('Amplitudes de los estados en superposicion generados')
plt.grid(axis='y', linestyle='--', alpha=0.5)
plt.xticks(labels, labels, rotation=0)
plt.tight_layout()
plt.show()
```

Listing 3.1: Código para la generación del estado $|\Psi\rangle$.

Capítulo 4

Conclusiones

Con este trabajo se logró construir un algoritmo capaz de generar K estados cuánticos arbitrarios en superposición uniforme, esto gracias a la implementación conjunta de los algoritmos propuestos por [20, 3, 5, 4, 12]. Además, dado que el algoritmo de amplificación de amplitudes tiene una complejidad de $O(\sqrt{\frac{M}{K}})$, la cual está establecida por la cantidad de veces que se aplica el operador G_{AA}; el que se aplique una sola vez este operador implica que la complejidad se transforma en $O(1)$.

Para el algoritmo de generación de M estados consecutivos se tiene una complejidad $O(\log_2(M))$ [20], de esta forma se tiene que la complejidad general del algoritmo propuesto en este trabajo es de $O(\log_2(M)) + O(1) = O(\log_2(M))$, esto debido a que para el caso que se aborda ($M = 4K$), $O(\log_2(M))$ es mayor que $O(1)$ y para conocer la complejidad del algoritmo se deben sumar las complejidades de cada parte de este, y acotar el comportamiento del resultado con una función mayor multiplicada por un factor c.

Sin embargo, la complejidad del algoritmo puede verse modificada de forma importante dependiendo de como se construya el operador S_χ, siendo así que este algoritmo a pesar de generar un estado en superposición de K estados arbitrarios puede no ser eficiente al implementar un oráculo con una complejidad mayor a $O(\log_2(M))$.

Apéndice A

Desarrollos y conceptos complementarios

A.1. Conversión entre sistemas numéricos

En el sistema decimal se trabaja en la base 10, esto quiere decir que para representar cualquier número en este sistema se debe realizar una suma de multiplicaciones en las que se debe multiplicar un número x_i en el conjunto $1, 2, 3, \ldots, 8, 9$ por 10 elevado a una potencia i. De esta forma cualquier número decimal positivo puede ser expresado como

$$\begin{aligned} x &= x_i 10^i + x_{i-1} 10^{i-1} + \cdots + x_2 10^2 + x_1 10^1 + x_0 10^0 \\ &= \sum_i x_i 10^i \end{aligned} \tag{A.1}$$

El sistema numérico binario se basa en la representación de todos los números reales utilizando la base 2 en lugar de la base 10, la cual es utilizada para representar los números tal y como los conocemos [2]. Así, cualquier número x que necesita n bits para ser representado en el sistema binario, tiene como su expansión binaria la expresión

$$\begin{aligned} x &= x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_k 2^{n-k} + \cdots + x_{n-1} 2^1 + x_n 2^0 \\ &= \sum_{j=1}^{n} x_j 2^{n-j} \end{aligned} \tag{A.2}$$

con $x_j = 0, 1$

Además, para la representación binaria del número x se tiene

$$x = x_{n-1} x_{n-2} x_{n-3} \cdots x_{n-k} \cdots x_1 x_0 \tag{A.3}$$

donde los términos $x_i = 0, 1$ y de la ecuación A.2 los terminos x_j toman su posición en la ecuación A.3 de acuerdo al valor de la potencia del número 2 en la ecuación A.2, así si x_k es igual a 1, el término $x_{n-k} = 1$(y si x_k es igual a 0, el término $x_{n-k} = 0$) de la ecuación A.3.

n puede ser calculado tomando al numero entero más cercano, menor o igual al resultado de calcular $\log_2(x)$ (esto puede ser expresado con el símbolo matemático $\lfloor\rfloor$) y sumarle al resultado un 1, así

$$n = \lfloor \log_2(x) \rfloor + 1 \tag{A.4}$$

Así, a través de la ecuación A.2 es posible convertir un número decimal x a su representación binaria.

A.2. Suma módulo 2

El símbolo matemático $\oplus$ representa la suma módulo 2. Esta no es más que un caso específico de la aritmética modular, la cual puede verse como la aritmética de los residuos [17]. En la artimética modular se toman dos números enteros positivos, x y n que pueden escribirse de forma única como

$$x = kn + r \tag{A.5}$$

donde k es un entero positivo, definido como el resultado de dividir x entre n, y r es el residuo de la división (si es que hay), que se encuentra entre los valores 0 a $n-1$. De esta forma se usa la notación $mod(n)$ para indicar que se está trabajando en la aritmética modular con respecto al número n, que para este caso está dado como el número 2. La forma de visualizar como funciona la suma módulo 2 de una forma sencilla es utilizando la compuerta XOR, una compuerta lógica muy conocida en la computación clásica, la cual actúa de la siguiente forma:

$$\begin{aligned} 1 \oplus 1 &= 0 \\ 1 \oplus 0 &= 1 = 0 \oplus 1 \\ 0 \oplus 0 &= 0 \end{aligned} \tag{A.6}$$

A.3. Desarrollo del algoritmo para la generación del estado compuesto por la superposición de uniforme de 84 estados $|\Psi_1\rangle$

Para la generación del estado $|\Psi_1\rangle$ de la ecuación 3.5 se deben seguir los pasos del algoritmo propuesto en la sección 2.1, de esta forma se tiene para cada paso lo siguiente:

1. Se calculan los valores $l_0, l_1, \ldots, l_k$, los cuales se obtienen a partir de la ecuación 3.2. De esta forma se tiene que

$$\begin{aligned} l_0 &= 2 \\ l_1 &= 4 \\ l_2 &= 6 \end{aligned} \tag{A.7}$$

2. Se inicia al estado $|\Theta_0\rangle$ como

$$|\Theta_0\rangle = |0\rangle_6 |0\rangle_5 |0\rangle_4 |0\rangle_3 |0\rangle_2 |0\rangle_1 |0\rangle_0 = |0\rangle^{\otimes 7} \tag{A.8}$$

3. Se aplica la compuerta X en los qubits $|q\rangle_i$ para $i = l_1, l_2 = 4, 6$, de esta forma

$$|\Theta_1\rangle = X_4 X_6 |0\rangle^{\otimes 7} = |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |0\rangle_1 |0\rangle_0 \tag{A.9}$$

4. Se establece $M_0 = 2^{l_0} = 2^2 = 4$.

5. Dado que $l_0 > 0$, se deben aplicar compuertas de Hadamard en los qubits $|q\rangle_i$ para $i = 0, 1$. Así

$$|\Theta_2\rangle = H_0 H_1 |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |0\rangle_1 |0\rangle_0 = |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0 \tag{A.10}$$

6. Se aplica la compuerta de rotación $R_Y(\theta_0)$ en el qubit $|q\rangle_{l_1} = |q\rangle_4$ donde se tiene que

$$\theta_0 = -2 \arccos\left(\sqrt{\frac{M_0}{M}}\right) = -2 \arccos\left(\sqrt{\frac{4}{84}}\right) \approx -2{,}7 \tag{A.11}$$

de esta forma la aplicación de la compuerta $R_Y(\theta_0)$ da como resultado al estado

$$\begin{aligned} |\Theta_3\rangle &= R_Y(\theta_0)_4 |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0 \\ &= a_0 |1\rangle_6 |0\rangle_5 |0\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0 + b_0 |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0 \end{aligned} \tag{A.12}$$

7. Ahora, se debe aplicar una compuerta Control-Hadamard en los qubits $|q\rangle_i$ para $i = l_0, l_0 + 1, \ldots l_1 - 1 = 2, 3$, con el qubit $|q\rangle_{l_1} = |q\rangle_4$ siendo el qubit de control, que además debe encontrarse en el estado $|0\rangle$. Así

$$\begin{aligned} |\Theta_4\rangle &= \left(CH_2^{q_4=0}\right)\left(CH_3^{q_4=0}\right)(a_0 |1\rangle_6 |0\rangle_5 |0\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0 + b_0 |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0) \\ &= a_0 |1\rangle_6 |0\rangle_5 |0\rangle_4 |+\rangle_3 |+\rangle_2 |+\rangle_1 |+\rangle_0 + b_0 |1\rangle_6 |0\rangle_5 |1\rangle_4 |0\rangle_3 |0\rangle_2 |+\rangle_1 |+\rangle_0 \end{aligned} \tag{A.13}$$

8. Para $m = 1$ a $k - 1 = 2 - 1 = 1$, por lo que solamente se tiene que para $m = 1$:

   a) Se aplica un compuerta Control-Rotación $CR_Y(\theta_m) = CR_Y(\theta_1)$ en el qubit $|q\rangle_{l_{m+1}} = |q\rangle_{l_{1+1}} = |q\rangle_{l_2} = |q\rangle_6$ condicionado a que el qubit de control, $|q\rangle_{l_m} = |q\rangle_{l_1} = |q\rangle_4$ se encuentre en el estado $|0\rangle$. Donde se tiene que

$$\begin{aligned} \theta_1 &= -2 \arccos\left(\sqrt{\frac{2^{l_1}}{M - M_{1-1}}}\right) \\ &= -2 \arccos\left(\sqrt{\frac{2^4}{84 - M_0}}\right) \\ &= -2 \arccos\left(\sqrt{\frac{16}{84 - 4}}\right) \approx -2{,}21 \end{aligned} \tag{A.14}$$

De esta forma con la aplicación de la compuerta Control-Rotación, se tiene al estado

$$\begin{aligned}|\Theta_5\rangle &= CR_Y(\theta_1)_6^{q_4=0}\left(a_0\,|1\rangle_6\,|0\rangle_5\,|0\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0 + b_0\,|1\rangle_6\,|0\rangle_5\,|1\rangle_4\,|0\rangle_3\,|0\rangle_2\,|+\rangle_1\,|+\rangle_0\right)\\ &= a_0a_1\,|0\rangle_6\,|0\rangle_5\,|0\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0 + a_0b_1\,|1\rangle_6\,|0\rangle_5\,|0\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0\\ &\quad + b_0\,|1\rangle_6\,|0\rangle_5\,|1\rangle_4\,|0\rangle_3\,|0\rangle_2\,|+\rangle_1\,|+\rangle_0\end{aligned} \tag{A.15}$$

b) Se aplica compuertas Control-Hadamard en los qubits $|q\rangle_i$ para $i = l_m, l_m+1, \ldots l_{m+1}-1 = l_1, l_1+1, \ldots l_2 - 1 = 4, 5$, donde el qubit de control $|q\rangle_{l_{m+1}} = |q\rangle_{l_{1+1}} = |q\rangle_{l_2} = |q\rangle_6$ debe encontrarse en el estado $|0\rangle$. Así

$$\begin{aligned}|\Theta_6\rangle &= \left(CH_4^{q_6=0}\right)\left(CH_5^{q_6=0}\right)[a_0a_1\,|0\rangle_6\,|0\rangle_5\,|0\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0\\ &\quad + a_0b_1\,|1\rangle_6\,|0\rangle_5\,|0\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0 + b_0\,|1\rangle_6\,|0\rangle_5\,|1\rangle_4\,|0\rangle_3\,|0\rangle_2\,|+\rangle_1\,|+\rangle_0]\\ &= a_0a_1\,|0\rangle_6\,|+\rangle_5\,|+\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0 + a_0b_1\,|1\rangle_6\,|0\rangle_5\,|0\rangle_4\,|+\rangle_3\,|+\rangle_2\,|+\rangle_1\,|+\rangle_0\\ &\quad + b_0\,|1\rangle_6\,|0\rangle_5\,|1\rangle_4\,|0\rangle_3\,|0\rangle_2\,|+\rangle_1\,|+\rangle_0\end{aligned} \tag{A.16}$$

c) Se establece $M_1 = M_{1-1} + 2^{l_1} = M_0 + 2^4 = 4 + 16 = 20$.

9. Finalmente, si se sustituyen los valores para los estados $|+\rangle$ y los valores de las amplitudes a_0, a_1, b_0 *y* b_1 de la ecuación A.16 se puede notar que el estado $|\Theta_6\rangle$ no es más que el estado $|\Psi_1\rangle$ de la ecuación 3.5. Para esto se tiene que

$$\begin{aligned}a_0 &= -\sin\left(\frac{\theta_0}{2}\right) = -\sin\left(\frac{-2\arccos\left(\sqrt{\frac{4}{84}}\right)}{2}\right) = \sqrt{1-\frac{4}{84}}\\ b_0 &= \cos\left(\frac{\theta_0}{2}\right) = \cos\left(\frac{-2\arccos\left(\sqrt{\frac{4}{84}}\right)}{2}\right) = \sqrt{\frac{4}{84}}\\ a_1 &= -\sin\left(\frac{\theta_1}{2}\right) = -\sin\left(\frac{-2\arccos\left(\sqrt{\frac{16}{80}}\right)}{2}\right) = \sqrt{1-\frac{16}{80}}\\ b_1 &= \cos\left(\frac{\theta_1}{2}\right) = \cos\left(\frac{-2\arccos\left(\sqrt{\frac{16}{80}}\right)}{2}\right) = \sqrt{\frac{16}{80}}\end{aligned} \tag{A.17}$$

De esta forma al sustituir estos valores y los estados $|+\rangle$ en la ecuación A.16 se tiene

$$\begin{aligned}|\Theta_6\rangle &= \sqrt{1-\frac{4}{84}}\sqrt{1-\frac{16}{80}}\frac{1}{\sqrt{2^6}}\,|0\rangle_6\,(|0\rangle_5+|1\rangle_5)\,(|0\rangle_4+|1\rangle_4)\,(|0\rangle_3+|1\rangle_3)\,(|0\rangle_2+|1\rangle_2)\,(|0\rangle_1+|1\rangle_1)\,(|0\rangle_0+|1\rangle_0)\\ &\quad + \sqrt{1-\frac{4}{84}}\sqrt{\frac{16}{80}}\frac{1}{\sqrt{2^4}}\,|1\rangle_6\,|0\rangle_5\,|0\rangle_4\,(|0\rangle_3+|1\rangle_3)\,(|0\rangle_2+|1\rangle_2)\,(|0\rangle_1+|1\rangle_1)\,(|0\rangle_0+|1\rangle_0)\\ &\quad + \sqrt{\frac{4}{84}}\frac{1}{\sqrt{2^2}}\,|1\rangle_6\,|0\rangle_5\,|1\rangle_4\,|0\rangle_3\,|0\rangle_2\,(|0\rangle_1+|1\rangle_1)\,(|0\rangle_0+|1\rangle_0)\end{aligned}$$

(A.18)

donde el producto de las amplitudes para cada término de la ecuación A.18 es

$$\begin{aligned} a_0 a_1 \frac{1}{\sqrt{2^6}} &= \sqrt{1-\frac{4}{84}}\sqrt{1-\frac{16}{80}}\frac{1}{\sqrt{2^6}} = \sqrt{\frac{80}{84}}\sqrt{\frac{64}{80}}\frac{1}{\sqrt{64}} = \sqrt{\frac{(80)(64)1}{(84)(80)(64)}} = \sqrt{\frac{1}{84}} \\ a_0 b_1 \frac{1}{\sqrt{2^4}} &= \sqrt{1-\frac{4}{84}}\sqrt{\frac{16}{80}}\frac{1}{\sqrt{2^4}} = \sqrt{\frac{80}{84}}\sqrt{\frac{16}{80}}\frac{1}{\sqrt{16}} = \sqrt{\frac{(80)(16)1}{(84)(80)(16)}} = \sqrt{\frac{1}{84}} \\ b_0 \frac{1}{\sqrt{2^2}} &= \sqrt{\frac{4}{84}}\frac{1}{\sqrt{4}} = \sqrt{\frac{4(1)}{84(4)}} = \sqrt{\frac{1}{84}} \end{aligned} \tag{A.19}$$

De esta forma al tener que el producto de las amplitudes es el mismo para cada término, secumple que existe una superposición uniforme de estados y, al desarrollar el producto de todos los estados que conforman $\sqrt{\frac{1}{84}}$ se tiene que $|\Theta_6\rangle = |\Psi_1\rangle$. Además, el circuito para la generación de $|\Psi_1\rangle$ puede verse en la figura 3.1.

Bibliografía

[1] George B Arfken, Hans J Weber, and Frank E Harris. *Mathematical methods for physicists a comprehensive guide*. Amsterdam (Holanda) Elsevier, 2013.

[2] Belal E. Baaquie and Leong-Chuan Kwek. *Quantum Computers*. Springer Nature, 01 2023.

[3] Gilles Brassard and Peter Hoyer. An exact quantum polynomial-time algorithm for simon's problem. *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*, page 12–23, 1997.

[4] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *arXiv:quant-ph/0005055*, 305:53–74, 2002.

[5] Gilles Brassard, Peter Hoyer, and Alain Tapp. Quantum counting. *Lecture Notes in Computer Science*, 1443:820–831, 05 1998.

[6] Barry Burd. *Quantum Computing Algorithms*. Packt Publishing Ltd, 09 2023.

[7] Goong Chen, Stephen A. Fulling, Hwang Lee, and Marlan O. Scully. Grover's algorithm for multiobject search in quantum computing. *Springer eBooks*, 561:165–175, 11 2007.

[8] Claude Cohen-Tannoudji, Bernard Diu, Franck Laloeì, Susan Reid Hemley, Nicole Ostrowsky, and Dan Ostrowsky. *Quantum mechanics. Volume I, Basic concepts, tools, and applications*. Wiley-Vch, 2020.

[9] Leonidas Deligiannidis. Explaining grover's quantum algorithm to college students. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, pages 1650–1657, 07 2023.

[10] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 06 1982.

[11] Niels Gleinig and Torsten Hoefler. An efficient algorithm for sparse quantum state preparation. pages 433–438, 11 2021.

[12] Lov K Grover. A fast quantum mechanical algorithm for database search. *arXiv (Cornell University)*, 01 1996.

[13] Chenxi Guo. Grover's algorithm – implementations and implications. *Highlights in Science Engineering and Technology*, 38:1071–1078, 03 2023.

[14] IBM Quantum. Qiskit - an open-source framework for quantum computing, 2024.

[15] Diana Jingle, Shylu Sam, Mano Paul, Ananth Jude, and Daniel Selvaraj. Design of grover's algorithm over 2, 3 and 4-qubit systems in quantum programming studio. *International Journal of Electronics and Telecommunications*, 68, 07 2023.

[16] Aamir Mandviwalla, Keita Ohshiro, and Bo Ji. Implementing grover's algorithm on the ibm quantum computers. *2018 IEEE International Conference on Big Data (Big Data)*, 12 2018.

[17] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 12 2010.

[18] Rajiv Pandey, Nidhi Srivastava, Neeraj K. Singh, and Kanishka Tyagi, editors. *Quantum Computing: A Shift from Bits to Qubits*. Springer Nature, 04 2023.

[19] Eleanor Rieffel and Wolfgang Polak. *Quantum computing : a gentle introduction*. Mit Press, 2011.

[20] Alok Shukla and Prakash Vedula. An efficient quantum algorithm for preparation of uniform quantum superposition states. *Quantum Information Processing*, 23, 01 2024.

[21] Robert S. Sutor. *Dancing with Qubits : How quantum computing works and how it may change the world*. Packt Publishing Limited, 2019.

[22] Paweł J. Szabłowski. Understanding mathematics of grover's algorithm. *Quantum Information Processing*, 20, 05 2021.

[23] Dinesh R. Vemula, Debanjan Konar, Sudeep Satheesan, Sri M. Kalidasu, and Attila Cangi. A scalable 5,6-qubit grover's quantum search algorithm, 04 2022.

[24] Hiu Y. Wong. *Introduction to Quantum Computing*. Springer Nature, 09 2023.

[25] Thomas G. Wong. *Introduction to classical and quantum computing*. Rooted Groove. Copyright, 2022.