Benemérita Universidad Autónoma de Puebla

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS
LICENCIATURA EN MATEMÁTICAS

TÍTULO DE LA TESIS

q- ALGORITMOS DE BÚSQUEDA

TESIS PRESENTADA COMO REQUISITO PARA OBTENER
EL TÍTULO DE
LICENCIADA EN MATEMÁTICAS

PRESENTA
MAGALI ROSETE TAPIA

DIRECTORES DE TESIS
DR. CÉSAR BAUTISTA RAMOS.
DR. CARLOS GUILLÉN GALVÁN

PUEBLA, PUE. OCTUBRE, 2014

Contenido

Agradecimientos

La presente tesis se la dedico a mi familia que gracias a su apoyo pude concluir mi carrera.

A agradezco a dios por ser maravilloso que me dio fuerza y fe.

A mis queridos padres : Carlos Rosete Modesto y Rosa Severiana Tapia Rosales, por brindarme los recursos necesarios, por todo su cariño, consejos y además por sus palabras de aliento para seguir adelante en todo momento. A mis hermanos Eder de Jesus, Cristy, por sus muestras de afecto.

Muy particularmente agradezco a mi asesor Dr. Cesar Bautista Ramos por ser un gran maestro, investigador y un gran guía para el asesorado.

A mis amigas y amigos que son las personas que han estado más cerca de mi en estos años de universidad impidiendo que me sienta sola, apoyándome y regañandome cuando era necesario, y haciéndome pasar momentos inolvidables.

Acronimos y Notación

EPR	Einstein, Podolski y Rosen.
qubit	bit cuántico.
$\|\rangle$	Notación de Dirac.
$\|X\rangle$	ket x.
$\langle X\|$	Bra.
$\langle X\|X\rangle$	Braket .
$\|X\rangle\langle X\|$	Ketbra.
$\otimes$	Tensor.
$\oplus$	Suma directa.

Introducción

La computación cuántica tiene sus orígenes en ideas de Richard Feynman (premio Nobel en 1965) sobre la miniaturización de las computadoras [4].

El objetivo principal de este trabajo es explicar el desarrollo del algoritmo Grover, como un problema de búsqueda de soluciones en sistemas de ecuaciones lineales no homogéneos y singulares.

Para lograr este objetivo se usarán, varias ramas de las matemáticas como: álgebra lineal, combinatoria, complejidad computacional, probabilidades, análisis complejo, ademas de mecánica cuántica, entre otros. Dando así a conocer información relevante de la computación cuántica, para lograr que el lector pueda comprender de manera didáctica este trabajo.

Se inicia con una breve descripción del campo teórico de la computación cuántica, con los axiomas de la computación cuántica, las compuertas cuántica y entrelazamientos cuánticos.

De acuerdo con lo anterior continuamos con el estudio de nuestros algoritmos cuántico. Primero, el algoritmo cuántico de Deutsch, posteriormente el algoritmo de Deutsch-Jozsa que es una generalización del algoritmo de Deutsch.

Se definen las compuertas controladas cuánticas. Se estudia una aplicación con mayor crecimiento en la teoría de la información cuántica como la comunicación cuántica. Dentro de ella se trata a la teleportación cuántica y sus ventajas sobre la computación clásica.

Continuamos analizando el algoritmo de Grover y funciones de orden. Luego se hace una generalización del algoritmo de Grover, series formales y por último se dan ejemplos de ecuaciones lineales utilizando algoritmos cuánticos.

Capítulo 1

Computación cuántica

1.1 Preeliminares

La computación cuántica es una forma radicalmente nueva de procesar información, posibilitada por propiedades exclusivas de la macánica cuántica. Dentro de la computación cuánticas se trabaja como $\mathbb{C}^n$ en espacio de Hilbert [6].

Definición 1.1. Un espacio de Hilbert es una pareja $(V, \cdot)$ donde el primer elemento V es un espacio vectorial sobre los $\mathbb{C}$ y $* \cdot * : v \times v \longrightarrow \mathbb{C}$ es una función producto interno (punto, bracket) tal que:

1. Para todo $v_1, w_2 \in V$ y $\lambda_1, \mu \in \mathbb{C}$ se debe de cumplir que $v \cdot (\lambda\omega_1 + \mu_2) = \lambda(v \cdot \omega_1) + \mu(v \cdot \omega_2)$ (es decir, $\cdot$ es lineal en la segunda entrada).

2. Para todo $v, w \in V$, tenemos que $(v \cdot w)^* = w \cdot v$ donde $*$ indica conjugación compleja.

3. El producto interno $v \cdot v \geq 0$, para todo $v \in V$, siendo $v \cdot v = 0$ si y sólo si $v = 0$.

4. El conjunto $\mathbb{C}^n$ con la distancia inducida $||V|| = \sqrt{V \cdot V}$, es un espacio métrico completo.

Probaremos primero el siguiente teorema.

Teorema 1.1. El conjunto $\mathbb{C}^n$ tiene un estructura de $\mathbb{C}$ de espacio vectorial.

Demostración. Sea

$$\mathbb{C}^n := \{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mid \quad a_1, a_2, \ldots, a_n \in \mathbb{C}\},$$

recordemos la suma de dos vectores complejos :

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{pmatrix},$$

es un vector complejo.

El producto de un vector complejo por un escalar $\lambda \in \mathbb{R}$,

$$\lambda \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \lambda a_1 \\ \lambda a_2 \\ \vdots \\ \lambda a_n \end{pmatrix},$$

es un vector complejo.

La suma y el producto por un escalar cumplen todas las propiedades requeridas para ser un espacio vectorial.

□

Ahora probaremos la estructura de espacio de Hilbert.

Teorema 1.2. Tenemos que $\mathbb{C}^n$ tiene la estructura de espacio de Hilbert complejo.

Demostración. Se verificaran los cuatro axiomas de un espacio de Hilbert. Se define el producto punto (escalar) hermitiano de la siguiente manera:

Sea $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1^* b_1 + a_2^* b_2 + \cdots + a_n^* b_n \in \mathbb{C}$, donde $*$ indica la conjugación compleja.

Notemos: El producto punto $\cdot$ es lineal en la segunda entrada:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \left(\lambda \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} + \mu \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \right)$$

$$= \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} \lambda b_1 + \mu c_1 \\ \lambda b_2 + \mu c_2 \\ \vdots \\ \lambda b_n + \mu c_n \end{pmatrix}$$

$$= a_1^*(\lambda b_1 + \mu c_1) + a_2^*(\lambda b_2 + \mu c_2) + \cdots + a_n^*(\lambda b_n + \mu c_n)$$

$$= (\lambda a_1^* b_1 + \lambda a_2^* b_2 + \cdots + \lambda a_n^* b_n) + (\mu a_1^* c_1 + a_2^* b_2 + \cdots + \mu a_n^* b_n)$$

$$= \lambda(a_1^* b_1 + \cdots + a_n^* b_n) + \mu(a_1^* c_1 + \cdots + a_n^* c_n)$$

$$= \lambda \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} + \mu \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}.$$

Es claro que "$\cdot$" es hermitiano ya que:

$$\left[\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \right]^* = [a_1^* b_1 + a_2^* b_2 + \cdots + a_n^* b_n]^*$$

$$
\begin{aligned}
&= (a_1^* b_1)^* + (a_2^* b_2)^* + \cdots + (a_n^* b_n)^* \\
&= a_1^{**} b_1^* + a_2^{**} b_2^* + \cdots + a_n^{**} b_n^* \\
&= a_1 b_1^* + a_2 b_2^* + \cdots + a_n b_n^* \\
&= b_1^* a_1 + b_2^* a_2 + \cdots + b_n^* a_n \\
&= \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.
\end{aligned}
$$

El producto de vectores es positivo:

$$
\begin{aligned}
\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} &= a_1^* a_1 + a_2^* a_2 + \cdots + a_n^* a_n \\
&= |a_1|^2 + |a_2|^2 + \cdots + |a_n|^2 \\
&\geq 0.
\end{aligned}
$$

Tenemos pues, que $0 = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, por consecuencia $|a_1|^2 + |a_2|^2 + \cdots +$ $|a_n|^2 = 0$, si sólo si $a_1 = a_2 = \cdots = a_n$, entonces $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

El conjunto $\mathbb{C}^n$ con la distancia inducida $||v|| = \sqrt{v \cdot v}$ es un espacio métrico completo, ya que $\mathbb{C}^n$ es isomorfo a $\mathbb{R}^{2n}$ el cuál es espacio métrico completo.

□

Por lo tanto tenemos que $\mathbb{C}^n$ es un espacio hermitiano complejo.

Los elementos básicos de la computación cuántica son los qubit.

1.2 Qubit cuántico

Un qubit (del ingles qubit, quantum bit) es un estado cuántico en un espacio de Hilbert y la mínima de información cuántica. Sus dos estados básicos se llaman, convencionalmente, $|1\rangle$ y $|0\rangle$ (se pronuncia ket cero y ket uno).

Un vector bra , es el transpuesta conjugado de un vector ket. Asumimos que para cada ket $|1\rangle$ existe un bra, y lo denotamos como $\langle 1|$.

1.3 Axiomas de la computación cuántica

En general, una teoría formal comienza con la formulación de axiomas [4]. La computación cuántica no es la excepción.

Axioma 1.1. a) Asociado a cada sistema físico aislado, está un espacio de Hilbert, llamado *espacio de estado.*

b) El sistema esta completamente descrito por un vector de estado que es un vector de norma uno.

El estado (puro) de una máquina (memoria) está descrito por un vector $v \in \mathbb{C}^n$ tal que $||v|| = 1$.

Ejemplo 1.1. El vector $|0\rangle = \binom{1}{0} \in \mathbb{C}^2$ es un estado puro, pues $||\binom{1}{0}|| = \sqrt{\binom{1}{0} \cdot \binom{1}{0}} = \sqrt{1+0} = 1$. También $|1\rangle = \binom{0}{1} \in \mathbb{C}^2$ es un estado puro, porque $||\binom{0}{1}|| = \sqrt{\binom{0}{1} \cdot \binom{0}{1}} = \sqrt{0+1} = 1$. Otro ejemplo es el vector $\binom{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} \in \mathbb{C}^2$ que una vez más es un estado puro: $||\binom{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}}||= \sqrt{\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} \cdot \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}} = \sqrt{\frac{1}{2}+\frac{1}{2}} = 1.$

Nótese que :$\binom{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} = \frac{1}{\sqrt{2}}\binom{1}{0} + \frac{1}{\sqrt{2}}\binom{0}{1} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

Axioma 1.2. La evolución de un sistema cuántico cerrado está descrita por una matriz unitaria.

Axioma 1.3 (Axioma de medición). Supóngase que se tienen $m_1, \ldots, m_n$ posibles mediciones de un experimento de un sistema cuántico, entonces las mediciones (observaciones) cuánticas están descritas por una colección de matrices M_{m_1}, $M_{m_2}, \ldots, M_{m_n}$ actuando sobre el espacio de estados, tales que $M_{m_1}M_{m_1}^* + M_{m_2}^*M_{m_2} + \cdots + M_{m_n}^*M_{m_n} = Id$ en la cual es la *ecuación de completez*.

Además si $|\psi\rangle$ es el estado del sistema antes de medición, entonces la probabilidad de observar (medir) m_i es $\rho_i = \langle\psi|M_{m_i}^*|\psi\rangle$ donde $\langle\psi| = |\psi\rangle^*$, $i = 1, \ldots, n$ y el estado del sistema se colapsa (después de la medición).

Es común denotar, los vectores no cero con $|v\rangle \in \mathbb{C}^n$. El estado del sistema (máquina) en tiempo t_1 es $|\psi_1\rangle$ y el estado del sistema en tiempo $t_2 > t_1$ es $|\psi_2\rangle$, entonces $|\psi_2\rangle = U|\psi_1\rangle$ donde U es matriz unitaria (esto es donde Id es matriz identidad y U^* es la transpuesta conjugada de U es decir $U^{-1} = U^*$).

Ejemplo 1.2. Sea

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

es una matriz unitaria. Luego el producto

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

entonces por el axioma 1.2, tenemos que W (llamada *matriz de Walsh-Hadamard*) sirve como una "instrucción" en una computadora cuántica.

En nuestro caso computadora cuántica es un concepto indefinido, pero sigue los cuatro axiomas de la computación cuántica (el cuarto axioma es presentado mas adelante). Además si supóngase que se tiene la máquina (sistema) con estado inicial $|\psi_0\rangle = |0\rangle$, el cual podemos usar el axioma(1.1). Ahora le aplicamos la

máquina de evolución descrita por W luego el estado cambia

$$|\psi_1\rangle = W|\psi_0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

esquématicamente tenemos el siguiente circuito:

$$|0\rangle \ —\boxed{W}— \ (\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle)$$

Mostraremos nuestro primer algoritmo cuántico, que genera bits al azar, utilizando los cuatro axiomas de la computación cuántica.

Algoritmo 1.1 Generar bits 0 ó 1 al azar

Entrada: nulo
Salida: 0 ó 1 al azar

1: Se prepara el sistema con estado inicial:
$$|\psi_0\rangle = |0\rangle = \tbinom{0}{1}$$
2: Se evoluciona el sistema aplicando W al estado anterior:
$$|\psi_1\rangle = W|\psi_0\rangle$$
3: Observar el sistema usando matrices de medición.

Analizando el algoritmo notemos que:

En el primer paso, utilizamos el axioma (1.1). Se prepara el sistema con estado inicial: $|\psi_0\rangle = |0\rangle = \binom{0}{1}$.

En el segundo paso, utilizamos el axioma (1.2). Se prepara el sistema con estado inicial: $|\psi_1\rangle = W|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

En el tercer paso utilizamos el axioma (1.3). Observando el sistema usando matrices de medición tenemos: $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, tal que

$$
\begin{aligned}
M_0^* M_0 + M_1^* M_1 &= M_0 M_0 + M_1 M_1 \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}
$$

Es decir M_0, M_1 cumplen la ecuación de completez. La matriz M_0 se asocia a observar 0 y M_1 se asocia a observar 1. Luego por axioma de medición, la probabilidad de observar 0 es: $p_0 = \langle\psi_1|M_0^* M_0|\psi_1\rangle$. Nótese $(M_0|\psi_1\rangle)^* = |\psi_1\rangle^* M_0^* = \langle\psi_1|M_0^*$ o bien $\frac{1}{\sqrt{p_0}} M_0|\psi_1\rangle$.

Pero notemos que: $|\psi_1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \binom{1}{0} = \binom{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}}$ y $M_0^* M_0 = M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Por consiguiente, $\langle\psi_1| = |\psi_1\rangle^* = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ y, por tanto $p_0 = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2}$.

Además el sistema se colapsa a $\frac{1}{\sqrt{\frac{1}{2}}} M_0|\psi_1\rangle = \sqrt{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \binom{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} = |0\rangle$.

Análogamente se hace con M_1, lo cual tenemos $p_1 = \frac{1}{2}$ y se colapsa a $|1\rangle$. Así el sistema se colapsa a : $|0\rangle$ con probabilidad $\frac{1}{2}$ y $|1\rangle$ con probabilidad $\frac{1}{2}$, lo cual genera 0,1 al azar.

Observación 1.1. Todas las matrices usadas son cuadradas, unitarias y las de mediciones cumplen la ecuación de completez.

Proposición 1.1. Si $|\psi\rangle$ y $|\varphi\rangle$ son vectores en $\mathbb{C}^n$, entonces

a) $\langle\psi|\varphi\rangle = \psi \cdot \varphi$

b) $\langle\psi|\psi\rangle = ||\psi||^2$.

Demostración. Sea $|\psi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ y $|\varphi\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$, entonces

a) $\langle\psi|\varphi\rangle = (a_1^*, a_2^*, \ldots, a_n^*) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1^* b_1 + a_2^* b_2 + \cdots + a_n^* b_n = \psi \cdot \varphi$

b) $\langle\psi|\psi\rangle = (a_1^*, a_2^*, \ldots, a_n^*) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = a_1^* a_1 + a_2^* a_2 + \cdots + a_n^* a_n = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$

$= ||\psi||^2.$

□

Observación 1.2. En general, es mejor tener las propiedades de un objeto en sí. Por ejemplo: en lugar de tener $a = 1.41423...$ es mejor tener a^2, es decir que $a = \sqrt{2}$.

Siguiendo este principio, revisemos la medición del algoritmo 1.1 de generación de números aleatorios. La medición de $|0\rangle\langle 0| = \binom{1}{0}(1,0) = M_0$ y $|1\rangle\langle 1| = \binom{0}{1}(0,1) = M_1$.

El sistema se colapsa a $\frac{1}{\sqrt{p_0}} M_0|\psi_1\rangle = \frac{1}{\sqrt{p_0}}|0\rangle\langle 0|(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) = \frac{1}{\sqrt{\frac{1}{2}}}\frac{1}{\sqrt{2}}|0\rangle = |0\rangle$, con probabilidad $\frac{1}{2}$ ya que $\langle 0|0\rangle = ||0\rangle\|^2 = 1$ y $\langle 0|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$

y además que $p_0 = \langle\psi_1|M_0^* M_0|\psi_1\rangle = \langle\psi_1|(|0\rangle\langle 0|)^*|0\rangle\langle 0|\psi_1\rangle = \langle 0|\psi_1\rangle^*\langle 0|\psi_1\rangle = |\langle 0|\psi_1\rangle|^2 = |\frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}\langle 0|1\rangle|^2 = \frac{1}{2}$.

Similarmente con M_1, tenemos el sistema se colapsa a $|1\rangle$, con probabilidad $\frac{1}{2}$.

Definición 1.2. Los escalares que acompañan a los estados (vector de norma) se llaman *Amplitudes* y los estados $|\psi\rangle$ y $e^{i\xi}|\psi\rangle$ ($i^2 = -1$, $\xi \in \mathbb{R}$, $|e^{i\xi}| = 1$) se consideran equivalentes.

Observación 1.3. Nótese que:

1. $\langle\psi|e^{-i\xi}e^{i\xi}|\psi\rangle = \langle\psi|\psi\rangle$,
2. $\alpha|\psi_1\rangle + e^{i\xi}|\psi_2\rangle$ con $\alpha \in \mathbb{C}$ no es equivalente a $\alpha|\psi_1\rangle + |\psi_2\rangle$, $i \in \mathbb{C}$;
3. $e^{i\xi}(\alpha|\psi_1\rangle + |\psi_2\rangle)$ si es equivalente a $\alpha|\psi\rangle + |\psi_2\rangle$.

Así las fases globales en mecánica cuántica se desprecián.

Físicamente, el producto tensorial permite hacer un tratamiento unificado de las propiedades cuánticas de los sistemas.

1.4 Productos tensoriales

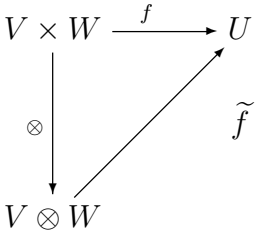
El producto tensorial es una forma de combinar espacios, operadores y vectores. Suponiendo que H_1 y H_2 son espacios de Hilbert de dimensión n y m respectivamente. Entonces el espacio generado por el producto tensorial $H_1 \otimes H_2$ es un nuevo y más grande espacio de Hilbert de dimensión $n \times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

Observación 1.4. El producto tensorial de los vectores $|\psi\rangle$ con $|\varphi\rangle$ es $|\psi\rangle \otimes |\varphi\rangle$ lo cual es un nuevo vector y el producto tensorial es bilineal.

Axioma 1.4. (**Sistemas Compuestos**) Si el sistema físico (Cuántico) A tiene espacio de estado, el espacio de Hilbert H_1 y se tiene un segundo sistema físico (cuántico) B con espacio de estado, el espacio de Hilbert H_2, entonces el sistema compuesto AB tiene espacio de estado, el espacio de Hilbert $H_1 \otimes H_2$. Además si $|\psi_1\rangle$ es el estado de sistema A y $|\psi_2\rangle$ es el estado del sistema de B en cierto tiempo t, el estado del sistema compuesto en tiempo t es : $|\psi_1\rangle \otimes |\psi_2\rangle$.

Consideremos la categoría de espacios vectoriales complejos: $Vect_C$. En $Vect_C$ el producto tensorial es un objeto que resuelve las siguientes propiedades universales:

Sean $V, W \in Vect_C$. Entonces la pareja $(V \otimes W, \otimes)$, formada por $V \otimes W \in Vect_C$ y una función $V \times W \longrightarrow V \otimes W$ bilineal, tiene la segunda propiedad universal, para todo $f : V \times W \longrightarrow U$ bilineal con $U \in Vect_C$, existe una única $\widetilde{f} : V \otimes W \longrightarrow U$ lineal que hace conmutar el siguiente diagrama:



Teorema 1.3. El producto tensorial existe en $Vect_C$.

Demostración. Sean $V, W \in Vect_C$, se toma R el espacio vectorial complejo con base $\{(v, w) | \, v \in V, w \in W\}$. Sea S el subespacio de $V \times W$ generado por

$$(v_1, \lambda w_1 + \mu w_2) - \lambda(v_1, w_1) - \mu(v_1, w_2),$$
$$(\lambda v_1 + \mu v_2, w) - \lambda(v_1, w_1) - \mu(v_2, w),$$
$$\lambda(v_1, w) - \lambda(v, w),$$
$$\mu(v, w) - (v, \lambda w).$$

Para todo $v, v_1, v_2 \in V$, para todo $w, w_1, w_2 \in W$, y para todo $\lambda, \mu \in \mathbb{C}$. Se define $T = R/S \in Vect_{\mathbb{C}}$, por consiguiente se tiene el morfismo lineal canónico $\rho : R \to R/S = T$ y $r \mapsto [r] = r + S$. Luego se define el tensor $\otimes : V \times W \to T$ y $(v, w) \mapsto \rho((v, w)) = (v, w) + S$.

Esto es $\otimes(v, w) = [(v, w)]$, para todo $v \in V$ y $w \in W$. Se define $v \otimes w := \otimes[(v, w)]$. □

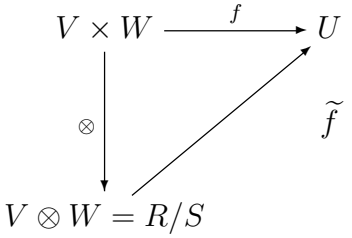
Afirmación 1.1. El $\otimes$ es bilineal.

Demostración. Sea $v \in V$ y $w_1, w_2 \in W$ con $\lambda, \mu \in \mathbb{C}$

$$\begin{aligned} v \otimes (\lambda w_1 + \mu w_2) - \lambda(v \otimes w_1) - \mu(\nu \otimes w_2) & \\ &= [(v_1, \lambda w_1 + \mu w_2)] - \lambda[(v, w_1)] - \mu[(v, w_2)] \\ &= [(v_1, \lambda w_1 + \mu w_2) - \lambda(v, w_1)] - \mu[(v, w_2)] \\ &= (v_1 \lambda w_1 + \mu w_2) - \lambda(v, w_1) - \mu[(v, w_2)] + S \\ &= 0 + S \\ &= 0. \end{aligned}$$

Por lo tanto $v \otimes (\mu\omega_1 + \lambda\omega_2) = \mu(v \otimes \omega_1) + \lambda(v \otimes \omega_2)$ es lineal derecho, de forma análoga es lineal izquierdo, lo cual concluimos que $\otimes$ es bilineal. □

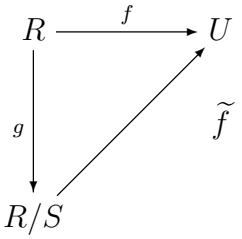
Afirmación 1.2. Existe $\tilde{f} : V \otimes W \to U$ lineal tal que, el diagrama conmuta.



Demostración. Sea $g : R \to U$ lineal definida por $g(v, w) = f(v, w)$ (recordar que las transformaciones lineales se pueden definir en bases). Ahora $S \subseteq \ker g$. En efecto, basta mostrar en los generadores:

$$\begin{aligned} g(\lambda(v, \omega) - (\lambda v, \omega)) &= \lambda g(v, \omega) - g(\lambda v, \omega)) \\ &= \lambda f(v, \omega) - f(\lambda v, \omega) \\ &= \lambda f(v, \omega) - \lambda f(v, \omega) \\ &= 0. \end{aligned}$$

Por lo tanto $S \subseteq \ker g$ entonces existe una función $\tilde{f} : R/S \to U$, tal que:



(1.1)

$$\tilde{f}[(v, w)] = g(v, w).$$

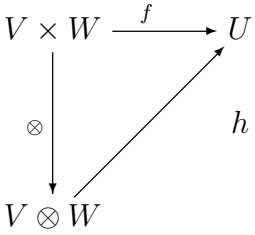
Ahora veamos que el diagrama (1.1) conmuta:

$$\begin{aligned}(\bar{f} \circ \otimes)(v, w) &= \bar{f}(\otimes(v, w)) \\ &= \bar{f}(v \otimes w) \text{ por notación de } \otimes \\ &= \bar{f}[(v, w)] \\ &= g(v, w) \text{ por diagrama (1.1)} \\ &= f(v, w), \forall v \in V, \forall w \in W.\end{aligned}$$

□

Afirmación 1.3. La función $\tilde{f}$ es la única que hace conmutar el diagrama (1.1).

Demostración. Supongamos que existe $h : V \otimes W \to U$ tal que conmuta el diagrama siguiente.



Sea $z \in V \otimes W = R/S$, luego $z = [r]$ con $r \in R$ pero R es el espacio vectorial complejo con base $\{(v, w)|v \in V, w \in W\}$, $\sigma(v_1, w) + \mu(v_1^{'}, w^{'}) + \delta(v^{''}, w^{''}) \in \mathbb{R}$, así $r = \sigma_1(v_1, w) + \cdots + \sigma_k(v_k, w_k)$. Entonces $z = [\sigma_1(v_1, w_1) + \cdots + \sigma_k(v_k, w_k)] = \sigma_1(v_1 \otimes w_1) + \cdots + \sigma_k(v_k \otimes w_k)$.

Lo cual tenemos

$$\begin{aligned}
h(z) &= h(\sigma_1(v_1 \otimes w_1) + \cdots + \sigma_k(v_k \otimes w_k)) \\
&= \sigma_1 h(v_1 \otimes w_1) + \cdots + \sigma_k h(v_k \otimes w_k) \quad \text{pues } h \text{ es lineal} \\
&= \sigma_1 f(v_1, w_1) + \cdots + \sigma_k f(v_k, w_k)) \quad \text{pues } h \text{ conmuta} \\
&= \sigma_1 \widetilde{f}(v_1 \otimes w_1) + \cdots + \sigma_k \widetilde{f}(v_k \otimes w_k) \quad \text{pues } \widetilde{f} \text{ conmuta el diagrama(1.1)} \\
&= \widetilde{f}(\sigma_1 v_1 \otimes w_1) + \cdots + \widetilde{f}(\sigma_k v_k \otimes w_k) \quad \text{pues } \widetilde{f} \text{ es lineal} \\
&= \widetilde{f}(z).
\end{aligned}$$

Por lo tanto $h(z) = \widetilde{f}(z)$, para todo z en $V \otimes W$, lo cual es único.

Dados $V, W \in Vect_{\mathbb{C}}$ existe $W \otimes W \in Vect_{\mathbb{C}}$ y $\otimes : V \times W \to V \otimes W$ bilineal tales que resuelven el siguiente problema universal. Dado $u \in Vect_{\mathbb{C}}$ y $f : v \times w \to u$ bilineal. □

Observación El producto tensorial abstracto de la propiedad universal, se puede "realizar" (concretar) con el *producto de Kronecker de matrices.*

Definición 1.3. Sean $A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$ matriz $m \times n$ y B otra matriz, se define el producto de Kronecker de A con B como: $A \otimes_K B = \begin{pmatrix} a_{11}B & a_{12}B \dots a_{1m}B \\ \vdots & \\ a_{n1}B & a_{n2}B \dots a_{nm}B \end{pmatrix}$.

Ejemplo 1.3. Con las matrices $\begin{pmatrix} 4 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} -1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} -4 & 8 \\ 8 & 16 \\ -2 & 4 \\ 4 & 8 \end{pmatrix}$ y para las matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}$.

Proposición 1.2. Si $|\varphi_1\rangle$,$|\varphi_2\rangle \in \mathbb{C}^n$ y $|\psi_1\rangle$,$|\psi_2\rangle \in \mathbb{C}^n$, entonces

1. $(|\varphi_1\rangle \otimes |\psi_1\rangle)^* = \langle\varphi_1| \otimes |\psi_1\rangle$
2. $(|\varphi_2\rangle \otimes |\psi_2\rangle) \cdot (|\varphi_1\rangle \otimes |\psi_1\rangle) = \langle\varphi_2|\varphi_1\rangle\langle\psi_2|\psi_1\rangle$

Realizamos el tensor $\otimes$ como producto de Kronecker, para demostrar la proposición.

Demostración. Sea $|\varphi_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, $|\varphi_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$, $|\psi_1\rangle = \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix}$, $|\psi_2\rangle = \begin{pmatrix} d_1 \\ \vdots \\ d_t \end{pmatrix}$

Tenemos

1.

$$
\begin{aligned}
[|\varphi_1\rangle \otimes |\psi_1\rangle]^* &= \left[\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} \right]^* \\
&= \begin{pmatrix} a_1c_1 \\ \vdots \\ a_1c_s \\ \vdots \\ a_nc_1 \\ \vdots \\ a_nc_s \end{pmatrix} \\
&= (a_1^*c_1^*, \ldots, a_1^*c_s^*, \ldots, a_n^*c_1^*, \ldots, a_n^*c_s^*) \\
&= (a_1^*, \ldots, a_n^*) \otimes (c_1^*, \ldots, c_s^*) \\
&= |\varphi_1\rangle^* \otimes |\psi_1\rangle^* \\
&= \langle\varphi_1| \otimes \langle\psi_1|.
\end{aligned}
$$

Por lo tanto $(|\varphi_1\rangle \otimes |\psi_1\rangle)^* = \langle\varphi_1| \otimes |\psi_1\rangle$.

2. Tenemos que el producto de tensores

$$
\begin{aligned}
(|\varphi_2\rangle \otimes |\psi_2\rangle) \cdot (|\varphi_1\rangle \otimes |\psi_1\rangle) &= \left[\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \otimes \begin{pmatrix} d_1 \\ \vdots \\ d_t \end{pmatrix} \right] \cdot \left[\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} \right] \\
&= \begin{pmatrix} b_1 d_1 \\ \vdots \\ b_1 d_t \\ \vdots \\ b_m d_1 \\ \vdots \\ b_m d_t \end{pmatrix} \cdot \begin{pmatrix} a_1 c_1 \\ \vdots \\ a_1 c_s \\ \vdots \\ a_n c_1 \\ \vdots \\ a_n c_s \end{pmatrix} \\
&= (b_1 d_1)^* a_1 c_1 + \cdots + (b_1 d_t)^* a_1 c_s + \cdots + \\
&(b_m d_1)^* a_n c_1 + \cdots + (b_m d_t)^* a_n c_s \\
&= b_1^* a_1 (d_1^* c_1 + \cdots + d_t c_s) \\
&+ \cdots + b_m^* a_n (d_1 c_1 + \cdots + d_t c_s) \\
&= (b_1^* a_1 + \cdots + b_m^* a_n)(d^* c_1 + \cdots + d_t^* c_s) \\
&= (b_1^*, \ldots, b_m^*) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} (d_1^*, \ldots, d_t^*) \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} \\
&= \langle \varphi_2 | \varphi_1 \rangle \langle \psi_1 | \psi_2 \rangle
\end{aligned}
$$

□

Observación 1.5. Si z_1,$z_2 \in \mathbb{C}$ entonces su producto de Kronecker es $z_1 \otimes z_2 = z_1 z_2$.

Notación: los ket se pueden expresar de la siguiente manera: $|00\rangle := |0\rangle \otimes |0\rangle$, $|01\rangle := |0\rangle \otimes |1\rangle$, $|000\rangle := |0\rangle \otimes |0\rangle \otimes |0\rangle$, etc.

Capítulo 2

Algoritmo de Deutsch

El algoritmo de Deutsch es un algoritmo cuántico, el cual fue uno de los primeros algoritmos diseñados para ejecutar sobre un computador cuántico y que tiene el potencial de ser más eficiente que los algoritmos clásicos.

El propósito del algoritmo de Deutsch es resolver el siguiente problema.

Problema 2.1. Sea $B = \{0, 1\}$, $f : B \longrightarrow B$ una función. Determinar si f es constante ó no, con solo una evaluación de f [2].

El algoritmo de Deutsch ayudará a saber si una función de un qubit es una función constante o una función balanceada, tal hace uso de los siguientes elementos.

2.1 Compuerta cuántica

Una *compuerta cuántica*[6] es un dispositivo capaz de realizar operaciones unitarias sobre los qubits (Deutch, 1985,1989). En mecánica cuántica, podemos actuar sobre un estado $|\psi\rangle$ con una transformación unitaria $\tilde{U}$. Algunas de las compuertas más importantes son: Hadamard(W), Pauli-X(X), Pauli(Y), Pauli(Z):

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

El primer paso es denotar un operador unitario U_f que actúe sobre dos qubits. Sea la trasformación : $U_f : \mathbb{C}^2 \otimes \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$.

Es fácil hacer ver que $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$ es base de $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Ejemplo 2.1. El producto tensorial de los vectores : $|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ y $|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ están en $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Basta definir U_f en esta base.

$$U_f(|i\rangle \otimes |j\rangle) = |i\rangle \otimes |j \oplus f(i)\rangle \quad i, j = 0, 1 \tag{2.1}$$

donde $\oplus$ es la suma módulo 2.

Ejemplo 2.2. Tenemos que la suma módulo 2:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Lema 2.1. La matriz U_f es matriz unitaria.

Teorema 2.1. Sea A una matriz $n \times n$ compleja. Entonces A es unitario si y sólo si A manda una base ortonormal en base ortonormal.

Afirmación 2.1. Sea $B = \{|i\rangle \otimes |j \oplus f(i)\rangle \mid j, i = 0, 1\}$. Entonces el conjunto B es la base canónica de $\mathbb{C}^4$.

Demostración. El conjunto B está formado por:

$$|0\rangle \otimes |0 \oplus f(0)\rangle = |0\rangle \otimes |f(0)\rangle,$$
$$|0\rangle \otimes |1 \oplus f(0)\rangle = |0\rangle \otimes |\neg f(0)\rangle,$$
$$|1\rangle \otimes |0 \oplus f(1)\rangle = |1\rangle \otimes |f(1)\rangle \quad \text{y}$$
$$|1\rangle \otimes |1 \oplus f(1)\rangle = |1\rangle \otimes |\neg f(1)\rangle.$$

Tenemos varios casos:

$$a) f(0) = 0 \quad \text{y} \quad f(1) = 0$$
$$b) f(0) = 0 \quad \text{y} \quad f(1) = 1$$
$$c) f(0) = 1 \quad \text{y} \quad f(1) = 0$$
$$d) f(0) = 1 \quad \text{y} \quad f(1) = 1$$

Caso a) $B = \{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$

Caso b) $B = \{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle\}$

Caso c) $B = \{|0\rangle \otimes |1\rangle, |0\rangle \otimes |0\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$

Caso d) $B = \{|0\rangle \otimes |1\rangle, |0\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle, |1\rangle \otimes |1\rangle\}$.

Luego U_f manda la base canónica de $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$, por consiguiente U_f es matriz unitaria. □

Ejemplo 2.3. Si $f : \{0,1\} \Rightarrow \{0,1\}$, es decir $f(0) = 1 \quad y \quad f(1) = 0$, entonces

$$U_f(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |f(0)\rangle = |0\rangle \otimes |1\rangle,$$
$$U_f(|0\rangle \otimes |1\rangle) = |0\rangle \otimes |1 + f(0)\rangle = |0\rangle \otimes |0\rangle,$$
$$U_f(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |0\rangle = |1\rangle \otimes |0\rangle,$$
$$U_f(|1\rangle \otimes |1\rangle) = |1\rangle \otimes |1 + 0\rangle = |1\rangle \otimes |1\rangle.$$

Luego $U_f(|0\rangle \otimes |0\rangle) = 0(|0\rangle \otimes |0\rangle) + 1(|0\rangle \otimes |1\rangle) + 0(|1\rangle \otimes |0\rangle) + 0(|1\rangle \otimes |1\rangle)$ de forma análoga con las tres bases.

Así tenemos la matriz $U_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Proposición 2.1. Si A,B son matrices cuadradas, entonces $(A \otimes B)^* = A^* \otimes B^*$.

Utilizando el producto de *kronecker* demostraremos la proposición.

Demostración. Sean A y B matrices cuadradas. Realizando el conjugado del producto tensorial, tenemos:

$$\begin{aligned}
(A \otimes B)^* &= \begin{pmatrix} a_{11}B & a_{12} & \cdots & a_{1m}B \\ \vdots & \vdots & & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{pmatrix}^* \\
&= \begin{pmatrix} (a_{11}B)^* & (a_{12}B)^* & \cdots & (a_{1m}B)^* \\ \vdots & \vdots & & \vdots \\ (a_{n1}B)^* & (a_{n2}B)^* & \cdots & (a_{nm}B)^* \end{pmatrix} \\
&= \begin{pmatrix} a_{11}^*B^* & a_{12}^*B^* & \cdots & a_{1m}^*B^* \\ \vdots & \vdots & & \vdots \\ a_{n1}^*B^* & a_{n2}B^* & \cdots & a_{nm}^*B^* \end{pmatrix} \\
&= A^* \otimes B^*
\end{aligned}$$

□

Observación 2.1. Para todo $|u\rangle, |v\rangle \in \mathbb{C}^n$, los productos tensoriales $|u\rangle \otimes |v\rangle$ están en $\mathbb{C}^n \otimes \mathbb{C}^n$.

No es cierto, en general que $|w\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$, existe $|u\rangle \in \mathbb{C}^n$ y $|v\rangle \in \mathbb{C}^n$ con $|w\rangle = |u\rangle \otimes |v\rangle$.

Contraejemplo: Uno de los estados *EPR (Einstein- Podolski-Rosen)* es:

$$|w\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Demostración. Sea $|w\rangle \neq |v\rangle \otimes |u\rangle$ para todo $|v\rangle$ y $|u\rangle$ en $\mathbb{C}^2$, en caso contrario si $|w\rangle = |v\rangle \otimes |u\rangle$, entonces $|v\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, es decir $|v\rangle = a|0\rangle + b|1\rangle$, similarmente $|u\rangle = c|0\rangle + d|1\rangle$.

Sustituyendo los valores de $|v\rangle$ y $|u\rangle$, tenemos:

$$\begin{aligned} |w\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac(|0\rangle \otimes |0\rangle) + ad(|0\rangle \otimes |1\rangle) + bc(|1\rangle \otimes |0\rangle) + bd(|1\rangle \otimes |1\rangle) \\ &= ac \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + ad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + bc \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + bd \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \end{aligned}$$

por lo cual $|w\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$

$$\begin{aligned} &= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \\ &\Rightarrow ac = \frac{1}{\sqrt{2}} \Rightarrow dac = \frac{d}{\sqrt{2}} \\ &\Leftrightarrow ad = 0, bc = 0, bd = \frac{1}{\sqrt{2}} \Rightarrow 0 = \frac{1}{\sqrt{2}}. \end{aligned}$$

Por lo tanto es una contradicción. □

2.2 Entrelazamiento cuántico

Una propiedad responsable de la potencia de los métodos del cálculo cuánticos es el *entrelazamiento*. El entrelazamiento es un recurso aprovechado en los métodos de búsqueda.

Definición 2.1. Un estado en un espacio de Hibert H se encuentra entrelazado si no puede ser escrito como un producto tensorial de sus estados.

En general, si $|w\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ y $|w\rangle$ no puede ser escrito como como $|w\rangle = |u\rangle \otimes |v\rangle$ se llama vector *Enredado (Entrelazado)* [1].

Ejemplo 2.4. El ket $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$ es un estado entrelazado; además $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |1\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle$, $|\beta_{10}\rangle = \frac{1}{\sqrt{0}}|0\rangle \otimes |0\rangle - \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$ y $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |1\rangle - \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle$, también son estados entrelazado.

Afirmación 2.2. La matriz U es unitaria si y sólo si:

1. $U^* = U^{-1} \Leftrightarrow$
2. $UU^* = Id = U^*U \Leftrightarrow$
3. U preserva norma $\Leftrightarrow U$ preserva producto punto.

Teorema 2.2. Si U y W son matrices unitarias entonces también lo es $U \otimes W$.

Demostración. Tenemos que, $(U \otimes W)(U \otimes W)^* = (U \otimes W)(U^* \otimes W^*) = (UU^{-1}) \otimes (WW^{-1}) = Id \otimes Id = Id$, por consiguiente $U \otimes W$ es unitario. □

Teorema 2.3. Si $M_1, \ldots, M_m$ son matrices de medición, entonces también lo son $M_1 \otimes Id, \ldots, M_m \otimes Id$ y $Id \otimes M_1, \ldots, Id \otimes M_m$.

Demostración.

Tenemos que $M_1^* M_1 + \cdots + M_m^* M_m = Id$ luego

$$\begin{aligned}
&(M_1 \otimes Id)^*(M_1 \otimes Id) + \cdots + (M_m \otimes Id)^*(M_m \otimes Id) \\
&= (M_1^* \otimes Id^*)(M_1 \otimes Id) + \cdots + (M_m^* \otimes Id^*)(M_m \otimes Id) \\
&= (M_1^* M_1 \otimes Id) + \cdots + (M_m M_m \otimes Id) \\
&= (M_1^* M_1 + \cdots + M_m^* M_m) \otimes Id) \\
&= Id \otimes Id \\
&= Id,
\end{aligned}$$

y por último

$$\begin{aligned}
&(Id \otimes M_1)^*(Id \otimes M_1) + \cdots + (Id \otimes M_m)^*(Id \otimes M_m) \\
&= (Id^* \otimes M_1^*)(Id \otimes M_1) + \cdots + (Id^* \otimes M_m)^*(Id \otimes M_m) \\
&= (Id \otimes M_1^* M_1) + \cdots + (Id \otimes M_m^* M_m) \\
&= (M_1^* M_1 + \cdots + M_m^* M_m) \otimes Id \\
&= Id \otimes Id \\
&= Id
\end{aligned}$$

□

Definición 2.2. Si $M_1, \ldots, M_m$ son matrices de medición actuando sobre $\mathbb{C}^n$ y se considera ademas el sistema compuesto $\mathbb{C}^n \otimes \mathbb{C}^m$, se dice que se observa (se mide) el primer sistema $\mathbb{C}^n$. Cuando se usan las matrices de medición $M_1 \otimes Id, \ldots, M_m \otimes Id$, similarmente se dice que se observa (mide) el segundo sistema cuando se usan $Id \otimes M_1, \ldots, Id \otimes M_m$ ($M_1, \ldots, M_m$ actuando sobre $\mathbb{C}^m$).

Definición 2.3. Consideremos $\mathbb{C}^n$, se dice que mide con respecto a la base del cálculo, cuando se usan las matrices:

$$P_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \ldots, P_n = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

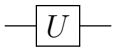
Observación 2.2. Un espacio(de estados) muy usual es del tipo $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$.

Donde se dice que se mide el primer qubit para indicar medición con respecto a la base del cálculo en el primer sistema. Esto es, se usan las siguientes matrices de medición $P_1 \otimes Id \otimes \cdots \otimes Id$ y $P_2 \otimes Id \otimes \cdots \otimes Id$, donde $P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, P_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

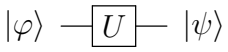
Similarmente, para observar el segundo qubit se usa $Id \otimes P_1 \otimes Id \otimes \cdots \otimes Id$, $Id \otimes P_2 \otimes Id \otimes \cdots \otimes Id$, etc.

También en $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, medir el qubit mas significativo, significa medir el primer qubit. El menos significativo, significa usar el $n-$ésimo qubit.

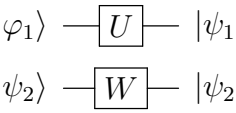
Observación 2.3. Si U es matriz unitaria, ésta se acostumbra dibujar como un circuito:



y la evolución por esta se dibuja:

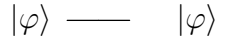


Ademas, si W es una segunda matriz unitaria, el producto tensorial $U \otimes W$ se representa por:



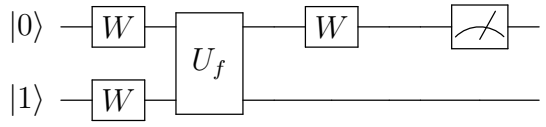
donde $(U \otimes W)(|\varphi_1\rangle \otimes |\varphi_2\rangle) = |\psi\rangle$ es decir $U|\varphi_1\rangle \otimes W|\varphi_2\rangle = |\psi_1\rangle$.

La matriz identidad Id se representa como:



Con todos los elementos anteriores presentamos, el algoritmo de Deutsch.

La solución del problema 2.1, tiene el siguiente diagrama:



Tiene como entrada los $|0\rangle$ y $|1\rangle$, donde se mide el qubit mas significativo.

El algoritmo de Deutsch (D.Deutsch [2]1985) utiliza los resultados anteriores para explotar el que un estado se encuentre en una superposición para obtener información sobre la propiedad global de una función.

El algoritmo de Deutsch, queda de la siguiente manera, en la cual vamos analizar paso a paso.

Algoritmo 2.1 Algoritmo de Deutsch

Entrada: $\{0, 1\}$
Salida: f es constante o no.
1: Se prepara el sistema compuesto: $|\psi_0\rangle = |0\rangle \otimes |1\rangle$
2: Se aplica la matriz $W^{\otimes n} \otimes Id$ al estado anterior. $|\psi_1\rangle = (W \otimes W)|\psi_0\rangle$
3: Se aplica U_f al estado anterior. $|\psi_2\rangle = U_f|\psi_1\rangle$
4: Se aplica $(W \otimes Id)$ al estado anterior. $|\psi_3\rangle = (W \otimes Id)|\psi_2\rangle$
5: Se observa el sistema.

Descripción del algoritmo de Deutsch

En el primer paso, utilizando el axioma (1.1).

Tenemos que $|\psi_0\rangle = |0\rangle \otimes |1\rangle$ estado de preparación el cual es un estado válido pues es unitario. Sea

$$\begin{aligned}
\langle\psi_0|\psi_0\rangle &= (|0\rangle \otimes |1\rangle)^*(|0\rangle \otimes |1\rangle) \\
&= (|0\rangle^* \otimes |1\rangle^*)(|0\rangle \otimes |1\rangle) \\
&= (\langle 0| \otimes \langle 1|)(|0\rangle \otimes |1\rangle) \\
&= \langle 0|0\rangle \otimes \langle 1|1\rangle \\
&= \langle 0|0\rangle\langle 1|1\rangle \\
&= 1 \cdot 1 \\
&= 1
\end{aligned}$$

Se aplica la matriz $W^{\otimes n} \otimes Id$ al estado anterior.

Sea

$$\begin{aligned}
|\psi_1\rangle &= (W \otimes W)|\psi_0\rangle \\
&= (W \otimes W)(|0\rangle \otimes |1\rangle) \\
&= (W|0\rangle) \otimes (W|1\rangle) \quad \text{por la propiedad universal} \\
&= (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) \quad \text{por definición de } W \\
&= \frac{1}{2}|0\rangle \otimes |0\rangle - \frac{1}{2}|0\rangle \otimes |1\rangle + \frac{1}{2}|1\rangle \otimes |0\rangle - \frac{1}{2}|1\rangle \otimes |1\rangle
\end{aligned}$$

En el paso tres aplicamos el axioma (1.2), por bilinealidad de $\otimes$ tenemos:

$$\begin{aligned}
|\psi_2\rangle &= U_f|\psi_1\rangle \\
&= U_f(\frac{1}{2}|0\rangle \otimes |0\rangle - \frac{1}{2}|0\rangle \otimes |1\rangle + \frac{1}{2}|1\rangle \otimes |0\rangle - \frac{1}{2}|1\rangle \otimes |1\rangle) \\
&= \frac{1}{2}U_f(|0\rangle \otimes |0\rangle) - \frac{1}{2}U_f(|0\rangle \otimes |1\rangle) + \frac{1}{2}U_f(|1\rangle \otimes |0\rangle) - \frac{1}{2}U_f(|1\rangle \otimes |1\rangle) \\
&= \frac{1}{2}|0\rangle \otimes |f(0)\rangle - \frac{1}{2}|0\rangle \otimes |\neg f(0)\rangle + \frac{1}{2}|1\rangle \otimes |f(1)\rangle - \frac{1}{2}|1\rangle \otimes |\neg f(1)\rangle.
\end{aligned}$$

Ahora, nótese que tenemos dos casos:

i) Si $f(0) = 0$, entonces $|f(0)\rangle - |\neg f(0)\rangle = |0\rangle - |1\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)$.

ii) Si $f(0) = 1$, entonces $|f(0)\rangle - |\neg f(0)\rangle = |1\rangle - |0\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)$

Por consiguiente, en cualquier caso

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

luego

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

Utilizando el axioma (1.3). Se mide en el primer qubit; es decir aplicar matrices de medición $p_1 \otimes Id, p_2 \otimes Id$. Así tenemos que si usamos p_1, el sistema se colapsa a: $|\varphi_c\rangle = \frac{1}{\eta_0}(p_1 \otimes Id)|\psi_3\rangle$, donde $\eta_0 = ||(p_1 \otimes Id)|\psi_3\rangle|| = \sqrt{\langle\psi_3|(p_1 \otimes Id)(p_1 \otimes Id)|\psi_3\rangle}$.

Ahora, si f es constante

$$
\begin{aligned}
|\psi_c\rangle &= \frac{1}{\eta_0}(p_1 \otimes Id)[(-1)^{f(0)}|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}] \\
&= \frac{(-1)^{f(0)}}{\eta_0} p_1 \otimes |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \frac{(-1)^{f(0)}}{\eta_0} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\end{aligned}
$$

donde

$$
\begin{aligned}
\eta_0 &= \sqrt{(-1)^{f(0)}(\langle 0| \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}})(-1)^{f(0)}(\langle 0| \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}})} \\
&= \langle 0|1\rangle \otimes \frac{1}{2}(\langle 0|0\rangle - \langle 0|1\rangle - \langle 1|0\rangle + \langle 1|1\rangle) \\
&= \sqrt{1 \otimes 1} \\
&= 1.
\end{aligned}
$$

Por lo tanto $|\psi_c\rangle = (-1)^{f(0)}|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ y f constante con probabilidad $\eta_0 = \langle\psi_3|(p_1 \otimes Id)^*(p_1 \otimes Id)|\psi_3\rangle = 1$. Si se usa p_1 y f es constante, el sistema se colapsa

a: $(-1)^{f(0)}(\langle 0| \otimes \frac{\langle 0|-|1\rangle}{\sqrt{2}})$ con probabilidad 1. Mientras que si se usa $p_2 \otimes Id$ y f constante, el sistema se colapsa a $\frac{1}{\eta_1}(p_2 \otimes Id)|\psi_3\rangle$. Esto resulta porque el uso de p_1 tiene probabilidad uno de ocurrir, mientras el evento relacionado con p_2 tiene probabilidad dada por

$$\begin{aligned} p_2 &= \langle\psi_3|(p_2 \otimes Id)^*(p_2 \otimes Id)|\psi_3\rangle \\ &= \langle\psi_3|(p_1 \otimes Id)(p_2 \otimes Id)|\psi_3\rangle \\ &= \langle\psi_3|p_2 \otimes Id|\psi_3\rangle \\ &= \langle 0|1\rangle\langle 1|0\rangle(\frac{\langle 0| - \langle 1|}{\sqrt{2}})(\frac{|0\rangle - \langle 1|}{\sqrt{2}}) \\ &= 0. \end{aligned}$$

Ahora si f no es constante, entonces $|\psi_3\rangle = (-1)^{f(0)}|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ y para medir se usa $(p_1 \otimes Id)$ o $(p_2 \otimes Id)$ y se procede similarmente que antes, para obtener que se observa $(-1)^{f(0)}|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, con probabilidad 1.

En conlusión: si se observa en el primer qubit el estado final $|1\rangle$ se dice que f no es constante; y si se observa $|0\rangle$, entonces f es constante.

Observación 2.4. La eficiencia de un algoritmo se mide contando el número de *instrucciones elementales* usada, según la teoría de complejidad de los algoritmos. En el algoritmo de Deutsch se usan tres instrucciones mas un llamado a la función, una tarea muy importante en computación es encontrar algoritmos con la mejor complejidad posible.

Capítulo 3

Algoritmo de Deustch-Jozsa

El algoritmo de Deutsch-Jozsa [3] es una generalización del algoritmo de Deutsch (1992). En el problema de Deutsch-Jozsa nos dan una función cuántica (que para nosotros es una caja negra) $f(x_1, x_2, \cdots, x_n)$ que toma n bits de entrada $x_1, x_2, ..., x_n$ y devuelve un valor binario $f(x_1, x_2, \cdots, x_n)$. Sabemos que la función es constante (0 en todas las entradas o 1 en todas las entradas) o balanceada (devuelve 1 para la mitad de las entradas y 0 para la otra mitad); el problema es entonces determinar cómo es la función (constante o balanceada) aplicando entradas a la caja negra y observando su salida. Sea $f : B \times \cdots \times B \longrightarrow B$ función donde $B = \{0, 1\}$ (i.e $f = f(x_1, \ldots, x_n)$ función booleana de aridad n). Supongase ademas que f es una de dos si es constante o balanceada.

Problema 3.1. Cual de estás posibilidades es f con sólo dos llamadas a f (dos "evaluaciones" de f).

3.1 Evaluación balanceada

Definición 3.1. Sea $f : B \times \cdots \times B \longrightarrow B$ con $B = \{0, 1\}$, la función f se llama *balanceada* si $|f^{-1}(0)| = |f^{-1}(1)|$.

Ejemplo 3.1. En la siguiente tabla muestra una función balanceada donde tenemos el mismo número de ceros que de unos en la segunda columna.

x	$\neg f(x)$
0	1
1	0

Ejemplo 3.2. Sea $f(x_1, x_2, x_3) = (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3)$ como observamos en la tabla es balanceada la función.

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

Las funciones booleanas constantes son tautologias o contradicciones.

Una vez más, en este problema se supone que f es una caja negra, uno tiene acceso a la fórmula de la función solo se tiene derecho a hacer evaluación de la función.

El siguiente lema es de gran importancia para nuestro algoritmo de Deustch Jozsa.

Lema 3.1. Sea $|K\rangle$ un elemento de la base del cálculo en $\mathbb{C}^{2n}$ (ie. K es una cadena de longitud n de ceros y unos) entonces

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

donde u se escribe en binario con n bits (u es cadena de longitud n de 0 y 1), con $W^{\otimes n} = \underbrace{W \otimes W \otimes \cdots \otimes W}_{n}$ y $K \cdot Ku = k_1u_1 + \cdots + k_nu_n$ donde a su vez $K = k_1, \ldots, k_n$, $u = u_1, \ldots, u_n$ con k_i,$u_i \in 0, 1$, $i = 1, \ldots, n$.

Demostración. Sea

$$\begin{aligned} W^{\otimes n}|K\rangle &= (\underbrace{W \otimes W \otimes \cdots \otimes W}_{n})|K\rangle \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + (-1)^{k_1}|1\rangle) \otimes (|0\rangle + (-1)^{k_2}|1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{k_n}|1\rangle) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2^n}}(|0\cdots 0\rangle + (-1)^{k_n}|0\cdots 01\rangle + (-1)^{k_{n-1}}|0\cdots 010\rangle + \\
&\qquad + (-1)^{k_{n-1}+k_n}|0\cdots 011\rangle + \\
&(-1)^{k_{n-2}}|0\cdots 0100\rangle + (-1)^{k_{n-2}+k_n}|0\cdots 0101\rangle + \cdots + \\
&(-1)^{k_{n-2}+k_{n-1}}|0\cdots 0110\rangle + (-1)^{k_{n-2}+k_{n-1}+k_n}|0\cdots 0111\rangle + \\
&+ (-1)^{k_1+k_2+\cdots+k_n}|111\cdots 1\rangle) \\
&= \frac{1}{\sqrt{2^n}}((-1)^{k_1\cdots k_n\cdot 0\cdots 0}|0\cdots 0\rangle + (-1)^{k_1\cdots k_n\cdot 0\cdots 01}|0\cdots 01\rangle + \\
&+ (-1)^{k_1\cdots k_n\cdot 0\cdots 010}|0\cdots 010\rangle + (-1)^{k_1\cdots k_n\cdot 0\cdots 011}|0\cdots 011\rangle + \\
&+ \cdots + (-1)^{k_1\cdots k_n\cdot 11\cdots 1}\underbrace{|1\cdots 11\rangle}_{2^n-1} \\
&= \frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{K\cdot u}|u\rangle
\end{aligned}
$$

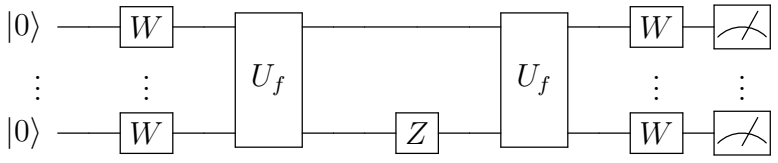
□

Definición 3.2. Para el algoritmo de Deutsch Jozsa utilizamos la matriz de *Pauli*, la matriz $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ lo cual a Z marca a $|1\rangle$ con cambio de fase -1; es decir $Z|0\rangle = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$ y $Z|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Consideremos la compuerta U_f de dos qubits que definimos en el algoritmo de Deutsch (2.1): $U_f(|i\rangle \otimes |j\rangle) = |i\rangle \otimes |j \oplus f(i)\rangle \quad i, j = 0, 1.$

En el algoritmo de Deutsch Jozsa, la compuerta U_f esta compuesto de $n+1$ qubits. Si $k_1 \cdots k_n \in \{0, 1\}$, entonces se define $U_f|k_1 \cdots k_n k_{n+1}\rangle = |k_1 \cdots k_n\rangle \otimes |f(k_1 \cdots k_n) \oplus k_{n+1}\rangle$ que es un elemento de la base del cálculo.

El algoritmo de Deutsch Jozsa tiene el siguiente circuito:



Para obtener la solución del problema de Deutsch-Jozsa, aplicamos el siguiente procedimiento.

Algoritmo 3.1 Algoritmo de Deutsch Jozsa

Entrada: La funcion $f(x_1, x_2, \cdots, x_n)$
Salida: Si el vector es igual a $\underbrace{|0, \ldots, 0\rangle}_{n}$ entonces f es balanceada, en otro caso un vector diferente de $|0, \ldots, 0\rangle$ no es balanceada.

1: Se prepara el sistema con estado inicial:

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

2: Se aplica la matriz $W^{\otimes n} \otimes Id$ al estado anterior.

$$\begin{aligned} |\psi_1\rangle &= (W^{\otimes n} \otimes Id)|\psi_0\rangle \\ &= (W^{\otimes n} \otimes Id)|00 \ldots 0\rangle \\ &= (W^{\otimes n} \otimes |00 \ldots 0\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u0\rangle \end{aligned}$$

3: Se aplica U_f al estado anterior.

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

4: Se aplica $(Id \otimes \cdots \otimes Id) \otimes Z$ al estado anterior.

$$|\psi_3\rangle = (\underbrace{Id \otimes \cdots \otimes Id}_{n}) \otimes Z|\psi_2\rangle$$

5: Se aplica U_f al estado anterior.

$$|\psi_4\rangle = U_f|\psi_3\rangle$$

6: Se aplica $W^{\otimes n} \otimes Id$ al estado anterior.

$$|\psi_5\rangle = W^{\otimes n} \otimes Id|\psi_4\rangle$$

7: Se observa el sistema.

Analizando el algoritmo de Deutsch Jozsa tenemos:

En el paso uno, utilizando el axioma (1.2).

Nuestro estado inicial es: $|\psi_0\rangle = |0 \ldots 0\rangle$.

Aplicando $W^{\otimes n} \otimes Id$ a nuestro estado anterior:

$$\begin{aligned}
|\psi_1\rangle &= (W^{\otimes n} \otimes Id)|\psi_0\rangle \\
&= (W^{\otimes n} \otimes Id)|00\ldots0\rangle \\
&= W^{\otimes n} \otimes |00\ldots0\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u0\rangle.
\end{aligned}$$

En el paso tres aplicamos el axioma (1.2) al estado anterior:

$$\begin{aligned}
|\psi_2\rangle &= U_f|\psi_1\rangle \\
&= U_f \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \otimes |f(u)\rangle
\end{aligned}$$

Aplicando los axiomas de la computación cuántica (1.1, 1.2, 1.3), obtenemos los siguientes pasos:

$$\begin{aligned}
|\psi_3\rangle &= ((Id \otimes \cdots \otimes Id) \otimes Z)|\psi_2\rangle \\
&= (Id \otimes \cdots \otimes Id) \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \otimes |f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (Id \otimes \cdots \otimes Id)(|u\rangle \otimes |f(u)\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \otimes Z|f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \otimes (-1)^{f(u)}|f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \otimes (-1)^{f(u)}|u\rangle \otimes |f(u)\rangle \\
|\psi_4\rangle &= U_f|\psi_3\rangle
\end{aligned}$$

$$
\begin{aligned}
&= U_f \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} |u\rangle \otimes |f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} U_f(|u\rangle \otimes |f(u)\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} |u\rangle \otimes |f(u) \oplus f(u)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} (|u\rangle \otimes |0\rangle \\
|\psi_5\rangle &= (W^{\otimes n} \otimes Id)|\psi_4\rangle \\
&= (W^{\otimes n} \otimes Id) \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} (|u\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} (W^{\otimes n} \otimes Id)(|u\rangle \otimes |0\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} W^n (|u\rangle \otimes |0\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{f(u)} \frac{1}{\sqrt{2^n}} \sum_{r=0}^{2^n-1} (-1)^{u \cdot r} |r\rangle \otimes |0\rangle \\
&= \frac{1}{2^n} \sum_{u=0}^{2^n-1} \sum_{r=0}^{2^n-1} (-1)^{f(u)+u \cdot r} |r0\rangle \\
&= \frac{1}{2^n} \sum_{u=0}^{2^n-1} (-1)^{f(u)} |0 \cdots 0\rangle + \frac{1}{2^n} \sum_{u=0}^{2^n-1} \sum_{r=1}^{2^n-1} (-1)^{f(u)+u \cdot r}) |r0\rangle.
\end{aligned}
$$

Luego para f tenemos tres casos:

1. Si $f \equiv 0$, el coeficiente de $\underbrace{|0 \cdots 00\rangle}_{n}$ en $|\psi_5\rangle$ es $|\frac{1}{2^n} 2^n|^2 = 1$, entonces $|0 \cdots 00\rangle$ se observa con probabilidad 1.

2. Si $f \equiv 1$, el coeficiente de $|0 \cdots 00\rangle$ es $\frac{1}{2^n}(-2^n) = -1$ por consiguiente, la probabilidad de observar $|0 \cdots 00\rangle$ es $|-1|^2 = 1$.

3. Si f es balanceada: el coeficiente de $|0 \cdots 00\rangle$ es 0, la probabilidad de observar $|0 \cdots 00\rangle$ es cero.

Por lo tanto si al hacer la medición en el algoritmo de Deutsch Jozsa, se observa $|0\cdots 00\rangle$, entonces se dice que f es balanceada.

En el algoritmo de Deutsch Jozsa se hizo uso de la siguiente proposición.

Proposición 3.1. Si $|0\rangle$,$|1\rangle$,...,$|2^n-1\rangle$ son elementos de la base del cálculo y supongase que el estado $|\psi\rangle = a_0|0\rangle + a_1|1\rangle + \cdots + a_{2^n-1}|2^n-1\rangle$, se observa con respecto a ésta base canónica, que $|\psi\rangle$ se colapsa al éstado $|i\rangle$ con probabilidad $|a_i|^2$, con $i = 0,\ldots,2^n-1$. Aquí $|0\rangle = \underbrace{|0\cdots 0\rangle}_{n}$, $|1\rangle = |0\cdots 01\rangle$,$|2\rangle = |0\cdots 10\rangle$,..., $|2^n\rangle = |1\cdots 1\rangle$.

Demostración. Por definición las matrices de medición que se usan, son las proyecciones canónicas, tales satisfacen la ecuación de completez. Calculemos el colapso y sus probabilidades; por el axioma de medición (1.3), el estado $|0\rangle$ se colapsa a:

$$|\psi_c\rangle = \frac{1}{\|P_0|\psi\rangle\|}P_0|\psi\rangle$$

donde

$$\begin{aligned} P_0|\psi\rangle &= (|0\rangle\langle 0|)|\psi\rangle \\ &= (|0\rangle\langle 0|)(a_0|0\rangle + a_1|1\rangle + \cdots + a_{2^n-1}|2^n-1\rangle) \\ &= a_0|0\rangle\langle 0|0\rangle + a_1|0\rangle\langle 0|1\rangle + \cdots + a_{2^n-1}|0\rangle\langle 0|2^n-1\rangle \\ &= a_0|0\rangle \end{aligned}$$

luego $|\psi_c\rangle = \frac{1}{\|P_0|\psi\rangle\|}P_0|\psi\rangle = \frac{1}{\sqrt{|a_0|^2}}P_0|0\rangle = \frac{a_0}{|a_0|}|0\rangle = e^{i\theta}|0\rangle$, donde $a_0 = |a_0|e^{i\theta}$ es la forma polar del complejo a_0.

Observación 3.1. Si $|\alpha\rangle$ y $|\beta\rangle$ son dos estados tales que $|\alpha\rangle = e^{i\theta}|\beta\rangle$, entonces $|\alpha\rangle$ se dice *equivalente* a $|\beta\rangle$ y $e^{i\theta}$ se llama *fase global*.

Así $|\psi\rangle$ se colapsa a $e^{i\theta}|0\rangle$ que es el estado equivalente a $|0\rangle$, se considera entonces que $|\psi\rangle$ se colapsa a $|0\rangle$ (salvo fase global). La probabilidad de que se de este colapso es $\langle\psi|P_0^*P_0|\psi\rangle = (a_0|0\rangle)^*a_0|0\rangle = a_0\langle 0|a_0|0\rangle = |a_0|^2$, similarmente $|1\rangle, |2\rangle, \ldots, |2^n-1\rangle$. □

Definición 3.3. Los números complejos $a_0, a_1, \ldots, a_{2^n-1}$ en $|\psi\rangle = a_0|0\rangle + a_1|1\rangle + \cdots + a_{2^n-1}|2^n - 1\rangle$ se llama *amplitudes.*

Observación 3.2. Si $|\psi\rangle \in \mathbb{C}^2$ tal que $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, con $a, b \in \mathbb{C}$ lo cual es de norma uno, es decir $\||\psi\rangle\| = \sqrt{|a|^2 + |b|^2} = 1$, por consiguiente $|\psi\rangle = a|0\rangle + b|1\rangle = |a|e^{i\theta}|0\rangle + |b|e^{i\varphi}|1\rangle = e^{i\theta}(|a||0\rangle + |b|e^{i(\varphi-\theta)}|1\rangle)$. Por la identidad de Euler $e^{i\theta} = \cos\theta + i\sin\theta$ y $|e^{i\theta}| = \cos^2\theta + \sin^2\theta = 1$, lo cual podemos escribir $|\psi\rangle \equiv |a||0\rangle + |b|e^{i\alpha}|1\rangle$, con $0 \leq \alpha \leq 2\pi$, donde $\alpha = \varphi - \theta$. Como $|a|^2 + |b|^2 = 1$ se puede escribir $|a| = \cos(\beta/2)$ y $|b| = \sin(\beta/2)$ con $0 \leq \beta \leq \pi$. Despreciando la fase global el nuevo estado equivalente $|\psi\rangle = \cos(\beta/2)|0\rangle + \sin(\beta/2)e^{i\alpha}|1\rangle$.

Capítulo 4

Algoritmo de Teleportación Cuántica

La teleportación es una tecnologia cuántica única que trasfiere un estado cuántico a una localización arbitrariamente alejada usando un estado de entrelazamiento cuántico distribuido y transmisión de cierta información clásica. La teleportación cuántica no transporta energia o materia, ni permite la comunicación de información a velocidad superior a la de la luz, pero es útil en comunicación y computación cuántica.

En la computación tradicional para transmitir bits, estos son clonados o copiados y luego enviados a través de diferentes medios . En computación cuántica no es posible clonar, copiar, o enviar qubits de un lugar a otro como se hacen con los bits.

4.1 No-clonación

El teorema de no-clonación establece que no se puede hacer una copia perfecta de un estado cuántico. Supongamos que tenemos dos registros: $|\psi\rangle$ (que queremos copiar) y $|B\rangle$.

Queremos realizar la transformación $|\psi\rangle \otimes |B\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$, para todo estado $|\psi\rangle$. Supongamos que se cumple $|0\rangle \otimes |B\rangle \rightarrow |0\rangle \otimes |0\rangle$ y $|1\rangle \otimes |B\rangle \rightarrow |1\rangle \otimes |1\rangle$. Se sigue del principio de superposición que un estado general transformará, como $(\alpha|0\rangle + \beta|1\rangle) \otimes |B\rangle \rightarrow \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle$, lo cual no es un par de copias del estado original.

Si enviamos un qubit $|0\rangle$ donde 0 es un estado desconocido, el receptor no podrá leer su estado con certidumbre, cualquier intento de medida podría modificar el estado del qubit, por lo tanto se perdería su estado, imposibilitado su recuperación. La teleportación cuántica, resuelve este problema, esta se basa en el "entrelazamiento cuántico" para poder transmitir un qubit sin necesidad de enviarlo.

Problema 4.1. Se tiene dos partes A (Alicia) y B (Beto) que quieren comunicarse. Alicia tiene acceso a dos canales cuánticos, donde un canal cuántico es un medio que permite qubits, tales canales corresponden dos sistemas compuestos que interfieren entre ellos (producto tensorial). Beto tiene acceso a uno de los canales de Alicia, a otro que sólo él puede usar; uno de los canales de Alicia es para su uso privado, el otro lo comparte con Beto. La computación cuántica permite tener una correlación Alicia con Beto [6].

Para cumplir este objetivo utilizamos las compuertas.

4.2 Compuerta controladas cuántica

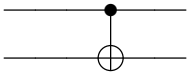
La compuerta Pauli-X es conocida también como la compuerta NOT cuántica, ya que trasforma $|0\rangle \rightarrow |1\rangle$ y $|1\rangle \rightarrow |0\rangle$. Sin embargo, no es una compuerta NOT cuántica universal, ya que no transforma $|\psi\rangle \rightarrow |\psi^{\perp}\rangle$.

Observación 4.1. Si $U : \mathbb{C}^N \rightarrow \mathbb{C}^N$ (U es $N \times N$) es matriz unitaria cualquiera entonces se define la matriz control-U denota $C(U) = \lambda(U)$ como la matriz

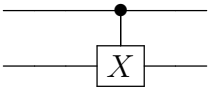
$C(U) = \mathbb{C}^2 \otimes \mathbb{C}^N \to \mathbb{C}^2 \otimes \mathbb{C}^N, |j\rangle$ en la base del calculo de $\mathbb{C}^n$ cualquiera, donde $C(U) = (|0\rangle \otimes |j\rangle) = |0\rangle \otimes |j\rangle$ y $C(U) = (|1\rangle \otimes |j\rangle) = |1\rangle \otimes U|j\rangle$. En este caso $|0\rangle$, $|1\rangle$ se llama qubit de control y $|j\rangle$ qubit controlado.

Ejemplo 4.1. La matriz $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; X : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$, entonces la matriz $C(X) : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$, con $C(X) = (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle = (|1\rangle \otimes |0\rangle) = |1\rangle \otimes X|0\rangle = |1\rangle \otimes |1\rangle$

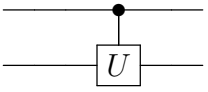
Diagramáticamente $C(X)$ se representan como control NOT:



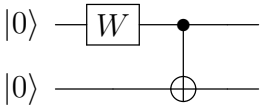
o bien



En general, las compuertas $C(U)$ se representan como:



Observación 4.2. La compuerta control-not $C(X)$ ayuda a construir estados EPR:



Analizando el circuito tenemos:

En el primer paso, utilizando el axioma (1.1): $|\psi_0\rangle = |0\rangle \otimes |0\rangle$.

Se aplica la matriz $W^{\otimes n} \otimes Id$ al estado anterior.

$$\begin{aligned}
|\psi_1\rangle &= (W \otimes Id) \otimes |\psi_0\rangle \\
&= (W \otimes Id) \otimes |0\rangle \\
&= W|0\rangle \otimes |0\rangle \\
&= (\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}) \otimes |0\rangle \\
&= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle
\end{aligned}$$

Aplicando control-not ($C(X)$), al estado anterior.

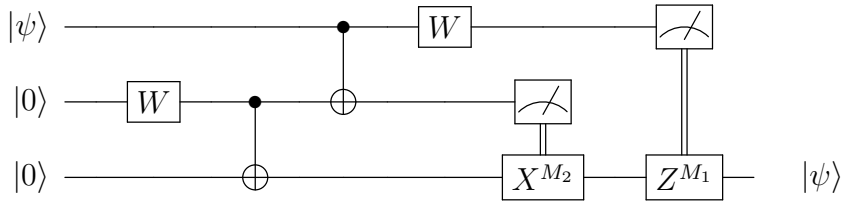
$$\begin{aligned}
|\psi_2\rangle &= C(X)|\psi_1\rangle \\
&= C(X)(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle) \\
&= \frac{1}{\sqrt{2}}C(X)|00\rangle + \frac{1}{\sqrt{2}}C(X)|10\rangle \\
&= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\
&= |B_{00}\rangle.
\end{aligned}$$

Lo cual $|B_{00}\rangle$ es un estado EPR, de forma analoga con los demas estados EPR.

Problema Tenemos que A quiere enviarle un qubit $|\psi\rangle$ a B donde $|\psi\rangle = a|0\rangle + b|1\rangle$, con $a, b \in \mathbb{C}$ y $|a|^2 + |b|^2 = 1$.

Observación 4.3. Alicia no puede enviarle la expresión de $|\psi\rangle$ a B por ejemplo, correo electrónico, pues al observar Alicia a $|\psi\rangle$ lo perturba y este se colapsa a $|0\rangle$ o $|1\rangle$, por el axioma de medición; las amplitudes desaparecen.

Consideremos el siguiente circuito para la solución del problema 4.2



El circuito esta descrito por el algoritmo de teleportación cuántica.

Algoritmo 4.1 Algoritmo de teleportacion cuántica

Entrada: Alicia tiene un $|\psi\rangle$
Salida: Beto tiene el $|\psi\rangle$

1: Se prepara el sistema con estado inicial:

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

2: Se aplica $(Id \otimes C(X))(Id \otimes W \otimes Id)$ al estado anterior.

$$(Id \otimes C(X))(Id \otimes W \otimes Id)|\psi_0\rangle$$

3: Se aplica $(W \otimes Id \otimes Id)(C(X) \otimes Id)$ al estado anterior.

$$|\psi_2\rangle = (W \otimes Id \otimes Id)(C(X) \otimes Id)|\psi_1\rangle$$

4: Se observa el sistema.

Analizando el algoritmo de teleportación tenemos:

1. Alicia coloca (sin observar) a $|\psi\rangle$ en su canal cuántico y al mismo tiempo Beto coloca a $|0\rangle$ en el canal compartido y $|0\rangle$ en su canal cuántico privado, en un sistema compuesto con el canal de Alicia. Para obtener $|\psi_0\rangle = |\psi\rangle \otimes |00\rangle$ y $|\psi_0\rangle = |\psi\rangle \otimes |0\rangle \otimes |0\rangle$

2. Beto aplica W al canal compartido y aplica una compuerta ($NOT(control - not) = C(X)$) el qubit compartido y a su qubit privado, por consiguiente:

$$
\begin{aligned}
|\psi_1\rangle &= (Id \otimes C(X))(Id \otimes w \otimes Id)|\psi_0\rangle \\
&= (Id \otimes C(X))(Id \otimes w \otimes Id)(|\psi\rangle \otimes |0\rangle \otimes |0\rangle) \\
&= (Id \otimes C(X))(|\psi\rangle \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes |0\rangle) \\
&= (Id \otimes C(X))(\frac{1}{\sqrt{2}}|\psi\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|\psi\rangle \otimes |1\rangle \otimes |0\rangle) \\
&= \frac{1}{\sqrt{2}}(Id \otimes C(X))(|\psi\rangle \otimes |00\rangle) + \frac{1}{\sqrt{2}}(Id \otimes C(X))(|\psi\rangle \otimes |0\rangle) \\
&= \frac{1}{\sqrt{2}}|\psi\rangle \otimes |00\rangle + \frac{1}{\sqrt{2}}|\psi\rangle|11\rangle.
\end{aligned}
$$

3. Alicia aplica una control-not, con qubit de control en su canal privado, entre su canal y el compartido con B y luego aplica W a su canal privado.

$$
\begin{aligned}
|\psi_2\rangle &= (W \otimes Id \otimes Id)(C(X) \otimes Id)(\frac{1}{\sqrt{2}}|\psi\rangle \otimes |00\rangle + \frac{1}{\sqrt{2}}|\psi\rangle \otimes |11\rangle) \\
&\text{(ponemos } |\psi\rangle = a|0\rangle + b|1\rangle) \\
&= (W \otimes Id \otimes Id)(C(X) \otimes Id)(\frac{a}{\sqrt{2}}|000\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|111\rangle) \\
&= (W \otimes Id \otimes Id)(\frac{a}{\sqrt{2}}|000\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|101\rangle) \\
&= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{2}|100\rangle + \frac{b}{2}|010\rangle - \frac{b}{2}|110\rangle + \frac{a}{2}|011\rangle + \frac{a}{2}|111\rangle + \frac{b}{2}|001\rangle \\
&- \frac{b}{2}|101\rangle \\
&= (\frac{|00\rangle}{2}(a|0\rangle + b|1\rangle) + \frac{|10\rangle}{2}(a|0\rangle - b|1\rangle) + \frac{|01\rangle}{2}(a|1\rangle + b|0\rangle + \frac{|11\rangle}{2}) \\
&(-\frac{b}{2}|0\rangle + \frac{a}{2}|1\rangle)
\end{aligned}
$$

4. Beto observa el canal compartido y Alicia observa su canal privado (ambas mediciones con respecto a la base canónica). Sea $|M_2\rangle$ el estado observado por Beto, y $|M_1^2\rangle$. Nótese que $M_1 = 0$ ó 1, $M_2 = 0$ ó 1.

5. Alicia le comunica M_1 a Beto, por un medio clásico (correo,teléfono,etc.) Beto aplica X^{M_2} en su canal privado y luego aplica Z^{M_1} a éste mismo canal.

Beto , después obtiene $|\psi\rangle$ en su canal privado.

Observe que en canal privado de Beto no se hace ninguna observación, lo que previene cualquier colapso, en este canal.

Caso a) En el canal (qubit privado Beto está $a|0\rangle + b|1\rangle$) al cual se le aplica $X^0 = Id$ y luego $Z^0 = Id$. Finalmente, Beto obtiene $|\psi\rangle$ en su canal.

Caso b) En el qubit privado de Beto está $a|1\rangle + b|0\rangle$ al cual Beto le aplica para obtener $a|0\rangle + b|1\rangle$, por lo que $X^{'} = X(X|0\rangle = 1,\ X|1\rangle = |0\rangle)$. Luego Beto le aplica $Z^0 = Id$ para finalmente obtener $|\psi\rangle = a|0\rangle + b|1\rangle$ en su canal privado.

Alicia observa	Beto observa
$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

caso c) En el qubit privado de Beto está $a|0\rangle - b|1\rangle$. A este Beto le aplica $X^0 = Id$ para $a|0\rangle - b|1\rangle$ y luego le aplica $Z^1 = Z\ Z|0\rangle = |0\rangle, Z|1\rangle = -1$ y obtiene $a|0\rangle + b|1\rangle = |\psi\rangle$.

Caso d) En el qubit privado de Beto está $-b|0\rangle + a|1\rangle$, Beto le aplica $X^{'} = X = -b|1\rangle + a|0\rangle$. luego Beto le aplica $Z^{'} = Z$ para finalmente obtener $|\psi\rangle = b|1\rangle + a|0\rangle = a|0\rangle + b|1\rangle$.

Como podemos notar Alicia tiene $|\psi\rangle$ que al final lo tiene Beto.

Capítulo 5

Algoritmo de Grover

Otra aplicación de la potencia de la mecánica cuántica en la resolución de problemas computacionalmente, en búsqueda de elementos en listas.

Problema 5.1. Sea $f(x_1, \ldots, x_n)$ función booleana tal que f es satis factible sólo para una asignación de las variables [5]. Es decir:

$$f(x_1, \ldots, x_n) = 1 \Leftrightarrow x_1 = b_2, x_2 = b_2, \ldots, x_n = b_n$$

donde $(b_1, \ldots, b_n)$ son valores booleanos fijos o equivalentes $|f^{-1}(1)| = 1$.

El problema es encontrar la asignación $(b_1, \ldots, b_n)$ que satisface a f. En la siguiente tabla mostramos la asignacion de $(b_1, \ldots, b_n)$ en la cual es marcada con 1

x_1	x_2	$\cdots$	x_n	$f(x_1, x_2, \ldots, x_n)$
0	0	$\cdots$	1	0
0	0	$\cdots$	1	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_1	b_2	$\cdots$	b_n	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\cdots$	1	0

Observación 5.1. La mejor estrategia conocida, clasicamente es hacer una búsqueda exhaustiva, que usa $\frac{2^n}{2}$ evaluación de f (en promedio), se puede hacer una búsqueda exhaustiva cuántica, que usa $\sqrt{2^n} = 2^{\frac{n}{2}}$ evaluaciones de f, cuánticamente aproximada, en la cual obtiene una ganancia cuadrática.

Ejemplo 5.1. Si la base de datos tiene $10,000$ registros, resolver la búsqueda clásicamente va a usar $5,000$ evaluaciones de f, pero cuánticamente se usa sólo 100 evaluaciones de f.

Observación 5.2. Sea $f(x_1, \ldots, x_n)$ función booleana de orden n, esta función se puede realizar cuánticamente como una matriz unitaria U_f.

De la forma siguiente definimos, una trasformación lineal: $U_f : \mathbb{C}^{2^n} \otimes \mathbb{C}^2 \to \mathbb{C}^{2^n} \otimes \mathbb{C}^2$, mediante la siguiente:

$$U_f(|x_1 \cdots x_n\rangle \otimes |y\rangle) = |x_1 \cdots x_n\rangle \otimes |f(x_1, \ldots, x_n)\rangle \oplus |y\rangle$$

donde y es 0 ó 1 y cada x_i, $i = 1, \ldots, n$ es también 0 ó 1 es decir $|x_1 \cdots x_n y\rangle$, $x_i = 0{,}1$, $y = 0$, 1 es la base canónica de $\mathbb{C}^{2^{n+1}}$.

El siguiente teorema es de gran utilidad para poder resolver el problema.

Teorema 5.1. Sea $Q = W^{\otimes n} U_0 W^{\otimes n} U_f$ donde $U_f|x\rangle = (-1)^{f(x)}|x\rangle$ y

$$U_0|x\rangle = \begin{cases} -|x\rangle & \text{si} \quad x = 0 \cdots 0 \\ |x\rangle & \text{otro caso} \end{cases}$$

para todo x en la base del calculo de $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$. Además, sea $|b\rangle = \frac{1}{\sqrt{2^n}}|b_1, \ldots, b_n\rangle$ donde $f^{-1}(1) = (b_1, \cdots b_n)$ y $|m\rangle = \frac{1}{\sqrt{2^n}} \sum_{|u\rangle \neq |b\rangle} |u\rangle$ (u en la base del cálculo de pertenece a la base canónica de $\mathbb{C}^2$) entonces

$$Q|b\rangle = (\frac{2}{2^{n-1}} - 1)|b\rangle + \frac{1}{2^{n-1}}|m\rangle \tag{5.1}$$

$$Q|m\rangle = 2(\frac{1}{2^n} - 1)|b\rangle + (\frac{2}{2^n} - 1)|m\rangle. \tag{5.2}$$

Demostración. Por hipótesis tenemos que $Q = W^{\otimes n}U_0W^{\otimes n}U_f$, por consiguiente:

$$
\begin{aligned}
Q|b\rangle &= W^{\otimes n}U_0W^{\otimes n}U_f|b\rangle \\
&= W^{\otimes n}U_0W^{\otimes n}U_f\frac{1}{\sqrt{2^n}}|b_1,\ldots,b_n\rangle \\
&= \frac{1}{\sqrt{2^n}}W^{\otimes n}U_0W^{\otimes n}(-1)^{f(b_1,\ldots,b_n)}|b_1,\ldots,b_n\rangle \\
&= -\frac{1}{\sqrt{2^n}}W^{\otimes n}U_0W^{\otimes n}|b_1,\ldots,b_n\rangle \\
&= -\frac{1}{\sqrt{2^n}}W^{\otimes n}U_0\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}|u\rangle \\
&= -\frac{1}{2^n}\sum_{u=0}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}W^{\otimes n}U_0|u\rangle \\
&= -\frac{1}{2^n}\sum_{u=1}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}W^{\otimes n}|u\rangle + (\frac{1}{2^n}W^{\otimes n}|0\rangle) \\
&= -\frac{1}{2^n}\sum_{u=1}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}W^{\otimes n}|u\rangle - \frac{1}{2^n}W^{\otimes n}|0\rangle + (\frac{1}{2^n}W^{\otimes n}|0\rangle) + \frac{1}{2^n}W^{\otimes n}|0\rangle \\
&= -\frac{1}{2^n}\sum_{u=0}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}W^{\otimes n}|u\rangle + \frac{1}{2^{n-1}}W^{\otimes n}|0\rangle \\
&= -\frac{1}{2^n}W^{\otimes n}[\sum_{u=0}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}|u\rangle] + \frac{1}{2^{n-1}}W^{\otimes n}|0\rangle \\
&= -\frac{1}{\sqrt{2^n}}W^{\otimes n}[\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}(-1)^{(b_1,\ldots,b_n)\cdot u}|u\rangle] + \frac{1}{2^{n-1}}W^{\otimes n}|0\rangle \\
&= -\frac{1}{\sqrt{2^n}}W^{\otimes n}W^{\otimes n}|b_1,\ldots,b_n\rangle + \frac{1}{2^{n-1}}W^{\otimes n}|0\rangle \\
&= -\frac{1}{\sqrt{2^n}}|b_1,\ldots,b_n\rangle + \frac{1}{2^{n-1}}(\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle) \\
&= -|b\rangle + \frac{1}{2^{n-1}}(\frac{1}{\sqrt{2^n}}|b_1,\ldots,b_n\rangle + \frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}|u\rangle) \\
&= -|b\rangle + \frac{1}{2^{n-1}}|b\rangle + \frac{1}{2^{n-1}}|m\rangle \\
&= (\frac{1}{2^{n-1}} - 1)|b\rangle + \frac{1}{2^{n-1}}|m\rangle.
\end{aligned}
$$

De forma analoga tenemos:

$$
\begin{aligned}
Q|m\rangle &= W^{\otimes n}U_0W^{\otimes n}U_f\frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}|u\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}W^{\otimes n}U_0W^{\otimes n}U_f|u\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}W^{\otimes n}U_0W^{\otimes n}(-1)^{f(u)}|u\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}(-1)^{f(u)}W^{n}U_0W^{\otimes}|u\rangle \\
&= \frac{1}{2^n}\sum_{u\neq b_1,\ldots,b_n}\sum_{\beta=0}^{2^n-1}(-1)^{\beta\cdot u}W^{\otimes n}U_0|\beta\rangle \\
&= \frac{1}{2^n}\sum_{u\neq b_1,\ldots,b_n}W^{\otimes n}(-|0\rangle+\sum_{\beta=1}^{2^n-1}(-1)^{\beta\cdot u}|\beta\rangle) \\
&= \frac{1}{2^n}\sum_{u\neq b_1,\ldots,b_n}W^{\otimes n}(-|0\rangle+\sum_{\beta=0}^{2^n-1}(-1)^{\beta\cdot u})|\beta\rangle-|0\rangle) \\
&= \frac{1}{2^n}\sum_{u\neq b_1,\ldots,b_n}W^{\otimes n}(-2|0\rangle+\sum_{\beta=0}^{2^n-1}(-1)^{\beta\cdot u}|\beta\rangle) \\
&= \frac{1}{2^n}\sum_{u\neq b_1,\ldots,b_n}W^{\otimes n}(-2|0\rangle+\sqrt{2^n}W^{\otimes n}|u\rangle) \\
&= \frac{-2}{2^n}(2^n-1)W^{\otimes n}|0\rangle+\frac{\sqrt{2^n}}{2^n}\sum_{u\neq b_1,\ldots,b_n}|u\rangle \\
&= \frac{-2}{2^n}(2^n-1)W^{\otimes n}|0\rangle+\frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}|u\rangle \\
&= -2(1-\frac{1}{2^n})\frac{1}{\sqrt{2^n}}\sum_{u=0}^{2^n-1}|u\rangle+|m\rangle \\
&= -2(1-\frac{1}{2^n})(\frac{1}{\sqrt{2^n}}\sum_{u\neq b_1,\ldots,b_n}|u\rangle+\frac{1}{\sqrt{2^n}}(b_1\cdots b_n))+|m\rangle \\
&= -2(1-\frac{1}{2^n})(|m\rangle+|b\rangle)+|m\rangle \\
&= 2(\frac{1}{2^n}-1)|b\rangle+2(\frac{1}{2^n}-1)|m\rangle+|m\rangle \\
&= 2(\frac{1}{2^n}-1)|b\rangle+(\frac{2}{2^n}-1)|m\rangle.
\end{aligned}
$$

□

Para "facilitar" cálculos se normalizarán los vectores, por el teorema 5.4, tenemos $|b\rangle = \frac{1}{\sqrt{2^n}}\ |b_1 \cdots b_n\rangle$ donde $f^{-1}(1) = \{(b_1, \ldots b_n)\}$, calculando su norma:

$$\begin{aligned}
\|b\| &= \sqrt{\langle b|b\rangle} \\
&= \sqrt{\frac{1}{\sqrt{2^n}}\langle b_1 \cdots b_n| \frac{1}{\sqrt{2^n}}|b_1 \cdots b_n\rangle} \\
&= \sqrt{\frac{1}{2^n}\langle b_1 \cdots b_n|b_1 \cdots b_n\rangle} \\
&= \sqrt{\frac{1}{2^n}}.
\end{aligned}$$

Luego, el normalizado de $|b\rangle$ es $|B\rangle = \frac{1}{|||b\rangle||}|b\rangle = \left(\frac{1}{\sqrt{\frac{1}{2^n}}}\right)\left(\frac{1}{\sqrt{2^n}}\right)|b_1 \cdots b_n\rangle$
$= |b_1 \cdots b_n\rangle$.

Calculando la norma de $|m\rangle$. Dada $|m\rangle = \frac{1}{\sqrt{2^n}}\sum_{u \neq b_1, \ldots b_n} |u\rangle$, tenemos

$$\begin{aligned}
|||m\rangle||^2 &= \langle m|m\rangle \\
&= (\frac{1}{\sqrt{2^n}} \sum_{u \neq b_1, \ldots b_n} \langle u|)(\frac{1}{\sqrt{2^n}} \sum_{u \neq b_1, \ldots b_n} \langle w|) \\
&= \frac{1}{2^n} \sum_{u \neq b_1, \ldots b_n} \langle u| \sum_{u \neq b_1, \ldots b_n} \langle u|w\rangle \\
&= \frac{1}{2^n} \sum_{w \neq b_1, \ldots b_n} 1 \\
&= \frac{1}{2^n}(2^n - 1) \\
&= 1 - \frac{1}{2^n}.
\end{aligned}$$

Por consiguiente $|||m\rangle|| = \sqrt{1 - \frac{1}{2^n}}$; y así, el normalizado de $|m\rangle$ es: $|M\rangle = \frac{1}{|||m\rangle||}|m\rangle = \frac{1}{\sqrt{1-\frac{1}{2^n}}}|m\rangle$.

Normalizamos a $Q|b\rangle = \left(\frac{2}{2^{n-1}} - 1\right)|b\rangle + \frac{2}{2^{n-1}}|m\rangle$. Multiplicando ambos lados de $Q|b\rangle = \left(\frac{2}{2^{n-1}} - 1\right)|b\rangle + \frac{1}{2^{n-1}}|m\rangle$ por $\frac{1}{\||b\rangle\|} = \sqrt{2^n}$ obtenemos:

$$\begin{aligned}
Q\sqrt{2^n}|b\rangle &= (\frac{1}{2^{n-1}} - 1)\sqrt{2^n}|b\rangle + \frac{1}{2^{n-1}}\sqrt{2^n}|m\rangle \\
Q|B\rangle &= (\frac{1}{2^{n-1}-1} - 1)|B\rangle + \||m\rangle\|\frac{\sqrt{2^n}}{2^n}\frac{1}{\||m\rangle\|}|m\rangle \\
&= (\frac{1}{2^{n-1}} - 1)|B\rangle + \left(\sqrt{1 - \frac{1}{2^n}}\right)\frac{\sqrt{2^n}}{\sqrt{2^n}}|M\rangle \\
&= (\frac{1}{2^{n-1}} - 1)|B\rangle + \sqrt{(}\frac{2^n - 1}{2^n})|M\rangle.
\end{aligned}$$

Normalizamos a $Q|m\rangle = 2(\frac{1}{2^n} - 1)|b\rangle + (\frac{2}{2^n} - 1)|m\rangle$. Multiplicamos ambos lados por $\frac{1}{\||m\rangle\|} = \frac{1}{\sqrt{1-\frac{1}{2^n}}}$, obtenemos:

$$\begin{aligned}
Q\left(\frac{1}{\sqrt{1-\frac{1}{2^n}}}\right)|m\rangle &= 2(\frac{1}{2^n} - 1)\frac{1}{\sqrt{1-\frac{1}{2^n}}}|b\rangle + (\frac{2}{2^n} - 1)\frac{1}{\sqrt{1-\frac{1}{2^n}}}|m\rangle \\
Q|M\rangle &= 2(\frac{1}{2^n} - 1)\frac{1}{\sqrt{1-\frac{1}{2^n}}}|b\rangle\frac{\||b\rangle\|}{\||b\rangle\|} + (\frac{2}{2^n} - 1)|M\rangle \\
&= 2(\frac{1}{2^n} - 1)\frac{1}{\sqrt{1-\frac{1}{2^n}}}|B\rangle\frac{1}{\sqrt{2^n}} + (\frac{1}{2^{n-1}} - 1)|M\rangle \\
&= (\frac{1}{2^{n-1}} - 1)|M\rangle + \frac{2(\frac{1}{2^n} - 1)}{\sqrt{2^n - 1}}|B\rangle \\
&= (\frac{1}{2^{n-1}} - 1)|M\rangle - \frac{\sqrt{2^n - 1}}{2^{n-1}}|B\rangle.
\end{aligned}$$

En resumen hemos llegado que:

$$\begin{aligned}
Q|M\rangle &= (\frac{1}{2^{n-1}} - 1)|M\rangle - \frac{\sqrt{2^n - 1}}{2^{n-1}}|B\rangle \\
Q|B\rangle &= \frac{\sqrt{2^n - 1}}{2^{n-1}}|M\rangle + (\frac{1}{2^{n-1}} - 1)|B\rangle.
\end{aligned}$$

Multiplicamos ambos ecuaciones anteriores por -1 tenemos:

$$-Q|M\rangle = (1 - \frac{1}{2^{n-1}})|M\rangle + \frac{\sqrt{2^n - 1}}{2^{n-1}}|B\rangle$$
$$-Q|B\rangle = -\frac{\sqrt{2^n - 1}}{2^n}|M\rangle + (1 - \frac{1}{2^{n-1}})|B\rangle.$$

El subespacio generado por $|M\rangle$, $|B\rangle$ es invariante ante $-Q|_S$, con lo que hemos demostrado el siguiente teorema.

Teorema 5.2. Tenemos que

$$-Q|_S = \begin{pmatrix} 1 - \frac{1}{2^{n-1}} & -\frac{\sqrt{2^n-1}}{2^n} \\ \frac{\sqrt{2^n-1}}{2^{n-1}} & 1 - \frac{1}{2^{n-1}} \end{pmatrix}$$

donde $\theta = \arcsin(\frac{\sqrt{2^n-1}}{2^{n-1}})$, $S = span\{|M\rangle, |B\rangle\}$.

Ahora queremos poner $-Q|_S$ en matriz de rotación de sin y cos. Note que: $\left(1 - \frac{1}{2^{n-1}}\right)^2 + \left(\frac{\sqrt{2^n-1}}{2^{n-1}}\right)^2 = 1 - \frac{1}{2^{n-2}} + \frac{1}{2^{2n-2}} + \frac{2^n-1}{2^{2n-2}} = 1.$

Así tenemos que $-Q|_S = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ es una matriz de rotación.

Teorema 5.3. (Espectral) Si A es normal entonces existe una matriz unitaria U tal que UAU^{-1} es diagonal:

$$UAU^{-1} = \begin{pmatrix} \xi_1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & \xi_n \end{pmatrix}.$$

Observación 5.3. En general las matrices unitarias son rotación, pues para el teorema espectral, si A es matriz unitaria, entonces A es similar a una matriz

diagonal de la forma

$$A = T \begin{pmatrix} e^{i\theta} & 0 & \dots & 0 \\ 0 & e^{i\theta_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \\ 0 & 0 & \dots & e^{i\theta_n} \end{pmatrix} T^{-1}.$$

Lema 5.1. Se tiene que $W^{\otimes n}|0\rangle = \cos(\frac{\theta}{2})|M\rangle + \sin(\frac{\theta}{2})|B\rangle$ donde $|0\rangle = \underbrace{|0\cdots 0\rangle}_{n \text{ ceros}}$ y $\theta = \arcsin(\frac{\sqrt{2^n-1}}{2^{n-1}})$.

Demostración. Sea

$$\begin{aligned} W^n|0\rangle &= \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} |u\rangle \\ &= \frac{1}{\sqrt{2^n}}|b_1, \dots, b_n\rangle + \frac{1}{\sqrt{2^n}} \sum_{u=b_1,\dots,b_n} |u\rangle \\ &= |b\rangle + |m\rangle \\ &= \||b\rangle\| \frac{1}{\||b\rangle\|}|b\rangle + \||m\rangle\| \frac{1}{\||m\rangle\|}|m\rangle \\ &= \||m\rangle\||M\rangle + \||b\rangle\||B\rangle \\ &= \sqrt{1 - \frac{1}{2^n}}|M\rangle + \frac{1}{2^n}|B\rangle. \end{aligned}$$

Para continuar usamos números complejos:

$$\begin{aligned} \left(\sqrt{1 - \frac{1}{2^n}} + i\frac{1}{\sqrt{2^n}}\right)^2 &= 1 - \frac{1}{2^n} - \frac{1}{2^n} + 2\sqrt{\frac{2^n-1}{2^n}}\sqrt{\frac{1}{2^n}}i \\ &= 1 - \frac{1}{2^{n-1}} + \frac{\sqrt{2^n-1}}{2^{n-1}}i \\ &= \cos\theta + \sin\theta i \\ &= e^{i\theta} (\text{identidad de Euler}) \end{aligned}$$

por lo tanto $\left(\sqrt{1-\frac{1}{2^n}}+i\frac{1}{\sqrt{2^n}}\right)^2 = e^{i\theta}$, sacando raíz cuadrada (rama principal) obtenemos:

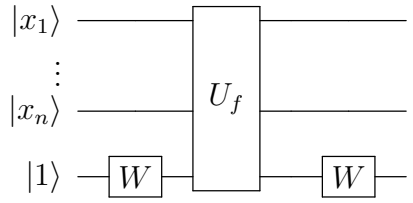
$$\begin{aligned}\sqrt{1-\frac{1}{2^n}}+i\frac{1}{\sqrt{2^n}} &= e^{i\frac{\theta}{2}} \\ &= \cos(\frac{\theta}{2})+i\sin(\frac{\theta}{2}) \\ &\Rightarrow \cos(\frac{\theta}{2}) = \sqrt{1-\frac{1}{2^n}}\end{aligned}$$

$$\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{2^n}} \tag{5.3}$$

sustituyendo tenemos: $W^{\otimes n}|0\rangle = \cos(\frac{\theta}{2})|M\rangle + \sin(\frac{\theta}{2})|B\rangle$. □

Teorema 5.4. Tenemos que $\tilde{U} = (Id^{\otimes n}\otimes W)U_f(Id^{\otimes n}\otimes W)$, entonces $\tilde{U}(|x_1,\ldots,x_n\rangle\otimes|1\rangle) = (-1)^{f(x_1,\ldots,x_n)}|x_1,\ldots,x_n\rangle\otimes|1\rangle$.

Para poder demostrar este teorema hacemos uso del siguiente circuito:



Demostración. Análisis: Por el axioma (1.1), tenemos como entrada: $|\psi_0\rangle = |x_1,\cdots,x_n\rangle\otimes|1\rangle$.

Aplicando $(Id\otimes W)$ al estado anterior:

$$\begin{aligned}|\psi_1\rangle &= (Id\otimes W)\otimes|\psi_0\rangle \\ &= (Id\otimes W)(|x_1\cdots x_n\rangle\otimes|1\rangle) \\ &= |x_1\cdots x_n\rangle\otimes(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) \\ &= \frac{1}{\sqrt{2}}|x_1\cdots x_n 0\rangle - \frac{1}{\sqrt{2}}|x_1\cdots x_n 1\rangle\end{aligned}$$

Por el axioma (1.2), aplicamos U_f al estado anterior:

$$
\begin{aligned}
|\psi_2\rangle &= U_f|\psi_1\rangle \\
&= U_f(\frac{1}{\sqrt{2}}|x_1 \dots x_n 0\rangle - \frac{1}{\sqrt{2}}|x_1 \dots x_n 1\rangle) \\
&= \frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \otimes |f(x_1, \dots, x_n) \oplus 0\rangle - \frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \otimes \\
&|f(x_1, \dots, x_n) \oplus 1\rangle \\
&= \frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \otimes |f(x_1, \dots, x_n)\rangle - \frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \otimes \left|\overline{f(x_1, \dots, x_n)}\right\rangle \\
&= (|x_1 \cdots x_n\rangle \otimes (-1)(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) \\
&= (-1)^{f(x_1,\dots,x_n)}|x_1 \cdots x_n\rangle \otimes W|1\rangle.
\end{aligned}
$$

Por último al estado anterior aplicamos $(Id \otimes W)$: $|\psi_3\rangle = (Id \otimes W)|\psi_2\rangle = (Id \otimes W)(-1)^{f(x_1,\dots,x_n)}|x_1, \cdots, x_n\rangle \otimes W|1\rangle = (-1)^{f(x_1,\dots,x_n)}|x_1, \cdots, x_n\rangle \otimes W^2|1\rangle = (-1)^{f(x_1,\dots,x_n)}|x_1, \cdots, x_n\rangle \otimes |1\rangle$, pues $W^2 = Id$. Entonces

$$(Id \otimes W)U_f(Id \otimes W)|x_1, \cdots, x_n 1\rangle = (-1)^{f(x_1,\dots,x_n)}|x_1, \cdots, x_n 1\rangle. \tag{5.4}$$

Del teorema (5.4) tenemos que $|x_1, \cdots, x_n 1\rangle$ es vector propio de $(Id \otimes W)U_f(Id \otimes W)$ con valor propio de $(-1)^{f(x_1,\dots,x_n)}$ luego tenemos dos casos para la ecuación (5.4):

Caso 1) Si $f(x_1, \dots, x_n) = 1$, entonces $(Id \otimes W)U_f(Id \otimes W)|x_1, \dots, x_n 1\rangle = (-1)|x_1, \dots, x_n 1\rangle$.

Caso 2) Si $f(x_1, \dots, x_n) = 0$, entonces $(Id \otimes W)U_f(Id \otimes W)|x_1, \dots, x_n\rangle = |x_1, \dots, x_n\rangle$.

Esto significa que la matriz unitaria $\tilde{U}_f = (Id \otimes W)U_f(Id \otimes W)$ marca a la asignación (registro) buscado. Podemos entonces suponer que tal matriz $\tilde{U}_f = U_f$ y que ésta tiene la propiedad siguiente $U_f|x_1, \dots, x_n\rangle = (-1)^{f(x_1,\dots,x_n}|x_1, \dots, x_n\rangle$. $\square$

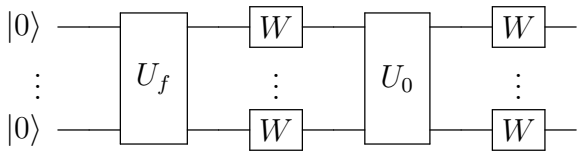
Definición 5.1. Sea $g(x_1, \ldots, x_n)$ la siguiente función boolena

$$g(x_1, \ldots, x_n) = \begin{cases} 1 & \text{si} \quad x_1 = 0, \ldots, x_n = 0 \\ 0 & \text{otro caso.} \end{cases}$$

La función g esta relacionada con U_0, donde U_0 es la versión cuántica de la función g, entonces $\tilde{U_g} = U_0$ como se definió en (5.1).

La forma de resolver el problema (5.1) cuánticamente será por medio del Algoritmo de Grover. Tal consiste, esencialmente en iterar el siguiente operador $Q = W^{\otimes n} U_0 W^{\otimes n} U_f$.

El algoritmo de Grover, tiene el siguiente diagrama:



Enseguida el análisis del Algoritmo de Grover, paso a paso:

Algoritmo 5.1

Entrada: La función f tal que $|f^{-1}(1)| = 1$
Salida: $f^{-1}(1)$

1: Se prepara el sistema con estado inicial:

$$\begin{aligned} |\psi_0\rangle &= \underbrace{|0 \cdots 0\rangle}_{n-\text{veces}} \\ &= |0\rangle^{\otimes n} \end{aligned}$$

2: Se le aplica $(W^{\otimes n})$ al estado anterior.

$$|\psi_1\rangle = (W^{\otimes n})|\psi_0\rangle.$$

3: Repetir $k+1$ veces

$$Q|\psi_1\rangle.$$

i) $|\psi_2\rangle = Q|\psi_1\rangle$

ii) $|\psi_1\rangle = |\psi_2\rangle$

Análisis:

Aplicando el axioma (1.1), tenemos nuestro estado inicial: $|\psi_0\rangle = \underbrace{|0\cdots 0\rangle}_{n-\text{veces}} = |0\rangle^{\otimes n}$.

Aplicando $W^{\otimes n}$, a nuestro estado inicial: $|\psi_1\rangle = (W^{\otimes n})|\psi_0\rangle = (W^{\otimes n})|0\cdots 0\rangle = \cos(\frac{\theta}{2})|M\rangle + \sin(\frac{\theta}{2})|B\rangle$.

Aplicando Q al estado anterior:

$$\begin{aligned}
|\psi_2\rangle &= Q|\psi_1\rangle \\
&= (-1)Q|\psi_1\rangle \\
&= (-1)Q(\cos(\frac{\theta}{2})|M\rangle) + \sin(\frac{\theta}{2})|B\rangle) \\
&= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}.
\end{aligned}$$

Donde éstas son coordenadas relativas a la base $|M\rangle, |B\rangle$.

De forma análoga con los siguientes estados:

$$\begin{aligned}
|\psi_3\rangle &= Q|\psi_2\rangle \\
&= (-1)Q|\psi_2\rangle \\
&= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} \\
&= \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} \\
&\vdots \\
|\psi_k\rangle &= Q|\psi_{k-1}\rangle \\
&= \begin{pmatrix} \cos(k-1)\theta & -\sin(k-1)\theta \\ \sin(k-1)\theta & \cos(k-1)\theta \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix} \\
&= \cos((k-1)\theta + \frac{\theta}{2})|M\rangle + \sin((k-1)\theta + \frac{\theta}{2})|B\rangle \\
&= \cos(\theta(k - \frac{1}{2}))|M\rangle + \sin(\theta(k - \frac{1}{2}))|B\rangle.
\end{aligned}$$

Luego; la probabilidad de éxito de obtener $|B\rangle$ es $\sin^2(\theta(k-\frac{1}{2}))$ después de k iteracion de Q, luego se quiere que $\sin^2(\theta(k-\frac{1}{2}))=1$, lo cual sugiere poner $\theta(k-\frac{1}{2})=\frac{\pi}{2}$, esto es $k-\frac{1}{2}=\frac{\pi}{2\theta}$, es decir $k=\frac{\pi}{2\theta}+\frac{1}{2}$, pero como k generalmente no es un número entero, es mejor poner $\lceil \frac{\pi}{2\arcsin\frac{\sqrt{2^n-1}}{2^{n-1}}}+\frac{1}{2}\rceil$ de donde, éste es el número de iteraciones de Q en el algoritmo de Grover. El número de iteraciones se toma el techo para tener una mejor aproximación.

Antes se mencionó que el número de iteraciones de Q en el algoritmo de Grover es $k\approx\sqrt{2^n}$. En lo que sigue se formalizará tal hecho.

5.1 Funciones de orden

Para justificar a k, necesitamos definir el orden de la función.

Definición 5.2. Sean $f,g:\mathbb{N}\to\mathbb{R}^+$ funciones

i) $f(n)\in O(g(n))$, si existe $c>0$ y $N\in\mathbb{R}$ tal que $f(n)<cg(n)$ para todo $n>N$. $f(n)\in O(g(n))$ se lee "$f(n)$ esta en el orden O de $g(n)$"

ii) $f(n)\in\Omega(g(n))$, si existe $c>0$ y $N\in\mathbb{R}$ tal que $f(n)>cg(n)$ para todo $n>N$. $f(n)\in\Omega(g(n))$ se lee "$f(n)$ esta en el orden omega grande de $g(n)$"

iii) $f(n)\in\Theta(g(n)$, si $f(n)\in O(g(n)$ y $f(n)\in\Omega(g(n))$. "$(f(n)\in\Theta(g(n))$ se lee $f(n)$ está en el orden exacto de $g(n)$".

Ejemplo 5.2. La función $2n^2\in\Omega(n^2)$.

Demostración. Existe $c>1$ y $N=1$, $(n\in\mathbb{N})$ tal que $2n^2>1n^2$, si $n>1$. □

Ejemplo 5.3. La función $2n^2\in O(n^2)$.

Demostración. Existe $c=3>0$ y $N=\frac{1}{2}$, $(n\in\mathbb{N})$ tal que $2n^2<3n^2$, si $n>\frac{1}{2}$. □

Expresemos aproximadamente k en términos de n (con $n \to \infty$), tal que $k \approx \frac{\pi}{2\theta} + \frac{1}{2}$ y θ de la siguiente forma:

$$\begin{aligned}\theta = \arcsin\left(\frac{2\sqrt{2^n - 1}}{2^n}\right) &= \arcsin\left(2\sqrt{\frac{2^n - 1}{2^{2n}}}\right) \\ &\approx \arcsin\left(2\sqrt{\frac{1}{2^n}}\right) \\ &\approx 2\sqrt{\frac{1}{2^n}}\end{aligned}$$

pues $\arcsin(x) \approx x$ si $x \approx 0$, luego $\theta \approx 2\sqrt{\frac{1}{2^n}}$ y $k \approx \frac{\pi}{2\theta} + \frac{1}{2}$, entonces $k \approx \frac{\pi}{4\sqrt{\frac{1}{2^n}}} + \frac{1}{2} = \frac{\pi}{4}\sqrt{2^n} + \frac{1}{2} \approx \sqrt{2^n}$.

En lo que sigue necesitamos la siguiente expresión para θ.

Afirmación 5.1. Sea $\theta = \arcsin(\frac{1}{\sqrt{2^n}}) = \arcsin(\frac{\sqrt{2^n-1}}{2^{n-1}})$.

Proposición 5.1. Si $k = \lceil \frac{\pi}{2\theta} + \frac{1}{2} \rceil$ con $\theta = \arcsin(\frac{\sqrt{2^n-1}}{2^n-1})$, entonces $k \in \Theta(\sqrt{2^n}) = O(\sqrt{2^n}) \cap \Omega(\sqrt{2^n})$.

Demostración. **i)** Por demostrar que $k \in O(\sqrt{2^n})$.

Tenemos que $\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{2^n}}$ por (5.3), entonces $\theta = 2\arcsin(\frac{1}{\sqrt{2^n}})$. Ademas si $0 \leq x \leq \pi$, tendremos que $0 \leq \sin x \leq x$. Luego $0 < \frac{1}{\sqrt{2^n}} < \pi$, para todo n, entonces $\sin(\frac{1}{\sqrt{2^n}}) \leq \frac{1}{\sqrt{2^n}}$ lo cual indica $0 < \frac{2}{\sqrt{2^n}} \leq 2\arcsin(\frac{1}{\sqrt{2^n}})$, entonces $\frac{2}{\sqrt{2^n}} \leq \theta$ despejando, nos da $\frac{2}{\theta} \leq \sqrt{2^n}$. Multiplicando por $\pi + \theta$ tenemos:

$2(\frac{\pi+\theta}{\theta}) \leq 2\pi\sqrt{2^n}$, por consiguiente $1 \leq (\frac{\pi+\theta}{2\theta}) \leq \frac{\pi}{2}\sqrt{2^n}$, como $2\theta \leq \pi + \theta$ y $\theta \leq \pi$, en general si $x \geq 1$, entonces $\lceil x \rceil \leq 2\pi$, pues $\lceil x \rceil - x \leq 1 \leq x$, de modo que $\lceil x \rceil \leq 2x$. luego $\lceil \frac{\pi+\theta}{2\theta} \rceil \leq 2(\frac{\pi+\theta}{2\theta}) \leq \pi\sqrt{2^n}$, entonces $k \leq \pi\sqrt{2^n}$, por lo tanto $k \in O(\sqrt{2^n})$.

ii) Por demostrar que $k \in \Omega(\sqrt{2^n})$.

Tenemos que $k = \lceil \frac{\pi}{2\theta} + \frac{1}{2} \rceil$ y $\theta = \arcsin(\frac{\sqrt{2^n-1}}{2^{n-1}})$ tal que θ satisface $\sin(\frac{\theta}{2}) = \sqrt{\frac{1}{2^n}}$ y $\cos(\frac{\theta}{2}) = \sqrt{1 - \frac{1}{2^n}}$. Si $0 < x < \frac{\pi}{2}$, de modo que $0 < x < \tan(x) = \frac{\sin(x)}{\cos(x)}$, entonces $x\cos(x) < \sin(x)$. En particular si $0 < x = \frac{\theta}{2} \leq \frac{\pi}{4} < \frac{\pi}{2}$, por

consiguiente

$$\begin{aligned}
\frac{\theta}{2}\cos(\frac{\theta}{2}) &< \sin(\frac{\theta}{2}) \Rightarrow \\
\frac{\theta}{2}\sqrt{1-\frac{1}{2^n}} &< \sqrt{\frac{1}{2^n}} \Rightarrow \\
\theta &< \frac{2\sqrt{\frac{1}{2^n}}}{\sqrt{1-\frac{1}{2^n}}} \\
&= \frac{2}{\sqrt{2^n}\sqrt{1-\frac{1}{2^n}}} \\
&= \frac{2}{\sqrt{2^n-1}}.
\end{aligned}$$

Si $n > 0$ entonces $2^n - 1 \geq 2^{n-1} = \frac{1}{2}2^n$, de modo que

$$\begin{aligned}
k = \left\lceil \frac{\pi}{2\theta} + \frac{1}{2} \right\rceil &\geq \frac{\pi}{2\theta} + \frac{1}{2} \\
&> \frac{\pi}{2}\frac{\sqrt{2^n-1}}{2} + \frac{1}{2} \\
&\geq \frac{\pi}{2}\frac{\sqrt{\frac{1}{2}2^n}}{2} + \frac{1}{2} \\
&\geq \frac{\pi}{4\sqrt{2}}\sqrt{2^n} + \frac{1}{2} \\
&\geq \frac{1}{2}\sqrt{2^n}.
\end{aligned}$$

Así pues $(\frac{\pi}{4\sqrt{2}} - \frac{1}{2})\sqrt{2^n} + \frac{1}{2} \geq 0$, entonces $k > \frac{1}{2}\sqrt{2^n}$ si $n > 0$. Luego $k \in \Omega(\sqrt{2^n})$, por $i)$ y $ii)$ se concluye que $k \in \Theta(\sqrt{2^n})$.

□

Todo lo que puede hacer una computadora clásica lo puede hacer (simular) una computadora cuántica. Uno puede darse una idea de este fenómeno recordando que esencialmente una computadora clásica calcula funciones del tipo $f : B^n \to B^m$ donde $B = 0, 1$ y $B^n = B \times \cdots \times B$ por lo cual,
$f(x_1, \ldots, x_n)$=$f_1(x_1, \ldots, x_n)$,...,$f_m(x_1, \ldots, x_n)$ donde cada $f_i : B^n \to B$ es función

booleana de aridad n, es decir f está completamente determinada por sus componentes $f_i, i = 1, \ldots, m$, luego, sabemos que tal f se puede escribir en términos de $\wedge$,$\vee$ y $\neg$ (AND, OR, NOT). Ahora, una computadora cuántica también puede similar $\wedge$, $\vee$ y $\neg$ con ayuda de la compuerta (matriz) de *Toffoli*, esta es $C(C(X))$ donde $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ es unitaria.

Observación 5.4. Para que dos estados $|\psi_1\rangle, |\psi_2\rangle$ sean distinguibles, éstos tienen que ser ortogonales: $\langle\psi_1|\psi_2\rangle$, porque en otro caso se obtienen problemas.

Ejemplo 5.4. Los vectores $|\psi_1\rangle = \frac{i}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}$ y $|\psi_2\rangle = |0\rangle$ no son perpendiculares, ya que $\langle\psi_2|\psi_1\rangle = \frac{i}{\sqrt{3}} \neq 0$.

Supongamos que tenemos un sistema que puede estar en los estados $|\psi_1\rangle$ y $|\psi_2\rangle$ y en base en ellos, tomemos una decisión. Se quiere definir una función $f : \{|\psi_1\rangle, |\psi_2\rangle\} \to \{0, 1\}$ tal que $f(|\psi_1\rangle) = 0$ y $f(|\psi_2\rangle) = 1$ Si el sistema está en el estado $|\psi_1\rangle$ y se observa (en la base del cálculo) luego se obtiene $|0\rangle = |\psi_2\rangle$ con probabilidad $\frac{1}{3}$ ó $|1\rangle$ con probabilidad $\frac{2}{3}$ luego $f(|2\rangle) = 1$ con probabilidad $\frac{1}{3}$.

Observación 5.5. Así, estados ajenos, en mecánica cuántica, son estados ortornomales.

Capítulo 6

Generalización del algoritmo del Grover

Se va estudiar la solución del algoritmo ha través de ecuaciones generales.

Problema 6.1. Dados las matrices P de tamaño $n \times n$ y $|B\rangle$ de tamaño $n \times 1$. Encontrar $|X\rangle$, tal que

$$P\overrightarrow{X} = |b\rangle, \tag{6.1}$$

donde P es hermitiana e idempontente .[7]

Generalmente, las matrices idempontentes son singulares.

Teorema 6.1. Si P es matriz cuadrada tal que $P^2 = P$, entonces P singular o $P = I$.

Demostración. Supongamos P matriz $n \times n$, tal que $P^2 = P$. Tenemos que $P^2 = P$, entonces $|P^2| = |P|$ y por tanto $|P^2| - |P| = 0$, luego $|P|(|P| - 1) = 0$ y por consiguiente $|P| = 0$ o $|P| = 1$, lo cual P es singular o P es invertible.

Si P invertible, entonces $P^2 = P$ y por tanto $P^{-1}P^2 = P^{-1}P$, así $P = I$, entonces P es singular o $P = I$. □

Observación 6.1.

1. Consideremos la ecuación del tipo $P\overrightarrow{X} = \overrightarrow{b}$ en casos no triviales, es decir $P \neq I$ y $P \neq 0$.

2. Queremos encontrar un algoritmo cuántico que resuelve la ecuación de la siguiente forma $P\overrightarrow{X} = \overrightarrow{b}$

3. Si A matriz cuadrada compleja, se define la exponencial e^A como $e^A := \sum_{n=0}^{\infty} \frac{1}{n!} A^n = \lim_{k\to\infty} \sum_{n=0}^{k} \frac{1}{n!} A^n$

4. Si la matriz A es diagonizable. Existe T matriz invertible tal que $A = \left[T \begin{pmatrix} \xi_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \xi_m \end{pmatrix} T^{-1} \right]$, entonces

$$
\begin{aligned}
e^A &= \lim_{k\to\infty} \sum_{n=0}^{k} \frac{1}{n!} \left[T \begin{pmatrix} \xi_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \xi_m \end{pmatrix} T^{-1} \right]^n \\
&= \lim_{k\to\infty} T \left[\sum_{n=0}^{k} \left[\begin{pmatrix} \frac{1}{n!}\xi_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \frac{1}{n!}\xi_m^n \end{pmatrix} \right] \right] T^{-1} \\
&= \lim_{k\to\infty} T \begin{pmatrix} \sum_{n=0}^{k} \frac{1}{n!}\xi_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sum_{n=0}^{k} \frac{1}{n!}\xi_m^n \end{pmatrix} T^{-1} \\
&= \begin{pmatrix} e^{\xi_1} & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & e^{\xi_n} \end{pmatrix}
\end{aligned}
$$

Definición 6.1. Una matriz cuadrada A se dice normal si $AA^* = A^*A$ donde A^* es la transpuesta conjugada de A.

1. Si la matriz $\begin{pmatrix} \xi_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n \end{pmatrix}$ es diagonal, entonces A es normal.

Demostración. Tenemos que

$$AA^* = \begin{pmatrix} \xi_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n \end{pmatrix} \begin{pmatrix} \xi_1^* & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n^* \end{pmatrix} = \begin{pmatrix} |\xi_1|^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & |\xi_n|^2 \end{pmatrix}$$

y por otro lado tenemos

$$A^*A = \begin{pmatrix} \xi_1^* & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n^* \end{pmatrix} = \begin{pmatrix} \xi_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n \end{pmatrix} \begin{pmatrix} |\xi_1|^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & |\xi_n|^2. \end{pmatrix}$$

Por consiguiente, la matriz a es normal. □

2. Si A es hermitiana, entonces A es normal.

   Demostración. Sea A una matriz hermitiana, entonces $A = A^*$ luego $A = A^* = AA = A^2 = A^*A$. □

3. Si A es unitaria, entonces A es normal.

   Demostración. Sea A una matriz unitaria, tal que $A^*A = Id = AA^*$. □

Observación 6.2. En la ecuación (6.1) supondremos que P y $|b\rangle$ son conocidos. Que P sea conocido significa que se puede usar $e^{i\phi P}$ para cualquier $0 < \phi < 2\pi$ análogamente, que $|b\rangle$ es conocido significa que se tiene A una matriz unitaria tal que $A|0\rangle = \frac{1}{\|b\|}|b\rangle$ donde $|0\rangle$ es un vector unitario inicial.

Teorema 6.2. Si U es una matriz unitaria, si sólo si existe una matriz hermitiana H tal que $U = e^{iH}$.

Demostración. ($\Rightarrow$) Si ξ es un valor propio de U, entonces existe $|v\rangle$ vector propio $\neq 0$ tal que $U|v\rangle = \xi|v\rangle$, por otro lado $(U|v\rangle)^*U|v\rangle = |v\rangle^*U^*U|v\rangle = \langle v|U^*U|v\rangle = \langle v|v\rangle$, entonces $(\xi|v\rangle)^*\xi|v\rangle = \langle v|v\rangle$, es decir $|\xi|^2\langle v|v\rangle = |v\rangle^*\xi^*\xi|v\rangle = \langle v|v\rangle$, en conclusión $|\xi| = 1$, en la cual $\xi = e^{i\theta}$, para $0 \leq \theta \leq 2\pi$. Por lo tanto los valores

de U son de la forma $e^{i\theta}$, además U es normal, entonces existe W unitario tal que *(por teorema espectral 5.3)*, tenemos que

$$WUW^{-1} = \begin{pmatrix} \xi_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n \end{pmatrix} = \begin{pmatrix} e^{i\theta_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{i\theta_n} \end{pmatrix}$$

donde $H_0 = \begin{pmatrix} \theta_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \theta_n \end{pmatrix} = e^{iH}$, donde $H = W^{-1}H_0W$, la cual es hermitiana por que $H^* = (W^{-1}H_0W)^* = W^{-1}H_0W = H$.

($\Leftarrow$) Supongamos $U = e^{iH}$ con $H^* = H$, luego $UU^* = e^{iH}(e^{iH})^* = e^{iH}e^{-iH} = e^{iH-iH} = Id$. Por lo tanto $U = e^{iH}$ es unitario. □

Una suposición importante para resolver (6.1) es que la solución $|x\rangle$, no sabemos cuál es , pero, si la vemos, la podemos distinguir.

Definición 6.2. Si $0 < \phi$ y $\varphi < 2\pi$, entonces $Q(\phi, \varphi, \rho) = e^{i\phi\rho}e^{i\varphi|X\rangle\langle X|}$ llamado operador de Grover (ó kernel de Grover).

Proposición 6.1. Si S el *P-espacio* cíclico generador por $|X\rangle$, entonces S es *Q-invariante.*

Demostración. Por definición S es el subespacio generado por $|X\rangle$, $P|X\rangle$,$P^2|X\rangle$, $P^3|X\rangle$,..., es decir $S = span\{|X\rangle, P|X\rangle\} = \{z_1|X\rangle + z_2P|X\rangle | z_1, z_2 \in \mathbb{C}\}$.

Debemos demostrar que si $w \in S$, entonces $Q|w\rangle \in S$. Para esto, basta probar que $Q|X\rangle \in S$ y $QP|X\rangle \in S$.

Tenemos que

$$\begin{aligned} e^{i\phi P} &= \sum_{n=0}^{\infty} \frac{(i\phi P)^n}{n!} \\ &= \sum_{n=0}^{\infty} \frac{(i\phi)^n}{n!} P^n \\ &= Id + \sum_{n=1}^{\infty} \frac{(i\phi)^n}{n!} P^n \\ &= Id + \sum_{n=1}^{\infty} \frac{(i\phi)^n}{n!} P \\ &= Id + \left[\sum_{n=0}^{\infty} \frac{(i\phi)^n}{n!} - 1 \right] P^n. \end{aligned}$$

Por consiguiente $e^{i\phi P} = Id + (e^{i\phi} - 1)P$, de forma similar $e^{i\varphi|X\rangle\langle X|} = Id + (e^{i\varphi} - 1)|X\rangle\langle X|$. Ahora $e^{i\varphi|X\rangle\langle X|}|X\rangle = (Id + (e^{i\varphi} - 1)|X\rangle\langle X|)|X\rangle = |X\rangle + (e^{i\varphi} - 1)|X\rangle\langle X|X\rangle = e^{i\varphi}|X\rangle$.

así

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

Por lo tanto $Q|X\rangle \in S$. análogamente $QP|X\rangle \in S$. □

Proposición 6.2. Si $\mu = \||b\rangle\|^2$, entonces

i) $\mu = \langle X|P|X\rangle$.

ii) Si $0 < \mu < 1$, entonces $|X\rangle$ y $P|X\rangle$ son linealmente independientes.

Demostración. **i)** Usando las definiciones, obtenemos que

$$\begin{aligned}\mu &= \|b\|^2 \\ &= \langle b|b\rangle \\ &= (|b\rangle)^* P|X\rangle \\ &= (P|X\rangle)^* P|X\rangle \\ &= |X\rangle^* P^* P|X\rangle \\ &= \langle X|PP|X\rangle \\ &= \langle X|P|X\rangle\end{aligned}$$

ii) Supongamos $z_1, z_2 \in \mathbb{C}$, tales que

$$z_1|X\rangle + z_2 P|X\rangle = 0. \tag{6.2}$$

Por demostrar que $z_1 = z_2 = 0$. Multiplicamos por $\langle X|$ a la izquierda ambos de (6.2), lo cual tenemos que $z_1\langle X|X\rangle + z_2\langle X|P|X\rangle = 0$, entonces $z_1 + \mu z_2 = 0$. ahora multiplicamos por $\langle b|$ ambos lados de (6.2), se tiene que, $z_1\langle b|X\rangle + z_2\langle b|P|X\rangle = 0$, entonces $z_1\langle X|P|X\rangle + z_2\langle b|b\rangle = 0$.

Tenemos las siguiente ecuación $z_1 + \mu z_2 = 0$ y $\mu z_1 + \mu z_2 = 0$, cuya matriz de coeficientes tiene determinantes $\begin{pmatrix} 1 & \mu \\ \mu & \mu \end{pmatrix} = \mu - \mu^2 = \mu(1-\mu) \neq 0$, entonces $z_1 = z_2 = 0$, por lo tanto $|X\rangle, P|X\rangle$ son linealmente independientes.

□

Tenemos que $\mu = \langle X|P|X\rangle = \langle P\rangle_X = E(P)$ donde μ es el valor promedio del observable P sobre el vector $|X\rangle$.

Proposición 6.3. Si $0 < \mu < 1$ entonces la matriz asociada a $e^{i\phi\rho}$ con respecto a la base $|X\rangle, P|X\rangle$ del P-espacio cíclico generado por $|X\rangle$ es $\begin{pmatrix} 1 & 0 \\ e^{i\phi} - 1 & 1 + (e^{i\phi} - 1) \end{pmatrix}$.

Demostración. El operador P en la base $|X\rangle, P|X\rangle$ se representa como $P|X\rangle = 0|X\rangle + 1P|X\rangle$, por otro lado $P|X\rangle = P^2|X\rangle = PP|X\rangle$, es decir $P = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$.

Pero $e^{i\phi\rho} = Id + (e^{i\phi} - 1)P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (e^{i\phi} - 1) \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ e^{i\phi} - 1 & 1 + (e^{i\phi} - 1) \end{pmatrix}$.

□

Lema 6.1. Si P es proyección ortogonal y $|X\rangle$ es vector unitario. El vector $|b\rangle = P|X\rangle$ tiene norma al cuadrado $\mu = |||b\rangle||^2$ tal que $0 \leq \mu \leq 1$.

Demostración. Por demostrar que $\mu \leq 1$. Sea $|\psi_0\rangle = P|X\rangle - a|X\rangle$, por definición tenemos

$$\begin{aligned} 0 \leq ||\psi_0||^2 &= \langle \psi_0 | \psi_0 \rangle \\ &= (\langle X|P - \langle X|\mu)(P|X\rangle - \mu|X\rangle) \\ &= \langle X|P|X\rangle - \mu\langle X|P|X\rangle - \mu|X\rangle P|X\rangle + \mu^2\langle X|X\rangle \\ &= \mu - 2\mu^2 + \mu^2. \end{aligned}$$

Por consiguiente $0 \leq \mu - \mu^2 = \mu(1 - \mu)$, entonces $0 \leq 1 - \mu$, por lo tanto $\mu \leq 1$.

□

Sabemos que si $0 < \mu < 1$ entonces $|X\rangle$ y $P|X\rangle$ son linealmente independientes formando una base del P-espacio cíclico S generado por $|X\rangle$, y ademas $S = span\{|X\rangle, P|X\rangle\}$.

ahora calculemos la representación matricial del $e^{i\varphi|X\rangle\langle X|}$ sobre la base $|X\rangle, P|X\rangle$. Notemos que $e^{i\varphi|X\rangle\langle X|}|X\rangle = e^{i\varphi}|X\rangle + 0P\langle X|$ y ademas $e^{i\varphi|X\rangle\langle X|}P|X\rangle = (Id + (e^{i\varphi} - 1)|X\rangle\langle X|)P|X\rangle = P|X\rangle + (e^{i\varphi} - 1)|X\rangle\langle X|P|X\rangle = \mu(e^{i\varphi} - 1)|X\rangle + P|X\rangle$.

Hemos demostrado la siguiente proposición.

Proposición 6.4. Sea $\mu = |||b\rangle||^2$, la representación matricial de $e^{i\varphi|X\rangle\langle X|}$ en la base $|X\rangle, P|X\rangle$ de S el P-espacio cíclico generado por $|X\rangle$ es:

$$\begin{pmatrix} e^{i\varphi} & \mu(e^{i\varphi}-1) \\ 0 & 1 \end{pmatrix}.$$

Corolario 6.1. Sea $Q = e^{i\phi\rho}e^{i\varphi|X\rangle\langle X|}$ y $\mu = |||b\rangle||^2$, entonces la representación matricial de Q en la base $|X\rangle, P|X\rangle$ de S el p-espacio cíclico generado por $|X\rangle$ es

$$\begin{pmatrix} e^{i\varphi} & \mu(e^{i\varphi}-1) \\ e^{i\varphi}(e^{i\phi})-1 & \mu(e^{i\varphi}-1)(e^{i\phi}-1)+e^{i\phi} \end{pmatrix}$$

Demostración. Por la proposición (6.3)y (6.4), tenemos que

$$\begin{aligned} Q &= e^{i\phi\rho}e^{i\varphi|X\rangle\langle X|} \\ &= \begin{pmatrix} 1 & 0 \\ e^{i\phi}-1 & e^{i\phi} \end{pmatrix} \begin{pmatrix} e^{i\varphi} & \mu(e^{i\varphi}-1) \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} e^{i\varphi} & \mu(e^{i\varphi}-1) \\ (e^{i\phi}-1)e^{i\varphi} & \mu(e^{i\varphi}-1)e^{i\phi}-1. \end{pmatrix} \end{aligned}$$

□

Problema: ajustar, ϕ, φ, n tales que $Q^n A|0\rangle = |X\rangle(A|0\rangle = \frac{1}{|||b\rangle||}|b\rangle$.

Observación 6.3. Sea A una matriz unitaria y $\mu = |||b\rangle||^2$ tal que

$$\begin{aligned} A|0\rangle &= \frac{1}{|||b\rangle||}|b\rangle \\ &= \frac{1}{|||b\rangle||}P|X\rangle \in span\{|X\rangle, P|X\rangle\}. \end{aligned}$$

Entonces $Q^n A|0\rangle \in S$ pues S es Q-invariante, es decir $Q^n A|0\rangle = \alpha_n|X\rangle + \beta_n P|X\rangle$ donde

$$\begin{pmatrix} e^{i\varphi} & \mu(e^{i\varphi}-1) \\ e^{i\varphi}(e^{i\varphi}-1) & \mu(e^{i\varphi}-1)(e^{i\phi}-1)+e^{i\phi} \end{pmatrix}^n \begin{pmatrix} 0 \\ \frac{1}{\sqrt{\mu}} \end{pmatrix} = \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}.$$

ahora;

$$\begin{aligned}\langle X|Q^nA|0\rangle &= \alpha_n\langle X|X\rangle + \beta_n\langle X|P|X\rangle \\ &= \alpha_n + \beta_n\mu \\ &= (1,\mu)\begin{pmatrix}\alpha_n \\ \beta_n\end{pmatrix} \\ &= (1,\mu)\begin{pmatrix}e^{i\varphi} & \mu(e^{i\varphi}-1) \\ e^{i\varphi}(e^{i\varphi}-1) & \mu(e^{i\varphi}-1)(e^{i\phi}-1)+e^{i\phi}\end{pmatrix}\begin{pmatrix}0 \\ \frac{1}{\sqrt{\mu}}\end{pmatrix}.\end{aligned}$$

La expresión anterior es útil pues:

$$\begin{aligned}Q^nA|0\rangle &= \alpha_n|X\rangle + \beta_nP|X\rangle \\ &= \alpha_n|X\rangle + \beta_n(|S\rangle + \mu|X\rangle) \\ &= (\alpha_n + \beta_n\mu)|X\rangle + \beta_n|S\rangle\end{aligned}$$

ya que $|S\rangle = P|X\rangle - \mu|X\rangle, \langle X|S\rangle = 0$. Luego, la probabilidad de observar $|X\rangle$ en Q^n, es $|\langle X|Q^nA|0\rangle|^2 = |(\alpha_n+\beta_n\mu)|^2$, lo cual queremos que cumpla $|\langle X|Q^nA|0\rangle|^2 = 1$.

Observación 6.4. Para continuar haremos uso de series formales con coeficiente complejo.

6.1 Series formales

Las series formales son de gran importancia a la probabilidad de éxito del algoritmo que se esta estudiando.

Definición 6.3. Sea R un anillo (no necesariamente conmutativo). Una serie formal con coeficiente en R es una función $f : \mathbb{N} \to R$.

Definición 6.4. Si $f : \mathbb{N} \to R$ y $g : \mathbb{N} \to R$. El conjunto de las series formales, con las operaciones de suma y producto es:

$$(Suma) \quad f + g : \mathbb{N} \to R; \quad (f+g)(n) = f(n) + g(n),$$
$$(Producto) \quad (f * g)(n); \quad (f * g)(n) = \sum_{\substack{i,j \\ i+j=n}} f(i)g(j).$$

Notación: Si $f : \mathbb{N} \to R$ es una serie formal se pone: $f = \sum_{n=0}^{\infty} a_n z^n$, donde $a_n = f(n)$, para todo $n \in \mathbb{N}$. Por consiguiente $f = \sum_{n=0}^{\infty} f(n) z^n$.

Teorema 6.3. Sea R un anillo y $R[\![z]\!]$ el conjunto de todas las series formales sobre R. Entonces $(R[\![z]\!], +, *,)$ es un anillo.

Demostración. Necesitamos ahora probar, que se verifican todos los axiomas de un anillo. Sean $h, s, t \in R[\![z]\!]$, para todo $n \in N$.

1. Por demostrar que $(h + s) \in R[\![z]\!]$. Sean h, $s \in R$. así $(h + s)(n) = h(n) + s(n)$, como $h(n) \in R[\![z]\!]$ y $s(n) \in R[\![z]\!]$. Entonces $h(n) + s(n) \in R[\![z]\!]$, así $(h + s) \in R[\![z]\!]$.

2. Por demostrar $[(h + s) + t](n) = [h + (s + t)](n)$.

   Como $[(h + s) + t](n) = (h + s)(n) + t(n) = [h(n) + s(n)] + t(n) = h(n) + [s(n) + t(n)] = h(n) + (s + n)(n) = [h + (s + t)](n)$.

3. Por demostrar $(h + s)(n) = (s + h)(n)$. Como $(h + s)(n) = h(n) + s(n) = s(n) + h(n) = (s + h)(n)$.

4. Por demostrar, que hay un elemento $0 \in R[\![z]\!]$, tal que $h + 0 = h$.

   Denotemos por $\mathbf{0}$ la serie cero: $\mathbf{0}(n) = 0$, $\forall n \in N.$, para cada $h \in R[\![z]\!]$, tenemos $(h + \mathbf{0})(n) = h(n) + \mathbf{0}(n) = h(n) + 0 = h(n)$, para todo $n \in N$. Así pues $h + 0 = h$ y 0 es el vector cero en $R[\![z]\!]$.

5. Por demostrar, que existe un elemento $-h$ en $R[\![z]\!]$ tal que $h + (-h) = 0$.

Se define $-h : \mathbb{N} \to R[\![z]\!]$ y $(-h)(n) = -h(n) \in R[\![z]\!]$. Si $-h \in R[\![z]\!]$ y $h \in R[\![z]\!]$. Ahora $(h+(-h))(n) = h(n)+(-h)(n) = h(n)-h(n) = 0 = \mathbf{0}(n)$. De aquí $h + (-h) = \mathbf{0}$

6. Por demostrar, $g \cdot h$ esta en $R[\![z]\!]$.

   Sean $g, h \in R[\![z]\!]$ y $n \in N$.

   Ahora bien $(g * h)(n) = h(n) * s(n)$, como $h(n) \in R$ y $s(n) \in R$. Entonces $h(n) * s(n) \in R[\![z]\!]$, así $(h * s) \in R[\![z]\!]$.

7. Por demostrar $(h * (s * t)) = ((h * s) * t)$.

   Sea $h, s, t \in R[\![z]\!]$. Ahora bien $(h * (s * t))(n) = h(n) * (s * t)(n) = h(n) * (s(n) * t(n)) = (h(n) * s(n)) * t(n) = ((h * s) * t)(n)$ ya que $h(n), s(n), t(n) \in R$, entonces $(h * (s * t)) = ((h * s) * t)$.

8. Por demostrar $h * (s + t) = h * s + h * t$ y $(s + t) * h = s * h + t * h$.

   Sean $h, s, t \in R[\![z]\!]$, entonces $(h * (s + t))(n) = h(n) * (s(n) + t(n)) = h(n) * s(n) + h(n) * t(n) = (h * s + h * t)(n)$, ya que $h(n), s(n), t(n)$ pertenece a $R[\![z]\!]$, por lo tanto $h * (s + t) = h * s + h * t$. De forma similar $(s + t) * h = s * h + t * h$.

□

Proposición 6.5. Sea R un anillo con unidad, la serie formal $\sum_{n=0}^{\infty} a_n z^n$ tiene inverso multiplicativo si sólo si a_0 es invertible en R.

Demostración. [⇐] Supongamos a_0 es invertible, existe $b_0 \in R$ tal que $a_0 b_0 = 1 = b_0 a_0$.

Por demostrar que existe $\sum_{m=0}^{\infty} b_m z^m$ tal que $(\sum_{n=0}^{\infty} a_n z^n)(\sum_{m=0}^{\infty} b_m z^m) = 1 = 1 + 0z + 0z^2 + 0z^2 + \cdots$.

Como

$$(\sum_{n=0}^{\infty} a_n z^n)(\sum_{m=0}^{\infty} b_m z^m) = a_0 b_0 + (a_0 b_1 + a_1 + a_1 b_0) z + (a_0 b_2 + a_1 b_1 + a_2 b_0) z^2 + \cdots$$

$$= 1 + 0z + 0z^2 + 0z^3 + \cdots$$

Nota: En general $\sum_{n=0}^{\infty} c_n z^n = \sum_{n=0}^{\infty} d_n z^n$, lo cual $c_n = d_n$, para $n = 0, 1, 2, \ldots$, en nuestro caso tenemos $a_0 b_0 = 1$, es decir $b_0 = a_0^{-1}$, ademas obtenemos que $a_0 b_1 + a_1 b_0 = 0$, consecuentemente $a_0 b_1 = -a_1 b_0$, por lo tanto $a_0^{-1} a_0 b_1 = -a_0^{-1} a_1 b_0$ $= -a_0^{-1} a_1 a_0^{-1}$.

Luego $b_1 = -a_0^{-1} a_1 a_0^{-1}$. En general $a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0 = 0$ lo cual tenemos que $b_k = a_0^{-1}[-a_1 b_{k-1} - a_2 b_{k-2} - \cdots - a_k b_0]$. Por consiguiente tenemos nuestra serie $\sum_{m=0}^{\infty} b_m z^m$.

[$\Rightarrow$] Por demostrar que a_0 es invertible, tal que $a_0 b_0 = 1$, par $b_0 \in R$.

Ahora bien sea $(\sum_{m=0}^{\infty} b_m z^m)$ el inverso multiplicativo de la serie $(\sum_{m=0}^{\infty} b_m z^m)$, tal que $(\sum_{m=0}^{\infty} b_m z^m))(\sum_{m=0}^{\infty} b_m z^m) = 1 = 1 + 0z + 0z^2 + 0z^2 + \cdots$. , dos series son iguale componente a componente, por consiguiente $a_0 b_0 = 1$. por lo tanto a_0 es invertible. □

Ejemplo 6.1. Sea R un anillo con unidad, tal que $(1 - z)^{-1} = \sum_{n=0}^{\infty} z^n$.

(Esta serie formal se llama serie geométrica).

Demostración. Sabemos que

$$\begin{aligned}(1 - z)(\sum_{n=0}^{\infty} z^n) &= (1 - z + 0z^2 + 0z^3 + \cdots)(1 + z + z^2 + z^3 + \cdots) \\ &= 1 + (1 - 1)z + (1 + (-1) + 0)z^2 + (1 - 1 + 0 + 0)z^3 + \cdots \\ &= 1\end{aligned}$$

y $(\sum_{n=0}^{\infty} z^n)(1 - z) = 1$. Por lo tanto $(1 - z)^{-1} = \sum_{n=0}^{\infty} z^n$ □

Ejemplo 6.2. Sea R un anillo con unidad y $r \in R$ cualquiera $(1 - rz)^{-1} = \sum_{n=0}^{\infty} r^n z^n$.

Ejemplo 6.3. Sea A una matriz $n \times n$ con coeficiente complejos $A \in M_n(\mathbb{C})$ anillo de matrices complejas $n \times n$. Entonces $(Id - Az)^{-1} = \sum_{n=0}^{\infty} a^n z^n$.

Definición 6.5. Se define la serie formal en variable z como $g(\phi, \varphi; z) = \sum_{n=0}^{\infty} \langle X|Q^n A|0\rangle z^n = \langle X| \sum_{n=0}^{\infty} Q^n z^n A|0\rangle = \langle X|(Id - Qz)^{-1} A|0\rangle z$.

Pues la serie $\sum_{n=0}^{\infty} Q^n z^n = (Id - Qz)^{-1}$ es una serie geométrica.

Observación 6.5. Sea $Id - Qz = Idz^0 + (-Q)z^1 + 0z^2 + 0z^3 + \cdots$ serie formal con coeficiente en el anillo $M_n(\mathbb{C})$ de matrices $n \times n$ complejos y $(Id - Qz)^{-1}$ es el inverso en el anillo de estas series formales.

Lema 6.2. Sea A matriz compleja $n \times n$, sea $|X\rangle, |Y\rangle \in \mathbb{C}^n$ arbitrarios, entonces $\sum_{k=0}^{\infty} \langle X|A^k|Y\rangle z^k = \langle X|(Id - zA)^{-1}|Y\rangle$ donde $Id - zQ$ es matriz con coeficientes y variable z.

Observación 6.6. Supongamos que $\phi = \varphi = \pi$ y $\mu = |||b\rangle||^2$, entonces $Q = \begin{pmatrix} -1 & -2\mu \\ 2 & 4\mu - 1 \end{pmatrix}$ en la base $|X\rangle, P|X\rangle$.

Calculemos la serie formal

$$\begin{aligned} g(\phi, \varphi; z) &= \sum_{n=0}^{\infty} \langle X|Q^n A|0\rangle z^n \\ &= \sum_{n=0}^{\infty} \langle X|(Id - zQ)^{-1} A|0\rangle \text{ por el lema} \quad (6.2) \end{aligned}$$

donde $|X\rangle = 1 \cdot |X\rangle + 0P|X\rangle$; luego $\langle X| = (1, 0)$ y como

$$\begin{aligned} \mu|0\rangle &= \frac{1}{||b||}|b\rangle \\ &= \frac{1}{\sqrt{\langle b|b\rangle}}|b\rangle \\ &= \frac{1}{\sqrt{\mu}} P|X\rangle \\ &= 0|X\rangle + \frac{1}{\sqrt{\mu}} P|X\rangle. \end{aligned}$$

Es decir $\mu|0\rangle = \begin{pmatrix} 1 \\ \frac{1}{\sqrt{\mu}} \end{pmatrix}$. Luego

$$\begin{aligned} g(\pi,\pi;z) &= \langle X| \begin{pmatrix} 1+z & 2\mu z \\ -2z & 1+(1-4\mu)z \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{\mu}} \end{pmatrix} \\ &= \langle X| \begin{pmatrix} \Sigma_1 \\ \Sigma_2 \end{pmatrix} \\ &= \langle X|(\Sigma_1|X\rangle + \Sigma_2 P|X\rangle) \\ &= \Sigma_1 + \Sigma_2 \langle X|P|X\rangle \\ &= \Sigma_1 + \Sigma_2 \mu \\ &= \frac{-\sqrt{\mu}(z-1)}{z^2+(2-4\mu)z+1} \end{aligned}$$

, donde $\Sigma_1 = \frac{-2\sqrt{\mu}z}{4\mu z^2+(z+1)((1-4\mu)z+1)}$ y $\Sigma_2 = \frac{z+1}{\sqrt{\mu}(4\mu z^2+(z+1))((1-4\mu)z+1)}$.

Por consiguiente hemos demostrado el siguiente.

Teorema 6.4. Sea $g(\phi,\varphi,z)$ una serie formal en variable z , donde $\phi = \varphi = \pi$ y $\mu = |||b\rangle||^2$, entonces

$$g(\pi,\pi;z) = \frac{-\sqrt{\mu}(z-1)}{z^2+(2-4\mu)z+1}. \tag{6.3}$$

Calculemos la serie de Taylor de lado derecho de la ecuación (6.3) alrededor de $z_0 = 0$, desarrollando las fracciones parciales. Sea

$$z^2 + 2(1-2\mu)^2 + 1 = 0 \tag{6.4}$$

tal que $z = \frac{-2(1-2\mu)\pm\sqrt{4(1-2\mu)^2-4}}{2} = (2\mu-1) \pm \sqrt{(1-2\mu)^2-1} = (2\mu-1) \pm 2i\sqrt{\mu(\mu-1)}$.

Es decir $\Sigma = 2\mu - 1 + 2i\sqrt{\mu(1-\mu)}$ y $\Sigma^* = 2\mu - 1 - 2i\sqrt{\mu(1-\mu)}$ son raices de la ecuación (6.4) y por consiguiente $|\Sigma|^2 = (2\mu-1)^2 + 4\mu(1-\mu) = 1$.

Sea $\sigma = e^{i\theta}$, para ángulos convariantes. Sabemos que

$$\begin{aligned} g(\pi,\pi;z) &= \frac{-\sqrt{\mu}(z-1)}{(z-e^{i\theta})(z-e^{-i\theta})} \\ &= \frac{-\sqrt{\mu}(z-1)}{(z-\sigma)(z-\sigma^{-1})} \\ &= \frac{A}{z-\sigma} + \frac{B}{Z-\Sigma^{-1}} \\ &= \frac{A(z-\sigma^{-1}) + B(z-\sigma)}{(z-\sigma)(z-\sigma^{-1})}, \end{aligned}$$

lo cual tenemos que $A = \frac{-\sqrt{\mu}e^{i\theta}}{e^{i\theta}+1}$,$B = \frac{-\sqrt{\mu}}{e^{i\theta}+1}$. así

$$\begin{aligned} g(\pi,\pi;z) &= \frac{\sqrt{\mu}}{\sigma+1}\sum_{k=0}^{\infty}\sigma^{-k}z^k + \frac{\sqrt{\mu}}{\sigma+1}\sum_{k=0}^{\infty}\sigma^{k+1}z^k \\ &= \sum_{k=0}^{\infty}(\sigma^{-k}\frac{\sqrt{\mu}}{\sigma+1} + \sigma^{k+1}\frac{\sqrt{\mu}}{\sigma+1})z^k \\ &= \sum_{k=0}^{\infty}\frac{\sqrt{\mu}}{(\sigma+1)\sigma^k}(1+\sigma^{2k+1})z^k. \end{aligned}$$

Entonces queremos que $1 = |\frac{\sqrt{\mu}}{(\sigma+1)\sigma^k}(1+\sigma^{2k+1})| = \frac{\sqrt{a}}{|(\sigma+1)|}|1+\sigma^{2k+1}|$, por definición $\sigma = e^{i\theta} = 2\mu - 1 + i2\sqrt{\mu}\sqrt{1-\mu}$, despejando tenemos $\sigma + 1 = 2\mu + i2\sqrt{\mu}\sqrt{1-\mu}$, entonces $|\sigma+1|^2 = 4\mu^2+4-4^2$, lo cual $1 = \frac{|1+\sigma^{2k+1}|^2}{4}$, por lo tanto $4 = |1+\sigma^{2k+1}|^2$. Como $\sigma^{2k+1} = e^{i\theta(2k+1)}$, tenemos $\theta(2k+1) = 2\pi$, luego $2k+1 = \frac{2\pi}{\theta}$, entonces $k = \frac{2\pi+\theta}{2\theta} \approx \lceil\frac{2\pi+\theta}{2\theta}\rceil$. Lo cual concluimos que $k = \lceil\frac{2\pi+\theta}{2\theta}\rceil$ para $\theta = \arcsin(2\sqrt{\mu}\sqrt{1-\mu})$.

6.2 Ejemplos

Dados las matrices P, $|b\rangle$, encontrar $|X\rangle$ tal que $P|X\rangle = |b\rangle$ donde $P^* = P$ y $P^2 = P$.

Ejemplo 6.4. Dado $P = \begin{pmatrix} \frac{1}{6} & -\frac{6\,i-7}{6\sqrt{17}} \\ \frac{6\,i+7}{6\sqrt{17}} & \frac{5}{6} \end{pmatrix}$ y $|b\rangle = \begin{pmatrix} -\frac{324\sqrt{2941}\,i+\left(-5\sqrt{17}-378\right)\sqrt{2941}}{1038\,17^{\frac{3}{2}}} \\ \frac{30\sqrt{2941}\,i+\left(270\sqrt{17}+35\right)\sqrt{2941}}{1038\,17^{\frac{3}{2}}} \end{pmatrix}$ tal que

$$\begin{pmatrix} \frac{1}{6} & -\frac{6\,i-7}{6\sqrt{17}} \\ \frac{6\,i+7}{6\sqrt{17}} & \frac{5}{6} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -\frac{324\sqrt{2941}\,i+\left(-5\sqrt{17}-378\right)\sqrt{2941}}{1038\,17^{\frac{3}{2}}} \\ \frac{30\sqrt{2941}\,i+\left(270\sqrt{17}+35\right)\sqrt{2941}}{1038\,17^{\frac{3}{2}}} \end{pmatrix}$$

Sabemos que P es hermitiana e indepotente. Queremos encontrar $|X\rangle = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$, tal que $\langle X|X\rangle = 1$ y se una única solución marcada. De modo que $|X\rangle = \begin{pmatrix} \frac{5}{\sqrt{2941}} \\ \frac{54}{\sqrt{2941}} \end{pmatrix}$. El algoritmo va a calcular esta solución, para distinguirla se marcara con la matriz $e^{i\varphi\langle X|X\rangle}$. Entonces se define $Q = e^{i\phi P}e^{i\varphi\langle X|X\rangle}$, con $\phi = \varphi = \pi$.

Por lo cual

$$\begin{aligned} Q &= \begin{pmatrix} \frac{2}{3} & -\frac{7-6\,i}{3\sqrt{17}} \\ -\frac{6\,i+7}{3\sqrt{17}} & -\frac{2}{3} \end{pmatrix} \begin{pmatrix} \frac{2891}{2941} & -\frac{540}{2941} \\ -\frac{540}{2941} & -\frac{2891}{2941} \end{pmatrix} \\ &= \begin{pmatrix} -\frac{3240\,i-5782\sqrt{17}-3780}{519\,17^{\frac{3}{2}}} & -\frac{17346\,i+1080\sqrt{17}-20237}{519\,17^{\frac{3}{2}}} \\ -\frac{17346\,i-1080\sqrt{17}+20237}{519\,17^{\frac{3}{2}}} & \frac{3240\,i+5782\sqrt{17}+3780}{519\,17^{\frac{3}{2}}} \end{pmatrix} \end{aligned}$$

Calculando el número de veces que aparece Q , tenemos que $\mu = \frac{3780\sqrt{17}+248285}{299982}$ y $\theta = 0.708650016424268$, por lo cual el número de iteraciones $K = \lceil \frac{2\pi+\theta}{2\theta} \rceil$, de modo que: $K = 5$.

Necesitamos A matriz unitaria tal que:

$$A|0\rangle = \begin{pmatrix} -\frac{324\sqrt{1038}\sqrt{2941}\,i+\left(-5\sqrt{17}-378\right)\sqrt{1038}\sqrt{2941}}{1038\sqrt{17}\sqrt{3780\sqrt{17}+248285}} \\ \frac{30\sqrt{1038}\sqrt{2941}\,i+\left(270\sqrt{17}+35\right)\sqrt{1038}\sqrt{2941}}{1038\sqrt{17}\sqrt{3780\sqrt{17}+248285}} \end{pmatrix}$$

Verifiquemos el resultado con el numero de iteraciones: $\langle X|Q^5A|0\rangle \approx -0.7276$, luego la probabilidad de observar $|X\rangle$ es aproximadamente $|\mu|^2 = 0.5294$.

Ejemplo 6.5. Dados las matrices P y $|b\rangle$:

$$P = \begin{pmatrix} \frac{52}{53} & \frac{-12i-104}{53\sqrt{41}} & \frac{-1764i+54}{\sqrt{53}\sqrt{541}\sqrt{9613}} \\ \frac{-104+12i}{53\sqrt{541}} & \frac{17713}{28673} & \frac{-184104i-15552}{541\sqrt{53}\sqrt{9613}} \\ \frac{1764i+54}{\sqrt{53}\sqrt{54}\sqrt{9613}} & \frac{184104i-15552}{541\sqrt{53}\sqrt{9613}} & \frac{217}{541} \end{pmatrix}$$

y

$$|b\rangle = \begin{pmatrix} \frac{(3\,i+4)\left(\frac{54}{\sqrt{53}\,\sqrt{541}\,\sqrt{9613}}-\frac{1764\,i}{\sqrt{53}\,\sqrt{541}\,\sqrt{9613}}\right)}{\sqrt{131}} - \frac{9\left(-\frac{12\,i}{53\,\sqrt{541}}-\frac{104}{53\,\sqrt{541}}\right)}{\sqrt{131}} + \frac{260\,i}{53\,\sqrt{131}} \\ \frac{(3\,i+4)\left(-\frac{184104\,i}{541\,\sqrt{53}\,\sqrt{9613}}-\frac{15552}{541\,\sqrt{53}\,\sqrt{9613}}\right)}{\sqrt{131}} + \frac{5\,i\left(\frac{12\,i}{53\,\sqrt{541}}-\frac{104}{53\,\sqrt{541}}\right)}{\sqrt{131}} - \frac{159417}{28673\,\sqrt{131}} \\ \frac{5\,i\left(\frac{1764\,i}{\sqrt{53}\,\sqrt{541}\,\sqrt{9613}}+\frac{54}{\sqrt{53}\,\sqrt{541}\,\sqrt{9613}}\right)}{\sqrt{131}} - \frac{9\left(\frac{184104\,i}{541\,\sqrt{53}\,\sqrt{9613}}-\frac{15552}{541\,\sqrt{53}\,\sqrt{9613}}\right)}{\sqrt{131}} + \frac{217\,(3\,i+4)}{541\,\sqrt{131}} \end{pmatrix}$$

Tenemos que P es hermitiano e idepotente. Queremos encontrar $|X\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, tal que sea unitaria es decir $\langle X|X\rangle = 1$ y que satisfaga dicha ecuación $P|X\rangle = |b\rangle$. El algoritmo va a calcular la solución. Para distinguirla se marcara con la matriz $e^{i\varphi|X\rangle\langle X|}$, digamos que nos interesa $\begin{pmatrix} \frac{5\,i}{\sqrt{131}} \\ -\frac{9}{\sqrt{131}} \\ \frac{3\,i+4}{\sqrt{131}} \end{pmatrix}$. Entonces se define

$$Q \approx \begin{pmatrix} -0.167\,i - 0.645 & -0.552\,i - 0.131 & 0.366, i + 0.317 \\ -0.0439\,i - 0.205 & 0.673\,i - 0.28 & 0.639\,i - 0.124 \\ -0.126\,i - 0.704 & 0.303\,i + 0.236 & -0.506\,i - 0.29 \end{pmatrix}.$$

Calculando el número de veces que aparece Q, tenemos que: $\mu = 0.4463577936872$ y $\theta = 1.463305034555196$. Por lo cual el número de iteraciones son $K = 3$.

Necesitamos A matriz unitaria tal que:

$$A|0\rangle = \begin{pmatrix} 0.5987\,i + 0.1427 \\ -0.3204\,i - 0.5675 \\ 0.1877 - 0.4016\,i \end{pmatrix}.$$

Verifiquemos el resultado con el número de iteraciones, tenemos que $Q^3\mu|0\rangle \approx \begin{pmatrix} 0.2367\,i - 0.07.629 \\ 0.1713\,i - 0.6988 \\ 0.5488\,i + 0.3451 \end{pmatrix}$. Entonces $\langle X|Q^3A|0\rangle \approx 0.00049\,i + 0.91$, luego la probabilidad de observa $|X\rangle$ es $|\mu|^2 = 0.83$.

Ejemplo 6.6. Dados $P =$

$$\begin{pmatrix} \frac{25}{73} & -\frac{648}{73\sqrt{566}} & \frac{9960}{\sqrt{219}\sqrt{283}\sqrt{19858}} & -\frac{108}{\sqrt{219}\sqrt{9929}} \\ -\frac{648}{73\sqrt{566}} & \frac{16285}{20659} & \frac{134460}{\sqrt{219}\sqrt{283}\sqrt{566}\sqrt{19858}} & -\frac{1458}{\sqrt{219}\sqrt{566}\sqrt{9929}} \\ \frac{9960}{\sqrt{219}\sqrt{283}\sqrt{19858}} & \frac{134460}{\sqrt{219}\sqrt{283}\sqrt{566}\sqrt{19858}} & \frac{2465457}{2809907} & \frac{7470}{\sqrt{283}\sqrt{9929}\sqrt{19858}} \\ -\frac{108}{\sqrt{219}\sqrt{9929}} & -\frac{1458}{\sqrt{219}\sqrt{566}\sqrt{9929}} & \frac{7470}{\sqrt{283}\sqrt{9929}\sqrt{19858}} & \frac{9848}{9929} \end{pmatrix}$$

y $|b\rangle =$

$$\begin{pmatrix} \frac{25\,(13\,i-5)}{146\sqrt{111}} + \frac{24900\,i}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{19858}} - \frac{3888\,i}{73\sqrt{111}\sqrt{566}} + \frac{486}{\sqrt{111}\sqrt{219}\sqrt{9929}} \\ -\frac{324\,(13\,i-5)}{73\sqrt{111}\sqrt{566}} + \frac{336150\,i}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{566}\sqrt{19858}} + \frac{97710\,i}{20659\sqrt{111}} + \frac{6561}{\sqrt{111}\sqrt{219}\sqrt{566}\sqrt{9929}} \\ \frac{4980\,(13\,i-5)}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{19858}} + \frac{806760\,i}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{566}\sqrt{19858}} + \frac{12327285\,i}{5619814\sqrt{111}} - \frac{33615}{\sqrt{111}\sqrt{283}\sqrt{9929}\sqrt{19858}} \\ -\frac{54\,(13\,i-5)}{\sqrt{111}\sqrt{219}\sqrt{9929}} + \frac{18675\,i}{\sqrt{111}\sqrt{283}\sqrt{9929}\sqrt{19858}} - \frac{8748\,i}{\sqrt{111}\sqrt{219}\sqrt{566}\sqrt{9929}} - \frac{44316}{9929\sqrt{111}} \end{pmatrix}$$

Sabemos que P es hermitiano e idempotente. Queremos encontrar un $|X\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$, tal que $\langle X|X\rangle = 1$, que satisfaga dicha ecuación $P|X\rangle = |b\rangle$.

El algoritmo va a calcular la solución, para distinguirla se marcara con la matriz $e^{i\varphi|X\rangle\langle X|}$, digamos que nos interesa $|X\rangle = \begin{pmatrix} \frac{13\,i-5}{2\sqrt{111}} \\ \frac{6\,i}{\sqrt{111}} \\ \frac{5\,i}{2\sqrt{111}} \\ -\frac{9}{2\sqrt{111}} \end{pmatrix}$. Entonces se define $Q = e^{i\phi P}e^{i\varphi\langle X|X\rangle}$, con $\phi = \varphi = \pi$.

Lo cual nos dice que

$$Q \approx \begin{pmatrix} 0.0605\,i - 0.348 & 0.194 - 0.157\,i & -0.0652\,i - 0.798 & 0.414\,i + 0.0292 \\ 0.577 - 0.236\,i & -0.242\,i - 0.64 & -0.101\,i - 0.349 & 0.0474\,i - 0.0985 \\ 0.389 - 0.139\,i & 0.184\,i + 0.49 & 0.0768\,i - 0.416 & 0.075 - 0.609\,i \\ 0.534\,i + 0.178 & 0.439\,i - 0.0566 & 0.183\,i - 0.122 & 0.105\,i - 0.655 \end{pmatrix}.$$

Calculando el número de veces que aparece Q, tenemos que la relación de Q la probabilidad es $\mu \approx 0.4852728392995$ y $\theta \approx 1.54133774484651$; esto implica que el número de iteraciones $K = 3$.

Necesitamos A matriz unitaria tal que: $A|0\rangle \approx \begin{pmatrix} 0.9498\,i - 0.07175 \\ 0.3689\,i + 0.1526 \\ 0.682\,i - 0.1161 \\ -0.08807\,i - 0.5832 \end{pmatrix}$. Verifiquemos el resultado con el número de iteraciones

$$\langle X|Q^3A|0\rangle \approx 7.3 \times 10^{-4}\,i + 7.8 \times 10^{-1}.$$

La probabilidad de observar $|X\rangle$ es aproximadamente $|\mu|^2 = 0.6023$.

Conclusión

El presente trabajo tuvo como objetivo el desarrollo del algoritmo de Grover, como un problema de búsqueda de soluciones en sistemas de ecuaciones lineales no homogéneos y singulares. Se hizo un análisis de la literatura sobre el tema y de los postulados matemáticos relacionados a la teoría de la computación cuántica.

Mencionamos tres ejemplos de ecuaciones lineales no homogéneas y singulares, para comprobar si nuestra aproximación al resultado es satisfactoria. Tuvimos una probabilidad de éxito mayor al 0.50, lo cual nos es favorable para nuestro trabajo.

A futuro queremos investigar ecuaciones cuyos coeficientes no sean idempotentes, por ejemplo tripotencia, tetrapotencia, etc.

Bibliografía

[1] G. Brassard, P. Hyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. *In AMS Contemporary Mathematics Millennium*, **305**:53–74, 2002.

[2] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Appeared in Proceedings of the Royal Society of London*, **400**:97–117, 1985.

[3] D. Deutsch and R. Jozsa. Rapid solutions of problems by quantum computation. *Proceedings of the Royal Society of London*, pages 439–354, 1992.

[4] R. P. Feynman. Simulating physics with computers. *International journal of theoretical physics*, **21**:467–488, 1982.

[5] L.K Grover. A fast quantum mechanical algorithm for database search. *Proceedings Annual ACM Symposium on the Theory of Computing*, page 212, May 1996.

[6] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*, volume **52**. Cambridge University Press, 2010.

[7] C.Bautista Ramos, C. Guillén Galván, and A. Rangel Huerta. From orthogonal projections to a generalized quantum search. *Quantum Information*, **12**:1–20, 2013.