Síntesis de Circuitos Cuánticos

Diego A. Quiñones Valles

Instituto de Física, UASLP

Universidad Autónoma de San Luis Potosí

Una tesis presentada para la obtención del título de

Maestría en Ciencias (Física)

29 de Agosto 2012

Abstract

En esta tesis se presenta un análisis teórico de operadores que actuán sobre sistemas de qubits. Su finalidad es encontrar un método para descomponer un operador arbitrario que opera sobre cualquier número de qubits como el producto de operadores elementales.

Para esto, primero introducimos el formalismo matemático con el que se trabajó y la representación gráfica que se dio a los operadores.

Comenzamos estudiando operadores que actúan sobre uno y dos qubits, encontrando su descomposición en compuertas cuánticas elementales. Para un número mayor de qubits establecemos un algoritmo que permite encontrar la descomposición de una tranformación como el producto reflexiones de Householder. Despues damos un método para obtener la representación de las reflexiones como una serie de compuertas cuánticas. El algoritmo de descomposición y el método de representación permiten sintetizar el circuito cuántico para cualquier transformación de qubits.

Observamos que, bajo un criterio especifico de selección de las reflexiones y de su representación, es posible encontrar una forma reducida del circuito cuántico resultante.

Contenido

Lista de Figuras

Capítulo 1

Introducción

En la física el concepto de *información* se refiere a las propiedades que caracterizan a un sistema, en especial aquellas que lo hacen distinguible de otros sistemas. Las propiedades físicas de un sistema son, por ejemplo, su posición, velocidad, masa, tamaño, etc.

La teoría de información cuántica es el resultado de la aplicación de la teoría de información a la mecánica cuántica. En un principio el concepto de información cuántica pudiera parecernos paradójico; las leyes de la mecánica cuántica nos dictan que es imposible conocer de forma precisa ciertas propiedades simultáneamente, como posición y momento. La mecánica cuántica también conlleva la limitante de que al obtener información de un sistema cuántico este se altera debido al proceso de medición, por lo que la información obtenida no representa al sistema actual.

Si embargo, la teoría de información cuántica ha logrado sobreponerse a las aparentes limitaciones impuestas por la mecánica cuántica, desarrollando una descripción formal y satisfactoria de la forma en que la información es manipulada y transmitida en sistemas cuánticos. En esta descripción se introduce el concepto de *qubit*.

1.1 El qubit

En el lenguaje de la computación cuántica, "qubit" se refiere a la unidad fundamental de información cuántica.

El qubit es similar al bit, la unidad de información clásica. Un bit es una variable con dos posibles valores que se representa numéricamente con un 0 o un 1. El qubit, a diferencia del bit, puede ser una combinación lineal de los estados 0 y 1 debido a la superposición que pueden presentar los sistemas cuánticos.

Cualquier sistema cuántico de dos niveles pueden servir como qubit, por ejemplo un átomo con un estado base al cual se le asigna el 0 y un estado excitado al cual se le asigna el 1, o un fotón con dos direcciones perpendiculares de polarización, horizontal equivalente a 0 y vertical equivalente a 1. Un gran número de sistemas ya han sido implementados experimentalmente para el estudio de la manipulación de la información [5; 6; 7; 8; 9; 10; 12; 13; 14; 15; 29].

1.2 Manipulación de la información

Un fenómeno físico que afecta a un sistema se puede entender como la alteración de la información contenida en el sistema. Tomemos por ejemplo que un átomo absorbe un fotón y uno de sus electrones pasa del estado base al estado excitado. Si un qubit representa el estado en que se encuentra el electrón, entonces el cambio en el estado del átomo es equivalente al la transformación del qubit.

El cambio en múltiples propiedades, o el cambio de una propiedad en múltiples subsistemas, se representa como la manipulación varios qubits.

Dado el estado inicial del sistema (antes de que ocurra el fenómeno físico) y el estado final (después de ocurrido), podemos describir matemáticamente el cambio en la información a traves de una transformación que es aplicada al estado inicial tal que nos de como resultado el estado final. Nuestro interés se enfoca en el estudio de estas transformaciones y sus diferentes representaciones.

A continuación daremos el formalismo matemático de la información y de su manipulación, con el cual realizaremos nuestro análisis.

Capítulo 2

Formalismo matemático y grafico

En este capítulo damos la representación matemática y gráfica de sistemas de qubits y de los fenómenos que transforman la información. Estas representaciones permitirán la realización de los cálculos que se llevaran a cabo en capítulos posteriores y permanecerán consistentes a lo largo de todo este trabajo.

2.1 Vectores de estado de qubits

El conjuto de todas las propiedades que definen a un sistema cuántico se conoce como *estado cuántico*. Las propiedades se enlistan en un tensor unitario, que en la notación de Bra-ket es $|\psi\rangle$ [1, pag. 109]. El tensor $|\psi\rangle$ contiene toda la información del sistema aunque no la detone explícitamente.

El estado cuántico estara dado en función de vectores de base. Para sistemas de qubits el número de vectores de base será 2^n, con n el número de qubits que componen al sistema.

2.1.1 Estados de un qubit

Un qubit representa un sistema con dos posibles estados. Estos estados los representamos matemáticamente con los vectores de base $|0\rangle$ y $|1\rangle$, respectivamente,

y por convención les damos la forma matricial

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.1}$$

De forma general, podemos representar un sistema de un qubit con un estado arbitrario $|\psi\rangle$ como la combinación lineal de los vectores de base,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.2}$$

con la condición de normalización $|\alpha|^2 + |\beta|^2 = 1$. Como α y β son números complejos, sería necesario tener cuatro factores (dos reales y dos imaginarios) para caracterizar el estado, pero debido a la condición de normalización solo se necesitan tres. Bajo este argumento podemos reescribir la representación (2.2) como

$$|\psi\rangle = e^{\imath\gamma}(cos\frac{\theta}{2}|0\rangle + e^{\imath\varphi}sin\frac{\theta}{2}|1\rangle). \tag{2.3}$$

El término $e^{\imath\gamma}$ es una fase global y no tiene efectos observables, por lo que generalmente se ignora. De tal modo, la representación efectiva resulta en

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{\imath\varphi}sin\frac{\theta}{2}|1\rangle. \tag{2.4}$$

Esta es la representación de un estado sobre la *esfera de Bloch*. La esfera de Bloch es una esfera unitaria cuyos puntos en su superficie representan todos las posibles superposiciones de $|0\rangle$ y $|1\rangle$. Los estados $|0\rangle$ y $|1\rangle$ se colocan respectivamente en polos opuestos de la esfera y los términos θ y φ representan los angulos que forma el vector $|\psi\rangle$ con respecto a los ejes de coordenadas (ver figura 2.1).

2.1.2 Estados de pares de qubits

Supongamos un sistema compuesto por dos qubits; cada uno de los qubits tiene dos vectores de base, $|0\rangle$ y $|1\rangle$. El sistema total tendrá un número de vectores de base dado por las todas las posibles combinaciones de los vectores de base de

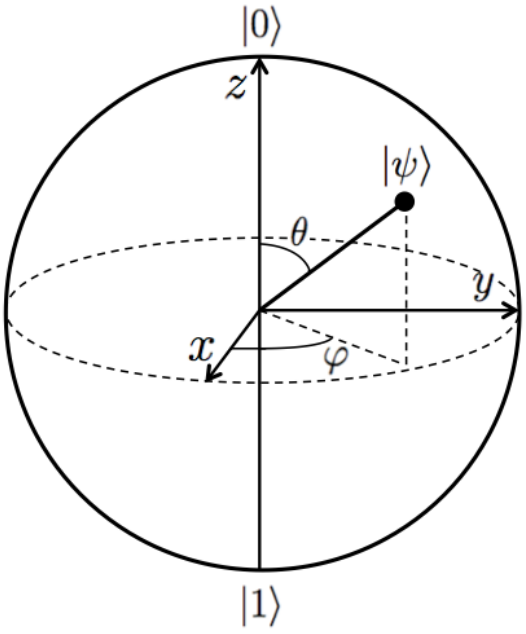

Figura 2.1: Esfera de Bloch. El estado $|\psi\rangle$ se encuentra en la superficie de la esfera unitaria y esta caracterizado por los angulos φ y θ.

cada uno de los qubits. Los vectores de base para un sistema de dos qubits seran

$$|00\rangle := |0\rangle_1 \otimes |0\rangle_2 \ , \ |01\rangle := |0\rangle_1 \otimes |1\rangle_2 \ , \ |10\rangle := |1\rangle_1 \otimes |0\rangle_2 \ , \ |11\rangle := |1\rangle_1 \otimes |1\rangle_2, \tag{2.5}$$

donde los subíndices 1 y 2 nos sirven para etiquetar el estado del primer y segundo qubit, respectivamente, y donde el símbolo $\otimes$ denota el producto tensorial [2, pag. 16].

Podemos representar un estado arbitrario $|\psi\rangle$ de un sistema de dos qubits como la combinación lineal de estos vectores, de la forma

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \tag{2.6}$$

donde los factores a_{00}, a_{01}, a_{10} y a_{11} satisfacen la condición de normalización $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$. La forma matricial de los vectores de base,

según la convención adoptada, será:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{2.7}$$

A partir de los vectores de base y de la representación de un estado en función de estos vectores desarrollaremos el formalismo matemático para las transformaciones de los estados cuánticos.

2.2 Transformaciones de estados cuánticos

Un fenómeno físico que afecta a un sistema realiza una transformación del estado cuántico, llevándolo de un estado inicial aa un estado final.

La representación matemática de esta transformación se realiza mediante un elemento llamado *operador* y se representa graficamente utilizando un diagrama nombrado *circuito cuántico*.

2.2.1 Operadores

Para representar una transformación que llevan el estado inicial $|\psi\rangle$ al estado final $|\psi'\rangle$ se aplica un operador, de la forma U, al estado inicial dando como resultado el estado final,

$$U|\psi\rangle = |\psi'\rangle. \tag{2.8}$$

En mecánica cuántica, los operadores son unitarios ($UU^\dagger = U^\dagger U = \mathbb{I}$, donde $\mathbb{I}$ es el operador identidad tal que $\mathbb{I}|\psi\rangle = |\psi\rangle$) y actuan *linealmente* sobre los vectores [2, pag. 18], de modo que para un sitema $|\psi\rangle$ con vectores de base

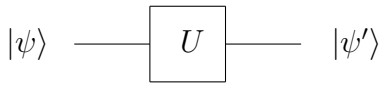

Figura 2.2: Circuito cuántico. El estado de entrada $|\psi\rangle$ es afectado por la compuerta U obteniendo el estado de salida $|\psi'\rangle$.

$\{|0\rangle, |1\rangle, |2\rangle, ...\}$ un operador U actuara como

$$\begin{aligned} U|\psi\rangle &= U[a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + ... \\ &= a_0U|0\rangle + a_1U|1\rangle + a_2U|2\rangle + ... \\ &= a_0|0'\rangle + a_1|1'\rangle + a_2|2'\rangle + ... \end{aligned} \tag{2.9}$$

Nuestra atención se enfocará en como el operador U modifica un vector de base arbitrario $|j\rangle$, ya que podemos obtener la forma en que actua un operador sobre un estado a partir del efecto que tiene en los vectores de base.

Para sistemas de qubits, los operadores son matrices de dimensiones $2^n \times 2^n$, siendo n el numero de qubits del sistema.

Todo fenómeno físico que afecta a los qubits se puede representar como un operador, pero no siempre es posible obtener la relación inversa para un operador arbitrario (encontrar el equivalente físico de un cierto operador dado); en muchos de los casos es necesario descomponer el operador como el producto de otros operadores de los que se conoce su analogo físico. Esta descomposición la representaremos en un circuito para facilitar su visualización.

2.2.2 Circuitos cuánticos

A una serie de operadores la podemos representar en un diagrama que muestra el estado individual de cada uno de los quibits al principio y al final del proceso, e ilustra los operadores a partir de los qubits sobre los cuales actúan. A este diagrama se le denomina circuito cuántico y a la representación de un operador en el circuito se le llama compuerta cuántica. En la figura 2.2 se ejemplifica la forma de un circuitos cuántico.

Los elementos que componen un circuito cuántico son:

Qubits de Entrada: Corresponden al estado inicial del sistema y se colocan a la izquierda del circuito.

Cables: Representan el transporte de la infromación. Dirigen a los qubits hacia las compuertas cuánticas y fuera del circuito.

Compuertas Cuánticas: Representan las operaciones realizadas sobre los qubits.

Qubits de Salida: Corresponden al estado final del sistema y se colocan a la derecha del circuito.

Los circuitos cuanticos son utilizados para facilitar la implementación física de los procesos de manipulación de la información. En los siguientes capítulos, los circuitos cuánticos nos ayudarán a visualizar la forma en que se descomponen y en que actúan los operadores.

Capítulo 3

Representaciones de operadores cuánticos

Una vez hecha la introducción al tema de los qubits y de los operadores, veremos como actuán los operadores sobre sistemas de qubits. La forma en que actuan determina su descomposición como el producto de otros operadores y su representación en el circuito cuántico.

La importancia de establecer la representación de los operadores en los circuitos cuánticos a partir de la forma en que actuán es que esto constituye un puente entre el análisis teórico y el desarrollo de arreglos experimentales.

Comenzaremos con el caso más simple, el de sistemas de un qubit.

3.1 Preparación de estados para un qubit

Estudiamos primero el caso de operadores no triviales que actúan sobre un qubit. Consideremos un proceso en el cual se cambia los estados $|0\rangle \to |1\rangle$ y $|1\rangle \to |0\rangle$. Representaremos este proceso con el operador X. Si este operador se aplica a un estado arbitrario $\alpha|0\rangle + \beta|1\rangle$ tendremos

$$X[\alpha|0\rangle + \beta|1\rangle] = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle. \tag{3.1}$$

El circuito cuántico que representa este proceso se muestra en la figura 3.1.

Este operador corresponde a la compuerta llamada NOT y su forma matricial

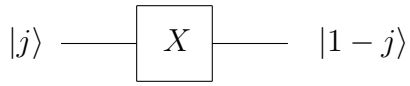

Figura 3.1: Compuerta NOT actuando sobre un qubit $|j\rangle$, invirtiendo su estado.

corresponde a la matiz de Pauli σ_x, por lo que también es llamada compuerta Pauli-X. En la tabla 3.1 se muestran diversas compuertas que seran usadas con regularidad en este y otros capitulos.

Las compuertas presentadas se conocen como compuertas logicas elementales [16]; han sido ampliamente estudiadas y se conoce su análogo físico para diversos tipos de qubits [5; 10; 15; 17].

La finalidad de esta tesis es construir un operador arbitrario haciendo uso solo de estas compuertas lógicas; esto permitiría deducir con relativa facilidad el arreglo experimental que reproduzca la acción del operador. En otros trabajos se ha realizado la busqueda de la representación de un operador como el producto de operaciones sencillas [18; 19; 20; 21], lo que nos sirve de base y justificación de este trabajo.

Nuestro primer objetivo será encontrar esta construcción para operadores que actuan sobre un qubit: La forma más general de una matriz unitaria de 2×2 es

$$U = e^{\imath\alpha} \begin{pmatrix} A & B \\ -B^* & A^* \end{pmatrix}, \tag{3.2}$$

donde A y B son dos números complejos que cumplen con la relación $|A|^2 + |B|^2 = AA^* + BB^* = 1$ para matrices unitarias. El término $e^{\imath\alpha}$ es solo una fase global que se ignora en la mayoria de los casos. Los dos números complejos los podemos expresar como

$$A \equiv e^{-\imath\vartheta} \cos\varphi \ , \ B \equiv e^{-\imath\varepsilon} \sin\varphi, \tag{3.3}$$

observando claramente que se satisface la condición de normalización.

Nombre	Operador	Matriz
Hadamard	H	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
Pauli-X	X	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
Pauli-Y	Y	$\begin{pmatrix}0 & -\imath\\ \imath & 0\end{pmatrix}$
Pauli-Z	Z	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$
Fase	S	$\begin{pmatrix}1 & 0\\ 0 & \imath\end{pmatrix}$
$\pi/8$	T	$\begin{pmatrix}1 & 0\\ 0 & e^{\imath\pi/4}\end{pmatrix}$
Desfase	R_θ	$\begin{pmatrix}1 & 0\\ 0 & e^{\imath\theta}\end{pmatrix}$

Tabla 3.1: Lista de las compuertas cuánticas fundamentales que actúan sobre un qubit con su respectiva representación como operador y matriz.

Esto nos permite encontrar una expresión general para matrices unitarias

$$U = \begin{pmatrix} e^{-\imath\vartheta}\cos\varphi & -e^{\imath\varepsilon}\sin\varphi \\ e^{-\imath\varepsilon}\sin\varphi & e^{\imath\vartheta}\cos\varphi \end{pmatrix}, \tag{3.4}$$

en donde se ha omitido la fase global $e^{\imath\alpha}$ ya que no tiene una manifestación observable.

Siguiendo nuestro objetivo, observamos que las matrices X, Y y Z dan origen a una serie de matrices unitarias llamadas *operadores de rotación*, que son

$$R_X(\theta) \equiv e^{-\imath\frac{\theta}{2}X} = \cos(\frac{\theta}{2})\mathbb{I} - \imath\sin(\frac{\theta}{2})X = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\imath\sin(\frac{\theta}{2}) \\ -\imath\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}, \tag{3.5}$$

$$R_Y(\theta) \equiv e^{-\imath\frac{\theta}{2}Y} = \cos(\frac{\theta}{2})\mathbb{I} - \imath\sin(\frac{\theta}{2})Y = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}, \tag{3.6}$$

$$R_Z(\theta) \equiv e^{-\imath\frac{\theta}{2}Z} = \cos(\frac{\theta}{2})\mathbb{I} - \imath\sin(\frac{\theta}{2})Z = \begin{pmatrix} e^{-\imath\frac{\theta}{2}} & 0 \\ 0 & e^{\imath\frac{\theta}{2}} \end{pmatrix}. \tag{3.7}$$

Los operadores R_X, R_Y y R_Z corresponden a rotaciones sobre la esfera de Bloch (ver figura 2.1) al rededor de los ejes $\hat{x}$, $\hat{y}$ y $\hat{z}$, respectivamente, y tienen la propiedad

$$XR_Y(\theta)X = R_Y(-\theta)\ ,\ XR_Z(\theta)X = R_Z(-\theta), \tag{3.8}$$

la cual nos será útil más adelante. Las transformaciones unitarias pueden verse como rotaciones que transladan un vector de un punto a otro sobre la superficie de la esfera de Bloch, por lo cual sería lógico pensar que podemos expresar las transformaciones en función de los operadores de rotación.

Si realizamos el producto de tres matrices $R_Z(\beta)$, $R_Y(\gamma)$ y $R_Z(\delta)$ encontramos que tiene la forma

$$R_Z(\beta)R_Y(\gamma)R_Z(\delta) = \begin{pmatrix} e^{-\imath\frac{\delta+\beta}{2}}\cos\frac{\gamma}{2} & -e^{\imath\frac{\delta-\beta}{2}}\sin\frac{\gamma}{2} \\ e^{-\imath\frac{\delta-\beta}{2}}\sin\frac{\gamma}{2} & e^{\imath\frac{\delta+\beta}{2}}\cos\frac{\gamma}{2} \end{pmatrix} \tag{3.9}$$

Esta matriz es equivalente a la identidad (3.4), que es la forma matricial de un

operador unitario arbitrario, si sustituimos los valores $\varphi = \frac{\gamma}{2}$, $\vartheta = \frac{\delta+\beta}{2}$ y $\varepsilon = \frac{\delta-\beta}{2}$. Esto nos indica que es posible encontrar tres números reales β, γ y δ que den la representación de cualquier operador como el producto de matrices R_Y y R_Z de la forma

$$U = R_Z(\beta)R_Y(\gamma)R_Z(\delta). \tag{3.10}$$

Los operadores R_Y y R_Z, de acuerdo con las ecuaciones (3.6) y (3.7), son funciones de los operadores Y y Z, por lo que la ecuación (3.10) de U nos da la representación de un operador arbitrario como el producto de compuertas Pauli-Y y Pauli-Z.

Otra representación de un operador unitario arbitrario que sera escencial es

$$U = AXBXC, \tag{3.11}$$

donde A B y C cumplen con la relacion $ABC = \mathbb{I}$ y donde X es la compuerta NOT. Para demostrar esta identidad primero proponemos tres operadores

$$A \equiv R_Z(\beta)R_Y(\frac{\gamma}{2}), \tag{3.12}$$

$$B \equiv R_Y(\frac{-\gamma}{2})R_Z(\frac{-(\delta+\beta)}{2}), \tag{3.13}$$

$$C \equiv R_Z(\frac{\delta-\beta}{2}), \tag{3.14}$$

cuyo producto resulta en la identidad,

$$ABC = R_Z(\beta)R_Y(\frac{\gamma}{2})R_Y(\frac{-\gamma}{2})R_Z(\frac{-(\delta+\beta)}{2})R_Z(\frac{\delta-\beta}{2}) = \mathbb{I}, \tag{3.15}$$

Multiplicando el operador B en ambos extremos por el operador X (teniendo en cuenta la propiedad (3.8) y que $XX = \mathbb{I}$) obtenemos que

$$XBX = XR_Y(\frac{-\gamma}{2})XXR_Z(\frac{-(\delta+\beta)}{2})X = R_Y(\frac{\gamma}{2})R_Z(\frac{\delta+\beta}{2}). \tag{3.16}$$

Ahora multiplicamos el resultado por los operadores A y C por la izquierda y por la derecha, respectivamente, y obtenemos

$$AXBXC = R_Z(\beta)R_Y(\frac{\gamma}{2})R_Y(\frac{\gamma}{2})R_Z(\frac{\delta+\beta}{2})R_Z(\frac{\delta-\beta}{2}) = R_Z(\beta)R_Y(\gamma)R_Z(\delta). \tag{3.17}$$

El término a la derecha de la identidad es la representación (3.10) de una matriz unitaria U en función de los operadores de rotación, por lo tanto se verifica la relación (3.11).

La ecuación (3.11) afirma que cualquier transformación unitaria U que actua en el espacio de un qubit puede ser desarrollada como el producto compuertas NOT y tres compuertas cuyo producto es la identidad. Esta relación nos ayudara a encontrar la representación en compuertas fundamentales de operadores que actúan sobre dos qubits.

3.2 Representación de operadores que actúan sobre dos qubits

Supongamos un proceso que cambia individualmente dos qubits, siendo $U^{(1)}$ y $U^{(2)}$ matices de dimensión 2×2 que representan la modificación al primer qubit $|j_1\rangle \xrightarrow{U^{(1)}} |j_1{}'\rangle$ y al segundo qubit $|j_2\rangle \xrightarrow{U^{(2)}} |j_2{}'\rangle$, de modo tal que la transformación efectiva sobre el sistema sera

$$\begin{aligned} U|j_1\rangle|j_2\rangle &= U^{(1)}|j_1\rangle U^{(2)}|j_2\rangle \equiv [U^{(1)}|j_1\rangle] \otimes [U^{(2)}|j_2\rangle] \\ &= (U^{(1)} \otimes U^{(2)})|j_1\rangle|j_2\rangle. \end{aligned} \tag{3.18}$$

La formula anterior muestra que la matriz U de dimensión 4×4 que actua sobre todo el sistema esta dada por el producto tensorial de las matrices $U^{(1)}$ y $U^{(2)}$ que actuan indidualmente sobre cada uno de los qubits, $U = U^{(1)} \otimes U^{(2)}$.

Aunque es claro que el producto tensorial de operadores que actúan en el espacio de un solo qubit se puede representar como un solo operador que actua sobre el espacio de todos los qubits ($U^{(1)} \otimes U^{(2)} \otimes U^{(3)} \otimes ... = U$), la relación

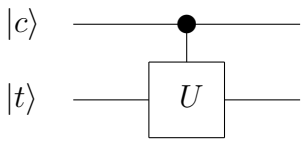

Figura 3.2: Compuerta controlada U. El qubit $|c\rangle$ es el qubit de control y el qubit $|t\rangle$ es el qubit objetivo.

inversa no se cumple para un operador U arbitrario ($U \neq U^{(1)} \otimes U^{(2)} \otimes U^{(3)} \otimes ...$), es decir, no siempre podremos descomponer una matriz $n \times n$ como el producto tensorial de matrices 2×2, lo cual mostraremos a continuación.

3.2.1 Compuertas controladas

Dado un operador U que actúa en el espacio de dos qubits, no siempre es posible representar este operador como el producto tensorial de operadores que actúan en el espacio de un solo qubit. Para ilustrar este argumento tomaremos un operador U_C, el cual estara dado como

$$U_C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}. \tag{3.19}$$

No es posible encontrar dos matrices de dimensión 2×2 tales que al realizar el producto tensorial entre ellas puedan reproducir la matiz U_C,

$$U_C \neq \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}. \tag{3.20}$$

Esta clase de operadores que no pueden descomponerse como el producto tensorial de operadores que actúan en el espacio de un solo qubit se les denomina *compuertas controladas*. En la figura 3.2 se muestra el diagrama de una compuerta cuántica controlada.

En una compuerta cuántica controlada los qubits de entrada se dividen en dos grupos, los *qubits de control*, que determinan la forma en que actúa la compuerta segun su estado, y los *qubits objetivo*, los cuales son afectados por la compuerta en

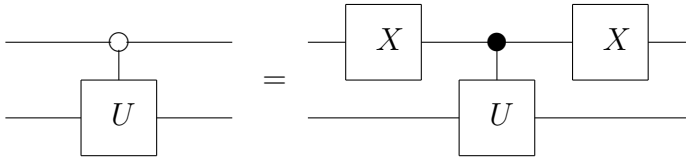

Figura 3.3: Compuerta controlada que requiere que el qubit de control sea $|0\rangle$. Es equivalente a una compuerta que requiere que el qubit de control sea $|1\rangle$ si se invierte el qubit de control antes y despues de la compuerta U.

función del estado de los qubits de control. En el caso del operador U_C definido en (3.19), si el primer qubit esta en el estado estado $|1\rangle$ entonces se modifica el segundo qubit, de otro forma el segundo qubit permanece inalterado; para esta compuerta el primer qubit es el de control y el segundo qubit es el objetivo.

Si para un operador $U_{|1\rangle}$ se requiere que el qubit de control este en el estado $|1\rangle$ para que tenga un efecto no tribial sobre el qubit de control, entoces podemos decir que el operador $U_{|1\rangle}$ actúa como

$$U_{|1\rangle}|c\rangle|t\rangle = |c\rangle U^c|t\rangle, \tag{3.21}$$

donde c puede adoptar los valores 0 o 1. En este caso c es un exponente para el operador U tal que $U^0 = \mathbb{I}$ es el operador identidad.

Supongamos ahora una compuerta controlada $U_{|0\rangle}$ que actúa de manera no trivial solo si el qubit de control es $|0\rangle$ a modo que

$$U_{|0\rangle}|c\rangle|t\rangle = |c\rangle U^{1-c}|t\rangle. \tag{3.22}$$

Podemos expresar este operador como un operador que requiere que el qubit de control sea $|1\rangle$ para actuar, si invertiremos el estado del qubit de control antes y después de aplicar la compuerta controlada,

$$U_{|0\rangle}|c\rangle|t\rangle = X^{(c)}U_{|1\rangle}X^{(c)}|c\rangle|t\rangle, \tag{3.23}$$

dode $X^{(c)}$ es la compuerta NOT que actúa en el espacio del qubit de control y donde $U_{|0\rangle}$ y $U_{|1\rangle}$ representan compuertas que requieren que el qubit de control sea $|0\rangle$ y $|1\rangle$, respectivamente, para actuar de forma no trivial. Este argumento se ilustra en la figura 3.3.

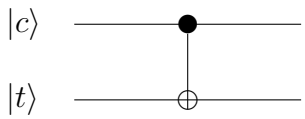

Figura 3.4: Diagrama de la compuerta CNOT (U_{CN}). El qubit $|t\rangle$ invertirá su estado si $|c\rangle = |1\rangle$ o permanecerá igual si $|c\rangle = |0\rangle$.

Continuamos con el análisis de las compuertas controladas introduciendo la compuerta $CNOT$, la cual es de suma importancia para este trabajo.

3.3 Compuerta CNOT

Sea el operador U_{CN} una compuerta controlada que actúa sobre dos qubits y cuya forma matricial es

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.24}$$

Si aplicamos el operador U_{CN} a los estados de base de un sistema de dos qubits obtenemos

$$U_{CN}|00\rangle = |00\rangle \ , \ U_{CN}|01\rangle = |01\rangle \ , \ U_{CN}|10\rangle = |11\rangle \ , \ U_{CN}|11\rangle = |10\rangle. \tag{3.25}$$

Se observa que el segundo qubit cambiará $|0\rangle \rightarrow |1\rangle$ y $|1\rangle \rightarrow |0\rangle$, similar al efecto del operador X, si el primer qubits es $|1\rangle$ o permanecerá igual si el primer qubit es $|0\rangle$. Debido a la forma en que actúa esta compuerta, invirtiendo el estado del segundo qubit en función del estado del primero, se le conoce como compuerta *NOT controlada* o compuerta *CNOT*. El diagrama de la compuerta U_{CN} se muestra en la figura 3.4.

El operador U_{CN} es la compuerta CNOT con el primer qubit como control y el segundo qubit como objetivo. Para el caso en que la compuerta CNOT tenga

como control el segundo y como objetivo el primero, definiremos el operador U_{NC} el cual tiene la forma matricial

$$U_{NC} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{3.26}$$

La compuerta CNOT es de gran importancia en la preparación de estados de dos qubits y en la descomposición de compuertas arbitrarias con un solo qubit de control.

3.3.1 Circuito de una compuerta con un qubit de control

Sea una compuerta controlada $U(2)$ que actúa sobre un sistema de dos qubits, uno de control $|c\rangle$ y uno objetivo $|t\rangle$ tal que

$$U(2)|c\rangle|t\rangle = |c\rangle U^c|t\rangle. \tag{3.27}$$

Se desea encontrar un circuito cuantico que utiliza solo compuertas elementales tal que reproduzca la acción de la compuerta U(2). La compuerta U actúa solo sobre un qubit, por lo que se puede sustituir por la relación (3.11) obteniendo

$$\begin{aligned} U|c\rangle|t\rangle &= |c\rangle U^c|t\rangle = |c\rangle(e^{\imath\alpha}AXBXC)^c|t\rangle \\ &= |c\rangle e^{\imath\alpha c}A^cX^cB^cX^cC^c|t\rangle. \end{aligned} \tag{3.28}$$

La forma en que actúa termino X^c es igual a la compuerta $CNOT$,

$$X^c \equiv U_{CN}. \tag{3.29}$$

El término $e^{\imath\alpha c}$ es una fase global que estará presente solo si $c = 1$ y que es equivalente a

$$e^{\imath\alpha c} \equiv R_\alpha{}^{(c)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\imath\alpha} \end{pmatrix}. \tag{3.30}$$

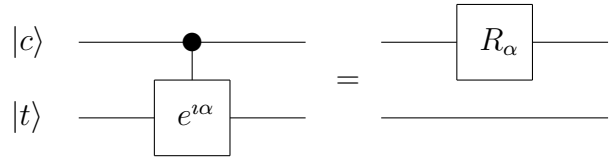

Figura 3.5: La fase controlada $e^{\imath\alpha}$ es equivalente a aplicar la compuerta R_α sobre el qubit de control.

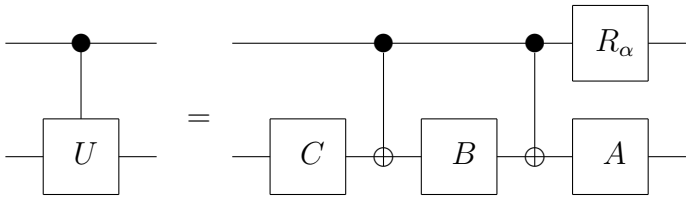

Figura 3.6: Representación de una compuerta controlada como una serie de compuertas que actúan sobre un qubit y compuertas $CNOT$.

donde ${R_\alpha}^{(c)}$ es un operador de desfasamiento que actúa en el espacio del qubit de control. Esta equivalencia se ilustra en la figura 3.5.

Cuando el parametro de control es $c = 0$, el operador X^c es la identidad, dejando el producto $(ABC)^c$, el cual se requiere que sea la identidad independientemente del valor de c. Por tal motivo, el conjunto de las compuertas A^c, B^c y C^c actúa de forma equivalente a las compuertas no controladas A B y C que actúan sobre el qubit objetivo.

$$A^c \equiv A^{(t)} \ , \ B^c \equiv B^{(t)} \ , \ C^c \equiv C^{(t)}. \tag{3.31}$$

Reuniendo las equivalencias en las ecuaciones (3.29), (3.30) y (3.31) se llega finalmente a la ecuación

$$U(2)|c\rangle|t\rangle = {R_\alpha}^{(c)} A^{(t)} U_{CN} B^{(t)} U_{CN} C^{(t)} |c\rangle|t\rangle, \tag{3.32}$$

refiriéndose la notación $U(2)$ a una compuerta que actua sobre dos qubits y donde los superíndices (c) y (t) indican que el operador actúa sobre el espacio del qubit de control $|c\rangle$ y del qubit objetivo $|t\rangle$, respectivamente. El circuito cuántico que representa esta equivalencia se muestra en la figura 3.6.

La ecuación (3.32) indica que podemos descomponer cualquier compuerta

controlada con un qubit de control y un qubit objetivo en función de compuertas CNOT y compuertas que actúan sobre un solo qubit, mostrando que la compuerta CNOT es una compuerta fundamental.

La compuerta CNOT también es indispensable para crea *entrelazamiento cuántico* entre dos qubits. El entrelazamiento cuántico forma parte de la preparación de estados de dos qubits y se explica a continuación.

3.4 Preparación de entrelazamiento cuántico

Nos interesa estudiar los estados de qubits entrelazados y la preparación de estos estados debido a que esto formará parte de la preparación de estados arbitrarios y debido a sus posibles aplicaciones en computación cuántica [22].

El entrelazamiento cuántico es un fenómeno de la mecánica cuántica sin análogo clásico en el que dos o más partículas comparten un estado indivisible, es decir, que el estado total del sistema no puede expresarse como el producto de los estados individuales de las partículas que lo componen.

Supongamos un sistema de dos qubits en un estado $|\Phi\rangle$ tal que

$$|\Phi\rangle = \frac{1}{\sqrt{2}}[|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2]. \tag{3.33}$$

Para este estado no es posible encontrar su descomposición como el producto tensorial del estado individual de dos qubits,

$$|\Phi\rangle \neq [a|1\rangle_1 + b|0\rangle_1] \otimes [c|1\rangle_2 + d|0\rangle_2]. \tag{3.34}$$

A este tipo de estados no factorizables se les conoce como estados entrelazados.

Si para un sistema en el estado $|\Phi\rangle$ realizamos una medición en la cual se determina el estado del primer qubit, tendremos como resultado $|\phi_1\rangle = |0\rangle$ o $|\phi_1\rangle = |1\rangle$ (con igula probabilidad para este caso). La medición tendrá el efecto de colapsar el estado total del sistema segun el resultado obtenido,

$$|\phi_1\rangle_1 \to |0\rangle_1 \Longrightarrow |\Phi\rangle \to |0\rangle_1|1\rangle_2, \tag{3.35}$$

$$|\phi_1\rangle_1 \rightarrow |1\rangle_1 \Longrightarrow |\Phi\rangle \rightarrow |1\rangle_1|0\rangle_2. \tag{3.36}$$

Si conocemos el resultado de la medición $|\phi_1\rangle$, es decir el estado del primer quibit después de la medición, podemos determinar el estado $|\Phi\rangle$ en el que colapso el sistema total y por lo tanto sabremos inmediatamente el estado del segundo qubit: $|1\rangle_2$ si el primer qubit se mide $|0\rangle_1$, o $|0\rangle_2$ si el primer qubit se mide $|1\rangle_1$.

En resumen, para dos qubits en un estado entrelazado el estado de uno de los qubits quedará determinado a partir del estado del otro.

A continuación mostraremos el proceso para crear estados estrelazados a partir de los estados base y el papel que juega la compuerta CNOT en este proceso.

3.4.1 Circuito para entrelazamiento máximo

Se desea encontrar un circuito que permita crear estados entrelazados a partir de estados factorizables. Comenzaremos con un caso particular, el de estados maximamente entrelazados, y luego extenderemos el análisis al caso general.

Para un sistema de dos qubits el operador U_{EM} realiza la transformación

$$|0\rangle|0\rangle \xrightarrow{U_{EM}} \frac{1}{\sqrt{2}}[|0\rangle|0\rangle + |1\rangle|1\rangle], \tag{3.37}$$

$$|0\rangle|1\rangle \xrightarrow{U_{EM}} \frac{1}{\sqrt{2}}[|0\rangle|1\rangle + |1\rangle|0\rangle], \tag{3.38}$$

$$|1\rangle|0\rangle \xrightarrow{U_{EM}} \frac{1}{\sqrt{2}}[|0\rangle|0\rangle - |1\rangle|1\rangle], \tag{3.39}$$

$$|1\rangle|1\rangle \xrightarrow{U_{EM}} \frac{1}{\sqrt{2}}[|0\rangle|1\rangle - |1\rangle|0\rangle], \tag{3.40}$$

en donde los estados después de la transformación son estados de máximo entrelazamiento, tambien llamados *estados de Bell*. El operador U_{EM} que entrelaza

maximamente dos qubits tiene la forma matricial

$$U_{EM} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}. \tag{3.41}$$

Para encontrar el circuito que produce estados de Bell, buscamos la descomposición del operador U_{EM} como el producto de operadores elementales.

Primero observamos que si se aplica el operador U_{EM} a un vector de la forma $|0\rangle|j\rangle$ este lo transformará de la forma

$$U_{EM}|0\rangle|j\rangle = |0\rangle|a\rangle + |1\rangle|b\rangle, \tag{3.42}$$

donde $a = 0$ y $b = 1$ para $j = 0$, o $a = 1$ y $b = 0$ para $j = 1$. Si se aplica a un estado de la forma $|1\rangle|j\rangle$ lo transformará a

$$U_{EM}|1\rangle|j\rangle = |0\rangle|a\rangle - |1\rangle|b\rangle. \tag{3.43}$$

Para el primer qubit esta transformación es similar a la forma en que actúa la compuerta Hadamard (ver tabla 3.1) sobre un qubit,

$$H|0\rangle = |0\rangle + |1\rangle \ , \ H|1\rangle = |0\rangle - |1\rangle. \tag{3.44}$$

Bajo esta observación se propone la factorización de la compuerta Hadamard actuando sobre el primer qubit ($H^{(1)} = H \otimes \mathbb{I}$) en el operador U_{EM},

$$U_{EM} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \tag{3.45}$$

donde la matriz de la derecha multiplicada por el inverso de la raíz cuadrada de dos es la compuerta Hadamard que actúa sobre el primer qubit. De la factorización se observa que la matriz de la izquierda en la ecuación (3.45) es la

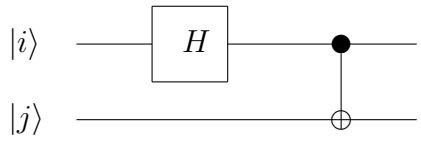

Figura 3.7: Circuito cuántico que prepara un estado maximamente entrelazado de dos qubits a partir de un estado separable $|i\rangle|j\rangle$.

compuerta controlada CNOT, por tanto podemos expresar el operador de etrelazamiento máximo como

$$U_{EM} = U_{CN} H^{(1)} \equiv U_{CN}(H \otimes \mathbb{I}), \tag{3.46}$$

con U_{CN} la compuerta CNOT, $H^{(1)}$ la compuerta Hadamard que actúa en el espacio del primer qubit e $\mathbb{I}$ el operador identidad. De esta representacion obtenemos el circuito cuántico que realiza el entrelazamiento máximo de dos qubits utilizando solo compuertas elementales, que se muestra en la figura 3.7.

Los estados de Bell son casos particulares de estados entrelazados. Buscaremos ahora un circuito para el caso general de entrelazamiento.

3.4.2 Circuito para entrelazamiento arbitrario

Una forma general estados entrelazados es

$$|\phi^+{}_\alpha\rangle = \cos\alpha|0\rangle|0\rangle + \sin\alpha|1\rangle|1\rangle, \tag{3.47}$$

$$|\psi^+{}_\beta\rangle = \cos\beta|0\rangle|1\rangle + \sin\beta|1\rangle|0\rangle, \tag{3.48}$$

$$|\phi^-{}_\alpha\rangle = \sin\alpha|0\rangle|0\rangle - \cos\alpha|1\rangle|1\rangle, \tag{3.49}$$

$$|\psi^-{}_\beta\rangle = \sin\beta|0\rangle|1\rangle - \cos\beta|1\rangle|0\rangle, \tag{3.50}$$

donde α y β determinan el grado de entrelazamiento, que es máximo para $\alpha = \beta = \frac{\pi}{2}$ (estados de Bell). Nuestro objetivo ahora es encontrar un operador

U_E que transforme los vectores de base $|i\rangle|j\rangle$ a los estados con entrelazamiento arbitrario $|\phi^{\pm}\rangle$ y $|\psi^{\pm}\rangle$.

Si aplicamos el operador U_{CN} sobre uno de los estados entrelazados, digamos $|\phi^{+}{}_{\alpha}\rangle$, obtenemos

$$U_{CN}|\phi^{+}{}_{\alpha}\rangle = \cos\alpha U_{CN}|0\rangle|0\rangle + \sin\alpha U_{CN}|1\rangle|1\rangle = \cos\alpha|0\rangle|0\rangle + \sin\alpha|1\rangle|0\rangle. \quad (3.51)$$

El estado a la derecha de la igualdad es factorizable como $[\cos\alpha|0\rangle+\sin\alpha|1\rangle]|0\rangle$. Aplicando nuevamente el operador U_{CN} (que tiene la propiedad $U_{CN}U_{CN} = \mathbb{I}$) recuperamos el estado entrelazado,

$$U_{CN}U_{CN}|\phi^{+}{}_{\alpha}\rangle = \ U_{CN}[\cos\alpha|0\rangle + \sin\alpha|1\rangle]|0\rangle. \quad (3.52)$$

$$|\phi^{+}{}_{\alpha}\rangle = \ U_{CN}[\cos\alpha|0\rangle + \sin\alpha|1\rangle]|0\rangle. \quad (3.53)$$

Procediendo de igual forma para el resto de los estados entrelazados llegamos a las relaciones

$$|\psi^{+}{}_{\beta}\rangle = U_{CN}[\cos\beta|0\rangle + \sin\beta|1\rangle]|1\rangle, \quad (3.54)$$

$$|\phi^{-}{}_{\alpha}\rangle = U_{CN}[\sin\alpha|0\rangle - \cos\alpha|1\rangle]|0\rangle, \quad (3.55)$$

$$|\psi^{-}{}_{\beta}\rangle = U_{CN}[\sin\beta|0\rangle - \cos\beta|1\rangle]|1\rangle, \quad (3.56)$$

donde se observa que el operador U_{CN} esta actuando sobre estados separables. Esto nos indica que la compuerta CNOT es la que realiza el entrelazamiento entre dos qubits.

Continuando con la búsqueda de la descomposición del operador U_E, a partir de las ecuaciones (3.53) - (3.56) requeriremos solo encontrar un operador $U_{\alpha\beta}$ que realice la transformación

$$|0\rangle|0\rangle \xrightarrow{U_{\alpha\beta}} [\cos\alpha|0\rangle + \sin\alpha|1\rangle]|0\rangle, \quad (3.57)$$

$$|0\rangle|1\rangle \xrightarrow{U_{\alpha\beta}} [\cos\beta|0\rangle + \sin\beta|1\rangle]|1\rangle, \tag{3.58}$$

$$|1\rangle|0\rangle \xrightarrow{U_{\alpha\beta}} [\sin\alpha|0\rangle - \cos\alpha|1\rangle]|0\rangle, \tag{3.59}$$

$$|1\rangle|1\rangle \xrightarrow{U_{\alpha\beta}} [\sin\beta|0\rangle - \cos\beta|1\rangle]|1\rangle, \tag{3.60}$$

para que al multiplicarlo por el operador U_{CN} nos de el operador U_E,

$$U_E = U_{CN}U_{\alpha\beta} \tag{3.61}$$

El operador $U_{\alpha\beta}$ que realiza las transformaciones (3.57) - (3.60) tiene la forma matricial

$$U_{\alpha\beta} = \begin{pmatrix} \cos\alpha & 0 & \sin\alpha & 0 \\ 0 & \cos\beta & 0 & \sin\beta \\ \sin\alpha & 0 & -\cos\alpha & 0 \\ 0 & \sin\beta & 0 & -\cos\beta \end{pmatrix}. \tag{3.62}$$

Como primera observación tenemos que el operador no altera el estado del segundo qubit. Tambien tenemos que el operador transforma el primer qubit en función de α si el segundo qubit está en el estado $|0\rangle$, o en función de β si está en el estado $|1\rangle$. El hecho de que actue diferente dependiendo del estado del segundo qubit indica que $U_{\alpha\beta}$ es una compuerta controlada. Este operador es equivalente a aplicar sobre el primer qubit el operador

$$U_\gamma = \begin{pmatrix} \cos\gamma & \sin\gamma \\ \sin\gamma & -\cos\gamma \end{pmatrix}, \tag{3.63}$$

donde γ es α si el segundo qubit es $|0\rangle$, o es β si es $|1\rangle$. Proponemos entonces que el operador $U_{\alpha\beta}$ es equivalente a aplicar sobre el primer qubit una compuerta controlada ${U_\alpha}^{(1)}$, que actua solo si el qubit de control esta en el estado $|0\rangle$, y aplicar una compuerta controlada ${U_\beta}^{(1)}$, que actua si el qubit de control esta en

el estado $|1\rangle$,

$$U_{\alpha\beta} = U^{(1)}_{\alpha|0\rangle} U^{(1)}_{\beta|1\rangle}. \tag{3.64}$$

Una compuerta controlada que depende de que el qubit de control sea $|0\rangle$ para actuar es equivalente a una compuerta que depende que el qubit de control sea $|1\rangle$ si se invierte el estado del qubit de control antes y después de que actúe la compuerta, como se indica en la ecuación (3.22). Por lo tanto podemos representar el operador $U_{\alpha\beta}$ como

$$U_{\alpha\beta} = U_\beta X^{(2)} U_\alpha X^{(2)}, \tag{3.65}$$

donde $X^{(2)}$ es al compuerta NOT que actúa sobre el segundo qubit y los operadores U_α y U_β tienen la forma matricial

$$U_\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\alpha & 0 & \sin\alpha \\ 0 & 0 & 1 & 0 \\ 0 & \sin\alpha & 0 & -\cos\alpha \end{pmatrix}, \; U_\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\beta & 0 & \sin\beta \\ 0 & 0 & 1 & 0 \\ 0 & \sin\beta & 0 & -\cos\beta \end{pmatrix}. \tag{3.66}$$

Por último realizamos el producto del operador U_{CN} por operador $U_{\alpha\beta}$, con lo que obtenemos que el operador U_E para entrelazamiento arbitrario de dos qubits se puede representar como

$$U_E(\alpha,\beta)|i\rangle|j\rangle = U_{CN}U_{\alpha\beta}|i\rangle|j\rangle = U_{CN}U_\beta X^{(2)} U_\alpha X^{(2)}|i\rangle|j\rangle. \tag{3.67}$$

El operador U_E tiene la forma matricial

$$U_E(\alpha,\beta) = \begin{pmatrix} \cos\alpha & 0 & \sin\alpha & 0 \\ 0 & \cos\beta & 0 & \sin\beta \\ 0 & \sin\beta & 0 & -\cos\beta \\ \sin\alpha & 0 & -\cos\alpha & 0 \end{pmatrix}. \tag{3.68}$$

El circuito de entrelazamiento arbitrario se muestra en la figura 3.8.

En la sección 3.2 demostramos que una compuerta controlada con un qubit de

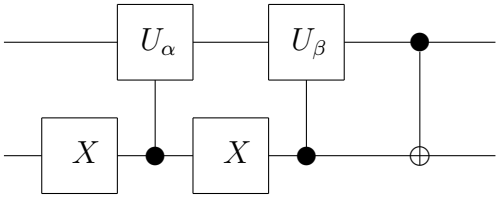

Figura 3.8: Circuito cuántico que prepara estados de dos qubits con entrelazamiento arbitrario a partir de estados factorizables. El grado de entrelazamiento depende del valor de α y β.

control y uno objetivo puede ser representada como el producto de compuertas que actúan en el espacio de un qubit y compuertas CNOT exclusivamente, según la ecuación (3.32). Daremos esta representación para las compuertas controladas U_α y U_β, con lo que obtendremos el circuito de entrelazamiento arbitrario que utiliza solo compuertas que actúan sobre un qubit y compuertas CNOT.

Para U_α tenemos la representación

$$U_\alpha|i\rangle|j\rangle = R_a{}^{(2)} A_\alpha^{(1)} U_{NC} B_\alpha^{(1)} U_{NC} C_\alpha^{(1)} |i\rangle|j\rangle, \tag{3.69}$$

donde la compuerta U_{NC} es la compuerta CNOT que actúa sobre el primer qubit teniendo como control el segundo qubit. La compuerta U_α tiene como objetivo el primer qubit, de aquí la diferencia con la descomposición hecha para $U(2)$ en la ecuación (3.32), que tiene como objetivo el segundo qubit.

Desarrollamos el producto $(\mathbb{I}\otimes R_a)(A\otimes\mathbb{I})U_{NC}(B\otimes\mathbb{I})U_{NC}(C\otimes\mathbb{I})$ y lo igualamos con la matriz U_α para encontrar que los operadores en los que se descompone U_α tienen la forma matricial

$$R_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\imath\frac{\pi}{2}} \end{pmatrix}. \tag{3.70}$$

$$A_\alpha = \begin{pmatrix} \cos(\frac{\alpha}{2}) & -\sin(\frac{\alpha}{2}) \\ \sin(\frac{\alpha}{2}) & \cos(\frac{\alpha}{2}) \end{pmatrix}, \tag{3.71}$$

$$B_\alpha = \begin{pmatrix} e^{-\imath\frac{\pi}{4}}\cos(\frac{\alpha}{2}) & e^{\imath\frac{\pi}{4}}\sin(\frac{\alpha}{2}) \\ -e^{-\imath\frac{\pi}{4}}\sin(\frac{\alpha}{2}) & e^{\imath\frac{\pi}{4}}\cos(\frac{\alpha}{2}) \end{pmatrix}, \tag{3.72}$$

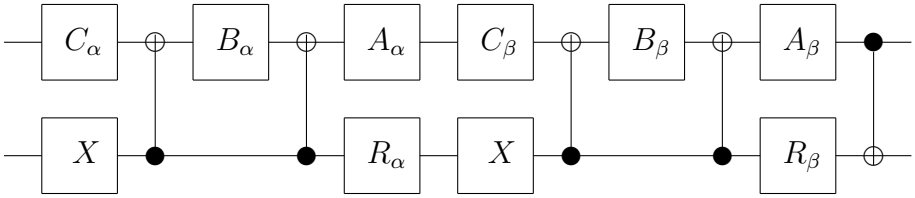

Figura 3.9: Circuito de entrelazamiento arbitrario que utiliza unicamente compuertas CNOT y compuertas que actúan sobre solo un qubit.

$$C_\alpha = \begin{pmatrix} e^{\imath\frac{\pi}{4}} & 0 \\ 0 & e^{-\imath\frac{\pi}{4}} \end{pmatrix}. \tag{3.73}$$

Estas ecuaciones nos dan el valor de los operadores A_α, B_α y C_α en función del parametro α.

El operador U_β tendrá una representación similar a la de U_α ya que sus formas matriciales son equivalentes. Por lo tanto

$$U_\beta|i\rangle|j\rangle = R_\beta^{(2)} A_\beta{}^{(1)} U_{NC} B_\beta{}^{(1)} U_{NC} C_\beta{}^{(1)} |i\rangle|j\rangle, \tag{3.74}$$

donde las matrices A_β, B_β y C_β son iguales a las matrices A_α, B_α, y C_α, respectivamente, excepto que se cambia el valor del parametro α por el valor del parametro β en las ecuaciones (3.71) - (3.73).

Finalmente tenemos que el operador de entrelazamiento arbitrario U_E se puede representar como

$$U_E(\alpha,\beta) = U_{CN} R_\beta{}^{(2)} A_\beta{}^{(1)} U_{NC} B_\beta{}^{(1)} U_{NC} C_\beta{}^{(1)} X^{(2)} R_\alpha{}^{(2)} A_\alpha{}^{(1)} U_{NC} B_\alpha{}^{(1)} U_{NC} C_\alpha{}^{(1)} X^{(2)}. \tag{3.75}$$

El circuito cuántico correspondiente a esta representación se muestra en la figura 3.9.

Para el caso especial en que $\alpha = \beta$ el operador $U_{\alpha\beta}$ se puede factorizar como

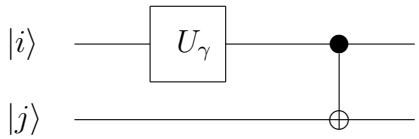

Figura 3.10: Circuito cuántico que prepara estados entrelazados con un grado arbitrario de entrelazamiento. El entrelazamiento es máximo para γ igual a valores semienteros de π y desaparece para γ igual a valores enteros de π.

el producto tensorial

$$U_{\alpha,\beta=\alpha} = \begin{pmatrix} \cos\alpha & 0 & \sin\alpha & 0 \\ 0 & \cos\alpha & 0 & \sin\alpha \\ \sin\alpha & 0 & -\cos\alpha & 0 \\ 0 & \sin\alpha & 0 & -\cos\alpha \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{3.76}$$

que tiene la misma forma que el operador U_γ (ver ecuación (3.63)) que actúa sobre el primer qubit, independientemente del estado del segundo qubit; en este caso no hay compuertas controladas. El operador de entrelazamiento cuando los angulos α y β son iguales sera entonces

$$U_E(\alpha)|i\rangle|j\rangle = U_{CN}{U_{\gamma=\alpha}}^{(1)}|i\rangle|j\rangle. \tag{3.77}$$

El circuito cuántico correspondiente se muestra en la figura 3.10. Se puede apreciar que resulta más simple que el circuito en la figura 3.9, el cual prepara estados con diversos grados de entrelazamiento, por lo que es más fácil de implementar experimentalmente.

Para el caso en que $\alpha = \beta = \frac{\pi}{2}$ los estados $|\phi^\pm\rangle$ y $|\psi^\pm\rangle$ que se preparan son estados de Bell. En este caso la matriz U_γ resulta en la compuerta Hadamard,

$$U_E(\frac{\pi}{2})|i\rangle|j\rangle = U_{CN}H^{(1)}|i\rangle|j\rangle. \tag{3.78}$$

Esta relación verifica el análisis hecho en la subsección 3.4.1.

Utilizando las herramientas vistas y los resultados obtenidos a lo largo del

capítulo seremos capaces de prepara estados arbitrarios para sistemas de pares de qubits, que es en lo que se enfoca el siguiente capítulo.

Capítulo 4

Preparacion de estados de dos qubits

En este capítulo nos enfocaremos en la preparación de estados arbitrarios para sistemas de dos qubits. Con este fin se introduce la *descomposición de Schmidt* de un tensor que, para un estado dado, nos identifica su carácter de entrelazamiento. Esta representación nos permitirá sintetizar el circuito que prepara estados arbitrario de dos qubits.

4.1 Valores singulares y descomposición de Schmidt

Dada una matriz M de dimensión $m \times n$, podemos expresar esta matriz como el producto

$$M_{mn} = A_{mm} D_{mn} {B_{nn}}^{\dagger}, \tag{4.1}$$

donde A y B son matrices unitarias ($AA^{\dagger} = BB^{\dagger} = \mathbb{I}$). En el caso de que M sea una matriz cuadrada, la matriz D será una matriz diagonal ($D_{ij} = 0$ para $i \neq j$) cuyos elementos de la diagonal corresponden a los *valores singulares* de la matriz M.

Los valores singulares son la raíz positiva de los valores propios de $MM^{\dagger}$ [3,

pag. 156],

$$det(MM^{\dagger} - \lambda I) = 0, \tag{4.2}$$

donde $det(U)$ es el determinante de U y $M^{\dagger}$ es el hermítico conjugado de M. Los elementos de la diagonal de la matriz D serán entonces

$$D = \begin{pmatrix} \sqrt{\lambda_1} & 0 & 0 & \cdots \\ 0 & \sqrt{\lambda_2} & 0 & \cdots \\ 0 & 0 & \sqrt{\lambda_3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{4.3}$$

Primero se calcula la matriz D a partir de las ecuaciones (4.2) y (4.3), y luego se determinan las matrices A y B a partir de la matriz D: Multiplicando la matriz M por su hermítico conjugado $M^{\dagger} = (ADB^{\dagger})^{\dagger} = BDA^{\dagger}$ obtenemos el producto

$$MM^{\dagger} = (ADB^{\dagger})(BDA^{\dagger}) = AD^2A^{\dagger}. \tag{4.4}$$

Esta es la descomposición de valores propios de la matriz resultado del producto $MM^{\dagger}$. La descomposición de valores propios de una matriz nos dice que una matriz μ puede representarse como

$$\mu = E\Lambda E^{-1}, \tag{4.5}$$

donde la matriz Λ es una matriz diagonal cuyos elementos son los valores propios de μ, y donde las columnas de la matriz E son los vectores propios de μ [4, pag. 288]. Por tanto, la ecuación (4.4) nos dice que la matriz A se forma al colocar como columnas los vectores propios de la matriz $(MM^{\dagger})$.

Si ahora realizamos el producto $M^{\dagger}M$ obtenemos la ecuación

$$M^{\dagger}M = BD^2B^{\dagger}. \tag{4.6}$$

que, bajo el mismo argumento hecho para la matriz A, nos indica que los vectores propios de la matriz $(M^{\dagger}M)$ son las columnas de la matriz B. Calculando las matrices A, B y D es como definimos la descomposición de valores singulares para una matriz M dada.

La descomposición de valores singulares de una matriz nos permitirá encontrar la descomposición de Schmidt de los estados cuánticos.

4.1.1 Descomposición de Schmidt

Pasamos a encontrar la descomposición de Schmidt par un estado arbitrario utilizando la descomposición de valores singulares.

Dado un estado $|\Psi\rangle$ para un sistema de dos qubits, podemos expresar este estado como

$$|\Psi\rangle = \sum_i \sum_j c_{ij}|i\rangle|j\rangle, \tag{4.7}$$

donde los coeficientes c_{ij} satisfacen la condición de normalización. Podemos interpretar el coeficiente c_{ij} como el término (i, j) de una matriz C. Como los indices i y j corren ambos de 0 a 1 para el caso de qubits, la matriz C será una matriz cuadrada de dimensión 2×2. Utilizando la descomposición de valores singulares (4.1) para la matriz C tendremos que

$$\begin{aligned} |\Psi\rangle &= \sum_i \sum_j (ADB^\dagger)_{ij}|i\rangle|j\rangle \\ &= \sum_i \sum_j \sum_k A_{ik} D_{kk} {B^\dagger}_{kj}|i\rangle|j\rangle \\ &= \sum_k D_{kk} (\sum_i A_{ik}|i\rangle)(\sum_j {B^\dagger}_{kj}|j\rangle). \end{aligned} \tag{4.8}$$

Definimos los términos

$$\chi_k \equiv D_{kk} \ , \ |A_k\rangle \equiv \sum_i A_{ik}|i\rangle \ , \ |B_k\rangle \equiv \sum_j {B^\dagger}_{kj}|j\rangle, \tag{4.9}$$

con lo que llegamos finalmente a la expresión

$$|\Psi\rangle = \sum_k \chi_k |A_k\rangle|B_k\rangle. \tag{4.10}$$

Esta representación es conocida como la descomposición de Schmidt y los

términos χ_k se conocen como *coeficientes de Schmidt*.

La descomposición de Schmidt nos permitirá encontrar el circuito cuántico para preparación de estados arbitrarios de dos qubits.

4.1.2 Descomposición de Schmidt para estados de dos qubits

Buscaremos ahora la descomposición de Schmidt de un estado arbitrario para sistemas de dos qubits. Esta representación nos dará el circuito cuántico para preparación de estados arbitrarios.

Podemos expresar un estado $|\Psi\rangle$ en la base $|i\rangle|j\rangle$ de los qubits como

$$|\Psi\rangle = c_{00}|0\rangle|0\rangle + c_{01}|0\rangle|1\rangle + c_{10}|1\rangle|0\rangle + c_{11}|1\rangle|1\rangle, \tag{4.11}$$

con la condición de normalización $|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$. Definimos los coeficientes c_{ij} como las componentes (i, j) de una matriz C_S de dimensión 2×2, tal que esta matriz resulta como

$$C_S = \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix}. \tag{4.12}$$

Obtenemos la descomposición de valores singulares de la matriz C_S

$$C_S = A_S D B_S{}^\dagger, \tag{4.13}$$

donde A_S y B_S son matrices unitarias y D es una matriz diagonal. Las componentes de la matriz D, según lo visto en la sección 4.1, seran la raíz positiva de los valores propios λ dados por

$$det(C_S C_S{}^\dagger - \lambda I) = 0. \tag{4.14}$$

El determinante de $C_S {C_S}^\dagger$ es

$$
\begin{aligned}
det(C_S {C_S}^\dagger - \lambda I) &= \begin{vmatrix} |c_{00}|^2 + |c_{01}|^2 - \lambda & c_{00}{c_{10}}^* + c_{01}{c_{11}}^* \\ {c_{00}}^* c_{10} + {c_{01}}^* c_{11} & |c_{10}|^2 + |c_{11}|^2 - \lambda \end{vmatrix} \\
&= (|c_{00}|^2 + |c_{01}|^2 - \lambda)(|c_{10}|^2 + |c_{11}|^2 - \lambda) - (c_{00}{c_{10}}^* + c_{01}{c_{11}}^*)({c_{00}}^* c_{10} + {c_{01}}^* c_{11}) \\
&= \lambda^2 - \lambda + (c_{00}c_{11} - c_{01}c_{10})({c_{00}}^* {c_{11}}^* - {c_{01}}^* {c_{10}}^*).
\end{aligned} \tag{4.15}
$$

Igualando este determinante a 0 y utilizando la formula general, obtenemos los valores propios

$$\lambda_\pm = \frac{1}{2} \pm \sqrt{\frac{1}{4} - |c_{00}c_{11} - c_{01}c_{10}|^2}, \tag{4.16}$$

que nos definen la matriz D

$$D = \begin{pmatrix} \sqrt{\lambda_-} & 0 \\ 0 & \sqrt{\lambda_+} \end{pmatrix}. \tag{4.17}$$

Para definir la matriz A_S es necesario encontrar los vectores propios de $C_S {C_S}^\dagger$,

$$C_S {C_S}^\dagger \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}. \tag{4.18}$$

Dada la matriz C_S tenemos que

$$\begin{pmatrix} |c_{00}|^2 + |c_{01}|^2 - \lambda_\pm & c_{00}{c_{10}}^* + c_{01}{c_{11}}^* \\ {c_{00}}^* c_{10} + {c_{01}}^* c_{11} & |c_{10}|^2 + |c_{11}|^2 - \lambda_\pm \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0, \tag{4.19}$$

$$\begin{pmatrix} x_1(|c_{00}|^2 + |c_{01}|^2 - \lambda_\pm) + x_2(c_{00}{c_{10}}^* + c_{01}{c_{11}}^*) \\ x_1({c_{00}}^* c_{10} + {c_{01}}^* c_{11}) + x_2(|c_{10}|^2 + |c_{11}|^2 - \lambda_\pm) \end{pmatrix} = 0. \tag{4.20}$$

De esta ecuación despejamos uno de los valores indeterminados para obtener

$$x_2 = \frac{x_1(\lambda_\pm - |c_{00}|^2 - |c_{01}|^2)}{c_{00}{c_{10}}^* + c_{01}{c_{11}}^*}, \tag{4.21}$$

con lo que los vectores propios resultan en

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ \frac{\lambda_\pm - |c_{00}|^2 - |c_{01}|^2}{c_{00}{c_{10}}^* + c_{01}{c_{11}}^*} \end{pmatrix}. \tag{4.22}$$

El segundo valor se determina a partir de la normalización del vector propio

$$|x_1|^2 + |x_2|^2 = 1, \tag{4.23}$$

obteniendo

$$x_1 = \left(1 + \frac{(\lambda_\pm - |c_{00}|^2 - |c_{01}|^2)^2}{|c_{00}c_{11} + c_{01}c_{10}|^2 + (|c_{00}|^2 - |c_{01}|^2)(|c_{10}|^2 - |c_{11}|^2)}\right)^{-1/2} \tag{4.24}$$

Utilizando los vectores propios como las columnas de la matriz A_S, obtenemos finalmente que

$$A_S = \begin{pmatrix} x_1(\lambda_-) & x_1(\lambda_+) \\ x_2(\lambda_-) & x_2(\lambda_+) \end{pmatrix}, \tag{4.25}$$

donde las entradas $(A_S)_{ij}$ estan dadas por los valores x_1 y x_2 utilizando los dos valores propios.

Para definir la matriz B_S se utiliza un método similar al utilizado para definir la matriz A_S. Se buscan los valores y vectores propios de ${C_S}^\dagger C_S$,

$${C_S}^\dagger C_S = \begin{pmatrix} |c_{00}|^2 + |c_{01}|^2 & {c_{00}}^* c_{10} + {c_{01}}^* c_{11} \\ c_{00}{c_{10}}^* + c_{01}{c_{11}}^* & |c_{10}|^2 + |c_{11}|^2 \end{pmatrix}. \tag{4.26}$$

Primero, los valores propios de ${C_S}^\dagger C_S$ estan dados por

$$\begin{aligned} det({C_S}^\dagger C_S - \lambda' I) &= \begin{vmatrix} |c_{00}|^2 + |c_{01}|^2 - \lambda' & {c_{00}}^* c_{10} + {c_{01}}^* c_{11} \\ c_{00}{c_{10}}^* + c_{01}{c_{11}}^* & |c_{10}|^2 + |c_{11}|^2 - \lambda' \end{vmatrix} \\ &= (|c_{00}|^2 + |c_{01}|^2 - \lambda)(|c_{10}|^2 + |c_{11}|^2 - \lambda) - ({c_{00}}^* c_{10} + {c_{01}}^* c_{11})(c_{00}{c_{10}}^* + c_{01}{c_{11}}^*) \\ &= \lambda^2 - \lambda + (c_{00}c_{11} - c_{01}c_{10})({c_{00}}^* {c_{11}}^* - {c_{01}}^* {c_{10}}^*). \end{aligned} \tag{4.27}$$

Se observa que el determinante es igual al de la ecuación (4.15), por lo tanto los valores propios de ${C_S}^\dagger C_S$ serán los valores $\lambda_\pm$ encontrados anteriormente. Los vectores propios se calculan al resolver

$$\begin{pmatrix} |c_{00}|^2 + |c_{01}|^2 - \lambda_\pm & {c_{00}}^* c_{10} + {c_{01}}^* c_{11} \\ c_{00}{c_{10}}^* + c_{01}{c_{11}}^* & |c_{10}|^2 + |c_{11}|^2 - \lambda_\pm \end{pmatrix} \begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = 0, \tag{4.28}$$

$$\begin{pmatrix} x_1'(|c_{00}|^2 + |c_{01}|^2 - \lambda_\pm) + x_2'({c_{00}}^* c_{10} + {c_{01}}^* c_{11}) \\ x_1'(c_{00}{c_{10}}^* + c_{01}{c_{11}}^*) + x_2'(|c_{10}|^2 + |c_{11}|^2 - \lambda_\pm) \end{pmatrix} = 0. \tag{4.29}$$

De aquí podemos despejar uno de los valores indeterminados como

$$x_2' = \frac{x_1'(\lambda_\pm - |c_{00}|^2 - |c_{01}|^2)}{{c_{00}}^* c_{10} + {c_{01}}^* c_{11}}, \tag{4.30}$$

y a partir de la condición de normalización se obtiene

$$x_1' = \left(1 + \frac{(\lambda_\pm - |c_{00}|^2 - |c_{01}|^2)^2}{|c_{00}c_{11} + c_{01}c_{10}|^2 + (|c_{00}|^2 - |c_{01}|^2)(|c_{10}|^2 - |c_{11}|^2)}\right)^{-1/2} \tag{4.31}$$

Comparando los términos x_1' y x_2' con x_1 y x_2 en las ecuaciones (4.24) y (4.21), respectivamente, se observa que podemos expresar los términos como

$$x_1' = {x_1}^* \ , \ x_2' = {x_2}^*, \tag{4.32}$$

por lo que la matriz B_S estara dada como

$$B_S = \begin{pmatrix} {x_1}^*(\lambda_-) & {x_1}^*(\lambda_+) \\ {x_2}^*(\lambda_-) & {x_2}^*(\lambda_+) \end{pmatrix}, \tag{4.33}$$

Reuniendo los resultados de esta sección encontramos finalmente que la matriz C_S, cuyos entradas c_{ij} son los coeficientes de los vectores $|i\rangle|j\rangle$ para el estado arbitrario de un sistema de dos qubits, puede expresarse como

$$C_S = A_S D {B_S}^\dagger = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} \sqrt{\lambda_-} & 0 \\ 0 & \sqrt{\lambda_+} \end{pmatrix} \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix}, \tag{4.34}$$

donde los valores a_k estan definidos como

$$a_1 = \left(1 + \frac{(\lambda_- - |c_{00}|^2 - |c_{01}|^2)^2}{|c_{00}c_{11} + c_{01}c_{10}|^2 + (|c_{00}|^2 - |c_{01}|^2)(|c_{10}|^2 - |c_{11}|^2)}\right)^{-1/2}, \tag{4.35}$$

$$a_2 = \left(1 + \frac{(\lambda_+ - |c_{00}|^2 - |c_{01}|^2)^2}{|c_{00}c_{11} + c_{01}c_{10}|^2 + (|c_{00}|^2 - |c_{01}|^2)(|c_{10}|^2 - |c_{11}|^2)}\right)^{-1/2}, \tag{4.36}$$

$$a_3 = \frac{\lambda_- - |c_{00}|^2 - |c_{01}|^2}{c_{00}{c_{10}}^* + c_{01}{c_{11}}^*}\left(1 + \frac{(\lambda_+ - |c_{00}|^2 - |c_{01}|^2)^2}{|c_{00}c_{11} + c_{01}c_{10}|^2 + (|c_{00}|^2 - |c_{01}|^2)(|c_{10}|^2 - |c_{11}|^2)}\right)^{-1/2}, \tag{4.37}$$

$$a_4 = \frac{\lambda_+ - |c_{00}|^2 - |c_{01}|^2}{c_{00}{c_{10}}^* + c_{01}{c_{11}}^*}\left(1 + \frac{(\lambda_+ - |c_{00}|^2 - |c_{01}|^2)^2}{|c_{00}c_{11} + c_{01}c_{10}|^2 + (|c_{00}|^2 - |c_{01}|^2)(|c_{10}|^2 - |c_{11}|^2)}\right)^{-1/2}. \tag{4.38}$$

Los valores $\lambda_\pm$ serán

$$\lambda_\pm = \frac{1}{2} \pm \sqrt{\frac{1}{4} - |c_{00}c_{11} - c_{01}c_{10}|^2}. \tag{4.39}$$

Esta representación nos permite encontrar la descomposición de Schmidt de un estado arbitrario $|\Psi\rangle$ para un sistema de dos qubits,

$$|\Psi\rangle = \chi_0|A_0\rangle|B_0\rangle + \chi_1|A_1\rangle|B_1\rangle, \tag{4.40}$$

donde estan definidos los estados

$$|A_i\rangle = A_S|i\rangle = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\begin{pmatrix} i \\ 1-i \end{pmatrix}, \tag{4.41}$$

$$|B_j\rangle = {B_S}^\dagger|j\rangle = \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix}\begin{pmatrix} j \\ 1-j \end{pmatrix}, \tag{4.42}$$

y donde los coeficientes de Schmidt χ_k están dados por

$$\chi_0{}^2 = \frac{1}{2} - \sqrt{\frac{1}{4} - |c_{00}c_{11} - c_{01}c_{10}|^2}\ ,\ \chi_1{}^2 = \frac{1}{2} + \sqrt{\frac{1}{4} - |c_{00}c_{11} - c_{01}c_{10}|^2}. \quad (4.43)$$

La descomposición de Schmidt nos servirá para sintetizar un circuito que permita preparar cualquier estado para un sistema de dos qubits.

4.2 Circuito para preparación de un estado arbitrario de dos qubits

Dada la descomposición de Schmidt para un sistema de dos qubits,

$$|\Psi\rangle = \chi_0|A_0\rangle|B_0\rangle + \chi_1|A_1\rangle|B_1\rangle, \quad (4.44)$$

nos interesa encontrar un circuito que transforme los estados en la base de los qubits $|i\rangle|j\rangle$ a la base de Schmidt. Este circuito será capaz de preparar cualquier estado de dos qubits.

Buscamos el operador U_S que realiza la transformación

$$|0\rangle|0\rangle \xrightarrow{U_S} \chi_0|A_0\rangle|B_0\rangle + \chi_1|A_1\rangle|B_1\rangle, \quad (4.45)$$

donde los términos χ_0 y χ_1 son los coeficientes de Schmidt (4.43) definidos entre 0 y 1, que cumplen con la condición de normalización $\chi_0{}^2 + \chi_1{}^2 = 1$. El lado derecho de la ecuación (4.45) es la descomposición de Schmidt de un estado arbitrario, por lo que el operador U_S que realiza esta transformación nos permite preparar cualquier estado a partir del estado $|0\rangle|0\rangle$.

Los estados $|A_i\rangle$ y $|B_j\rangle$ pueden representarse a partir de los operadores A_S y B_S y los estados $|0\rangle$ y $|1\rangle$,

$$\begin{aligned}\chi_0|A_0\rangle|B_0\rangle + \chi_1|A_1\rangle|B_1\rangle &= \chi_0 A|0\rangle B^\dagger|0\rangle + \chi_1 A|1\rangle B^\dagger|1\rangle \\ &= {A_S}^{(1)}{B_S}^{\dagger(2)}[\chi_0|0\rangle|0\rangle + \chi_1|1\rangle|1\rangle],\end{aligned} \quad (4.46)$$

donde factorizamos los operadores A_S y ${B_S}^\dagger$ que actúan sobre el primer y segundo qubit, respectivamente. A partir de aquí solo es necesario buscar un operador S que realice la transformación

$$|0\rangle|0\rangle \xrightarrow{S} \chi_0|0\rangle|0\rangle + \chi_1|1\rangle|1\rangle, \tag{4.47}$$

tal que al multiplicarlo por los operadores A_S y B_S resulte en el operador U_S,

$$U_S = {A_S}^{(1)} {B_S}^{(2)} S. \tag{4.48}$$

Si al estado que se desea prepara le aplicamos dos compuertas CNOT continuas (recordadndo que $U_{CN}U_{CN} = \mathbb{I}$), obtenemos

$$U_{CN}U_{CN}[\chi_0|0\rangle|0\rangle + \chi_1|1\rangle|1\rangle] = U_{CN}[\chi_0|0\rangle|0\rangle + \chi_1|1\rangle|0\rangle]. \tag{4.49}$$

El estado a la derecha de la identidad es un estado separable, que podemos obtener si aplicamos el operador ${U_\chi}^{(1)}$ al estado $|0\rangle|0\rangle$, siendo este operador

$$U_\chi = \begin{pmatrix} \chi_0 & \chi_1 \\ \chi_1 & -\chi_0 \end{pmatrix}. \tag{4.50}$$

El operador S es igual al producto $S = U_{CN}U_\chi$. Por lo tanto, el operador U_S que permite preparar cualquier estado a partir del estado $|0\rangle|0\rangle$,

$$|\Psi\rangle = U_S|0\rangle|0\rangle, \tag{4.51}$$

esta dado por

$$U_S = {A_S}^{(1)} {B_S}^{\dagger(2)} U_{CN} {U_\chi}^{(1)}, \tag{4.52}$$

donde los operadores A_S y ${B_S}^\dagger$ tienen la forma matricial

$$A_S = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \ , \ {B_S}^\dagger = \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix}, \tag{4.53}$$

cuyas entradas a_i se relacionan con el estado a preparar $|\Psi\rangle$ como lo indican las ecuaciones (4.35) - (4.38). El circuito cuántico que prepara un estado arbitrario

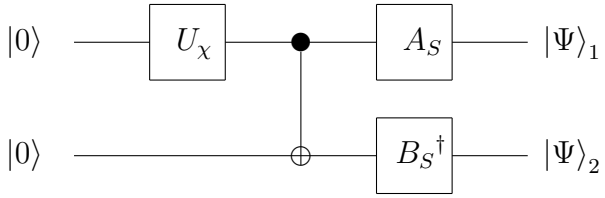

Figura 4.1: Circuito cuántico que prepara un estado arbitrario $|\Psi\rangle$ de dos qubits a partir del estado $|0\rangle|0\rangle$.

a partir del estado $|0\rangle|0\rangle$ se muestra en la figura 4.1.

Cabe destacar que las dos primeras compuertas del circuito que prepara un estado arbitrario son iguales al circuito de entrelazamiento arbitrario (ver figura 3.10). Esto nos indica que para preparar un estado arbitrario primero se prepara el entrelazamiento del estado, sí es que tiene algun grado de entrelazamiento, y luego se actúa individualmente sobre los qubits.

Una vez vista la preparación de estado de dos qubits, pasamos a extender nuestro análisis a sistemas de múltiples qubits.

Capítulo 5

Múltiples qubits

Extenderemos el estudio hecho para pares de qubits y qubits individuales a sistemas de múltiples qubits, con el objetivo de encontrar el circuito cuánticos que prepara estados arbitrarios para estos sistemas.

Primero daremos los vectores de estado y la forma en que etiquetaremos estos vectores en el caso de sistemas de multi-qubits, lo que nos permitirá realizar el desarrollo matemático en el resto de este trabajo.

5.1 Vectores de estado para sistemas de múltiples qubits

Utilizando el mismo razonamiento que para el caso de dos qubits (seccion 2.1.2), podemos establecer los vectores de estado para un sistema de múltiples qubits. Los vectores de base están dados por el producto tensorial de todas las combinaciones de los estados de los qubits individuales, por lo que para un sistema de n qubits tendremos 2^n vectores de base. Para n qubits los vectores de base serán

$$\begin{aligned} &|00...00\rangle \equiv |0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |0\rangle_{n-1} \otimes |0\rangle_n \ , \ |00...01\rangle \equiv |0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |0\rangle_{n-1} \otimes |1\rangle_n, \\ &|00...10\rangle \equiv |0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |1\rangle_{n-1} \otimes |0\rangle_n \ , \ |00...01\rangle \equiv |0\rangle_1 \otimes |0\rangle_2 \otimes ... \otimes |1\rangle_{n-1} \otimes |1\rangle_n \dots \end{aligned} \tag{5.1}$$

Según nuestra conveción adoptada, los vectores de base tendrán la forma

matricial

$$|00...00\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, |00...01\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \cdots, |11...10\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, |11...11\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{5.2}$$

Par un sistema con un gran numero de qubits es conveniente etiquetar los vectores de estado de una forma simplificada; utilizaremos los números naturales para remplazar la secuencia de ceros y unos según su equivalente en numeración binaria, de tal forma que

$$|0\rangle \equiv |00...00\rangle \ , \ |1\rangle \equiv |00...01\rangle, \ \ \ldots \ , |2^n - 2\rangle \equiv |11...10\rangle \ , \ |2^n - 1\rangle \equiv |11...11\rangle. \tag{5.3}$$

Una vez establecida la convención para los vectores estado, continuamos con el anaĺisis de las compuertas cuánticas controladas por múltiples qubits y la convención que adoptaremos para denotar la forma en que actúan.

5.2 Compuertas con dos qubits de control

Primero estableceremos la convención para las compuertas controladas en función de los qubits de control y los qubits objetivo. Supongamos un operador U que actúa en un sistema de tres qubits $|c\rangle_1|i\rangle_2|t\rangle_3$, tal que el primer qubit $|c\rangle_1$ es el qubit de control y el tercer qubit $|t\rangle_3$ será el qubit objetivo. Utilizaremos la notación $U^{(c,t)}$ para denotar que la compuerta U actúa en el espacio de los qubits $|c\rangle_1$ y $|t\rangle_3$, teniendo $|c\rangle$ como control y $|t\rangle$ como objetivo. En el caso en el que se requiera que el estado del qubit de control sea $|1\rangle$ para que la compuerta controlada U actúe, se tendrá la ecuación

$$U^{(c,t)}|c\rangle|i\rangle|t\rangle = |c\rangle|i\rangle U^c|t\rangle, \tag{5.4}$$

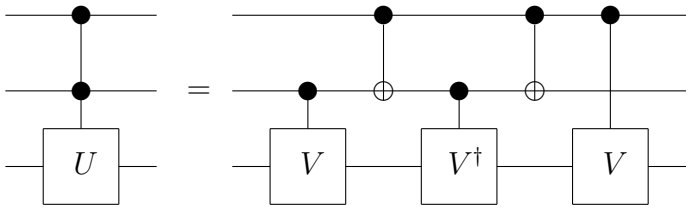

Figura 5.1: Representación de una compuerta U controlada por dos qubits como compuertas V controladas por un qubit y compuertas CNOT con $V^2 = U$.

donde el término c en la parte derecha de la ecuación es el exponente del operador U, actuando de igual forma como que se vio en la subsección 3.2.1 para sistemas de dos qubits.

Para una compuerta U con dos qubits de control $|c_1\rangle$ y $|c_2\rangle$, utilizaremos la notación $U^{(c_1c_2,t)}$, y en el caso de que requiera el estado $|1\rangle$ en ambos qubits de control para actuar tendremos la ecuación

$$U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle = |c_1\rangle|c_2\rangle U^{c_1\cdot c_2}|t\rangle, \tag{5.5}$$

donde el término $c_1 \cdot c_2$ en el exponente de U denota el producto del valor numérico de c_1 y c_2.

Una compuerta con dos qubits de control puede descomponerse como el producto de compuertas con un qubit de control y compuertas CNOT, segun la ecuación

$$U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle = V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}V^{\dagger(c_2,t)}{U_{CN}}^{(c_1,c_2)}V^{(c_2,t)}|c_1\rangle|c_2\rangle|t\rangle, \tag{5.6}$$

con $V^2 = U$. La demostración de esta identidad se da en el Apendice A.1 y su representación como circuito cuántico se encuentra en la figura 5.1.

Las compuertas controladas V pueden a su vez descomponerse en función de compuertas que actúan sobre un solo qubit y compuertas CNOT, visto en la sección 3.3.1. De esta forma podemos encontrar la representación de una compuerta arbitraria con dos qubits de control como el producto compuertas que actuan sobre un qubit y compuertas CNOT.

Una compuerta con dos qubits de control de gran importancia es la compuerta

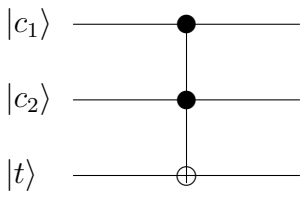

Figura 5.2: Diagrama de la compuerta U_{CCN} (Toffoli). El qubit $|t\rangle$ invertira su estado si $|c_1\rangle = |1\rangle$ y $|c_2\rangle = |1\rangle$, de otra forma no será alterado.

Toffoli, la cual introduciremos a continuación. Esta compuerta nos ayudara a ilustrar la forma en que actúan compuertas con dos qubits de control y la notación adoptada.

5.2.1 Compuerta Toffoli

Para un sistema de tres qubits existe un análogo a la compuerta CNOT, que es la compuerta Toffoli, también llamada compuerta *CCNOT*, que representaremos con el operador U_{CCN}. Cuando los dos primeros qubits son los qubits de control y el tercero es el qubit objetivo, la compuerta Toffoli tiene forma matricial

$$U_{CCN} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \tag{5.7}$$

y su representación como elemento de un circuito cuántico se muestra en la figura 5.2.

La compuerta Toffoli actúa invirtiendo el estado del qubit objetivo si el estado de los dos qubits de control es $|1\rangle$. Esto es equivalente a la expresión

$$U_{CCN}|c_1\rangle|c_2\rangle|t\rangle = |c_1\rangle|c_2\rangle X^{c_1 \cdot c_2}|t\rangle. \tag{5.8}$$

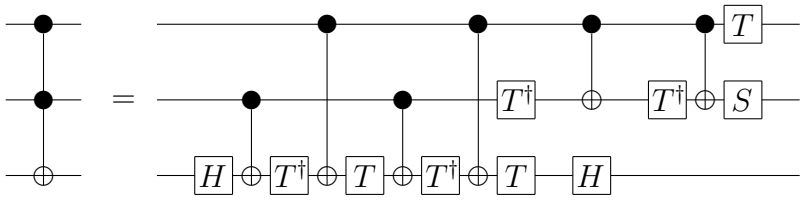

Figura 5.3: Compuerta Toffoli en función de las compuertas H (Hadamard), S (Fase), T ($\pi/8$) que actúan sobre un qubit y compuertas controladas CNOT.

donde X es la compuerta NOT. Esta equivalencia nos ayudara a encontrar la descomposición de la compuerta Toffoli.

Primero encontramos la descomposición de la compuerta Toffoli como el producto de compuertas con un solo qubit de control. Dada la forma en que actúa el operador U_{CCN} en la ecuación (5.8), necesitamos de un operador V_X tal que ${V_X}^2 = X$. Este operador tiene la forma matricial

$$V_X = \frac{1-\imath}{2}\begin{pmatrix} 1 & \imath \\ \imath & 1 \end{pmatrix}, \tag{5.9}$$

Con este operador, según la ecuación (5.6), obtenemos la representación

$$U_{CCN}|c_1\rangle|c_2\rangle|t\rangle = {V_X}^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}{V_X}^{\dagger(c_2,t)}{U_{CN}}^{(c_1,c_2)}{V_X}^{(c_2,t)}|c_1\rangle|c_2\rangle|t\rangle. \tag{5.10}$$

Las compuertas controladas V_X pueden representarse en función de compuertas que actúan sobre un solo qubit y compuertas CNOT. Remplazando esta descomposición y tras manipulación algebraica [2, pag. 182] llegamos a la expresión

$$\begin{aligned} U_{CCN}|c_1\rangle|c_2\rangle|t\rangle =& T^{(c_1)}S^{(c_2)}{U_{CN}}^{(c_1,c_2)}T^{\dagger(c_2)}{U_{CN}}^{(c_1,c_2)}T^{\dagger(c_2)}T^{(t)}{U_{CN}}^{(c_1,t)}\otimes \\ & T^{\dagger(t)}{U_{CN}}^{(c_2,t)}T^{(t)}{U_{CN}}^{(c_1,t)}T^{\dagger(t)}{U_{CN}}^{(c_2,t)}H^{(t)}|c_1\rangle|c_2\rangle|t\rangle, \end{aligned} \tag{5.11}$$

donde T es la compuerta $\pi/8$, S es la compuerta Fase, H es la compuerta Hadamard (ver la tabla 3.1) y U_{CN} es la compuerta CNOT. El diagrama de esta descomposición se muestra en la figura 5.3.

Nos interesa extender el análisis hecho para la compuerta Toffoli a compuertas que estan controladas por un número arbitrario de qubits, siempre con la meta de encontrar su descomposición en compuertas fundamentales y por tanto su circuito cuántico.

5.3 Compuertas controladas para múltiples qubits

Estudiaremos ahora las compuertas controladas por un número arbitrario de qubits, teniendo siempre como meta el econtrar una representación en compuertas elementales.

Para una operación controlada $U(n)$ que actua en n qubits y que realiza una transformación U sobre k qubits objetivos dados l qubits de control (con $k + l = n$), definimos la ecuación

$$U(n)|c_1c_2...c_l\rangle|t_1t_2...t_k\rangle = |c_1c_2...c_l\rangle U^{c_1 \cdot c_2 \cdot ... \cdot c_l}|t_1t_2...t_k\rangle, \tag{5.12}$$

donde el exponente $c_1 \cdot c_2 \cdot ... \cdot c_l$ del operador U significa el producto de valor númerico de c_1, c_2, ..., c_l y donde $U^0 = \mathbb{I}$ es el operador identidad. Esta expresión indica que la compuerta actúe diferente de la identidad sí y solo sí el estado de todos los qubits de control es $|1\rangle$.

Nos interesa encontrar la descomposición de $U(n)$ en función de compuertas cada vez más simples hasta obtener su descomposicion en compuertas fundamentales. Para esto, analizaremos primero el caso de una compuerta con un solo qubit objetivo que requiere que todos los qubits de control estén en el estado $|1\rangle$ para actuár no trivialmente.

5.3.1 Compuertas con palabra de control arbitraria

A la secuencia de estados $|0\rangle$ y $|1\rangle$ de los qubits de control requerida para que la compuerta actúe diferente de la identidad se llama *palabra de control*. Tomemos por ejemplo una compuerta controlada $U_{|11...1\rangle}$ que actúa sobre n qubits con l qubits de control y un solo qubit objetivo. Esta compuerta requiere que todos los qubits de control estén en el estado $|1\rangle$ para actuar diferente de la identidad,

entonces su palabra de control seria $|11...1\rangle$. La compuerta $U_{|11...1\rangle}$ actuará como

$$U_{|11...1\rangle}|c_1c_2...c_l\rangle|t_1\rangle = |c_1c_2...c_l\rangle U^{c_1\cdot c_2\cdot ....\cdot c_l}|t\rangle. \tag{5.13}$$

donde el exponente $c_1 \cdot c_2 \cdot ... \cdot c_l$ indica el producto del valor númerico de c_1, c_2, c_3, etc.

La ecuación (3.11) nos dice que podemos expresar una compuerta que actúa sobre un solo qubit como el producto de compuertas cuyo producto es la identidad y compuertas CNOT tal que al hacer la substitución en la ecuación anterior obtenemos

$$\begin{aligned} U^{c_1\cdot c_2\cdot ....\cdot c_l} &= (e^{\imath\alpha}AXBXC)^{c_1\cdot c_2\cdot ....\cdot c_l} \\ &= e^{\imath\alpha(c_1\cdot c_2\cdot ....\cdot c_l)}A^{c_1\cdot c_2\cdot ....\cdot c_l}X^{c_1\cdot c_2\cdot ....\cdot c_l}B^{c_1\cdot c_2\cdot ....\cdot c_l}X^{c_1\cdot c_2\cdot ....\cdot c_l}C^{c_1\cdot c_2\cdot ....\cdot c_l}. \end{aligned} \tag{5.14}$$

Expandemos el término exponencial

$$e^{\imath\alpha(c_1\cdot c_2\cdot ....\cdot c_l)} = e^{\imath\alpha c_1}e^{\imath\alpha c_2}...e^{\imath\alpha c_l}. \tag{5.15}$$

Los exponentes $e^{\imath\alpha c_i}$ son equivalentes al operador ${R_\alpha}^{(c_i)}$ que actúa sobre el qubit $|c_i\rangle$, como lo indica la ecuación (3.30). Bajo los mismos argumento utilizados en la subsección 3.3.1 remplazamos los términos $A^{c_1\cdot c_2\cdot ....\cdot c_l}$, $B^{c_1\cdot c_2\cdot ....\cdot c_l}$ y $C^{c_1\cdot c_2\cdot ....\cdot c_l}$ por los operadores $A^{(t)}$, $B^{(t)}$ y $C^{(t)}$, respectivamente, que actúan solo sobre el qubit objetivo, con lo que llegamos a la identidad

$$U_{|11...1\rangle}|c_1c_2...c_l\rangle|t\rangle = |c_1c_2...c_l\rangle {R_\alpha}^{(c_1)}{R_\alpha}^{(c_2)}...{R_\alpha}^{(c_l)}A^{(t)}X^{c_1\cdot c_2\cdot ....\cdot c_l}B^{(t)}X^{c_1\cdot c_2\cdot ....\cdot c_l}C^{(t)}|t\rangle, \tag{5.16}$$

donde el superíndice (c_i) indica que el operador actúa en el espacio del qubit $|c_i\rangle$ y donde X es la compuerta NOT. La ecuación (5.16) indica la descomposición de una compuerta con palabra de control $|11...1\rangle$ como el producto de compuertas que actúan solo un qubit y compuertas NOT controladas por múltiples qubits.

Es posible representar una compuerta con una palabra de control arbitraria como una compuerta con palabra de control $|11...1\rangle$ si invertimos el estado de los qubits que se requiere que esten en el estado $|0\rangle$ antes y después de la compuerta.

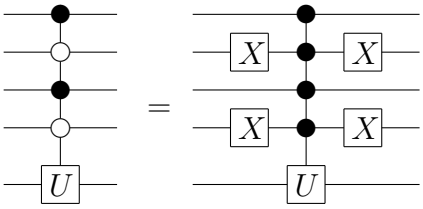

Figura 5.4: La compuerta U con palabra de control $|1010\rangle$ es equivalente a una compuerta U con palabra de control $|1111\rangle$ y compuertas NOT.

Para ejemplificar esto, supongamos ahora una compuerta $U_{|1010\rangle}$ que tiene como palabra de control el estado $|1010\rangle$. Esta compuerta será equivalente a una compuerta con palabra de control $|1111\rangle$ si invertimos el estado del segundo y cuarto qubit antes y después de aplicar el operador, similar a la ecuacion (3.22),

$$U_{|1010\rangle}|c_1c_2c_3c_4\rangle|t\rangle = X^{(c_2)}X^{(c_4)}U_{|1111\rangle}X^{(c_2)}X^{(c_4)}|c_1c_2c_3c_4\rangle|t\rangle, \tag{5.17}$$

donde $U_{|1111\rangle}$ es una compuerta con palabra de control $|1111\rangle$ y $X^{(c_i)}$ es la compuerta NOT que actúa sobre el qubit $|c_i\rangle$. Esta equivalencia se ilustra en la figura 5.4.

Con esta consideración y la ecuación (5.16) concluimos que un operador con un solo qubit objetivo puede representarse como el producto de operadores que actuan sobre en el espacio de un qubit y operadores de la forma $X^{c_1\cdot c_2\cdot \ldots \cdot c_n}$. Procederemos a simplificar aun más esta representación.

5.3.2 Circuito de una compuerta con palabra de control $|111...11\rangle$

Demostraremos a continuación que un compuerta con un solo qubit objetivo y una palabra de control $|111...11\rangle$ se puede descomponer como el producto de compuertas fundamentales.

Existe al menos un algoritmo que permite representar una compuerta controlada por un número arbitrario de qubits como el producto de compuertas Toffoli y una compuerta controlada por un solo qubit. Para una compuerta $U_{|111...11\rangle}$ con

$|c_1c_2...c_l\rangle$ qubits de control y un qubit objetivo $|t\rangle$ utilizaremos $(l-1)$ *qubits de trabajo*, todos ellos en un estado inicial $|w_i\rangle = |0\rangle$. El estado del sistema total $|\phi\rangle$ estara dado por

$$|\phi\rangle = |c_1c_2...c_l\rangle|w_1 = 0\rangle|w_2 = 0\rangle...|w_{l-1} = 0\rangle|t_1t_2...t_k\rangle \equiv |c_1c_2...c_l\rangle|00...0\rangle|t\rangle. \tag{5.18}$$

La compuerta $U_{|111...11\rangle}$ esta controlada solo por los qubits $|c_i\rangle$ y tiene como objetivo solo el qubit $|t\rangle$,por lo que la inclusión de los qubits de trabajo no afectara la forma en que actúa,

$$U^{(c_1c_2...c_l,t)}|c_1c_2...c_l\rangle|00...0\rangle|t\rangle = |c_1c_2...c_l\rangle|00...0\rangle U^{c_1\cdot c_2\cdot ...\cdot c_l}|t\rangle. \tag{5.19}$$

La idea general del algoritmo consiste en utilizar compuertas Toffoli para transformar el estado del primer qubit de trabajo al estado $|c_1 \cdot c_2\rangle$, el del segundo qubit de trabajo al estado $|c_1 \cdot c_2 \cdot c_3\rangle$ y asi sucesivamente hasta que el último qubit de trabajo sea transformado al estado $|c_1 \cdot c_2 \cdot ... \cdot c_l\rangle$. El estado del último de trabajo contendrá la información del estado de todos los qubits de control, resultando $|w_{l-1}\rangle = |1\rangle$ solo sí todos los qubits de control estan en el estado en el estado $|1\rangle$, o resultará $|w_{l-1}\rangle = |0\rangle$ en cualquier otro caso. Por lo tanto, la compuerta controlada $U_{|111...11\rangle}$ que requiere que todos los qubits de control esten en el estado $|1\rangle$ será equivalente a la compuerta controlada U que requiere que el último qubit de trabajo esté en el estado $|w_{l-1} = 1\rangle$.

La forma en que procede el algoritmo es la siguiente: Primero aplicamos una compuerta Toffoli con $|c_1\rangle$ y $|c_2\rangle$ como qubits de control y el primer qubit de trabajo como el objetivo. Con esto se cambiará el estado del qubit de trabajo al

estado $|c_1 \cdot c_2\rangle$, refiriendose $c_1 \cdot c_2$ al producto del valor númerico de c_1 y c_2,

$$\begin{aligned} {U_{CCN}}^{(c_1c_2,w_1)}|c_1c_2...c_l\rangle|00...0\rangle|t\rangle &= |c_1c_2...c_l\rangle(X^{(w_1)})^{c_1\cdot c_2}|00...0\rangle|t\rangle \\ &= |c_1c_2...c_l\rangle|w_1 = c_1 \cdot c_2\rangle|0\rangle|0\rangle...|w_{l-1} = 0\rangle|t\rangle \\ &\equiv |c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle|00...0\rangle|t\rangle. \end{aligned} \tag{5.20}$$

donde el superíndice (c_1c_2, w_1) indica que la compuerta Toffoli tiene como control los qubits $|c_1\rangle$ y $|c_2\rangle$ y como objetivo el qubit $|w_1\rangle$. El siguiente paso consiste en aplicar otra compuerta Toffoli, esta vez utilizando el qubit $|c_3\rangle$ y el primer qubit de trabajo en el estado $|w_1 = c_1 \cdot c_2\rangle$ como qubits de control y el segundo qubit de trabajo como qubit objetivo. Despues de aplicar la compuerta Toffoli, el estado del segundo qubit de trabajo resultará en $|w_2\rangle = |c_1 \cdot c_2 \cdot c_3\rangle$,

$$\begin{aligned} {U_{CCN}}^{(c_3w_1,w_2)}|c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle|00...0\rangle|t\rangle &= |c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle(X^{(w_2)})^{c_1\cdot c_2\cdot c_3}|00...0\rangle|t\rangle \\ &= |c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle|c_1 \cdot c_2 \cdot c_3\rangle|0...0\rangle|t\rangle. \end{aligned} \tag{5.21}$$

Repetimos este procedimiento para todos los qubits de control hasta obtener que el último qubit de trabajo tendrá el estado $|c_1 \cdot c_2 \cdot ... \cdot c_l\rangle$.

$$\begin{aligned} {U_{CCN}}^{(w_1w_2...w_{l-2}c_l,w_{l-1})}{U_{CCN}}^{(w_1w_2..w_{l-3}c_{l-1},w_{l-2})}...{U_{CCN}}^{(c_1c_2,w_1)}|c_1c_2...c_l\rangle|00...0\rangle|t\rangle \\ = |c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle|c_1 \cdot c_2 \cdot c_3\rangle...|c_1 \cdot c_2 \cdot ... \cdot c_l\rangle|t\rangle. \end{aligned} \tag{5.22}$$

Ahora aplicamos la compuerta controlada U que tiene como control el último qubit de control $|w_{l-1} = c_1 \cdot c_2 \cdot ... \cdot c_n\rangle$ y como objetivo el qubit objetivo original de la compuerta $U_{|111...11\rangle}$,

$$\begin{aligned} &U^{(w_{l-1},t)}|c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle|c_1 \cdot c_2 \cdot c_3\rangle...|c_1 \cdot c_2 \cdot ... \cdot c_l\rangle|t\rangle \\ &= |c_1c_2...c_l\rangle|c_1 \cdot c_2\rangle|c_1 \cdot c_2 \cdot c_3\rangle...|c_1 \cdot c_2 \cdot ... \cdot c_l\rangle U^{c_1\cdot c_2\cdot ...\cdot c_l}|t\rangle. \end{aligned} \tag{5.23}$$

Comparando esta ecuación con la ecuación (5.19) podemos observar que la compuerta $U^{(w_{l-1},t)}$ actua igual que la compuerta $U_{|111...11\rangle}$, que es la compuerta que se desea expresar en términos de compuertas fundamentales.

Por último regresamos los qubits de trabajo a su estado original utilizando las mismas compuertas Toffoli en orden inverso.

$$\begin{aligned} &{U_{CCN}}^{(c_1c_2,w_1)}...{U_{CCN}}^{(w_1w_2..w_{l-3}c_{l-1},w_{l-2})}{U_{CCN}}^{(w_1w_2...w_{l-2}c_l,w_{l-1})}\otimes \\ &|c_1c_2...c_l\rangle|c_1\cdot c_2\rangle|c_1\cdot c_2\cdot c_3\rangle...|c_1\cdot c_2\cdot ...\cdot c_l\rangle U^{c_1\cdot c_2\cdot ....\cdot c_l}|t\rangle \\ &=|c_1c_2...c_l\rangle|00...0\rangle U^{c_1\cdot c_2\cdot ....\cdot c_l}|t\rangle. \end{aligned} \tag{5.24}$$

El estado al final de la ecuación es el mismo que aquel en la identidad (5.19), por lo que podemos afirmar que una compuerta con palabra de control $|111...11\rangle$, con l qubits de trabajo y con un solo qubit objetivo se puede representar como

$$\begin{aligned} &U^{(c_1c_2...c_l,t)}|c_1c_2...c_l\rangle|00...0\rangle|t\rangle = \\ &{U_{CCN}}^{(c_1c_2,w_1)}...{U_{CCN}}^{(w_1w_2..w_{l-3}c_{l-1},w_{l-2})}{U_{CCN}}^{(w_1w_2...w_{l-2}c_l,w_{l-1})}U^{(w_{l-1},t)}\otimes \\ &{U_{CCN}}^{(w_1w_2...w_{l-2}c_l,w_{l-1})}{U_{CCN}}^{(w_1w_2..w_{l-3}c_{l-1},w_{l-2})}...{U_{CCN}}^{(c_1c_2,w_1)}|c_1c_2...c_l\rangle|00...0\rangle|t\rangle \end{aligned} \tag{5.25}$$

La figura 5.5 muestra el diagrama del algoritmo propuesto, para el caso de una compuerta con 5 qubits de control; el circuito es facíl de interpretar y de extender para un número arbitrario de qubits.

La compuerta Toffoli puede descomponerse a su vez como compuertas que actúan sobre un solo qubit y compuertas CNOT (ver ecuación (5.11)).

Resumiendo lo visto en el capítulo, podemos encontrar la descomposición de una compuerta cuántica arbitraria con un solo qubit objetivo como el producto de compuertas fundamentales: Primero cambiamos su representación al de una compuerta con palabra de control $|111...11\rangle$, luego aplicamos el algoritmo para la compuerta con palabra de control $|111...11\rangle$ en función de compuertas Toffoli y por último representamos las compuertas Toffoli y la compuerta con un solo qubit de control como el producto de compuertas que actúan sobre un qubit y compuertas CNOT. En algunos casos se puede implementar la compuerta Toffoli

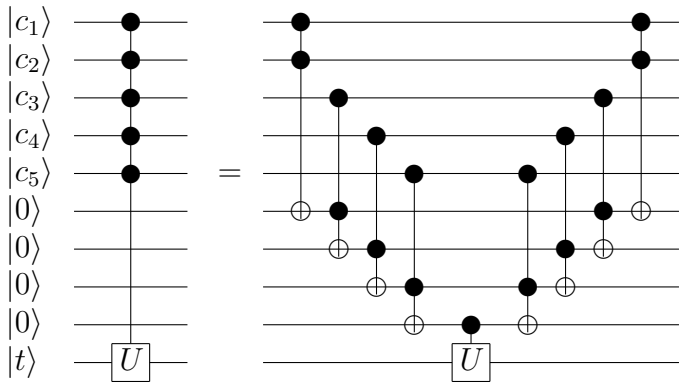

Figura 5.5: Representación de una compuerta con $n = 5$ qubits de control utilizando compuertas Toffoli y una compuerta con un solo qubit objetivo. Se utilizan $(n-1)$ qubits de trabajo en el estado $|0\rangle$.

directamente [23; 24; 25], por lo que no será necesario realizar la descomposición en compuertas fundamentales de las compuertas Toffoli para la implementación física del circuito.

Se desea extender el análisis a compuertas que tiene como control y objetivo un número arbitrario de qubits. Con el estudio hecho hasta el momento, se puede observar que la descomposición de los operadores en compuertas elementales escala en complejidad rápidamente conforme se aumenta el número de qubits sobre los que actúa el operador. Para compuertas con más de dos qubits objetivo necesitamos desarrollar un algoritmo que permita encontrar la descomposición del operador.

Capítulo 6

Algoritmo para la síntesis de circuitos cuánticos

El objetivo de este trabajo es encontrar un algoritmo que permita encontrar la representación en compuertas elementales de un operador arbitrario. Para esto, representaremos los operadores como una serie de operaciones que intercambian el vector en diferentes espacios hasta llevarlo al estado final.

6.1 Intercambio de vectores

Utilizaremos una suceción de intercambios de vectores para llevar el sistema de un estado inicial al estado final, reproduciendo la acción de la transformación original. El intercambio de vectores será realizado utilizando los operadores conocidos como *reflexiones de Householder*, los cuales introduciremos a continuación.

6.1.1 Reflexiones de Householder

Definimos un operador $[\vec{x}]$ que actúa sobre un vector $\vec{x}$ de la forma

$$[\vec{x}]\vec{x} = -\vec{x}. \tag{6.1}$$

Sí aplicamos el operador $[\vec{x}]$ a un vector $\vec{x}^{\perp}$, ortogonal al vector $\vec{x}$, este actuará

como la identidad,

$$[\vec{x}]\vec{x}^{\perp} = \vec{x}^{\perp}. \tag{6.2}$$

El operador $[\vec{x}]$ es un "operador de reflexión", también llamado reflexión de Householder. Las reflexiones de Householder son hermitianas ($[\vec{x}] = [\vec{x}]^{\dagger}$) y unitarias ($[\vec{x}]^{\dagger}[\vec{x}] = [\vec{x}][\vec{x}]^{\dagger} = [\vec{x}]^2 = \mathbb{I}$) [26].

Cada reflexión puede ser escrita como

$$[\vec{x}] = \mathbb{I} - 2\frac{\vec{x}\vec{x}^*}{\|\vec{x}\|^2}, \tag{6.3}$$

donde $\mathbb{I}$ es el operador identidad, $\vec{x}^*$ es el conjugado de $\vec{x}$ y $\|\vec{x}\| = \sqrt{(\vec{x}^*\vec{x})}$ es la norma de $\vec{x}$. En el caso especial de que $\vec{x}$ sea el vector nulo tomamos la reflexión como la identidad ($[\vec{x} = 0] = \mathbb{I}$).

A continuación mostraremos como serán utilizados estas reflexiones para realizar el intercambio entre vectores.

6.1.2 Intercambio de dos vectores por reflexión

Tomaremos como lema que existe una y solo una reflexión $[\vec{r}]$ que permite la transformación de un vector $\vec{x}$ a otro vector $\vec{y}$ tal que

$$[\vec{r}]\vec{x} = z^*\frac{\|\vec{x}\|}{\|\vec{y}\|}\vec{y}, \tag{6.4}$$

donde z es un numero complejo y el vector $\vec{r} = z\|\vec{y}\|\vec{x} - \|\vec{x}\|\vec{y}$ es el vector perpendicular al vector sobre el cual se realiza la reflexión. Este intercambio de vectores se ilustra en la figura 6.1.

Nuestro interés reside en aplicar este lema a la factorización de operadores unitarios. El operador de reflexión $[\vec{r}]$ se tomará como una transformación unitaria que al aplicarse dos veces en sucesión nos da el vector original ($[\vec{r}][\vec{r}] = \mathbb{I}$).

Dada la representación (6.3), el operador $[\vec{r}]$ ser escrito como

$$[\vec{r}] = \mathbb{I} - 2\frac{\vec{r}\vec{r}^*}{\|\vec{r}\|^2}. \tag{6.5}$$

Para encontrar el valor de z dados dos vectores $\vec{x}$ y $\vec{y}$, sustituimos el valor de

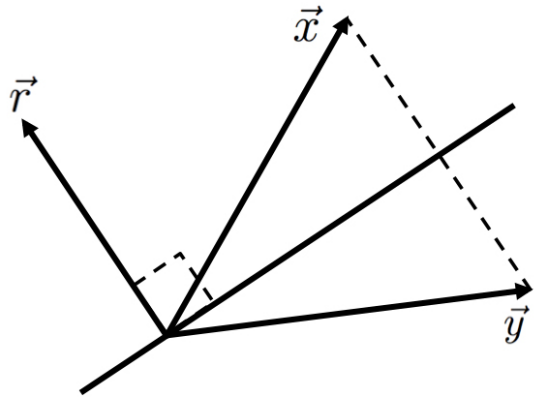

Figura 6.1: Intercambio o "reflexión" de dos vectores $\vec{x}$ y $\vec{y}$ a través del operador de reflexión $[\vec{r}]$.

$\vec{r}$ en la definición (6.5) de $[\vec{r}]$ con lo que obtenemos

$$\begin{aligned}[\vec{r}] &= \mathbb{I} - 2\frac{\vec{r}\vec{r}^*}{\|\vec{r}\|^2} = \mathbb{I} - 2\frac{(z\|\vec{y}\|\vec{x} - \|\vec{x}\|\vec{y})(z\|\vec{y}\|\vec{x} - \|\vec{x}\|\vec{y})^*}{(z\|\vec{y}\|\vec{x} - \|\vec{x}\|\vec{y})^*(z\|\vec{y}\|\vec{x} - \|\vec{x}\|\vec{y})} \\ &= \mathbb{I} - 2\frac{|z|^2\|\vec{y}\|^2\vec{x}\vec{x}^* - z\|\vec{x}\|\|\vec{y}\|\vec{x}\vec{y}^* - z^*\|\vec{x}\|\|\vec{y}\|\vec{y}\vec{x}^* + \|\vec{x}\|^2\vec{y}\vec{y}^*}{|z|^2\|\vec{x}\|^2\|\vec{y}\|^2 - z^*\|\vec{x}\|\|\vec{y}\|(\vec{x}^*\vec{y}) - z\|\vec{x}\|\|\vec{y}\|(\vec{y}^*\vec{x}) + \|\vec{x}\|^2\|\vec{y}\|^2},\end{aligned} \tag{6.6}$$

recordando que $(\vec{\imath}^*\vec{\jmath})$ denota el producto interno entre los vectores $\vec{\imath}$ y $\vec{\jmath}$. Aplicamos ahora el operador de reflexión al vector $\vec{x}$, lo que nos da

$$\begin{aligned}[\vec{r}]\vec{x} &= \vec{x} - 2\frac{|z|^2\|\vec{y}\|^2\vec{x}(\vec{x}^*\vec{x}) - z\|\vec{x}\|\|\vec{y}\|\vec{x}(\vec{y}^*\vec{x}) - z^*\|\vec{x}\|\|\vec{y}\|\vec{y}(\vec{x}^*\vec{x}) + \|\vec{x}\|^2\vec{y}(\vec{y}^*\vec{x})}{|z|^2\|\vec{x}\|^2\|\vec{y}\|^2 - z^*\|\vec{x}\|\|\vec{y}\|(\vec{x}^*\vec{y}) - z\|\vec{x}\|\|\vec{y}\|(\vec{y}^*\vec{x}) + \|\vec{x}\|^2\|\vec{y}\|^2} \\ &= \vec{x} - 2\frac{|z|^2\|\vec{x}\|^2\|\vec{y}\|^2\vec{x} - z\|\vec{x}\|\|\vec{y}\|(\vec{y}^*\vec{x})\vec{x} - z^*\|\vec{x}\|^3\|\vec{y}\|\vec{y} + \|\vec{x}\|^2(\vec{y}^*\vec{x})\vec{y}}{|z|^2\|\vec{x}\|^2\|\vec{y}\|^2 - z^*\|\vec{x}\|\|\vec{y}\|(\vec{x}^*\vec{y}) - z\|\vec{x}\|\|\vec{y}\|(\vec{y}^*\vec{x}) + \|\vec{x}\|^2\|\vec{y}\|^2}\end{aligned} \tag{6.7}$$

Igualamos esta ecuación con la ecuación (6.4) y comparamos los términos dependientes de $\vec{x}$ y de $\vec{y}$ en ambos lados de la ecuación. Con los términos dependientes de $\vec{x}$ obtenemos las ecuaciones

$$1 - 2\frac{|z|^2\|\vec{x}\|^2\|\vec{y}\|^2 - z\|\vec{x}\|\|\vec{y}\|(\vec{y}^*\vec{x})}{|z|^2\|\vec{x}\|^2\|\vec{y}\|^2 - z^*\|\vec{x}\|\|\vec{y}\|(\vec{x}^*\vec{y}) - z\|\vec{x}\|\|\vec{y}\|(\vec{y}^*\vec{x}) + \|\vec{x}\|^2\|\vec{y}\|^2} = 0, \tag{6.8}$$

$$|z|^2\|\vec{x}\|\|\vec{y}\| - z^*(\vec{x}^*\vec{y}) + z(\vec{y}^*\vec{x}) - \|\vec{x}\|^2\|\vec{y}\|^2 = 0. \tag{6.9}$$

La solución a esta última ecuación nos da el valor

$$z = \frac{(\vec{x}^*\vec{y})^{1/2}}{(\vec{y}^*\vec{x})^{1/2}}, \tag{6.10}$$

el cual reescribiremos para obtener finalmente que

$$z = \frac{(\vec{x}^*\vec{y})}{|\vec{y}^*\vec{x}|} \ , \ z^* = \frac{(\vec{y}^*\vec{x})}{|\vec{y}^*\vec{x}|}. \tag{6.11}$$

Sustituimos estos valores de z y z^* en nuestras ecuaciones originales con lo que obtenemos que, dados los vectores $\vec{x}$ y $\vec{y}$, la reflexión $[\vec{r}]$ que produce el intercambio entre estos vectores será

$$[\vec{r}]\vec{x} = \frac{(\vec{y}^*\vec{x})}{|\vec{x}^*\vec{y}|}\frac{\|\vec{x}\|}{\|\vec{y}\|}\vec{y}, \tag{6.12}$$

donde el operador $[\vec{r}]$ en función de los vectores $\vec{x}$ y $\vec{y}$ es

$$[\vec{r}] = \mathbb{I} - \frac{\vec{x}\vec{x}^* - \frac{(\vec{x}^*\vec{y})}{|\vec{x}^*\vec{y}|}\frac{\|\vec{x}\|}{\|\vec{y}\|}\vec{x}\vec{y}^* - \frac{(\vec{y}^*\vec{x})}{|\vec{y}^*\vec{x}|}\frac{\|\vec{x}\|}{\|\vec{y}\|}\vec{y}\vec{x}^* + \frac{\|\vec{x}\|^2}{\|\vec{y}\|^2}\vec{y}\vec{y}^*}{\|\vec{x}\|^2 - \frac{\|\vec{x}\|}{\|\vec{y}\|}|\vec{y}^*\vec{x}|}. \tag{6.13}$$

El operador $[\vec{r}]$ es la reflexión del vector $\vec{r}$ que, en función de los vectores $\vec{x}$ y $\vec{y}$, es

$$\vec{r} = \frac{(\vec{x}^*\vec{y})}{|\vec{y}^*\vec{x}|}\|\vec{y}\|\vec{x} - \|\vec{x}\|\vec{y}. \tag{6.14}$$

Una vez comprendido el intercambio de vectores a través de las reflexiones de Householder, aplicaremos las reflexiones a estados de sistemas cuánticos.

6.1.3 Intercambio de estados cuánticos

Utilizaremos los conceptos de reflexión e intercambio de vectores aplicados a estados cuánticos para luego enfocarnos en sistemas de qubits.

Dado el estado inicial $|x\rangle$ y el estado final $|y\rangle$, con $|x\rangle \neq |y\rangle$, el operador de

reflexión $[r]$ que produce el intercambio de estos dos estados,

$$[r]|x\rangle = \frac{\langle y|x\rangle}{|\langle x|y\rangle|}\frac{\langle x|x\rangle^{1/2}}{\langle y|y\rangle^{1/2}}|y\rangle, \tag{6.15}$$

estará dado, en analogía con la ecuación (6.13), por

$$[r] = \mathbb{I} - \frac{|x\rangle\langle x| - \frac{\langle x|y\rangle}{|\langle x|y\rangle|}\frac{\langle x|x\rangle^{1/2}}{\langle y|y\rangle^{1/2}}|x\rangle\langle y| - \frac{\langle y|x\rangle}{|\langle x|y\rangle|}\frac{\langle x|x\rangle^{1/2}}{\langle y|y\rangle^{1/2}}|y\rangle\langle x| + \frac{\langle x|x\rangle}{\langle y|y\rangle}|y\rangle\langle y|}{\langle x|x\rangle - \frac{\langle x|x\rangle^{1/2}}{\langle y|y\rangle^{1/2}}|\langle x|y\rangle|}. \tag{6.16}$$

El vector $|r\rangle$ que es reflejado por el operador $[r]$,

$$[r]|r\rangle = -|r\rangle, \tag{6.17}$$

quedará en función de los vectores $|x\rangle$ y $|y\rangle$ como

$$|r\rangle = \frac{\langle x|y\rangle}{|\langle x|y\rangle|}\langle y|y\rangle^{1/2}|x\rangle - \langle x|x\rangle^{1/2}|y\rangle. \tag{6.18}$$

Se puede verificar esta identidad aplicando el operador $[r]$ dado en (6.16) sobre la ecuación (6.18), con lo que se reproduce la ecuación (6.17). También se puede verificar aplicando el operador $[r]$ a un vector $|r^{\perp}\rangle$ perpendicular al vector $|r\rangle$ ($\langle r|r^{\perp}\rangle = 0$) observando que se respeta la definición de reflexión, según lo visto en la sección 6.1.1,

$$[r]|r^{\perp}\rangle = |r\rangle. \tag{6.19}$$

Para el caso en que el vector $|y\rangle$ sea paralelo al vector $|x\rangle$ ($|y\rangle = \alpha|x\rangle$), el operador $[r]$ será el operador identidad $\mathbb{I}$.

Si los vectores $|x\rangle$ y $|y\rangle$ fueran perpendiculares, el término del producto interno de estos vectores sobre el valor absoluto del producto interno resultará

$$\frac{\langle x|y\rangle}{|\langle x|y\rangle|} = \frac{\langle y|x\rangle}{|\langle x|y\rangle|} = 1 \;\forall\; |x\rangle \perp |y\rangle. \tag{6.20}$$

La fórmula (6.16) nos permite encontrar el operador de reflexión $[r]$ dados los dos vectores de estado $|x\rangle$ y $|y\rangle$, que se desean intercambiar. Este es el principal

componente del algoritmo que nos permitirá encontrar la descomposición de los operadores en función de reflexiones de Householder.

6.2 Algoritmo principal de factorización

Utilizaremos las identidades vistas en la sección anterior para encontrar la descomposición de un operador arbitrario como el producto de operadores de reflexión. Esta representacioń no será única, por lo que será necesario establecer un criterio de cual representación es la más eficiente.

Para un sistema de n qubits con vectores de base $\{|0\rangle, |1\rangle, |2\rangle, ..., |2^n - 1\rangle\}$ tenemos que un operador U actuará sobre los vectores de base como

$$U|0\rangle = |U_0\rangle \ , \ U|1\rangle = |U_1\rangle \ , \ U|2\rangle = |U_2\rangle \ , \ ... \ , \ U|2^n - 1\rangle = |U_{2^n-1}\rangle. \tag{6.21}$$

Nos concentraremos primero en uno solo de los vectores de estados, el vector $|U_0\rangle$. Utilizaremos el operador de reflexión $[r_1^{(0)}]$ para intercambiar el estado $|j_1\rangle$ por el vector $|\mathbb{I}_{j1,k1}\rangle$, que es la proyección del vector $|U_0\rangle$ sobre el plano donde habitan los vectores $|j_1\rangle$ y $|k_1\rangle$. La reflexión, dada por la ecuación (6.15), será tal que

$$[r_1^{(0)}]|\mathbb{I}_{j1,k1}\rangle = \frac{\langle j_1|\mathbb{I}_{j1,k1}\rangle}{|\langle j_1|\mathbb{I}_{j1,k1}\rangle|} \frac{\langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle^{1/2}}{\langle j_1|j_1\rangle^{1/2}}|j_1\rangle, \tag{6.22}$$

con

$$|\mathbb{I}_{j1,k1}\rangle = (|j_1\rangle\langle j_1| + |k_1\rangle\langle k_1|)|U_0\rangle. \tag{6.23}$$

El vector de proyección $|\mathbb{I}_{j1,k1}\rangle$ no está necesariamente normalizado, pero los vectores de base $|j_1\rangle$ si lo están ($\langle j_1|j_1\rangle = 1$), por lo que tendremos

$$[r_1^{(0)}]|\mathbb{I}_{j1,k1}\rangle = \frac{\langle j_1|\mathbb{I}_{j1,k1}\rangle}{|\langle j_1|\mathbb{I}_{j1,k1}\rangle|} \langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle^{1/2}|j_1\rangle, \tag{6.24}$$

El operador que realiza esta reflexión, según la ecuación (6.16) y dada la

normalización de los vectores $|j_1\rangle$, será

$$[r_1^{(0)}] = \mathbb{I} - \frac{\langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle |j_1\rangle\langle j_1| - \frac{\langle j_1|\mathbb{I}_{j1,k1}\rangle}{|\langle j_1|\mathbb{I}_{j1,k1}\rangle|}\langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle^{1/2}|j_1\rangle\langle \mathbb{I}_{j1,k1}|}{\langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle - \langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle^{1/2}|\langle j_1|\mathbb{I}_{j1,k1}\rangle|} + \frac{\frac{\langle \mathbb{I}_{j1,k1}|j_1\rangle}{|\langle \mathbb{I}_{j1,k1}|j_1\rangle|}\langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle^{1/2}|\mathbb{I}_{j1,k1}\rangle\langle j_1| - |\mathbb{I}_{j1,k1}\rangle\langle \mathbb{I}_{j1,k1}|}{\langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle - \langle \mathbb{I}_{j1,k1}|\mathbb{I}_{j1,k1}\rangle^{1/2}|\langle j_1|\mathbb{I}_{j1,k1}\rangle|}. \tag{6.25}$$

Ahora aplicamos el operador de reflexión $[r_2^{(0)}]$ para intercambiar el vector $|j_1\rangle$ por el vector $|\mathbb{I}_{j1,k2}\rangle$, definido como la proyección del vector $[r_1^{(0)}]|U_0\rangle$ sobre el plano donde habitan los vectores $|j_1\rangle$ y $|k_2\rangle$, de forma que

$$[r_2^{(0)}]|\mathbb{I}_{j1,k2}\rangle = \frac{\langle j_1|\mathbb{I}_{j1,k2}\rangle}{|\langle j_1|\mathbb{I}_{j1,k2}\rangle|}\langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle^{1/2}|j_1\rangle, \tag{6.26}$$

con

$$|\mathbb{I}_{j1,k2}\rangle = (|j_1\rangle\langle j_1| + |k_2\rangle\langle k_2|)[r_1^{(0)}]|U_0\rangle. \tag{6.27}$$

El operador que realizá la reflexión será

$$[r_2^{(0)}] = \mathbb{I} - \frac{\langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle |j_1\rangle\langle j_1| - \frac{\langle j_1|\mathbb{I}_{j1,k2}\rangle}{|\langle j_1|\mathbb{I}_{j1,k2}\rangle|}\langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle^{1/2}|j_1\rangle\langle \mathbb{I}_{j1,k2}|}{\langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle - \langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle^{1/2}|\langle j_1|\mathbb{I}_{j1,k2}\rangle|} + \frac{\frac{\langle \mathbb{I}_{j1,k2}|j_1\rangle}{|\langle \mathbb{I}_{j1,k2}|j_1\rangle|}\langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle^{1/2}|\mathbb{I}_{j1,k2}\rangle\langle j_1| - |\mathbb{I}_{j1,k2}\rangle\langle \mathbb{I}_{j1,k2}|}{\langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle - \langle \mathbb{I}_{j1,k2}|\mathbb{I}_{j1,k2}\rangle^{1/2}|\langle j_1|\mathbb{I}_{j1,k2}\rangle|}. \tag{6.28}$$

Proseguimos aplicando el operador $[r_3^{(0)}]$ para intercambiar el vector $|j_1\rangle$ por el vector $|\mathbb{I}_{j1,k3}\rangle \equiv (|j_1\rangle\langle j_1| + |k_3\rangle\langle k_3|)[r_2^{(0)}][r^{(0)_1}]|U_0\rangle$ y así sucesivamente hasta aplicar el operador de reflexión $[r_{2^n-1}^{(0)}]$ para intercambiar el vector $|j_1\rangle$ por el vector $|\mathbb{I}_{j1,k2^n-1}\rangle \equiv (|j_1\rangle\langle j_1| + |k_{2^n-1}\rangle\langle k_{2^n-1}|)[r_{2^n-2}^{(0)}]...[r_2^{(0)}][r_1^{(0)}]|U_0\rangle$. Utilizaremos el operador $[r^{(0)}]$ para denotar el producto de los operadores de reflexión,

$$[r^{(0)}] = [r_{2^n-1}^{(0)}][r_{2^n-2}^{(0)}]...[r_2^{(0)}][r_1^{(0)}]. \tag{6.29}$$

Repetimos este proceso para el resto de los vectores $|U_{i\neq 1}\rangle$: Aplicamos el

operador de reflexión $[r_1^{(1)}]$ sobre el estado $|j_2\rangle$, tal que

$$[r_1^{(1)}]|\mathbb{I}_{j2,k2}\rangle = \frac{\langle j_2|\mathbb{I}_{j2,k2}\rangle}{|\langle j_2|\mathbb{I}_{j1,k2}\rangle|}\langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle^{1/2}|j_2\rangle, \tag{6.30}$$

con

$$|\mathbb{I}_{j2,k2}\rangle = (|j_2\rangle\langle j_2| + |k_2\rangle\langle k_2|)|U_1\rangle. \tag{6.31}$$

$$\begin{aligned}[r_1^{(1)}] = \mathbb{I} - \frac{\langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle|j_2\rangle\langle j_2| - \frac{\langle j_2|\mathbb{I}_{j2,k2}\rangle}{|\langle j_2|\mathbb{I}_{j2,k2}\rangle|}\langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle^{1/2}|j_2\rangle\langle \mathbb{I}_{j2,k2}|}{\langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle - \langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle^{1/2}|\langle j_2|\mathbb{I}_{j2,k2}\rangle|} \\ + \frac{\frac{\langle \mathbb{I}_{j2,k2}|j_2\rangle}{|\langle \mathbb{I}_{j2,k2}|j_2\rangle|}\langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle^{1/2}|\mathbb{I}_{j2,k2}\rangle\langle j_2| - |\mathbb{I}_{j2,k2}\rangle\langle \mathbb{I}_{j2,k2}|}{\langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle - \langle \mathbb{I}_{j2,k2}|\mathbb{I}_{j2,k2}\rangle^{1/2}|\langle j_2|\mathbb{I}_{j2,k2}\rangle|}.\end{aligned} \tag{6.32}$$

La elección de los vectores $|j_2\rangle$ y $|k_2\rangle$ es arbitraria con la única restricción de que no pueden ser iguales entre ellos o iguales al vector $|j_1\rangle$.

Continuamos aplicando operadores de reflexión, siguiendo el mismo procedimiento que para el caso de $|U_0\rangle$, hasta obtener el operador $[r^{(1)}]$, definido como

$$[r^{(1)}] = [r_{2^n-2}^{(1)}][r_{2^n-3}^{(1)}]...[r_2^{(1)}][r_1^{(1)}], \tag{6.33}$$

Esto se repite para todos los vectores restantes $|U_{i\neq 1,2}\rangle$, obteniendo los operadores $[r^{(3)}]$, $[r^{(4)}]$, ... , $[r^{(2^n-2)}]$. Al aplicar todos los operadores $[r^{(i)}]$ a los vectores transformados recuperamos los estados originales $\{|0\rangle, |1\rangle, |2\rangle, ..., |2^n-1\rangle\}$, hasta un cierto coeficiente de proporcionalidad [26],

$$[r^{(2^n-2)}][r^{(2^n-3)}]...[r^{(1)}][r^{(0)}]|U_k\rangle = d_k|k\rangle. \tag{6.34}$$

$$\begin{aligned}&\frac{1}{d_k}[r^{(2^n-2)}]_1[r^{(2^n-3)}]_2[r^{(2^n-3)}]_1 \ldots [r^{(2)}]_{2^n-3}...[r^{(2)}]_1 \otimes \\ &[r^{(1)}]_{2^n-2}...[r^{(1)}]_2[r^{(1)}]_1[r^{(0)}]_{2^n-1}...[r^{(0)}]_2[r^{(0)}]_1 U|k\rangle = |k\rangle.\end{aligned} \tag{6.35}$$

Las reflexiones de Householder son su propio operador inverso ($[r][r] = \mathbb{I}$), lo que nos permite despejar las reflexiones en la última ecuación obteniendo que un

operador U arbitrario se puede representar como

$$\begin{aligned} U =&[r_1^{(0)}][r_2^{(0)}]...[r_{2^n-1}^{(0)}][r_1^{(1)}][r_2^{(1)}]...[r_{2^n-2}^{(1)}]\otimes \\ &[r_1^{(2)}]...[r_{2^n-3}^{(2)}]\dots[r_1^{(2^n-3)}][r_2^{(2^n-3)}][r_1^{(2^n-2)}]D, \end{aligned} \tag{6.36}$$

donde D es una matriz diagonal ($D_{(i,j)} = 0$ para $i \neq j$) cuyas entradas en la diagonal principal son $D_{(k,k)} = d_k$. La ecuación anterior afirma que toda transformación unitaria puede representares como el producto de reflexiones de Householder y una matriz diagonal, lo cual será nuestro lema principal.

Dentro del algoritmo para encontrar la descomposición de la matriz como reflexiones de Householder, podemos seleccionar cualquiera de los vectores de base como los vectores $|j\rangle$ y $|k\rangle$. Una selección diferente de los vectores de proyección dará como resultado diferentes reflexiones, por lo que existe un gran número de posibles representaciones de un operador como el producto de reflexiones de Householder.

A continuación aplicaremos el algoritmo de factorización a operadores que afectan un solo de qubit. Esto nos servirá para ejemplificar la forma en que se implementa el algoritmo y nos permitirá identificar ciertas compuertas a partir de las reflexiones obtenidas.

6.2.1 Identificación de compuertas que actúan sobre un solo qubit

Sea el operador $U^{(1)}$ un operador que actúa en un sistema de dos qubits modificando el primer qubit y dejando el segundo qubit sin alterar. La forma general de la transformación de este tipo de operadores es

$$U^{(1)}|00\rangle = [u_0|0\rangle + u_1|1\rangle]|0\rangle \equiv |U_0\rangle, \tag{6.37}$$

$$U^{(1)}|01\rangle = [u_0|0\rangle + u_1|1\rangle]|1\rangle \equiv |U_1\rangle, \tag{6.38}$$

$$U^{(1)}|10\rangle = [u_1{}^*|0\rangle - u_0{}^*|1\rangle]|0\rangle \equiv |U_2\rangle, \tag{6.39}$$

$$U^{(1)}|11\rangle = [{u_1}^*|0\rangle - {u_0}^*|1\rangle]|1\rangle \equiv |U_3\rangle. \tag{6.40}$$

Utilizaremos el algoritmo descrito en la sección 6.2 para encontrar la descomosición del operador $U^{(1)}$ como el producto de reflexiones de Householder.

Primero intercambiamos el vector $|00\rangle$ por el vector $|\mathbb{I}_{0,1}\rangle$ a través de la reflexión $[r_1^{(0)}]$ tal que

$$[r_1^{(0)}]|\mathbb{I}_{0,1}\rangle = \frac{\langle 00|\mathbb{I}_{0,1}\rangle}{|\langle 00|\mathbb{I}_{0,1}\rangle|}\langle \mathbb{I}_{0,1}|\mathbb{I}_{0,1}\rangle^{1/2}|00\rangle, \tag{6.41}$$

con

$$\begin{aligned} |\mathbb{I}_{0,1}\rangle &= [|00\rangle\langle 00| + |01\rangle\langle 01|]|U_0\rangle \\ &= [|00\rangle\langle 00| + |01\rangle\langle 01|][u_0|00\rangle + u_1|10\rangle] \\ &= u_0|00\rangle \end{aligned} \tag{6.42}$$

Como los vectores $|00\rangle$ y $|\mathbb{I}_{0,1}\rangle$ son paralelos, el operador $[r_1^{(0)}]$ será simplemente la identidad,

$$[r_1^{(0)}] = \mathbb{I}. \tag{6.43}$$

Ahora intercambiamos los vectores $|00\rangle$ y $|\mathbb{I}_{0,2}\rangle$ con la reflexión $[r_2^{(0)}]$,

$$[r_2^{(0)}]|\mathbb{I}_{0,2}\rangle = \frac{\langle 00|\mathbb{I}_{0,2}\rangle}{|\langle 00|\mathbb{I}_{0,2}\rangle|}\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle^{1/2}|00\rangle, \tag{6.44}$$

donde el vector $|\mathbb{I}_{0,2}\rangle$ es

$$\begin{aligned} |\mathbb{I}_{0,2}\rangle &= [|00\rangle\langle 00| + |10\rangle\langle 10|][r_1^{(0)}]|U_0\rangle \\ &= u_0|00\rangle + u_1|10\rangle. \end{aligned} \tag{6.45}$$

La reflexión $[r_2^{(0)}]$ estará dada entonces como

$$\begin{aligned}[r_2^{(0)}] = \mathbb{I} - \frac{\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle |00\rangle\langle 00| - \frac{\langle 00|\mathbb{I}_{0,2}\rangle}{|\langle 00|\mathbb{I}_{0,2}\rangle|}\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle^{1/2}|00\rangle\langle \mathbb{I}_{0,2}|}{\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle - \langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle^{1/2}|\langle 00|\mathbb{I}_{0,2}\rangle|} \\ + \frac{\frac{\langle \mathbb{I}_{0,2}|00\rangle}{|\langle \mathbb{I}_{0,2}|00\rangle|}\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle^{1/2}|\mathbb{I}_{0,2}\rangle\langle 00| - |\mathbb{I}_{0,2}\rangle\langle \mathbb{I}_{0,2}|}{\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle - \langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle^{1/2}|\langle 00|\mathbb{I}_{0,2}\rangle|},\end{aligned} \tag{6.46}$$

$$[r_2^{(0)}] = \mathbb{I} - (1-|u_0|)|00\rangle\langle 00| + \frac{u_0 {u_1}^*}{|u_0|}|00\rangle\langle 10| + \frac{{u_0}^* u_1}{|u_0|}|10\rangle\langle 00| - (1+|u_0|)|10\rangle\langle 10|. \tag{6.47}$$

Utilizamos la reflexión $[r_3^{(0)}]$ para intercambiar los vectores $|00\rangle$ y $|\mathbb{I}_{0,3}\rangle$,

$$[r_3^{(0)}]|\mathbb{I}_{0,3}\rangle = \frac{\langle 00|\mathbb{I}_{0,3}\rangle}{|\langle 00|\mathbb{I}_{0,3}\rangle|}\langle \mathbb{I}_{0,3}|\mathbb{I}_{0,3}\rangle^{1/2}|00\rangle. \tag{6.48}$$

El vector $|\mathbb{I}_{0,3}\rangle$ está dado por

$$\begin{aligned}|\mathbb{I}_{0,3}\rangle &= [|00\rangle\langle 00| + |11\rangle\langle 11|][r_2^{(0)}][r_1^{(0)}]|U_0\rangle \\ &= [|00\rangle\langle 00| + |11\rangle\langle 11|][u_0|00\rangle] \\ &= u_0|00\rangle.\end{aligned} \tag{6.49}$$

Como los vectores $|00\rangle$ y $|\mathbb{I}_{0,3}\rangle$ son paralelos tenemos que

$$[r_3^{(0)}] = \mathbb{I}. \tag{6.50}$$

Pasamos ahora a intercambiar el vector $|01\rangle$ por el vector $|\mathbb{I}_{1,2}\rangle$ a través de la reflexión $[r_1^{(1)}]$,

$$[r_1^{(1)}]|\mathbb{I}_{1,2}\rangle = \frac{\langle 01|\mathbb{I}_{1,2}\rangle}{|\langle 01|\mathbb{I}_{1,2}\rangle|}\langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle^{1/2}|01\rangle, \tag{6.51}$$

donde el vector $|\mathbb{I}_{1,2}\rangle$

$$\begin{aligned} |\mathbb{I}_{1,2}\rangle &= [|01\rangle\langle 01| + |10\rangle\langle 10|]|U_1\rangle \\ &= [|01\rangle\langle 01| + |10\rangle\langle 10|][u_0|01\rangle + u_1|11\rangle] \\ &= u_0|01\rangle, \end{aligned} \tag{6.52}$$

Nuevamente tenemos que los vectores a intercambiar, $|01\rangle$ y $|\mathbb{I}_{1,2}\rangle$, son paralelos por lo que

$$[r_1^{(1)}] = \mathbb{I}. \tag{6.53}$$

Ahora buscamos la reflexión de los vectores $|01\rangle$ y $|\mathbb{I}_{1,3}\rangle$ tal que

$$[r_2^{(1)}]|\mathbb{I}_{1,3}\rangle = \frac{\langle 01|\mathbb{I}_{1,3}\rangle}{|\langle 01|\mathbb{I}_{1,3}\rangle|}\langle \mathbb{I}_{1,3}|\mathbb{I}_{1,3}\rangle^{1/2}|01\rangle, \tag{6.54}$$

Tendremos que

$$\begin{aligned} |\mathbb{I}_{1,3}\rangle &= [|01\rangle\langle 01| + |11\rangle\langle 11|][r_1^{(1)}]|U_1\rangle \\ &= [|01\rangle\langle 01| + |11\rangle\langle 11|][u_0|01\rangle + u_1|11\rangle] \\ &= u_0|01\rangle + u_1|11\rangle, \end{aligned} \tag{6.55}$$

por lo que la reflexión quedara como

$$\begin{aligned} [r_2^{(1)}] = \mathbb{I} &- \frac{\langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle|01\rangle\langle 01| - \frac{\langle 01|\mathbb{I}_{1,2}\rangle}{|\langle 01|\mathbb{I}_{1,2}\rangle|}\langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle^{1/2}|01\rangle\langle \mathbb{I}_{1,2}|}{\langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle - \langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle^{1/2}|\langle 01|\mathbb{I}_{1,2}\rangle|} \\ &+ \frac{\frac{\langle \mathbb{I}_{1,2}|01\rangle}{|\langle \mathbb{I}_{1,2}|01\rangle|}\langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle^{1/2}|\mathbb{I}_{1,2}\rangle\langle 01| - |\mathbb{I}_{1,2}\rangle\langle \mathbb{I}_{1,2}|}{\langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle - \langle \mathbb{I}_{1,2}|\mathbb{I}_{1,2}\rangle^{1/2}|\langle 01|\mathbb{I}_{1,2}\rangle|}, \end{aligned} \tag{6.56}$$

$$[r_2^{(1)}] = \mathbb{I} - (1 - |u_0|)|01\rangle\langle 01| + \frac{u_0 {u_1}^*}{|u_0|}|01\rangle\langle 11| + \frac{{u_0}^* u_1}{|u_0|}|11\rangle\langle 01| - (1 + |u_0|)|11\rangle\langle 11|. \tag{6.57}$$

Finalmente tenemos el intercambio de los vectores $|10\rangle$ y $|\mathbb{I}_{2,3}\rangle$ a través de la

reflexión $[r^{(2)}]_1$,

$$[r_1^{(2)}]|\mathbb{I}_{2,3}\rangle = \frac{\langle 10|\mathbb{I}_{2,3}\rangle}{|\langle 10|\mathbb{I}_{2,3}\rangle|}\langle \mathbb{I}_{2,3}|\mathbb{I}_{2,3}\rangle^{1/2}|10\rangle. \tag{6.58}$$

con

$$\begin{aligned} |\mathbb{I}_{2,3}\rangle &= [|10\rangle\langle 10| + |11\rangle\langle 11|]|U_2\rangle \\ &= [|10\rangle\langle 10| + |11\rangle\langle 11|][{u_1}^*|00\rangle - {u_0}^*|10\rangle] \\ &= -{u_0}^*|10\rangle, \end{aligned} \tag{6.59}$$

Identificando que los vectores $|11\rangle$ y $|\mathbb{I}_{2,3}\rangle$ son paralelos concluimos que

$$[r_1^{(2)}] = \mathbb{I}. \tag{6.60}$$

Una vez que hemos obtenido todas las reflexiones, solo requerimos encontrar los valores de las entradas de la matriz diagonal D. Al aplicar la matriz D sobre los vectores de base, debido a que es diagonal, obtendremos

$$D|00\rangle = d_0|00\rangle \ , \ D|01\rangle = d_1|01\rangle \ , \ D|10\rangle = d_2|10\rangle \ , \ D|11\rangle = d_3|11\rangle, \tag{6.61}$$

donde los factores d_i corresponden a las entradas de la matriz D. Tendremos entonces que

$$\begin{aligned} U^{(1)}|00\rangle &= [r_2^{(0)}][r_2^{(1)}]D|00\rangle = d_0[r^{(1)}]_2[r^{(0)}]_2|00\rangle \\ &= d_0|u_0||00\rangle + d_0\frac{{u_0}^*u_1}{|u_0|}|10\rangle. \end{aligned} \tag{6.62}$$

Igualando esta ecuación con la transformación establecida en la ecuación (6.37) obtenemos que el factor d_0 es

$$d_0 = \frac{u_0}{|u_0|}. \tag{6.63}$$

Repetimos este procedimiento para el resto de los vectores de base, con lo que

encontramos el valor de todos los factores d_i, obteniendo finalmente que la matriz D es

$$D = \frac{1}{|u_0|}\begin{pmatrix} u_0 & 0 & 0 & 0 \\ 0 & u_0 & 0 & 0 \\ 0 & 0 & {u_0}^* & 0 \\ 0 & 0 & 0 & {u_0}^* \end{pmatrix}, \tag{6.64}$$

la cual podemos reescribir como

$$D = \frac{1}{|u_0|}\begin{pmatrix} u_0 & 0 \\ 0 & {u_0}^* \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{6.65}$$

Tenemos entonces que la matriz D se identifica como la compuerta $D^{(1)}$,

$$D^{(1)} = \frac{1}{|u_0|}\begin{pmatrix} u_0 & 0 \\ 0 & {u_0}^* \end{pmatrix}, \tag{6.66}$$

que actúa sobre el primer qubit.

Las reflexiones $[r_2^{(0)}]$ y $[r_2^{(1)}]$, que son las reflexiones diferentes de la identidad, pueden ser representadas cada una en función de un vector $|r^{(i)}\rangle$, como lo indica la ecuación (6.5). Estos vectores serán

$$|r_2^{(0)}\rangle = (|u_0| - 1)|00\rangle + \frac{{u_0}^* u_1}{|u_0|}|10\rangle = [(|u_0| - 1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|1\rangle]|0\rangle, \tag{6.67}$$

$$|r_2^{(1)}\rangle = (|u_0| - 1)|10\rangle + \frac{{u_0}^* u_1}{|u_0|}|11\rangle = [(|u_0| - 1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|1\rangle]|1\rangle. \tag{6.68}$$

Observamos que los vectores reflejados son factorizables. Es razonable suponer que si los estado después de la transformación son factorizables, debido a que el operador actua solo sobre un qubit, entonces los vectores de reflexión seran también factorizables. Para un sistema de n qubits, tendremos que la descomposición de un operador U que altera un solo qubit estará dada por operadores

de reflexión $[r_j^{(i)}]$, con

$$[r_j^{(i)}] = \mathbb{I} - 2\frac{|r_j^{(i)}\rangle\langle r_j^{(i)}|}{\langle r_j^{(i)}|r_j^{(i)}\rangle}, \tag{6.69}$$

donde el vector $|r_j^{(i)}\rangle$ es el producto tensorial del vector de reflexion de un solo qubit $|r^{(1)}\rangle$ multiplicado por alguna combinación del resto de los estados,

$$|r_j^{(i)}\rangle = |r^{(1)}\rangle|j_1 j_2 j_3 ... j_{n-1}\rangle. \tag{6.70}$$

La demostración de esta identidad se muestra en el Apéndice A.2.

Para poder encontrar la representación en compuertas cuánticas de una reflexión arbitraria es necesario encontrar la forma analítica del algoritmo de factorización.

6.2.2 Forma analítica del algoritmo de factorización

Para un sistema de n qubits tenemos 2^n vectores de base, dados por todas las combinaciones posibles de los estados de los qubits individuales. Para simplificar las ecuaciones utilizaremos la notación

$$|0\rangle \equiv |000...00\rangle \ , \ |1\rangle \equiv |000...01\rangle \ , \ |2\rangle \equiv |000...10\rangle \ , \ ... \ , \ |2^n - 1\rangle \equiv |111...11\rangle. \tag{6.71}$$

Un operador U arbitrario actuaŕa de forma general como

$$\begin{aligned}
U|0\rangle &= u_{0,0}|0\rangle + u_{0,1}|1\rangle + u_{0,2}|2\rangle + ... + u_{0,2^n-1}|2^n-1\rangle \equiv |U_0\rangle, \\
U|1\rangle &= u_{1,0}|0\rangle + u_{1,1}|1\rangle + u_{1,2}|2\rangle + ... + u_{1,2^n-1}|2^n-1\rangle \equiv |U_1\rangle, \\
U|2\rangle &= u_{2,0}|0\rangle + u_{2,1}|1\rangle + u_{2,2}|2\rangle + ... + u_{2,2^n-1}|2^n-1\rangle \equiv |U_2\rangle, \\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
U|2^n-1\rangle &= u_{2^n-1,0}|0\rangle + u_{2^n-1,1}|1\rangle + u_{2^n-1,2}|2\rangle + ... + u_{2^n-1,2^n-1}|2^n-1\rangle \equiv |U_{2^n-1}\rangle,
\end{aligned} \tag{6.72}$$

donde los factores $u_{i,j}$ son números complejos que cumplen con la condición

de normalización

$$|u_{i,0}|^2 + |u_{i,1}|^2 + |u_{i,2}|^2 + ... + |u_{i,2^n-1}|^2 = 1. \tag{6.73}$$

Utilizamos el algoritmo descrito en la sección 6.2 para encontrar la descomposición del operador U como el producto de reflexiones de Householder.

Primero intercambiamos los vectores $|0\rangle$ y $|\mathbb{I}_{0,1}\rangle$ con el operador de relfexión $[r_1^{(0)}]$, con

$$\begin{aligned} |\mathbb{I}_{0,1}\rangle &= [|0\rangle\langle 0| + |1\rangle\langle 1|]|U_0\rangle \\ &= u_{0,0}|0\rangle + u_{0,1}|1\rangle. \end{aligned} \tag{6.74}$$

El operador de reflexión resultante es

$$\begin{aligned} [r_1^{(0)}] = \mathbb{I} - \left(1 - \frac{|u_{0,0}|}{(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}}\right)|0\rangle\langle 0| + \frac{u_{0,0}{u_{0,1}}^*}{|u_{0,0}|(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}}|0\rangle\langle 1| \\ + \frac{{u_{0,0}}^* u_{0,1}}{|u_{0,0}|(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}}|1\rangle\langle 0| - \left(1 + \frac{|u_{0,0}|}{(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}}\right)|1\rangle\langle 1|. \end{aligned} \tag{6.75}$$

Ahora utilizamos el operador $[r_2^{(0)}]$ para intercambiar los vectores $|0\rangle$ y $|\mathbb{I}_{0,2}\rangle$, donde

$$\begin{aligned} |\mathbb{I}_{0,2}\rangle &= [|0\rangle\langle 0| + |2\rangle\langle 2|][r_1^{(0)}]|U_0\rangle \\ &= \frac{u_{0,0}}{|u_{0,0}|}(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}|0\rangle + u_{0,2}|2\rangle. \end{aligned} \tag{6.76}$$

El operador de reflexión se calcula como

$$\begin{aligned}[r_2^{(0)}] = \mathbb{I} &- \left(1 - \frac{(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}}{(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}}\right)|0\rangle\langle 0| \\ &+ \frac{u_{0,0}{u_{0,2}}^*}{|u_{0,0}|(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}}|0\rangle\langle 2| \\ &+ \frac{{u_{0,0}}^* u_{0,2}}{|u_{0,0}|(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}}|2\rangle\langle 0| \\ &- \left(1 + \frac{(|u_{0,0}|^2 + |u_{0,1}|^2)^{1/2}}{(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}}\right)|2\rangle\langle 2|.\end{aligned} \tag{6.77}$$

Continuamos aplicando el operador $[r_3^{(0)}]$ para realizar el intercambio entre los vectores $|0\rangle$ y $|\mathbb{I}_{0,3}\rangle$, definiendo

$$\begin{aligned}|\mathbb{I}_{0,3}\rangle &= [|0\rangle\langle 0| + |3\rangle\langle 3|][r_2^{(0)}][r_1^{(0)}]|U_0\rangle \\ &= \frac{u_{0,0}}{|u_{0,0}|}(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}|0\rangle + u_{0,2}|2\rangle.\end{aligned} \tag{6.78}$$

El operador que realiza este intercambio es

$$\begin{aligned}[r_3^{(0)}] = \mathbb{I} &- \left(1 - \frac{(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}}{(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2 + |u_{0,3}|^2)^{1/2}}\right)|0\rangle\langle 0| \\ &+ \frac{u_{0,0}{u_{0,3}}^*}{|u_{0,0}|(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2 + |u_{0,3}|^2)^{1/2}}|0\rangle\langle 3| \\ &+ \frac{{u_{0,0}}^* u_{0,3}}{|u_{0,0}|(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2 + |u_{0,3}|^2)^{1/2}}|3\rangle\langle 0| \\ &- \left(1 + \frac{(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2)^{1/2}}{(|u_{0,0}|^2 + |u_{0,1}|^2 + |u_{0,2}|^2 + |u_{0,3}|^2)^{1/2}}\right)|3\rangle\langle 3|.\end{aligned} \tag{6.79}$$

Analizando la sucesión de los vectores de reflexión, se puede deducir la forma en que se calculan los factores que acompañan a los operadores $|i\rangle\langle j|$. Encon-

tramos que los operadores de reflexión están dados como

$$[r_j^{(i)}] = \mathbb{I} - (1 - r_{i,i})|i\rangle\langle i| + r_{i,j}^*|i\rangle\langle j| + r_{i,j}|j\rangle\langle i| - (1 + r_{i,i})|j\rangle\langle j|, \tag{6.80}$$

con

$$\begin{aligned} r_{i,i} &= \left(\frac{\sum_i^{j-1} |u_{i,j}|^2}{\sum_i^j |u_{i,j}|^2} \right)^{1/2}, \\ r_{i,j} &= \frac{{u_{i,i}}^* u_{i,j}}{|u_{i,i}|} \left(\sum_i^j |u_{i,j}|^2 \right)^{-1/2}, \end{aligned} \tag{6.81}$$

Utilizando esta expresión, tenemos que un operador arbitrario U actuando sobre un sistema de n qubits se puede representar como el producto de reflexiones de Householder tal que

$$U = \left(\prod_{i=0}^{n} [r^{(i)}] \right) D, \tag{6.82}$$

donde D es una matriz diagonal y donde

$$[r^{(i)}] = \prod_{j=i}^{n} [r_j^{(i)}]. \tag{6.83}$$

Las ecuaciones (6.80) - (6.83) nos dan la forma analítica en que se puede descomponer un operador arbitrario como el producto de reflexiones de Householder. Ahora daremos la representación de las reflexiones como compuertas cuánticas elementales.

6.3 Representación en compuertas cuánticas de las reflexiones de Householder

Tenemos que una reflexion de Householder arbitraria

$$[r_j^{(i)}] = \mathbb{I} - (1 - r_{i,i})|i\rangle\langle i| + r_{i,j} * |i\rangle\langle j| + r_{i,j}|j\rangle\langle i| - (1 + r_{i,i})|j\rangle\langle j|, \tag{6.84}$$

actua sobre los vectores $|i\rangle$ y $|j\rangle$ como

$$\begin{aligned} [r_j^{(i)}]|i\rangle &= r_{i,i}|i\rangle + r_{i,j}|j\rangle, \\ [r_j^{(i)}]|j\rangle &= r_{i,j}^*|i\rangle - r_{i,i}|j\rangle, \end{aligned} \tag{6.85}$$

y como la identidad para el resto de los vectores

$$[r_j^{(i)}]|k \neq i, j\rangle = |k\rangle. \tag{6.86}$$

Nuestro objetivo es encontrar una serie de compuertas con un solo qubit objetivo que en conjunto actuen igual que la reflexión $[r_j^{(i)}]$. Para esto es necesario expander los vectores que son reflejados en funcion del estado de los qubits que los componen,

$$\begin{aligned} |i\rangle &= |i_1 i_2 i_3 ... i_{n-1} i_n\rangle, \\ |j\rangle &= |j_1 j_2 i_3 ... j_{n-1} j_n\rangle. \end{aligned} \tag{6.87}$$

Como primer paso, identificamos los qubits que tienen el mismo estado en los vectores $|i\rangle$ y $|j\rangle$. Representamos la reflexión $[r_j^{(i)}]$ como una compuerta controlada que tiene los qubits en estados iguales como qubits de control, los qubits en estados diferentes como qubit objetivo y como palabra de control el estado de los qubits

iguales. Tenemos por ejemplo el caso en que la compuerta $[r^{(a)}]$ refleja los estados

$$\begin{aligned} |i\rangle &= |a_1 a_2 a_3 i_4 i_5 ... i_{n-1} i_n\rangle, \\ |j\rangle &= |a_1 a_2 a_3 j_4 j_5 ... j_{n-1} j_n\rangle. \end{aligned} \tag{6.88}$$

donde los qubits a_l son iguales en ambos vectores y los qubits i_m estan en un estado diferente a los qubits j_m. En este caso representaremos la reflexión $[r^{(a)}]$ como la compuerta controlada Ra que utiliza los tres primeros qubits como control y que tiene como palabra de control el estado $|a_1 a_2 a_3\rangle$,

$$[r^{(a)}]|a_1 a_2 a_3 i_4 i_5 ... i_{n-1} i_n\rangle = Ra^{(123,45...n)}_{|a_1 a_2 a_3\rangle}|a_1 a_2 a_3 i_4 i_5 ... i_{n-1} i_n\rangle. \tag{6.89}$$

A partir de aquí nos concentraremos unicamente en descomponer el operador Ra y las compuertas en las que se encuentre su descomposición serán controladas por los tres primeros qubits, con palabra de control $|a_1 a_2 a_3\rangle$.

El segundo paso consiste en encontrar una compuerta con un solo qubit objetivo que actúe solo sobre los estados formados por los qubits que son diferentes en los vectores $|i\rangle$ y $|j\rangle$. En nuestro ejemplo, el operador Ra actua diferente de la identidad sobre los estados $|i_4 i_5 ... i_{n-1} i_n\rangle$ y $|j_4 j_5 ... j_{n-1} j_n\rangle$, cuyos qubits se encuentran en estados opuestos,

$$j_l = 1 - i_l. \tag{6.90}$$

por lo que podemos expresar el estado $|j_4 j_5 ... j_{n-1} j_n\rangle$ como

$$|j_4 j_5 ... j_{n-1} j_n\rangle = |(1 - i_4)(1 - i_5)...(1 - i_{n-1})(1 - i_n)\rangle. \tag{6.91}$$

Realizamos la observación de que sí aplicamos una compuerta CNOT entre dos quibits de los vectores con estados contrarios obtendremos el mismo resultado. En nuestro ejemplo sí aplicamos a los vectores $|i_4 i_5 ... i_{n-1} i_n\rangle$ y $|j_4 j_5 ... j_{n-1} j_n\rangle$ la compuerta CNOT $U^{(l,m)}_{CN}$ la cual tiene el qubit l como control y el qubit m como objetivo,

$$U^{(l,m)}_{CN}|i_4 j_5 ... i_l ... i_m ... i_{n-1} i_n\rangle = |i_4 j_5 ... i_l ... (i_m - i_l)^2 ... i_{n-1} i_n\rangle. \tag{6.92}$$

$$
\begin{aligned}
U_{CN}^{(l,m)}|j_4 j_5 ... j_l ... j_m ... j_{n-1} j_n\rangle &= |j_4 j_5 ... j_l ... (j_m - j_l)^2 ... j_{n-1} j_n\rangle \\
&= |j_4 j_5 ... j_l ... ((1 - i_m) - (1 - i_l))^2 ... j_{n-1} j_n\rangle \\
&= |j_4 j_5 ... j_l ... (i_m - i_l)^2 ... j_{n-1} j_n\rangle.
\end{aligned} \tag{6.93}
$$

Observamos que el qubit m tiene el mismo estado en ambos casos.

Si aplicamos compuertas CNOT controladas por el ultimo qubit para todos qubits restantes obtenemos

$$
U_{CN}^{(4,n)} U_{CN}^{(5,n)} ... U_{CN}^{(n-1,n)} |i_4 j_5 ... i_{n-1} i_n\rangle = |(i_4 - i_n)^2 (i_5 - i_n)^2 ... (i_{n-1} - i_n)^2 i_n\rangle, \tag{6.94}
$$

$$
U_{CN}^{(4,n)} U_{CN}^{(5,n)} ... U_{CN}^{(n-1,n)} |j_4 j_5 ... j_{n-1} j_n\rangle = |(i_4 - i_n)^2 (i_5 - i_n)^2 ... (i_{n-1} - i_n)^2 (1 - i_n)\rangle, \tag{6.95}
$$

en donde los qubits tienen el mismo estado en ambos casos, excepto el último qubit. Proponemos entonces que la compuerta Ra actúa sobre el último qubit de la forma

$$
\begin{aligned}
Ra^{(n)}|i_n\rangle &= r_{i,i}|i_n\rangle + r_{j,i}|j_n\rangle, \\
Ra^{(n)}|j_n\rangle &= r_{i,j}|i_n\rangle - r_{j,j}|j_n\rangle,
\end{aligned} \tag{6.96}
$$

teniendo como palabra de control el estado $|(i_4 - i_n)^2 (i_5 - i_n)^2 ... (i_{n-1} - i_n)^2\rangle$. Luego de aplicar la compuerta $Ra^{(n)}$ es necesario aplicar nuevamente las compuertas CNOT para regresar los qubits alterados a su estado original. Por lo tanto podemos representar el operador Ra como

$$
Ra = U_{CN}^{(n-1,n)} ... U_{CN}^{(5,n)} U_{CN}^{(4,n)} Ra^{(n)}_{|(i_4 - i_n)^2 (i_5 - i_n)^2 ... (i_{n-1} - i_n)^2\rangle} U_{CN}^{(4,n)} U_{CN}^{(5,n)} ... U_{CN}^{(n-1,n)}. \tag{6.97}
$$

Por último, agregamos a la palabra de control el estado de los qubits iguales

en los vectores $|i\rangle$ y $|j\rangle$. Para nuestro ejemplo, y de acuerdo a la ecuación (6.89), tenemos que la reflexión $[r^{(a)}]$ es la compuerta controlada Ra con palabra de control $|a_1a_2a_3\rangle$, por lo tanto tendremos que esta reflexión se puede representar como

$$[r^{(a)}] = U_{CN}^{(n-1,n)}...U_{CN}^{(5,n)}U_{CN}^{(4,n)}Ra^{(n)}_{|a_1a_2a_3(i_4-i_n)^2(i_5-i_n)^2...(i_{n-1}-i_n)^2\rangle}U_{CN}^{(4,n)}U_{CN}^{(5,n)}...U_{CN}^{(n-1,n)}, \tag{6.98}$$

donde la compuerta Ra es simplemente

$$Ra = \begin{pmatrix} r_{i,i} & r_{i,j} \\ r_{i,j}^* & r_{i,i} \end{pmatrix}. \tag{6.99}$$

Resumiendo, el método para encontrar la representación de una reflexión arbitraria $[r_j^{(i)}]$ como el producto de compuertas con un solo qubit de objetivo es

1. Identificar en los vectores $|i\rangle$ y $|j\rangle$, que son los vectores en los que la reflexión actúa diferente de la identidad, los qubits que en ambos vectores están en el mismo estado (estados iguales) y los qubits en el vector $|i\rangle$ están en un estado diferente al mismo qubit en el vector $|j\rangle$ (estados opuestos).

2. Aplicar compuertas CNOT que tienen como control uno de los qubits con estado opuesto y como objetivo cada uno del resto de los qubits con estado opuesto.

3. Aplicar sobre el qubit de control una compuerta controlada R_H, cuya palabra de control será los estados iguales y los estados que resulten después de aplicar las compuertas CNOT a los estados opuestos.

4. Aplicar las mismas compuertas CNOT que se aplicaron en el segundo paso después de la compuerta R_H.

La compuerta R_H dependerá de la reflexión original, y tendrá la forma matricial

$$R_H = \begin{pmatrix} r_{i,i} & r_{i,j} \\ r_{i,j}^* & r_{i,i} \end{pmatrix}. \tag{6.100}$$

A continuación daremos un ejemplo más especifico: Supongamos la reflexión $[r^{(37)}]$ tal que

$$\begin{aligned}[r^{(37)}] = \mathbb{I} - (1 - r_{37,37})|100101\rangle\langle 100101| + r^{*}_{37,43}|100101\rangle\langle 101011| \\ + r_{37,43}|101011\rangle\langle 100101| - (1 + r_{37,37})|101011\rangle\langle 101011|,\end{aligned} \tag{6.101}$$

donde se refleja los estados $|100101\rangle$ y $|101011\rangle$.

Siguiendo nuestro método, observamos que en los estados reflejados el primero, segundo y ultimo qubit tienen el mismo estado, por lo que la reflexión $[r^{(37)}]$ se puede representar en primeras instancias como la compuerta Rh controlada por el primer, segundo y último qubit,

$$[r^{(37)}] = Rh^{(126,345)}_{|1\rangle_1|0\rangle_2|1\rangle_6}. \tag{6.102}$$

Como el siguiente paso, aplicamos compuertas CNOT a los qubits que en los estados reflejados tienen estados diferentes. Aplicaremos una compuerta CNOT que tiene como control el quinto qubit y como objetivo el tercer qubit, y también una compuerta CNOT que tiene como control el quinto qubit y como objetivo el cuarto qubit. De esta forma, la compuerta Rh se podrá representar como una compuerta controlada con palabra de control $|01\rangle$, controlada por el tercer y cuarto qubit y con objetivo el quinto quibit. Aplicando nuevamente las compuertas CNOT, para regresar los qubits a su estado original, tendremos la representación

$$Rh = U^{(5,4)}_{CN} U^{(5,3)}_{CN} Rh^{(34,5)}_{|01\rangle} U^{(5,3)}_{CN} U^{(5,4)}_{CN}. \tag{6.103}$$

Debido a que la compuerta Rh esta controlada por el primer, segundo y sexto qubit, agregamos a la palabra de control el estado $|1\rangle_1|0\rangle_2|1\rangle_6$, obteniendo finalmente que la reflexión $[r^{(37)}]$ se puede representar en compuertas cuánticas como

$$[r^{(37)}] = U^{(5,4)}_{CN} U^{(5,3)}_{CN} Rh^{(5)}_{|1\rangle_1|0\rangle_2|0\rangle_3|1\rangle_4|1\rangle_6} U^{(5,3)}_{CN} U^{(5,4)}_{CN}, \tag{6.104}$$

donde la matriz Rh es de la forma que se muestra en la ecuación (6.100) . El

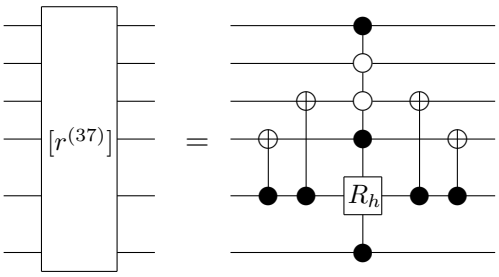

Figura 6.2: Representación de la reflexión $[r^{(37)}]$ como compuertas CNOT y una compuerta controlada Rh con un solo qubit objetivo.

circuito cuántico de esta representación se muestra en la figura 6.2.

Para encontrar la representación del operador D como compuertas cuánticas, primero observamos que esta matriz diagonal tiene la forma

$$D = \begin{pmatrix} d_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & 0 & \cdots & 0 \\ 0 & 0 & 0 & d_4 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & d_{2^n} \end{pmatrix}, \tag{6.105}$$

que podemos descomponer como el producto

$$D = \begin{pmatrix} d_1 & 0 & 0 & 0 & \cdots \\ 0 & d_2 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & d_3 & 0 & \cdots \\ 0 & 0 & 0 & d_4 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdots, \tag{6.106}$$

La primera matriz actúa diferente de la identidad sobre estados de la forma $|000...00\rangle|i\rangle$, la segunda matriz actúa diferente de la identidad sobre estados del tipo $|000...01\rangle|i\rangle$, y así sucesivamente hasta tener que la última matriz del producto actúa diferente de la identidad sobre estados de la forma $|111...11\rangle|i\rangle$. Por lo tanto, podemos representar la primera matriz como una compuerta que actúa sobre el último qubit con palabra de control $|000...00\rangle$, el segundo qubit como una compuerta que actúa sobre el último qubit con palabra de control $|000...01\rangle$,

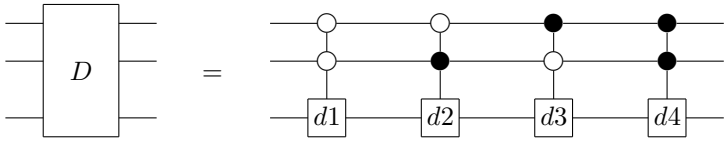

Figura 6.3: Representación de la matriz diagonal D como compuertas con un solo qubit objetivo, para el caso de tres qubits.

etcétera, obteniendo que la matriz diagonal D se puede representar como

$$D = d1^{(2^n)}_{|000...00\rangle} d2^{(2^n)}_{|000...01\rangle} ... dm^{(2^n)}_{|111...11\rangle}. \tag{6.107}$$

Un ejemplo de esta representación se muestra en la figura 6.3.

En esta sección se dio un método para encontrar la representación en compuertas cuánticas de una reflexión de Householder arbitraria. Combinando este metodo, el metodo de representación de un operador con una palabra de control arbitraria (seccion 5.3) y el algoritmo que da la representación de un operador arbitrario como el producto de reflexiones de Householder, es posible encontrar la representacion de un operador arbitrario como el producto de compuertas cuánticas fundamentales, dando el circuito cuántico que reproduce la acción de dicho operador. En ciertas implementaciones físicas no es necesario desarrollar la compuerta con palabra arbitraria en función de compuertas más simples [27; 28; 29; 30], por lo que la representación dada en este capítulo para las reflexiones será suficiente para establecer el arreglo experimental que reproduzca la acción del operador.

El procedimiento descrito no dan una representación única del operador como reflexiones y de las reflexiones como compuertas, por lo que es importante establecer un criterio que optimice el circuito cuántico resultante.

6.4 Reducción del circuito cuántico para reflexiones de Householder

Anteriormente se ha buscado la manera de optimizar la síntesis de circuitos cuánticos debido a que el número de compuertas necesarias crece rapidamente

conforme aumenta el número de qubits del sistema [32; 33]. Nuestro método de sintesis permite la reducción del ciruito cuántico al utilizar una metodología que describiremos a continuación.

Cuando se plantea el algoritmo para encontrar la represetación de un operador como el producto de reflexiones de Householder, en la sección 6.2, se tiene que solo existe una restricción para la selección de los vectores sobre cuyo espacio se realiza la reflexión: que la pareja de vectores no se haya utilizado para una reflexión anterior. Esta restricción es muy flexible y permite que exista un gran número de representaciones equivalentes. Tenemos también que la representación en compuertas de cada reflexión no es única (ver sección 6.3).

Estas libertades de selección plantean la posibilidad de establecer algún criterio que permita "optimizar" el circuito finál; la definición de "óptimo" dependerá de la implementacíon que se le desee dar al circuito. Algunas compuertas cuánticas son más faciles realizar experimentalmente que otras según el tipo de sistema que sirva como qubits, o se pudiera desear simplemente que el circuito fuese el más corto posible.

A continuación mostraremos como una selección particular de los vectores, al aplicar el algoritmo descrito en la sección 6.2, así como una selección especifica de la representación en compuertas cuánticas de las reflexiones, darán como resultado un circuito que es evidentemente más reducido (compuesto por un número menor de compuertas) que cualquier otra selección. La selección de los vectores y de la representación de las reflexiones la haremos tal que coloquemos continuas dos compuertas CNOT iguales el mayor número de veces posible.

Comenzaremos reduciendo la serie de compuertas $[r^{(0)}]$, definida como

$$[r^{(0)}] = [r_1^{(0)}][r_2^{(0)}][r_3^{(0)}]...[r_{2^n}^{(0)}]. \tag{6.108}$$

La reducción de esta representación permitirá intuir la forma en que se reducirán el resto de las series de reflexiones $[r^{(1)}]$, $[r^{(2)}]$, $[r^{(3)}]$, etc.

Tomaremos la primera reflexion $[r_1^{(0)}]$,

$$\begin{aligned}[r_1^{(0)}] = \mathbb{I} - (1 - r_{0,0})|00...000\rangle\langle 00...000| + r_{0,1}^*|00...000\rangle\langle 00...001| \\ + r_{0,1}|00...001\rangle\langle 00...000| - (1 + r_{1,1})|00...001\rangle\langle 00...001|,\end{aligned} \tag{6.109}$$

que refleja los vectores $|00...000\rangle$ y $|00...001\rangle$. Utilizando la metodología descrita en la sección 6.3 obtenemos que esta reflexión se puede representar como

$$[r_1^{(0)}] = R1^{(n)}_{|0\rangle_1|0\rangle_2...|0\rangle_{n-1}}, \tag{6.110}$$

donde la compuerta $R1$ actúa sobre el último qubit, tiene palabra de control $|00...00\rangle$ y tiene una forma matricial como se indica en la ecuación (6.100).

Para la compuerta $[r_2^{(0)}]$ seleccionaremos los vectores $|00...000\rangle$ y $|00...011\rangle$ como los vectores reflejados tal que

$$\begin{aligned}[r_2^{(0)}] = \mathbb{I} - (1 - r'_{0,0})|00...000\rangle\langle 00...000| + r^*_{0,3}|00...000\rangle\langle 00...011| \\ + r_{0,3}|00...011\rangle\langle 00...000| - (1 + r_{3,3})|00...011\rangle\langle 00...011|.\end{aligned} \tag{6.111}$$

Para esta reflexión encontramos la representación

$$[r_2^{(0)}] = U_{CN}^{(n,n-1)} R2^{(n)}_{|0\rangle_1|0\rangle_2...|0\rangle_{n-1}} U_{CN}^{(n,n-1)}, \tag{6.112}$$

similar a la representación de la compuerta $[r_1^{(0)}]$, excepto que se aplica una compueta CNOT con el último qubit como control y el penúltimo qubit como objetivo, antes y después de la compuerta controlada $R2$.

El siguiente paso es seleccionar los vectores $|00...000\rangle$ y $|00...111\rangle$ como los vectores reflejados por $[r_3^{(0)}]$,

$$\begin{aligned}[r_3^{(0)}] = \mathbb{I} - (1 - r''_{0,0})|00...000\rangle\langle 00...000| + r^*_{0,5}|00...000\rangle\langle 00...111| \\ + r_{0,5}|00...111\rangle\langle 00...000| - (1 + r_{5,5})|00...111\rangle\langle 00...111|.\end{aligned} \tag{6.113}$$

La representación de esta reflexión en compuertas sera

$$[r_3^{(0)}] = U_{CN}^{(n,n-1)} U_{CN}^{(n,n-2)} R3^{(n)}_{|0\rangle_1|0\rangle_2...|0\rangle_{n-1}} U_{CN}^{(n,n-2)} U_{CN}^{(n,n-1)}, \tag{6.114}$$

Continuamos con este procedimiento para las reflexiones $[r_4^{(0)}]$, $[r_5^{(0)}]$, etcétera, hasta que seleccionemos los vectores $|00...000\rangle$ y $|11...111\rangle$ para la reflexión $[r_n^{(0)}]$,

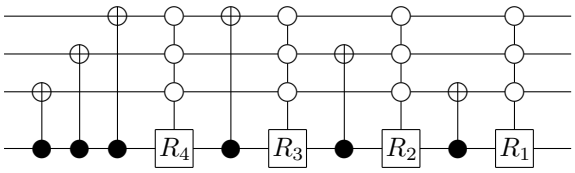

Figura 6.4: Circuito reducido del producto $[r_1^{(0)}][r_2^{(0)}][r_3^{(0)}][r_4^{(0)}]$ bajo nuestro criterio de selección, para el caso de cuatro qubits.

que representaremos como

$$[r_n^{(0)}] = U_{CN}^{(n,n-1)} U_{CN}^{(n,n-2)} ... U_{CN}^{(n,2)} U_{CN}^{(n,1)} Rn^{(n)}_{|0\rangle_1 |0\rangle_2 ... |0\rangle_{n-1}} U_{CN}^{(n,1)} U_{CN}^{(n,2)} ... U_{CN}^{(n,n-2)} U_{CN}^{(n,n-1)}, \tag{6.115}$$

Si realizamos el producto de las relfexiones bajo esta representación tendremos que las compuertas CNOT se "eliminan" mutuamente (debido a la propiedad $U_{CN} U_{CN} = \mathbb{I}$), por lo que la representación de la serie se reduce,

$$\begin{aligned}[r_1^{(0)}][r_2^{(0)}]...[r_{n-1}^{(0)}][r_n^{(0)}] =& R1^{(n)}_{|00..00\rangle} U_{CN}^{(n,n-1)} R2^{(n)}_{|00..00\rangle} U_{CN}^{(n,n-2)} R3^{(n)}_{|00..00\rangle} U_{CN}^{(n,n-3)} \otimes ... \\ & \otimes U_{CN}^{(n,1)} Rn^{(n)}_{|00..00\rangle} U_{CN}^{(n,1)} U_{CN}^{(n,2)} ... U_{CN}^{(n,n-2)} U_{CN}^{(n,n-1)}.\end{aligned} \tag{6.116}$$

La representación del producto de las refelxiones $[r_i^{(0)}]$ dado en la ecuación (6.116) utiliza solamente una compuerta con un qubit objetivo y dos compuertas CNOT por cada reflexión en el producto, exepto para $[r_1^{(0)}]$ que no utiliza compuertas CNOT (ver figura 6.4). Esta representación es evidentemente más reducida que cualquier otra representación que pueda construirse seleccionando otro orden de vectores y otra representación para las reflexiones resultantes.

Para el resto de las reflexiones que componen a $[r^{(0)}]$ procederemos de forma similar. Primero seleccionamos los vectores $|00...000\rangle$ y $|00...010\rangle$ como los vectores reflejados por $[r_{n+1}^{(0)}]$, por lo que su representación sera simplemente

$$[r_{n+1}^{(0)}] = R(n+1)^{(n-1)}_{|0\rangle_1 |0\rangle_2 ... |0\rangle_{n-2} |0\rangle_n}, \tag{6.117}$$

que es una compuerta que actua sobre el penúltimo qubit, con todos los qubits de control requeridos en el estado $|0\rangle$.

Operando de forma similar al caso de las compuertas $[r_1^{(0)}]$-$[r_n^{(0)}]$, seleccionaremos los vectores $|00...000\rangle$ y $|00...110\rangle$ para la reflexión $[r_{n+2}^{(0)}]$, la cual representaremos como

$$[r_{n+2}^{(0)}] = U_{CN}^{(n-1,n-2)} R(n+2)_{|0\rangle_1|0\rangle_2...|0\rangle_{n-2}|0\rangle_n}^{(n-1)} U_{CN}^{(n-1,n-2)}. \tag{6.118}$$

El operador $[r_{n+3}^{(0)}]$ reflejará los estados $|0...0000\rangle$ y $|0...1110\rangle$, y así sucesivamente hata tener que el operador $[r_{2n-1}^{(0)}]$ refleja los vectores $|00...000\rangle$ y $|11...110\rangle$, que estará representado como

$$\begin{aligned}[r_{2n-1}^{(0)}] =& U_{CN}^{(n-1,n-2)} U_{CN}^{(n-1,n-3)} ... U_{CN}^{(n-1,2)} U_{CN}^{(n-1,1)} R(2n-1)_{|0\rangle_1|0\rangle_2...|0\rangle_{n-2}|0\rangle_n}^{(n-1)} \\ & \otimes U_{CN}^{(n-1,n-2)} U_{CN}^{(n-1,1)} U_{CN}^{(n-1,2)} ... U_{CN}^{(n-1,n-3)} U_{CN}^{(n-1,n-2)}.\end{aligned} \tag{6.119}$$

Si realizamos el producto de las compuertas $[r_{n+i}^{(0)}]$ encontraremos nuevamente una reducción en el número total de compuertas necesarias,

$$\begin{aligned}[r_{n+1}^{(0)}][r_{n+2}^{(0)}]...[r_{2n-1}^{(0)}] =& R(n+1)_{|0...00\rangle}^{(n-1)} U_{CN}^{(n-1,n-2)} R(n+2)_{|0...00\rangle}^{(n-1)} U_{CN}^{(n-1,n-3)} R(n+3)_{|0...00\rangle}^{(n-1)} \otimes \\ & ... \otimes U_{CN}^{(n-1,1)} R(2n-1)_{|0...00\rangle}^{(n-1)} U_{CN}^{(n-1,1)} U_{CN}^{(n-1,2)} ... U_{CN}^{(n-1,n-2)}.\end{aligned} \tag{6.120}$$

En este punto resulta claro la forma en que se requiere realizar la selección de los vectores reflejados y la representación de las reflexiones en compuertas para lograr la reducción del número de compuertas necesarias. Este razonamiento será aplicado para el resto de los productos $[r^{(1)}]$, $[r^{(2)}]$, etcétera, con lo que se obtendrá la reducción del circuito final.

En esta sección se describe una metodología para la selección de las reflexiones de Householder en las que se descompone un operador arbitrario y de la representación de estas reflexiones que permite la reducción del circuito cuántico que representa al operador arbitrario.

Nuestro algoritmo de síntesis de circuitos cuáticos ofrece la ventaja de ser flexible, con lo que se puede obtener una representación optima acorde a las necesidades del usuario. Además, utilizando el criterio de selección propuesto se

logra la reducción del circuito al momento de la síntesis para el caso general, en comparación con otros métodos que reducen el circuito una vez dada la representación, actuando diferente para cada caso en particular [32; 33].

Capítulo 7

Conclusiones y Perspectivas

Se logró desarrollar un algoritmo mediante el cual es posible encontrar la representación de un operador arbitrario que actúa sobre cualquier número de qubits como el producto de compuertas cuánticas elementales. El algoritmo opera primero encontrando la descomposición del operador como el producto de reflexiones de Householder y segundo dando la representación de cada reflexion en compuertas cuánticas. Por último, se representan las compuertas obtenidas en función de compuertas cada vez más simples hasta que solo se utilicen las compuertas definidas como elmentales.

El algoritmo permite encontrar diferentes representaciones para un mismo operador, lo cual puede ser explotado en la búsqueda del circuito más eficiente, según sea su implementación física. También se tiene la ventaja de que, mediante un criterio de selección sencillo, se puede encontrar la representación cuyo circuito equivalente contiene el menor número de compuertas cuánticas.

Como trabajo a futuro se pretende ampliar el algoritmo de busqueda para que obtenga el circuito cuántico más eficiente: Al establecer la definición de eficiencia, se impondran condiciones en el criterio de selección durante el desarrollo del algoritmo lo que resultará en la representación óptima del operador, facilitando su implementación experimental.

Apendice A

.1 Descomposición de compuertas controladas por dos qubits

Dado un operador U que actúa en el espacio de tres qubits $|c_1\rangle|c_2\rangle|t\rangle$ donde los qubits $|c_1\rangle$ y $|c_2\rangle$ son los qubits de control que requieren estar en el estado $|1\rangle$ para que el operador actúe diferente de la identidad sobre el qubit objetivo $|t\rangle$, se tiene la ecuación

$$U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle = |c_1\rangle|c_2\rangle U^{c_1\cdot c_2}|t\rangle, \tag{1}$$

donde el superindice (c_1c_2, t) indica que la compuerta esta controlada por los qubits $|c_1\rangle|c_2\rangle$ y tiene como objetivo el qubit $|t\rangle$, y donde el exponente $c_1 \cdot c_2$ es el producto del valor numérico de c_1 y c_2, con $U^0 = I$ el operador identidad. Proponemos un operador V tal que $V^2 = U$ de forma que

$$\begin{aligned} U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle &= |c_1\rangle|c_2\rangle U^{c_1\cdot c_2}|t\rangle \\ &= |c_1\rangle|c_2\rangle (V^2)^{c_1\cdot c_2}|t\rangle \\ &= |c_1\rangle|c_2\rangle V^{2c_1\cdot c_2}|t\rangle. \end{aligned} \tag{2}$$

Colocamos dentro de la ecuación el producto $V^{c_1}V^{-c_1}$ el cual es igual al operador identidad para cualquier valor de c_1, lo que no altera la ecuación, con lo

que obtenemos

$$U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle = |c_1\rangle|c_2\rangle V^{c_1}V^{-c_1}V^{2c_1\cdot c_2}|t\rangle. \tag{3}$$

El término V^{c_1} es la forma en que actua un operador V que tiene como control el qubit $|c_1\rangle$, por lo que podemos reescribir la ecuación como

$$\begin{aligned} U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle &= |c_1\rangle|c_2\rangle V^{c_1}V^{-c_1}V^{2c_1\cdot c_2}|t\rangle \\ &= V^{(c_1,t)}|c_1\rangle|c_2\rangle V^{-c_1}V^{2c_1\cdot c_2}|t\rangle. \end{aligned} \tag{4}$$

Procediendo de igual manera introducimos el producto ${U_{CN}}^{c_1}{U_{CN}}^{c_1}$, recordando que $U_{CN}U_{CN} = I$, de tal manera que

$$U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle = V^{(c_1,t)}|c_1\rangle{U_{CN}}^{c_1}{U_{CN}}^{c_1}|c_2\rangle V^{-c_1}V^{2c_1\cdot c_2}|t\rangle. \tag{5}$$

El operadro ${U_{CN}}^{c_1}$ actúa sobre el qubit $|c_2\rangle$, modificandolo como ${U_{CN}}^{c_1}|c_2\rangle = |c_2 + c_1 - 2c_1\cdot c_2\rangle$, y es equivalente al operador U_{CN} que tiene como control el qubit $|c_1\rangle$ y como objetivo el qubit $|c_2\rangle$. De tal forma se obtiene la ecuación

$$\begin{aligned} U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle &= V^{(c_1,t)}|c_1\rangle{U_{CN}}^{c_1}{U_{CN}}^{c_1}|c_2\rangle V^{-c_1}V^{2c_1\cdot c_2}|t\rangle \\ &= V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}|c_1\rangle|c_2 + c_1 - 2c_1\cdot c_2\rangle V^{-c_1}V^{2c_1\cdot c_2}|t\rangle. \end{aligned} \tag{6}$$

Ahora introducimos el producto $V^{-c_2-c_1+2c_1}V^{c_2+c_1-2c_1}$, tal que

$$\begin{aligned} &V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}|c_1\rangle|c_2 + c_1 - 2c_1\cdot c_2\rangle V^{-c_2-c_1+2c_1}V^{c_2+c_1-2c_1}V^{-c_1}V^{2c_1\cdot c_2}|t\rangle \\ &= V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}|c_1\rangle|c_2 + c_1 - 2c_1\cdot c_2\rangle V^{-c_2-c_1+2c_1}V^{c_2}|t\rangle. \end{aligned} \tag{7}$$

El término $V^{-c_2-c_1+2c_1} = (V^{-1})^{c_2+c_1-2c_1}$ es la forma en que actua un operador V^{-1} que tiene como control el segundo qubit (que esta en el estado $|c_2 + c_1 - 2c_1\cdot$

$c_2\rangle$), con lo que llegamos a

$$\begin{aligned} &V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}|c_1\rangle|c_2+c_1-2c_1\cdot c_2\rangle V^{-c_2-c_1+2c_1}V^{c_2}|t\rangle \\ &= V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}(V^{-1})^{(c_2,t)}|c_1\rangle|c_2+c_1-2c_1\cdot c_2\rangle V^{c_2}|t\rangle. \end{aligned} \tag{8}$$

Volvemos a introducir el producto ${U_{CN}}^{c_1}{U_{CN}}^{c_1}$, para que el segundo qubit vuelva a su estado original ${U_{CN}}^{c_1}|c_2+c_1-2c_1\cdot c_2\rangle = |c_2\rangle$,

$$\begin{aligned} &V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}|c_1\rangle{U_{CN}}^{c_1}{U_{CN}}^{c_1}|c_2+c_1-2c_1\cdot c_2\rangle V^{-c_2-c_1+2c_1}V^{c_2}|t\rangle \\ &= V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}(V^{-1})^{(c_2,t)}{U_{CN}}^{(c_1,c_2)}|c_1\rangle|c_2\rangle V^{c_2}|t\rangle. \end{aligned} \tag{9}$$

El término V^{c_2} es equivalente a la forma en que actúa un operado V que tiene como control el qubit $|c_2\rangle$, con notación $V^{(c_2,t)}$. Por ultimo tenemos que para un operador unitario, el operador inverso es el hermítico conjugado $V^{-1} = V^\dagger$, con lo que llegamos finalmente a la ecuación

$$U^{(c_1c_2,t)}|c_1\rangle|c_2\rangle|t\rangle = V^{(c_1,t)}{U_{CN}}^{(c_1,c_2)}{V^\dagger}^{(c_2,t)}{U_{CN}}^{(c_1,c_2)}V^{(c_2,t)}|c_1\rangle|c_2\rangle|t\rangle. \tag{10}$$

Esta ecuación nos da la descomposición de una compuerta con dos qubits de control U como el producto de compuertas con un qubit de control V, tal que $V^2 = U$, y compuertas CNOT.

.2 Compuertas que actúan sobre un solo qubit como reflexiones de Householder

Sea un operador unitario $U^{(0)}$ que actúa sobre un sistema de n qubits, tal que realiza la transformación

$$U^{(0)}|0j_1j_2...j_{n-1}\rangle = [u_0|0\rangle + u_1|1\rangle]|j_1j_2...j_{n-1}\rangle, \tag{11}$$

$$U^{(0)}|1j_1j_2...j_{n-1}\rangle = [u_1{}^*|0\rangle - u_0{}^*|1\rangle]|j_1j_2...j_{n-1}\rangle. \tag{12}$$

El operador $U^{(0)}$ altera solo el primer qubit.

Para encontrar la representación de esta compuerta como el producto de reflexiones de Householder utilizamos el algoritmo descrito en la sección 6.2. A modo simplificar la ecuaciones, etiquetaremos los estados de base con la notación de los números naturales tal que

$$|0\rangle \equiv |000...00\rangle \ , \ |1\rangle \equiv |000...01\rangle \ , \ |2\rangle \equiv |000...10\rangle \ ... \ |2^n - 1\rangle \equiv |111...11\rangle. \tag{13}$$

Primero intercambiamos el vector $|\mathbb{I}_{0,1}\rangle$ por el vector $|0\rangle$,

$$[r^{(0)}]_1|\mathbb{I}_{0,1}\rangle = \frac{\langle 0|\mathbb{I}_{0,1}\rangle}{|\langle 0|\mathbb{I}_{0,1}\rangle|}\langle \mathbb{I}_{0,1}|\mathbb{I}_{0,1}\rangle^{1/2}|0\rangle, \tag{14}$$

con

$$\begin{aligned} |\mathbb{I}_{0,1}\rangle &= [|0\rangle\langle 0| + |1\rangle\langle 1|]|U_0\rangle \\ &= [|0\rangle\langle 0| + |1\rangle\langle 1|][u_0|0\rangle + u_1|2^{n-1}\rangle] \\ &= u_0|0\rangle. \end{aligned} \tag{15}$$

Como los vectores $|\mathbb{I}_{0,1}\rangle$ y $|0\rangle$ son paralelos, el operador de reflexión será igual

a la identidad,

$$[r^{(0)}]_1 = \mathbb{I}. \tag{16}$$

acorde a la sección 6.1.3. Ahora intercambiamos los vectores $|\mathbb{I}_{0,2}\rangle$ y $|0\rangle$,

$$[r^{(0)}]_2|\mathbb{I}_{0,2}\rangle = \frac{\langle 0|\mathbb{I}_{0,2}\rangle}{|\langle 0|\mathbb{I}_{0,2}\rangle|}\langle \mathbb{I}_{0,2}|\mathbb{I}_{0,2}\rangle^{1/2}|0\rangle, \tag{17}$$

donde

$$\begin{aligned} |\mathbb{I}_{0,2}\rangle &= [|0\rangle\langle 0| + |2\rangle\langle 2|][r^{(0)}]_1|U_0\rangle \\ &= [|0\rangle\langle 0| + |2\rangle\langle 2|][u_0|0\rangle + u_1|2^{n-1}\rangle] \\ &= u_0|0\rangle. \end{aligned} \tag{18}$$

De nuevo tenemos que los vectores $|\mathbb{I}_{0,2}\rangle$ y $|0\rangle$ son paralelos, por lo que

$$[r^{(0)}]_2 = \mathbb{I}. \tag{19}$$

Esto se repite al intercambiar el vector $|0\rangle$ con los vectores $|\mathbb{I}_{0,3}\rangle$, $|\mathbb{I}_{0,4}\rangle$, ... , $|\mathbb{I}_{0,2^{n-1}-1}\rangle$. Al intercambiar los vectores $|0\rangle$ y $|\mathbb{I}_{0,2^{n-1}}\rangle$,

$$[r^{(0)}]_{2^{n-1}}|\mathbb{I}_{0,2^{n-1}}\rangle = \frac{\langle 0|\mathbb{I}_{0,2^{n-1}}\rangle}{|\langle 0|\mathbb{I}_{0,2^{n-1}}\rangle|}\langle \mathbb{I}_{0,2^{n-1}}|\mathbb{I}_{0,2^{n-1}}\rangle^{1/2}|0\rangle, \tag{20}$$

tendremos que el vector

$$\begin{aligned} |\mathbb{I}_{0,2^{n-1}}\rangle &= [|0\rangle\langle 0| + |2^{n-1}\rangle\langle 2^{n-1}|][r^{(0)}]_{2^{n-1}-1}[r^{(0)}]_{2^{n-1}-2}\cdots[r^{(0)}]_2[r^{(0)}]_1|U_0\rangle \\ &= [|0\rangle\langle 0| + |2^{n-1}\rangle\langle 2^{n-1}|][u_0|0\rangle + u_1|2^{n-1}\rangle] \\ &= u_0|0\rangle + u_1|2^{n-1}\rangle, \end{aligned} \tag{21}$$

no es paralelo al vector $|0\rangle$. En este caso el operador de reflexión, dada la

ecuación (6.5), será

$$[r^{(0)}]_{2^{n-1}} = \mathbb{I} - 2\frac{|r^{(0)}_{2^{n-1}}\rangle\langle r^{(0)}_{2^{n-1}}|}{\langle r^{(0)}_{2^{n-1}}|r^{(0)}_{2^{n-1}}\rangle}, \tag{22}$$

donde el vector $|r^{(0)}_{2^{n-1}}\rangle$ está dado como

$$\begin{aligned} |r^{(0)}_{2^{n-1}}\rangle &= \frac{\langle \mathbb{I}_{0,2^{n-1}}|0\rangle}{|\langle \mathbb{I}_{0,2^{n-1}}|0\rangle|}|\mathbb{I}_{0,2^{n-1}}\rangle - \langle \mathbb{I}_{0,2^{n-1}}|\mathbb{I}_{0,2^{n-1}}\rangle^{1/2}|0\rangle \\ &= \frac{{u_0}^*}{|u_0|}[u_0|0\rangle + u_1|2^{n-1}\rangle] - |0\rangle \\ &= (|u_0| - 1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|2^{n-1}\rangle \\ &= [(|u_0| - 1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|1\rangle]|000...00\rangle. \end{aligned} \tag{23}$$

Realizamos ahora el intercambio de los vectores $|\mathbb{I}_{1,i\neq 1}\rangle$ con el vector $|1\rangle$. Al proceder de igual forma que en el caso de los operadores $[r^{(0)}]_j$, obtenemos que todos los operadores de reflexión son igual al operador identidad, excepto en el caso en que se realiza el intercambio

$$[r^{(1)}]|\mathbb{I}_{1,2^{n-1}+1}\rangle = \frac{\langle 1|\mathbb{I}_{1,2^{n-1}+1}\rangle}{|\langle 1|\mathbb{I}_{1,2^{n-1}+1}\rangle|}\langle \mathbb{I}_{1,2^{n-1}+1}|\mathbb{I}_{1,2^{n-1}+1}\rangle^{1/2}|1\rangle, \tag{24}$$

donde el vector $|\mathbb{I}_{1,2^{n-1}+1}\rangle$ está dado como

$$|\mathbb{I}_{1,2^{n-1}+1}\rangle = u_0|1\rangle + u_1|2^{n-1}+1\rangle. \tag{25}$$

El operador de reflexión estará dado en función del vector de reflexión $|r^{(1)}\rangle$,

similar a la ecuación (22),

$$\begin{aligned} |r^{(1)}\rangle &= \frac{\langle \mathbb{I}_{1,2^{n-1}+1}|1\rangle}{|\langle \mathbb{I}_{1,2^{n-1}+1}|1\rangle|}|\mathbb{I}_{1,2^{n-1}+1}\rangle - \langle \mathbb{I}_{1,2^{n-1}+1}|\mathbb{I}_{1,2^{n-1}+1}\rangle^{1/2}|1\rangle \\ &= (|u_0|-1)|1\rangle + \frac{{u_0}^* u_1}{|u_0|}|2^{n-1}+1\rangle \\ &= [(|u_0|-1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|1\rangle]|000...01\rangle. \end{aligned} \tag{26}$$

Continuando con el análisis para el resto de los vectores, tendremos que las únicas reflexiones que no son equivalentes al operador identidad ocurren cuando se realiza un intercambio de la forma

$$[r^{(k)}]|\mathbb{I}_{k,2^{n-1}+k}\rangle = \frac{\langle k|\mathbb{I}_{k,2^{n-1}+k}\rangle}{|\langle 1|\mathbb{I}_{1,2^{n-1}+k}\rangle|}\langle \mathbb{I}_{1,2^{n-1}+k}|\mathbb{I}_{1,2^{n-1}+k}\rangle^{1/2}|k\rangle, \tag{27}$$

donde el vector $|\mathbb{I}_{k,2^{n-1}+k}\rangle$ es

$$|\mathbb{I}_{k,2^{n-1}+k}\rangle = u_0|k\rangle + u_1|2^{n-1}+k\rangle. \tag{28}$$

El operador de reflexión $[r^{(k)}]$ estará dado por el vector de reflexión

$$\begin{aligned} |r^{(k)}\rangle &= (|u_0|-1)|k\rangle + \frac{{u_0}^* u_1}{|u_0|}|2^{n-1}+k\rangle \\ &= [(|u_0|-1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|1\rangle]|k_1k_2k_3...k_{2^n-2}k_{2^n-1}\rangle. \end{aligned} \tag{29}$$

Se observa que en todos los vectores de reflexión $|r^{(k)}\rangle$ podemos factorizar el término $(|u_0|-1)|0\rangle + \frac{{u_0}^* u_1}{|u_0|}|1\rangle$ que es igual al vector de reflexión para operadores que actúan sobre un qubit. Podemos afirmar que para operadores que actúan sobre un número arbitrario de qubits, afectando solo uno de ellos, las reflexiones de Householder en las que se descompone este operador están dadas en función de vectores de reflexión factorizables en el qubit sobre el cual actúa el operador.

Referencias

[1] Claude Cohen-Tannoudji, Bernard Diu and Frank Laloe, *Quantum Mechanics*. Vol. 1, Wiley, 1977. 3

[2] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 5, 6, 46

[3] Sheldon Axler, *Linear Algebra Done Right*. Second Edition Springer, 1997. 31

[4] Gilbert Strang, *Introduction to Linear Algebra*. Third Edition Welleslely-Cambridge Press, 2003. 32

[5] H. Haffner and C.F. Roos and R. Blatt, (2008), *Quantum computing with trapped ions*. Physics Reports, **469**, 155-203. 2, 10

[6] H. Azuma, (2008) *Quantum computation with Kerr-nonlinear photonic crystals*. J. Phys. D: Appl. Phys., **41**. 2

[7] V. W. Scarola, K. Park and S. Das Sarma, (2005), *Pseudo-spin quantum computation in semiconductor nanostructures*. New Journal of Physics, **7**. 2

[8] M. Wallquist, J. Lantz, V. S. Shumeiko and G. Wendin, (2005), *Superconducting qubit network with controllable nearest-neighbour coupling*. New Journal of Physics, **7**. 2

[9] C. Ospelkaus, U. Warring, Y. Colombe, K. R. Brown, J. M. Amini, D. Leibfried and D. J. Wineland, (2011), *Microwave quantum logic gates for trapped ions*. Nature, **476**, 181-185. 2

[10] A. Blais, J. Gambetta, A. Wallraff, D. I. Schuster, S. M. Girvin, M. H. Devoret and R. J. Schoelkopf, (2007), *Quantum-information processing with circuit quantum electrodynamics*. Phys. Rev. A, **75**. 2, 10

[11] J. Shu, X. Zou, Y. Xiao and G. Guo, (2007), *Quantum phase gate of photonic qubits in a cavity QED system*. Phys. Rev. A, **75**. 2, 78

[12] X. Hao and S. Zhu, (2007), *Quantum computation in semiconductor quantum dots of electron-spin asymmetric anisotropic exchange*. Phys. Rev. A, **76**. 2

[13] N. Timoney, V. Elman, S. Glaser, C. Weiss,1 M. Johanning, W. Neuhauser and Chr. Wunderlich, (2008), *Error-resistant single-qubit gates with trapped ions*. Phys. Rev. A, **77**. 2

[14] Q. Lin and B. He, (2009), *Single-photon logic gates using minimal resources*. Phys. Rev. A, **80**. 2

[15] L. F. Wei, Y. Liu and F. Nori, (2005), *Quantum computation with Josephson qubits using a current-biased information bus*. Phys. Rev. B, **71**. 2, 10

[16] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin and H. Weinfurteri, (1995), *Elementary gates for quantum computation*. Phys. Rev. A, **52**, 34573467. 10

[17] R. Ozeri, (2011), *The trapped-ion qubit tool box*. Contemporary Physics, **52**, 531550. 10

[18] P. B. M. Sousa and R. V. Ramos, (2007), *Universal quantum circuit for N-qubit quantum gate: a programmable quantum gate*. Quantum Information and Computation, **7**, 228-242. 10

[19] D. Maslov, G. W. Dueck and D. M. Miller, (2005), *Toffoli Network Synthesis With Templates*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, **24**, 807 - 817. 10

[20] V. V. Shende, S. S. Bullock and I. L. Markov, (2006), *Synthesis of Quantum Logic Circuits*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, **24**, 1000 - 1010. 10

[21] M. Plesch and C. Brukner, (2011), *Quantum-state preparation with universal gate decompositions*. Phys. Rev. A, **83**. 10

[22] S. Felloni and G. Strini, (2009), *Entanglement-based Quantum Computing by Diagrams of States*. International Journal of Mathematical and Computer Sciences, **5**. 20

[23] A. Fedorov, L. Steffen, M. Baur, M. P. da Silva and A. Wallraff, (2012), *Implementation of a Toffoli gate with superconducting circuits*. Nature, **481**, 170 - 172. 53

[24] M. Borrelli, L. Mazzola, M. Paternostro, and S. Maniscalco, (2011), *Simple trapped-ion architecture for high-fidelity Toffoli gates*. Phys. Rev. A, **84**. 53

[25] T. Monz, K. Kim, W. Hansel, M. Riebe, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich and R. Blatt, (2009), *Realization of the Quantum Toffoli Gate with Trapped Ions*. Phys. Rev. Lett., **102**. 53

[26] J. Urías, (2010), *Householder factorizations of unitary matrices*. Journal of Mathematical Physics, **51**. 55, 61

[27] Ch. Yang and S. Hans, (2006), *Realization of an n-qubit controlled-U gate with superconducting quantum interference devices or atoms in cavity QED*. Phys. Rev. A, **73**. 78

[28] X. Zou, K. Li and G. Guo, (2006), *Linear optical scheme for direct implementation of a nondestructive N-qubit controlled phase gate*. Phys. Rev. A, **74**. 78

[29] Y. Xiao, X. Zou and G. Guo, (2007), *One-step implementation of an N-qubit controlled-phase gate with neutral atoms trapped in an optical cavity*. Phys. Rev. A, **75**. 2, 78

[30] Z. J. Deng, X. L. Zhang, H. Wei, K. L. Gao and M. Feng, (2007), *Implementation of a nonlocal N-qubit conditional phase gate by single-photon interference*. Phys. Rev. A, **76**. 78

[31] K. N. Patel, I. L. Markov and J. P. Hayes, (2008), *Optimal synthesis of linear reversible circuits*. Quantum Information and Computation, **8**, 282294. 79, 83

[32] D. Maslov, G. W. Dueck, D. M. Miller, and C. Negrevergne, (2008), *Quantum Circuit Simplification and Level Compaction*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, **27**, 436 - 444. 79, 83

[33] I. Tsai and S. Kuo, (2006), *An algorithm for minimun space quantum Boolean circuits construction*. Journal of Circuits, Systems, and Computers, **15**, 719738. 79, 83