Algoritmos cuánticos y matrices singulares tripotentes.

por

Juan Manuel Amezcua Ortega.

Tesis presentada en cumplimiento parcial de los requisitos
para la obtención del grado de

Maestro en Ciencias de la Computación

Benemérita Universidad Autónoma de Puebla, Facultad de Ciencias de la Computación

Asesores:
Dr. César Bautista Ramos
Dr. Daniel Alejandro Valdés Amaro

Puebla, Pue. México, octubre 2012.

Índice general

Agradecimientos

En primer lugar quiero agradecer a Dios de quien viene todo don, a mis padres por el don de la vida y a mis maestros por ensearme a vivirla. En segundo lugar quiero mencionar que este trabajo de tesis fue posible gracias a la ayuda de mi asesor el Dr. César Bautista Ramos y mi coasesor el Dr. Daniel Alejandro Valdés Amaro, quienes en todo momento me apoyaron y guiaron en este trabajo de investigación. Gracias también a los que formaron parte de mi comite de tesis, el Dr. Carlos Guillen Galván, el Dr. José Alejandro Rangel Huerta y la Dra. Blanca Bermúdez Juárez por sus enseanzas y consejos. De igual manera quiero hacer un reconocimiento especial a todos los maestros que participaron en mi formación durante el tiempo que estuve estudiando la maestria en ciencias de la computación en la Benemérita Universidad Autónoma de Puebla.

Índice de figuras

Acrónimos y abreviaturas

AAC	Algoritmo amplificación de amplitud cuántica.
D	Algoritmo de Deutsch.
DJ	Algoritmo de Deutsch-Josza.
EPR	Einstein-Podolsky-Rosen.
RW	Caminatas Aleatorias (Random Walks).

Símbolos y notación

a	Probabilidad de éxito de un algoritmo, con $0 < a < 1$.
A	Matriz de preparación en la computadora cuántica.
α	Valor esperado, valor promedio ó primer momento de probabilidad ($\alpha = \langle X \vert P \vert X \rangle$).
β	Segundo momento de probabilidad ($\beta = \langle X \vert P^2 \vert X \rangle$).
$\beta - \alpha^2$	Varianza.
$\sqrt{\beta - \alpha^2}$	Desviación estandar.
$\langle X \vert$	Bra X.
$\langle X \vert X \rangle$	Braket X.
ψ_i	Cualquier estado del algoritmo.
ψ_0	El estado inicial del algoritmo.
ψ_n	El estado final del algoritmo.
φ	Ángulo de marcado.
ϕ	Ángulo de difusión.
D	Matriz de difusión.
F	Transformada cuántica de Fourier.
G	Operador de Grover.
Id	Matriz identidad.
$\vert X \rangle$	Ket X.
$\vert X \rangle \langle X \vert$	Ketbra X.
M	Matriz de marcado.
N	Matriz de negación.
P	Matriz de coeficientes.
Q	Operador generalizado de Grover.
U	Matriz unitaria.

Capítulo 1

Introducción

El presente proyecto trata de computación cuántica. La computación cuántica consiste en el estudio del procesamiento de la información utilizando los sistemas de la mecánica cuántica. La mecánica cuántica es un marco matemático; es decir, un conjunto de teoremas para la construcción de teorías físicas [10].

Cabe mencionar que en este trabajo de investigación se mencionarán algunos conceptos físicos de la mecánica cuántica, sin embargo, debemos aclarar que nuestra propuesta no se enfocará a los aspectos físicos (hardware) de la computación cuántica, sino que tocará lo referente a los algoritmos (software) que se pueden implementar en una computadora cuántica.

La información que se presenta en este capítulo, se basa en su mayor parte en el libro de Nielsen y Chuang [10].

Los origenes de la computación cuántica estan basados en las ideas de Richard Feymann, quien en 1982, usó los conceptos de la mecánica cuántica para hacer cálculos de forma eficiente y rápida [6]. Podemos decir que la computación cuántica es un conjunto de normas dentro de un marco teórico; es decir, el arte de usar un conjunto de postulados básicos que rigen la teoría de la información cuántica, en nuestro caso en específico del software cuántico.

La popularidad de la computación cuántica se vió incrementada con el descubrimiento de un algoritmo cuántico eficiente para la factorización de números enteros muy grandes, diseñado por Peter Shor en 1994, este suceso cuestionó la fortaleza de los algoritmos criptográficos que basan su seguridad en la dificultad para factorizar un número entero muy grande.

Después del algoritmo cuántico de Shor, le sigue en importancia el algoritmo cuántico de Grover que sirve para hacer búsquedas en bases de datos llamadas *no estructuradas.* Este último algoritmo es cuadráticamente más veloz que sus contrapartes clásicas.

En la década de 1980, surgió el interés por utilizar efectos cuánticos más rápidos que la luz, pero de acuerdo con la teoría de la relatividad de Einstein, esto no es posible.

La posibilidad clonar un estado cuántico desconocido, depende de la utilización de un efecto cuántico más rápido que la luz, pero como no es posible tener una señal más rápida que la luz, entonces, no es possible construir una copia de un estado cuántico dentro de la mecánica cuántica.

El teorema de no clonación es uno de los primeros resultados de la computación cuántica [10], y a partir de dicho teorema se han desarrollado otros conceptos, ahora se tienen las herramientas conceptuales que permiten comprender hasta qué punto, un dispositivo de clonación cuántica podría funcionar. Estas herramientas, a su vez, se han aplicado para comprender otros aspectos de la mecánica cuántica.

Desde la década de 1970, muchas técnicas para regular los sistemas cuánticos se han desarrollado. Por ejemplo, se desarrollaron métodos para la captura de un sólo átomo en una *trampa de átomos*, aislándolo del resto del mundo, lo que nos permite sondear los diferentes aspectos de su comportamiento con una precisión increíble. El microscopio de efecto túnel se ha utilizado para mover átomos individuales, creando así, aparatos electrónicos, cuyo funcionamiento implica la transferencia de electrones individuales y el diseño de arreglos de átomos a voluntad. Se ha logrado modificar cada átomo del areglo al cambiar su estado energético.

La capacidad de control individual de los sistemas cuánticos es esencial para aprovechar el poder de la mecánica cuántica en aplicaciones que tengan que ver con la información cuántica. Sin embargo, los esfuerzos por construir sistemas de procesamiento de información cuántica se han traducido en un éxito modesto hasta la fecha.

Pequeños computadores cuánticos, capaces de hacer docenas de operaciones con pocos bits cuánticos (qubits) representan el estado del arte en la computación cuántica. Nótese que la unidad mínima de información en computación cuántica se llama qubit.

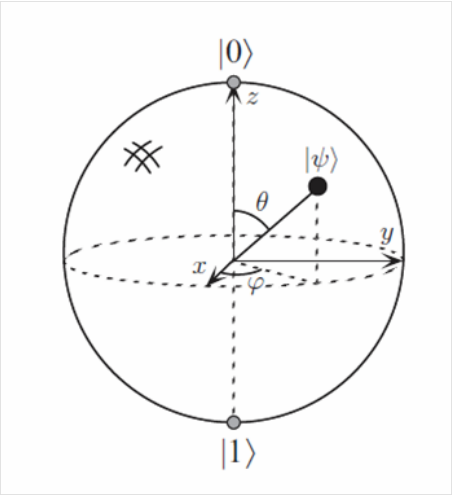

Figura 1.1: Representación geométrica de un qubit a través de la esfera de Bloch.

Prototipos experimentales para hacer criptografía cuántica, es decir, comunicarse en secreto a través de largas distancias, se han demostrado a un nivel que puede ser útil para algunas aplicaciones en el mundo real. Sin embargo, sigue siendo un gran reto para los

físicos e ingenieros del futuro, desarrollar técnicas para el procesamiento de información cuántica a gran escala.

Cabe recordar que Alan Turing en 1936 desarrolló en detalle la noción de lo que hoy llamaríamos una computadora programable, un modelo para el cálculo que ahora se le conoce como la máquina de Turing, el mismo Turing demostró que la Máquina Universal de Turing se puede utilizar para simular cualquier otra máquina de Turing. Por otra parte, afirmó que tal máquina universal lleva a cabo una tarea por medio de algoritmos, es decir, si un algoritmo se puede realizar en determinado hardware (por ejemplo, una computadora personal moderna), entonces existe un algoritmo equivalente en una Máquina Universal de Turing, que realiza exactamente la misma tarea que el algoritmo que se ejecuta en el ordenador personal. Esta afirmación, conocida como la tesis de Church-Turing en honor a Turing y otro de los pioneros de la informática, Alonzo Church, afirma la equivalencia entre el hardware programable y los algoritmos del concepto matemático riguroso de la Máquina Universal de Turing.

La amplia aceptación de la tesis de la máquina de Alan Turing, sentó las bases para el desarrollo de la teoría de la informática. No mucho después de las aportaciones de Turing, las primeras computadoras fueron construidos a partir de componentes electrónicos. John Von Neumann desarrolló un modelo teórico simple para ensamblar de una manera práctica todos los componentes necesarios para armar una computadora funcional, que sea capaz de hacer lo que una Máquina Universal de Turing puede realizar.

El desarrollo del hardware se ha realizado rápidamente, desde 1947, cuando John Bardeen, Walter Brattain y Shockley desarrollaron el transistor, por lo que el crecimiento de la computación fue descrito por Gordon Moore en 1965 en lo que se conoce como la ley de Moore, que afirma que el poder de las computadoras se duplicará cada dos años. Los enfoques convencionales para la fabricación de la tecnología informática están comenzando a llegar al límite de la miniaturización de los componentes electrónicos, y los efectos cuánticos están empezando a interferir en el funcionamiento de los dispositivos electrónicos, ya que se hacen cada vez más pequeños. Una posible solución al problema planteado es pasar a un paradigma de computación distinto, la teoría de la computación cuántica, que se basa en la idea de usar la mecánica cuántica para realizar cálculos, en lugar de la física clásica.

Una computadora convencional no puede simular de manera eficiente una computadora cuántica, las computadoras cuánticas ofrecen un elemento esencial en la velocidad para realizar cálculos, mostrando una ventaja sobre las computadoras clásicas. Esta ventaja de la velocidad es tan importante que muchos de los investigadores creen que ninguna cantidad de avances en la computación clásica va a ser capaz de superar la brecha entre la potencia de una computadora clásica y el poder de una computadora cuántica.

En los años posteriores a Turing, muchos investigadores se dieron cuenta de que ciertos tipos de computadoras analógicas pueden resolver problemas de manera eficiente, y que dichos problemas no tienen una solución eficiente en una máquina de Turing. Por desgracia para la computación analógica, resulta que la presencia del ruido en este tipo de computadoras afecta considerablemente, por lo que los efectos de tal ruido se deben tener en cuenta para la evaluación de la eficiencia de un modelo computacional.

Uno de los grandes retos de la computación e información cuántica es controlar la presencia de ruido, dicho reto fue superado con éxito por el desarrollo de una teoría cuántica de códigos de corrección de errores y tolerancia a fallos. Por lo tanto, a diferencia de la computación analógica, la computación cuántica puede tolerar, en principio, un número finito de cantidad de ruido y aún conservan sus ventajas computacionales.

Un gran reto surgió a mediados de 1970: crear un algoritmo para determinar con certeza si un entero dado es primo o compuesto. Pero sólo se logró crear un algoritmo que puede determinar si un número es probablemente primo o compuesto, esto se debe a que no existe ninguna prueba de primalidad determinista, por lo tanto, las computadoras con acceso a un generador real de números aleatorios, serían capaces de realizar con eficiencia esta tarea. Este descubrimiento inspiró la búsqueda de otros algoritmos aleatorios.

Los algoritmos aleatorios pueden resolver problemas de manera eficiente, problemas que no se podrían resolver en una máquina de Turing determinista. En particular, David Deutsch definió un dispositivo de cómputo capaz de simular de manera eficiente un sistema físico arbitrario. Deutsch consideró los dispositivos de computación basados en los principios de la mecánica cuántica. Estos dispositivos, análogos cuánticos de las máquinas definidas cuarenta y nueve años antes por Turing, nos llevan a la concepción moderna de una computadora cuántica. Dichas computadoras cuánticas pueden tener poderes de cómputo superiores a los de las computadoras clásicas.

En 1994 Peter Shor encontró un algoritmo para resolver el problema de encontrar los factores primos de un entero, que puede ser resuelto de manera eficiente en una computadora cuántica. Esto suscitó un gran interés debido a que este problema no tiene una solución eficiente en una computadora clásica. Los resultados de Shor son una poderosa evidencia de que las computadoras cuánticas en ciertos casos resuelven problemas de forma más rápida que las máquinas de Turing clásicas.

Otra prueba de la potencia de las computadoras cuánticas llegó en 1995 cuando Lov Grover mostró que el problema de llevar a cabo una búsqueda en una base de datos no estructurada podría acelerarse en una computadora cuántica.

En 1982, Richard Feynman señaló que había algunas dificultades esenciales en la simulación de la mecánica cuántica en las computadoras clásicas, y propuso que las computadoras basadas en la construcción de los principios de la mecánica cuántica nos permitirían evitar esas dificultades.

En 1990 varios equipos de investigadores comenzaron a darle cuerpo a la idea de construir computadoras basadas en los principios de la mecánica cuántica, mostrando que sí es posible el uso de las computadoras cuánticas para simular de manera eficiente los sistemas de la mecánica cuántica, por lo que es muy probable que una de las principales aplicaciones de las computadoras cuánticas en el futuro vaya a ser, la realización de simulaciones de la mecánica cuántica, muy difíciles de simular en una computadora clásica. Este problema, se cree, tendrá profundas implicaciones científicas y tecnológicas.

Un algoritmo que se pueda implementar en una computadora cuántica deberá ser mejor que cualquier otro algoritmo existente clásico, lo que hace difícil la construcción de un

algoritmo cuántico. Sin embargo los algoritmos cuánticos tienen múltiples aplicaciones, una de ellas está muy relacionada con la información en la red y la seguridad de la misma.

El estudio de la teoría cuántica de la información en red está todavía en sus inicios, incluso se sabe muy poco acerca de la información que llevan las redes de canales cuánticos, sin embargo, la red de información cuántica, puede tener implicaciones en el cifrado de claves de seguridad para mensajes secretos, mejor conocido como criptografía. En términos generales, la criptografía es el problema de hacer posible la comunicación entre dos o más partes que no pueden confiar unos en otros, este problema es conocido también como el cifrado de mensajes secretos para su transmisión.

Una aplicación práctica de las computadoras cuánticas es la ruptura de ciertos códigos criptográficos, lo cual ha despertado el interés por la computación e información cuántica [5]. Además de su uso en criptografía, otra aplicación de las computadoras cuánticas es la búsqueda de archivos en bases de datos no estructuradas, como se mencionó anteriormente. El problema de ésta búsqueda es resuelto por el algoritmo de Grover, tema principal de éste trabajo de tesis. El algoritmo de Grover ofrece una aceleración cuadrática con respecto a sus contrapartes clásicas en las búsquedas de archivos en bases de datos no estructuradas [7].

Finalmente, este trabajo de investigación trata de generalizar el algoritmo de Grover. Existen ya trabajos de de investigación al respecto, uno de ellos es el algoritmo de amplificación de amplitud cuántica.

Amplificación de amplitud cuántica (Quantum Amplitude Amplification) es la técnica más popular para la construcción de algoritmos cuánticos. Esta técnica es una generalización del algoritmo de Grover [4].

La técnica de amplificación de amplitud cuántica es llamada así, porque amplifica o incrementa la amplitud cuántica en la ecuación de onda de una partícula. En un problema de búsqueda en una base de datos no estructurada, para encontrar un índice de un archivo dado, la técnica de amplificación de amplitud cuántica, ubica el vector del estado inicial con baja amplitud, dicho valor se sustituye por otro, de tal forma que el resto de las amplitudes son sustituidas por otras amplitudes con un valor absoluto menor. Esto ocurre automáticamente porque las transformaciones efectuadas son unitarias, es decir, preservan el valor del producto interno y por lo tanto de las normas de los vectores también, de esta forma al realizar una observación, el algoritmo retorna un valor con una probabilidad bastante alta [4].

Amplificación de amplitud cuántica mejora la probabilidad de éxito de un algoritmo dado, aumentando la posibilidad de encontrar un archivo deseado dentro de una base de datos no estructurada, y al mismo tiempo reduce el tiempo de búsqueda de dicho archivo [4].

El algoritmo de Grover funciona de manera similar, aplicando primero a un estado inicial, un operador que genera un nuevo vector o estado, es decir, una superposición del anterior, pero con la misma amplitud para todos los elementos de la base. Luego, se aplica un determinado número de veces dos operadores unitarios: el operador de una función oráculo, y el operador de difusión. El primero es un operador de cambio de fase, y su acción se basa en cambiarle el signo a la amplitud de la base dejando el resto sin alterar. El segundo

vuelve a difundir las amplitudes, y este proceso se repite hasta que se encuentre con una probabilidad muy alta un archivo deseado en una base de datos no estructurada [10].

Una segunda generalización del algoritmo de Grover es usando caminatas aleatorias. La caminata aleatoria o paseo aleatorio, abreviado en inglés como RW (Random Walks), es una formalización matemática de la trayectoria que resulta de realizar pasos aleatorios sucesivos. Por ejemplo, la ruta trazada por una molécula mientras viaja por un líquido o gas, el camino que sigue un animal en su búsqueda por comida, el precio de una acción fluctuante y la situación financiera de un jugador, pueden tratarse como caminatas aleatorias.

El término caminata aleatoria fue introducido por Karl Pearson en 1905. Los resultados del análisis de paseo aleatorio han sido aplicados en muchos campos como la computación, la física, la química, la ecología, la biología, la psicología y la economía. Varios tipos de caminos aleatorios son de interés. Algunos caminos aleatorios están en la recta, el plano, o en dimensiones mayores. En su forma más general, las caminatas aleatorias son cualquier proceso aleatorio donde la posición de una partícula en cierto instante de tiempo depende sólo de su posición en algún instante previo y alguna variable aleatoria que determina su subsecuente dirección y la longitud del paso [1].

Los caminos aleatorios también varían con respecto al tiempo. Algunos ejemplos específicos de caminatas aleatorias son: la caminata de un borracho, el vuelo de Lévy y el movimiento browniano. Los paseos aleatorios están relacionados con los modelos de difusión y son un tema fundamental en los procesos de probabilidad de Markov [11].

Un tercer trabajo de investigación es generalizar el algoritmo de Grover para resolver sistemas de ecuaciones lineales donde la matriz de coeficientes es hermitiana y singular, es decir que el determinante de la matriz es cero [2].

En éste último trabajo se usaron ya matrices idempotentes de grado 2. El significado de una matriz idempotente de grado 2 es generar un subespacio invariante de dos dimensiones, estas dimensiones son:

1. una dimensión para marcar el ó los archivos que se buscan y
2. una otra dimensión para distinguir el ó los archivos que se buscan, de los que no interesan [3].

La clasificación en dos dimensiones de este subespacio invariante es buena bajo ciertas condiciones, es decir, mientras no haya un error en el algoritmo propuesto, pero si hubiera un error en el algoritmo, se desprende una tercera dimensión.

En el presente trabajo de investigación, se propone trabajar con matrices idempotentes de grado 3, que generen un subespacio invariante de tres dimensiones.

1. La primera dimensión para marcar el ó los archivos que se buscan,
2. la segunda dimensión para distinguir el ó los archivos que se buscan, de los que no interesan y

3. la tercera dimensión para distinguir el ó los archivos que no interesan, pero que se desprenden de un error en el algoritmo propuesto.

El resultado de este trabajo de investigación es el diseño de un algoritmo cuántico que resuelva sistemas de ecuaciones lineales con una matriz de coeficientes hermitiana, singular e idempotente de grado 3.

Se pretende simular el algoritmo propuesto para el caso tripotente, y demostrar que a través del mismo, sí es posible obtener la solución de un sistema de ecuaciones lineales, donde la matriz de coeficientes es singular, hermitiana y tripotente.

También se buscará encontrar ángulos de fase adecuados, con los cuales sea posible encontrar la solución de un sistema de ecuaciones propuesto. Esto se debe a que el vector que marca la solución del sistema de ecuaciones, puede rotar en ángulos de fase diferentes de π [8].

Una aplicación del algoritmo diseñado, donde se muestra el algoritmo de amplificación de amplitud cuántica modificado, permite afirmar: que un estado deseado, puede encontrarse con *certeza* a través del algoritmo extendido de Grover en un subespacio invariante posible de tres dimensiones, dicho estado contiene los archivos que son buscados dentro de la base de datos no estructurada, a diferencia de lo que afirma Jin, W. L. y Chen, X. D. que mencionan que: "un estado deseado, no puede encontrarse con *certeza* dentro de un subespacio posible de tres dimensiones a través del algoritmo de amplificación de amplitud cuántica, que es una generalización del algoritmo de Grover"[9].

Cabe mencionar, que encontrar con certeza un estado deseado dentro de una base de datos no estructurada, en un subespacio invariante de tres dimensiones, es equivalente a resolver un sistema de ecuaciones lineales.

Capítulo 2

Axiomas y algoritmos de la computación cuántica

El presente capítulo presenta los principios fundamentales bajo los cuales se gobiernan los algoritmos de la computación cuántica. Así como también se mencionan sus principales algoritmos.

La información que se menciona en este capítulo, esta basada en su mayor parte en el libro de Nielsen y Chuang [10], además en el artículo de Bautista, Guillen y Rangel [3].

2.1. Axiomas de la computación cuántica.

La Computación Cuántica se rige por ciertos principios básicos llamados *axiomas*, tales axiomas se heredan de las leyes de la mecánica cuántica. A continuación se presentan los axiomas de la computación cuántica.

2.1.1. Postulado 1: sobre los estados del sistema.

El estado de un sistema cuántico aislado es un vector $|\psi\rangle$, tal que $\langle\psi|\psi\rangle = 1$, es decir, que la norma de dicho vector es siempre uno. Las entradas del vector $|\psi\rangle$, son complejas.

Ejemplo 1. El vector *ket cero* se define de la sigueinte manera:

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

entonces el *braket cero* se define así:

$$\langle 0|0\rangle = 1^2 + 0^2 = 1$$

El vector *ket uno* se define como:

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

entonces el *braket uno* es:

$$\langle 1|1\rangle = 0^2 + 1^2 = 1$$

Otro ejemplo es:

Si el vector *ket lambda* es:

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

entonces el *braket lambda* es:

$$\langle \lambda|\lambda\rangle = 1^2 + 0^2 + 0^2 = 1$$

2.1.2. Postulado 2: sobre la evolución del sistema.

Los estados de un sistema cuántico cambian por la multiplicación de *matrices unitarias* U. Si $|\psi_0\rangle$ es un estado presente de un sistema cuántico y U es una matriz unitaria, entonces $|\psi_1\rangle = U\,|\psi_0\rangle$ es el siguiente estado del sistema cuántico [10].

En otras palabras, en un sistema cuántico la transición de un estado a otro se da a través de la multiplicación de matrices, y dichas matrices deben ser *unitarias*.

Definición 1. Una matriz cuadrada U se dice que es una matriz unitaria, si al multiplicar dicha matriz por su transpuesta conjugada, da como resultado la matriz identidad.

$$UU^* = Id \text{ y } U^*U = Id$$

donde U^* es la matriz transpuesta conjugada de U y Id es la matriz identidad, es decir:

si

$$U = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix},$$

la transpuesta conjugada de la matriz U es:

$$U^* = \begin{pmatrix} a_{11} & a_{21} & a_{31} & \cdots & a_{m1} \\ a_{12} & a_{22} & a_{32} & \cdots & a_{m2} \\ a_{13} & a_{23} & a_{33} & \cdots & a_{m3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \cdots & a_{mn} \end{pmatrix},$$

Como se observa la matriz transpuesta conjugada se forma al cambiar las filas por las columnas, pero también se debe invertir el signo de las entradas que son imaginarias en la matriz U.

A continuación presentaremos algunos ejemplos que apoyan la definición mencionada:

Ejemplo 2. si

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

y transpuesta conjugada de la matriz U es:

$$U^* = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix},$$

entonces U es una matriz unitaria, porque:

$$UU^* = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Otro ejemplo es:

Si

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

y transpuesta conjugada de U es:

$$U^* = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

entonces U es un matriz unitaria, porque:

$$UU^* = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2.1.3. Postulado 3: para la medición ú observación.

La medición es lo que se necesita para finalmente observar un resultado al final de un algoritmo cuántico. Tal medición consiste en multiplicar el último estado del algoritmo por otra matriz, la cual se denomina *matriz de medición* y tiene las siguientes características:

1. Los posibles resultados u observaciones de un sistema cuántico son:

$$m_1, m_2, m_3, \ldots, m_k$$

Estos posibles resultados tienen asociadas las matrices:

$$M_{m_1}, M_{m_2}, M_{m_3}, \ldots, M_{m_k}$$

Tal que:

$$M_{m_1}^* M_{m_1} + M_{m_2}^* M_{m_2} + M_{m_3}^* M_{m_3} + \cdots + M_{m_k}^* M_{m_k} = Id$$

Esta es llamada *ecuación de completez o completitud.*

2. Si $|\varphi\rangle$ es el estado de un sistema cuántico antes de ser observado, después de la observación, el sistema se colapsa al estado $\frac{M_{m_i}|\varphi\rangle}{||M_{m_i}|\varphi\rangle||}$ con probabilidad $P(m_i)$ de ser observado [10], donde:

$$P(m_i) = \langle\varphi| M_{m_i}^* M_{m_i} |\varphi\rangle$$

$$\langle\varphi| = |\varphi\rangle^*$$

También el braket es: $\langle\psi|\psi\rangle$ y el ketbra de ψ es: $|\psi\rangle\langle\psi|$.

Después de medir el estado del sistema, este se colapsa al nuevo estado observable.

Observación 1. La ecuación de completez asegura que la suma de las probabilidades de observar los diferentes posibles resultados es igual a 1.

$$\begin{aligned} P(m_1) + P(m_2) + \cdots + P(m_k) &= \langle\psi| M_{m_1} M_{m_1}^* + M_{m_2} M_{m_2}^* + \cdots + M_{m_k} M_{m_k}^* |\psi\rangle \\ &= \langle\psi|\psi\rangle \\ &= || \psi ||^2 \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 1.

2.1.4. Postulado 4: sobre los sistemas compuestos.

Supóngase que se tiene un sistema cuántico compuesto por otros dos. Si $|\lambda_1\rangle$ es el estado del sistema cuántico A y $|\lambda_2\rangle$ es el estado del sistema cuántico B, entonces $|\lambda_1\rangle \otimes |\lambda_2\rangle$ es el estado del *sistema cuántico compuesto* de A con B.

La operación descrita por el estado del sistema cuántico compuesto se llama *producto tensorial* de $|\lambda_1\rangle$ con $|\lambda_2\rangle$. El producto tensorial es también llamado *producto de Kronecker* [10].

El producto tensorial de dos matrices se define de la siguiente manera:

Definición 2. Si

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

y por otro lado

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{12} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

entonces el producto tensorial de A con B es:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{12}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

Un ejemplo que apoya la definición anterior es:

Ejemplo 3. Si

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

y por otro lado

$$B = \begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 3 & 8 \end{pmatrix}$$

entonces el producto tensorial de A con B es:

$$A \otimes B = \begin{pmatrix} 1 & 1 & 2 & 2 \\ -1 & 0 & -2 & 0 \\ 3 & 8 & 6 & 16 \\ 3 & 3 & 4 & 4 \\ -3 & 0 & -4 & 0 \\ 9 & 24 & 12 & 32 \end{pmatrix}.$$

Los vectores canónicos resultan de:

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

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

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

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

Definición 3. Tenemos que:

$$|\psi_1\rangle |\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

pero también:

$$|\psi_1\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

2.2. Algoritmos de la computación cuántica.

En computación cuántica existen algunos algoritmos que se ha demostrado representan una ganancia notable en complejidad con respecto a sus contrapartes clásicas.

Definición 4. Un algoritmo cuántico es la aplicación sucesiva de matrices unitarias a un estado inicial, para luego observar el estado final.

Esquemáticamente:

1. $|\psi_0\rangle$ es el estado inicial *(Axioma 1, Axioma 4)*
2. $|\psi_1\rangle = U_1 |\psi_0\rangle$ *(Axioma 2)*
3. $|\psi_2\rangle = U_2 |\psi_1\rangle$ *(Axioma 2)*
4. $|\psi_3\rangle = U_3 |\psi_2\rangle$ *(Axioma 2)*

   ⋮

n+1. $|\psi_n\rangle = U_n |\psi_n - 1\rangle$ *(Axioma 2)*

n+2. Medir (observar) *(Axioma 3)*

Donde $U_1, U_2, \ldots, U_n$ son matrices unitarias y $|\psi_0\rangle$ es un vector de norma uno *(estado puro).*

Para medir u observar el estado resultante, se usan matrices de medición, dichas matrices se nombran como: $M_1, M_2, \ldots, M_m$.

Las matrices de medición deben satisfacer la ecuación de completitud.

$$M_1^* M_1 + M_2^* M_2 + \ldots + M_m^* M_m = Id.$$

Finalmente se observa a:

$$|\psi_i\rangle = \frac{1}{\sqrt{P_i}} M_i |\psi_n\rangle$$

Donde $P_i = \langle\psi_n| M_i^* M_i |\psi_n\rangle$ y es la probabilidad de observar el estado $|\psi_i\rangle$.

Apartir de la definición anterior podemos tener las siguientes observaciones:

1. $\langle\psi_n| = |\psi_n\rangle^*$, es decir, un vector *bra* cualquiera, es igual al transpuesto conjugado del *ket* de ese mismo vector.
2. $(M_i |\psi_n\rangle)^* = |\psi_n\rangle^* M_i^*$, debido a que existe una propiedad que enuncia lo siguiente: $(AB)^* = B^* A^*$, donde A y B son matrices.
3. Si $|\psi_n\rangle = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}$, también $||\psi_n||^2 = |X_1|^2 + |X_2|^2 + \cdots + |X_n|^2$.
4. El modelo matemático de computación cuántica que vamos a emplear se llama *modelo de circuito*, y se esquematiza de la siguiente manera:

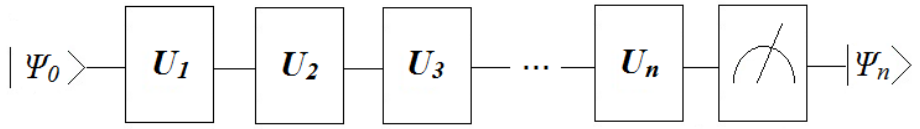

FIGURA 2.1: Modelo de circuito que inicia con el estado $|\psi_0\rangle$, para alcanzar el estado deseado $|\psi_n\rangle$ a través de la multiplicación sucesiva de matrices unitarias U_i.

Además del modelo de circuito, existen otros modelos para esquematizar sistemas cuánticos, tal es el caso del modelo adiabático, pero cabe mencionar que dicho modelo de representación es equivalente al modelo de circuito.

Otra característica del modelo que estudiamos aquí es que presupone que el sistema cuántico es *cerrado*, es decir, que el sistema no tiene interferencia del exterior debido

a que la naturaleza podría estar observando; y si la naturaleza llegara a observar el sistema cuántico se colapsaría.

2.2.1. Ejemplos de algoritmos cuánticos.

En esta parte del trabajo de investigación se describirá como es la estructura de un algoritmo cuántico y también se darán algunos ejemplos de algoritmos cuánticos que son conocidos por su ganancia en la complejidad del algoritmo con respecto a sus contrapartes clásicas.

Un ejemplo de un algoritmo cuántico que genera bits al azar es el siguiente:

1. El algoritmo cuántico parte de un estado inicial, el cuál generalmente es:

$$|000\ldots0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes \ldots \otimes |0\rangle .$$

2. La evolución del sistema cuántico se hace al multiplicar el estado inicial por la matriz W de Walsh-Hadamard, es decir, $|\psi_1\rangle = W\,|\psi_0\rangle$, donde:

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

   Si el estado inicial del sistema cuántico es: $|\psi_0\rangle = |0\rangle$, entonces el siguiente estado será:

$$|\psi_1\rangle = W\,|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle .$$

3. Para observar el sistema se usan las *matrices de medición*, como son:
   $M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ y $M_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, dichas matrices también se les conoce como *matrices de proyección canónica.*

   Estas matrices cumplen la condición de completitud o completez:

$$\begin{aligned} M_1^* M_1 + M_2^* M_2 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

   Para ver los cálculos completos remitirse al Apéndice A, Ecuación 2.

   Entonces el sistema se colapsa:

$$\begin{aligned}|\alpha_1\rangle &= \frac{1}{\sqrt{P_1}} M_1 |\psi_1\rangle \\ &= \frac{1}{\sqrt{P_1}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \frac{1}{\sqrt{P_1}} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \\ 0 \end{pmatrix}\end{aligned}$$

donde:

$$\begin{aligned}P_1 &= \langle\psi_1| M_1^* M_1 |\psi_1\rangle \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}}, & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \frac{1}{2}\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 3.

y así:

$$\begin{aligned}|\alpha_1\rangle &= \frac{1}{\sqrt{\frac{1}{2}}} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= |0\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 4.

En resumen: El sistema se colapsa de $|\alpha_1\rangle$ a $|0\rangle$ con probabilidad de $\frac{1}{2}$.
Ahora podemos ver que el sistema nuevamente se colapsa:

$$\begin{aligned}|\alpha_2\rangle &= \frac{1}{\sqrt{P_2}} M_2 |\psi_1\rangle \\ &= \frac{1}{\sqrt{P_2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \frac{1}{\sqrt{P_2}} \begin{pmatrix} 0 \frac{1}{\sqrt{2}} \end{pmatrix}\end{aligned}$$

donde:

$$\begin{aligned} P_2 &= \langle\psi_1| M_2^* M_2 |\psi_1\rangle \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}}, & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \frac{1}{2}. \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 5.

Así:

$$\begin{aligned} |\alpha_2\rangle &= \frac{1}{\sqrt{\frac{1}{2}}} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= |1\rangle . \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 6.

En resumen, el sistema se colapsa de $|\alpha_2\rangle$ a $|1\rangle$ con probabilidad de $\frac{1}{2}$.

Las proyecciones canónicas son:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle \langle 0|$$

$$M_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |1\rangle \langle 1|$$

pues:

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

$$|1\rangle \langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0, & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Luego:

$$M_1 |0\rangle = |0\rangle \langle 0|0\rangle = |0\rangle$$

$$M_1 |1\rangle = |0\rangle \langle 0|1\rangle = 0$$

$$M_2 |0\rangle = |1\rangle \langle 1|0\rangle = 0$$

$$M_2 |1\rangle = |1\rangle \langle 1|1\rangle = |1\rangle$$

Ejemplo 4.

$$\begin{aligned} M_1 W |0\rangle &= M_1(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle) \\ &= |0\rangle \langle 0| (\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle) \\ &= \frac{1}{\sqrt{2}} |0\rangle . \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 7.

Este resultado hay que normalizarlo según el axioma del colapso:

$$|\alpha_1\rangle = \frac{1}{\sqrt{P_1}} M_1 W |0\rangle$$

$$P_1 = \langle 0| \frac{1}{\sqrt{2}}^* \frac{1}{\sqrt{2}} |0\rangle = \frac{1}{2}\langle 0|0\rangle 0 = \frac{1}{2}.$$

Así: $|\alpha_1\rangle = \frac{1}{\sqrt{\frac{1}{2}}} \frac{1}{\sqrt{2}} |0\rangle = |0\rangle$ que se observa con probabilidad $P_1 = \frac{1}{2}$.

Para calcular la complejidad del algoritmo se cuentan el número de instrucciones usadas. El ejemplo anterior tiene complejidad 1.

2.2.2. Algoritmo de Deutsch.

El Algoritmo de Deutsch es una de las primeras aplicaciones que se le dieron a los algoritmos cuánticos. El poder reducir el número de veces que se tiene que evaluar una función, para determinar si esta es constante ó no. Veamos el siguiente problema:

Problema: Sea $f(x)$ una función booleana de aridad uno (caja negra). Determinar si $f(x)$ es constante ó no con sólo una llamada a la función (oráculo).

$$f(x) = \begin{cases} Si\, |\alpha\rangle = |0\rangle & \text{, entonces } f(x) \text{ es constante.} \\ Si\, |\alpha\rangle = |1\rangle & \text{, entonces } f(x) \text{ no es constante.} \end{cases}.$$

El Algoritmo Clásico que resuelve este problema se puede expresar de la siguiente manera:

1. $a := f(0)$.
2. $b := f(1)$.
3. if $a = b$ then *f(x) es constante.*
   else *f(x) no es constante.*

Ahora, el algoritmo cuántico que resuelve el mismo problema pero de una forma más rápida es:

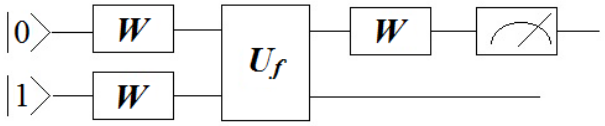

FIGURA 2.2: Modelo de circuito del algoritmo de Deutsch.

$$U_f |x\rangle |y\rangle = |x\rangle |f(x) \oplus y\rangle .$$

El análisis del algoritmo cuántico antes presentado es el siguiente:

1. *Estado inicial:*
$$|\psi_0\rangle = |0\rangle |1\rangle .$$
2. *Estado* $|\psi_1\rangle$*:*
$$\begin{aligned} |\psi_1\rangle &= (W \otimes W) |\psi_0\rangle \\ &= (W \otimes W)(|0\rangle |1\rangle) \\ &= \frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle . \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 8.

3. *Estado* $|\psi_2\rangle$*:*
$$\begin{aligned} |\psi_2\rangle &= U_f |\psi_1\rangle \\ &= U_f(\frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle) \\ &= \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 9.

4. *Estado* $|\psi_3\rangle$*:*

$$|\psi_3\rangle = (W \otimes Id)\,|\psi_2\rangle = \begin{cases} (-1)^{f(0)} W(\frac{|0\rangle+|1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle-|1\rangle}{\sqrt{2}}) & \text{si } f \text{ es constante,} \\ \pm W(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle-|1\rangle}{\sqrt{2}}) & \text{si } f \text{ no es constante} \end{cases}.$$

Si U es una matriz unitaria, entonces U^{-1} también es una matriz unitaria.

En general si A es una matriz unitaria podemos decir que:

$$\begin{aligned} AA^{-1} &= Id \\ (AA^{-1})^* &= Id^* \\ (AA^{-1})^* &= Id \\ (A^{-1})^* A^* &= Id. \end{aligned}$$

Por lo tanto:

$$(A^*)^{-1} = (A^{-1})^* = A.$$

Luego:

$$(U^{-1})^* = (U^*)^{-1}$$

$$(U^{-1})^* = (U^{-1})^{-1}$$

Por lo tanto: U^{-1} es una matriz unitaria.

Si U_1, U_2 son matrices unitarias, entonces, la matriz U_1U_2 también es unitaria pues:

$$\begin{aligned} (U_1U_2)^* &= U_2^* U_1^* \\ &= {U_2}^{-1} {U_1}^{-1} \\ &= U_1 {U_2}^{-1} \end{aligned}$$

Como consecuencia de U^{-1}, en computación cuántica una instrucción es reversible y las instrucciones son reversibles antes de medir.

2.2.3. Teorema de no clonación.

El teorema de no clonación fué descubierto en la década de 1980 y es uno de los primeros resultados de la computación cuántica [10].

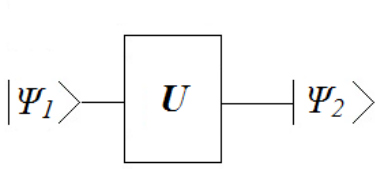

FIGURA 2.3: Modelo de circuito que muestra la transición de un estado inicial $|\psi_1\rangle$ a otro estado $|\psi_2\rangle$ a través de la instrucción de la matriz unitaria U.

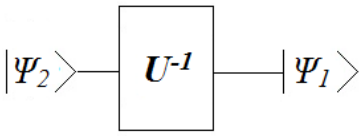

FIGURA 2.4: Modelo de circuito que muestra que las instrucciones que se dan por la multiplicación de matrices unitarias U, son reversibles antes de medir.

La clonación, tan fácil de lograr con la información clásica, resulta que no es posible en la mecánica cuántica, pues, si la clonación fuera posible; entonces, sería posible tener una señal más rápida que la luz utilizando los efectos cuánticos, lo cual contradice la teoría de la relatividad de Einstein, de la que se deduce que no es posible clonar información cuántica.

Teorema 1. En computación no existe un algoritmo cuántico que copie todas sus entradas.

Demostración. Supongamos que A es un algoritmo cuántico que copia todas sus entradas,

$$A\,|Inicio\rangle$$

con $A = U_k U_{k-1} \cdots U_2 U_1$; es decir, $(U_k U_{k-1} \cdots U_2 U_1)\,|Inicio\rangle$,

pero como el algoritmo A es reversible antes de la medición, entonces,

$$A\,|\psi\rangle = |\varphi\rangle \otimes |\psi\rangle$$

lo cual no es posible, pues la matriz A debe ser cuadrada. Luego se debe de tener

$$A(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\varphi\rangle$$

En particular:

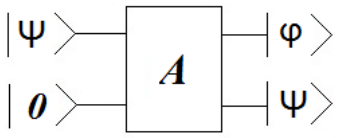

FIGURA 2.5: Modelo de circuito que muestra como la instrucción de la matriz unitaria A, debe ser cuadrada.

$$|\psi\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$$

donde: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ y $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$.

También:

$$\begin{aligned} A(|\psi\rangle \otimes |0\rangle &= |\psi\rangle \otimes |\psi\rangle \\ &= (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \\ &= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \end{aligned}$$

y por otro lado:

$$\begin{aligned} A(|\psi\rangle \otimes |0\rangle &= A(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle) \\ &= \frac{1}{\sqrt{2}}A|00\rangle + \frac{1}{\sqrt{2}}A|10\rangle \\ &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \end{aligned}$$

lo cual es absurdo, por lo tanto no existe un algoritmo cuántico que copie todas sus entradas. □

Definición 5. Si A es una matriz y n es un entero positivo.

$$A^{\otimes n} = A \otimes A \otimes \ldots \otimes A.$$

Definición 6. Los vectores $|00\ldots0\rangle$, $|00\ldots1\rangle$, $|00\ldots10\rangle$, $|00\ldots11\rangle$, $\cdots$, $|11\ldots1\rangle$ se llaman *base del cálculo.*

La base canónica es:

$$\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\\vdots\\0\end{pmatrix}, \cdots, \begin{pmatrix}0\\0\\0\\\vdots\\1\end{pmatrix}.$$

Propiedad 1. Sea W la matriz de Walsh - Hadamard y n es un entero positivo. Entonces, para cualquier $|k\rangle$ en la base del cálculo se cumple que:

$$W^{\otimes n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{k\cdot u} |u\rangle$$

donde $|u\rangle$ es un elemento de la base del cálculo y $k \cdot u$ es el producto punto.

Ejemplo 5.

$$\begin{aligned} W^{\otimes 2}|10\rangle &= (W \otimes W)(|1\rangle \otimes |0\rangle \\ &= \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right) \\ &= \frac{1}{2}\left((-1)^{1000}|00\rangle + (-1)^{1001}|01\rangle - (-1)^{1010}|10\rangle - (-1)^{1011}|11\rangle\right) \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 10.

2.2.4. Algoritmo de Deutsch-Josza.

El Algoritmo de Deutsch-Josza generaliza el algoritmo de Deutsch para n variables de entrada.

Problema: se da una función booleana de aridad n: $f(x_1, x_2, \ldots, x_n)$ que se sabe es constante ó balanceada. El problema es determinar si la función es constante ó balanceada.

Se supone que $f : \{0,1\}^n \to \{0,1\}$ es una caja negra y sólo se tiene acceso a evaluarla.

Definición 7. Sea una función boleana f se llama *balanceada* si $|f^{-1}(0)| = |f^{-1}(1)|$.

El algoritmo clásico que resuelve este problema se puede expresar de la siguiente manera:

1. $b := f(1)$.
2. Para $k = 0$ hasta $2^{n-1} + 1$, si $f(k) \neq b$ entonces f(x) es balanceada. En otro caso f(x) es constante.

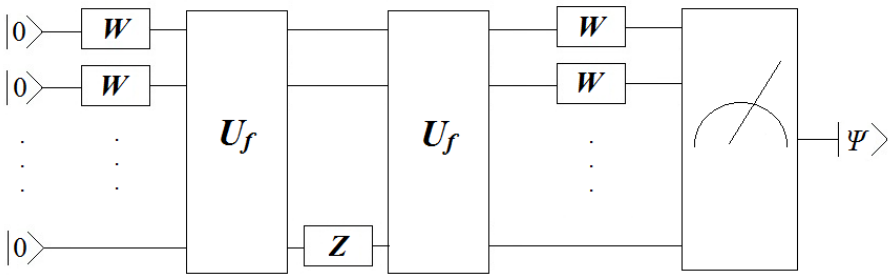

FIGURA 2.6: Modelo de circuito del algoritmo de Deutsch-Josza.

Luego, el algoritmo cuántico que resuelve el mismo problema pero de una forma más eficiente, se puede presentar de la siguiente forma:

El análisis del algoritmo cuántico antes presentado es el siguiente:

1. *Estado Inicial:*

$$|\psi_0\rangle = |00\ldots00\rangle$$

2. *Estado* $|\psi_1\rangle$*:*

$$\begin{aligned}|\psi_1\rangle &= (W^{\otimes n} \otimes Id)(|00\ldots0\rangle \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{00\ldots0}(|u\rangle \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (|u\rangle \otimes |0\rangle)\end{aligned}$$

Por superposición homogenea.

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 11.

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned}|\psi_2\rangle &= U_f(\frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} U_f(|u\rangle \otimes |0\rangle)\end{aligned}$$

Propiedad distributiba del producto de matrices ó paralelismo.

$$= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (|u\rangle \otimes |f(u) \oplus 0\rangle)$$

Por definición de U_f.

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 12.

4. *Estado* $|\psi_3\rangle$*:*

$$\begin{aligned}|\psi_3\rangle &= \left(Id^{\otimes n} \otimes z\right)\left(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle \otimes |f(u)\rangle\right)\\ &= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle \otimes z\,|f(u)\rangle\\ &= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle \otimes (-1)^{f(u)}\,|f(u)\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 13.

5. *Estado* $|\psi_4\rangle$*:*

$$\begin{aligned}|\psi_4\rangle &= U_f\left(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle \otimes (-1)^{f(u)}\,|f(u)\rangle\right)\\ &= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}U_f(|u\rangle \otimes |f(u)\rangle)\\ &= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\,|u\rangle \otimes |0\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 14.

6. *Estado* $|\psi_5\rangle$*:*

$$\begin{aligned}|\psi_5\rangle &= (W^{\otimes n} \otimes Id)\,|\psi_4\rangle\\ &= (W^{\otimes n} \otimes Id)(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\,|u\rangle \otimes |0\rangle)\\ &= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}W^{\otimes n}\,|u\rangle \otimes |0\rangle\\ &= \frac{1}{2^n}\left(\sum_{u=0}^{2^n-1}(-1)^{f(u)}\right)|00\ldots0\rangle\,|0\rangle + \cdots\end{aligned}$$

En esta etapa podemos ver la interferencia $\sum_{u=0}^{2^n-1}(-1)^{f(u)}$.

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 15.

Ahora, si f fuera balanceada la amplitud de $|00\ldots0\rangle\,|0\rangle$ sería 0, es decir, $|00\ldots0\rangle$ y también sería imposible de observar. Pero si f fuera constante, la amplitud de $|00\ldots0\rangle\,|0\rangle$ sería $(\frac{1}{2^n})(2^n) = 1$ ó $(\frac{1}{2^n})(-2^n) = -1$, es decir, $|00\ldots0\rangle$ se observaría con una probabilidad igual a 1.

2.2.5. Estados EPR.

Un estado EPR es un estado que es llamado así por *Einstein-Podolsky-Rosen.* Dicho estado EPR es un estado entrelazado, es decir, *entanglement state* [10].

Definición 8. Si un vector $|\psi\rangle$ no se puede escribir como $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, entonces se denomina *enlazado.*

Los estados EPR son: $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ y $|\beta_{11}\rangle$.

Para construir los estados EPR, consideramos el siguiente circuito:

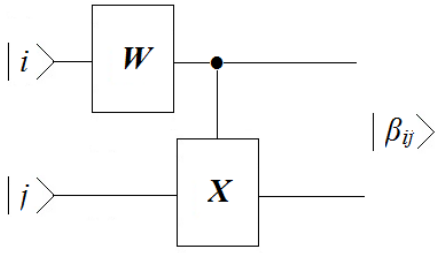

FIGURA 2.7: Modelo de circuito del estado EPR $|\beta_{ij}\rangle$.

A continuación se mostrarán los modelos de cicuito de los estados enlazados EPR o Einstein-Podolsky-Rosen:

Modelo de circuito del estado EPR $|\beta_{00}\rangle$.

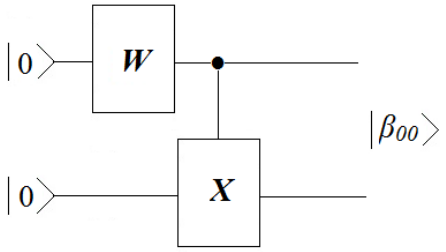

FIGURA 2.8: Modelo de circuito del estado EPR $|\beta_{00}\rangle$.

Análisis del algoritmo cuántico:

1. *Estado Inicial:*

$$|\psi_0\rangle = |0\rangle \otimes |0\rangle$$

2. *Estado* $|\psi_1\rangle$*:*

$$\begin{aligned}|\psi_1\rangle &= (W \otimes Id)(|0\rangle \otimes |0\rangle) \\ &= \left(\frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle\right)|0\rangle \\ &= \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|00\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 16.

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned}|\psi_2\rangle &= C(X)(\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|00\rangle) \\ &= \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|00\rangle \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= |\beta_{00}\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 17.

Teorema 2. $|\beta_{00}\rangle$ esta enlazado.

Demostración. Supongamos que $|\beta_{00}\rangle$ no esta enlazado, es decir, que $|\beta_{00}\rangle$ se puede escribir como $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, pero $|\alpha\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $|\beta\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ y

$$|\beta_{00}\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} + \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

Si $ac = \frac{1}{\sqrt{2}}$ y $ad = 0$, entonces $a \neq 0$ y $d = 0$. Pero si $bc = 0$ y $bd = \frac{1}{\sqrt{2}}$, entonces $d \neq 0$, lo cual es un absurdo.

Por lo tanto $|\beta_{00}\rangle$ esta enlazado. □

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Otro ejemplo es:

Ejemplo 6. *Modelo de circuito del estado EPR* $|\beta_{01}\rangle$*.*

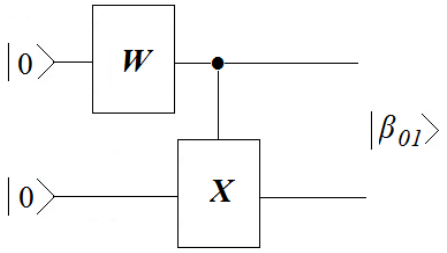

FIGURA 2.9: Modelo de circuito del estado EPR $|\beta_{01}\rangle$.

Teorema 3. $|\beta_{01}\rangle$ esta enlazado.

Demostración. Supongamos que $|\beta_{01}\rangle$ no esta enlazado, es decir, que $|\beta_{01}\rangle$ se puede escribir como $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, pero $|\alpha\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $|\beta\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ y

$$|\beta_{01}\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

Si $ac = 0$ y $ad = \frac{1}{\sqrt{2}}$, entonces $a \neq 0$ y $c = 0$. Pero si $bc = \frac{1}{\sqrt{2}}$ y $bd = 0$, entonces $c \neq 0$, lo cual es un absurdo.

Por lo tanto $|\beta_{01}\rangle$ esta enlazado. □

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

Ahora para:

Ejemplo 7. *Modelo de circuito del estado EPR* $|\beta_{10}\rangle$.

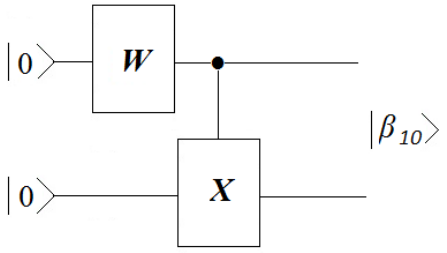

FIGURA 2.10: Modelo de circuito del estado EPR $|\beta_{10}\rangle$.

Teorema 4. $|\beta_{10}\rangle$ que también esta enlazado.

Demostración. Supongamos que $|\beta_{10}\rangle$ no esta enlazado, es decir, que $|\beta_{10}\rangle$ se puede escribir como $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, pero $|\alpha\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $|\beta\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ y

$$|\beta_{10}\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

Si $ac = \frac{1}{\sqrt{2}}$ y $ad = 0$, entonces $a \neq 0$ y $d = 0$. Pero si $bc = 0$ y $bd = -\frac{1}{\sqrt{2}}$, entonces $d \neq 0$, lo cual es un absurdo.

Por lo tanto $|\beta_{10}\rangle$ esta enlazado. □

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

Finalmente para:

Ejemplo 8. *Modelo de circuito del estado EPR $|\beta_{11}\rangle$.*

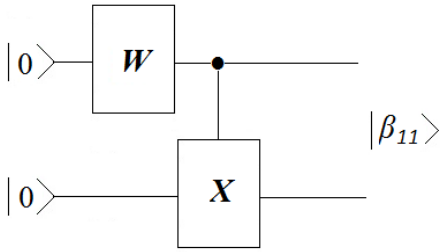

FIGURA 2.11: Modelo de circuito del estado EPR $|\beta_{11}\rangle$.

Teorema 5. $|\beta_{11}\rangle$ esta enlazado.

Demostración. Supongamos que $|\beta_{11}\rangle$ no esta enlazado, es decir, que $|\beta_{11}\rangle$ se puede escribir como $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, pero $|\alpha\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $|\beta\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ y

$$|\beta_{11}\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

Si $ac = 0$ y $ad = \frac{1}{\sqrt{2}}$, entonces $a \neq 0$ y $c = 0$. Pero si $bc = -\frac{1}{\sqrt{2}}$ y $bd = 0$, entonces $c \neq 0$, lo cual es un absurdo.

Por lo tanto $|\beta_{11}\rangle$ esta enlazado. □

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

2.2.6. Protocolo de teleportación.

Un *protocolo* es un algoritmo que se ejecuta entre varias computadoras comunicadas entre si.

Se tienen dos participantes A (Alicia) y B (Beto). Ambos tienen computadoras cuánticas conectadas entre si por canales cuánticos, es decir, canales que pueden transmitir qubits. Tal canal usa un sólo qubit que comparten Alicia y Beto. Pero Alicia tiene acceso a dos quibits y Beto tiene acceso a otros dos qubits.

Alicia le quiere enviar un qubit arbitrario a Beto.

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Algoritmo cuántico solución:

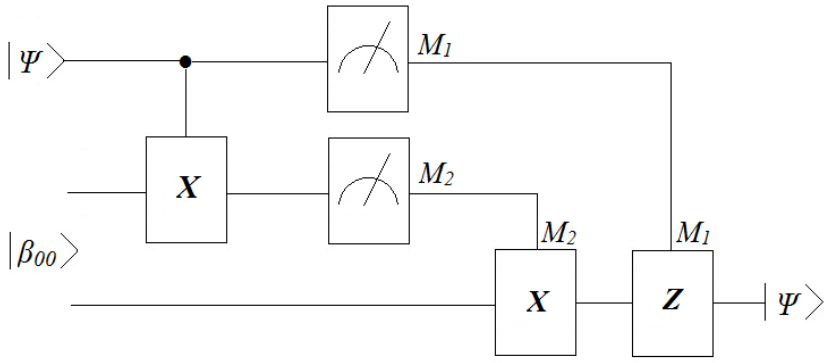

FIGURA 2.12: Modelo de circuito del algoritmo de teleportación.

Análisis del algoritmo cuántico:

1. *Estado Inicial:*
$$|\psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle$$

2. *Estado* $|\psi_1\rangle$*:*

$$\begin{aligned}|\psi_1\rangle &= C(X)^{\otimes Id}(|\psi\rangle \otimes |\beta_{00}\rangle) \\ &= C(X)^{\otimes Id}((a|0\rangle + b|1\rangle) \otimes |\beta_{00}\rangle) \\ &= C(X)^{\otimes Id}((a|0\rangle + b|1\rangle) \otimes (\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle)) \\ &= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle\,.\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 18.

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned}|\psi_2\rangle &= (W \otimes Id \otimes Id)(\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle \\ &+ \frac{b}{\sqrt{2}}W|0\rangle|110\rangle + \frac{b}{\sqrt{2}}|101\rangle) \\ &= \frac{a}{\sqrt{2}}W|0\rangle|00\rangle + \frac{a}{\sqrt{2}}W|0\rangle|11\rangle \\ &+ \frac{b}{\sqrt{2}}W|1\rangle|10\rangle + \frac{b}{\sqrt{2}}W|1\rangle|01\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle\frac{|0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(a|1\rangle + b|0\rangle)}{\sqrt{2}} \\ &+ \frac{1}{\sqrt{2}}|1\rangle\frac{|0\rangle(a|0\rangle - b|1\rangle) + |1\rangle(a|1\rangle - b|0\rangle)}{\sqrt{2}}\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 19.

Alicia mide y observa $|0\rangle$ con probabilidad de $\frac{1}{2}$, ú observa $|1\rangle$ con probabilidad de $\frac{1}{2}$; es decir, $M_1 = 0$ ó $M_1 = 1$ con probabilidad de $\frac{1}{2}$.

Y cuando Beto observa: $|0\rangle$ ó $|1\rangle$; es decir, $M_2 = 0$ ó $M_1 = 0$ con cierta probabilidad.

$$|\psi_2\rangle = \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$$

Si $M_1 = 0$ y $M_2 = 0$, entonces en el sistema de la computadora cuántica de Beto está:

$$|\psi\rangle = a|0\rangle + b|1\rangle.$$

2.2.7. Algoritmo de Grover.

El algoritmo de Grover hace búsquedas en bases de datos no estructuradas. Tal no estructura se modela con funciones booleanas, es decir, con tablas de verdad.

Problema: sea $f(x_1, x_2, \ldots, x_n)$ una función booleana de aridad n. Tal que $f(x_1, x_2, \ldots, x_n)$ sólo es satisfactible para una asignación.

$$x_1 = b_1, x_2 = b_2, x_3 = b_3, \ldots, x_n = b_n$$

Es decir,

$$f(b_1, b_2, b_3, \ldots, b_n) = 1.$$

Ejemplo 9. Si $n = 3$, entonces buscamos un artículo en una base de datos de 8 elementos, ya que $2^3 = 8$.

Problema: encontrar la asignación b_1, b_2, b_3.

La no estructura de la base de datos obliga a buscar de uno en uno los artículos.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	0	0	0
0	1	0	0
1	1	1	0
0	1	1	0
1	1	0	0
1	0	1	1
0	0	0	0
0	0	1	0

Ahora, el algoritmo cuántico que resuelve dicho problema de manera eficiente es:

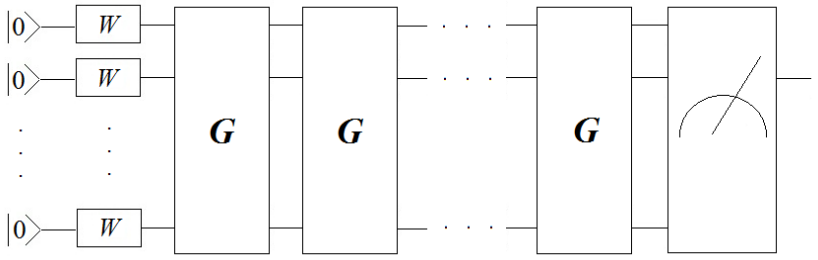

FIGURA 2.13: Modelo de circuito del algoritmo de Grover.

donde G se repite: $\left\lceil \frac{\pi - \arcsin \frac{\sqrt{2^n-1}}{2^n-1}}{2 \arcsin \frac{\sqrt{2^n-1}}{2^n-1}} \right\rceil$ veces.

El análisis de este algoritmo cuántico es el siguiente:

1. *Estado Inicial:*
$$|\psi_0\rangle = |0 \ldots 0\rangle$$

2. *Estado* $|\psi_1\rangle$*:*
$$\begin{aligned} |\psi_1\rangle &= \left(W^{\otimes n}\right) |\psi_0\rangle \\ &= \left(W^{\otimes n}\right) |0 \ldots 0\rangle \\ &= \cos\frac{\theta}{2} |M\rangle + \sin\frac{\theta}{2} |X_0\rangle \end{aligned}$$
por lema, con:

$$\theta = \arcsin \frac{\sqrt{2^n - 1}}{2^{n-1}}$$

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned} |\psi_2\rangle &= G\,|\psi_1\rangle \\ &= G\left(\cos\frac{\theta}{2}\,|M\rangle + \sin\frac{\theta}{2}\,|X_0\rangle\right) \\ &= -\begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix} \end{aligned}$$

4. *Estado* $|\psi_3\rangle$*:*

$$\begin{aligned} |\psi_3\rangle &= G\,|\psi_2\rangle \\ &= G^2\,|\psi_1\rangle \\ &= \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}^2\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix} \\ &= \begin{pmatrix}\cos\frac{5\theta}{2} \\ \sin\frac{5\theta}{2}\end{pmatrix} \end{aligned}$$

5. *Estado* $|\psi_4\rangle$*:*

$$|\psi_4\rangle = \begin{pmatrix}\cos\frac{7\theta}{2} \\ \sin\frac{7\theta}{2}\end{pmatrix}$$

$\vdots$

k. *Estado* $|\psi_k\rangle$*:*

$$|\psi_k\rangle = \begin{pmatrix}\cos\frac{(2k-1)(\theta)}{2} \\ \sin\frac{(2k-1)(\theta)}{2}\end{pmatrix}$$

k+1. *Estado* $|\psi_{k+1}\rangle$*:*

$$\begin{aligned} |\psi_{k+1}\rangle &= \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}^k\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix} \\ &= \begin{pmatrix}\cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta)\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix} \\ &= \begin{pmatrix}\cos\left(k\theta + \frac{\theta}{2}\right) \\ \sin\left(k\theta + \frac{\theta}{2}\right)\end{pmatrix} \end{aligned}$$

Así que:

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

y entonces:

$$k = \frac{\frac{\pi}{2} - \frac{\theta}{2}}{\theta}.$$

2.2.8. Aplicación del algoritmo de Grover para búsquedas en bases de datos no estructuradas.

El algoritmo de Grover se utiliza para realizar búsquedas de archivos en bases de datos no estructuradas.

Ejemplo 10. Pongamos $n = 2$, buscamos un artículo en una base de datos de tamaño $2^2 = 4$. El índice del artículo buscado es: $10_2 = 2$.

El algoritmo cuántico que resuelve el problema antes mencionado de manera eficiente es:

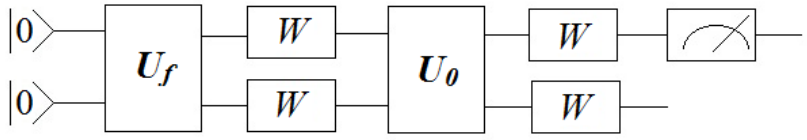

FIGURA 2.14: Modelo de circuito del algoritmo de Grover para búsquedas en bases de datos no estructuradas.

El análisis del algoritmo cuántico es el siguiente:

1. *Estado inicial:*
$$|\psi_0\rangle = |0\rangle\,|0\rangle$$
2. *Estado* $|\psi_1\rangle$*:*
$$|\psi_1\rangle = U_f\,|\psi_0\rangle = U_f\,|00\rangle$$
3. *Estado* $|\psi_2\rangle$*:*
$$|\psi_2\rangle = W^{\otimes 2}\,|\psi_1\rangle = (W \otimes W)U_f\,|00\rangle$$
4. *Estado* $|\psi_3\rangle$*:*
$$|\psi_3\rangle = U_0\,|\psi_2\rangle = U_0(W \otimes W)U_f\,|00\rangle$$
5. *Estado* $|\psi_4\rangle$*:*

$$\begin{aligned}|\psi_4\rangle &= W^{\otimes 2}\,|\psi_3\rangle = (W \otimes W)U_0(W \otimes W)U_f\,|00\rangle \\ &= (W \otimes W)(Id_4 - 2\,|00\rangle\,\langle 00|)(W \otimes W)U_f\,|00\rangle \\ &= (W \otimes W)(Id_4 - 2\,|00\rangle\,\langle 00|)(W \otimes W)(Id_4 - 2\,|10\rangle\,\langle 10|)\,|00\rangle \\ &= -\,|10\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 20.

Simulación:

1. *Estado inicial:*
$$|\psi_0\rangle = |00\rangle\,.$$

2. *Estado* $|\psi_1\rangle$*:*

$$\begin{aligned} |\psi_1\rangle &= W^{\otimes 2} |\psi_0\rangle \\ &= W^{\otimes 2} |00\rangle . \end{aligned}$$

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned} |\psi_2\rangle &= G |\psi_1\rangle \\ &= \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix} \\ &= - |10\rangle . \end{aligned}$$

La probabilidad de éxito del algoritmo es:

$$\begin{aligned} a &= \sqrt{(-1)^2 + (0)^2} \\ &= \sqrt{1} \\ &= 1. \end{aligned}$$

2.2.9. Aplicación del algoritmo de Grover para resolver sistemas de equaciones lineales singulares.

El problema de busqueda también se puede ver como la solución de un sistema de ecuaciones lineales, donde la matriz de coeficientes es cuadrada e invariante de dos dimensiones (el ó los artículos que busco y los que no busco). Dicha matriz también es singular, idempotente e igual a la transpuesta conjugada de dicha matriz.

Sistema de ecuaciones lineales que resuelve el algoritmo de Grover:

$$P |X\rangle = |b\rangle$$

donde:

$$
\begin{aligned}
P &= A\left|00\right\rangle\left\langle 00\right|A^{-1} = W^{\otimes 2}\left|00\right\rangle\left\langle 00\right|W^{\otimes 2} = (W\otimes W)\left|00\right\rangle\left\langle 00\right|(W\otimes W) \\
&= \left(\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\right)\left|00\right\rangle\left\langle 00\right| \left(\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\right) \\
&= \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1, & 0, & 0, & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \\
&= \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \end{pmatrix}
\end{aligned}
$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 21.

el vector de incógnitas $|X\rangle$ es:

$$|X\rangle = 2\,|\psi_1\rangle$$

y el vector de valores conocidos $|b\rangle$ es:

$$|b\rangle = \begin{pmatrix} \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{4} \end{pmatrix}.$$

2.2.10. Amplificación de amplitud cuántica.

Amplificación de amplitud cuántica es una generalización del algoritmo de Grover y más que un algoritmo cuántico es una técnica para mejorar la probabilidad de éxito de un algoritmo.

Se supone un algoritmo cuántico A (sin medición) con probabilidad de éxito a, donde $0 < a < 1$. El algoritmo cuántico que resuelve dicho problema de manera eficiente se muestra a continuación.

La iteración del operador: $Q = Q(A, \phi, \varphi) = -AU_0^{\phi}A^{-1}U^{\varphi}$ mejora la probabilidad de éxito de a a $\sqrt{a}$. (Ejemplo: de $a = \frac{1}{4}$ a $\sqrt{a} = \frac{1}{2}$). Donde $0 < \phi < 2\pi$, $0 < \varphi < 2\pi$ y U_0, U son matrices unitarias para cualquier $|X\rangle$ en la base de cálculo.

1. $U^{\varphi}\,|x\rangle = e^{i\varphi}\,|x\rangle$ si $|x\rangle$ es el buscado.
2. $U^{\varphi}\,|x\rangle = |x\rangle$ si $|x\rangle$ no es el buscado.

El análisis del algoritmo cuántico antes presentado es el siguiente:

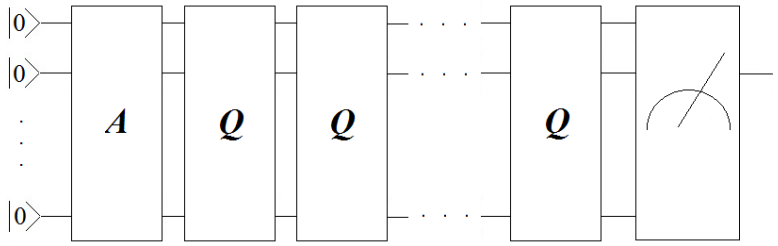

FIGURA 2.15: Modelo de circuito del algoritmo de amplificación de amplitud cuántica.

1. *Estado Inicial:*

$$|\psi_0\rangle = |0\ldots0\rangle\,.$$

2. *Estado* $|\psi_1\rangle$*:*

$$\begin{aligned}|\psi_1\rangle &= A\,|\psi_0\rangle \\ &= A\,|0\ldots0\rangle\,.\end{aligned}$$

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned}|\psi_2\rangle &= Q\,|\psi_1\rangle \\ &= QA\,|0\ldots0\rangle \\ &= -\begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix}.\end{aligned}$$

4. *Estado* $|\psi_3\rangle$*:*

$$\begin{aligned}|\psi_3\rangle &= Q\,|\psi_2\rangle = Q^2\,|\psi_1\rangle \\ &= \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}^2\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix} \\ &= \begin{pmatrix}\cos\frac{5\theta}{2} \\ \sin\frac{5\theta}{2}\end{pmatrix}.\end{aligned}$$

5. *Estado* $|\psi_4\rangle$*:*

$$|\psi_4\rangle = \begin{pmatrix}\cos\frac{7\theta}{2} \\ \sin\frac{7\theta}{2}\end{pmatrix}.$$

$\vdots$

k. *Estado* $|\psi_k\rangle$*:*

$$|\psi_k\rangle = \begin{pmatrix}\cos\frac{(2k-1)(\theta)}{2} \\ \sin\frac{(2k-1)(\theta)}{2}\end{pmatrix}.$$

k+1. *Estado* $|\psi_{k+1}\rangle$*:*

$$\begin{aligned}|\psi_{k+1}\rangle &= Q^k(\cos\frac{\theta}{2})(|\psi_0\rangle) + (\sin\frac{\theta}{2})(|\psi_1\rangle)\\ &= \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}^k \begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix}\\ &= \begin{pmatrix}\cos(k\theta) & -\sin(k\theta)\\ \sin(k\theta) & \cos(k\theta)\end{pmatrix} \begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix}\\ &= \begin{pmatrix}\cos\left(k\theta+\frac{\theta}{2}\right)\\ \sin\left(k\theta+\frac{\theta}{2}\right)\end{pmatrix}.\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 22.

Así que:

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

y entonces:

$$k = \frac{\frac{\pi}{2} - \frac{\theta}{2}}{\theta}.$$

Este valor de k nos indicará cuantas veces tenemos que repetir el operador generalizado de Grover.

Capítulo 3

Solución de sistemas de ecuaciones utilizando matrices tripotentes

El presente capítulo presentará el problema principal que se desea solucionar y describirá las principales características del mismo, como son la propiedades que tienen las matrices con las que se va a trabajar en el algoritmo cuántico que resuelve dicho problema.

Las matrices con las que se va a trabajar son tripotentes, por lo que la siguiente sección comenta las características de dichas matirces.

3.1. Generalidades de las matrices tripotentes.

Una *matriz tripotente* es aquella que al ser multiplicada por ella misma tres veces es igual a la misma matriz, es decir:

$$P^3 = P.$$

Las matrices tripotentes también son conocidas como matrices idempotentes de grado tres, es decir la pocencia a la cual esta elevada la matriz P indica el grado de idempotencia.

Ejemplo 11. Aqui tenemos un ejemplo de matriz tripotente:

Si $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y $P^3 = P$, entonces, $P^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, pero también esta matriz es idempotente de grado dos.

Ejemplo 12. Otro ejemplo de matriz tripotente, que no es idempotente de grado dos pero si de grado tres, sería:

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

entonces,

$$P^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Este tipo de matrices las vamos a ocupar en el problema que se quiere resolver en este trabajo de investigación, debido a que se desea resolver un sistema de ecuaciones y la matriz de este sistema de eciaciones es *tripotente* ó idempotente de grado tres.

3.2. Problema principal.

El problema que debemos resolver es encontrar la solución al siguiente sistema de ecuaciones:

$$P\,|X\rangle = |b\rangle$$

donde:

1. La matriz de coeficientes es P y es conocida, dicha matriz es tripotente; es decir, $P^3 = P$.
2. P es una *matriz hermitiana*, es decir, que $P^* = P$, lo cual significa que el transpuesto conjugado de la matriz P es igual a P.
3. También P es una *matriz singular*, es decir, que el determinante de dicha matriz P es igual a cero.
4. El vector $|b\rangle$, también es conocido y por último,
5. $|X\rangle$ es el vector desconocido, este vector de incógnitas, es el que se desea encontrar con el algoritmo cuántico que se va a diseñar.

3.2.1. Significado de las matrices tripotentes.

En este trabajo se propone generalizar el algoritmo extendido de Grover para resolver sistemas de ecuaciones lineales donde la matriz de coeficientes sea singular y tripotente.

Antes de mencionar el significado de una matriz tripotente o idempotente de grado 3, primero mencionaremos el significado de una matriz idempotente de grado 2, que es generar un subespacio invariante de dos dimensiones, estas dimensiones son:

1. Una primera dimensión es para marcar el ó los archivos buenos; es decir, el ó los archivos que busco,
   $U^{\varphi}\,|x\rangle = e^{i\varphi}\,|x\rangle$ si $|x\rangle$,
   $U_0^{\phi}\,|x\rangle = e^{i\phi}\,|x\rangle$ si $X = 0$.

2. Una segunda dimensión es para marcar el ó los archivos malos; es decir, el ó los archivos que no busco,
   $U^{\varphi} |x\rangle = |x\rangle$ si $|x\rangle$,
   $U_0^{\phi} |x\rangle = |x\rangle$ si x diferente de 0 [3].

Esta clasificación en dos dimensiones es buena bajo ciertas condiciones, es decir, mientras no haya un error en el algoritmo, pero si hubiera un error en el algoritmo, se desprende una tercera dimensión.

El significado de las tres dimensiones es:

1. La primera dimensión para marcar el ó los archivos buenos,
   $U^{\varphi} |x\rangle = e^{i\varphi} |x\rangle$ si $|x\rangle$,
   $U_0^{\phi} |x\rangle = e^{i\phi} |x\rangle$ si $X = 0$.
2. La segunda dimensión para marcar el ó los archivos malos,
   $U^{\varphi} |x\rangle = |x\rangle$ si $|x\rangle$,
   $U_0^{\phi} |x\rangle = |x\rangle$ si x diferente de 0, y
3. La tercera dimensión para marcar el ó los archivos malos que se desprenden por un error en el algoritmo.

En el presente trabajo de tesis se usará un subespacio invariante de 3 dimensiones, por lo que ocuparemos matrices idempotentes de grado 3, tomando para cada dimensión el significado antes mencionado.

El significado de las tres dimensiones que se proponen en este trabajo de investigación, son los ejes de la matriz de proyección P, la cual es idempotente de grado tres ($P^3 = P$).

Cabe mencionar que el sistema es completamente aislado y bajo condiciones ideales. El error que estamos suponiendo ocurre cuando se carga la base de datos a la computadora cuántica al inicio del algoritmo, es decir, cuando multiplicamos $A |00\ldots0\rangle$.

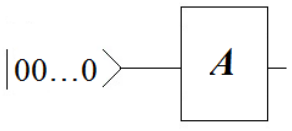

FIGURA 3.1: Modelo de circuito del algoritmo $A |00\ldots0\rangle$.

El algoritmo A puede tener errores, pero no es posible desecharlo debido a que no se tiene disponible algo mejor.

Al multiplicar el estado inicial $|0\rangle$ por el algoritmo A, se obtiene:

$A\,|0\rangle = \frac{1}{\sqrt{a}}\,|b\rangle$, donde $a = \langle b|b\rangle$.

También $A\,|0\rangle = \alpha\,|b\rangle + |C\rangle$, donde $|C\rangle$ es el posible error.

Podemos analizar el error el el sistema de ecuaciones $Q\,|X\rangle = \beta\,|C\rangle$, con $Q^2 = Q$.

Entonces $(P - Q)\,|X\rangle = |C\rangle$ y también $A\,|0\rangle - \alpha\,|b\rangle = |C\rangle$.

En resumen el significado de las tres dimensiones lo podemos enumerar:

1. La primera dimensión es el ó los archivos que se buscan.
2. La segunda dimensión son los archivos que no se buscan sin considerar un error en el algoritmo A.
3. La tercera dimensión son los archivos que no se buscan, considerando que hubo un error en el algoritmo A.

3.3. Solución del problema principal.

La solución al problema antes planteado, consistirá en extender el algoritmo de Grover, más especificamente, extender el operador de Grover.

Definición 9. El operador extendido de Grover es: $Q(\phi, \varphi) = e^{i\varphi P} e^{i\phi P|X\rangle\langle X|}$, donde

$e^{i\varphi P}$ marca el estado inicial y $e^{i\phi P|X\rangle\langle X|}$ marca el archivo buscado, con: $0 < \phi < 2\pi$ y $0 < P < 2\pi$.

Observación 2.

1. En general, si A y B son matrices cuadradas, $e^A e^B \neq e^{A+B}$.
2. Pero si $AB = BA$, entonces, $e^A e^B = e^{A+B}$.
3. En general hay una fórmula para calcular: $e^A e^B = e^{A+B}(factores)$. Dicha fórmula se le conoce con el nombre de: *Fórmula Haussdorf - Cambell - Birkhoff.*

3.3.1. Algoritmo que resuelve el problema principal.

Como ya se había mencionado, el problema principal de esta tesis es resolver el siguiente sistema de ecuaciones:

$$P\,|X\rangle = |b\rangle$$

como el vector $|b\rangle$ es conocido, debe haber un algoritmo cuántico A, tal que:

$$A\,|00\ldots0\rangle = \frac{1}{\sqrt{a}}\,|b\rangle$$

donde $a = \langle b|b\rangle$.

Observación 3. El uso de exponenciales no es extraño en mecánica cuántica, viene sugerido por la ecuación de Schroedinger que rige la evolución de un sistema cuántico cerrado.

Luego el algoritmo que resuelve la ecuación es:

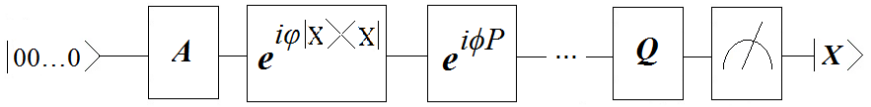

FIGURA 3.2: Modelo de circuito del algoritmo que resuelve el sistema de ecuaciones: $P\left|X\right\rangle = \left|b\right\rangle$.

3.3.2. Ecuación de Schroedinger.

Supóngase que H es el *hamiltoniano* del sistema, entonces:

$$i\hbar\frac{\delta\left|\psi\right\rangle}{\delta t} = H\left|\psi\right\rangle, \tag{3.1}$$

donde $\hbar$ es la constante de Plank.

El hamiltoniano del sistema es una *matriz hermitiana*, es decir, que $H^* = H$, lo cual significa que el transpuesto conjugado de la matriz H es igual a H.

La ecuación (3.1) tiene solución: $\left|\psi(t)\right\rangle = e^{i\frac{1}{\hbar}Ht}\left|\psi_0\right\rangle$, donde $\left|\psi_0\right\rangle$ es un vector constante.

Luego

$$\frac{\delta\left|\psi(t)\right\rangle}{\delta t} = -i\frac{1}{h}He^{-i\frac{1}{\hbar}Ht}\left|\psi_0\right\rangle,$$

y así

$$i\hbar\frac{\delta\left|\psi(t)\right\rangle}{\delta t} = H\left|\psi(t)\right\rangle.$$

Como el operador de Grover utiliza exponenciales de matrices, necesitamos conocer cuales son sus propiedades, las cuales se detallan a continuación:

Observación 4. Si A es una matriz cuadrada, ¿qué significa e^A?

Hay dos formas al menos de calcular e^A:

1. Teorema espectral.

   Si $AA^* = A^*A$ se dice que A es una *matriz normal*, entonces, existe una matriz U unitaria, tal que:

$$A = U \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix} U^{-1}.$$

Así, si A es una matriz normal, entonces:

$$e^A = U \begin{pmatrix} e^{\lambda_1} & 0 & 0 & \cdots & 0 \\ 0 & e^{\lambda_2} & 0 & \cdots & 0 \\ 0 & 0 & e^{\lambda_3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & e^{\lambda_n} \end{pmatrix} U^{-1}.$$

2. Límites al infinito.

   Supongamos que tenemos matrices $A_1, A_2, A_3, \ldots$ del mismo tamaño, entonces:

$$A_1 = (a_{ij}(1))$$

$$A_2 = (a_{ij}(2))$$

$$A_3 = (a_{ij}(3))$$

$$\vdots$$

   luego $\lim_{n\to\infty} A_n = \lim_{n\to\infty} a_{ij}(n)$.

   Ejemplo 13. Un ejemplo de A_n es:

$$A_n = \begin{pmatrix} \frac{1}{n} & \frac{1}{n^2} \\ \frac{n}{n+1} & \frac{1}{n^3} \end{pmatrix}$$

   con $n = 1, 2, 3, 4, \ldots$, entonces:

$$\lim_{n\to\infty} A_n = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

   Definición 10.

$$\sum_{i=1}^{\infty} A_i = \lim_{n\to\infty} (\sum_{i=1} nA_i) = \lim_{n\to\infty} (A_1 + A_2 + A_3 + \cdots).$$

Observación 5. Recordemos el desarrollo de Taylor de la exponencial real:

$$\forall x \in \mathbb{R}, e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

Luego, $\forall A$ matriz cuadrada:

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

Observación 6. En general no es fácil calcular e^A. Para elevar la exponencial a una matriz se usan matrices cuadradas.

Ejemplo 14. Sea $A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ y calculamos e^A por la serie de Taylor.

Primero vamos a calcular las potencias de la matriz A.

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

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

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\vdots$$

Después vamos a calcular e^A por la serie de Taylor.

$$e^A = \sum_{n=0}^{\infty} \frac{1}{n!} A^n = Id + \frac{1}{1!}A + \frac{1}{2!}A^2 + 0 + 0 + \cdots$$

$$e^A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \frac{3}{2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

En resumen:

$$e^{\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}} = \begin{pmatrix} 1 & 1 & \frac{3}{2} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Tratamos de repetir el cálculo usando el teorema espectral, para este cálculo, la matriz A, tiene que ser una matriz *normal*; es decir, $AA^* = A^*A$.

Veamos ahora que: $AA^* = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Luego: $A^*A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$.

Notese que la matriz A no es *normal* y por lo tanto no se puede usar el teorema espectral.

Pero A si es *nilpotente*; es decir, $A^k = 0$.

Ahora calcularemos las exponenciales de matrices de:

1. Matrices idempotentes.
2. Matrices tripotentes.

3.3.3. Matrices idempotentes.

Supongamos que $P^2 = P$; $e^{i\varphi P} = \sum_{n=0}^{\infty} \frac{1}{n!}(i\varphi P)^n$. Ahora si desarrollamos la fórmula anterior obtenemos:

$$e^{i\varphi P} = Id + \frac{1}{1!}i\varphi P + \frac{1}{2!}i^2\varphi^2 P^2 + \frac{1}{3!}i^3\varphi^3 P^3 + \frac{1}{4!}i^4\varphi^4 P^4 + \cdots$$

Desarrollando las potencias de la matriz idempotente P, tenemos:

$$P^0 = Id$$

$$P^1 = P$$

$$P^2 = P$$

$$P^3 = P$$

$$\vdots$$

Luego sustituyendo las potencias de la matriz P, obtenemos:

$$e^{i\varphi P} = Id + \frac{1}{1!}i\varphi P + \frac{1}{2!}i^2\varphi^2 P + \frac{1}{3!}i^3\varphi^3 P + \frac{1}{4!}i^4\varphi^4 P + \frac{1}{5!}i^5\varphi^5 P + \frac{1}{6!}i^6\varphi^6 P + \frac{1}{7!}i^7\varphi^7 P + \cdots$$

$$e^{i\varphi P} = Id + \frac{1}{1!}i\varphi P + \frac{1}{2!}i^2\varphi^2 P + \frac{1}{3!}i^3\varphi^3 P + \frac{1}{4!}i^4\varphi^4 P + \frac{1}{5!}i^5\varphi^5 P + \frac{1}{6!}i^6\varphi^6 P + \frac{1}{7!}i^7\varphi^7 P + \cdots$$

$$e^{i\varphi P} = Id + \left(\sum_{n=0}^{\infty} \frac{1}{n!}\left(i\varphi\right)^n\right) P$$

Por definición de como elevar una exponencial a una matriz, obtenemos:

$$e^{i\varphi P} = Id + (e^{i\varphi} - 1)P.$$

3.3.4. Matrices tripotentes.

Supongamos que $P^3 = P$; entonces,

$$e^{i\varphi P} = \sum_{n=0}^{\infty} \frac{1}{n!}(i\varphi P)^n.$$

Desarrollando la fórmula anterior:

$$e^{i\varphi P} = Id + \frac{1}{1!}i\varphi P + \frac{1}{2!}i^2\varphi^2 P^2 + \frac{1}{3!}i^3\varphi^3 P^3 + \frac{1}{4!}i^4\varphi^4 P^4 + \ldots$$

Ahora desarrollando las potencias de la matriz tripotente P, tenemos:

$$P^0 = Id$$

$$P^1 = P$$

$$P^2 = P^2$$

$$P^3 = P$$

$$P^4 = P^2$$

$$P^5 = P$$

$$\vdots$$

Luego sustituyendo las potencias de la matriz tripotente P, obtenemos:

$$e^{i\varphi P} = Id + \frac{1}{1!}i\varphi P + \frac{1}{2!}i^2\varphi^2 P^2 + \frac{1}{3!}i^3\varphi^3 P + \frac{1}{4!}i^4\varphi^4 P^2 + \frac{1}{5!}i^5\varphi^5 P + \frac{1}{6!}i^6\varphi^6 P^2 + \frac{1}{7!}i^7\varphi^7 P + \cdots$$

$$e^{i\varphi P} = Id + \frac{1}{1!}i\varphi P - \frac{1}{2!}\varphi^2 P^2 - \frac{1}{3!}i\varphi^3 P + \frac{1}{4!}\varphi^4 P^2 + \frac{1}{5!}i\varphi^5 P - \frac{1}{6!}\varphi^6 P^2 - \frac{1}{7!}i\varphi^7 P + \cdots$$

$$e^{i\varphi P} = Id + iP(\frac{\varphi}{1!} - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!} - \frac{\varphi^7}{7!} + \cdots) + P^2\left(-\frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} - \frac{\varphi^6}{6!} + \frac{\varphi^8}{8!} - \cdots\right)$$

$$e^{i\varphi P} = Id + iP\sum_{n=0}^{\infty}(-1)^n\frac{\varphi^{2n+1}}{(2n+1)!} + P^2\sum_{n=1}^{\infty}(-1)^n\frac{\varphi^{2n}}{(2n)!}.$$

Sustituyendo el desarrollo en serie de Taylor del seno y coseno, se obtiene:

$$e^{i\varphi P} = Id + i(\sin\varphi)P + (\cos\varphi - 1)P^2.$$

Observación 7. Si se tienen dos estados $|\alpha_1\rangle$ y $|\alpha_2\rangle$ no ortogonales; es decir, $\langle\alpha_1|\alpha_2\rangle \neq 0$, entonces no se pueden distinguir ($\langle\alpha_1|\alpha_2\rangle = \cos\beta \neq 0$), distinguir significa que antes de la medición, la suma de las probabilidades de todos los estados que se están considerando como posibles resultados, es igual a uno.

Si $|\alpha_1\rangle$ y $|\alpha_2\rangle$ son ortogonales y usamos para medir $|\alpha_1\rangle\langle\alpha_1| = M_1$ y $M_2 = Id - M_1$, donde se cumple la condición de completitud: $M_1M_1^* + M_2M_2^* = Id$.

En efecto, si $M_1 = |\alpha_1\rangle\langle\alpha_1|$, entonces,

$$\begin{aligned} M_1^* &= (|\alpha_1\rangle\langle\alpha_1|)^* \\ &= \langle\alpha_1|^* |\alpha_1\rangle^* \\ &= |\alpha_1\rangle\langle\alpha_1| \\ &= M_1. \end{aligned}$$

Si $M_2 = Id - M_1$, entonces,

$$\begin{aligned} M_2^* &= (Id - M_1)^* \\ &= Id^* - M_1^* \\ &= Id - M_1 \\ &= M_2 \end{aligned}$$

y también, $M_1M_1^* + M_2M_2^* = M_1M_1 + M_2M_2$.

Pero, $M_1M_1 = |\alpha_1\rangle\langle\alpha_1|\alpha_1\rangle\langle\alpha_1| = |\alpha_1\rangle\langle\alpha_1| = M_1$ y

$M_2M_2 = M_2^2 = (Id - M_1)^2 = Id^2 - 2M_1 + M_1^2 = Id - 2M_1 + M_1 = Id - M_1 = M_2$.

Por lo tanto $M_1M_1^* + M_2M_2^* = M_1 + M_2 = M_1 + (Id - M_1) = Id$.

Digamos que de un experimento obtenemos $|\alpha_1\rangle$,

luego medimos $\langle\alpha_1| M_1 |\alpha_1\rangle = \langle\alpha_1|\alpha_1\rangle\langle\alpha_1|\alpha_1\rangle = 1$

y $\langle\alpha_2| M_1 |\alpha_1\rangle = \langle\alpha_2|\alpha_1\rangle\langle\alpha_1|\alpha_1\rangle = 0$, ahora,

$$\begin{aligned} \langle\alpha_1| M_2 |\alpha_1\rangle &= \langle\alpha_1| (Id - M_1) |\alpha_1\rangle \\ &= \langle\alpha_1|\alpha_1\rangle - \langle\alpha_1| M_1 |\alpha_1\rangle \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

$$\begin{aligned}\langle\alpha_2| M_2 |\alpha_1\rangle &= \langle\alpha_2| (Id - M_1) |\alpha_1\rangle \\ &= \langle\alpha_2|\alpha_1\rangle - \langle\alpha_2| M_1 |\alpha_1\rangle \\ &= 0 - 0 \\ &= 0.\end{aligned}$$

Lo anterior demuestra que los dos estados $|\alpha_1\rangle$ y $|\alpha_2\rangle$ son ortogonales, es decir, distinguibles.

Como analistas del sistema tenemos que considerar estados distinguibles, es decir, ortogonales. Los estados que estamos considerando son:

1. $P^0 |X\rangle$ para el ó los archivos que se buscan.
2. $P^1 |X\rangle$ para el ó los archivos que no se buscan sin considerar un error en el algoritmo A.
3. $P^2 |X\rangle$ para el ó los archivos que no se buscan, considerando que hubo un error en el algoritmo A.

Pero pudiera ser que los estados no fueran distinguibles, en tal caso, se realiza el proceso de ortogonalización de Gram-Schmidt.

3.3.5. Algoritmo de Gram-Schmidt.

El proceso de Gram-Schmidt tiene como entrada: $|V_1\rangle, |V_2\rangle, \ldots, |V_m\rangle$ vectores linealmente independientes, y como salida: $|W_1\rangle, |W_2\rangle, \ldots, |W_m\rangle$ vectores ortogonales, tales que el espacio generado por los vectores de la entrada es igual al espacio generado por los vectores de salida; es decir, $gen(|W_1\rangle, |W_2\rangle, \ldots, |W_m\rangle) = gen(|V_1\rangle, |V_2\rangle, \ldots, |V_m\rangle)$.

Los vectores ortogonales de salida no salen del mismo espacio, es decir, se trata de un espacio invariante.

Para ortogonalizar los vectores que no son distinguibles se sigue el procedimiento siguiente:

Supongamos que tenemos vectores de salida $|W_1\rangle, |W_2\rangle, \ldots, |W_m\rangle$, donde, $|W_1\rangle = |V_1\rangle$ y

$$\begin{aligned}|W_2\rangle &= |V_2\rangle - \underset{W1}{\Pr} |V_2\rangle \\ &= |V_2\rangle - \frac{\langle W_1|W_2\rangle}{\langle W_1|W_1\rangle} |W_1\rangle\end{aligned}$$

con:

$$\begin{aligned}\langle W_1|W_2\rangle &= \langle V_1|V_2\rangle - \frac{\langle W_1|V_2\rangle}{\langle W_1|W_1\rangle}\langle V_1|W_1\rangle \\ &= \langle V_1|V_2\rangle - \langle W_1|V_2\rangle \\ &= 0\end{aligned}$$

y

$$\begin{aligned}|W_3\rangle &= |V_3\rangle - \Pr_{W1}|V_3\rangle - \Pr_{W2}|V_3\rangle \\ &= |V_3\rangle - \frac{\langle W_1|V_3\rangle}{\langle W_1|W_1\rangle}|W_1\rangle - \frac{\langle W_2|V_3\rangle}{\langle W_2|W_2\rangle}|W_2\rangle\end{aligned}$$

con:

$$\begin{aligned}\langle W_1|W_2\rangle &= \langle W_1|V_3\rangle - \frac{\langle W_1|V_3\rangle}{\langle W_1|W_1\rangle}\langle W_1|W_1\rangle - \frac{\langle W_2|V_3\rangle}{\langle W_2|W_2\rangle}\langle W_1|W_2\rangle \\ &= \langle W_1|V_3\rangle - \langle W_1|V_3\rangle \\ &= 0\end{aligned}$$

y

$$\begin{aligned}\langle W_2|W_3\rangle &= \langle W_2|V_3\rangle - \frac{\langle W_1|V_3\rangle}{\langle W_1|W_1\rangle}\langle W_2|W_1\rangle - \frac{\langle W_2|V_3\rangle}{\langle W_2|W_2\rangle}\langle W_2|W_2\rangle \\ &= \langle W_2|\,|\rangle\rangle\, V_3 - \langle W_2|V_3\rangle \\ &= 0\end{aligned}$$

$$\vdots$$

$$|W_m\rangle = |V_m\rangle - \Pr_{W1}|V_m\rangle - \ldots - \Pr_{W_{m-1}}|V_m\rangle\,.$$

En general una proyección se define de la siguiente manera:

Definición 11.

$$\Pr_U|V\rangle = \frac{\langle U|V\rangle}{\langle U|V\rangle}|U\rangle\,.$$

Esta definición la utilizamos dentro del proceso de Gram-Schmidt para ortogonalizar vectores que nos son distinguibles.

Suponiendo que $P^0|X\rangle$, $P^1|X\rangle$ y $P^2|X\rangle$ son vectores independientes, entonces:

1. $P^0|X\rangle = V_1$,
2. $P^1|X\rangle = V_2$ y
3. $P^2|X\rangle = V_3$.

Ocuparemos el proceso de Gram-Schmidt para distinguir estos vectores de entrada.

3.4. Algoritmo solución en el caso idempotente.

Aunque el interés de esta tesis es trabajar con matrices tripotentes, se desarrolló el caso idempotente, para tomarlo como base y después desarrollar el caso tripotente, que es el que se desea analizar en este trabajo de investigación.

Problema a resolver: encontrar $|X\rangle$ en $P|X\rangle = |b\rangle$, donde:

1. P es la matriz de coeficientes y es conocida. En computación cuántica y clásica se conoce como matriz de proyección. Dicha matriz es idempotente, es decir, $P^2 = P$.
2. La matriz P es singular, es decir, el determinante de P es igual a cero.
3. También la matriz P es hermitiana, es decir, $P^* = P$.
4. $|b\rangle$ es un vector conocido también.
5. $|X\rangle$ es un vector desconocido, este es el vector de las incógnitas.

Algoritmo solución en el caso idempotente:

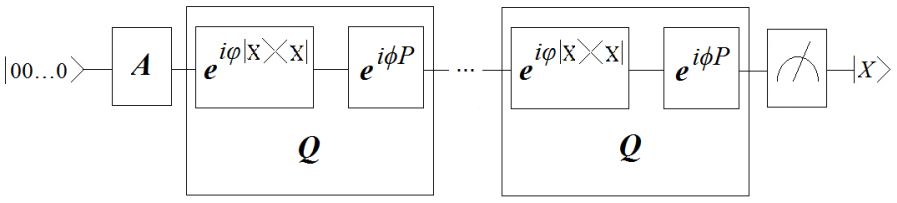

FIGURA 3.3: Modelo de circuito del algoritmo solución del sistema de ecuaciones en el caso idempotente.

Análisis del algoritmo solución en el caso idempotente:

El primer paso del algoritmo es cargar $|b\rangle$ en la computadora cuántica, para ello se parte de un estado inicial, el cual puede ser $|0\rangle$, $|1\rangle$ o alguno de los vectores canónicos de la base que se está utilizando.

Después se multiplica dicho estado inicial por una matriz A, que es unitaria y que permitirá que se realice la transición en la computadora cuántica del estado inicial al estado donde ya se tiene en memoria el vector $|b\rangle$.

Notese que cargar $|b\rangle$ significa:

$A|0\rangle = \frac{1}{\sqrt{a}}|b\rangle$, donde $a = \langle b|\,|b\rangle$

$A|0\rangle = \frac{1}{\sqrt{a}}P|X\rangle$

Es decir:

$|\psi_0\rangle = |0\rangle$

$|\psi_1\rangle = A|0\rangle = \frac{1}{\sqrt{a}}P|X\rangle$

$|\psi_2\rangle = e^{i\varphi|X\rangle\langle X|}(\frac{1}{\sqrt{a}}P|X\rangle)$

Se desea distinguir $|X\rangle$ solución de las no soluciones $P|X\rangle$, y se aplica el proceso de Gram-Schmidt.

$|W_1\rangle = |X\rangle$

$|W_2\rangle = P|X\rangle - \mathrm{Pr}_{W1}\,P|X\rangle$, donde $\mathrm{Pr}_U|V\rangle = \frac{\langle U|V\rangle}{\langle U|U\rangle}|U\rangle$, entonces,

$$\begin{aligned}|W_2\rangle &= P|X\rangle - \frac{\langle X|\,P|X\rangle}{\langle X|X\rangle}|X\rangle \\ &= P|X\rangle - \langle X|\,P|X\rangle\,|X\rangle \\ &= P|X\rangle - a|X\rangle \\ &= (P - aId)|X\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 23.

Teorema 6. El algoritmo propuesto no sale del espacio generado por $|X\rangle$ y $P|X\rangle$.

Demostración. 1. *Estado inicial:*

$$|\psi_0\rangle = |0\rangle$$

2. *Estado $|\psi_1\rangle$:*

$$|\psi_1\rangle = A|0\rangle = \frac{1}{\sqrt{a}}|b\rangle = \frac{1}{\sqrt{a}}P|X\rangle$$

3. *Estado* $|\psi_2\rangle$*:*

$$\begin{aligned}|\psi_2\rangle &= e^{i\varphi|X\rangle\langle X|}\,|\psi_1\rangle \\ &= e^{i\varphi|X\rangle\langle X|}(\frac{1}{\sqrt{a}}P\,|X\rangle) \\ &= (Id + (e^{i\varphi}-1)\,|X\rangle\,\langle X|)(\frac{1}{\sqrt{a}}P\,|X\rangle) \\ &= \frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 24.

El siguiente estado de la computadora cuántica será:

4. *Estado* $|\psi_3\rangle$*:*

$$\begin{aligned}|\psi_3\rangle &= e^{i\phi P}\,|\psi_2\rangle \\ &= e^{i\phi P}(\frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle) \\ &= (Id + (e^{i\phi}-1)P)(\frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle) \\ &= (e^{i\varphi}-1)\sqrt{a}\,|X\rangle + (\frac{1}{\sqrt{a}} + (e^{i\phi}-1)\frac{1}{\sqrt{a}} + \sqrt{a}(e^{i\varphi})^2 P\,|X\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 25.

□

Ahora, aplicaremos el proceso de Gram-Sctmidt a $|X\rangle$ y $P\,|X\rangle$, para distinguirlos, y así obtenemos los vectores ortogonales:

$|X\rangle$ y $P\,|X\rangle - a\,|X\rangle$, tales que

$$gen(|X\rangle, P\,|X\rangle) = gen(|X\rangle, P\,|X\rangle - a\,|X\rangle)$$

y también:

$$a = \langle b|b\rangle = \langle X|\,PP\,|X\rangle = \langle X|\,PP\,|X\rangle$$

Para el análisis del algoritmo consideramos las siguientes compuertas cuánticas que se iteran varias veces, hasta que el algoritmo encuentra el archivo buscado:

1. la compuerta del marcador es: $e^{i\varphi|X\rangle\langle X|} = Id + (e^{i\varphi}-1)\,|X\rangle\,\langle X|$ y
2. La compuerta del difusor es: $e^{i\phi P} = Id + (e^{i\phi}-1)P$.

Teorema 7. La matriz $e^{i\phi P}$ es unitaria.

Demostración.

$$\begin{aligned}(e^{i\phi P})(e^{i\phi P})^* &= (e^{i\phi P})(e^{(i\phi P)^*}) \\ &= (e^{i\phi P})(e^{P^*\phi(-i)}) \\ &= (e^{i\phi P})(e^{-i\phi P}) \\ &= Id\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 26.

□

Ahora se analizará que pasa cuando se multiplica las compuestas del marcador y el difusor por los vectores ortogonales $|X\rangle$ y $P|X\rangle - a|X\rangle$.

Primero se evaluará el producto punto del marcador $e^{i\varphi|X\rangle\langle X|}$ por el vector $|X\rangle$.

$$\begin{aligned}e^{i\varphi|X\rangle\langle X|}|X\rangle &= (Id + (e^{i\varphi} - 1)|X\rangle\langle X|)|X\rangle \\ &= |X\rangle + (e^{i\varphi} - 1)|X\rangle\langle X|X\rangle \\ &= |X\rangle + e^{i\varphi}|X\rangle - |X\rangle \\ &= e^{i\varphi}|X\rangle\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 27.

A continuación se analizará el producto punto del marcador $e^{i\varphi|X\rangle\langle X|}$ por el vector $P|X\rangle - a|X\rangle$.

$$\begin{aligned}e^{i\varphi|X\rangle\langle X|}(P|X\rangle - a|X\rangle) &= (Id + (e^{i\varphi} - 1)|X\rangle\langle X|)(P|X\rangle - a|X\rangle) \\ &= P|X\rangle - a|X\rangle + (e^{i\varphi} - 1)|X\rangle\langle X|P|X\rangle \\ &- a(e^{i\varphi} - 1)|X\rangle\langle X||X\rangle \\ &= P|X\rangle - a|X\rangle\end{aligned}$$

Significa que la compuerta de marcador $e^{i\varphi|X\rangle\langle X|}$, en el subespacio generado por $|X\rangle$ y $P|X\rangle - a|X\rangle$ se comporta como la siguiente matriz:

$$e^{i\varphi|X\rangle\langle X|} = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix}$$

Ahora se evaluará el producto punto del difusor $e^{i\phi P}$ por el vector $|X\rangle$.

$$\begin{aligned} e^{i\phi P}|X\rangle &= (Id + (e^{i\phi} - 1)P)|X\rangle \\ &= |X\rangle + (e^{i\phi} - 1)P|X\rangle \\ &= |X\rangle + (e^{i\phi} - 1)(P|X\rangle - a|X\rangle) + a(e^{i\phi} - 1)|X\rangle \\ &= (1 + a(e^{i\phi} - 1))|X\rangle + (e^{i\phi} - 1)(P|X\rangle - a|X\rangle) \end{aligned}$$

Finalmente se examinará el producto punto del difusor $e^{i\phi P}$ por el vector $P|X\rangle - a|X\rangle$.

$$\begin{aligned} e^{i\phi P}(P|X\rangle - a|X\rangle) &= (Id + (e^{i\phi} - 1)P)(P|X\rangle - a|X\rangle) \\ &= P|X\rangle - a|X\rangle + (e^{i\phi} - 1)P^2|X\rangle - a(e^{i\phi} - 1)P|X\rangle \\ &= -a|X\rangle + (e^{i\phi} - a(e^{i\phi} - 1))(P|X\rangle - a|X\rangle) \\ &+ a(e^{i\phi} - a(e^{i\phi} - 1))|X\rangle \\ &= (-a + a(e^{i\phi} - a(e^{i\phi} - 1)))|X\rangle + (e^{i\phi} \\ &- a(e^{i\phi} - 1))(P|X\rangle - a|X\rangle) \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 28.

Eso significa que la compuerta del difusor $e^{i\phi P}$, en el subespacio generado por $|X\rangle$ y $P|X\rangle - a|X\rangle$ se comporta como la siguiente matriz:

$$e^{i\phi P} = \begin{pmatrix} 1 + a(e^{i\phi} - 1) & -a + a(e^{i\phi} - a(e^{i\phi} - 1)) \\ e^{i\phi} - 1 & e^{i\phi} - a(e^{i\phi} - 1) \end{pmatrix}$$

Se puede observar que tanto la matriz del marcador como la del difusor son matrices unitarias.

El marcador $e^{i\varphi|X\rangle\langle X|}$ es una matriz unitaria:

$$\begin{aligned} e^{i\varphi|X\rangle\langle X|}e^{i\varphi|X\rangle\langle X|^*} &= e^{i\varphi|X\rangle\langle X| - i\varphi|X\rangle\langle X|} \\ &= e^0 \\ &= Id \end{aligned}$$

y también el difusor $e^{i\phi P}$ es una matriz unitaria.

Ahora se analizará el operador extendido de grover Q, que se itera k veces, hasta lograr encontrar el archivo buscado en la base de datos.

$$Q = e^{i\phi P} e^{i\varphi |X\rangle\langle X|} = \begin{pmatrix} e^{i\phi}(1 + a(e^{i\phi} - 1)) & -a + a(e^{i\phi} - a(e^{i\phi} - 1)) \\ e^{i\phi}(e^{i\phi} - 1) & e^{i\phi} - a(e^{i\phi} - 1) \end{pmatrix}$$

Se puede observar que cargar nuestra base de datos es colocar $|b\rangle$ en el sistema.

Observación 8.

$$\begin{aligned} A|0\rangle &= \frac{1}{\sqrt{a}}|b\rangle \\ &= \frac{1}{\sqrt{a}} P|X\rangle \\ &= \frac{1}{\sqrt{a}}(P|X\rangle - a|X\rangle) + \sqrt{a}|X\rangle \\ &= \sqrt{a}|X\rangle + \frac{1}{\sqrt{a}}(P|X\rangle - a|X\rangle) \end{aligned}$$

Así el trabajo consiste en analizar:

$$Q^k \begin{pmatrix} \sqrt{a} \\ \frac{1}{\sqrt{a}} \end{pmatrix} = \begin{pmatrix} \alpha_k \\ \beta_k \end{pmatrix}$$

también sabemos que el operador generalizado de Grover es igual a:

$$(e^{i\phi P} e^{i\varphi |X\rangle\langle X|})^k A|0\rangle = \alpha_k |X\rangle + \beta_k (P|X\rangle - a|X\rangle)$$

el objetivo de este operador es que:

$$|\beta_k|^2 \approx 0$$

y también:

$$|\alpha_k|^2 \approx 1.$$

Luego:

$$\begin{aligned} |X\rangle e^{i\phi P} e^{i\varphi |X\rangle\langle X|} A|0\rangle &= \alpha_k \langle X|X\rangle + \beta_k \langle X| P|X\rangle - a|X\rangle \\ &= \alpha_k \end{aligned}$$

y además:

$$\left(1,0\right) Q^k \begin{pmatrix} \sqrt{a} \\ \frac{1}{\sqrt{a}} \end{pmatrix} = \left(1,0\right) \begin{pmatrix} \alpha_k \\ \beta_k \end{pmatrix}$$

con $k = 0, 1, 2, \ldots$

Ahora se considera la función generatriz de $k = 0, 1, 2, \ldots$

$$\begin{aligned} g(x) &= \sum_{k=0}^{\infty} \alpha_k x^k \\ &= \sum_{k=0}^{\infty} \left(1,0\right) Q^k \begin{pmatrix} \sqrt{a} \\ \frac{1}{\sqrt{a}} \end{pmatrix} x^k \\ &= \left(1,0\right) \sum_{k=0}^{\infty} Q^k x^k \begin{pmatrix} \sqrt{a} \\ \frac{1}{\sqrt{a}} \end{pmatrix} \\ &= \left(1,0\right) \left(Id - Qx\right)^{-1} \begin{pmatrix} \sqrt{a} \\ \frac{1}{\sqrt{a}} \end{pmatrix} \end{aligned}$$

Cabe mencionar que x es una variable dummy.

$$Q = e^{i\phi P} e^{i\varphi |X\rangle\langle X|} = \begin{pmatrix} e^{i\phi}(1 + a(e^{i\phi} - 1)) & -a + a(e^{i\phi} - a(e^{i\phi} - 1)) \\ e^{i\phi}(e^{i\phi} - 1) & e^{i\phi} - a(e^{i\phi} - 1) \end{pmatrix}.$$

Por otro lado, si:

$$\begin{aligned} g(x) &= \sum_{k=0}^{\infty} \alpha_k x^k \\ &= \sum_{k=0}^{\infty} \left(1,0\right) Q^k \begin{pmatrix} \sqrt{a} \\ \frac{1}{\sqrt{a}} \end{pmatrix} x^k \\ &= \frac{ax - x}{\sqrt{a}(e^{i\phi P + i\varphi |X\rangle\langle X|} x^2 + ((-ae^{i\phi P} a - 1)e^{i\varphi |X\rangle\langle X|} + (a-1)e^{i\phi} - a)x + 1)} \\ &= \frac{\sqrt{a}(x-1)}{e^{i\phi P + i\varphi |X\rangle\langle X|} x^2 + ((-ae^{i\phi P} a - 1)e^{i\varphi |X\rangle\langle X|} + (a-1)e^{i\phi} - a)x + 1} \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 29.

Luego, si $\varphi = \phi$ entonces:

$$g(x) = \frac{\sqrt{a}(x-1)}{e^{2i\phi} x^2 - (a(e^{i\phi} - 1)^2 + 2e^{i\phi})x + 1}$$

también, podemos considerar a la función generatriz $g(x)$ como:

$g(x) = \frac{Ax+B}{Cx^2+Dx+E}$ entonces,

$$\begin{aligned} Ax + B &= g(x)(Cx^2 + Dx + E) \\ &= \sum_{k=0}^{\infty} \alpha_k x^k (Cx^2 + Dx + E) \\ &= \sum_{k=0}^{\infty} C\alpha_k x^{k+2} + \sum_{k=0}^{\infty} D\alpha_k x^{k+1} + \sum_{k=0}^{\infty} E\alpha_k x^k \\ &= E\alpha_0 + (D\alpha_0 + E\alpha_1)x + \sum_{j=2}^{\infty} (C\alpha_{j-2} + D\alpha_{j-1} + E\alpha_j)x^j \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 30.

Por lo tanto: $D\alpha_0 + E\alpha_1 = A$, $E\alpha_0 = B$ y $C\alpha_{j-2} + D\alpha_{j-1} + E\alpha_j = 0$, si $j \geq 2$.

Luego: $\alpha_0 = \frac{B}{E}$, $\alpha_1 = \frac{A - D\alpha_0}{E}$ y $\alpha_j = \frac{-C\alpha_{j-2} + D\alpha_{j-1}}{E}$.

Debido a que: $g(x) = \frac{Ax+B)}{Cx^2+Dx+E} = \frac{-\sqrt{a}x+\sqrt{a}}{e^{2i\phi}x^2 - (a(e^{i\phi}-1)^2+2e^{i\phi})x+1}$; entonces,

$$\alpha_0 = -\sqrt{a}$$

y por otro lado:

$$\alpha_1 = \sqrt{a} - (a(e^{i\phi} - 1)^2 + 2e^{i\phi})\sqrt{a}.$$

En general:

$$\alpha_j = -(e^{2i\phi}\alpha_{j-2} - (a(e^{i\phi} - 1)^2 + 2e^{i\phi})\alpha_{j-1})$$

También debemos tomar en cuenta que a no puede tomar cualquier valor en estas expresiones, primero recordemos que es a.

Sea $a = \langle x| P |x\rangle$,

Teorema 8. Si $P^2 = P$ y $P^* = P$, entonces, $0 < \langle x| P |x\rangle < 1$.

Demostración. Tenemos que $P|x\rangle = |b\rangle$ con $|b\rangle \neq 0$, debido a que no tiene sentido que no tengamos ningun archivo en nuestra base de datos.

Luego: $0 < \langle b| |b\rangle \leq 1$, debido a que la norma de $|b\rangle$ es igual a 1, que la norma al cuadrado de $|b\rangle$ es el $\langle b| |b\rangle$, y a que las normas al cuadrado son siempre son positivas.

Entonces, tenemos que:

$$\begin{aligned}\langle b|b\rangle &= \| \, |b\rangle \, \|^2 \\ &= \langle x| \, P^*P \, |x\rangle = \langle x| \, PP \, |x\rangle \\ &= \langle x| \, P^2 \, |x\rangle = \langle x| \, P \, |x\rangle \\ &= a\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 31.

Por lo tanto $a > 0$.

Sabemos también que $|x\rangle$ es ortogonal a $P\,|x\rangle - a\,|x\rangle$. Luego: $0 \leq \| \, P\,|x\rangle - a\,|x\rangle \, \|^2$, debido a que la norma al cuadrado de $P\,|x\rangle - a\,|x\rangle$, es positiva. Entonces tenemos que:

$$\begin{aligned}\| \, P\,|x\rangle - a\,|x\rangle \, \|^2 &= (\langle x| \, P^* - a\,|x\rangle)(P\,|x\rangle - a\,|x\rangle) \\ &= (\langle x| \, P)(P\,|x\rangle - a\,|x\rangle - 0) \\ &= \langle b| \, P\,|b\rangle - a^2 \\ &= a - a^2\end{aligned}$$

Por lo tanto $a - a^2 \geq 0$, $a^2 \leq a$ y $a \leq 1$, debido a que $a > 0$. □

3.5. Propuesta de algoritmo en el caso tripotente.

El caso tripotente es la propuesta de este trabajo de tesis. Se parte de la explicación del problema que queremos resolver, sus caractersticas, así como el método para resolverlo.

Problema a resolver: encontrar $|X\rangle$ en $P\,|X\rangle = |b\rangle$, donde:

1. P es la matriz de coeficientes conocida. Dicha matriz es tripotente, es decir, $P^3 = P$.
2. La matriz P es singular, es decir, el determinante de P es igual a cero.
3. También la matriz P es hermitiana, es decir, $P^* = P$.
4. $|b\rangle$ es un vector conocido también.
5. $|X\rangle$ es un vector desconocido, este es el vector de las incógnitas.

Algoritmo solución en el caso tripotente y su análisis:

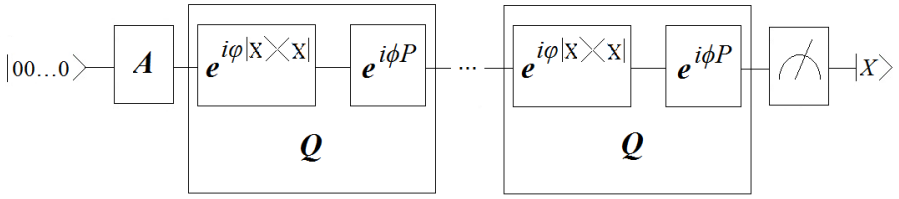

FIGURA 3.4: Modelo de circuito del algoritmo solución del sistema de ecuaciones en el caso tripotente.

El primer paso del algoritmo propuesto para el caso tripotente es cargar $|b\rangle$ en la computadora cuántica, para ello se parte de un estado inicial, el cual puede ser $|0\rangle$, $|1\rangle$ o alguno de los vectores canónicos de la base que se está utilizando.

Después se multiplica dicho vector del estado inicial por una matriz A, que es unitaria y que permitirá que se realice la transición en la computadora cuántica del estado inicial, al estado donde ya se tiene en memoria el vector $|b\rangle$.

Una matriz A que se puede implementar en una computadora cuántica es la matriz de Walsh-Hadamard ó el producto tensiorial de matrices de Walsh-Hadamard.

Notese que cargar $|b\rangle$ significa:

$A|0\rangle = |b\rangle$, donde:

$$\begin{aligned} \| \, |b\rangle \, \|^2 &= \langle b|b\rangle \\ &= \langle x| \, P^* P \, |x\rangle \\ &= \langle x| \, PP \, |x\rangle \\ &= \langle x| \, P^2 \, |x\rangle = \beta \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 32.

Se asignará un valor a α y β en expresiones subsecuentes, con la finalidad de que dichas expresiones no resulten tan largas para su análisis.

Observación 9. El valor de α es el valor esperado, valor promedio ó primer momento de probabilidad y se puede expresar como:

$$\alpha = \langle x| \, P \, |x\rangle$$

y por otro lado el valor de β es el segundo momento de probabilidad, que también se puede expresar como:

$$\beta = \langle x| \, P^2 \, |x\rangle \, ,$$

también el valor de $\beta - \alpha^2$ es la varianza y $\sqrt{\beta - \alpha^2}$ es la desviación estandar. Sólo en el caso de que $\alpha = 0$, el valor de β es la varianza. Este caso se tratará más adelante cuando se simule encontrar a $|X\rangle$ en $P|X\rangle = |b\rangle$, donde P es una matriz de coeficientes tripotente, es decir, $P^3 = P$.

Tomando en cuenta la observacion anterior, se analizarán las siguientes expresiones que forman parte del algoritmo:

$$\begin{aligned}\frac{1}{\| |b\rangle \|}|b\rangle &= \frac{1}{\| |b\rangle \|}P|x\rangle \\ &= \frac{1}{\sqrt{\beta}}P|x\rangle \\ &= \frac{1}{\sqrt{\beta}}P|x\rangle - \frac{\alpha}{\sqrt{\beta}}|x\rangle + \frac{\alpha}{\sqrt{\beta}}|x\rangle \\ &= \frac{1}{\sqrt{\beta}}(P|x\rangle - \alpha|x\rangle) + \frac{\alpha}{\sqrt{\beta}}|x\rangle\end{aligned}$$

es decir, tenemos que:

$$|\psi_0\rangle = |0\rangle$$

$$|\psi_1\rangle = A|0\rangle = \frac{1}{\sqrt{\beta}}(P|x\rangle - \alpha|x\rangle) + \frac{\alpha}{\sqrt{\beta}}|x\rangle$$

$$|\psi_2\rangle = e^{i\varphi|X\rangle\langle X|}(\frac{1}{\sqrt{\beta}}(P|x\rangle - \alpha|x\rangle) + \frac{\alpha}{\sqrt{\beta}}|x\rangle).$$

Se desea distinguir $|X\rangle$, $P|x\rangle$ y $P^2|x\rangle$ de entre si, debido a que $|X\rangle$ es la solución del sistema, mientras $P|x\rangle$ y $P^2|x\rangle$, no son soloción al sistema, y la última de estas dos se produce por un error en el algoritmo. Para este proceso de distinción se aplicó el proceso de Gram-Schmidt.

Se tienen las siguientes entradas: $V_1 = P^0|X\rangle$, $V_2 = P|X\rangle$ y $V_3 = P^2|X\rangle$.

Después se analizaron las siguientes salidas:

$|W_1\rangle = P^0|X\rangle = |X\rangle$ y $|W_2\rangle = P|x\rangle - \mathrm{Pr}_{W1}P|x\rangle$, donde $\mathrm{Pr}_U|V\rangle = \frac{\langle U|V\rangle}{\langle U|U\rangle}|U\rangle$, entonces

$$\begin{aligned}|W_2\rangle &= P\,|X\rangle - \frac{\langle W_1|\,P\,|X\rangle}{\langle W_1|W_1\rangle}\,|W_1\rangle \\ &= P\,|X\rangle - \frac{\langle X|\,P\,|X\rangle}{\langle X|\,|X\rangle}\,|X\rangle \\ &= P\,|X\rangle - \langle X|\,P\,|X\rangle\,|X\rangle \\ &= P\,|X\rangle - \alpha\,|X\rangle\end{aligned}$$

debido a que $\alpha = \langle x|\,P\,|x\rangle$.

Despues, $|W_3\rangle = V_3 - \mathrm{Pr}_{W1}\,V_3 - \mathrm{Pr}_{W2}\,V_3$; entonces:

$$\begin{aligned}|W_3\rangle = |W_3\rangle &= P^2\,|x\rangle - \underset{W1}{\mathrm{Pr}}\,P^2\,|x\rangle - \underset{W2}{\mathrm{Pr}}\,P^2\,|x\rangle \\ &= P^2\,|X\rangle - \frac{\langle W_1|\,P^2\,|X\rangle}{\langle W_1|W_1\rangle}\,|W_1\rangle - \frac{\langle W_2|\,P^2\,|X\rangle}{\langle W_2|W_2\rangle}\,|W_2\rangle \\ &= P^2\,|X\rangle - \langle X|\,P^2\,|X\rangle\,|X\rangle - \frac{(P\,|X\rangle - \alpha\,|X\rangle)P^2\,|X\rangle}{(P\,|X\rangle - \alpha\,|X\rangle)^*P\,|X\rangle - \alpha\,|X\rangle}(P\,|X\rangle - \alpha\,|X\rangle) \\ &= P^2\,|X\rangle - \beta\,|X\rangle - \frac{(P\,|X\rangle - \alpha\,|X\rangle)P^2\,|X\rangle}{(P\,|X\rangle - \alpha\,|X\rangle)^*P\,|X\rangle - \alpha\,|X\rangle}(P\,|X\rangle - \alpha\,|X\rangle)\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 33.

Recordemos que $\alpha = \langle x|\,P\,|x\rangle$ y $\beta = \langle x|\,P^2\,|x\rangle$. Para continuar con el análisis del algoritmo propuesto se consideran las siguientes compuertas cuánticas, que se iteran varias veces hasta que el algoritmo propuesto para el caso tripotente encuentra el archivo buscado:

1. La compuerta del marcador es: $M = e^{i\varphi|X\rangle\langle X|} = Id + (e^{i\varphi} - 1)\,|X\rangle\,\langle X|$.
2. La compuerta del difusor es: $D = e^{i\phi P} = Id + i(\sin\phi)P + (\cos\phi - 1)P^2$.

Ahora vamos a analizar el resultado de multiplicar las compuertas del marcador M y el difusor D por los vectores ortogonales $|W_1\rangle$, $|W_2\rangle$ y $|W_3\rangle$.

Primero se analizará el producto punto entre el marcador:

$$M = e^{i\varphi|X\rangle\langle X|}$$

por el vector:

$$|W_1\rangle = |X\rangle$$

$$\begin{aligned} M\left|X\right\rangle &= e^{i\varphi\left|X\right\rangle\left\langle X\right|}\left|X\right\rangle \\ &= \left(Id + \left(e^{i\varphi}-1\right)\left|X\right\rangle\left\langle X\right|\right)\left|X\right\rangle \\ &= \left|X\right\rangle + \left(e^{i\varphi}-1\right)\left|X\right\rangle\left\langle X|X\right\rangle \\ &= \left|X\right\rangle + e^{i\varphi}\left|X\right\rangle - \left|X\right\rangle = e^{i\varphi}\left|X\right\rangle \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 34.

A continuación se analizará el producto punto entre el marcador:

$$M = e^{i\varphi\left|X\right\rangle\left\langle X\right|}$$

por el vector:

$$\left|W_2\right\rangle = P\left|X\right\rangle - \alpha\left|X\right\rangle$$

$$\begin{aligned} M\left|W_2\right\rangle &= e^{i\varphi\left|X\right\rangle\left\langle X\right|}\left|W_2\right\rangle \\ &= \left(Id + \left(e^{i\varphi}-1\right)\left|X\right\rangle\left\langle X\right|\right)\left|W_2\right\rangle \\ &= \left|W_2\right\rangle + \left(e^{i\varphi}-1\right)\left|X\right\rangle\left\langle X|W_2\right\rangle \\ &= \left|W_2\right\rangle \end{aligned}$$

Por último se analizará el producto punto entre el marcador:

$$M = e^{i\varphi\left|X\right\rangle\left\langle X\right|}$$

por el vector:

$$\left|W_3\right\rangle = P^2\left|X\right\rangle - \beta\left|X\right\rangle - \frac{\left(P\left|X\right\rangle - \alpha\left|X\right\rangle\right)P^2\left|X\right\rangle}{\left(P\left|X\right\rangle - \alpha\left|X\right\rangle\right)^* P\left|X\right\rangle - \alpha\left|X\right\rangle}\left(P\left|X\right\rangle - \alpha\left|X\right\rangle\right)$$

$$\begin{aligned} M\left|W_3\right\rangle &= e^{i\varphi\left|X\right\rangle\left\langle X\right|}\left|W_3\right\rangle \\ &= \left(Id + \left(e^{i\varphi}-1\right)\left|X\right\rangle\left\langle X\right|\right)\left|W_3\right\rangle \\ &= \left|W_3\right\rangle + \left(e^{i\varphi}-1\right)\left|X\right\rangle\left\langle X|W_3\right\rangle \\ &= \left|W_3\right\rangle \end{aligned}$$

Significa que la compuerta de marcador $M = e^{i\varphi\left|X\right\rangle\left\langle X\right|}$, en el subespacio generado por los vectores $\left|X\right\rangle$, $\left|W_2\right\rangle$ y $\left|W_3\right\rangle$ se comporta como la siguiente matriz:

$$\begin{aligned} M &= e^{i\varphi|X\rangle\langle X|} \\ &= Id + i(\sin\phi)P + (\cos\phi - 1)P^2 \\ &= \begin{pmatrix} e^{i\varphi} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Ahora se va a analizar el producto punto del difusor:

$$D = e^{i\phi P} = Id + i(\sin\phi)P + (\cos\phi - 1)P^2$$

por el vector:

$$|W_1\rangle = |X\rangle$$

el vector:

$$|W_2\rangle = P\,|X\rangle - \alpha\,|X\rangle$$

y el vector:

$$|W_3\rangle = P^2\,|X\rangle - \beta\,|X\rangle - \frac{(P\,|X\rangle - \alpha\,|X\rangle)P^2\,|X\rangle}{(P\,|X\rangle - \alpha\,|X\rangle)^* P\,|X\rangle - \alpha\,|X\rangle}(P\,|X\rangle - \alpha\,|X\rangle)$$

Para ello se desarrolla el estado $P\,|X\rangle$:

$$\begin{aligned} P\,|X\rangle &= P\,|X\rangle - \alpha\,|X\rangle + \alpha\,|X\rangle \\ &= |W_2\rangle + \alpha\,|W_1\rangle \\ &= \alpha\,|W_1\rangle + |W_2\rangle \end{aligned}$$

A continuación se analizará el estado $P\,|W_2\rangle$:

$$\begin{aligned} P\,|W_2\rangle &= P^2\,|X\rangle - \alpha P\,|X\rangle \\ &= |W_3\rangle + \frac{\alpha(1-\beta)}{\beta - \alpha^2}\,|W_2\rangle + \beta\,|X\rangle - \alpha P\,|X\rangle \\ &= |W_3\rangle + \frac{\alpha(1-\beta)}{\beta - \alpha^2}\,|W_2\rangle + \beta\,|X\rangle - \alpha\,|W_2\rangle - \alpha^2\,|W_1\rangle \\ &= (\beta - \alpha^2)\,|W_1\rangle + \left(\frac{\alpha(1-\beta)}{\beta - \alpha^2} - \alpha\right)|W_2\rangle + |W_3\rangle \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 35.

Finalmente se analizará el estado $P|W_3\rangle$:

$$\begin{aligned} P|W_3\rangle &= P^3|X\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}(P^2|X\rangle - \alpha P|X\rangle) - \beta P|X\rangle \\ &= P|X\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}P^2|X\rangle + \frac{\alpha^2(1-\beta)}{\beta-\alpha^2}P|X\rangle \\ &= \left(1 + \frac{\alpha^2(1-\beta)}{\beta-\alpha^2} - \beta\right)P|X\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}P^2|X\rangle \\ &= \left(\frac{\alpha^2(1-\beta)}{\beta-\alpha^2} - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2} - \beta + 1\right)|W_2\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}|W_3\rangle \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 36.

De los coeficientes de:

$$P|X\rangle = \alpha|W_1\rangle + |W_2\rangle$$

$$P|W_2\rangle = (\beta-\alpha^2)|W_1\rangle + (\frac{\alpha(1-\beta)}{\beta-\alpha^2} - \alpha)|W_2\rangle + |W_3\rangle$$

$$P|W_3\rangle = (\frac{\alpha^2(1-\beta)}{\beta-\alpha^2} - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2} - \beta + 1)|W_2\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}|W_3\rangle$$

puestos como columnas, se obtiene la siguiente matriz P:

$$P = \begin{pmatrix} \alpha & \beta-\alpha^2 & 0 \\ 1 & -\frac{\alpha(2\beta-\alpha^2-1)}{\beta-\alpha^2} & \frac{(\beta-1)(\beta-\alpha)(\beta+\alpha)}{(\beta-\alpha^2)^2} \\ 0 & 1 & -\frac{\alpha(1-\beta)}{\beta-\alpha^2} \end{pmatrix}.$$

Eso significa que la compuerta del difusor $D = e^{i\phi P} = Id + i(\sin\phi)P + (\cos\phi - 1)P^2$, en el subespacio generado por los vectores $|X\rangle$, $|W_2\rangle$ y $|W_3\rangle$, se comporta como la siguiente matriz:

$$\begin{aligned} D &= e^{i\phi P} \\ &= Id + i(\sin\phi)P + (\cos\phi - 1)P^2 \\ &= \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{pmatrix}. \end{aligned}$$

Donde las entradas de la matriz del difusor $D = e^{i\phi P} = Id + i(\sin\phi)P + (\cos\phi - 1)P^2$ son:

$d_{11} = i\alpha \sin\phi + \beta\cos\phi - \beta + 1,$

$d_{12} = i\beta \sin\phi - i\alpha^2 \sin\phi - \alpha\beta\cos\phi + \alpha\cos\phi + \alpha\beta - \alpha,$

$d_{13} = -\frac{(\beta-1)(\beta-\alpha)(\beta+\alpha)(\cos\phi-1)}{\beta-\alpha^2},$

$d_{21} = \frac{i\beta\sin\phi - i\alpha^2\sin\phi - \alpha\beta\cos\phi + \alpha\cos\phi + \alpha\beta - \alpha}{\beta-\alpha^2},$

$d_{22} = \frac{2i\alpha\beta\sin\phi - i\alpha^3\sin\phi - i\alpha\sin\phi - \alpha^2\beta\cos\phi - \beta\cos\phi + 2\alpha^2\cos\phi + \alpha^2\beta - \alpha^2}{\beta-\alpha^2},$

$d_{23} = -\frac{(\beta-1)(\beta-\alpha)(\beta+\alpha)(i\sin\phi - \alpha\cos\phi + \alpha)}{(\beta-\alpha^2)^2},$

$d_{31} = \cos\phi - 1,$

$d_{32} = i\sin\phi - \alpha\cos\phi + \alpha\mathrm{y}$

$d_{33} = \frac{i\alpha\beta\sin\phi - i\alpha\sin\phi - \beta^2\cos\phi + \beta\cos\phi + \beta^2 - \alpha^2}{\beta-\alpha^2}.$

Se puede observar que tanto la matriz del marcador $M = e^{i\varphi|X\rangle\langle X|}$ como la del difusor $D = e^{i\phi P}$ son matirces unitarias.

El marcador $M = e^{i\varphi|X\rangle\langle X|}$ es una matriz unitaria debido a que:

$$\begin{aligned} MM^* &= e^{i\varphi|X\rangle\langle X|} e^{i\varphi|X\rangle\langle X|^*} \\ &= e^{i\varphi|X\rangle\langle X| - i\varphi|X\rangle\langle X|} \\ &= e^0 \\ &= Id \end{aligned}$$

y también el difusor $D = e^{i\phi P}$ es una matriz unitaria.

Ahora se analizará también el operador extendido de Grover Q, que se forma al multiplicar la matriz del difusor $D = e^{i\phi P}$ por la del marcador $M = e^{i\varphi|X\rangle\langle X|}$, donde dicho operador de Grover se itera k veces hasta lograr encontrar el archivo buscado en la base de datos. La matriz del operador extendido de Grover es:

$$\begin{aligned} Q &= DM \\ &= e^{i\phi P} e^{i\varphi|X\rangle\langle X|} \\ &= (Id + i(\sin\phi)P + (\cos\phi - 1)P^2)(Id + (e^{i\varphi} - 1)\,|X\rangle\,\langle X|) \\ &= \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{pmatrix}. \end{aligned}$$

Donde las entradas de la matriz del operador extendido de Grover Q son:

$q_{11} = (i\alpha \sin\phi + (\cos\phi - 1)\alpha^2 + 1)e^{i\varphi}$,

$q_{12} = i\beta \sin\phi - i\alpha^2 \sin\phi - \alpha\beta\cos\phi + \alpha\cos\phi + \alpha\beta - \alpha$,

$q_{13} = -\frac{(\beta-1)(\beta-\alpha)(\beta+\alpha)(\cos\phi-1)}{\beta-\alpha^2}$,

$q_{21} = \frac{(i\beta \sin\phi - i\alpha^2 \sin\phi - \alpha\beta\cos\phi + \alpha\cos\phi + \alpha\beta - \alpha)e^{i\varphi}}{\beta-\alpha^2}$,

$q_{22} = \frac{2i\alpha\beta \sin\phi - i\alpha^3 \sin\phi - i\alpha \sin\phi - \alpha^2\beta\cos\phi - \beta\cos\phi + 2\alpha^2\cos\phi + \alpha^2\beta - \alpha^2}{\beta-\alpha^2}$,

$q_{23} = -\frac{(\beta-1)(\beta-\alpha)(\beta+\alpha)(i\sin\phi - \alpha\cos\phi + \alpha)}{(\beta-\alpha^2)^2}$,

$q_{31} = (\cos\phi - 1)e^{i\varphi}$,

$q_{32} = i\sin\phi - \alpha\cos\phi + \alpha$y

$q_{33} = \frac{i\alpha\beta \sin\phi - i\alpha \sin\phi - \beta^2\cos\phi + \beta\cos\phi + \beta^2 - \alpha^2}{\beta-\alpha^2}$.

Recordar que cargar la base de datos en la computadora cuántica es colocar $|b\rangle$ en el sistema:

$$|b\rangle = A\,|0\rangle\,.$$

Observación 10.

$$\begin{aligned} \| b \| &= \langle b|b\rangle \\ &= \langle x|\, P^*P\,|x\rangle \\ &= \langle x|\, PP\,|x\rangle = \langle x|\, P^2\,|x\rangle \\ &= \beta \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 37.

$$\begin{aligned} A\,|0\rangle &= |b\rangle \\ &= \frac{1}{\| b \|}\,|b\rangle \\ &= \frac{1}{\| b \|} P\,|X\rangle \\ &= \frac{1}{\sqrt{\beta}}(P\,|X\rangle - \alpha\,|X\rangle) + \frac{\alpha}{\sqrt{\beta}}\,|X\rangle \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 38.

Así el trabajo será ahora analizar:

$$Q^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma_k \\ \eta_k \\ \mu_k \end{pmatrix}.$$

También sabemos que el operador generalizado de Grover es: $Q = DM = e^{i\phi P} e^{i\varphi |X\rangle\langle X|}$, entonces,

$$(DM)^k A\,|0\rangle = (e^{i\phi P} e^{i\varphi |X\rangle\langle X|})^k A\,|0\rangle = \gamma_k\,|W_1\rangle + \eta_k\,|W_2\rangle + \mu_k\,|W_3\rangle)$$

El objetivo de este operador generalizado de Grover es que: $|\ \mu_k\ |^2 \approx 0$, $|\ \eta_k\ |^2 \approx 0$ y $|\ \gamma_k\ |^2 \approx 1$.

Luego:

$$\begin{aligned} \langle W_1|\, e^{i\phi P} e^{i\varphi |X\rangle\langle X|} A\,|0\rangle &= \gamma_k \langle W_1|W_1\rangle + \eta_k \langle W_1|W_2\rangle + \mu_k \langle W_1|W_3\rangle \\ &= \gamma_k(1) + \eta_k(0) + \mu_k(0) \\ &= \gamma_k \end{aligned}$$

y también:

$$\begin{pmatrix} 1, & 0, & 0 \end{pmatrix} Q^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} = \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} \begin{pmatrix} \gamma_k \\ \eta_k \\ \mu_k \end{pmatrix}$$

con $k = 0, 1, 2, \ldots$

3.6. Cálculos de probabilidad a través de series formales.

Al analizar la simulación del algoritmo generalizado de Grover para el caso tripotente, se observó que existen otros ángulos de marcado y difusión con los cuales se encuentra el vector $|X\rangle$ que es la solución del sistema de ecuaciones $P\,|X\rangle = |b\rangle$. Estos ángulos de marcado y difusión son múltiplos de los ángulos que se presentan en la simulación anterior, el conjunto de estos múltiplos nos generan una serie formal de ángulos con los que es posible alcanzar el vector solución $|X\rangle$.

Por ejemplo si el ángulo inicial de marcado es $\frac{2\pi}{3}$ con el que se encuentra el vector solución del sistema de ecuaciones, otros ángulos con el que se alcanza la misma solución son: $\frac{4\pi}{3}$, $\frac{6\pi}{3}$, $\frac{8\pi}{3}$, etc.

Esto se debe a que la matriz de marcado es análoga a una matriz de rotación, la cual al rotar en un ángulo múltiplo del inicial con el que se encontró el vector solución $|X\rangle$, se vuelve a encontrar el mismo vector solución al sistema de ecuaciones.

Una serie formal es semejante a un ˜tendedero ˝en el cual se pueden colocar ordenadamente todos los ángulos con los cuales es posible alcanzar la misma solución $|X\rangle$.

Ahora consideraremos la función generatriz $g(x) = \sum_{k=0}^{\infty} \gamma_k x^k$ con $k = 0, 1, 2, \ldots$

$$\begin{aligned} g(x) &= \sum_{k=0}^{\infty} \gamma_k x^k \\ &= \sum_{k=0}^{\infty} \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} Q^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} x^k \\ &= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} (Id - Qx)^{-1} \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 39.

Cabe mencionar que x es una variable dummy, y que el operador generalizado de Grover es la matriz antes mencionada:

$$Q = \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{pmatrix}$$

por otro lado, si:

$$g(x) = \gamma_0 x^0 + \gamma_1 x^1 + \gamma_2 x^2 + \ldots = \sum_{k=0}^{\infty} \gamma_k x^k = \sum_{k=0}^{\infty} \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} Q^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} x^k$$

$$= \frac{(\alpha \cos\phi - i\beta \sin\phi)x^2 + (i\beta \sin\phi - \alpha \cos\phi - \alpha)x + \alpha}{\sqrt{\beta}(-\sin^2\phi - \cos^2\phi)e^{i\varphi}x^3 + \sqrt{\beta}((\beta \sin^2\phi + i\alpha \sin\phi + \beta \cos^2\phi}$$

$$\overline{+(2-\beta)\cos\phi)e^{i\varphi} + (1-\beta)\sin^2\phi - i\alpha \sin\phi + (1-\beta)\cos^2\phi + \beta\cos\phi)x^2}$$

$$\overline{+\sqrt{\beta}((-i\alpha \sin\phi - \beta\cos\phi + \beta - 1)e^{i\varphi} + i\alpha \sin\phi + (\beta-2)\cos\phi - \beta)x + \sqrt{\beta}}.$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 40.

Luego, si $\varphi \neq \phi$, entonces:

$$g(x) = \frac{(\alpha\cos\phi - i\beta\sin\phi)x^2 + (i\beta\sin\phi - \alpha\cos\phi - \alpha)x + \alpha}{\sqrt{\beta}(-\sin^2\phi - \cos^2\phi)e^{i\varphi}x^3 + \sqrt{\beta}((\beta\sin^2\phi + i\alpha\sin\phi + \beta\cos^2\phi + (2-\beta)\cos\phi)e^{i\varphi} + (1-\beta)\sin^2\phi}$$

$$\overline{-i\alpha\sin\phi + (1-\beta)\cos^2\phi + \beta\cos\phi)x^2 + \sqrt{\beta}((-i\alpha\sin\phi - \beta\cos\phi + \beta - 1)e^{i\varphi} + i\alpha\sin\phi + (\beta-2)\cos\phi - \beta)x + \sqrt{\beta}}.$$

También, podemos considerar a la generatriz $g(x)$ como: $g(x) = \frac{Ax^2+Bx+C}{Dx^3+Ex^2+Fx+G}$, entonces,

$$\begin{aligned}
Ax^2 + Bx + C &= g(x)(Dx^3 + Ex^2 + Fx + G) \\
&= \sum_{k=0}^{\infty} \gamma_k x^k (Dx^3 + Ex^2 + Fx + G) \\
&= \sum_{k=0}^{\infty} D\gamma_k x^{k+3} + \sum_{k=0}^{\infty} E\gamma_k x^{k+2} + \sum_{k=0}^{\infty} F\gamma_k x^{k+1} + \sum_{k=0}^{\infty} G\gamma_k x^k \\
&= G\gamma_0 + (F\gamma_0 + G\gamma_1)x + (E\gamma_0 + F\gamma_1 + G\gamma_2)x^2 \\
&+ \sum_{j=3}^{\infty} (D\gamma_{j-3} + E\gamma_{j-2} + F\gamma_{j-1} + G\gamma_j)x^j.
\end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 41.

Por lo tanto: $E\gamma_0 + F\gamma_1 + G\gamma_2 = A$, $F\gamma_0 + G\gamma_1 = B$, $G\gamma_0 = C$ y $D\gamma_{j-3} + E\gamma_{j-2} + F\gamma_{j-1} + G\gamma_j = 0$, si $j \geq 3$.

Luego: $\gamma_0 = \frac{C}{G}$, $\gamma_1 = \frac{B - F\gamma_0}{G}$, $\gamma_2 = \frac{A - F\gamma_1 - E\gamma_0}{G}$ y $\gamma_j = \frac{-D\gamma_{j-3} - E\gamma_{j-2} - F\gamma_{j-1}}{G}$.

Debido a que: $g(x) = \frac{Ax^2+Bx+C}{Dx^3+Ex^2+Fx+G}$ y también

$$g(x) = \frac{(\alpha\cos\phi - i\beta\sin\phi)x^2 + (i\beta\sin\phi - \alpha\cos\phi - \alpha)x + \alpha}{\sqrt{\beta}(-\sin^2\phi - \cos^2\phi)e^{i\varphi}x^3 + \sqrt{\beta}((\beta\sin^2\phi + i\alpha\sin\phi + \beta\cos^2\phi + (2-\beta)\cos\phi)e^{i\varphi} + (1-\beta)\sin^2\phi}$$

$$\overline{-i\alpha\sin\phi + (1-\beta)\cos^2\phi + \beta\cos\phi)x^2 + \sqrt{\beta}((-i\alpha\sin\phi - \beta\cos\phi + \beta - 1)e^{i\varphi} + i\alpha\sin\phi + (\beta-2)\cos\phi - \beta)x + \sqrt{\beta}}.$$

entonces:

$$\begin{aligned}
\gamma_0 &= \frac{C}{G} \\
&= \frac{\alpha\beta^4 - 4\alpha^3\beta^3 + 6\alpha^5\beta^2 - 4\alpha^7\beta + \alpha^9}{\sqrt{\beta}(\beta^4 - 4\alpha^2\beta^3 + 6\alpha^4\beta^2 - 4\alpha^6\beta + \alpha^8)} \\
&= \frac{\alpha}{\sqrt{\beta}}
\end{aligned}$$

$$\gamma_1 = \frac{B - F\gamma_0}{G}$$
$$= \frac{i\alpha^2 \sin\phi e^{i\varphi} + \alpha\beta\cos\phi e^{i\varphi} - \alpha\beta e^{i\varphi} + \alpha e^{i\varphi} + i\beta\sin\phi}{\frac{-i\alpha^2\sin\phi - \alpha\beta\cos\phi + \alpha\cos\phi + \alpha\beta - \alpha}{\sqrt{\beta}}}$$
$$= \frac{-(\alpha^2\sin\phi - i\alpha\beta\cos\phi + i\alpha\beta - i\alpha)\sin\varphi + (-i\alpha^2\sin\phi - \alpha\beta\cos\phi}{\frac{+\alpha\beta - \alpha)\cos\varphi + (i\alpha^2 - i\beta)\sin\phi + (\alpha\beta - \alpha)\cos\phi - \alpha\beta + \alpha)}{\sqrt{\beta}}}$$

$$\gamma_2 = \frac{A - F\gamma_1 - E\gamma_0}{G}$$
$$= \frac{-((((2i\alpha\beta^2 + 2i\alpha^3)\sin^2\phi + (4\alpha^2\beta\cos\phi - 4\alpha^2\beta + 2\alpha^2)\sin\phi + (4i\alpha\beta^2 - 4i\alpha\beta)}{\cos\phi - 4i\alpha\beta^2 + 4i\alpha\beta - 2i\alpha)\cos\varphi + (-2i\alpha\beta^2 + 4i\alpha\beta - 2i\alpha^3)\sin^2\phi + ((\beta^2 - 4\alpha^2\beta}$$
$$\frac{+3\alpha^2)\cos\phi - \beta^2 + (4\alpha^2 + 1)\beta - 4\alpha^2)\sin\phi + (-4i\alpha\beta^2 + 5i\alpha\beta - i\alpha)\cos\phi + 4i\alpha\beta^2}{-5i\alpha\beta + i\alpha)\sin\varphi + ((2\alpha\beta^2 + 2\alpha^3)\sin^2\phi + (-4i\alpha^2\beta\cos\phi + 4i\alpha^2\beta - 4i\alpha^2)\sin\phi}$$
$$\frac{+(4\alpha\beta^2 - 4\alpha\beta)\cos\phi - 4\alpha\beta^2 + 4\alpha\beta - 2\alpha)\cos^2\varphi + ((-2\alpha\beta^2 + 4\alpha\beta - 2\alpha^3)\sin^2\phi}{+((-i\beta^2 + 4i\alpha^2\beta - 3i\alpha^2)\cos\phi + i\beta^2 + (-4i\alpha^2 - i)\beta + 4i\alpha^2)\sin\phi + (-4\alpha\beta^2}$$
$$\frac{+5\alpha\beta - \alpha)\cos\phi + 4\alpha\beta^2 - 5\alpha\beta + \alpha)\cos\varphi + (2\alpha - 4\alpha\beta)\sin^2\phi + ((i\beta^2 - 2i\beta}{+3i\alpha^2)\cos\phi - i\beta^2 + i\beta)\sin\phi + (\alpha - \alpha\beta)\cos\phi + \alpha\beta)}{\sqrt{\beta}}$$

y $\gamma_j = \frac{-D\gamma_{j-3} - E\gamma_{j-2} - F\gamma_{j-1}}{G}$.

Tenemos que $P|x\rangle = |b\rangle$ con $|b\rangle \neq 0$, debido a que no tiene sentido que no tengamos ningun archivo en nuestra base de datos.

También debemos tomar en cuenta que α y β, no puede tomar cualquier valor en estas expresiones, y para ello mostraremos el siguiente teorema:

Teorema 9. Si:

1. $P^3 = P$,
2. $P^* = P$,

3. $\langle x|x\rangle = 1$,
4. $P\,|x\rangle \neq \langle x|\,P\,|x\rangle\,|x\rangle$ y
5. $\langle x|\,P^2\,|x\rangle \neq 1$.

Entonces, $0 \leq \langle x|\,P\,|x\rangle < \beta = \langle x|\,P^2\,|x\rangle < 1$, y P^2 es idempotente; es decir, $(P^2)^2 = P^4 = P^3P = PP = P^2$. Por lo tanto $1 \geq \langle x|\,P^2\,|x\rangle \geq 0$.

Demostración. Sea $\alpha = \langle x|\,P\,|x\rangle$, $\beta = \langle x|\,P^2\,|x\rangle$, $|w_1\rangle = |x\rangle$ y $|w_2\rangle = P\,|x\rangle - \alpha\,|x\rangle$. Sabemos que $|w_1\rangle \perp |w_1\rangle$. Luego: $0 \geq \| \, |w_2\rangle \, \|^2$, debido a que las normas al cuadrado son siempre son positivas. Entonces, tenemos que:

$$\begin{aligned} \| \, |w_2\rangle \, \|^2 &= \langle w_2|w_2\rangle \\ &= (\langle x|\,P - \alpha\,\langle x|)(P\,|x\rangle - \alpha\,|x\rangle) \\ &= \langle x|\,P^2\,|x\rangle - \alpha\,\langle x|\,P\,|x\rangle - 0 \\ &= \beta - \alpha\alpha = \beta - \alpha^2 \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 42.

Por lo tanto $0 < \beta - \alpha^2$ y $\alpha^2 < \beta$. En particular $\alpha^2 \neq \beta$. □

Sabemos también que $|w_3\rangle$ es ortogonal a $|w_2\rangle$ y a $|w_1\rangle$. Luego:

$$|w_3\rangle = P^2\,|x\rangle - \beta P\,|x\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\,|w_2\rangle\,.$$

También sabemos que $|w_2\rangle \perp |w_3\rangle$ y

$$\begin{aligned} \| \, |w_3\rangle \, \|^2 &= \langle w_3|w_3\rangle \\ &= \left(\langle x|\,(P^2)^* - \beta\,\langle x|\,P^* - \langle w_2|\,\frac{\alpha(1-\beta)}{\beta-\alpha^2}\right)\left(P^2\,|x\rangle - \beta P\,|x\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\,|w_2\rangle\right) \\ &= \left(\langle x|\,P^2 - \beta\,\langle x|\,P\right)\left(P^2\,|x\rangle - \beta P\,|x\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\,|w_2\rangle\right) \\ &= (1-\beta)\left(\beta - \alpha\frac{\alpha(1-\beta)}{\beta-\alpha^2}\right) = \beta - \beta^2 - \frac{\alpha^2(1-\beta)^2}{\beta-\alpha^2} \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 43.

Por lo tanto $0 < \beta - \beta^2 - \frac{\alpha^2(1-\beta)^2}{\beta-\alpha^2}$,

$$\frac{\alpha^2(1-\beta)^2}{\beta-\alpha^2} < \beta - \beta^2,$$

$$\frac{\alpha^2(1-\beta)^2}{\beta-\alpha^2} < \beta(1-\beta),$$

$$\frac{\alpha^2(1-\beta)^2}{1-\beta} < \beta(\beta-\alpha^2),$$

$$\alpha^2(1-\beta) < \beta(\beta-\alpha^2),$$

$$\alpha^2 - \alpha^2\beta < \beta^2 - \beta\alpha^2,$$

$$\alpha^2 < \beta^2,$$

$$\sqrt{\alpha^2} < \sqrt{\beta^2},$$

$$\alpha < \beta,$$

por lo tanto $0 \leq \mid \alpha \mid < \beta < 1$.

Se puede concluir que existen otros ángulos de marcado y difusión con los cuales es posible encontrar la solución $|\beta\rangle$. Esto se debe a que el vector de marcado es análogo a un vector de rotación, el cual vuelve a encontrar la solución al rotar.

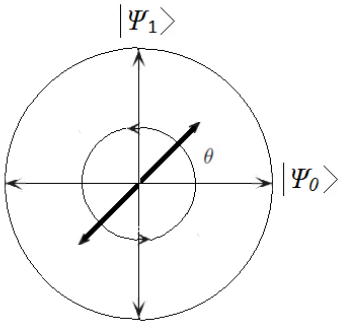

FIGURA 3.5: Vector de marcado rotando para hallar la solución del sistema de ecuaciones.

La serie formal contiene todos los ángulos con los cuales es posible alcanzar la solución del sistema de ecuaciones, y se puede expresar como una sumatoria infinita.

Un ejemplo de esta sumatoria sería:

$$g\left(\frac{2\pi}{3}, \pi, z\right) = \frac{iz}{2} - iz^2 + \frac{iz^3}{2} + \frac{iz^5}{2} - iz^6 + \cdots$$

Dicha serie formal de ángulos, se ocupará después en la simulación de un ejemplo concreto.

3.7. Construcción de matrices tripotentes.

En esta sección se darán a conocer las técnicas para construir matrices tripotentes a partir de matrices idempotentes, así como también se mostrará la estrecha relación que existe entre las matrices tripotentes e idempotentes.

Sea P una matriz idempotente entonces $P \otimes N$ es una matriz tripotente, donde N es la matriz de negación.

$$N = \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

También se puede demostrar que la diferencia entre dos matrices idempotentes, genera una matriz tripotente; es decir, si A y B son dos matrices idempotentes, $A - B$ es una matriz tripotente.

Teorema 10. Así, una matriz P es hermitiana y tripotente, si y sólo si, existe una matriz A y una matriz B idempotentes y hermitianas, tales que $P = A - B$, con $AB = 0$ y $BA = 0$.

Demostración. Entonces se tiene que: $P = A - B$ con $A^2 = A$ y $B^2 = B$; por lo tanto,

$$\begin{aligned} P^2 &= (A - B)(A - B) \\ &= A^2 - AB - BA + B^2 \\ &= A + B \end{aligned}$$

y similarmente:

$$\begin{aligned} P^3 &= (A-B)^2(A-B) \\ &= (A-B)(A-B) \\ &= A^2 - B^2 \\ &= A - B = P. \end{aligned}$$

Entonces también tenemos:

$$\begin{aligned} P^* &= (A-B)^* \\ &= A^* - B^* \\ &= A - B \\ &= P. \end{aligned}$$

Se sabe que $P = P^*$, entonces P es una matriz normal, es decir, $PP^* = P^*P$.

Implica por el teorema espectral, que existe una matriz U unitaria y una matriz D matriz diagonal tal que $P = UDU^{-1}$ con:

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

donde $\lambda_1, \lambda_2, \ldots, \lambda_n$ son los valores propios de la matriz, y ${\lambda_i}^3 = \lambda_i$, con $\lambda_i = 0, 1y - 1$. Si se sustituyen los valores propios $0, 1y - 1$ en la matriz D, se obtiene:

$$D = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & -1 & 0 & 0 \\ 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}.$$

La matriz P de coeficientes se puede formar uttilizando la matriz diagonal D de la siguiente manera:

$$\begin{aligned} P &= U(D)U^{-1} \\ &= U(D_1 - D_2)U^{-1} \\ &= UD_1U^{-1} - UD_2U^{-1} \end{aligned}$$

con $UD_1U^{-1} = A$ y $UD_2U^{-1} = B$.

A es matriz idempotente, es decir,

$$\begin{aligned} A^2 &= UD_1U^{-1}UD_1U^{-1} \\ &= UD_1{}^2U^{-1} \\ &= AD_1U^{-1} = A. \end{aligned}$$

Además,

$$\begin{aligned} AB &= UD_1U^{-1}UD_2U^{-1} \\ &= UD_1D_2U^{-1} \\ &= 0 \end{aligned}$$

y

$$\begin{aligned} BA &= UD_2U^{-1}UD_1U^{-1} \\ &= UD_2D_1U^{-1} \\ &= 0. \end{aligned}$$

También,

$$\begin{aligned} A^* &= (U(D)U^{-1})^* \\ &= (U^{-1})^*(D_1)^*U^* \\ &= (U^*)^*D_1U^{-1} \\ &= UD_1U^{-1} = A. \end{aligned}$$

□

Por otro lado, si se tiene un sistema de ecuaciones $P\,|X\rangle = |b\rangle$, donde P es una matriz tripotente, al multiplicar ambos lados del sistema de ecuaciones por la matriz P, se obtiene:

$$PP\,|X\rangle = P\,|b\rangle$$

$$P^2\,|X\rangle = P\,|b\rangle$$

donde P^2 es una matriz de coeficientes idempotente, $|X\rangle$ es el vector de incógnitas y ahora $P\,|b\rangle$ es el vector cuyas entradas son conocidas.

Se puede concluir por este razonamiento que el caso de un sistema de ecuaciones con una matriz de coeficientes idempotente, engloba al caso donde se tiene un sistema de ecuaciones con una matriz tripotente.

Capítulo 4

Simulación y resultados

En el presente capítulo se presentará la simulación que se realizó del algoritmo cuántico propuesto como solución a un sistema de ecuaciones, donde la matriz de coeficientes es singular, hermitiana y tripotente. Dicha simulación se dará a conocer a través de un ejemplo concreto, donde se presentará la matriz de coeficientes P, el vector de incógnitas $|x\rangle$ y el vector de resultados $|b\rangle$ del ejemplo.

Se presentará la solución al sistema de ecuaciones propuesto y también cada resultado de la simulación hasta llegar a conocer los valores del vector de incógnitas $|x\rangle$.

4.1. Simulación.

Simular: es realizar los cálculos; es decir, la multiplicación de matrices unitarias para llegar al resultado deseado [2].

La simulación del algoritmo generalizado de Grover para el caso tripotente se realizó con el software de wx-Maxima, version 11.08, dicho software se utilizó debido a que se especializa en realizar cálculos simbólicos.

Ejemplo 15. *Problema a resolver:* encontrar $|X\rangle$ en $P|X\rangle = |b\rangle$, donde P es la matriz de coeficientes y es una matriz singular, hermitiana, tripotente y no idempotente.

Para este ejemplo la matriz P será:

$$P = \begin{pmatrix} 0 & \frac{3}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} \\ \frac{3}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{3}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} \\ \frac{1}{4} & 0 & \frac{3}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\ 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{3}{4} & 0 & \frac{1}{4} \\ -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{3}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{3}{4} \\ \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{3}{4} & 0 \end{pmatrix}.$$

El vector de incógnitas $|X\rangle$ que se desea encontrar es:

$$|X\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

Cabe notar que el valor $|X\rangle$ no es conocido pero si es posible distinguirlo.

El vector de resultados $|b\rangle$ es:

$$|b\rangle = \begin{pmatrix} \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

El primer paso del algoritmo es cargar $|b\rangle$ en la computadora cuántica, para ello se parte de un estado inicial, el cual en el ejemplo es $|1\rangle$.

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

Después se multiplica dicho vector por una matriz A, que es unitaria y que permitirá que se realice la transición en la computadora cuántica del estado inicial al estado donde ya se tiene en memoria el vector $|b\rangle$.

Una matriz A que es posible implementar en una computadora cuántica es la matriz de *Walsh-Hadamard* ó el producto tensiorial de matrices de *Walsh-Hadamard* [10].

En este ejemplo la matriz A es:

$$A = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

El resultado de multiplicar el vector inicial $|1\rangle$ por la matriz unitaria A es:

$$A\,|1\rangle = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix}.$$

El segundo paso es multiplicar este vector resultante por el operador generalizado de Grover Q.

El sistema de ecuaciones de este ejemplo se resolvió con sólo dos iteraciones de operador generalizado de Grover Q. Recordemos que para formar el operador generalizado de Grover Q, se necesita la multiplicación de dos matrices, una es la matriz del marcador $M = e^{i\varphi|X\rangle\langle X|}$ y otra es la matriz del difusor $D = e^{i\phi P}$, donde el operador generalizado de Grover Q es el resultado de dicho producto.

$$\begin{aligned} Q &= DM \\ &= e^{i\phi P} e^{i\varphi|X\rangle\langle X|} \\ &= (Id + i(\sin\phi)P + (\cos\phi - 1)P^2)(Id + (e^{i\varphi} - 1)|X\rangle\langle X|). \end{aligned}$$

La matriz del marcador es $M = e^{i\varphi|X\rangle\langle X|}$, pero en el ejemplo el ángulo de marcado es $\varphi = \pi$, entonces la matriz del marcador $M = e^{i\varphi|X\rangle\langle X|}$ se simplifica a:

$$
\begin{aligned}
M &= e^{i\varphi|X\rangle\langle X|} \\
&= Id + (e^{i\varphi} - 1)|X\rangle\langle X| \\
&= Id + (e^{i\pi} - 1)|X\rangle\langle X| \\
&= \begin{pmatrix}
-\frac{2^{\frac{3}{2}}-3}{6} & 0 & \frac{1}{6} & 0 & -\frac{2^{\frac{3}{2}}+3}{6} & 0 & \frac{1}{6} & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}+3}{6} & 0 & \frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}-3}{6} & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-\frac{2^{\frac{3}{2}}+3}{6} & 0 & \frac{1}{6} & 0 & -\frac{2^{\frac{3}{2}}-3}{6} & 0 & \frac{1}{6} & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}-3}{6} & 0 & \frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}+3}{6} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\end{aligned}
$$

Y la matriz del difusor es $D = e^{i\phi P}$, pero debido a que en el ejemplo el ángulo para difundir es $\phi = \frac{2\pi}{3}$, entonces la matriz del difusor $D = e^{i\phi P}$ se simplifica a:

$$
\begin{aligned}
D &= e^{i\phi P} \\
&= Id + i(\sin\phi)P + (\cos\phi - 1)P^2 \\
&= Id + i(\sin\frac{2\pi}{3})P + (\cos\frac{2\pi}{3} - 1)P^2 \\
&= \begin{pmatrix}
-\frac{1}{8} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{3}{8} & -\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} \\
\frac{3^{\frac{3}{2}}i}{8} & -\frac{1}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & -\frac{\sqrt{3}i}{8} & \frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} \\
-\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{1}{8} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{3}{8} & -\frac{\sqrt{3}i}{8} \\
\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{1}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & -\frac{\sqrt{3}i}{8} & \frac{3}{8} \\
-\frac{3}{8} & -\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{1}{8} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} \\
-\frac{\sqrt{3}i}{8} & \frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{1}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} \\
-\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{3}{8} & -\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{1}{8} & \frac{3^{\frac{3}{2}}i}{8} \\
\frac{\sqrt{3}i}{8} & -\frac{3}{8} & -\frac{\sqrt{3}i}{8} & \frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{1}{8}
\end{pmatrix}.
\end{aligned}
$$

Con la matriz del marcador y el difusor simplificadas, y adecuadas al ejemplo que se esta simulando, se obtiene una nueva matriz Q, que es la matriz del operador generalizado de Grover para el ejemplo.

$$
\begin{aligned}
Q &= DM \\
&= e^{i\phi P} e^{i\varphi |X\rangle\langle X|} \\
&= (Id + i(\sin\phi)P + (\cos\phi - 1)P^2)(Id + (e^{i\varphi} - 1)|X\rangle\langle X|) \\
&= (Id + i(\sin\frac{2\pi}{3})P + (\cos\frac{2\pi}{3} - 1)P^2)(Id + (e^{i\pi} - 1)|X\rangle\langle X|) \\
&= \begin{pmatrix}
-\frac{2^{\frac{3}{2}}+9}{24} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{32^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}i}{8} & -\frac{2^{\frac{3}{2}}-3}{24} & -\frac{\sqrt{3}i}{8} & -\frac{32^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}i}{8} \\
-\frac{(2^{\frac{3}{2}}-7)i}{8\sqrt{3}} & -\frac{1}{8} & \frac{(2^{\frac{3}{2}}+1)i}{8\sqrt{3}} & -\frac{3}{8} & -\frac{(2^{\frac{3}{2}}+5)i}{8\sqrt{3}} & \frac{3}{8} & \frac{(2^{\frac{3}{2}}+1)i}{8\sqrt{3}} & -\frac{3}{8} \\
\frac{32^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}i}{8} & \frac{2^{\frac{3}{2}}-9}{24} & \frac{3^{\frac{3}{2}}i}{8} & \frac{32^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}i}{8} & \frac{2^{\frac{3}{2}}+3}{24} & -\frac{\sqrt{3}i}{8} \\
-\frac{(2^{\frac{3}{2}}-1)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{(2^{\frac{3}{2}}+7)i}{8\sqrt{3}} & -\frac{1}{8} & -\frac{(2^{\frac{3}{2}}-1)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{(2^{\frac{3}{2}}-5)i}{8\sqrt{3}} & \frac{3}{8} \\
-\frac{2^{\frac{3}{2}}-3}{24} & -\frac{\sqrt{3}i}{8} & -\frac{32^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}i}{8} & -\frac{2^{\frac{3}{2}}+9}{24} & \frac{3^{\frac{3}{2}}i}{8} & -\frac{32^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}i}{8} \\
-\frac{(2^{\frac{3}{2}}+5)i}{8\sqrt{3}} & \frac{3}{8} & \frac{(2^{\frac{3}{2}}+1)i}{8\sqrt{3}} & -\frac{3}{8} & -\frac{(2^{\frac{3}{2}}-7)i}{8\sqrt{3}} & -\frac{1}{8} & \frac{(2^{\frac{3}{2}}+1)i}{8\sqrt{3}} & -\frac{3}{8} \\
\frac{32^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}i}{8} & \frac{2^{\frac{3}{2}}+3}{24} & -\frac{\sqrt{3}i}{8} & \frac{32^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}i}{8} & \frac{2^{\frac{3}{2}}-9}{24} & \frac{3^{\frac{3}{2}}i}{8} \\
-\frac{(2^{\frac{3}{2}}-1)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{(2^{\frac{3}{2}}-5)i}{8\sqrt{3}} & \frac{3}{8} & -\frac{(2^{\frac{3}{2}}-1)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{(2^{\frac{3}{2}}+7)i}{8\sqrt{3}} & -\frac{1}{8}
\end{pmatrix}.
\end{aligned}
$$

Después se multiplica el operador generalizado de Grover Q por el vector resultante de multiplicar $A|1\rangle$ y entonces se obtiene el vector $QA|1\rangle$:

$$
QA|1\rangle = \begin{pmatrix}
\frac{\sqrt{3}i}{4} \\ -\frac{1}{4} \\ \frac{\sqrt{3}i}{4} \\ -\frac{1}{4} \\ \frac{\sqrt{3}i}{4} \\ -\frac{1}{4} \\ \frac{\sqrt{3}i}{4} \\ -\frac{1}{4}
\end{pmatrix}.
$$

El tercer paso es realizar una segunda iteración del operador generalizado de Grover Q para obtener el vector $Q^2A|1\rangle$, es decir,

$$
Q^2A|1\rangle = \begin{pmatrix}
-\frac{(\sqrt{2}+1)i}{2\sqrt{3}} \\ 0 \\ \frac{(\sqrt{2}-1)i}{2\sqrt{3}} \\ 0 \\ -\frac{(\sqrt{2}+1)i}{2\sqrt{3}} \\ 0 \\ \frac{(\sqrt{2}-1)i}{2\sqrt{3}} \\ 0
\end{pmatrix}.
$$

Dicho vector $Q^2A\,|1\rangle$ es la solución del sistema de ecuaciones $P\,|x\rangle = |b\rangle$; es decir, el vector $Q^2A\,|1\rangle$ es igual al vector $|x\rangle$, salvo una fase global, que en el ejemplo es igual a $-i$.

Así el vector $|x\rangle$ es:

$$|x\rangle = \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}$$

y el vector $Q^2A\,|1\rangle$ es:

$$Q^2A\,|1\rangle = \begin{pmatrix} -\frac{(\sqrt{2}+1)i}{2\sqrt{3}} \\ 0 \\ \frac{(\sqrt{2}-1)i}{2\sqrt{3}} \\ 0 \\ -\frac{(\sqrt{2}+1)i}{2\sqrt{3}} \\ 0 \\ \frac{(\sqrt{2}-1)i}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

4.2. Resultados.

Los resultados que arroja la simulación son:

1. A través del algoritmo propuesto para el caso tripotente, sí se obtiene la solución del sistema de ecuaciones propuesto al inicio de la simulación.

2. Los ángulos de marcado y difusión no necesariamente son iguales en el caso tripotente, mientras que en el caso idepotente sí deben ser iguales.

3. Es importante aclarar que con el algoritmo cuántico generalizado de Grover para el caso idempotente, también se puede resolver el sistema de ecuaciones, pero partiendo de otras condiciones, por ejemplo el ángulo de marcado y el ángulo de difusión deben ser iguales, la matriz unitaria A del primer paso puede tener otra forma y eso puede tener implicaciones en el momento de la implementación física, por lo que se plantea el algoritmo cuántico generalizado de Grover para el caso tripotente como

una opción más para resolver sistemas de ecuaciones donde la matriz de coeficientie es singular, hermitiana y tripotente.

Capítulo 5

Corrección al algoritmo de amplificación de amplitud cuántica

En éste capítulo se realizará una modificación al algoritmo de amplificación de amplitud cuántica, dicha modificación consistirá en hacer una generalización del algoritmo de amplificación de amplitud cuántica, de tal forma que sea posible encontrar con certeza, en un subespacio invariante de tres dimensiones, un estado deseado, dicho estado contiene los archivos que son buscados dentro de una base de datos no estructurada.

5.1. Modificaciones al algoritmo de amplificación de amplitud.

El presente trabajo de tesis, pretende afirmar: que un estado deseado, puede encontrarse con *certeza* a través del algoritmo extendido de Grover en un subespacio invariante posible de tres dimensiones, a diferencia de lo que afirman Jin, W. L. y Chen, X. D. en su artículo sobre información cuántica donde mencionan que un estado deseado, no puede encontrarse con certeza dentro de un subespacio posible de tres dimensiones a través del algoritmo de amplificación de amplitud cuántica, que es una generalización del algoritmo de Grover [9].

En el contexto de amplificación de amplitud cuántica:

Sea A un algoritmo (sin medición) con un estado inicial $|s\rangle$. La posibilidad de éxito del algoritmo A es mayor que 0 y menor que 1; es decir, $0 < a < 1$, donde a es la posiblidad de éxito del algoritmo A.

Sea también $T = X_0, X_1, \ldots, X_{N-1}$, un conjunto de elementos de una base de datos, tales que $A|s\rangle = \sum_{i=0}^{N-1} C_i |X_i\rangle$ para ciertas amplitudes $C_0, C_1, \ldots, C_{N-1}$ que son complejas y

$$\langle X_i | X_j \rangle = \begin{cases} 0 & , \text{si } i \neq j \\ 1 & , \text{si } i = j \end{cases}$$

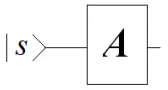

FIGURA 5.1: Modelo de circuito del algoritmo $A|s\rangle$.

Lo que se quiere es mejorara la probabilidad de éxito del algoritmo A.

El algoritmo de amplificación de amplitud cuántica es el siguiente:

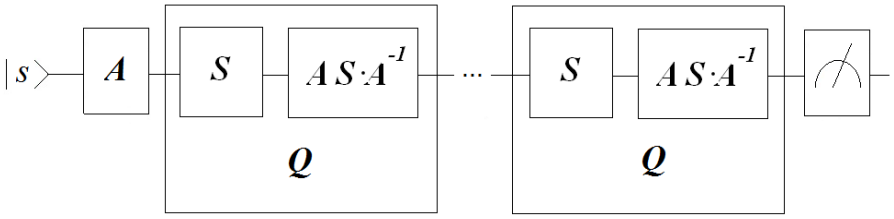

FIGURA 5.2: Modelo de circuito del algoritmo de amplificación de amplitud cuántica, donde $Q = AS \cdot A^{-1}S$.

En principio podemos escribir: $A|s\rangle = \sum_{X_i \in B} C_i |X_i\rangle + \sum_{X_i \notin B} C_i |X_i\rangle$, donde B es el conjunto de los archivos que se buscan (estados buenos). Pero también podemos escribir: $A|s\rangle = |\psi_1\rangle + |\psi_0\rangle$, donde $|\psi_1\rangle$ son los estados buenos y $|\psi_0\rangle$ los estados malos; es decir que, $A|s\rangle = |buenos\rangle + |malos\rangle$, con $\langle buenos|malos\rangle = 0$.

Ahora se supone que el espacio de búsqueda esta incluido en un espacio más grande, además se asume que los estados malos son muchos y que tienen mucho espacio hacia abajo, por lo que se descomponen en dos partes, de tal manera que el estado $A|s\rangle$ no esté en el espacio generado por los estados buenos y sólo una parte de los estados malos:

$$A|s\rangle = |\psi_1\rangle + |\psi_{0,1}\rangle + |\psi_{0,2}\rangle .$$

Así tenemos tres vectores que son linealmente independientes:

1. El vector de los estados buenos: $|\psi_1\rangle$,
2. El vector de los estados malos: $|\psi_0\rangle$ y
3. El vector $A|s\rangle$.

Jin, W. L. y Chen, X. D. ponen como estado inicial, al vector de norma uno: $|\gamma_0\rangle = |\psi_1\rangle + |\psi_{0,1}\rangle$, el cuál tiene a los estados buenos y sólo una parte de los malos. A diferencia del vector $A|s\rangle$, que es una combinación lineal de los estados buenos y las dos partes que forman los estados malos:

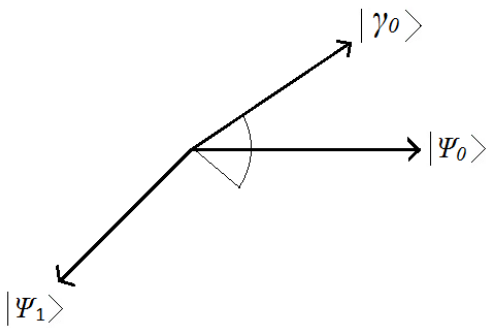

FIGURA 5.3: $|\gamma_0\rangle$ no está en el espacio generado por los estados buenos $|\psi_1\rangle$ y los estados malos $|\psi_0\rangle$.

$$A\,|s\rangle = |\psi_1\rangle + |\psi_{0,1}\rangle + |\psi_{0,2}\rangle\,.$$

También el vector del estado inicial $|\gamma_0\rangle$ se puede normalizar y definir como:

$$|\gamma_0\rangle = \cos\theta \frac{1}{\parallel \psi_1 \parallel} |\psi_1\rangle + \sin\theta \frac{e^{i\xi}}{\parallel \psi_{0,1} \parallel} |\psi_{0,1}\rangle\,,$$

ó también,

$$|\gamma_0\rangle = \cos\theta\,|\alpha\rangle + \sin\theta e^{i\xi}\,|\beta\rangle\,.$$

Pero más adelante se mostrará que con este estado inicial $|\gamma_0\rangle$, no es posible alcanzar la solución del sistema de ecuaciones $P\,|X\rangle = |b\rangle$, como se muestra en el siguiente diagrama de circuito:

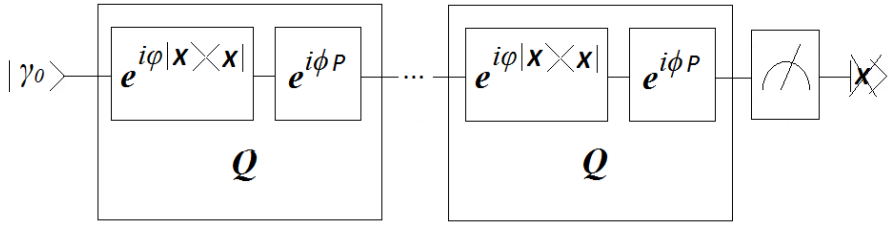

FIGURA 5.4: Modelo de circuito del algoritmo de amplificación de amplitud cuántica modificado, que parte del estado inicial $|\gamma_0\rangle$ y a través de cuál no se encuentra la solución del sistema de ecuaciones.

Definición 12. El $P-$*espacio* cíclico generado por $|X\rangle$ es:

$$\begin{aligned} W &= span(|X\rangle\,, P\,|X\rangle) \\ &= \{x\,|X\rangle + yP\,|X\rangle\,|x, y \in \mathbb{C}\}. \end{aligned}$$

Se quiere demostrar que: $Q(x\,|X\rangle + yP\,|X\rangle) = x'\,|X\rangle + y'P\,|X\rangle$ para cualesquiera x, y que sean complejos, y algunos x', y' que sean complejos también, es decir, que el $P - espacio$ cíclico generado por $|X\rangle$ es $Q - invariante$.

Teorema 11. Sea P una matriz idempotente, $|X\rangle$ un vector unitario y $Q = e^{i\phi P}e^{i\varphi|X\rangle\langle X|}$.

Entonces el $P - espacio$ cíclico generado por $|X\rangle$ es $Q - invariante$.

Demostración. Como $Q(x\,|X\rangle + yP\,|X\rangle) = xQ\,|X\rangle + yQP\,|X\rangle$, basta con checar que:

$Q\,|X\rangle \in W = span(|X\rangle, P\,|X\rangle)$ y también que $QP\,|X\rangle \in W = span(|X\rangle, P\,|X\rangle)$.

En efecto:

$$\begin{aligned} Q\,|X\rangle &= e^{i\phi P}e^{i\varphi|X\rangle\langle X|}\,|X\rangle \\ &= [Id + (e^{i\phi} - 1)P][Id + (e^{i\varphi} - 1)\,|X\rangle\,\langle X|]\,|X\rangle \\ &= [Id + (e^{i\phi} - 1)P][|X\rangle + (e^{i\varphi} - 1)\,|X\rangle\,\langle X|X\rangle] \\ &= e^{i\varphi}\,|X\rangle + e^{i\varphi}(e^{i\phi} - 1)P\,|X\rangle\,. \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 44.

donde se puede ver que: $e^{i\varphi}\,|X\rangle + e^{i\varphi}(e^{i\phi} - 1)P\,|X\rangle \in W = span(|X\rangle, P\,|X\rangle)$.

Ahora también considerando $\langle X|\,P\,|X\rangle = \alpha$, y P idempotente; es decir, $P^2 = P$ para:

$$\begin{aligned} QP\,|X\rangle &= e^{i\phi P}e^{i\varphi|X\rangle\langle X|}P\,|X\rangle \\ &= [Id + (e^{i\phi} - 1)P][Id + (e^{i\varphi} - 1)\,|X\rangle\,\langle X|]P\,|X\rangle \\ &= [Id + (e^{i\phi} - 1)P][P\,|X\rangle + (e^{i\varphi} - 1)\,|X\rangle\,\langle X|\,P\,|X\rangle] \\ &= \alpha(e^{i\varphi} - 1)\,|X\rangle + [e^{i\phi} + \alpha(e^{i\phi} - 1)(e^{i\varphi} - 1)]P\,|X\rangle \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 45.

donde se puede ver que:

$$\alpha(e^{i\varphi} - 1)\,|X\rangle + [e^{i\phi} + \alpha(e^{i\phi} - 1)(e^{i\varphi} - 1)]P\,|X\rangle \in W = span(|X\rangle, P\,|X\rangle).$$

□

Corolario 1. En el algoritmo cuántico de la figura 5.4 donde $Q = e^{i\phi P}e^{i\varphi|X\rangle\langle X|}$, $P^2 = P$, $P^* = P$ y $\langle X|X\rangle = 1$. Si $|\gamma_0\rangle$ no está en el $P - espacio$ cíclico generado por $|X\rangle$ entonces, $Q^j\,|\gamma_0\rangle \neq |X\rangle$, $\forall j$ entero no negativo.

Demostración. Por contradicción suponemos que $Q^j |\gamma_0\rangle = |X\rangle$, $\forall j$ entero no negativo.

Entonces $|\gamma_0\rangle = Q^{-j} |X\rangle$, pero $|X\rangle$ esta en el $P - espacio$ cíclico generado por $|X\rangle$, pero este espacio es también $Q^{-1} - invariante$; es decir,

$$Q(x |X\rangle + yP |X\rangle) = x' |X\rangle + y'P |X\rangle$$

$$x |X\rangle + yP |X\rangle = Q^{-1}(x' |X\rangle + y'P |X\rangle).$$

Entonces, $|\gamma_0\rangle$ está en el $P - espacio$ cíclico generado por $|X\rangle$, pero esto es una contradicción.

En conclusión $|\gamma_0\rangle$ no está en el $P - espacio$ cíclico generado por $|X\rangle$, por lo que a través del estado inicial $|\gamma_0\rangle$, no es posible con el algoritmo de amplificación de amplitud cuántica alcanzar la solución $|X\rangle$, como se muestra en el diagrama de circuito de la figura 5.4. □

Observación 11. Tratamos ahora de escribir este resultado en términos del algoritmo de amplificación de amplitud cuántica. Recordemos que en el algoritmo de amplificación de amplitud cuántica, tenemos un algoritmo A, con un estado inicial $|s\rangle$ y una probabilidad de éxito mayor que 0 y menor que 1, dicha probabilidad de éxito del algoritmo A se busca mejorar a través de multiplicaciones iteradas de las matrices que forman el operador generalizado de Grover Q.

$$Q = AU_0(\phi)A^{-1}U(\varphi).$$

Donde: $A |s\rangle = |\psi_1\rangle + |\psi_0\rangle$, y también:

$$\begin{aligned} U_0(\phi) &= Id + (e^{i\phi} - 1) |s\rangle \langle s| \\ &= e^{i\phi |s\rangle\langle s|} \end{aligned}$$

$$\begin{aligned} U(\varphi) &= Id + (e^{i\varphi} - 1)\frac{1}{a} |\psi_1\rangle \langle \psi_1| \\ &= \frac{1}{a} e^{i\varphi |\psi_1\rangle\langle\psi_1|}. \end{aligned}$$

La probabilidad de éxito del algoritmo A es igual a a, donde: $a = \langle\psi_1|\psi_1\rangle$, y $A |s\rangle = |\psi_1\rangle + |\psi_0\rangle$.

Definición 13.

$$\begin{aligned} P &= \frac{1}{1 - e^{i\varphi}}(AA^{-1} - AU_0(\phi)A^{-1}) \\ &= \frac{1}{1 - e^{i\varphi}} A(Id - U_0(\phi))A^{-1} \\ &= \frac{1}{1 - e^{i\varphi}} A(-(e^{i\varphi} - 1) |s\rangle \langle s|)A^{-1} \\ &= A |s\rangle \langle s| A^{-1}. \end{aligned}$$

Podemos comprobar que P es idempoptente:

$$\begin{aligned} P^2 &= PP \\ &= (A\left|s\right\rangle \left\langle s\right| A^{-1})(A\left|s\right\rangle \left\langle s\right| A^{-1}) \\ &= A\left|s\right\rangle \left\langle s\right| A^{-1} \\ &= P. \end{aligned}$$

También podemos comprobar que P es hermitiana:

$$\begin{aligned} P^* &= (A\left|s\right\rangle \left\langle s\right| A^{-1})^* \\ &= (A^{-1})^*(\left\langle s\right|)^*(\left|s\right\rangle)^* A* \\ &= (A*)^* \left|s\right\rangle \left\langle s\right| A^{-1} \\ &= A\left|s\right\rangle \left\langle s\right| A^{-1} \\ &= P. \end{aligned}$$

Ahora se escribe el algoritmo de amplificación de amplitud cuántica en términos de un sistema de ecuaciones.

Definición 14. Se define al vector solución del sistema de ecuaciones $P\left|X\right\rangle = \left|b\right\rangle$, como:

$$\begin{aligned} \left|X\right\rangle &= \frac{1}{\parallel \psi_1 \parallel} \left|\psi_1\right\rangle \\ &= \frac{1}{\sqrt{\left\langle \psi_1 | \psi_1 \right\rangle}} \left|\psi_1\right\rangle \\ &= \frac{1}{\sqrt{a}} \left|\psi_1\right\rangle . \end{aligned}$$

Se define el vector conocido $\left|b\right\rangle$ como:

$$\begin{aligned} \left|b\right\rangle = P\left|X\right\rangle &= A\left|s\right\rangle \left\langle s\right| A^{-1} \frac{1}{\sqrt{a}} \left|\psi_1\right\rangle \\ &= \frac{1}{\sqrt{a}} A\left|s\right\rangle \left\langle s\right| A^{-1} \left|\psi_1\right\rangle = \frac{1}{\sqrt{a}} A\left|s\right\rangle \left\langle s\right| A^* \left|\psi_1\right\rangle \\ &= \frac{1}{\sqrt{a}} (\left|\psi_1\right\rangle + \left|\psi_0\right\rangle) a = \frac{a}{\sqrt{a}} (\left|\psi_1\right\rangle + \left|\psi_0\right\rangle) \\ &= \sqrt{a}(\left|\psi_1\right\rangle + \left|\psi_0\right\rangle) = \sqrt{a}\left|\psi_1\right\rangle + \sqrt{a}\left|\psi_0\right\rangle . \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 46.

Finalmente, $\left|b\right\rangle = \sqrt{a}\left|\psi_1\right\rangle + \sqrt{a}\left|\psi_0\right\rangle$ y cumple la condición $P\left|X\right\rangle = \left|b\right\rangle$.

Lo anterior muestra como se pasa el algoritmo de amplificación de amplitud cuántica a un algoritmo en términos de un sistema de ecuaciones, donde: $P = A\left|s\right\rangle \left\langle s\right| A^{-1}$, $\left|b\right\rangle = \sqrt{a}\left|\psi_1\right\rangle + \sqrt{a}\left|\psi_0\right\rangle$ y $a = \left\langle \psi_1 | \psi_1 \right\rangle$.

También: $A\left|s\right\rangle = \left|\psi_1\right\rangle + \left|\psi_0\right\rangle$ y $\left|X\right\rangle = \frac{1}{\sqrt{a}}\left|\psi_1\right\rangle$.

Corolario 2. Sea A un algoritmo cuántico sin medición, con un estado inicial $\left|s\right\rangle$ y $\left|\gamma_0\right\rangle = \cos\theta\frac{1}{\|\psi_1\|}\left|\psi_1\right\rangle + \sin\theta\frac{e^{i\xi}}{\|\psi_{0,1}\|}\left|\psi_{0,1}\right\rangle$, tal que $A\left|s\right\rangle$ no esta en el subespacio generado por $\left|\psi_1\right\rangle$ y $\left|\psi_{0,1}\right\rangle$; entonces, $\langle\gamma_0|\gamma_0\rangle = 1$ y $Q^j\left|\gamma_0\right\rangle \neq \left|X\right\rangle$, $\forall j$ entero no negativo.

Demostración. Se sabe que: $Q = AU_0(\phi)A^{-1}U(\varphi)$, donde:

$$\begin{aligned} U_0(\phi) &= Id + (e^{i\phi} - 1)\left|s\right\rangle\langle s| \\ &= e^{i\phi|s\rangle\langle s|} \end{aligned}$$

$$\begin{aligned} U(\varphi) &= Id + (e^{i\varphi} - 1)\frac{1}{a}\left|\psi_1\right\rangle\langle\psi_1| \\ &= \frac{1}{a}e^{i\varphi|\psi_1\rangle\langle\psi_1|} \end{aligned}$$

Luego, la norma al cuadrado de $\left|\gamma_0\right\rangle$ es:

$$\begin{aligned} \langle\gamma_0|\gamma_0\rangle =& |\cos\theta|^2 + |\sin\theta e^{i\xi}|^2 \\ =& |\cos\theta|^2 + |\sin\theta|^2|e^{i\xi}|^2 \\ =& |\cos^2\theta| + |\sin^2\theta| \\ =& 1. \end{aligned}$$

El estado: $A\left|0\right\rangle = \left|\psi_1\right\rangle + \left|\psi_{0,1}\right\rangle + \left|\psi_{0,2}\right\rangle$, en donde se pueden distinguir dos ejes de un plano: los estados buenos $\left|\psi_1\right\rangle$, y las dos partes que forman los estados malos $\left|\psi_{0,1}\right\rangle + \left|\psi_{0,2}\right\rangle$, mientras que el estado $\left|\gamma_0\right\rangle = \left|\psi_1\right\rangle + \left|\psi_{0,1}\right\rangle$; es decir, el vector $\left|\gamma_0\right\rangle$ es una combinación lineal de los estados buenos $\left|\psi_1\right\rangle$, y sólo una parte de los estados malos $\left|\psi_{0,1}\right\rangle$, formándose un vector se sale del plano generado por los estados buenos y las dos partes que forman los estados malos.

Por lo tanto el estado $A\left|0\right\rangle$ no esta en el subespacio generado por $\left|\psi_1\right\rangle$ y $\left|\psi_{0,1}\right\rangle$. □

Corolario 3. $\left|\gamma_0\right\rangle$ no esta en el $P - espacio$ cíclico generado por $\left|X\right\rangle$.

Demostración. Por contradicción, supongamos que $\left|\gamma_0\right\rangle$ si esta en el $P - espacio$ cíclico generado por $\left|X\right\rangle$.

Esto significa que existen x, y números complejos, tales que:

$$\begin{aligned} \left|\gamma_0\right\rangle &= x\left|X\right\rangle + yP\left|X\right\rangle = x\left|X\right\rangle + yA\left|s\right\rangle\langle s|A^{-1}\left|X\right\rangle \\ &= x\left|X\right\rangle + yA\left|s\right\rangle(\langle\psi_1| + \langle\psi_0|)\left|X\right\rangle \\ &= x\frac{1}{\|\psi_1\|}\left|\psi_1\right\rangle + yA\left|s\right\rangle\langle\psi_1|\frac{1}{\|\psi_1\|}\left|\psi_1\right\rangle \\ &= \frac{x}{\sqrt{a}}\left|\psi_1\right\rangle + yA\left|s\right\rangle\sqrt{a}. \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 47.

Con $y \neq 0$, pues si hay malos y también:

$$A\left|s\right\rangle = \frac{1}{y\sqrt{a}}\left|\gamma_0\right\rangle - \frac{x}{ya}\left|\psi_1\right\rangle,$$

entonces $A\left|s\right\rangle$ es generado por $\left|\psi_1\right\rangle$ y $\left|\psi_0\right\rangle$, lo cuál contradice la hipótesis.

Por lo tanto $\left|\gamma_0\right\rangle$ no esta en el $P-espacio$ cíclico generado por $\left|X\right\rangle$ y entonces $Q^j\left|\gamma_0\right\rangle \neq \left|X\right\rangle$, $\forall j$ entero no negativo. □

Para Jin, W. L. y Chen, X. D. que afirman que un estado deseado no puede encontrarse con *certeza* dentro de un subespacio posible de tres dimensiones siguiendo el algoritmo de amplificación de amplitud cuántica, M es el número de estados (vectores de norma uno) deseados dentro de una base de datos desordenada y N es el número de estados totales (registros en general) [9].

Sea $T = \{C_0, \ldots, C_{N-1}\}$ un conjunto de números complejos tales que:

$$\mid C_0 \mid^2 + \cdots + \mid C_{N-1} \mid^2 = 1.$$

Sea también $\left|\gamma_0\right\rangle = \sum_{x=0}^{N-1} C_x\left|X\right\rangle$ donde $\left|0\right\rangle, \left|1\right\rangle, \ldots, \left|N-1\right\rangle$ es una base ortonormal, y Y el conjunto de estados deseados, con $\mid Y \mid = M$.

$\left|\gamma_0\right\rangle = \sum_{x\in Y} C_x\left|X\right\rangle + \sum_{x\in\tilde{Y}} C_x\left|X\right\rangle$, donde $\tilde{Y}$ es el complemento de Y. Es decir, que el estado inicial $\left|\gamma_0\right\rangle$ contiene a los estados que son deseados y una parte de los estados que no son deseados.

Definición 15. Sea $\left|\beta\right\rangle = \frac{1}{\sqrt{\sum_{x\in Y}|C_x|^2}} \sum_{x\in Y} C_x\left|X\right\rangle$ y $\left|\alpha\right\rangle = \frac{1}{\sqrt{\sum_{x\in\tilde{Y}}|C_x|^2}} \sum_{x\in\tilde{Y}} C_x\left|X\right\rangle$.

$\left|\gamma_0\right\rangle = \parallel \beta \parallel \left|\beta\right\rangle + \parallel \alpha \parallel \left|\alpha\right\rangle$, de forma más general es:

$\left|\gamma_0\right\rangle = b\left|\beta\right\rangle + a\left|\alpha\right\rangle$, con $\mid a \mid^2 + \mid b \mid^2 = 1$, donde a y b son números complejos.

$$\begin{aligned}
\left|\gamma_0\right\rangle &= \parallel \beta \parallel \left|\beta\right\rangle + \parallel \alpha \parallel \left|\alpha\right\rangle \\
&= \mid b \mid e^{i\xi_1}\left|\beta\right\rangle + \mid a \mid e^{i\xi_2}\left|\alpha\right\rangle \\
&= e^{i\xi_2}(\mid a \mid \left|\alpha\right\rangle + \mid b \mid e^{i(\xi_1-\xi_2)}\left|\beta\right\rangle) \\
&\equiv \mid a \mid \left|\alpha\right\rangle + \mid b \mid e^{i\xi}\left|\beta\right\rangle \\
&= \cos(\beta_0)\left|\alpha\right\rangle + \sin(\beta_0)e^{i\xi}\left|\beta\right\rangle.
\end{aligned}$$

Esta forma de considerar a $\left|\gamma_0\right\rangle$ como el estado inicial del algoritmo es más general que el estado inicial del que partía el algoritmo de amplificación de amplitud cuántica, ya que a y b pueden tomar cualquier valor de las coordenadas que forman la esfera de Bloch.

Hipótesis: supóngase que $A|0\rangle$ no esta en el espacio generado por $|\alpha\rangle$ y $|\beta\rangle$ donde $|\alpha\rangle$ son los archivos malos o que no se buscan y $|\beta\rangle$ son los archivos buenos o buscados.

De la hipótesis anterior se sigue que $|\alpha\rangle$, $|\beta\rangle$ y $A|0\rangle$ son linealmente independientes.

Luego se aplica el procedimiento de Gram Schmidt para ortogonalizar los vectores $|\alpha\rangle$, $|\beta\rangle$ y $A|0\rangle$, de esta forma se pueden distinguir estos estados:

$$\begin{aligned} |u_0\rangle &= |\beta\rangle \\ |u_1\rangle &= |\alpha\rangle \\ |u_2\rangle &= A|0\rangle - Y_1|\beta\rangle + Y_2|\alpha\rangle . \end{aligned}$$

Esto para ciertos Y_1 y Y_2 que son complejos.

Después se normaliza y de esta manera se tiene:

$$\frac{1}{\| u_2 \|}|u_2\rangle = \frac{1}{\| u_2 \|}A|0\rangle - \frac{Y_1}{\| u_2 \|}|\beta\rangle - \frac{Y_2}{\| u_2 \|}|\alpha\rangle .$$

Ahora se renombra:

$$\frac{1}{\| u_2 \|}|u_2\rangle = |\sigma\rangle .$$

Por lo tanto:

$$|\sigma\rangle = \frac{1}{\| u_2 \|}A|0\rangle - \frac{Y_1}{\| u_2 \|}|\beta\rangle - \frac{Y_2}{\| u_2 \|}|\alpha\rangle$$

$$\frac{1}{\| u_2 \|}A|0\rangle = \frac{Y_1}{\| u_2 \|}|\beta\rangle + \frac{Y_2}{\| u_2 \|}|\alpha\rangle - |\sigma\rangle .$$

Se puede escribir que:

$$A|0\rangle = Y_1|\beta\rangle + Y_2|\alpha\rangle + Y_3|\sigma\rangle ,$$

donde $Y_1|\beta\rangle$ son los archivos buenos o buscados y $Y_2|\alpha\rangle + Y_3|\sigma\rangle$ son los archivos malos o no buscados.

Ahora se desea relacionar esta información con la información que se tiene en términos de sistemas de ecuaciones, donde:

$$P_0|X\rangle = |b\rangle .$$

El algoritmo que resuelve este sistema de ecuaciones es:

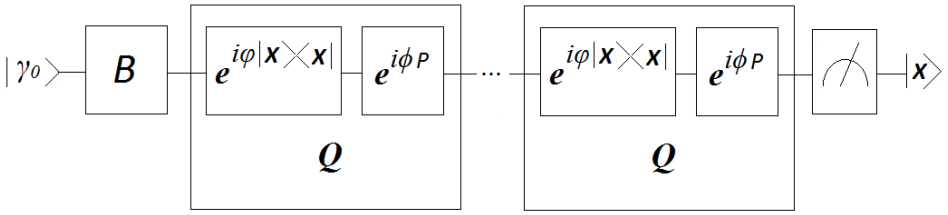

FIGURA 5.5: Modelo de circuito del algoritmo de amplificación de amplitud cuántica modificado, a través de cuál si se encuentra la solución del sistema de ecuaciones.

donde $B|s\rangle = \frac{1}{\|b\|}|b\rangle$.

Definición 16. Al pasar el algoritmo de amplificación de amplitud cuántica a un algoritmo que resuelva un sistema de ecuaciones, se define:

$$P_0 = A|0\rangle\langle 0|A^{-1}$$

$$|X\rangle = |\beta\rangle$$

$$|b\rangle = \sqrt{a}|\psi_1\rangle + \sqrt{a}|\psi_0\rangle$$

donde $|\psi_1\rangle = Y_1|\beta\rangle$, $|\psi_0\rangle = Y_2|\alpha\rangle + Y_3|\sigma\rangle$ y

$$\begin{aligned} a &= \langle\psi_1|\psi_1\rangle \\ &= Y_1^*\langle\beta|Y_1|\beta\rangle \\ &= Y_1^*Y_1\langle\beta|\beta\rangle \\ &= \| Y_1 \|^2 . \end{aligned}$$

Se recuerda también que:

$$|\gamma_0\rangle = \cos\theta\frac{1}{\| \psi_1 \|}|\psi_1\rangle + \sin\theta\frac{e^{i\xi}}{\| \psi_{0,1} \|}|\psi_{0,1}\rangle .$$

De una forma más general se tiene:

$$|\gamma_0\rangle = z_1|\beta\rangle + z_2|\alpha\rangle , con \ | z_1 |^2 + | z_2 |^2 = 1,$$

donde z_1 y z_2 son números complejos, y además $z_1 \neq 0$, también $z_2 \neq 0$ y despejando $|\beta\rangle$ se tiene:

$$|\beta\rangle = \frac{1}{z_1}|\gamma_0\rangle - \frac{z_2}{z_1}|\alpha\rangle$$

y sustituyendo en:

$$|b\rangle = \sqrt{a}\,|\psi_1\rangle + \sqrt{a}\,|\psi_0\rangle\,,$$

entonces se obtiene:

$$\begin{aligned}
|b\rangle &= \sqrt{a}Y_1|\beta\rangle + \sqrt{a}Y_2|\alpha\rangle + \sqrt{a}Y_3|\sigma\rangle \\
&= \frac{\sqrt{a}Y_1}{z_1}|\gamma_0\rangle - \frac{\sqrt{a}Y_1 z_2}{z_1}|\alpha\rangle + \sqrt{a}Y_2|\alpha\rangle + \sqrt{a}Y_3|\sigma\rangle \\
&= \frac{\sqrt{a}Y_1}{z_1}|\gamma_0\rangle + (\sqrt{a}Y_2 - \frac{\sqrt{a}Y_1 z_2}{z_1})|\alpha\rangle + \sqrt{a}Y_3|\sigma\rangle\,.
\end{aligned}$$

Sea R_0 una matriz idempotente, singular y hermitiana, tal que:

$R_0|X\rangle = (\sqrt{a}Y_2 - \frac{\sqrt{a}Y_1 z_2}{z_1})|\alpha\rangle + \sqrt{a}Y_3|\sigma\rangle$ y $P_0R_0 = 0$, pero también $R_0P_0 = 0$. En tal caso $P_0|X\rangle = |b\rangle = \frac{\sqrt{a}Y_1}{z_1}|\gamma_0\rangle + R_0|X\rangle$, $P_0|X\rangle - R_0|X\rangle = \frac{\sqrt{a}Y_1}{z_1}|\gamma_0\rangle$ y $(P_0 - R_0)|X\rangle = \frac{\sqrt{a}Y_1}{z_1}|\gamma_0\rangle$. Ahora sea $|c\rangle = \frac{\sqrt{a}Y_1}{z_1}|\gamma_0\rangle$, entonces se obtiene:

$$(P_0 - R_0)|X\rangle = |c\rangle$$

con P_0, R_0 matrices idempotentes y $P_0R_0 = 0 = R_0P_0$. También se define la diferencia de matrices idempotentes $P_0 - R_0$ como una matriz tripotente.

Así para resolver el sistema de ecuaciones $(P_0 - R_0)|X\rangle = |c\rangle$, se tienen dos formas:

1. Aplicando la teoría para matrices tripotentes y
2. Aplicando la teoría para matrices idempotentes.

Para la primera consideramos que las matrices P_0 y R_0, son idempotentes, pero la diferencia de dos matrices idempotentes genera una matriz tripotente; es decir, $P_0 - R_0$ es una matriz tripotente.

Se quiere resolver el sistema de ecuaciones $(P_0 - R_0)|X\rangle = |c\rangle$ y tomando $(P_0 - R_0) = P$, también se puede expresar como:

$$P|X\rangle = |c\rangle\,,$$

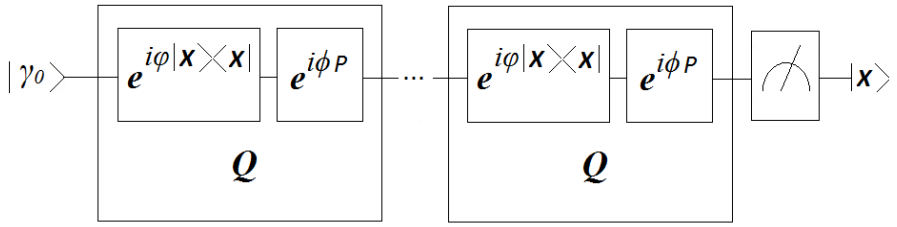

FIGURA 5.6: Modelo de circuito del algoritmo que resuelve el sistema de ecuaciones: $P\,|X\rangle = |c\rangle$.

donde $|c\rangle = |\gamma_0\rangle$ pero normalizado y P es una matriz tripotente.

Para la segunda forma multiplicamos ambos lados del sistema de ecuaciones $(P_0 - R_0)\,|X\rangle = |c\rangle$ por la diferencia $P_0 - R_0$ y se obtiene:

$$\begin{aligned}(P_0 - R_0)(P_0 - R_0)\,|X\rangle &= (P_0 - R_0)\,|c\rangle \\ (P_0 - R_0)^2\,|X\rangle &= (P_0 - R_0)\,|c\rangle \\ (P_0 - R_0)^2\,|X\rangle &= |c'\rangle \\ (P_0^2 + R_0^2)\,|X\rangle &= |c'\rangle \\ (P_0 + R_0)\,|X\rangle &= |c'\rangle \\ P^2\,|X\rangle &= P\,|c\rangle\end{aligned}$$

con $P_0 + R_0 = P^2$ como una matriz idempotente.

Ya que se tiene que:

$$\begin{aligned}(P_0 - R_0)^2 &= P_0^2 - P_0R_0 - R_0P_0 + R_0^2 \\ &= P_0^2 + R_0^2 \\ &= P_0 + R_0\end{aligned}$$

porque $P_0R_0 = 0 = R_0P_0$, también $P_0 + R_0$ es idempoptente; es decir,

$$\begin{aligned}(P_0 + R_0)^2 &= P_0^2 + P_0R_0 + R_0P_0 + R_0^2 \\ &= P_0^2 + R_0^2 \\ &= P_0 + R_0.\end{aligned}$$

Así que:

$$\begin{aligned} e^{i\phi(P_0-R_0)^2} &= e^{i\phi(P_0+R_0)} \\ &= e^{i\phi P_0+i\phi R_0} \\ &= e^{i\phi P_0}e^{i\phi R_0}. \end{aligned}$$

Ya se había definido P_0 como $P_0 = A\left|0\right\rangle\left\langle 0\right|A^{-1}$ y ahora también se define R_0 como $R_0 = A\left|1\right\rangle\left\langle 1\right|A^{-1}$, entonces:

$$\begin{aligned} P_0R_0 &= A\left|0\right\rangle\left\langle 0\right|A^{-1}A\left|1\right\rangle\left\langle 1\right|A^{-1} \\ &= A\left|0\right\rangle(0)\left\langle 1\right|A^{-1} \\ &= 0 \end{aligned}$$

y también:

$$\begin{aligned} R_0P_0 &= A\left|1\right\rangle\left\langle 1\right|A^{-1}A\left|0\right\rangle\left\langle 0\right|A^{-1} \\ &= A\left|1\right\rangle(0)\left\langle 0\right|A^{-1} \\ &= 0. \end{aligned}$$

Ahora tanto P_0 como R_0 son matrices idempotentes, y se demuestra que:

$$\begin{aligned} P_0^2 &= P_0P_0 \\ &= A\left|0\right\rangle\left\langle 0\right|A^{-1}A\left|0\right\rangle\left\langle 0\right|A^{-1} \\ &= A\left|0\right\rangle(1)\left\langle 0\right|A^{-1} \\ &= A\left|0\right\rangle\left\langle 0\right|A^{-1} \\ &= P_0 \end{aligned}$$

y también:

$$\begin{aligned} R_0^2 &= R_0R_0 \\ &= A\left|1\right\rangle\left\langle 1\right|A^{-1}A\left|1\right\rangle\left\langle 1\right|A^{-1} \\ &= A\left|1\right\rangle(1)\left\langle 1\right|A^{-1} \\ &= A\left|1\right\rangle\left\langle 1\right|A^{-1} \\ &= R_0. \end{aligned}$$

También tanto P_0 como R_0 son matrices hermitianas, y se demuestra que:

$$\begin{aligned} P_0^* &= (A\left|0\right\rangle\left\langle 0\right|A^{-1})^* \\ &= (A^{-1})^*\left\langle 0\right|^*\left|0\right\rangle^*A^* \\ &= (A^*)^*\left|0\right\rangle\left\langle 0\right|A^{-1} \\ &= A\left|0\right\rangle\left\langle 0\right|A^{-1} \\ &= P_0 \end{aligned}$$

y también:

$$\begin{aligned} R_0^* &= (A\,|1\rangle\,\langle 1|\,A^{-1})^* \\ &= (A^{-1})^*\,\langle 1|^*\,|1\rangle^*\,A^* \\ &= (A^*)^*\,|1\rangle\,\langle 1|\,A^{-1} \\ &= A\,|1\rangle\,\langle 1|\,A^{-1} \\ &= R_0. \end{aligned}$$

Ahora se define $|c\rangle$ como $(P_0 - R_0)\,|X\rangle = |c\rangle$, con $|X\rangle = |\beta\rangle$, que es el estado bueno o buscado, entonces tenemos el sistema de ecuaciones: $(P_0 - R_0)\,|\beta\rangle = |c\rangle\,.$

Mientras que $|c\rangle$ son todos los estados de la base de datos que se cargan en la computadora cuántica, y se define como:

$$\begin{aligned} |c\rangle &= \xi\,|\gamma_0\rangle \\ &= z_1\,|\beta\rangle + z_2\,|\alpha\rangle\,. \end{aligned}$$

También sabemos que $A\,|0\rangle$ no esta en el espacio generado por $|\alpha\rangle$ y $|\beta\rangle$; es decir, que: $A\,|0\rangle \notin span(|\beta\rangle\,, |\alpha\rangle)$.

$|\alpha\rangle$ y $|\beta\rangle$ son estados distinguibles, es decir, $\langle\beta|\alpha\rangle = 0$ y $\langle\beta|\beta\rangle = 1$. También $|\alpha\rangle$ son los estados malos o no buscados, y se puede definir como $|\alpha\rangle = |c\rangle - \langle\beta|c\rangle\,|\beta\rangle$. El estado $|\alpha\rangle$ normalizado será: $|\alpha\rangle = \frac{1}{\sqrt{\langle\alpha|\alpha\rangle}}\,|\alpha\rangle$.

Considerando el sistema de ecuaciones: $(P_0 - R_0)\,|\beta\rangle = |c\rangle$, donde $P_0 - R_0 = P$; entonces tenemos que: $P\,|\beta\rangle = |c\rangle$, y si multiplicamos ambos miembros de la ecuación por P, nos queda $P^2\,|\beta\rangle = P\,|c\rangle$, con P^2 como matriz idempotente y hermitiana; es decir, $(P^2)^2 = P^2$ y $(P^2)^* = P^2$.

El algoritmo que soluciona este sistema de ecuaciones $P^2\,|\beta\rangle = P\,|c\rangle$ será:

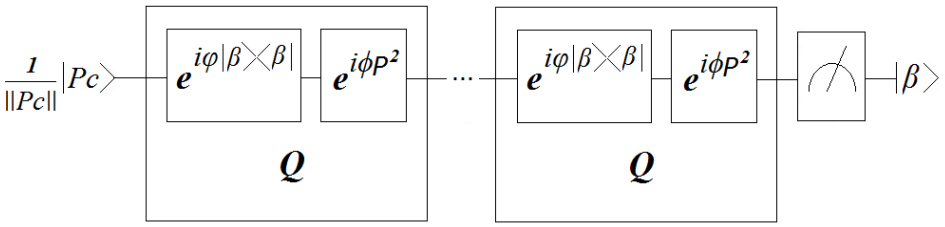

FIGURA 5.7: Algoritmo que resuelve el sistema de ecuaciones: $P^2\,|\beta\rangle = P\,|c\rangle$.

Ahora el diagrama de circuito anterior, nos muestra el algoritmo que deseamos mejorar, donde el estado inicial del algoritmo es el vector: $|\gamma_0\rangle = z_1\,|\beta\rangle + z_2\,|\alpha\rangle$ y $Q = AU_0(\phi)A^{-1}U_f(\varphi)$.

Se sabe que $A\,|s\rangle = |\psi_1\rangle + |\psi_{0,1}\rangle + |\psi_{0,2}\rangle$, pero $A\,|s\rangle$ no esta en el espacio generado por $|\alpha\rangle$ y $|\beta\rangle\,.$

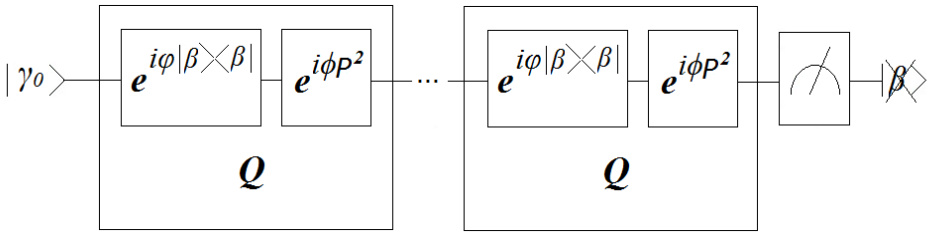

FIGURA 5.8: Modelo de circuito del algoritmo que parte del estado inicial: $|\gamma_0\rangle$, y que se modificará para que resuelva el sistema de ecuaciones: $P^2|\beta\rangle = P|c\rangle$.

Ya que $|\gamma_0\rangle = |\psi_1\rangle + |\psi_{0,1}\rangle$; es decir, que sólo contiene parte de los malos, y con este estado inicial no es posible llegar al vector solución $|\beta\rangle$ a través del algoritmo de amplificación de amplitud cuántica.

En la mejora que se realiza al algoritmo de amplificación de amplitud cuántica, se multiplica este estado inicial $|\gamma_0\rangle$ por una matriz unitaria B, donde:

$$B = e^{i\pi\langle\beta|R_0|\beta\rangle^{-1}R_0|\beta\rangle\langle\beta|R_0} y B|\gamma_0\rangle = \frac{1}{\| P|c\rangle \|} P|c\rangle .$$

Esta matriz unitaria B resulta de comparar $P|c\rangle = (P_0 + R_0)|\beta\rangle$ con $|c\rangle = (P_0 - R_0)|\beta\rangle$, y esto debido a que:

$$\begin{aligned} P|c\rangle &= PP|\beta\rangle \\ &= P^2|\beta\rangle \\ &= (P_0 - R_0)^2|\beta\rangle \\ &= (P_0^2 + R_0^2)|\beta\rangle \\ &= (P_0 + R_0)|\beta\rangle . \end{aligned}$$

Con $P_0R_0 = 0$, $R_0P_0 = 0$, $P_0^2 = P_0$ y $R_0^2 = R_0$ por ser P_0 y R_0 matrices idempotentes.

Ahora nótese que $|c\rangle = (P_0 - R_0)|\beta\rangle$, entonces, $|c\rangle$ y $P|c\rangle$ sólo son diferentes en el signo menos de R_0.

Propiedad 2. $B = \langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0$ es una matriz idempotente, también es una matriz hermitiana.

Demostración. 1. $\langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0$ es una matriz idempotente.

$$\begin{aligned} \langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0 &= \langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0 \langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0 \\ &= \langle\beta| R_0 |\beta\rangle^{-2} R_0 |\beta\rangle \langle\beta| R_0 |\beta\rangle \langle\beta| R_0 \\ &= \langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0. \end{aligned}$$

2. $\langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0$ es una matriz hermitiana.

$$\begin{aligned}(\langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0)^* &= (R_0 |\beta\rangle \langle\beta| R_0)^* (\langle\beta| R_0 |\beta\rangle^{-1})^* \\ &= (\langle\beta| R_0 |\beta\rangle^{-1})^* (R_0 |\beta\rangle \langle\beta| R_0)^* \\ &= (|\beta\rangle^* R_0^* \langle\beta|^*) -1 R_0^* \langle\beta|^* |\beta\rangle^* R_0^* \\ &= (\langle\beta| R_0 |\beta\rangle)^{-1} R_0 |\beta\rangle \langle\beta| R_0.\end{aligned}$$

Entonces B es una matriz unitaria y hermitiana. □

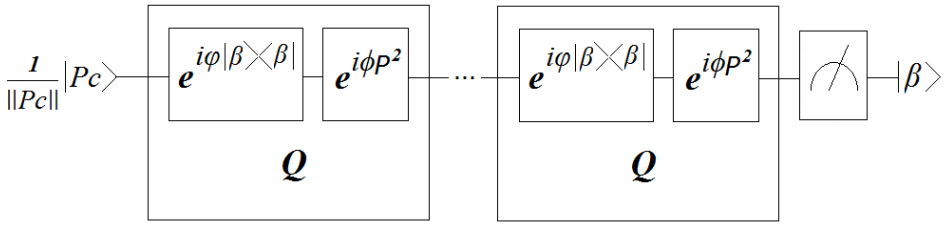

FIGURA 5.9: Modelo de circuito del algoritmo que parte del estado inicial: $P|c\rangle$, y que resuelve el sistema de ecuaciones: $P^2|\beta\rangle = P|c\rangle$.

Propiedad 3. En general, la matriz $U = Id - 2\langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0$ es unitaria.

Demostración. $A = \langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0$ es una matriz hermitiana y $\varphi \in \mathbb{R}$, entonces, $e^{i\varphi A}$ es una matriz unitaria.

$$\begin{aligned}e^{i\varphi A}(e^{i\varphi A})^* &= e^{i\varphi A} e^{(i\varphi A)^*} \\ &= e^{i\varphi A} e^{-i\varphi A^*} \\ &= e^{i\varphi A} e^{-i\varphi A} \\ &= e^0 \\ &= Id.\end{aligned}$$

Además recordemos que si P es una matriz idempotente, entonces, $e^{i\phi P} = Id + (e^{i\varphi} - 1)P$.

Luego:

$$\begin{aligned}e^{i\pi\langle\beta|R_0|\beta\rangle^{-1} R_0|\beta\rangle\langle\beta|R_0} &= Id + (e^{i\pi} - 1)\langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0 \\ &= Id - 2\langle\beta| R_0 |\beta\rangle^{-1} R_0 |\beta\rangle \langle\beta| R_0.\end{aligned}$$

□

Teorema 12. Al multiplicar la matriz unitaria B por el vector $|\gamma_0\rangle$, se carga en la computadora cuántica el vector $P|c\rangle$ pero normalizado; es decir, con esta instrucción se

cargan todos los archivos de la base de datos no estructurada, tanto los que se buscan como los que no, en otras palabras:

$$B\left|\gamma_0\right\rangle = \frac{1}{\parallel P\left|c\right\rangle \parallel} P\left|c\right\rangle .$$

Demostración.

$$\begin{aligned} B\left|\gamma_0\right\rangle &= U\frac{1}{\parallel \left|c\right\rangle \parallel}\left|c\right\rangle = \frac{1}{\parallel \left|c\right\rangle \parallel} B\left|c\right\rangle = \frac{1}{\parallel \left|c\right\rangle \parallel} U(P_0 - R_0)\left|\beta\right\rangle \\ &= \frac{1}{\parallel \left|c\right\rangle \parallel}(Id - 2\left\langle\beta\right| R_0\left|\beta\right\rangle^{-1} R_0\left|\beta\right\rangle \left\langle\beta\right| R_0)(P_0 - R_0)\left|\beta\right\rangle \\ &= \frac{1}{\parallel \left|c\right\rangle \parallel}(P_0 - R_0)\left|\beta\right\rangle + 2\left\langle\beta\right| R_0\left|\beta\right\rangle^{-1} R_0\left|\beta\right\rangle \left\langle\beta\right| R_0^2\left|\beta\right\rangle \\ &= \frac{1}{\parallel \left|c\right\rangle \parallel}(P_0 - R_0)^2\left|\beta\right\rangle = \frac{1}{\parallel \left|c\right\rangle \parallel} P^2\left|\beta\right\rangle = \frac{1}{\parallel \left|c\right\rangle \parallel} P\left|c\right\rangle . \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 48.

Pero también sabemos que:

$$\begin{aligned} \parallel \left|c\right\rangle \parallel &= \sqrt{\left\langle c\right| \left|c\right\rangle} = \sqrt{\left\langle\beta\right| (P_0^* - R_0^*)(P_0 - R_0)\left|\beta\right\rangle} \\ &= \sqrt{\left\langle\beta\right| (P_0 - R_0)(P_0 - R_0)\left|\beta\right\rangle} = \sqrt{\left\langle\beta\right| (P_0 - R_0)^2\left|\beta\right\rangle} \\ &= \sqrt{\left\langle\beta\right| P^2\left|\beta\right\rangle} = \sqrt{\left\langle\beta\right| (P^2)^2\left|\beta\right\rangle} \\ &= \sqrt{\left\langle c\right| P^* P\left|c\right\rangle} = \sqrt{\parallel P\left|c\right\rangle \parallel^2} = \parallel P\left|c\right\rangle \parallel . \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 49.

Entonces: $\parallel \left|c\right\rangle \parallel = \parallel P\left|c\right\rangle \parallel$. Por lo tanto: $B\left|\gamma_0\right\rangle = \frac{1}{\|P\left|c\right\rangle\|} P\left|c\right\rangle$. □

Observación 12. Regresando a la modificación al algoritmo de amplificación de amplitud cuántica. El estado inicial del algoritmo $\left|\gamma_0\right\rangle$ se multiplicará por la matriz unitaria B, así $B\left|\gamma_0\right\rangle$ será el estado de preparación del algoritmo. A su vez el estado $B\left|\gamma_0\right\rangle$ se multiplica por el operador generalizado de Grover Q, el cuál se compone del producto de dos matrices: la de marcado $e^{i\varphi\left|\beta\right\rangle\left\langle\beta\right|}$ y la de difusión $e^{i\phi P^2}$. Dicho operador generalizado de Grover Q se itera hasta encontrar el estado $\left|\beta\right\rangle$ que es la solución del sistema de ecuaciones $(P_0 - R_0)\left|\beta\right\rangle = \left|c\right\rangle$.

Observación 13. En el caso idempotente, el diagrama de circuito expresa como el algoritmo propuesto corrige a amplificación de amplitud cuántica. El algoritmo propuesto resuelve el siguiente sistema de ecuaciones:

$$(P_0 + R_0)\left|\beta\right\rangle = (P_0 - R_0)\left|c\right\rangle$$

$$P^2\left|\beta\right\rangle = P\left|c\right\rangle .$$

Propiedad 4. $e^{i\phi P^2} = AS_0(\phi)A^{-1}e^{i\phi R_0}$.

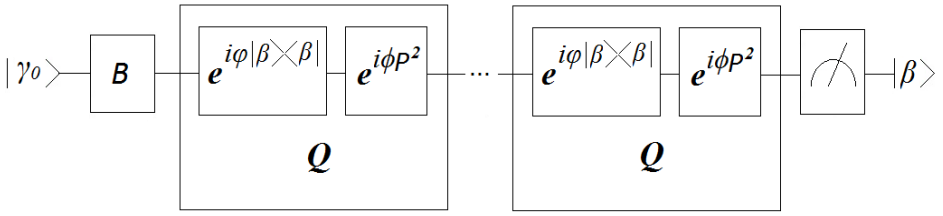

FIGURA 5.10: Modelo de circuito del algoritmo de amplificación de amplitud cuántica modificado, que parte del estado inicial: $|\gamma_0\rangle$.

Demostración.

$$\begin{aligned} e^{i\phi P^2} &= e^{i\phi(P_0+R_0)} = e^{i\phi P_0 + i\phi R_0} = e^{i\phi P_0} e^{i\phi R_0} \\ &= [Id + (e^{i\phi} - 1)P] e^{i\phi R_0} = [Id + (e^{i\phi} - 1)A \left|0\right\rangle \left\langle 0\right| A^{-1}] e^{i\phi R_0} \\ &= A[Id + (e^{i\phi} - 1) \left|0\right\rangle \left\langle 0\right|] A^{-1} e^{i\phi R_0}. \end{aligned}$$

Para ver los cálculos completos remitirse al Apéndice A, Ecuación 50.

Hay que recordar que: $P = P_0 - R_0$, $P^2 = P_0 + R_0$ y $P_0 R_0 = R_0 P_0 = 0$. Por otor lado:

$$\begin{aligned} S_0(\phi) \left|0\right\rangle &= e^{i\phi} \left|0\right\rangle = (Id + (e^{i\phi} - 1) \left|0\right\rangle \left\langle 0\right|) \left|0\right\rangle \\ &= \left|0\right\rangle + (e^{i\phi} - 1) \left|0\right\rangle \left\langle 0|0\right\rangle \\ &= \left|0\right\rangle + (e^{i\phi} - 1) \left|0\right\rangle \\ &= \left|0\right\rangle + e^{i\phi} \left|0\right\rangle - \left|0\right\rangle = e^{i\phi} \left|0\right\rangle \end{aligned}$$

y si $|X\rangle$ es ortogonal a $|0\rangle$; entonces,

$$\begin{aligned} S_0(\phi) \left|X\right\rangle &= \left|X\right\rangle \\ &= (Id + (e^{i\phi} - 1) \left|0\right\rangle \left\langle 0\right|) \left|X\right\rangle \\ &= \left|X\right\rangle + (e^{i\phi} - 1) \left|0\right\rangle \left\langle 0|X\right\rangle = \left|X\right\rangle. \end{aligned}$$

Por lo tanto: $S_0(\phi) = Id + (e^{i\phi} - 1) \left|0\right\rangle \left\langle 0\right|$. □

Observación 14. En el caso tripotente, el siguiente diagrama de circuito expresa como el algoritmo propuesto corrige a amplificación de amplitud cuántica de forma diferente a como se corrige en el caso idempotente.

El algoritmo resuelve el siguiente sistema de ecuaciones:

$$(P_0 - R_0) \left|\beta\right\rangle = \left|c\right\rangle$$

$$P \left|\beta\right\rangle = \left|c\right\rangle.$$

Propiedad 5. $e^{i\phi P} = A S_0(\phi) A^{-1} e^{-i\phi R_0}$.

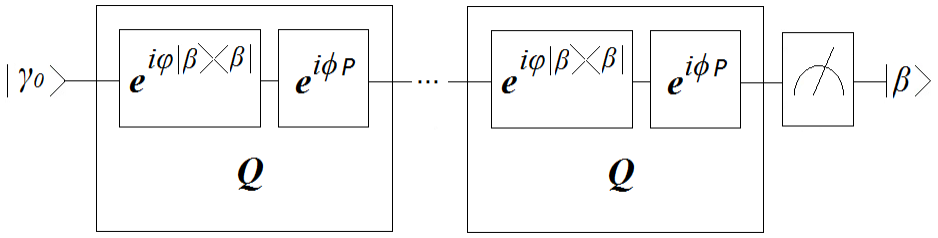

FIGURA 5.11: Modelo de circuito del algoritmo que parte del estado inicial: $|\gamma_0\rangle$, y que resuelve el sistema de ecuaciones: $P|\beta\rangle = |c\rangle$.

Demostración. Nuevamente hay que recordar: $P = P_0 - R_0$ y $P_0R_0 = R_0P_0 = 0$.

$$\begin{aligned} e^{i\phi P} &= e^{i\phi(P_0-R_0)} = e^{i\phi P_0 - i\phi R_0} \\ &= e^{i\phi P_0}e^{-i\phi R_0} = [Id + (e^{i\phi}-1)P]e^{-i\phi R_0} \\ &= [Id + (e^{i\phi}-1)A|0\rangle\langle 0|A^{-1}]e^{-i\phi R_0} \\ &= [AA^{-1} + (e^{i\phi}-1)A|0\rangle\langle 0|A^{-1}]e^{-i\phi R_0} \\ &= A[Id + (e^{i\phi}-1)|0\rangle\langle 0|]A^{-1}e^{-i\phi R_0} \end{aligned}$$

donde nuevamente:

$$\begin{aligned} S_0(\phi)|0\rangle = e^{i\phi}|0\rangle &= (Id + (e^{i\phi}-1)|0\rangle\langle 0|)|0\rangle \\ &= |0\rangle + (e^{i\phi}-1)|0\rangle\langle 0|0\rangle = |0\rangle + (e^{i\phi}-1)|0\rangle \\ &= |0\rangle + e^{i\phi}|0\rangle - |0\rangle = e^{i\phi}|0\rangle. \end{aligned}$$

Y si $|X\rangle$ es ortogonal a $|0\rangle$, entonces:

$$\begin{aligned} S_0(\phi)|X\rangle &= (Id + (e^{i\phi}-1)|0\rangle\langle 0|)|X\rangle \\ &= |X\rangle + (e^{i\phi}-1)|0\rangle\langle 0|X\rangle = |X\rangle. \end{aligned}$$

Por lo tanto: $S_0(\phi) = Id + (e^{i\phi}-1)|0\rangle\langle 0|$. □

5.2. Ejemplos.

La presente sección mostrará la simulación que se realizó de la mejor al algoritmo de amplificación de amplitud cuántica, donde se muestra sí es posible encontrar con certeza un estado deseado en un subespacio invariante de tres dimensiones.

Dicha simulación se dará a conocer a través de un ejemplo concreto, donde se resuelve un sistema de ecuaciones de la forma: $(P_0 - R_0)\,|\beta\rangle = |c\rangle$. Se presentarán las matrices P_0, R_0, su diferencia $P_0 - R_0$; el vector de incógnitas $|\beta\rangle$ y el vector de resultados $|c\rangle$. Finalmente se mostrará la solución al sistema de ecuaciones propuesto y también cada resultado de la simulación hasta llegar a conocer los valores del vector de incógnitas $|\beta\rangle$.

Ejemplo 16. *Problema a resolver:* encontrar el estado $|\beta\rangle$ en el sistema de ecuaciones $(P_0 - R_0)\,|\beta\rangle = |c\rangle$, donde las matrices P_0 y R_0 son idempotentes y estan definidas como: $P_0 = A\,|0\rangle\,\langle 0|\,A^{-1}$ y $R_0 = A\,|1\rangle\,\langle 1|\,A^{-1}$.

Hay que recordar que la diferencia de matrices idempotentes, genera una matriz tripotente, es decir, $P = P_0 - R_0$ es una matriz tripotente. También hay que recordar que si se multiplican ambos lados del sistema de ecuaciones: $(P_0 - R_0)\,|\beta\rangle = |c\rangle$ por la diferencia $P_0 - R_0$, se obtiene:

$$\begin{aligned}(P_0 - R_0)(P_0 - R_0)\,|\beta\rangle &= (P_0 - R_0)\,|c\rangle \\ (P_0 - R_0)^2\,|\beta\rangle &= (P_0 - R_0)\,|c\rangle \\ P^2\,|\beta\rangle &= P\,|c\rangle\,,\end{aligned}$$

ya que se tiene que:

$$\begin{aligned}(P_0 - R_0)^2 &= P_0^2 - P_0R_0 - R_0P_0 + R_0^2 \\ &= P_0^2 + R_0^2 \\ &= P_0 + R_0.\end{aligned}$$

Entonces: $(P_0 + R_0)\,|\beta\rangle = P\,|c\rangle$. Después como $P_0R_0 = 0 = R_0P_0$, también $P_0 + R_0$ es idempoptente, es decir,

$$\begin{aligned}(P_0 + R_0)^2 &= P_0^2 + P_0R_0 + R_0P_0 + R_0^2 \\ &= P_0^2 + R_0^2 \\ &= P_0 + R_0.\end{aligned}$$

En conclusión $P^2 = P_0 + R_0$ es una matriz idempotente.

5.2.1. Solución del sistema de ecuaciones con matrices idempotentes.

Para simular como resolver un sistema de ecuaciones a través de la teoria para matrices idempotentes, se va a considerar el siguiente sistema de ecuaciones:

$$(P_0 - R_0)^2\,|\beta\rangle = (P_0 - R_0)\,|c\rangle\,,$$

Es decir, $P^2\,|\beta\rangle = P\,|c\rangle$, donde P^2 es una matriz idempotente.

Las matrices idempotentes P_0 y R_0, se van a definir de la siguiente manera:

$$P_0 = A\left|0\right\rangle\left\langle 0\right|A^{-1} y R_0 = A\left|1\right\rangle\left\langle 1\right|A^{-1},$$

Para ello se utilizarán las matrices: A y A^{-1}, y los vectores: $|0\rangle$, $\langle 0|$, $|1\rangle$ y $\langle 1|$.

A continuación se enumeran los pasos a realizar para obtener las matrices P_0 y R_0:

1. Se obtiene la matriz A, para este ejemplo, A será el producto tensorial de tres matrices de Walsh-Hadamard.

   $$A = W \otimes W \otimes W.$$

   Por lo tanto:

   $$A = \begin{pmatrix} \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \end{pmatrix}.$$

2. Entonces, A^{-1} será:

   $$A^{-1} = \begin{pmatrix} \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \end{pmatrix}.$$

3. Se utiliza el vector $|0\rangle$ de tamaño adecuado:

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

4. el $\langle 0|$ utilizado será:
$$\langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

5. $|1\rangle$ será:
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

6. y $\langle 1|$ será:
$$\langle 1| = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Así en el ejemplo, $P_0 = A|0\rangle\langle 0|A^{-1}$ será:

$$P_0 = \begin{pmatrix} \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{pmatrix},$$

y $R_0 = A|1\rangle\langle 1|A^{-1}$ será:

$$R_0 = \begin{pmatrix} \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \end{pmatrix}.$$

$P = P_0 - R_0$ será:

$$P = \begin{pmatrix} 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \end{pmatrix}.$$

$P^2 = P_0 + R_0$ será:

$$P^2 = \begin{pmatrix} \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \end{pmatrix}.$$

Se desea encontrar:

$$|\beta\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

Cabe notar que el valor $|\beta\rangle$ no se conoce, pero sí se puede distinguir.

El vector $|c\rangle$ es conocido:

$$|c\rangle = \begin{pmatrix} 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \end{pmatrix}.$$

El primer paso del algoritmo es normalizar el vector $P|c\rangle$ y cargarlo en la computadora cuántica, para ello se parte de un estado inicial $|\gamma_0\rangle$, y se multiplica por la matriz B que es unitaria, de tal forma que el primer paso del algoritmo propuesto es: $B|\gamma_0\rangle$.

El estado $|\gamma_0\rangle$ esta definido como:

$$|\gamma_0\rangle = \begin{pmatrix} 0\frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix}.$$

Al multiplicar $|\gamma_0\rangle$ por B, se realizará en la computadora cuántica, la transición del estado inicial $|\gamma_0\rangle$, al estado de preparación:

$$B\,|\gamma_0\rangle = \frac{1}{\parallel P\,|c\rangle \parallel} P\,|c\rangle\,.$$

B esta definida como: $B = Id - 2\,\langle\beta|\,R_0\,|\beta\rangle^{-1}\,R_0\,|\beta\rangle\,\langle\beta|\,R_0$.

$$B = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} & \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} \end{pmatrix}.$$

El resultado de multiplicar $|\gamma_0\rangle$ por B es:

$$B\,|\gamma_0\rangle = \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}.$$

El segundo paso es multiplicar este vector resultante por el operador generalizado de Grover Q.

El sistema de ecuaciones de este ejemplo se resolvió con sólo una iteracion de operador generalizado de Grover Q, el número de iteraciones de dicho operador, en el caso idempotente es el techo de $n = \left\lceil \frac{\arccos\sqrt{a}}{\arcsin 2\sqrt{a}\sqrt{1-a}} \right\rceil$, donde $a = \langle c|\,P^2\,|c\rangle$ y $|c\rangle = P\,|\beta\rangle$. En el ejemplo:

$$a = \langle c|\,(P_0 + R_0)\,|c\rangle = \frac{1}{3},$$

$$n = \left\lceil \frac{\arccos\sqrt{a}}{\arcsin 2\sqrt{a}\sqrt{1-a}} \right\rceil = \lceil 0.776074828029885 \rceil = 1,$$

donde el techo de n es 1.

Recordar que para formar el operador generalizado de Grover Q se necesita multiplicar dos matrices, una es la compuerta del marcador M y otra es la compuerta del difusor D y el operador Q es el resultado de dicha multiplicación.

La compuerta de marcado esta definida como: $M = e^{i\varphi|\beta\rangle\langle\beta|} = Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta|$.

También se debe considerar que en el caso idempotente el ángulo de marcado se obtiene con la fórmula:

$$\varphi = 2\arcsin\left(\frac{1}{\sqrt{a}}\sin\frac{\pi}{4n+2}\right).$$

$$\varphi = 2\arcsin\left(\frac{1}{\sqrt{a}}\sin\frac{\pi}{6}\right) = \frac{2\pi}{3}.$$

Así el ángulo de marcado para el ejemplo es: $\varphi = \frac{2\pi}{3}$. Entonces la matriz del marcador se simplifica de la siguiente forma:

$$\begin{aligned} M &= e^{i\varphi|\beta\rangle\langle\beta|} \\ &= Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta| \\ &= Id + (e^{i\frac{2\pi}{3}} - 1)|\beta\rangle\langle\beta|. \end{aligned}$$

Por lo tanto:

$$M = Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta| = Id + (e^{i\frac{2\pi}{3}} - 1)|\beta\rangle\langle\beta| =$$

$$\begin{pmatrix} \frac{(2^{\frac{3}{2}}+3)\sqrt{3}i-3\,2^{\frac{3}{2}}+15}{24} & 0 & -\frac{\sqrt{3}\,i-3}{24} & 0 & \frac{(2^{\frac{3}{2}}+3)\sqrt{3}i-3\,2^{\frac{3}{2}}-9}{24} & 0 & -\frac{\sqrt{3}\,i-3}{24} & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{\sqrt{3}\,i-3}{24} & 0 & \frac{(3-2^{\frac{3}{2}})\sqrt{3}i+3\,2^{\frac{3}{2}}+15}{24} & 0 & -\frac{\sqrt{3}\,i-3}{24} & 0 & \frac{(3-2^{\frac{3}{2}})\sqrt{3}i+3\,2^{\frac{3}{2}}-9}{24} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{(2^{\frac{3}{2}}+3)\sqrt{3}i-3\,2^{\frac{3}{2}}-9}{24} & 0 & -\frac{\sqrt{3}\,i-3}{24} & 0 & \frac{(2^{\frac{3}{2}}+3)\sqrt{3}i-3\,2^{\frac{3}{2}}+15}{24} & 0 & -\frac{\sqrt{3}\,i-3}{24} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -\frac{\sqrt{3}\,i-3}{24} & 0 & \frac{(3-2^{\frac{3}{2}})\sqrt{3}i+3\,2^{\frac{3}{2}}-9}{24} & 0 & -\frac{\sqrt{3}\,i-3}{24} & 0 & \frac{(3-2^{\frac{3}{2}})\sqrt{3}i+3\,2^{\frac{3}{2}}+15}{24} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

La compuerta de difusión esta definida como: $D = e^{i\phi P^2} = Id + (e^{i\phi} - 1)P^2$.

El ángulo de difusión en la teoría de matrices idempotentes se obtiene con la misma fórmula que se obtuvo el ángulo de marcado; es decir:

$$\phi = 2\arcsin\left(\frac{1}{\sqrt{a}}\sin\frac{\pi}{4n+2}\right).$$

$$\phi = 2\arcsin\left(\frac{1}{\sqrt{a}}\sin\frac{\pi}{6}\right) = \frac{2\pi}{3}.$$

Así la compuerta del difusor se simplifica de la siguiente forma:

$$
\begin{aligned}
D &= e^{i\phi P^2} \\
&= Id + (e^{i\phi} - 1)P^2 \\
&= Id + (e^{i(\frac{2\pi}{3})} - 1)P^2 \\
&= \begin{pmatrix}
\frac{\sqrt{3}i+5}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 \\
0 & \frac{\sqrt{3}i+5}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} \\
\frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i+5}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 \\
0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i+5}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} \\
\frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i+5}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 \\
0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i+5}{8} & 0 & \frac{\sqrt{3}i-3}{8} \\
\frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i+5}{8} & 0 \\
0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i-3}{8} & 0 & \frac{\sqrt{3}i+5}{8}
\end{pmatrix}.
\end{aligned}
$$

Con la matriz del marcador y el difusor simplificadas, y adecuadas al ejemplo que se esta simulando, se obtiene el operador extendido de Grover Q.

$$
\begin{aligned}
Q &= DM \\
&= e^{i\phi P^2} e^{i\varphi|\beta\rangle\langle\beta|} \\
&= (Id + (e^{i\phi} - 1)P^2)(Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta|) \\
&= (Id + (e^{i(\frac{2\pi}{3})} - 1)P^2)(Id + (e^{i\frac{2\pi}{3}} - 1)|\beta\rangle\langle\beta|).
\end{aligned}
$$

Por lo tanto:

$$
Q = (Id+(e^{i\phi}-1)P^2)(Id+(e^{i\varphi}-1)|\beta\rangle\langle\beta|) = (Id+(e^{i(\frac{2\pi}{3})}-1)P^2)(Id+(e^{i\frac{2\pi}{3}}-1)|\beta\rangle\langle\beta|) =
$$

$$
\begin{pmatrix}
\frac{9-\sqrt{18}-\sqrt{6}\,i+\sqrt{27}\,i}{24} & 0 & \frac{\sqrt{54}\,i-\sqrt{3}\,i-\sqrt{18}-3}{24} & 0 & \frac{\sqrt{27}\,i-\sqrt{6}\,i-\sqrt{18}-15}{24} & 0 & \frac{\sqrt{54}\,i-\sqrt{3}\,i-\sqrt{18}-3}{24} & 0 \\
0 & \frac{\sqrt{3}\,i+5}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} \\
\frac{\sqrt{18}-3-\sqrt{54}\,i-\sqrt{3}\,i}{24} & 0 & \frac{\sqrt{6}\,i+\sqrt{27}\,i+\sqrt{18}+9}{24} & 0 & \frac{\sqrt{18}-3-\sqrt{54}\,i-\sqrt{3}\,i}{24} & 0 & \frac{\sqrt{6}\,i+\sqrt{27}\,i+\sqrt{18}-15}{24} & 0 \\
0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i+5}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} \\
\frac{\sqrt{27}\,i-\sqrt{6}\,i-\sqrt{18}-15}{24} & 0 & \frac{\sqrt{54}\,i-\sqrt{3}\,i-\sqrt{18}-3}{24} & 0 & \frac{9-\sqrt{18}-\sqrt{6}\,i+\sqrt{27}\,i}{24} & 0 & \frac{\sqrt{54}\,i-\sqrt{3}\,i-\sqrt{18}-3}{24} & 0 \\
0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i+5}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} \\
\frac{\sqrt{18}-3-\sqrt{54}\,i-\sqrt{3}\,i}{24} & 0 & \frac{\sqrt{6}\,i+\sqrt{27}\,i+\sqrt{18}-15}{24} & 0 & \frac{\sqrt{18}-3-\sqrt{54}\,i-\sqrt{3}\,i}{24} & 0 & \frac{\sqrt{6}\,i+\sqrt{27}\,i+\sqrt{18}+9}{24} & 0 \\
0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i-3}{8} & 0 & \frac{\sqrt{3}\,i+5}{8}
\end{pmatrix}
$$

y después se multiplica el operador Q por el vector $B\,|\gamma_0\rangle$, para obtener:

$$
QB\,|\gamma_0\rangle = \begin{pmatrix}
\frac{\left(\sqrt{2}+1\right)\sqrt{3}\,i-3\,\sqrt{2}-3}{12} \\
0 \\
-\frac{\left(\sqrt{2}-1\right)\sqrt{3}\,i-3\,\sqrt{2}+3}{12} \\
0 \\
\frac{\left(\sqrt{2}+1\right)\sqrt{3}\,i-3\,\sqrt{2}-3}{12} \\
0 \\
-\frac{\left(\sqrt{2}-1\right)\sqrt{3}\,i-3\,\sqrt{2}+3}{12} \\
0
\end{pmatrix}.
$$

Dicho vector $QB\left|\gamma_\phi 0\right\rangle$ es la solución del sistema de ecuaciones $\left(P_0 - R_0\right)\left|\beta\right\rangle = \left|c\right\rangle$, es decir, $QB\left|\gamma_0\right\rangle$ es igual a $\left|\beta\right\rangle$ salvo la fase global $\frac{2\sqrt{3}}{\sqrt{3}i-3}$.

$$QB\left|\gamma_0\right\rangle = \begin{pmatrix} \frac{\left(\sqrt{2}+1\right)\sqrt{3}\,i-3\,\sqrt{2}-3}{12} \\ 0 \\ -\frac{\left(\sqrt{2}-1\right)\sqrt{3}\,i-3\,\sqrt{2}+3}{12} \\ 0 \\ \frac{\left(\sqrt{2}+1\right)\sqrt{3}\,i-3\,\sqrt{2}-3}{12} \\ 0 \\ -\frac{\left(\sqrt{2}-1\right)\sqrt{3}\,i-3\,\sqrt{2}+3}{12} \\ 0 \end{pmatrix} = \frac{2\sqrt{3}}{\sqrt{3}i-3} \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

Así se comprueba que la solución es:

$$\left|\beta\right\rangle = \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

5.2.2. Solución del sistema de ecuaciones con matrices tripotentes.

Para simular esta segunda forma de como resolver un sistema de ecuaciones a través de la teoria para matrices tripotentes, se va a considerar el siguiente sistema de ecuaciones $\left(P_0 - R_0\right)\left|\beta\right\rangle = \left|c\right\rangle$, es decir, $P\left|\beta\right\rangle = \left|c\right\rangle$, donde $P = P_0 - R_0$ es una matriz tripotente.

Las matrices idempotentes P_0 y R_0 para este ejemplo, se van a definir de la siguiente manera:

$$P_0 = F\left|0\right\rangle\left\langle 0\right|F^{-1} y R_0 = F\left|4\right\rangle\left\langle 4\right|F^{-1},$$

para ello se utilizarán las matrices: F y F^{-1}, y los vectores: $\left|0\right\rangle$, $\left\langle 0\right|$, $\left|4\right\rangle$ y $\left\langle 4\right|$.

La matriz $F = f\left|k\right\rangle$ es la transformada cuántica de Fourier, donde $\left|k\right\rangle$ es un vector en la base del cálculo, cuyas entradas son números complejos c^{2^n}. La Transformada cuántica de Fourier F esta definida de la siguiente manera:

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

es decir,

$$F = \begin{pmatrix} \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{i+1}{4} & \frac{i}{2^{\frac{3}{2}}} & \frac{i-1}{4} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i+1}{4} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{i-1}{4} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{i-1}{4} & -\frac{i}{2^{\frac{3}{2}}} & \frac{i+1}{4} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i-1}{4} & \frac{i}{2^{\frac{3}{2}}} & -\frac{i+1}{4} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{i+1}{4} & \frac{i}{2^{\frac{3}{2}}} & -\frac{i-1}{4} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i+1}{4} & -\frac{i}{2^{\frac{3}{2}}} & \frac{i-1}{4} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{i-1}{4} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{i+1}{4} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i-1}{4} & \frac{i}{2^{\frac{3}{2}}} & \frac{i+1}{4} \end{pmatrix} .$$

Entonces, F^{-1} será:

$$F^{-1} = \begin{pmatrix} \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{i-1}{4} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{i+1}{4} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i-1}{4} & \frac{i}{2^{\frac{3}{2}}} & \frac{i+1}{4} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{i+1}{4} & \frac{i}{2^{\frac{3}{2}}} & -\frac{i-1}{4} & -\frac{1}{2^{\frac{3}{2}}} & \frac{i+1}{4} & -\frac{i}{2^{\frac{3}{2}}} & \frac{i-1}{4} \\ \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{i-1}{4} & -\frac{i}{2^{\frac{3}{2}}} & \frac{i+1}{4} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i-1}{4} & \frac{i}{2^{\frac{3}{2}}} & -\frac{i+1}{4} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} & \frac{1}{2^{\frac{3}{2}}} & \frac{i}{2^{\frac{3}{2}}} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i}{2^{\frac{3}{2}}} \\ \frac{1}{2^{\frac{3}{2}}} & \frac{i+1}{4} & \frac{i}{2^{\frac{3}{2}}} & \frac{i-1}{4} & -\frac{1}{2^{\frac{3}{2}}} & -\frac{i+1}{4} & -\frac{i}{2^{\frac{3}{2}}} & -\frac{i-1}{4} \end{pmatrix} .$$

El $|0\rangle$ adecuado será:

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

$\langle 0|$ será:

$$\langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} ,$$

$|4\rangle$ será:

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

y $\langle 4|$ será:

$$\langle 4| = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Así en el ejemplo, $P_0 = F\,|0\rangle\,\langle 0|\,F^{-1}$ es:

$$P_0 = \begin{pmatrix} \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{pmatrix}$$

y $R_0 = F\,|4\rangle\,\langle 4|\,F^{-1}$ es:

$$R_0 = \begin{pmatrix} \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \end{pmatrix}.$$

$P = P_0 - R_0$ es:

$$P = \begin{pmatrix} 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \end{pmatrix}.$$

Se desea encontrar:

$$|\beta\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

Cabe notar que el valor $|\beta\rangle$ no se conoce, pero sí se puede distinguir.

$|c\rangle$ es conocido:

$$|c\rangle = \begin{pmatrix} 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \\ 0 \\ \frac{1}{2\sqrt{3}} \end{pmatrix}.$$

El primer paso del algoritmo propuesto es cargar el vector $|c\rangle$ en la computadora cuántica; entonces, el estado inicial del cual se parte es $|\gamma_0\rangle = |c\rangle$, el cual debe ser de norma uno y en el ejemplo es:

$$|\gamma_0\rangle = \begin{pmatrix} 0\frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix}.$$

El segundo paso es multiplicar este vector resultante por el operador generalizado de Grover Q.

El sistema de ecuaciones de este ejemplo se resolvió con sólo dos iteraciones de operador generalizado de Grover Q, hay que recordar que para formar el operador Q, se necesita de la multiplicación dos matrices, una es la compuerta del marcador M y otra es la compuerta del difusor D, el operador Q es el resultado de dicho producto.

La compuerta de marcado esta definida como: $M = e^{i\varphi|\beta\rangle\langle\beta|} = Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta|$.

El ángulo de marcado para este ejemplo es: $\varphi = \frac{2\pi}{3}$. Entonces la matriz del marcador se simplifica de la siguiente forma:

$$
\begin{aligned}
M &= e^{i\varphi|\beta\rangle\langle\beta|} \\
&= Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta| \\
&= Id + (e^{i\frac{2\pi}{3}} - 1)|\beta\rangle\langle\beta| \\
&= \begin{pmatrix}
-\frac{2^{\frac{3}{2}}-3}{6} & 0 & \frac{1}{6} & 0 & -\frac{2^{\frac{3}{2}}+3}{6} & 0 & \frac{1}{6} & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}+3}{6} & 0 & \frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}-3}{6} & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-\frac{2^{\frac{3}{2}}+3}{6} & 0 & \frac{1}{6} & 0 & -\frac{2^{\frac{3}{2}}-3}{6} & 0 & \frac{1}{6} & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}-3}{6} & 0 & \frac{1}{6} & 0 & \frac{2^{\frac{3}{2}}+3}{6} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\end{aligned}
$$

La compuerta de difusión esta definida como: $D = e^{i\phi P}$.

El ángulo de difusión para este ejemplo es: $\phi = \pi$. Así la matriz del difusor se simplifica de la siguiente forma:

$$
\begin{aligned}
D &= e^{i\phi P} \\
&= Id + i\sin\phi P + (\cos\phi - 1)P^2 \\
&= Id + i\sin\pi P + (\cos\pi - 1)P^2 \\
&= \begin{pmatrix}
\frac{5}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} \\
\frac{\sqrt{3}i}{8} & \frac{5}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} \\
-\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{5}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} \\
\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{5}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} \\
-\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{5}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} \\
\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{5}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} \\
-\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{5}{8} & \frac{\sqrt{3}i}{8} \\
\frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & -\frac{3}{8} & \frac{\sqrt{3}i}{8} & \frac{5}{8}
\end{pmatrix}.
\end{aligned}
$$

Con la matriz del marcador y el difusor simplificadas, y adecuadas al ejemplo que se esta simulando, se obtiene el operador extendido de Grover Q.

$$
\begin{aligned}
Q &= DM \\
&= e^{i\phi P} e^{i\varphi|\beta\rangle\langle\beta|} \\
&= (Id + i(\sin\phi)P + (\cos\phi - 1)P^2)(Id + (e^{i\varphi} - 1)|\beta\rangle\langle\beta|) \\
&= (Id + i(\sin\pi)P + (\cos\pi - 1)P^2)(Id + (e^{i\frac{2\pi}{3}} - 1)|\beta\rangle\langle\beta|) \\
&= \begin{pmatrix}
-\frac{2^{\frac{3}{2}}-9}{24} & \frac{\sqrt{3}\,i}{8} & -\frac{3\,2^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}\,i}{8} & -\frac{2^{\frac{3}{2}}+15}{24} & \frac{\sqrt{3}\,i}{8} & -\frac{3\,2^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}\,i}{8} \\
-\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & \frac{5}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & -\frac{3}{8} & -\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & -\frac{3}{8} \\
\frac{3\,2^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}\,i}{8} & \frac{2^{\frac{3}{2}}+9}{24} & \frac{\sqrt{3}\,i}{8} & \frac{3\,2^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}\,i}{8} & \frac{2^{\frac{3}{2}}-15}{24} & \frac{\sqrt{3}\,i}{8} \\
-\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & \frac{5}{8} & -\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & -\frac{3}{8} \\
-\frac{2^{\frac{3}{2}}+15}{24} & \frac{\sqrt{3}\,i}{8} & -\frac{3\,2^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}\,i}{8} & -\frac{2^{\frac{3}{2}}-9}{24} & \frac{\sqrt{3}\,i}{8} & -\frac{3\,2^{\frac{3}{2}}-1}{24} & \frac{\sqrt{3}\,i}{8} \\
-\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & -\frac{3}{8} & -\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & \frac{5}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & -\frac{3}{8} \\
\frac{3\,2^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}\,i}{8} & \frac{2^{\frac{3}{2}}-15}{24} & \frac{\sqrt{3}\,i}{8} & \frac{3\,2^{\frac{3}{2}}+1}{24} & \frac{\sqrt{3}\,i}{8} & \frac{2^{\frac{3}{2}}+9}{24} & \frac{\sqrt{3}\,i}{8} \\
-\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & -\frac{3}{8} & -\frac{\left(2^{\frac{3}{2}}-1\right)i}{8\sqrt{3}} & -\frac{3}{8} & \frac{\left(2^{\frac{3}{2}}+1\right)i}{8\sqrt{3}} & \frac{5}{8}
\end{pmatrix}.
\end{aligned}
$$

Después se multiplica el operador Q por el vector $|\gamma_0\rangle$, y se obtiene:

$$
Q\,|\gamma_0\rangle = \begin{pmatrix}
\frac{\sqrt{3}\,i}{4} \\ -\frac{1}{4} \\ \frac{\sqrt{3}\,i}{4} \\ -\frac{1}{4} \\ \frac{\sqrt{3}\,i}{4} \\ -\frac{1}{4} \\ \frac{\sqrt{3}\,i}{4} \\ -\frac{1}{4}
\end{pmatrix}.
$$

El tercer paso es realizar una segunda iteración del operador Q, para obtener:

$$
Q^2\,|\gamma_0\rangle = \begin{pmatrix}
-\frac{\left(\sqrt{2}+1\right)i}{2\sqrt{3}} \\ 0 \\ \frac{\left(\sqrt{2}-1\right)i}{2\sqrt{3}} \\ 0 \\ -\frac{\left(\sqrt{2}+1\right)i}{2\sqrt{3}} \\ 0 \\ \frac{\left(\sqrt{2}-1\right)i}{2\sqrt{3}} \\ 0
\end{pmatrix}.
$$

Dicho vector $Q^2 |\gamma_0\rangle$ es la solución del sistema de ecuaciones $(P_0 - R_0) |\beta\rangle = |c\rangle$, es decir, $Q^2 |\gamma_0\rangle$ es igual al vector $|\beta\rangle$ salvo la fase global: i.

$$Q^2 |\gamma_0\rangle = \begin{pmatrix} -\frac{\left(\sqrt{2}+1\right) i}{2\sqrt{3}} \\ 0 \\ \frac{\left(\sqrt{2}-1\right) i}{2\sqrt{3}} \\ 0 \\ -\frac{\left(\sqrt{2}+1\right) i}{2\sqrt{3}} \\ 0 \\ \frac{\left(\sqrt{2}-1\right) i}{2\sqrt{3}} \\ 0 \end{pmatrix} = i \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

Así se comprueba que la solución es:

$$|\beta\rangle = \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \\ \frac{\sqrt{2}+1}{2\sqrt{3}} \\ 0 \\ -\frac{\sqrt{2}-1}{2\sqrt{3}} \\ 0 \end{pmatrix}.$$

Capítulo 6

Conclusiones y trabajo futuro

En este último capítulo se darán a conocer las conclusiones a las que se llegaron después de simular y analizar el algoritmo cuántico propuesto para el caso tripotente.

También se darán a conocer las aportaciónes que se hicieron al algoritmo de amplificación de amplitud cuántica.

6.1. Conclusiones.

1. La simulación de capítulo anterior prueba que a través del algoritmo propuesto para el caso tripotente, que sí es posible obtener la solución de un sistema de ecuaciones donde la matriz de coeficientes es singular, hermitiana y tripotente.

2. El presente trabajo de investigación presenta el algoritmo propuesto para el caso tripotente como una opción más para obtener la solución de un sistema de ecuaciones como se describió anteriormente.

3. El algoritmo propuesto para el caso tripotente es diferente al del caso idempotente, debido a que en el caso idempotente el ángulo de marcado y el ángulo de difusión son necesariamente iguales, mientras que en el caso tripotente el ángulo de marcado y el ángulo de difusión no necesariamente son iguales.

4. Se encontró que hay una infinidad de ángulos de marcado y difusión, con los cuales es posible encontrar la solución de un sistema de ecuaciones. Esto se debe a que el vector de marcado es análogo a un vector de rotación, el cual vuelve a encontrar la solución al rotar.

5. Los ángulos de marcado y difusión, con los cuales es posible alcanzar la solución del sistema de ecuaciones, se pueden colocar en una serie formal, y esta a su vez, se puede expresar como una sumatoria infinita.

6. Se encontró un algoritmo, que es una generalización del algoritmo de amplificación de amplitud cuántica, tal que le es posible encontrar con certeza un estado deseado

dentro de un subespacio invariante de tres dimensiones. Dicho estado contiene los archivos que son buscados dentro de la base de datos no estructurada.

7. También se encontró que existe una matriz B que modifica el algoritmo de amplificación de amplitud cuántica, de tal forma, que puede encontrarse con *certeza* a través del algoritmo generalizado de Grover en un subespacio invariante de tres dimensiones, un estado deseado que contiene los archivos que son buscados dentro de una base de datos no estructurada.

8. El encontrar con certeza un estado deseado dentro de una base de datos no estructurada, en un subespacio invariante de tres dimensiones, es equivalente a resolver un sistema de ecuaciones donde la matriz de coeficientes es singular, hermitiana, tripotente y el cuál se puede resolver usando la teoría para matrices idempotentes o la teoría para matrices tripotentes.

6.2. Limitaciones

1. El algoritmo tiene la limitación de que sólo resuelve sistemas de ecuaciones lineales que tienen matrices de coeficientes singulares, hermitianas y tripotentes.

2. El rango de los problemas que se pueden resolver con el algoritmo diseñado, esta limitado a matrices de coeficientes tripotantes y sólo para la búsqueda de archivos en bases de datos no estructuradas.

3. No se ha estudiado la complejidad del algoritmo, en cuanto que este resuelve sistemas de ecuaciones lineales.

6.3. Trabajo futuro.

1. Generalizar los teoremas encontrados en la teoría del caso idempotente y tripotente, para luego plantear el caso $n - potente$.

2. Encontrar nuevas generalizaciones al algoritmo de Grover o la técnica de amplificación de amplitud cuántica, para incrementar el rango de problemas que se pueden resolver en la búsqueda de archivos deseados en una base de datos no estructurada.

3. Hacer un análisis de las modificaciones que se le hicieron al algoritmo de amplificación de amplitud cuántica y seguir trabajando con las mismas, de tal manera que se logre reducir la complejidad del algoritmo diseñado exponencialmente, en cuanto que este resuelve sistemas de ecuaciones lineales, en comparación con algunos algoritmos clásicos que también resuelven sistemas de ecuaciones donde la matriz de coeficientes es singular, por ejemplo el algoritmo de Gauss-Jordan.

Apéndice A

Apéndice de ecuaciones

Ecuación 1.

$$\begin{aligned} P(m_1) + P(m_2) + \cdots + P(m_k) &= \langle\psi| M_{m_1} M_{m_1}^* + M_{m_2} M_{m_2}^* + \cdots + M_{m_k} M_{m_k}^* |\psi\rangle \\ &= \langle\psi| Id |\psi\rangle \\ &= \langle\psi|\psi\rangle \\ &= || \psi ||^2 \end{aligned}$$

Ecuación 2.

$$\begin{aligned} M_1^* M_1 + M_2^* M_2 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Ecuación 3.

$$\begin{aligned} P_1 &= \langle\psi_1| M_1^* M_1 |\psi_1\rangle \\ &= \left(\tfrac{1}{\sqrt{2}}, \ \tfrac{1}{\sqrt{2}}\right) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \left(\tfrac{1}{\sqrt{2}}, \ \tfrac{1}{\sqrt{2}}\right) \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\ &= \frac{1}{2} + 0 \\ &= \frac{1}{2} \end{aligned}$$

Ecuación 4.

$$\begin{aligned}
|\alpha_1\rangle &= \frac{1}{\sqrt{P_1}} M_1 |\psi_1\rangle \\
&= \frac{1}{\sqrt{P_1}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \frac{1}{\sqrt{P_1}} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\
&= \frac{1}{\sqrt{\frac{1}{2}}} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\
&= \sqrt{2} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= |0\rangle
\end{aligned}$$

Ecuación 5.

$$\begin{aligned}
P_2 &= \langle \psi_1 | M_2^* M_2 |\psi_1\rangle \\
&= \begin{pmatrix} \frac{1}{\sqrt{2}}, & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} \frac{1}{\sqrt{2}}, & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= 0 + \frac{1}{2} \\
&= \frac{1}{2}
\end{aligned}$$

Ecuación 6.

$$\begin{aligned}
|\alpha_2\rangle &= \frac{1}{\sqrt{P_2}} M_2 |\psi_1\rangle \\
&= \frac{1}{\sqrt{P_2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \frac{1}{\sqrt{P_2}} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \frac{1}{\sqrt{\frac{1}{2}}} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \sqrt{2} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
&= |1\rangle
\end{aligned}$$

Ecuación 7.

$$\begin{aligned}
M_1 W |0\rangle &= M_1 (\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle) \\
&= |0\rangle \langle 0| (\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle) \\
&= \frac{1}{\sqrt{2}} |0\rangle \langle 0|0\rangle + \frac{1}{\sqrt{2}} |1\rangle \langle 0|1\rangle \\
&= \frac{1}{\sqrt{2}} |0\rangle
\end{aligned}$$

Ecuación 8.

$$\begin{aligned}
|\psi_1\rangle &= (W \otimes W) |\psi_0\rangle \\
&= (W \otimes W)(|0\rangle |1\rangle) \\
&= W |0\rangle \otimes W |1\rangle \\
&= \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) \\
&= \frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle
\end{aligned}$$

Ecuación 9.

$$\begin{aligned}
|\psi_2\rangle &= U_f\,|\psi_1\rangle \\
&= U_f\left(\frac{1}{2}\,|00\rangle - \frac{1}{2}\,|01\rangle + \frac{1}{2}\,|10\rangle - \frac{1}{2}\,|11\rangle\right) \\
&= \frac{1}{2}U_f\,|00\rangle - \frac{1}{2}U_f\,|01\rangle + \frac{1}{2}U_f\,|10\rangle - \frac{1}{2}U_f\,|11\rangle \\
&= \frac{1}{2}\,|0\rangle\,|f(0)\oplus 0\rangle - \frac{1}{2}\,|0\rangle\,|f(0)\oplus 1\rangle + \frac{1}{2}\,|1\rangle\,|f(1)\oplus 0\rangle \\
&- \frac{1}{2}\,|1\rangle\,|f(1)\oplus 1\rangle \\
&= |0\rangle\otimes(-1)^{f(0)}\left(\frac{|0\rangle-|1\rangle}{2}\right) + |1\rangle\otimes(-1)^{f(1)}\left(\frac{|0\rangle-|1\rangle}{2}\right) \\
&= \left(\frac{|0\rangle-|1\rangle}{2}\right)\left(|0\rangle\otimes(-1)^{f(0)} + |1\rangle\otimes(-1)^{f(1)}\right) \\
&= \frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}
\end{aligned}$$

Ecuación 10.

$$\begin{aligned}
W^{\otimes 2}\,|10\rangle &= (W\otimes W)(|1\rangle\otimes|0\rangle \\
&= \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\right) \\
&= \frac{1}{2}\,|00\rangle + \frac{1}{2}\,|01\rangle - \frac{1}{2}\,|10\rangle - \frac{1}{2}\,|11\rangle \\
&= \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right) \\
&= \frac{1}{2}\left((-1)^{1000}\,|00\rangle + (-1)^{1001}\,|01\rangle - (-1)^{1010}\,|10\rangle - (-1)^{1011}\,|11\rangle\right)
\end{aligned}$$

Ecuación 11.

$$\begin{aligned}
|\psi_1\rangle &= (W^{\otimes n}\otimes Id)(|00\ldots0\rangle\otimes|0\rangle) \\
&= W^{\otimes n}\,|00\ldots0\rangle\otimes Id\,|0\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{00\ldots0}(|u\rangle\otimes|0\rangle) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(|u\rangle\otimes|0\rangle)
\end{aligned}$$

Por superposición homogenea.

Ecuación 12.

$$\begin{aligned}
|\psi_2\rangle &= U_f\,|\psi_1\rangle \\
&= U_f\left(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle\otimes|0\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}U_f(|u\rangle\otimes|0\rangle)
\end{aligned}$$

Propiedad distributiba del producto de matrices ó paralelismo.

$$= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(|u\rangle\otimes|f(u)\oplus 0\rangle)$$

Por definición de U_f.

Ecuación 13.

$$\begin{aligned}
|\psi_3\rangle &= (Id^{\otimes n}\otimes z)\,|\psi_2\rangle \\
&= (Id^{\otimes n}\otimes z)\left(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle\otimes|f(u)\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(Id^{\otimes n}\otimes z)(|u\rangle\otimes|f(u)\rangle) \\
z\,|0\rangle &= |0\rangle,\ z\,|1\rangle = -\,|1\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle\otimes z\,|f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle\otimes(-1)^{f(u)}\,|f(u)\rangle
\end{aligned}$$

Ecuación 14.

$$\begin{aligned}
|\psi_4\rangle &= U_f\,|\psi_3\rangle \\
&= U_f\left(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle\otimes(-1)^{f(u)}\,|f(u)\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}U_f(|u\rangle\otimes|f(u)\rangle) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\,|u\rangle\otimes|f(u)\oplus f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\,|u\rangle\otimes|0\rangle
\end{aligned}$$

Ecuación 15.

$$
\begin{aligned}
|\psi_5\rangle &= (W^{\otimes n} \otimes Id)\,|\psi_4\rangle \\
&= (W^{\otimes n} \otimes Id)\left(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\,|u\rangle \otimes |0\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}W^{\otimes n}\,|u\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{uw}\,|w\rangle\,|0\rangle \\
&= \frac{1}{2^n}\sum_{u=0}^{2^n-1}\left(\sum_{u=0}^{2^n-1}(-1)^{f(u)+uw}\,|w\rangle\,|0\rangle\right) \\
&= \frac{1}{2^n}\sum_{u=0}^{2^n-1}(-1)^{f(u)}\,|0\ldots0\rangle\,|0\rangle + \frac{1}{2^n}\sum_{u=0}^{2^n-1}(-1)^{f(u)+uw}\,|w\rangle\,|0\rangle \\
&= \frac{1}{\sqrt{2^n}}\frac{1}{\sqrt{2^n}}\left(\sum_{u=0}^{2^n-1}(-1)^{f(u)}\right)|00\ldots0\rangle\,|0\rangle + \cdots \\
&= \frac{1}{2^n}\left(\sum_{u=0}^{2^n-1}(-1)^{f(u)}\right)|00\ldots0\rangle\,|0\rangle + \cdots
\end{aligned}
$$

En esta etapa podemos ver la Interferencia $\sum_{u=0}^{2^n-1}(-1)^{f(u)}$.

Ecuación 16.

$$
\begin{aligned}
|\psi_1\rangle &= (W \otimes Id)(|0\rangle \otimes |0\rangle) \\
&= (W \otimes Id)\,|00\rangle \\
&= \left(\frac{1}{\sqrt{2}}\,|1\rangle + \frac{1}{\sqrt{2}}\,|0\rangle\right)|0\rangle \\
&= \frac{1}{\sqrt{2}}\,|10\rangle + \frac{1}{\sqrt{2}}\,|00\rangle
\end{aligned}
$$

Ecuación 17.

$$\begin{aligned}
|\psi_2\rangle &= C(X)(\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|00\rangle) \\
&= \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|00\rangle \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} \\
&= \begin{pmatrix}0\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix} + \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{pmatrix} \\
&= \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix} \\
&= |\beta_{00}\rangle
\end{aligned}$$

Ecuación 18.

$$\begin{aligned}
|\psi_1\rangle &= C(X)^{\otimes Id}(|\psi\rangle \otimes |\beta_{00}\rangle) \\
&= C(X)^{\otimes Id}((a|0\rangle + b|1\rangle) \otimes |\beta_{00}\rangle) \\
&= C(X)^{\otimes Id}\left((a|0\rangle + b|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle\right)\right) \\
&= C(X)^{\otimes Id}\left(\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle\right) \\
&= \frac{a}{\sqrt{2}}C(X)^{\otimes Id}|000\rangle + \frac{a}{\sqrt{2}}C(X)^{\otimes Id}|011\rangle \\
&+ \frac{b}{\sqrt{2}}C(X)^{\otimes Id}|100\rangle + \frac{b}{\sqrt{2}}C(X)^{\otimes Id}|111\rangle \\
&= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle .
\end{aligned}$$

Ecuación 19.

$$
\begin{aligned}
|\psi_2\rangle &= (W \otimes Id \otimes Id)\,|\psi_1\rangle \\
&= (W \otimes Id \otimes Id)(\frac{a}{\sqrt{2}}\,|000\rangle + \frac{a}{\sqrt{2}}\,|011\rangle \\
&+ \frac{b}{\sqrt{2}} W\,|0\rangle\,|110\rangle + \frac{b}{\sqrt{2}}\,|101\rangle) \\
&= \frac{a}{\sqrt{2}} W\,|0\rangle\,|00\rangle + \frac{a}{\sqrt{2}} W\,|0\rangle\,|11\rangle \\
&+ \frac{b}{\sqrt{2}} W\,|1\rangle\,|10\rangle + \frac{b}{\sqrt{2}} W\,|1\rangle\,|01\rangle \\
&= \frac{a}{\sqrt{2}}(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle)\,|00\rangle \\
&+ \frac{a}{\sqrt{2}}(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle)\,|11\rangle \\
&+ \frac{b}{\sqrt{2}}(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle)\,|10\rangle \\
&+ \frac{b}{\sqrt{2}}(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle)\,|01\rangle \\
&= \frac{a}{2}\,|000\rangle + \frac{a}{2}\,|100\rangle + \frac{a}{2}\,|011\rangle + \frac{a}{2}\,|111\rangle \\
&+ \frac{b}{2}\,|010\rangle - \frac{b}{2}\,|110\rangle + \frac{b}{2}\,|001\rangle - \frac{b}{2}\,|101\rangle \\
&= \frac{1}{2}\,|00\rangle\,(a\,|0\rangle + b\,|1\rangle) + \frac{1}{2}\,|01\rangle\,(a\,|1\rangle + b\,|0\rangle) \\
&+ \frac{1}{2}\,|10\rangle\,(a\,|0\rangle - b\,|1\rangle) + \frac{1}{2}\,|11\rangle\,(a\,|1\rangle - b\,|0\rangle) \\
&= \frac{1}{\sqrt{2}}\,|0\rangle\,\frac{|0\rangle\,(a\,|0\rangle + b\,|1\rangle) + |1\rangle\,(a\,|1\rangle + b\,|0\rangle)}{\sqrt{2}} \\
&+ \frac{1}{\sqrt{2}}\,|1\rangle\,\frac{|0\rangle\,(a\,|0\rangle - b\,|1\rangle) + |1\rangle\,(a\,|1\rangle - b\,|0\rangle)}{\sqrt{2}}
\end{aligned}
$$

Ecuación 20. $|\psi_4\rangle = W^{\otimes 2}\,|\psi_3\rangle = (W \otimes W)U_0(W \otimes W)U_f\,|00\rangle$
$= (W \otimes W)(Id_4 - 2\,|00\rangle\,\langle 00|)(W \otimes W)U_f\,|00\rangle$
$= (W \otimes W)(Id_4 - 2\,|00\rangle\,\langle 00|)(W \otimes W)(Id_4 + (e^{i\pi} - 1)\,|10\rangle\,\langle 10|)\,|00\rangle$
$= (W \otimes W)(Id_4 - 2\,|00\rangle\,\langle 00|)(W \otimes W)(Id_4 - 2\,|10\rangle\,\langle 10|)\,|00\rangle$
$= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} (Id_4 - 2\,|00\rangle\,\langle 00|)$
$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} (Id_4 - 2\,|10\rangle\,\langle 10|)(|00\rangle)$
$= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - 2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1, & 0, & 0, & 0 \end{pmatrix}$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - 2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0, & 0, & 1, & 0 \end{pmatrix} =$$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

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

$$= -\left|10\right\rangle$$

Ecuación 21.

$$\begin{aligned} P &= A\left|00\right\rangle\left\langle 00\right|A^{-1} = W^{\otimes 2}\left|00\right\rangle\left\langle 00\right|W^{\otimes 2} \\ &= (W \otimes W)\left|00\right\rangle\left\langle 00\right|(W \otimes W) \\ &= \left(\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\right)\left|00\right\rangle\left\langle 00\right|\left(\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\right) \\ &= \left(\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\right) \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1, & 0, & 0, & 0 \end{pmatrix} \\ &\quad \left(\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\right) \\ &= \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1, & 0, & 0, & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \end{pmatrix} \end{aligned}$$

Ecuación 22.

$$\begin{aligned}
|\psi_{k+1}\rangle &= Q^k A\,|0\ldots0\rangle \\
&= Q^k\left(\cos\frac{\theta}{2}\,|\psi_0\rangle + \sin\frac{\theta}{2}\,|\psi_1\rangle\right) \\
&= \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}^k \begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix} \\
&= \begin{pmatrix}\cos(k\theta) & -\sin(k\theta)\\ \sin(k\theta) & \cos(k\theta)\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}\end{pmatrix} \\
&= \begin{pmatrix}\cos(k\theta+\frac{\theta}{2})\\ \sin(k\theta+\frac{\theta}{2})\end{pmatrix}
\end{aligned}$$

Ecuación 23.

$$\begin{aligned}
|W_2\rangle &= P\,|X\rangle - \frac{\langle X|\,P\,|X\rangle}{\langle X|X\rangle}\,|X\rangle \\
&= P\,|X\rangle - \langle X|\,P\,|X\rangle\,|X\rangle \\
&= P\,|X\rangle - \langle X|\,PP\,|X\rangle\,|X\rangle \\
&= P\,|X\rangle - \langle X|\,P^*P\,|X\rangle\,|X\rangle \\
&= P\,|X\rangle - \langle X|\,P^*\,|b\rangle\,|X\rangle \\
&= P\,|X\rangle - (P\,|X\rangle)^*\,|b\rangle\,|X\rangle \\
&= P\,|X\rangle - |b\rangle^*\,|b\rangle\,|X\rangle \\
&= P\,|X\rangle - \langle b|\,|b\rangle\,|X\rangle \\
&= P\,|X\rangle - a\,|X\rangle \\
&= (P - aId)\,|X\rangle
\end{aligned}$$

Ecuación 24.

$$\begin{aligned}
|\psi_2\rangle &= e^{i\varphi|X\rangle\langle X|}\,|\psi_1\rangle \\
&= e^{i\varphi|X\rangle\langle X|}(\frac{1}{\sqrt{a}}P\,|X\rangle) \\
&= (Id + (e^{i\varphi}-1)\,|X\rangle\,\langle X|)(\frac{1}{\sqrt{a}}P\,|X\rangle) \\
&= \frac{1}{\sqrt{a}}P\,|X\rangle + \frac{(e^{i\varphi}-1)}{\sqrt{a}}\,|X\rangle\,\langle X|\,P\,|X\rangle \\
&= \frac{1}{\sqrt{a}}P\,|X\rangle + \frac{(e^{i\varphi}-1)}{\sqrt{a}}\,|X\rangle\,a \\
&= \frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle
\end{aligned}$$

Ecuación 25.

$$\begin{aligned}
|\psi_3\rangle &= e^{i\phi P}\,|\psi_2\rangle \\
&= e^{i\phi P}(\frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle) \\
&= (Id + (e^{i\phi}-1)P)(\frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle) \\
&= \frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle + (e^{i\phi}-1)P)(\frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle) \\
&= \frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle + (e^{i\phi}-1)\frac{1}{\sqrt{a}}P^2\,|X\rangle + \sqrt{a}(e^{i\varphi})^2P^2\,|X\rangle \\
&= \frac{1}{\sqrt{a}}P\,|X\rangle + (e^{i\varphi}-1)\sqrt{a}\,|X\rangle + (e^{i\phi}-1)\frac{1}{\sqrt{a}}P\,|X\rangle + \sqrt{a}(e^{i\varphi})^2P\,|X\rangle \\
&= (e^{i\varphi}-1)\sqrt{a}\,|X\rangle + (\frac{1}{\sqrt{a}} + (e^{i\phi}-1)\frac{1}{\sqrt{a}} + \sqrt{a}(e^{i\varphi})^2P\,|X\rangle
\end{aligned}$$

Ecuación 26.

$$\begin{aligned}
(e^{i\phi P})(e^{i\phi P})^* &= (e^{i\phi P})(e^{(i\phi P)^*}) \\
&= (e^{i\phi P})(e^{P^*\phi(-i)}) \\
&= (e^{i\phi P})(e^{-i\phi P}) \\
&= e^{i\phi P - i\phi P} \\
&= e^0 \\
&= Id
\end{aligned}$$

Ecuación 27.

$$\begin{aligned}
e^{i\varphi|X\rangle\langle X|}\,|X\rangle &= (Id + (e^{i\varphi}-1)\,|X\rangle\,\langle X|)\,|X\rangle \\
&= |X\rangle + (e^{i\varphi}-1)\,|X\rangle\,\langle X|X\rangle \\
&= |X\rangle + (e^{i\varphi}-1)\,|X\rangle \\
&= |X\rangle + e^{i\varphi}\,|X\rangle - |X\rangle \\
&= e^{i\varphi}\,|X\rangle
\end{aligned}$$

Ecuación 28.

$$\begin{aligned}
e^{i\phi P}(P\left|X\right\rangle - a\left|X\right\rangle) &= (Id + (e^{i\phi}-1)P)(P\left|X\right\rangle - a\left|X\right\rangle) \\
&= P\left|X\right\rangle - a\left|X\right\rangle + (e^{i\phi}-1)P^2\left|X\right\rangle - a(e^{i\phi}-1)P\left|X\right\rangle \\
&= P\left|X\right\rangle - a\left|X\right\rangle + (e^{i\phi}-1)P\left|X\right\rangle - a(e^{i\phi}-1)P\left|X\right\rangle \\
&= -a\left|X\right\rangle + (1 + (e^{i\phi}-1) - a(e^{i\phi}-1))P\left|X\right\rangle \\
&= -a\left|X\right\rangle + (e^{i\phi} - a(e^{i\phi}-1))P\left|X\right\rangle \\
&= -a\left|X\right\rangle + (e^{i\phi} - a(e^{i\phi}-1))(P\left|X\right\rangle - a\left|X\right\rangle) \\
&+ a(e^{i\phi} - a(e^{i\phi}-1))\left|X\right\rangle \\
&= (-a + a(e^{i\phi} - a(e^{i\phi}-1)))\left|X\right\rangle + (e^{i\phi} \\
&- a(e^{i\phi}-1))(P\left|X\right\rangle - a\left|X\right\rangle)
\end{aligned}$$

Ecuación 29.

$$\begin{aligned}
g(x) &= \alpha_0 x^0 + \alpha_1 x^1 + \alpha_2 x^2 + \dots \\
&= \sum_{k=0}^{\infty} \alpha_k x^k \\
&= \sum_{k=0}^{\infty} \begin{pmatrix}1, & 0\end{pmatrix} Q^k \begin{pmatrix}\sqrt{a} \\ \frac{1}{\sqrt{a}}\end{pmatrix} x^k \\
&= \begin{pmatrix}1, & 0\end{pmatrix} \sum_{k=0}^{\infty} Q^k x^k \begin{pmatrix}\sqrt{a} \\ \frac{1}{\sqrt{a}}\end{pmatrix} \\
&= \begin{pmatrix}1, & 0\end{pmatrix} (Id - Qx)^{-1} \begin{pmatrix}\sqrt{a} \\ \frac{1}{\sqrt{a}}\end{pmatrix} \\
&= \begin{pmatrix}1, & 0\end{pmatrix} \left(\begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix} - Qx \right)^{-1} \begin{pmatrix}\sqrt{a} \\ \frac{1}{\sqrt{a}}\end{pmatrix} \\
&= \begin{pmatrix}1, & 0\end{pmatrix} \left(\begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix} - e^{i\phi P} e^{i\varphi \left|X\right\rangle\left\langle X\right|} x \right)^{-1} \begin{pmatrix}\sqrt{a} \\ \frac{1}{\sqrt{a}}\end{pmatrix} \\
&= \begin{pmatrix}1, & 0\end{pmatrix} \\
&\left(\begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix} - \begin{pmatrix} e^{i\phi}(1 + a(e^{i\phi}-1)) & -a + a(e^{i\phi} - a(e^{i\phi}-1)) \\ e^{i\phi}(e^{i\phi}-1) & e^{i\phi} - a(e^{i\phi}-1) \end{pmatrix} x \right)^{-1} \begin{pmatrix}\sqrt{a} \\ \frac{1}{\sqrt{a}}\end{pmatrix} \\
&= \frac{ax - x}{\sqrt{a}(e^{i\phi P + i\varphi \left|X\right\rangle\left\langle X\right|}x^2 + ((-ae^{i\phi P}a - 1)e^{i\varphi \left|X\right\rangle\left\langle X\right|} + (a-1)e^{i\phi} - a)x + 1)} \\
&= \frac{\sqrt{a}(x-1)}{e^{i\phi P + i\varphi \left|X\right\rangle\left\langle X\right|}x^2 + ((-ae^{i\phi P}a - 1)e^{i\varphi \left|X\right\rangle\left\langle X\right|} + (a-1)e^{i\phi} - a)x + 1}
\end{aligned}$$

Ecuación 30.

$$\begin{aligned}
Ax + B &= g(x)(Cx^2 + Dx + E) \\
&= \sum_{k=0}^{\infty} \alpha_k x^k (Cx^2 + Dx + E) \\
&= \sum_{k=0}^{\infty} C\alpha_k x^{k+2} + \sum_{k=0}^{\infty} D\alpha_k x^{k+1} + \sum_{k=0}^{\infty} E\alpha_k x^k \\
&= \sum_{j=2}^{\infty} C\alpha_{j-2} x^j + \sum_{j=1}^{\infty} D\alpha_{j-1} x^j + \sum_{j=0}^{\infty} E\alpha_j x^j \\
&= \sum_{j=2}^{\infty} C\alpha_{j-2} x^j + \sum_{j=2}^{\infty} D\alpha_{j-2} x^j + D\alpha_0 x^0 \\
&+ \sum_{j=2}^{\infty} E\alpha_{j-2} x^j + E\alpha_0 x^0 + E\alpha_1 x^1 \\
&= E\alpha_0 + (D\alpha_0 + E\alpha_1)x + \sum_{j=2}^{\infty} (C\alpha_{j-2} + D\alpha_{j-1} + E\alpha_j) x^j
\end{aligned}$$

Ecuación 31.

$$\begin{aligned}
\langle b|b\rangle &= \| \, |b\rangle \, \|^2 \\
&= \langle x| \, P^* P \, |x\rangle \\
&= \langle x| \, PP \, |x\rangle \\
&= \langle x| \, P^2 \, |x\rangle \\
&= \langle x| \, P \, |x\rangle \\
&= a
\end{aligned}$$

Ecuación 32.

$$\begin{aligned}
\| \, |b\rangle \, \|^2 &= \langle b|b\rangle \\
&= \langle x| \, P^* P \, |x\rangle \\
&= \langle x| \, PP \, |x\rangle \\
&= \langle x| \, P^2 \, |x\rangle \\
&= \beta
\end{aligned}$$

Ecuación 33.

$$
\begin{aligned}
|W_3\rangle = |W_3\rangle &= P^2|x\rangle - \Pr_{W1} P^2|x\rangle - \Pr_{W2} P^2|x\rangle \\
&= P^2|X\rangle - \frac{\langle W_1| P^2|X\rangle}{\langle W_1|W_1\rangle}|W_1\rangle - \frac{\langle W_2| P^2|X\rangle}{\langle W_2|W_2\rangle}|W_2\rangle \\
&= P^2|X\rangle - \frac{\langle X| P^2|X\rangle}{\langle X|X\rangle}|X\rangle - \frac{\langle W_2| P^2|W_2\rangle}{\langle W_2|W_2\rangle}|W_2\rangle \\
&= P^2|X\rangle - \langle X| P^2|X\rangle |X\rangle - \frac{\langle W_2| P^2|W_2\rangle}{\langle W_2|W_2\rangle}|W_2\rangle \\
&= P^2|X\rangle - \langle X| P^2|X\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}|W_2\rangle \\
&= P^2|X\rangle - \langle X| P^2|X\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle) \\
&= P^2|X\rangle - \langle X| PP|X\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle) \\
&= P^2|X\rangle - \langle X| P^*|b\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle) \\
&= P^2|X\rangle - (P|X\rangle)^*|b\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle) \\
&= P^2|X\rangle - (|b\rangle)^*|b\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle) \\
&= P^2|X\rangle - \langle b|b\rangle |X\rangle \\
&- \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle) \\
&= P^2|X\rangle - \beta|X\rangle - \frac{(P|X\rangle - \alpha|X\rangle)P^2|X\rangle}{(P|X\rangle - \alpha|X\rangle)^* P|X\rangle - \alpha|X\rangle}(P|X\rangle - \alpha|X\rangle)
\end{aligned}
$$

Ecuación 34.

$$\begin{aligned} M\left|X\right\rangle &= e^{i\varphi\left|X\right\rangle\left\langle X\right|}\left|X\right\rangle \\ &= \left(Id + (e^{i\varphi}-1)\left|X\right\rangle\left\langle X\right|\right)\left|X\right\rangle \\ &= \left|X\right\rangle + (e^{i\varphi}-1)\left|X\right\rangle\left\langle X|X\right\rangle \\ &= \left|X\right\rangle + (e^{i\varphi}-1)\left|X\right\rangle \\ &= \left|X\right\rangle + e^{i\varphi}\left|X\right\rangle - \left|X\right\rangle \\ &= e^{i\varphi}\left|X\right\rangle \end{aligned}$$

Ecuación 35.

$$\begin{aligned} P\left|W_2\right\rangle &= P^2\left|X\right\rangle - \alpha P\left|X\right\rangle \\ &= \left|W_3\right\rangle + \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_2\right\rangle + \beta\left|X\right\rangle - \alpha P\left|X\right\rangle \\ &= \left|W_3\right\rangle + \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_2\right\rangle + \beta\left|X\right\rangle - \alpha\left|W_2\right\rangle - \alpha^2\left|W_1\right\rangle \\ &= \left|W_3\right\rangle + \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_2\right\rangle + \beta\left|X\right\rangle - \alpha\left|W_2\right\rangle - \alpha^2\left|X\right\rangle \\ &= (\beta-\alpha^2)\left|X\right\rangle + \left(\frac{\alpha(1-\beta)}{\beta-\alpha^2} - \alpha\right)\left|W_2\right\rangle + \left|W_3\right\rangle \\ &= (\beta-\alpha^2)\left|W_1\right\rangle + \left(\frac{\alpha(1-\beta)}{\beta-\alpha^2} - \alpha\right)\left|W_2\right\rangle + \left|W_3\right\rangle \end{aligned}$$

Ecuación 36.

$$
\begin{aligned}
P\left|W_3\right\rangle &= P^3\left|X\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}(P^2\left|X\right\rangle - \alpha P\left|X\right\rangle) - \beta P\left|X\right\rangle \\
&= P\left|X\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}P^2\left|X\right\rangle + \frac{\alpha^2(1-\beta)}{\beta-\alpha^2}P\left|X\right\rangle \\
&= \left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right)P\left|X\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}P^2\left|X\right\rangle \\
&= \left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right)(\left|W_2\right\rangle + \alpha\left|X\right\rangle) - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&+ \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_2\right\rangle + \beta\left|X\right\rangle \\
&= \left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right)\left|W_2\right\rangle + \left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right)\alpha\left|X\right\rangle \\
&- \left(\frac{\alpha(1-\beta)}{\beta-\alpha^2}\right)\left|W_3\right\rangle - \left(\frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2}\right)\left|W_2\right\rangle - \left(\frac{\alpha\beta(1-\beta)}{\beta-\alpha^2}\right)\left|X\right\rangle \\
&= \left(\left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right)\alpha - \frac{\alpha\beta(1-\beta)}{\beta-\alpha^2}\right)\left|X\right\rangle \\
&+ \left(\left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right) - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2}\right)\left|W_2\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&= \left(\left(\frac{\beta-\alpha^2+\alpha^2(1-\beta)-\beta^2+\beta\alpha^2}{\beta-\alpha^2}\right)\alpha - \frac{\alpha\beta(1-\beta)}{\beta-\alpha^2}\right)\left|X\right\rangle \\
&+ \left(\left(\frac{\beta-\alpha^2+\alpha^2(1-\beta)-\beta^2+\beta\alpha^2}{\beta-\alpha^2}\right)\alpha - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2}\right)\left|W_2\right\rangle \\
&- \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&= \left(\left(\frac{\beta-\alpha^2+\alpha^2-\beta\alpha^2-\beta^2+\beta\alpha^2}{\beta-\alpha^2}\right)\alpha - \frac{\alpha\beta(1-\beta)}{\beta-\alpha^2}\right)\left|X\right\rangle \\
&+ \left(\left(\frac{\beta-\alpha^2+\alpha^2-\beta\alpha^2-\beta^2+\beta\alpha^2}{\beta-\alpha^2}\right)\alpha - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2}\right)\left|W_2\right\rangle \\
&- \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&= \left(\frac{\beta-\beta^2}{\beta-\alpha^2}\alpha - \frac{\beta-\beta^2}{\beta-\alpha^2}\alpha\right)\left|X\right\rangle \\
&+ \left(\left(\frac{\beta-\alpha^2+\alpha^2-\beta\alpha^2-\beta^2+\beta\alpha^2}{\beta-\alpha^2}\right)\alpha - \frac{\alpha\beta(1-\beta)}{\beta-\alpha^2}\right)\left|W_2\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&= \left(\left(\frac{\beta-\alpha^2+\alpha^2-\beta\alpha^2-\beta^2+\beta\alpha^2}{\beta-\alpha^2}\right)\alpha - \frac{\alpha\beta(1-\beta)}{\beta-\alpha^2}\right)\left|W_2\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&= \left(\left(1+\frac{\alpha^2(1-\beta)}{\beta-\alpha^2}-\beta\right) - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2}\right)\left|W_2\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle \\
&= \left(\frac{\alpha^2(1-\beta)}{\beta-\alpha^2} - \frac{\alpha^2(1-\beta)^2}{(\beta-\alpha^2)^2} - \beta + 1\right)\left|W_2\right\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\left|W_3\right\rangle
\end{aligned}
$$

Ecuación 37.

$$\begin{aligned} \| b \| &= \langle b|b\rangle \\ &= \langle x| P^* P |x\rangle \\ &= \langle x| PP |x\rangle \\ &= \langle x| P^2 |x\rangle \\ &= \beta \end{aligned}$$

Ecuación 38.

$$\begin{aligned} A|0\rangle &= |b\rangle \\ &= \frac{1}{\| b \|} |b\rangle \\ &= \frac{1}{\| b \|} P |X\rangle \\ &= \frac{1}{\sqrt{\beta}} P |X\rangle \\ &= \frac{1}{\sqrt{\beta}} (P|X\rangle - \alpha |X\rangle) + \frac{\alpha}{\sqrt{\beta}} |X\rangle \end{aligned}$$

Ecuación 39.

$$\begin{aligned} g(x) &= \sum_{k=0}^{\infty} \gamma_k x^k \\ &= \sum_{k=0}^{\infty} \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} Q^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} x^k \\ &= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} \sum_{k=0}^{\infty} Q^k x^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} (Id - Qx)^{-1} \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \end{aligned}$$

Ecuación 40.

$$
\begin{aligned}
g(x) &= \gamma_0 x^0 + \gamma_1 x^1 + \gamma_2 x^2 + \dots \\
&= \sum_{k=0}^{\infty} \gamma_k x^k \\
&= \sum_{k=0}^{\infty} \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} Q^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} x^k \\
&= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} \sum_{k=0}^{\infty} Q^k x^k \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} (Id - Qx)^{-1} \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - Qx \right)^{-1} \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - e^{i\phi P} e^{i\varphi |X\rangle\langle X|} x \right)^{-1} \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{pmatrix} x \right)^{-1} \begin{pmatrix} \frac{\alpha}{\sqrt{\beta}} \\ \frac{1}{\sqrt{\beta}} \\ 0 \end{pmatrix} \\
&= \frac{(\alpha \cos\phi - i\beta \sin\phi)x^2 + (i\beta \sin\phi - \alpha \cos\phi - \alpha)x + \alpha}{\sqrt{\beta}((-\sin^2\phi - \cos^2\phi)e^{i\varphi}x^3 + ((\beta \sin^2\phi + i\alpha \sin\phi + \beta \cos^2\phi} \\
&\quad \overline{+(2-\beta)\cos\phi)e^{i\varphi} + (1-\beta)\sin^2\phi - i\alpha \sin\phi + (1-\beta)\cos^2\phi + \beta \cos\phi)x^2} \\
&\quad \overline{+((-i\alpha \sin\phi - \beta \cos\phi + \beta - 1)e^{i\varphi} + i\alpha \sin\phi + (\beta - 2)\cos\phi - \beta)x + 1)} \\
&= \frac{(\alpha \cos\phi - i\beta \sin\phi)x^2 + (i\beta \sin\phi - \alpha \cos\phi - \alpha)x + \alpha}{\sqrt{\beta}(-\sin^2\phi - \cos^2\phi)e^{i\varphi}x^3 + \sqrt{\beta}((\beta \sin^2\phi + i\alpha \sin\phi + \beta \cos^2\phi} \\
&\quad \overline{+(2-\beta)\cos\phi)e^{i\varphi} + (1-\beta)\sin^2\phi - i\alpha \sin\phi + (1-\beta)\cos^2\phi + \beta \cos\phi)x^2} \\
&\quad \overline{+\sqrt{\beta}((-i\alpha \sin\phi - \beta \cos\phi + \beta - 1)e^{i\varphi} + i\alpha \sin\phi + (\beta - 2)\cos\phi - \beta)x + \sqrt{\beta}}
\end{aligned}
$$

Ecuación 41.

$$\begin{aligned}
Ax^2+Bx+C &= g(x)(Dx^3+Ex^2+Fx+G)\\
&= \sum_{k=0}^{\infty}\gamma_k x^k(Dx^3+Ex^2+Fx+G)\\
&= \sum_{k=0}^{\infty}D\gamma_k x^{k+3}+\sum_{k=0}^{\infty}E\gamma_k x^{k+2}+\sum_{k=0}^{\infty}F\gamma_k x^{k+1}+\sum_{k=0}^{\infty}G\gamma_k x^k\\
&= \sum_{j=3}^{\infty}D\gamma_{j-3}x^j+\sum_{j=2}^{\infty}E\gamma_{j-2}x^j+\sum_{j=1}^{\infty}F\gamma_{j-1}x^j+\sum_{j=0}^{\infty}G\gamma_j x^j\\
&= \sum_{j=3}^{\infty}D\gamma_{j-3}x^j+\sum_{j=3}^{\infty}E\gamma_{j-2}x^j+E\gamma_0x^2\\
&+\sum_{j=3}^{\infty}F\gamma_{j-1}x^j+F\gamma_0x^1+F\gamma_1x^2\\
&+\sum_{j=3}^{\infty}G\gamma_j x^j+G\gamma_0x^0+G\gamma_1x^1+G\gamma_2x^2\\
&= \sum_{j=3}^{\infty}D\gamma_{j-3}x^j+\sum_{j=3}^{\infty}E\gamma_{j-2}x^j+E\gamma_0x^2\\
&+\sum_{j=3}^{\infty}F\gamma_{j-1}x^j+F\gamma_0x+F\gamma_1x^2\\
&+\sum_{j=3}^{\infty}G\gamma_j x^j+G\gamma_0+G\gamma_1x+G\gamma_2x^2\\
&= G\gamma_0+(F\gamma_0+G\gamma_1)x+(E\gamma_0+F\gamma_1+G\gamma_2)x^2\\
&+\sum_{j=3}^{\infty}(D\gamma_{j-3}+E\gamma_{j-2}+F\gamma_{j-1}+G\gamma_j)x^j
\end{aligned}$$

Ecuación 42.

$$\begin{aligned}
\parallel|w_2\rangle\parallel^2 &= \langle w_2|w_2\rangle\\
&= (\langle x|P-\alpha\langle x|)(P|x\rangle-\alpha|x\rangle)\\
&= \langle x|P^2|x\rangle-\alpha\langle x|P|x\rangle-0\\
&= \beta-\alpha\alpha\\
&= \beta-\alpha^2
\end{aligned}$$

Ecuación 43.

$$\begin{aligned}
\| \, |w_3\rangle \, \|^2 &= \langle w_3|w_3\rangle \\
&= (\langle x| \, (P^2)^* - \beta \, \langle x| \, P^* - \langle w_2| \, \frac{\alpha(1-\beta)}{\beta-\alpha^2})(P^2 \, |x\rangle - \beta P \, |x\rangle \\
&- \frac{\alpha(1-\beta)}{\beta-\alpha^2} \, |w_2\rangle) \\
&= (\langle x| \, P^2 - \beta \, \langle x| \, P)(P^2 \, |x\rangle - \beta P \, |x\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2} \, |w_2\rangle) \\
&= \langle x| \, P^4 \, |x\rangle - \beta \, \langle x| \, P^2 \, |x\rangle - \frac{\alpha(1-\beta)}{\beta-\alpha^2}(\langle x| \, P^3 \, |x\rangle - \alpha \, \langle x| \, P^2 \, |x\rangle) \\
&= \langle x| \, P^4 \, |x\rangle - \beta^2 - \frac{\alpha(1-\beta)}{\beta-\alpha^2}(\alpha - \alpha\beta \\
&= \langle x| \, P^2 \, |x\rangle - \beta^2 - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\alpha(1-\beta) \\
&= \beta - \beta^2 - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\alpha(1-\beta) \\
&= \beta(1-\beta) - \frac{\alpha(1-\beta)}{\beta-\alpha^2}\alpha(1-\beta) \\
&= (1-\beta)(\beta - \alpha\frac{\alpha(1-\beta)}{\beta-\alpha^2} \\
&= \beta - \beta^2 - \frac{\alpha^2(1-\beta)^2}{\beta-\alpha^2}
\end{aligned}$$

Ecuación 44.

$$\begin{aligned}
Q \, |X\rangle &= e^{i\phi P} e^{i\varphi |X\rangle\langle X|} \, |X\rangle \\
&= [Id + (e^{i\phi} - 1)P][Id + (e^{i\varphi} - 1) \, |X\rangle \, \langle X|] \, |X\rangle \\
&= [Id + (e^{i\phi} - 1)P][|X\rangle + (e^{i\varphi} - 1) \, |X\rangle \, \langle X|X\rangle] \\
&= [Id + (e^{i\phi} - 1)P][|X\rangle + |X\rangle \, e^{i\varphi} - |X\rangle] \\
&= [Id + (e^{i\phi} - 1)P][|X\rangle \, e^{i\varphi}] \\
&= e^{i\varphi} \, |X\rangle + e^{i\varphi}(e^{i\phi} - 1)P \, |X\rangle
\end{aligned}$$

Ecuación 45.

$$\begin{aligned}
QP\,|X\rangle &= e^{i\phi P}e^{i\varphi|X\rangle\langle X|}P\,|X\rangle \\
&= [Id + (e^{i\phi}-1)P][Id + (e^{i\varphi}-1)\,|X\rangle\,\langle X|]P\,|X\rangle \\
&= [Id + (e^{i\phi}-1)P][P\,|X\rangle + (e^{i\varphi}-1)\,|X\rangle\,\langle X|\,P\,|X\rangle] \\
&= [Id + (e^{i\phi}-1)P][P\,|X\rangle + (e^{i\varphi}-1)\,|X\rangle\,\alpha] \\
&= P\,|X\rangle + (e^{i\phi}-1)P^2\,|X\rangle + (e^{i\varphi}-1)\,|X\rangle\,\alpha + \alpha(e^{i\phi}-1)(e^{i\varphi}-1)P\,|X\rangle \\
&= P\,|X\rangle + (e^{i\phi}-1)P\,|X\rangle + (e^{i\varphi}-1)\,|X\rangle\,\alpha + \alpha(e^{i\phi}-1)(e^{i\varphi}-1)P\,|X\rangle \\
&= \alpha(e^{i\varphi}-1)\,|X\rangle + [1 + e^{i\phi} - 1 + \alpha(e^{i\phi}-1)(e^{i\varphi}-1)]P\,|X\rangle \\
&= \alpha(e^{i\varphi}-1)\,|X\rangle + [e^{i\phi} + \alpha(e^{i\phi}-1)(e^{i\varphi}-1)]P\,|X\rangle
\end{aligned}$$

Ecuación 46.

$$\begin{aligned}
|b\rangle &= P\,|X\rangle \\
&= A\,|s\rangle\,\langle s|\,A^{-1}\frac{1}{\sqrt{a}}\,|\psi_1\rangle \\
&= \frac{1}{\sqrt{a}}A\,|s\rangle\,\langle s|\,A^{-1}\,|\psi_1\rangle \\
&= \frac{1}{\sqrt{a}}A\,|s\rangle\,\langle s|\,A^{*}\,|\psi_1\rangle \\
&= \frac{1}{\sqrt{a}}A\,|s\rangle\,(\langle\psi_1|\,A\,|s\rangle)^{*} \\
&= \frac{1}{\sqrt{a}}(|\psi_1\rangle + |\psi_0\rangle)(\langle\psi_1|\,A\,|s\rangle)^{*} \\
&= \frac{1}{\sqrt{a}}(|\psi_1\rangle + |\psi_0\rangle)(\langle\psi_1|\,(|\psi_1\rangle + |\psi_0\rangle))^{*} \\
&= \frac{1}{\sqrt{a}}(|\psi_1\rangle + |\psi_0\rangle)(\langle\psi_1|\psi_1\rangle + \langle\psi_0|\psi_1\rangle) \\
&= \frac{1}{\sqrt{a}}(|\psi_1\rangle + |\psi_0\rangle)a \\
&= \frac{a}{\sqrt{a}}(|\psi_1\rangle + |\psi_0\rangle) \\
&= \sqrt{a}(|\psi_1\rangle + |\psi_0\rangle) \\
&= \sqrt{a}\,|\psi_1\rangle + \sqrt{a}\,|\psi_0\rangle
\end{aligned}$$

Ecuación 47.

$$\begin{aligned}
|\gamma_0\rangle &= x\,|X\rangle + yP\,|X\rangle \\
&= x\,|X\rangle + yA\,|s\rangle\,\langle s|\,A^{-1}\,|X\rangle \\
&= x\,|X\rangle + yA\,|s\rangle\,(\langle\psi_1| + \langle\psi_0|)\,|X\rangle \\
&= x\frac{1}{\parallel \psi_1 \parallel}\,|\psi_1\rangle + yA\,|s\rangle\,\langle\psi_1|\,\frac{1}{\parallel \psi_1 \parallel}\,|\psi_1\rangle \\
&= \frac{x}{\sqrt{a}}\,|\psi_1\rangle + yA\,|s\rangle\,\frac{1}{\parallel \psi_1 \parallel}\langle\psi_1|\psi_1\rangle \\
&= \frac{x}{\sqrt{a}}\,|\psi_1\rangle + yA\,|s\rangle\,\frac{a}{\sqrt{a}} \\
&= \frac{x}{\sqrt{a}}\,|\psi_1\rangle + yA\,|s\rangle\,\sqrt{a}
\end{aligned}$$

Ecuación 48.

$$\begin{aligned}
U\,|\gamma_0\rangle &= U\frac{1}{\parallel |c\rangle \parallel}\,|c\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}U\,|c\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}U(P_0 - R_0)\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}(Id - 2\,\langle\beta|\,R_0\,|\beta\rangle^{-1}\,R_0\,|\beta\rangle\,\langle\beta|\,R_0)(P_0 - R_0)\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}(P_0 - R_0)\,|\beta\rangle + 2\,\langle\beta|\,R_0\,|\beta\rangle^{-1}\,R_0\,|\beta\rangle\,\langle\beta|\,R_0^2\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}(P_0 - R_0)\,|\beta\rangle + 2\,\langle\beta|\,R_0\,|\beta\rangle^{-1}\,R_0\,|\beta\rangle\,\langle\beta|\,R_0\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}(P_0 - R_0)\,|\beta\rangle + 2R_0\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}P_0\,|\beta\rangle - R_0\,|\beta\rangle + 2R_0\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}P_0\,|\beta\rangle + R_0\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}(P_0 + R_0)\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}(P_0 - R_0)^2\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}T^2\,|\beta\rangle \\
&= \frac{1}{\parallel |c\rangle \parallel}T\,|c\rangle
\end{aligned}$$

Ecuación 49.

$$\begin{aligned}
\| \, |c\rangle \, \| &= \sqrt{\langle c| \, |c\rangle} \\
&= \sqrt{\langle \beta| \, (P_0^* - R_0^*)(P_0 - R_0) \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, (P_0 - R_0)(P_0 - R_0) \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, (P_0 - R_0)^2 \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, (P_0 + R_0) \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, T^2 \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, (T^2)^2 \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, T^2 T^2 \, |\beta\rangle} \\
&= \sqrt{\langle \beta| \, T^2 T \, |c\rangle} \\
&= \sqrt{\langle c| \, T^* T \, |c\rangle} \\
&= \sqrt{\| \, T \, |c\rangle \, \|^2} \\
&= \| \, T \, |c\rangle \, \|
\end{aligned}$$

Ecuación 50.

$$\begin{aligned}
e^{i\phi T^2} &= e^{i\phi(P_0 + R_0)} \\
&= e^{i\phi P_0 + i\phi R_0} \\
&= e^{i\phi P_0} e^{i\phi R_0} \\
&= [Id + (e^{i\phi} - 1)P] e^{i\phi R_0} \\
&= [Id + (e^{i\phi} - 1) A \, |0\rangle \, \langle 0| \, A^{-1}] e^{i\phi R_0} \\
&= [AA^{-1} + (e^{i\phi} - 1) A \, |0\rangle \, \langle 0| \, A^{-1}] e^{i\phi R_0} \\
&= A[Id + (e^{i\phi} - 1) \, |0\rangle \, \langle 0|] A^{-1} e^{i\phi R_0}
\end{aligned}$$

Bibliografía

[1] A. Ambainis. Quantum walks and their algorithmic applications. *Int. J. Quantum Information*, 2003.

[2] C. Bautista and N. Castillo. Möbius transformation in quantum amplitude amplification with generalized phases. *Int. J. Quantum Information*, 8(6):923–935, Diciembre 2010.

[3] C. Bautista, C. Guillen, and A. Rangel. From projections to a generalized quantum search. *Quantum Information Processing*, 2012.

[4] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. *Quantum amplitude amplification and estimation, in Quantum Computation and Information.*, volume 305 of *Mathematics*. AMS, Providence, 2002.

[5] E. Desurvire. *Clasical and Quantum Information Theory: An Introduction for the Telecom Scientist.* Cambridge University, 2009.

[6] R. P. Feynman. Simulating Physics with Computers. *Int. J. Theor. Physics*, 21(6/7):467–488, 1982.

[7] L. K. Grover. Quantum Mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett*, 79(2):325, 2010.

[8] P. Høyer. Arbitrary phases in quantum amplification. *Phys. Rev*, 62, 2000.

[9] W. L. Jin and X. D. Chen. A desired state can not be found with certainty for grover's algorithm in a posible three-dimensional cumplex subspace. *Quantum Information Process*, (10), Enero 2011.

[10] J. M. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge Univ. Press, 2010.

[11] S. E. Venegas Andraca. *Quantum walks for computer scientists.* Morgan & Claypool, 2008.