



**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.

27 DE FEBRERO DEL 2015

Para mis padres con todo mi amor y gratitud.

Agradecimientos

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

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.

A mis profesores que son parte esencial de este logro.

Muy particularmente agradezco a mi asesor Dr. César Bautista Ramos por ser un gran maestro, investigador y un gran guía para culminar este último paso en mi carrera profesional.

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 regañándome cuando era necesario, y haciéndome pasar momentos inolvidables.

Contenido

Acronimos y Notación	iv
Introducción	1
Conceptos preliminares	3
1 Computación cuántica	5
1.1 Preliminares	5
1.2 Qubit cuántico	9
1.3 Axiomas de la computación cuántica	9
1.4 Productos tensoriales	14
2 Algoritmo de Deutsch	21
2.1 Compuerta cuántica	21
2.2 Entrelazamiento cuántico	25
3 Algoritmo de Deutsch-Jozsa	33
3.1 Evaluación balanceada	33
4 Algoritmo de Teleportación Cuántica	41
4.1 No-clonación	41
4.2 Compuerta controladas cuántica	42
5 Algoritmo de Grover	48
5.1 Funciones de orden	60
6 Generalización del algoritmo del Grover	63
6.1 Series formales	71
6.2 Ejemplos	77
Conclusión	81
Bibliografía	82

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 módulo 2 o or exclusivo.

Introducción

La computación cuántica tiene sus orígenes en ideas de Richard Feynman (premio Nobel en 1965) sobre la miniaturización de las computadoras [3].

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, además 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.

En el presente trabajo de tesis, identificamos a las matrices con sus operadores lineales asociados por multiplicación a la derecha.

Conceptos preliminares

El **traspuesto conjugado de una matriz** $A = (a_{ij}) \in \mathbb{C}$ es definido como $A^* = (\bar{a}_{ji})$, el traspuesto de A y todas las posiciones a_{ij} conjugadas.

La **matriz U es unitaria** si satisface algunas de las condiciones siguientes:

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

Sean $\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \vdots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$ matriz $n \times m$ y B otra matriz, se define el **producto de**

Kronecker de A con B como: $A \otimes_K B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nm}B \end{pmatrix}$.

Una matriz **Hermitiana** es una matriz cuadrada de elementos complejos que tiene la característica de ser igual a su propia traspuesta conjugada. Es decir, $a_{i,j} = \bar{a}_{j,i}$ o escrita como la traspuesta conjugada $A^* : A^* = A$.

Una matriz **idempotente** es una matriz la cual es igual a su cuadrado, es decir: $A^2 = A$

Sea V un espacio vectorial sobre K , n vectores v_1, \dots, v_n son **linealmente independientes** si $k_1v_1 + k_2v_2 + \dots + k_nv_n = 0$ implica que $(k_1, k_2, \dots, k_n) = (0, 0, \dots, 0)$, para $k_1, k_2, \dots, k_n \in K$.

Una **base** del espacio V es una familia de vectores $\beta = \{v_1, \dots, v_n\}$ tal que β es linealmente independiente y β genera V .

Capítulo 1

Computación cuántica

1.1 Preliminares

La computación cuántica es una forma radicalmente nueva de procesar información, posibilitada por propiedades exclusivas de la mecánica cuántica. Dentro de la computación cuántica se trabaja en \mathbb{C}^n como espacio de Hilbert [8].

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

1. Para todo $v, w_1, w_2 \in V$ y $\lambda, \mu \in \mathbb{C}$ se debe de cumplir que $v \cdot (\lambda w_1 + \mu w_2) = \lambda(v \cdot w_1) + \mu(v \cdot w_2)$ (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 es definitivamente positivo, es decir $v \cdot v \geq 0$, para todo $v \in V$, siendo $v \cdot v = 0$ si y sólo si $v = 0$.
4. El conjunto V 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 una estructura de \mathbb{C} espacio vectorial.

Demostración. Sea

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

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. El conjunto \mathbb{C}^n tiene la estructura de espacio de Hilbert complejo.

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

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

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

$$\begin{aligned} & \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \left(\lambda \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} + \mu \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \right) \\ &= \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} \lambda b_1 + \mu c_1 \\ \lambda b_2 + \mu c_2 \\ \vdots \\ \lambda b_n + \mu c_n \end{pmatrix} \\ &= a_1^*(\lambda b_1 + \mu c_1) + a_2^*(\lambda b_2 + \mu c_2) + \cdots + a_n^*(\lambda b_n + \mu c_n) \\ &= (\lambda a_1^* b_1 + \lambda a_2^* b_2 + \cdots + \lambda a_n^* b_n) + (\mu a_1^* c_1 + \mu a_2^* c_2 + \cdots + \mu a_n^* c_n) \\ &= \lambda(a_1^* b_1 + \cdots + a_n^* b_n) + \mu(a_1^* c_1 + \cdots + a_n^* c_n) \\ &= \lambda \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} + \mu \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}. \end{aligned}$$

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 definitivamente positivo:

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

Además, si suponemos 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 $a_1 = a_2 = \cdots = a_n = 0$, 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 (ket)** es un estado cuántico en un espacio de Hilbert y la mínima unidad de información cuántica. Matemáticamente es un vector de módulo uno, denotada con el símbolo $|\rangle$. Dos estados básicos son $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ y $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (se pronuncia ket unos y ket cero respectivamente). Un **bra** es el transpuesto conjugado del ket, su símbolo es $\langle|$.

Ejemplo 1.1. Si $|\alpha\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, entonces el bra $\langle\alpha| = (1 \ 0 \ 0)$. Por consiguiente la

operación ketbra de α es denotada $|\alpha\rangle\langle\alpha|$, que cumple $|\alpha\rangle\langle\alpha| = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} (1 \ 0 \ 0) =$

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ y la operación braket de α es denotada $\langle\alpha|\alpha\rangle$, que cumple $\langle\alpha|\alpha\rangle =$
 $(1 \ 0 \ 0) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 1$

1.3 Axiomas de la computación cuántica

En general, una teoría formal comienza con la formulación de axiomas [3]. 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 está 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 1.2. El vector $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2$ es un estado puro, pues $\| \begin{pmatrix} 1 \\ 0 \end{pmatrix} \| = \sqrt{\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \sqrt{1+0} = 1$. También $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$ es un estado puro, porque $\| \begin{pmatrix} 0 \\ 1 \end{pmatrix} \| = \sqrt{\begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}} = \sqrt{0+1} = 1$. Otro ejemplo es el vector $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \in \mathbb{C}^2$ que una vez

más es un estado puro: $\| \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \| = \sqrt{\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}} = \sqrt{\frac{1}{2} + \frac{1}{2}} = 1$.

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

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, \dots, m_n posibles mediciones de un experimento de un sistema cuántico, entonces las mediciones (observaciones) cuánticas están descritas por una colección de matrices $M_{m_1}, M_{m_2}, \dots, M_{m_n}$ actuando sobre el espacio de estados, tales que $M_{m_1}M_{m_1}^* + M_{m_2}M_{m_2}^* + \dots + M_{m_n}M_{m_n}^* = Id$, la cual es llamada la *ecuación de completitud* (esto es, donde Id es la matriz identidad y M^* es la transpuesta conjugada de M).

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 $\langle \psi | = |\psi\rangle^*$, $i = 1, \dots, n$ y el estado del sistema se colapsa (después de la medición).

Es común denotar, los vectores no cero con $|v\rangle \in \mathbb{C}^n$. Si 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 una matriz unitaria.

Ejemplo 1.3. La matriz

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

es una matriz unitaria, por que 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 más adelante). Además, supóngase que se tiene la máquina (sistema) con estado inicial $|\psi_0\rangle = |0\rangle$, en el cual podemos usar el axioma(1.1). Ahora le aplicamos la máquina de evolución descrita por W , entonces el estado cambia, es decir;

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

Esquématicamente tenemos el siguiente circuito:

$$|0\rangle \text{ --- } \boxed{W} \text{ --- } \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right)$$

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:

$$|\psi_0\rangle = |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- 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: $|\psi_0\rangle = |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

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

$$\begin{aligned} M_0^*M_0 + M_1^*M_1 &= M_0M_0 + M_1M_1 \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

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

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

Además el sistema se colapsa a $\frac{1}{\sqrt{p_0}} M_0 | \psi_1 \rangle = \sqrt{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |0\rangle$.

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 completitud.

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

b) $\langle\psi|\psi\rangle = (a_1^*, a_2^*, \dots, a_n^*) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = a_1^* a_1 + a_2^* a_2 + \dots + a_n^* a_n = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \|\psi\|^2$.

□

Observación 1.2. En general, es mejor tener las propiedades de un objeto en sí. Por ejemplo: en lugar de tener $a = 1.41423\dots$ 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 $|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1, 0) = M_0$ y $|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0, 1) = M_1$.

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 $\langle 0|0\rangle = \|\lvert 0\rangle\|^2 = 1$ 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 $\alpha|\psi_1\rangle + |\psi_2\rangle$.

Así las fases globales en mecánica cuántica se desprecian.

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: $Vect_{\mathbb{C}}$. En $Vect_{\mathbb{C}}$ el producto tensorial es un objeto que resuelve las siguientes propiedades universales:

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

$$\begin{array}{ccc}
 V \times W & \xrightarrow{f} & U \\
 \downarrow \otimes & \nearrow \tilde{f} & \\
 V \otimes W & &
 \end{array}$$

Teorema 1.3. El producto tensorial existe en $Vect_{\mathbb{C}}$.

Demostración. Sean $V, W \in Vect_{\mathbb{C}}$, 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

$$\begin{aligned}
 &(v, \lambda w_1 + \mu w_2) - \lambda(v, w_1) - \mu(v, w_2), \\
 &(\lambda v_1 + \mu v_2, w) - \lambda(v_1, w) - \mu(v_2, w).
 \end{aligned}$$

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 $\rho : R \rightarrow R/S = T$ y $r \mapsto [r] = r + S$. Luego se define el tensor $\otimes : V \times W \rightarrow T$ 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 $v \otimes w := \otimes[(v, w)]$. \square

Afirmación 1.1. El \otimes es bilineal.

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

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

Por lo tanto $v \otimes (\lambda w_1 + \mu w_2) = \lambda(v \otimes w_1) + \mu(v \otimes w_2)$. Así \otimes es lineal derecho. De forma análoga es lineal izquierdo. Por lo cual concluimos que \otimes es bilineal. \square

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

$$\begin{array}{ccc} V \times W & \xrightarrow{f} & U \\ \downarrow \otimes & \nearrow \tilde{f} & \\ V \otimes W = R/S & & \end{array}$$

Demostración. Sea $g : R \rightarrow U$ 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:

$$\begin{aligned} g((\lambda v_1 + \mu v_2, w) - \lambda(v_1, w) - \mu(v_2, w)) &= g(\lambda v_1 + \mu v_2, w) - \lambda g(v_1, w) - \mu g(v_2, w) \\ &= f(\lambda v_1 + \mu v_2, w) - \lambda f(v_1, w) - \mu f(v_2, w) \\ &= 0. \end{aligned}$$

En los otros generadores es análogo.

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

$$\begin{array}{ccc}
 R & \xrightarrow{f} & U \\
 \downarrow g & & \nearrow \tilde{f} \\
 R/S & &
 \end{array} \tag{1.1}$$

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

Ahora veamos que el diagrama (1.1) conmuta:

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

□

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

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

$$\begin{array}{ccc}
 V \times W & \xrightarrow{f} & U \\
 \downarrow \otimes & & \nearrow h \\
 V \otimes W & &
 \end{array}$$

Sea $z \in V \otimes W = R/S$, luego $z = [r]$ con $r \in R$ pero R es el espacio vectorial complejo con base $\{(v, w) | v \in V, w \in W\}$. Entonces $z = [\lambda_1(v_1, w_1) + \dots + \lambda_k(v_k, w_k)] = \lambda_1[(v_1, w_1)] + \dots + \lambda_k[(v_k, w_k)] = \lambda_1 v_1 \otimes w_1 + \dots + \lambda_k v_k \otimes w_k$.

De lo cual tenemos

$$\begin{aligned}
 h(z) &= h(\lambda_1(v_1 \otimes w_1) + \cdots + \lambda_k(v_k \otimes w_k)) \\
 &= \lambda_1 h(v_1 \otimes w_1) + \cdots + \lambda_k h(v_k \otimes w_k) \quad \text{pues } h \text{ es lineal} \\
 &= \lambda_1 f(v_1, w_1) + \cdots + \lambda_k f(v_k, w_k) \quad \text{pues } h \text{ conmuta el diagrama} \\
 &= \lambda_1 \tilde{f}(v_1 \otimes w_1) + \cdots + \lambda_k \tilde{f}(v_k \otimes w_k) \quad \text{pues } \tilde{f} \text{ conmuta el diagrama (1.1)} \\
 &= \tilde{f} \lambda_1(v_1 \otimes w_1) + \cdots + \tilde{f} \lambda_k(v_k \otimes w_k) \quad \text{pues } \tilde{f} \text{ es lineal} \\
 &= \tilde{f}(z).
 \end{aligned}$$

Por lo tanto $h(z) = \tilde{f}(z)$, para todo z en $V \otimes W$, de ahí que, \tilde{f} es única. \square

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

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

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

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

2. Tenemos que el producto de tensores

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

$$\begin{aligned}
 &= (b_1 d_1)^* a_1 c_1 + \cdots + (b_1 d_t)^* a_1 c_s + \cdots + \\
 &(b_m d_1)^* a_n c_1 + \cdots + (b_m d_t)^* a_n c_s \\
 &= b_1^* a_1 (d_1^* c_1 + \cdots + d_t^* c_s) \\
 &+ \cdots + b_m^* a_n (d_1^* c_1 + \cdots + d_t^* c_s) \\
 &= (b_1^* a_1 + \cdots + b_m^* a_n) (d_1^* c_1 + \cdots + d_t^* c_s) \\
 &= (b_1^*, \dots, b_m^*) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} (d_1^*, \dots, d_t^*) \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} \\
 &= \langle \varphi_2 | \varphi_1 \rangle \langle \psi_1 | \psi_2 \rangle
 \end{aligned}$$

□

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 $B = \{0, 1\}$, $f : B \rightarrow B$ 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 algoritmo hace uso de los siguientes elementos: compuerta cuántica, entrelazamiento cuántico, entre otros.

2.1 Compuerta cuántica

Una *compuerta cuántica*[8] es un dispositivo capaz de realizar operaciones unitarias sobre los qubits (Deutsch, 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 transformación : $U_f : \mathbb{C}^2 \otimes \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$.

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.

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

donde \oplus es la suma módulo 2.

Ejemplo 2.2. Tenemos que la suma módulo 2:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Los siguientes lema y teorema, son hechos bien conocidos en Álgebra Lineal [4].

Lema 2.1. La matriz U_f es matriz unitaria.

Teorema 2.1. Sea A una matriz $n \times n$ compleja. Entonces A es unitaria si y sólo si A mapea 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:

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

Tenemos varios casos:

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

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 $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$ con ella misma, por consiguiente U_f es matriz unitaria. □

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

$$\begin{aligned} U_f(|0\rangle \otimes |0\rangle) &= |0\rangle \otimes |f(0)\rangle = |0\rangle \otimes |1\rangle, \\ U_f(|0\rangle \otimes |1\rangle) &= |0\rangle \otimes |1 + f(0)\rangle = |0\rangle \otimes |0\rangle, \\ U_f(|1\rangle \otimes |0\rangle) &= |1\rangle \otimes |0\rangle = |1\rangle \otimes |0\rangle, \\ U_f(|1\rangle \otimes |1\rangle) &= |1\rangle \otimes |1 + 0\rangle = |1\rangle \otimes |1\rangle. \end{aligned}$$

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 $U_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Utilizando el producto de *kroncker* demostraremos la proposición siguiente.

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

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

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

□

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. Se cumple que $|w\rangle \neq |v\rangle \otimes |u\rangle$ 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 $|w\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$

$$= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

$$\Rightarrow ac = \frac{1}{\sqrt{2}} \Rightarrow dac = \frac{d}{\sqrt{2}}$$

$$\Leftrightarrow ad = 0, bc = 0, bd = \frac{1}{\sqrt{2}} \Rightarrow 0 = \frac{1}{\sqrt{2}}.$$

Por lo tanto se obtiene 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 Hilbert H se encuentra entrelazado si no puede ser escrito 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 $|w\rangle = |u\rangle \otimes |v\rangle$ 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 $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |1\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle$, $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle - \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$ 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. \square

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

Demostración.

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

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

$$\begin{aligned}
 & \text{y por último } (Id \otimes M_1)^*(Id \otimes M_1) + \dots + (Id \otimes M_m)^*(Id \otimes M_m) \\
 &= (Id^* \otimes M_1^*)(Id \otimes M_1) + \dots + (Id^* \otimes M_m^*)(Id \otimes M_m) \\
 &= (Id \otimes M_1^*M_1) + \dots + (Id \otimes M_m^*M_m)
 \end{aligned}$$

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

□

Definición 2.2. Si M_1, \dots, M_m son matrices de medición actuando sobre \mathbb{C}^n y se considera además 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 $M_1 \otimes Id, \dots, M_m \otimes Id$, similarmente se dice que se observa (mide) el segundo sistema cuando se usan $Id \otimes M_1, \dots, Id \otimes M_m$ (M_1, \dots, 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:

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

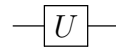
Observación 2.2. Un espacio (de estados) muy usual es del tipo $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$.

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 más significativo, significa medir el primer qubit. El menos significativo, significa usar el n -ésimo qubit.

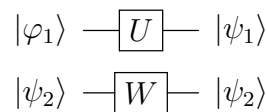
Observación 2.3. Si U es matriz unitaria, ésta se acostumbra dibujar como un circuito:



y la evolución por esta se dibuja:

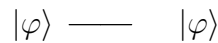


Ademas, si W es una segunda matriz unitaria, el producto tensorial $U \otimes W$ se representa por:



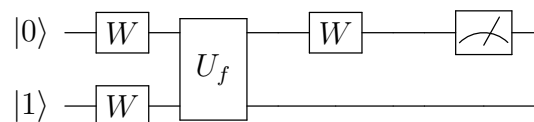
donde $(U \otimes W)(|\varphi_1\rangle \otimes |\varphi_2\rangle) = |\psi\rangle$ es decir $U|\varphi_1\rangle \otimes W|\varphi_2\rangle = |\psi_1\rangle$.

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

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

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

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

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

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

luego $|\psi_3\rangle = (W \otimes Id)|\psi_2\rangle$

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

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

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: $(-1)^{f(0)}(\langle 0| \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}})$ 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:

$$\begin{aligned} p_2 &= \langle\psi_3|(p_2 \otimes Id)^*(p_2 \otimes Id)|\psi_3\rangle \\ &= \langle\psi_3|(p_1 \otimes Id)(p_2 \otimes Id)|\psi_3\rangle \end{aligned}$$

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

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 conclusión: 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 Deutsch-Jozsa

El algoritmo de Deutsch-Jozsa [9] 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) $f(x_1, x_2, \dots, x_n)$ que toma n bits de entrada x_1, x_2, \dots, x_n y devuelve un valor binario $f(x_1, x_2, \dots, x_n)$. 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 $f : B \times \dots \times B \rightarrow B$ función donde $B = \{0, 1\}$ (i.e $f = f(x_1, \dots, x_n)$ función booleana de aridad n). Supongase además que f es una de dos: constante o balanceada.

Problema 3.1.Cuál de estas posibilidades es f con sólo dos llamadas a f (dos “evaluaciones” de f).

3.1 Evaluación balanceada

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

Ejemplo 3.1. En la siguiente tabla se 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 $f(x_1, x_2, x_3) = (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3)$.

Como observamos en la tabla, la función es balanceada .

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 tautologías o contradicciones.

Una vez más, en este problema se supone que f es una caja negra: uno no tiene acceso a la fórmula de la función, sólo se tiene derecho a hacer evaluación de esta.

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}^{2^n} (ie. K es una cadena de ceros y unos de longitud n) 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 cero y uno), con $W^{\otimes n} = \underbrace{W \otimes W \otimes \dots \otimes W}_n$ y $K \cdot u = k_1 u_1 + \dots + k_n u_n$ donde a su vez $K = (k_1, \dots, k_n)$, $u = (u_1, \dots, u_n)$ con $k_i, u_i \in \{0, 1\}$, $i = \{1, \dots, n\}$.

Demostración. Sea

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

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

□

Para el algoritmo de Deutsch-Jozsa utilizamos la matriz de *Pauli*.

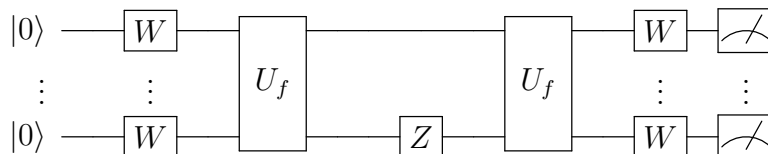
Definición 3.2. La matriz $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ se llama *matriz zeta de Pauli*. Tal matriz

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 una generalización de la compuerta U_f de dos qubits que definimos en el algoritmo de Deutsch (2.1).

En el algoritmo de Deutsch-Jozsa, la compuerta U_f está compuesta de $n + 1$ qubits. Si $k_1, \dots, k_n, \in \{0, 1\}$, entonces se define $U_f|k_1 \dots k_n k_{n+1}\rangle = |k_1 \dots k_n\rangle \otimes |f(k_1 \dots k_n) \oplus k_{n+1}\rangle$ 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 función $f(x_1, x_2, \dots, x_n)$.

Salida: Si el vector es igual a $\underbrace{|0, \dots, 0\rangle}_n$ entonces f es balanceada, en otro caso un vector diferente de $|0, \dots, 0\rangle$ no es balanceada.

1: Se prepara el sistema con estado inicial:

$$|\psi_0\rangle = |0 \dots 0\rangle.$$

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

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

3: Se aplica U_f al estado anterior:

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

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

$$|\psi_3\rangle = \underbrace{(Id \otimes \dots \otimes Id)}_n \otimes Z|\psi_2\rangle.$$

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 (1.1), nuestro estado inicial es: $|\psi_0\rangle = |0 \dots 0\rangle$.

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

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

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:

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

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

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

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

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

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

Luego para f tenemos tres casos:

1. Si $f \equiv 0$, el módulo al cuadrado del coeficiente de $\underbrace{|0 \dots 00\rangle}_n$ en $|\psi_5\rangle$ es $|\frac{1}{2^n} 2^n|^2 = 1$, entonces $|0 \dots 00\rangle$ se observa con probabilidad 1.
2. Si $f \equiv 1$, el coeficiente de $|0 \dots 00\rangle$ es $\frac{1}{2^n}(-2^n) = -1$ por consiguiente, la probabilidad de observar $|0 \dots 00\rangle$ es $|-1|^2 = 1$.
3. Si f es balanceada: el coeficiente de $|0 \dots 00\rangle$ es 0, la probabilidad de observar $|0 \dots 00\rangle$ es cero.

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

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

Proposición 3.1. Sean $|0\rangle, |1\rangle, \dots, |2^n - 1\rangle$ elementos de la base del cálculo. Supóngase que el estado $|\psi\rangle = a_0|0\rangle + a_1|1\rangle + \dots + a_{2^n-1}|2^n - 1\rangle$ se observa con respecto a ésta base canónica. Entonces $|\psi\rangle$ se colapsa al estado $|i\rangle$ con probabilidad $|a_i|^2$, $i = 0, \dots, 2^n - 1$, donde $|0\rangle = \underbrace{|0 \dots 0\rangle}_n$, $|1\rangle = |0 \dots 01\rangle, |2\rangle = |0 \dots 10\rangle, \dots, |2^n\rangle = |1 \dots 1\rangle$.

Demostración. Por definición, las matrices de medición que se usan, son las proyecciones canónicas. Tales satisfacen la ecuación de completéz. 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

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

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 $|1\rangle, |2\rangle, \dots, |2^n - 1\rangle$. □

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

Observación 3.2. Sea $|\psi\rangle \in \mathbb{C}^2$ de norma uno con $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ y $a, b \in \mathbb{C}$. Entonces $\| |\psi\rangle \| = \sqrt{|a|^2 + |b|^2} = 1$, 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 $|e^{i\theta}| = \cos^2\theta + \sin^2\theta = 1$, por 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 $|\psi\rangle = \cos(\beta/2)|0\rangle + \sin(\beta/2)e^{i\alpha}|1\rangle$, que da origen a la llamada *esfera de Bloch*.

Capítulo 4

Algoritmo de Teleportación Cuántica

La teleportación es una tecnología 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 energía 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.

Por otro lado, si enviamos un qubit, 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 [8].

Para cumplir este objetivo utilizamos las compuertas.

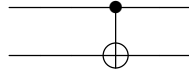
4.2 Compuerta controladas cuántica

La compuerta Pauli- X es conocida también como la compuerta NOT cuántica, ya que trasforma $|0\rangle \rightarrow |1\rangle$ y $|1\rangle \rightarrow |0\rangle$. Denotada como: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

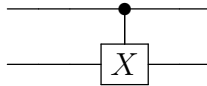
Observación 4.1. Si $U : \mathbb{C}^N \rightarrow \mathbb{C}^N$ (U es $N \times N$) es matriz unitaria cualquiera entonces se define la matriz control- U denotada $C(U) = \lambda(U)$ como la matriz $C(U) : \mathbb{C}^2 \otimes \mathbb{C}^N \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^N, |j\rangle$ en la base del cálculo 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. Consideremos la matriz $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $X : \mathbb{C}^2 \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$. Entonces la matriz $C(X) : \mathbb{C}^2 \otimes \mathbb{C}^2 \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$, cumple $C(X)(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$, $C(X)(|1\rangle \otimes |0\rangle) = |1\rangle \otimes X|0\rangle = |1\rangle \otimes |1\rangle$.

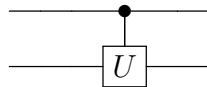
Diagramáticamente $C(X)$ se representan como:



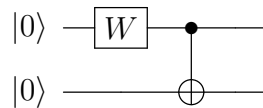
o bien



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: 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:

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

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

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

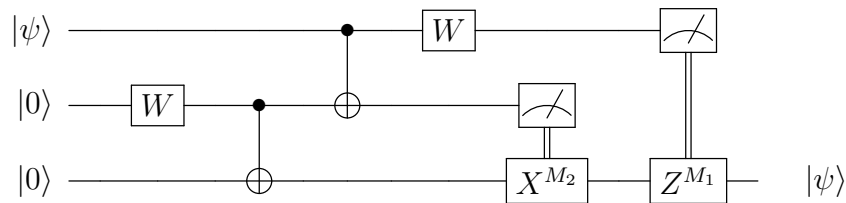
Tal $|B_{00}\rangle$ es un estado llamado *EPR* (Einstein, Podolski y Rosen). De forma análoga se define los demás estados EPR: $|B_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$, $|B_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ y $|B_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$.

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

A la parte A se le llama Alicia y a la parte B se le llama Beto.

Consideremos el siguiente circuito para la solución del problema 4.2



El circuito describe el algoritmo de teleportación cuántica.

Algoritmo 4.1 Algoritmo de teleportación 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: Beto observa el sistema: observa M_2 , el bit correspondiente al qubit del canal compartido; y Alicia observa M_1 que es el qubit correspondiente al qubit de su canal. Alicia envía M_1 a Beto por una canal clásico.

5: Beto aplica X^{M_2} y luego Z^{M_1} al qubit de su canal.

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 control-not $C(X)$ al 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.

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

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 $|M_1\rangle$ el qubit observado por Alicia. 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.

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

Dividimos el análisis en los casos dados en la siguiente tabla:

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

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 X para obtener $a|0\rangle + b|1\rangle$. Luego Beto le aplica $Z^0 = Id$ para finalmente obtener $|\psi\rangle = a|0\rangle + b|1\rangle$ en su canal privado.

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, el qubit $|\psi\rangle$ que originalmente tiene Alicia, al final del procedimiento lo obtiene Beto.

Capítulo 5

Algoritmo de Grover

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

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

$$f(x_1, \dots, x_n) = 1 \Leftrightarrow x_1 = b_1, x_2 = b_2, \dots, x_n = b_n$$

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

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

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

Observación 5.1. La mejor estrategia conocida clásicamente, es hacer una búsqueda exhaustiva, que usa $\frac{2^n}{2}$ evaluaciones de f (en promedio). Se puede hacer una búsqueda exhaustiva cuántica, que usa $\sqrt{2^n} = 2^{\frac{n}{2}}$ evaluaciones de f aproximadamente. Se 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 usan sólo 100 evaluaciones de f .

Observación 5.2. Sea $f(x_1, \dots, x_n)$ función booleana de aridad n . Esta función se puede realizar cuánticamente como una matriz unitaria U_f , de la forma siguiente: definimos una transformación lineal $U_f : \mathbb{C}^{2^n} \otimes \mathbb{C}^2 \rightarrow \mathbb{C}^{2^n} \otimes \mathbb{C}^2$ mediante la siguiente:

$$U_f(|x_1 \cdots x_n\rangle \otimes |y\rangle) = |x_1 \cdots x_n\rangle \otimes |f(x_1, \dots, x_n)\rangle \oplus |y\rangle \quad (5.1)$$

donde y es 0 ó 1 y cada x_i , $i = 1, \dots, n$ 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 $\mathbb{C}^{2^{n+1}}$.

Teorema 5.1. Si definimos $\tilde{U} = (Id^{\otimes n} \otimes W)U_f(Id^{\otimes n} \otimes W)$, entonces $\tilde{U}(|x_1, \dots, x_n\rangle \otimes |1\rangle) = (-1)^{f(x_1, \dots, x_n)}|x_1, \dots, x_n\rangle \otimes |1\rangle$ para todo $|x_1, \dots, x_n\rangle$ en la base del cálculo.

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

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

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

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

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

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

$$(Id \otimes W)U_f(Id \otimes W)|x_1, \dots, x_n 1\rangle = (-1)^{f(x_1, \dots, x_n)}|x_1, \dots, x_n 1\rangle. \quad (5.2)$$

□

De la ecuación 5.2, tenemos que $|x_1, \dots, x_n 1\rangle$ 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 (5.2):

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 $(Id \otimes W)U_f(Id \otimes W)|x_1, \dots, x_n 1\rangle = |x_1, \dots, x_n 1\rangle$.

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 $U_f|x_1, \dots, x_n\rangle = (-1)^{f(x_1, \dots, x_n)}|x_1, \dots, x_n\rangle$.

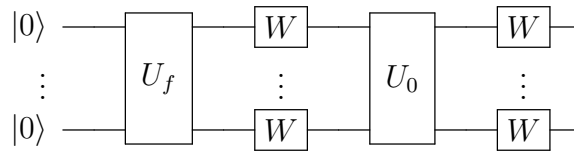
Definición 5.1. Sea $g(x_1, \dots, x_n)$ la siguiente función booleana

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

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 la ecuación 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 $Q = W^{\otimes n}U_0W^{\otimes n}U_f$.

El algoritmo de Grover, tiene el siguiente diagrama:



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

Teorema 5.2. Sea $Q = W^{\otimes n}U_0W^{\otimes n}U_f$ y

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

para todo x en la base del calculo de $\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$. Además, sea $|b\rangle = \frac{1}{\sqrt{2^n}}|b_1, \dots, b_n\rangle$ donde $f^{-1}(1) = (b_1, \dots, b_n)$ 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

$$Q|b\rangle = \left(\frac{1}{2^{n-1}} - 1\right)|b\rangle + \frac{1}{2^{n-1}}|m\rangle \tag{5.3}$$

$$Q|m\rangle = 2\left(\frac{1}{2^n} - 1\right)|b\rangle + \left(\frac{2}{2^n} - 1\right)|m\rangle. \tag{5.4}$$

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

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

De forma análoga tenemos:

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

□

Para “facilitar” cálculos se normalizarán los vectores, por el teorema 5.2, tenemos $|b\rangle = \frac{1}{\sqrt{2^n}} |b_1 \cdots b_n\rangle$ donde $f^{-1}(1) = \{(b_1, \dots, b_n)\}$, calculando su norma:

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

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

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

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

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

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

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

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

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

En resumen, hemos obtenido que:

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

Multiplicamos ambas ecuaciones anteriores por -1 para obtener:

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

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

Teorema 5.3. Se cumple 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 $S = \text{span}\{|M\rangle, |B\rangle\}$.

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, donde $\theta = \arcsin\left(\frac{\sqrt{2^n - 1}}{2^{n-1}}\right)$.

Teorema 5.4. (Espectral)[4] Si A es normal entonces existe una matriz unitaria U tal que UAU^{-1} es diagonal:

$$UAU^{-1} = \begin{pmatrix} \xi_1 & 0 & \dots & 0 \\ 0 & \xi_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \xi_n \end{pmatrix}.$$

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

diagonal de la forma

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

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

Demostración. Tenemos:

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

Para continuar usamos números complejos:

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

según la identidad de Euler. 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: $\sqrt{1 - \frac{1}{2^n}} + i \frac{1}{\sqrt{2^n}} = e^{i\frac{\theta}{2}} = \cos(\frac{\theta}{2}) + i \sin(\frac{\theta}{2})$,

lo que implica que $\cos(\frac{\theta}{2}) = \sqrt{1 - \frac{1}{2^n}}$ y

$$\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{2^n}}. \quad (5.5)$$

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

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: Calcular $k = \lceil \frac{\pi}{2\theta} + \frac{1}{2} \rceil$. Repetir $k + 1$ veces:

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:

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

donde éstas son coordenadas relativas a la base $\{|M\rangle, |B\rangle\}$. De forma análoga con los siguientes estados:

$$\begin{aligned}
 |\psi_3\rangle &= Q|\psi_2\rangle \\
 &\equiv (-1)Q|\psi_2\rangle \\
 &= \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \frac{\theta}{2} \\ \sin \frac{\theta}{2} \end{pmatrix} \\
 &= \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} \begin{pmatrix} \cos \frac{\theta}{2} \\ \sin \frac{\theta}{2} \end{pmatrix}
 \end{aligned}$$

⋮

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

Luego; la probabilidad de éxito de obtener $|B\rangle$ es $\sin^2(\theta(k - \frac{1}{2}))$ después de k iteraciones de Q , luego se quiere que $\sin^2(\theta(k - \frac{1}{2})) = 1$, lo cual sugiere poner $\theta(k - \frac{1}{2}) = \frac{\pi}{2}$, es decir $k = \frac{\pi}{2\theta} + \frac{1}{2}$, pero como k generalmente no es un número entero, es mejor poner $\lceil \frac{\pi}{2 \arcsin \frac{\sqrt{2^n-1}}{2}} + \frac{1}{2} \rceil$ 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 una función.

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

- 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 “ $f(n)$ está 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 $N = 1$, 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 $n \rightarrow \infty$), 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 formalizaremos tales aproximaciones.

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 (5.5), entonces $\theta = 2 \arcsin(\frac{1}{\sqrt{2^n}})$. Además, si $0 \leq x \leq \pi$, tendremos que $0 \leq \sin x \leq x$. Como $0 < \frac{1}{\sqrt{2^n}} < \pi$, 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 $1 \leq (\frac{\pi+\theta}{2\theta}) \leq \frac{\pi}{2}\sqrt{2^n}$, pues $2\theta \leq \pi + \theta$ y $\theta \leq \pi$. Por otro lado, 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 $0 < x < \frac{\pi}{2}$, entonces $0 < x < \tan(x) = \frac{\sin(x)}{\cos(x)}$, luego $x \cos(x) < \sin(x)$. En particular si $0 < x = \frac{\theta}{2} \leq \frac{\pi}{4} < \frac{\pi}{2}$, por consiguiente $\frac{\theta}{2} \cos(\frac{\theta}{2}) < \sin(\frac{\theta}{2})$, luego $\frac{\theta}{2}\sqrt{1 - \frac{1}{2^n}} < \sqrt{\frac{1}{2^n}}$ y despejando $\theta < \frac{2\sqrt{\frac{1}{2^n}}}{\sqrt{1 - \frac{1}{2^n}}} = \frac{2}{\sqrt{2^n-1}}$.

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 $k \in \Theta(\sqrt{2^n})$.

□

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

$$P|X\rangle = |b\rangle, \quad (6.1)$$

donde P es hermitiana e idempotente .[7]

Generalmente, las matrices idempotentes 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 $P^2 = P$, 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 indica que P es singular o P es invertible.

Si P invertible, como $P^2 = P$ se sigue que $P^{-1}P^2 = P^{-1}P$, así $P = I$, entonces P es singular o $P = I$. □

Observación 6.1. 1. Consideremos la ecuación del tipo $P|X\rangle = |b\rangle$ en casos no triviales, es decir $P \neq I$ y $P \neq 0$.

2. Queremos encontrar un algoritmo cuántico que resuelve la ecuación 6.1.
3. Si A matriz cuadrada compleja, se define la exponencial e^A como $e^A := \sum_{n=0}^{\infty} \frac{1}{n!} A^n = \lim_{k \rightarrow \infty} \sum_{n=0}^k \frac{1}{n!} A^n$
4. Si la matriz A es diagonalizable. Existe T matriz invertible tal que

$$A = T \begin{pmatrix} \xi_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \xi_m \end{pmatrix} T^{-1},$$

entonces

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

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

Ejemplos 6.1. 1. Si la matriz $\begin{pmatrix} \xi_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \xi_n \end{pmatrix}$ es diagonal, entonces A es normal, pues

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

y por otro lado tenemos

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

2. Si A es hermitiana, entonces A es normal, pues de $A = A^*$ se obtiene $AA^* = AA = A^2 = A^*A$.

3. Si A es unitaria, entonces A es normal, por 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 y 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 $|\xi|^2\langle v|v\rangle = \langle v|v\rangle$, 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 5.4), tenemos que

$$WUW^{-1} = \begin{pmatrix} \xi_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \xi_n \end{pmatrix} = \begin{pmatrix} e^{i\theta_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{i\theta_n} \end{pmatrix} = e^{iH_0},$$

donde $H_0 = \begin{pmatrix} \theta_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \theta_n \end{pmatrix}$. Luego $H = W^{-1}H_0W$, la cual es hermitiana (porque $H^* = (W^{-1}H_0W)^* = W^{-1}H_0W = H$), cumple que $U = W^{-1}e^{iH_0}W = e^{iH}$.

(\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 unitaria. \square

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 $0 < \phi, \varphi < 2\pi$, entonces $Q(\phi, \varphi, \rho) = e^{i\phi\rho}e^{i\varphi|X\rangle\langle X|}$ es 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 $|X\rangle, P|X\rangle, P^2|X\rangle, P^3|X\rangle, \dots$, es decir $S = \text{span}\{|X\rangle, P|X\rangle\} = \{z_1|X\rangle + z_2P|X\rangle | z_1, z_2 \in \mathbb{C}\}$. 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

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

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

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

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

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 $|\psi_0\rangle = P|X\rangle - \mu|X\rangle$, 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 $\mu \leq 1$. □

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

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

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

$$z_1 |X \rangle + z_2 P |X \rangle = 0. \quad (6.2)$$

Por demostrar que $z_1 = z_2 = 0$. Multiplicamos por $\langle X |$ a la izquierda de ambos lados 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 obtiene 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 la siguiente ecuación $z_1 + \mu z_2 = 0$ y $\mu z_1 + \mu z_2 = 0$, cuya matriz de coeficientes tiene determinante $\begin{vmatrix} 1 & \mu \\ \mu & \mu \end{vmatrix} = \mu - \mu^2 = \mu(1 - \mu) \neq 0$, entonces $z_1 = z_2 = 0$. Por lo tanto $|X \rangle, P |X \rangle$ son linealmente independientes.

□

La cantidad $\mu = \langle X | P |X \rangle = \langle P \rangle_X = E(P)$ es conocida como el valor promedio del observable P sobre el vector $|X \rangle$.

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

$$\begin{pmatrix} 1 & 0 \\ e^{i\phi} - 1 & e^{i\phi} \end{pmatrix}.$$

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 $P^2|X\rangle = 0|X\rangle + 1P|X\rangle$, es decir $P = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Pero $e^{i\phi P} = Id + (e^{i\phi} - 1)P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (e^{i\phi} - 1) \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ e^{i\phi} - 1 & 1 + (e^{i\phi} - 1) \end{pmatrix}$. □

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 además $S = \text{span}\{|X\rangle, P|X\rangle\}$.

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

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 $Q = e^{i\phi P} e^{i\varphi|X\rangle\langle X|}$ 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 las proposiciones (6.3) y (6.4), tenemos que

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

□

En lo que sigue, queremos ajustar, ϕ, φ, n tales que $Q^n A|0\rangle = |X\rangle$, donde $A|0\rangle = \frac{1}{\| |b\rangle \|} |b\rangle$.

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

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

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

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

Ahora;

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

La expresión anterior es útil pues:

$$\begin{aligned} Q^n A|0\rangle &= \alpha_n |X\rangle + \beta_n P|X\rangle \\ &= \alpha_n |X\rangle + \beta_n (|\sigma\rangle + \mu|X\rangle) \\ &= (\alpha_n + \beta_n \mu) |X\rangle + \beta_n |\sigma\rangle \end{aligned}$$

donde $|\sigma\rangle = P|X\rangle - \mu|X\rangle$ y $\langle X|\sigma\rangle = 0$. Luego, la probabilidad de observar $|X\rangle$ en Q^n es $|\langle X|Q^n A|0\rangle|^2 = |(\alpha_n + \beta_n \mu)|^2$, lo cual queremos que cumpla $|\langle X|Q^n A|0\rangle|^2 = 1$. Para continuar haremos uso de series formales con coeficiente complejo.

6.1 Series formales

Las series formales son de gran importancia en el estudio de la probabilidad de éxito del algoritmo que se está estudiando.

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

Definición 6.4. Si $f : \mathbb{N} \rightarrow R$ y $g : \mathbb{N} \rightarrow R$. El conjunto de las series formales, denotado por $R[[z]]$, tiene operaciones de suma y producto definidas por:

$$\begin{aligned} (\text{Suma}) \quad f + g : \mathbb{N} \rightarrow R, \quad (f + g)(n) &= f(n) + g(n), \\ (\text{Producto}) \quad f * g : \mathbb{N} \rightarrow R, \quad (f * g)(n) &= \sum_{\substack{i,j \\ i+j=n}} f(i)g(j). \end{aligned}$$

Notación: Si $f : \mathbb{N} \rightarrow R$ 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 $h, s, t \in R[[z]]$.

1. Por demostrar que existe $(h + s) \in R[[z]]$. Sean $h, s \in R$. Se define $h + s : \mathbb{N} \rightarrow R$, $(h + s)(n) = h(n) + s(n)$. Como $h(n) \in R[[z]]$ y $s(n) \in R[[z]]$, entonces $h(n) + s(n) \in R$, así $(h + s) \in R[[z]]$.

2. Por demostrar $(h + s) + t = h + (s + t)$. Por definición:

$$[(h+s)+t](n) = (h+s)(n)+t(n) = [h(n)+s(n)]+t(n) = h(n)+[s(n)+t(n)] = h(n) + (s+n)(n) = [h + (s + t)](n), \text{ para cualquier } n \in \mathbb{N}. \text{ De donde se sigue que } (h + s) + t = h + (s + t).$$

3. Por demostrar $h + s = s + h$. Como $(h + s)(n) = h(n) + s(n) = s(n) + h(n) = (s + h)(n)$, para todo $n \in \mathbb{N}$, se obtiene $h + s = s + h$.

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

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 $h + \mathbf{0} = h$.

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

Se define $-h : \mathbb{N} \rightarrow R$, $(-h)(n) = -h(n)$. 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, $g * h$ esta en $R[[z]]$.

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

Ahora bien $(g * h)(n) = \sum_{i+j=n}^{i,j} g(i)h(j)$. Como $g(i) \in R$ y $h(j) \in R$, entonces $g(i)h(j) \in R$, así $(g * h) \in R[[z]]$.

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

Sea $h, s, t \in R[[z]]$. Ahora bien $(h * (s * t))(n) = \sum_{i+j=n}^{i,j} h(i)(s * t)(j) = \sum_{i+j=n}^{i,j} h(i) \left(\sum_{a+b=j}^{i,j} s(a)t(b) \right) = \sum_{i+j=n}^{i,j} \sum_{a+b=j}^{i,j} h(i)(s(a)t(b)) = \sum_{i+a+b=n}^{i,j} h(i)(s(a)t(b)) = \sum_{i+a+b=n}^{i,j} (h(i)s(a))t(b) = ((h * s) * t)(n)$ ya que $h(i), s(a), t(b) \in R$, 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 $(h * (s + t))(n) = \sum_{i+j=n}^{i,j} h(i)(s + t)(j) = \sum_{i+j=n}^{i,j} h(i)[s(j) + t(j)] = \sum_{i+j=n}^{i,j} h(i)s(j) + \sum_{i+j=n}^{i,j} h(i)t(j) = (h * s)(n) + (h * t)(n)$, ya que $h(i), s(j), t(j)$ pertenece a R , 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. [\Leftarrow] 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 $(\sum_{n=0}^{\infty} a_n z^n)(\sum_{m=0}^{\infty} b_m z^m) = 1 = 1 + 0z + 0z^2 + 0z^2 + \dots$.

Como

$$\begin{aligned} \left(\sum_{n=0}^{\infty} a_n z^n\right)\left(\sum_{m=0}^{\infty} b_m z^m\right) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)z + (a_0 b_2 + a_1 b_1 + a_2 b_0)z^2 + \dots \\ &= 1 + 0z + 0z^2 + 0z^3 + \dots \end{aligned}$$

Nota: En general $\sum_{n=0}^{\infty} c_n z^n = \sum_{n=0}^{\infty} d_n z^n$, si y sólo si $c_n = d_n$, para $n = 0, 1, 2, \dots$, en nuestro caso tenemos $a_0 b_0 = 1$, es decir $b_0 = a_0^{-1}$, además 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 $a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0 = 0$ lo cual tenemos que $b_k = a_0^{-1}[-a_1 b_{k-1} - a_2 b_{k-2} - \dots - a_k b_0]$. Por consiguiente tenemos nuestra serie $\sum_{m=0}^{\infty} b_m z^m$ que es inversa multiplicativa de $\sum_{n=0}^{\infty} a_n z^n$.

[\Rightarrow] Por demostrar que a_0 es invertible, esto es, que existe $b_0 \in R$ tal que $a_0 b_0 = 1$. Ahora bien sea $(\sum_{m=0}^{\infty} b_m z^m)$ el inverso multiplicativo de la serie $\sum_{m=0}^{\infty} a_m z^m$: $(\sum_{m=0}^{\infty} a_m z^m)(\sum_{m=0}^{\infty} b_m z^m) = 1 = 1 + 0z + 0z^2 + 0z^2 + \dots$. Dos series son iguales si lo son coeficiente a coeficiente, por consiguiente $a_0 b_0 = 1$. Por lo tanto a_0 es invertible. □

Ejemplo 6.1. Sea R un anillo con unidad, entonces $(1 - z)^{-1} = \sum_{n=0}^{\infty} z^n$. (Esta serie formal se llama serie geométrica).

Demostración. Sabemos que

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

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 entradas complejas, es decir; $A \in M_n(\mathbb{C})$, con $M_n(\mathbb{C})$ el anillo de matrices complejas $n \times n$. Entonces $(Id - Az)^{-1} = \sum_{n=0}^{\infty} A^n z^n$.

Definición 6.5. Para $0 \leq \varphi, \phi \leq 2\pi$ cualesquiera 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 6.4. Sea $Id - Qz = Idz^0 + (-Q)z^1 + 0z^2 + 0z^3 + \dots$ 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.

En [6] se prueba el siguiente lema.

Lema 6.2. Sea A matriz compleja $n \times n$, sea $|X\rangle, |Y\rangle \in \mathbb{C}^n$ arbitrarios, entonces

$$\sum_{k=0}^{\infty} \langle X|A^k|Y\rangle z^k = \langle X|(Id - zA)^{-1}|Y\rangle.$$

Observación 6.5. Supongamos que $\phi = \varphi = \pi$ y $\mu = \|\lvert b \rangle\|^2$, entonces $Q = \begin{pmatrix} -1 & -2\mu \\ 2 & 4\mu - 1 \end{pmatrix}$ en la base $\lvert X \rangle, P\lvert X \rangle$. Calculemos la serie formal

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

Además,

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

Es decir $A \lvert 0 \rangle = \begin{pmatrix} 1 \\ \frac{1}{\sqrt{\mu}} \end{pmatrix}$ en la base $\lvert X \rangle, P\lvert X \rangle$. Luego

$$\begin{aligned} g(\pi, \pi; z) &= \langle X \lvert \begin{pmatrix} 1+z & 2\mu z \\ -2z & 1+(1-4\mu)z \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{\mu}} \end{pmatrix} \\ &= \langle X \lvert \begin{pmatrix} \sigma_1 \\ \sigma_2 \end{pmatrix} \\ &= \langle X \lvert (\sigma_1 \lvert X \rangle + \sigma_2 P \lvert X \rangle) \\ &= \sigma_1 + \sigma_2 \langle X \lvert P \lvert X \rangle \\ &= \sigma_1 + \sigma_2 \mu \\ &= \frac{-\sqrt{\mu}(z-1)}{z^2 + (2-4\mu)z + 1} \end{aligned}$$

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 lo siguiente.

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

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

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

$$z^2 + 2(1-2\mu)z + 1 = 0 \quad (6.4)$$

luego $z = \frac{-2(1-2\mu) \pm \sqrt{4(1-2\mu)^2 - 4}}{2} = (2\mu - 1) \pm \sqrt{(1-2\mu)^2 - 1} = (2\mu - 1) \pm 2i\sqrt{\mu(1-\mu)}$. Es decir $\sigma = 2\mu - 1 + 2i\sqrt{\mu(1-\mu)}$ y $\sigma^* = 2\mu - 1 - 2i\sqrt{\mu(1-\mu)}$ son raíces de la ecuación (6.4) y por consiguiente $|\sigma|^2 = (2\mu - 1)^2 + 4\mu(1-\mu) = 1$.

Podemos poner $\sigma = e^{i\theta}$, para θ un ángulo conveniente. Sabemos que

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

donde $A = \frac{-\sqrt{\mu}e^{i\theta}}{e^{i\theta}+1}$, $B = \frac{-\sqrt{\mu}}{e^{i\theta}+1}$. Así

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

Entonces queremos que $1 = \left| \frac{\sqrt{\mu}}{(\sigma+1)\sigma^k} (1 + \sigma^{2k+1}) \right| = \frac{\sqrt{\mu}}{|(\sigma+1)|} |1 + \sigma^{2k+1}|$. 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 $|\sigma + 1|^2 = 4\mu$, luego, requerimos que $1 = \frac{|1 + \sigma^{2k+1}|^2}{4}$, por lo tanto $4 = |1 + \sigma^{2k+1}|^2$. Como $\sigma^{2k+1} = e^{i\theta(2k+1)}$, necesitamos que $\theta(2k+1) = 2\pi$, luego

$2k + 1 = \frac{2\pi}{\theta}$, entonces $k = \frac{2\pi + \theta}{2\theta} \approx \lceil \frac{2\pi + \theta}{2\theta} \rceil$. Por 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 $P = \begin{pmatrix} \frac{1}{6} & -\frac{6i-7}{6\sqrt{17}} \\ \frac{6i+7}{6\sqrt{17}} & \frac{5}{6} \end{pmatrix}$ y $|b\rangle = \begin{pmatrix} -\frac{324\sqrt{2941}i + (-5\sqrt{17}-378)\sqrt{2941}}{1038 \cdot 17^{\frac{3}{2}}} \\ \frac{30\sqrt{2941}i + (270\sqrt{17}+35)\sqrt{2941}}{1038 \cdot 17^{\frac{3}{2}}} \end{pmatrix}$ tal que

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

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

Por lo cual

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

Calculando el número de veces que se debe iterar 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:

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

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

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

Tenemos que P es hermitiana e idempotente. Queremos encontrar $|X\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$,

tal que sea unitario, es decir $\langle X|X\rangle = 1$ y que satisfaga dicha ecuación $P|X\rangle = |b\rangle$.

El algoritmo va a calcular tal solución. Para distinguirla se marcará con la matriz

$e^{i\varphi|X\rangle\langle X|}$. Digamos que nos interesa $|X\rangle = \begin{pmatrix} \frac{5i}{\sqrt{131}} \\ -\frac{9}{\sqrt{131}} \\ \frac{3i+4}{\sqrt{131}} \end{pmatrix}$. Entonces se define

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

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:

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

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

$$\begin{pmatrix} \frac{25(13i-5)}{146\sqrt{111}} + \frac{2490i}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{19858}} - \frac{3888i}{73\sqrt{111}\sqrt{566}} + \frac{486}{\sqrt{111}\sqrt{219}\sqrt{9929}} \\ -\frac{324(13i-5)}{73\sqrt{111}\sqrt{566}} + \frac{336150i}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{566}\sqrt{19858}} + \frac{97710i}{20659\sqrt{111}} + \frac{6561}{\sqrt{111}\sqrt{219}\sqrt{566}\sqrt{9929}} \\ \frac{4980(13i-5)}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{19858}} + \frac{806760i}{\sqrt{111}\sqrt{219}\sqrt{283}\sqrt{566}\sqrt{19858}} + \frac{12327285i}{5619814\sqrt{111}} - \frac{33615}{\sqrt{111}\sqrt{283}\sqrt{9929}\sqrt{19858}} \\ -\frac{54(13i-5)}{\sqrt{111}\sqrt{219}\sqrt{9929}} + \frac{18675i}{\sqrt{111}\sqrt{283}\sqrt{9929}\sqrt{19858}} - \frac{8748i}{\sqrt{111}\sqrt{219}\sqrt{566}\sqrt{9929}} - \frac{44316}{9929\sqrt{111}} \end{pmatrix}$$

sabemos que P es hermitiano e idempotente. Queremos encontrar un $|X\rangle =$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \text{ tal que } \langle X|X\rangle = 1, \text{ que satisfaga dicha ecuación } P|X\rangle = |b\rangle. \text{ El algoritmo}$$

va a calcular la solución. Para distinguirla se marcará con la matriz $e^{i\varphi|X\rangle\langle X|}$.

Digamos que nos interesa $|X\rangle = \begin{pmatrix} \frac{13i-5}{2\sqrt{111}} \\ \frac{6i}{\sqrt{111}} \\ \frac{5i}{2\sqrt{111}} \\ -\frac{9}{2\sqrt{111}} \end{pmatrix}$. Entonces se define $Q = e^{i\phi P} e^{i\varphi \langle X|X\rangle}$,

con $\phi = \varphi = \pi$. Lo cual nos dice que

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

Calculando el número de veces que aparece Q . Tenemos que $\mu \approx 0.4852728392995$ y $\theta \approx 1.54133774484651$; esto implica que el número de iteraciones $k = 3$.

Necesitamos A matriz unitaria tal que: $A|0\rangle \approx \begin{pmatrix} 0.9498i - 0.07175 \\ 0.3689i + 0.1526 \\ 0.682i - 0.1161 \\ -0.08807i - 0.5832 \end{pmatrix}$. Veri-

ficquemos el resultado con el número de iteraciones

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

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 homogéneas 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] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, **21**:467–488, 1982.
- [4] S. H. Friedberg, A. J. Insel, and L. E. Spence. *Linear Álgebra*, volume 4. Cambridge University Press, 2010.
- [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] C. Bautista Ramos, C. Guillén Galván, and A. Rangel Huerta D. Valdés Amaro y J.M. Amezcua Ortega. From orthogonal projections to a generalized quantum search. *Inexact and exact quantum searches with a preparation state in a three dimensional subspare*, **13**:2483–2498, 2014.
- [7] C. Bautista Ramos and C. Guillén Galván y A. Rangel Huerta. *Quantum Information Processing*, **12**:1–20, 2013.
- [8] M. A. Nielsen y I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

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