Universidad de Oviedo

Facultad de Ciencias

Trabajo Fin de Grado en Matemáticas

Computación Cuántica Basada en Medidas

Autor: Nacho Tuñón Rubio

Tutores: Elías Fernández-Combarro Álvarez

Ignacio Fernández Rúa

Curso 2023-2024

Índice general

1. Preliminares Matemáticos **9**

1.1. Espacios de Hilbert 9

1.2. Álgebra Lineal 11

1.3. Mecánica Cuántica 13

2. Modelo Cuántico de Circuitos **19**

2.1. Introducción 19

2.2. Esfera de Bloch 22

2.3. Puertas Cuánticas de un Qubit 23

2.4. Puertas Cuánticas de dos Qubits 30

2.5. Universalidad de las Puertas Cuánticas 35

2.6. Puertas Cuánticas de N qubits 36

2.7. Modelo Cuántico de Circuitos 38

2.8. Algoritmos Cuánticos 42

3. Measurement Based Quantum Computing **47**

3.1. Teleportación Cuántica 47

3.2. Measurement Based Quantum Computing 51

3.3. Algoritmos Cuánticos en MBQC 65

4. Universalidad del modelo MBQC **69**

4.1. Equivalencia del Modelo MBQC con el Modelo de Circuitos 69

4.2. Estado Brickwork 70
4.3. Observaciones acerca de la Universalidad del Estado Brickwork 78
4.4. Universalidad de un Estado Clúster 79
4.5. Transformada de Fourier Cuántica 81

5. Blind Quantum Computing **85**
5.1. Protocolo de BQC 85

Introducción

La computación cuántica es un área de investigación científica en la que se concentran grandes esfuerzos por las implicaciones que supondría llegar a implementarla. La computación cuántica hace uso de propiedades exclusivas del mundo cuántico como son la **superposición**, el **entrelazamiento** o la **teleportación**. La integración de estas propiedades cuánticas no es en vano, sino que permite alcanzar la conocida como **supremacía cuántica** con respecto a los ordenadores clásicos. Este término hace referencia al potencial de la computación cuántica para resolver ciertos problemas en un tiempo mucho menor que la computación clásica. Por ejemplo, no se conocen algoritmos eficientes en computación clásica para la factorización de números enteros lo suficientemente grandes. De hecho, sistemas de encriptación como el sistema RSA se basan en la dificultad de factorizar el producto de dos números primos grandes. La computación cuántica propone una solución eficiente a este problema mediante el algoritmo de Shor, lo que implicaría la necesidad de buscar alternativas criptográficas a sistemas basados en la factorización de números primos [1].

Qubits

En electrónica digital, los elementos básicos de los circuitos son los bits, la unidad mínima de información. Es un sistema binario que se basa en el álgebra de Boole. En computación cuántica, aparecen los qubits. La diferencia esencial es que un qubit se puede hallar en una superposición de estados. De esta manera, mientras que n bits contienen n unidades de información, n qubits pueden contener 2^n estados en superposición.

Por la naturaleza probabilística de la mecánica cuántica, el resultado de medir un qubit no es determinista, por lo que podría ser necesario implementar múltiples veces un algoritmo para hallar una respuesta correcta. Esto no supone un obstáculo cuando este tipo de algoritmos son eficientes.

Computación Cuántica

Para llegar a implementar ordenadores cuánticos, es necesario desde un punto de vista teórico tener en cuenta distintos enfoques.

Por un lado, se requieren conocimientos de ingeniería y física para diseñar dispositivos o sistemas físicos que actúen como qubits. La dificultad de crear un ordenador cuántico reside en la capacidad de escalar e integrar cientos de qubits en un dispositivo conjunto. Cada qubit no es un sistema aislado, sino que se ve afectado por las variaciones en su entorno. Para crear un sistema de dimensión 2^n, los n qubits han de ser entrelazados, y además han de poder ser medidos individualmente. Físicamente supone un reto aislar los qubits del ruido de manipular o medir cada qubit vecino [2].

Se han creado qubits basándose en distintos fenómenos físicos [3]. Los qubits superconductores como el transmón son actualmente los más estudiados, pero también se ha investigado el uso de fotones, átomos, o fermiones para crear este tipo de dispositivos.

Por otro lado, es necesario el desarrollo de modelos matemáticos que sienten los fundamentos para crear algoritmos. Esta es la parte matemática de la investigación, y es en la descripción de dos modelos alternativos en lo que basará este trabajo. El **objetivo** es explorar y comparar el modelo cuántico de circuitos y el modelo MBQC (*Measurement Based Quantum Computing*) basado en medidas.

Modelo Cuántico de Circuitos y Modelo MBQC

En toda operación de computación se requieren tres componentes: los datos, las operaciones y los resultados. En la Figura 1 se muestra un esquema de una operación computacional.

Figura 1: Representación esquemática de toda operación computacional.

En computación clásica, se emplean puertas lógicas para realizar operaciones sobre los bits. Existen puertas universales como NAND a partir de las cuales es posible construir cualquier otra operación.

El modelo cuántico de circuitos es el modelo cuántico análogo al de puertas lógicas clásicas. En el modelo de circuitos, los datos son representados por los estados de los qubits, las operaciones por puertas cuánticas y los resultados por mediciones de los qubits. Al hacer una observación del estado de un qubit, la función de onda colapsará a uno de los estados de la base en la que se realiza. Esta medición es de naturaleza probabilística tal y como se postula en mecánica cuántica.

Por otro lado, estas mediciones, junto con el entrelazamiento, son la base del modelo MBQC. Si se conoce el resultado de una medición de un qubit, se puede inducir el estado de un qubit que fue entrelazado previamente. Así, modificando y regulando las bases de cada medición, se puede obtener el resultado esperado.

El objetivo de este trabajo es exponer los dos modelos y llegar a probar que son equivalentes a la hora de computar. Es decir, cualquier operación que se realice mediante puertas cuánticas puede ser implementada a partir de mediciones, y viceversa.

Por último, se expone una aplicación del modelo MBQC a blind quantum computing, o computación cuántica ciega. Es un protocolo para proteger la privacidad de usuarios que, a través de la nube, empleen los servidores de proveedores de ordenadores cuánticos. Es razonable pensar que el número de ordenadores cuánticos será limitado, sobre todo en los comienzos, restringiendo el acceso universal a ellos. Este protocolo permitiría garantizar la privacidad de quienes empleen los recursos de un tercero.

Estructura del trabajo

El trabajo se compone de 5 capítulos, además de uno de conclusiones:

- El capítulo 1 presenta los fundamentos teóricos que se aplican durante el resto del trabajo como recordatorio. Incluye conceptos de álgebra lineal, análisis funcional y mecánica cuántica. No es indipensable su lectura para seguir el hilo del trabajo, por lo que es posible comenzar directamente la lectura por el capítulo 2.
- El capítulo 2 expone el modelo cuántico de circuitos: la definición de un qubit, las puertas cuánticas, y el funcionamiento del modelo, además de algunos algoritmos cuánticos como el de Deutsch Jozsa o la Transformada Cuántica de Fourier.
- El capítulo 3 presenta el modelo MBQC. Se incluye una versión del algoritmo de Deutsch Jozsa a partir del modelo MBQC.

- En el capítulo 4 se prueba la universalidad del modelo MBQC, es decir, la equivalencia entre los dos modelos.
- Por último, el capítulo 5 expone una aplicación del modelo MBQC a la conocida como computación cuántica ciega, donde se incluye un protocolo de computación basada en medidas que asegura la privacidad de computaciones en servidores externos.

Capítulo 1

Preliminares Matemáticos

Es importante tener en cuenta los fundamentos teóricos en los que se basan los modelos de computación cuántica. Durante este trabajo, se supone cierta familiaridad con el álgebra lineal, pero se exponen definiciones y resultados como recordatorio de conceptos menos comunes. Por ello no se incluyen demostraciones de los resultados. Para el lector que no conoce la mecánica cuántica, se exponen también sus postulados y la notación de Dirac.

Para profundizar o recordar los conceptos aquí expuestos, además de encontrar las demostraciones, se remite a [4] para álgebra lineal, [5] para análisis funcional y [6] para mecánica cuántica.

1.1. Espacios de Hilbert

Definición 1.1 (Espacio pre-Hilbert)**.** *Un espacio pre-Hilbert es un $\mathbb{K}$-espacio vectorial V junto con un producto escalar $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{K}$ que satisface las siguientes propiedades:*

- *Es positivo y real para $u \in V$:* $\langle u, u \rangle \geq 0 \quad y \quad \langle u, u \rangle = 0 \iff u = 0 \quad \forall u \in V$.
- *Es lineal en su primer argumento:*

$$\langle au + bv, w \rangle = a\langle u, w \rangle + b\langle v, w \rangle \qquad \forall u, v, w \in V \quad a, b \in \mathbb{K}.$$

- *Si se intercambian los argumentos es igual al original conjugado:*

$$\langle u, v \rangle = \overline{\langle v, u \rangle} \qquad \forall u, v \in V.$$

Proposición 1.1. *Todo espacio de pre-Hilbert es un espacio normado con la norma* $\|x\|_2 = \sqrt{\langle x, x\rangle}$.

En ese caso se dice que la norma proviene de un producto escalar.

Definición 1.2 (Espacio de Banach)**.** *Un espacio normado* $(V, \|\cdot\|)$ *se dice de Banach si toda sucesión de Cauchy contenida en él es convergente.*

La completitud es una propiedad esencial de los espacios de Hilbert.

Definición 1.3 (Espacio de Hilbert)**.** *Un espacio pre-Hilbert se dice de Hilbert si el espacio normado que induce el producto escalar es de Banach.*

Es importante también el concepto de espacio dual:

Definición 1.4 (Espacio Dual)**.** *Dado un espacio de Hilbert* $\mathcal{H}$*, el espacio dual de* $\mathcal{H}$ *está compuesto por todos los operadores lineales y continuos* $f : \mathcal{H} \longrightarrow \mathbb{K}$ *y se denota* $\mathcal{L}(\mathcal{H}, \mathbb{K})$ *o* $\mathcal{H}'$*.*

Definición 1.5. *Dado* $\mathcal{H}$ *un espacio de Hilbert y* $u \in \mathcal{H}$*, se define:*

$$\begin{aligned} u^* \colon \mathcal{H} &\longrightarrow \mathbb{K} \\ v &\longmapsto \langle v, u\rangle \end{aligned}$$

Teorema 1.1 (Teorema de Riesz)**.** *Sea* $\mathcal{H}$ *un espacio de Hilbert y* $f : \mathcal{H} \longrightarrow \mathbb{K}$ *lineal y continua, es decir,* $f \in \mathcal{L}(\mathcal{H}, \mathbb{K})$*. Entonces existe un único vector* $u \in \mathcal{H}$ *tal que* $f(x) = \langle x, u\rangle = u^*(x)$ *para todo* $x \in \mathcal{H}$*.*

Existe por tanto una correspondecia entre un espacio de Hilbert $\mathcal{H}$ y su dual $\mathcal{H}'$:

$$\begin{aligned} \varphi \colon \mathcal{H} &\longrightarrow \mathcal{H}' \\ u &\longmapsto u^* \end{aligned}$$

Esta relación será importante a la hora de definir la notación de Dirac empleada en mecánica cuántica.

Nota 1.1. *La noción de espacio dual se puede extender a espacios vectoriales [4].*

Teorema 1.2 (Clasificación de los Espacios de Hilbert de dimensión finita)**.** *Si* $\dim \mathcal{H} = n$*, H es linealmente isométrico a* $\ell_2^n = \mathbb{K}^n$ *con el isomorfismo isométrico*

$$\begin{aligned} \mathcal{T} \colon \mathcal{H} &\longrightarrow \ell_2^n \\ x &\longmapsto (\langle x, u_k\rangle)_{k=1}^n \end{aligned}$$

donde $\{u_1, \ldots, u_n\}$ *es una base ortonormal de* $\mathcal{H}$.

Se tienen en cuenta únicamente espacios de dimensión finita puesto que el número de qubits en este trabajo será finito.

1.2. Álgebra Lineal

En sistemas de qubits, cuyos estados están representados por vectores de un espacio $\mathcal{H}$, las puertas cuánticas serán endomorfismos $A\colon \mathcal{H} \longrightarrow \mathcal{H}$. En lo que sigue, se usa indistintamente la notación A para hacer referencia a un endormorfismo o a la matriz coordenada asociada a ese endormorfismo en una base ortonormal fijada.

Matrices Hermíticas

Las matrices hermíticas son fundamentales en mecánica cuántica ya que se postula que todo observable (propiedad física) es hermítico. En operaciones con qubits, no se trabaja siempre con observables físicos, pero es necesario comprender el concepto para tener mayor entendimiento de la mecánica cuántica.

Definición 1.6 (Aplicación Dual)**.** *Sea* H *un* $\mathbb{K}$*-espacio vectorial y* $A \in End(\mathcal{H})$*. La aplicación dual de* A*, denotada por* A' *es:*

$$\begin{aligned} A'\colon \mathcal{H}' &\longrightarrow \mathcal{H}' \\ w &\longmapsto w \circ A \end{aligned}$$

Definición 1.7 (Aplicación Adjunta)**.** *Sea* V *un* $\mathbb{K}$*-espacio vectorial con un producto escalar* $\langle \cdot, \cdot \rangle$*. Para un endomorfismo* $A : V \to V$*, la aplicación adjunta de* A*, denotada por* A^**, se define como el único endomorfismo tal que para todo* $v, w \in V$*,*

$$\langle Av, w \rangle = \langle v, A^* w \rangle.$$

Se puede ver que $A^* = \varphi^{-1} \circ A' \circ \varphi$, con φ la correspondencia entre un espacio vectorial y su dual. En la Figura 1.1 se muestra un diagrama conmutativo de esta relación.

Proposición 1.2. *En el caso complejo, dado* $\mathcal{H}$ *un* $\mathbb{C}$*-espacio de Hilbert, la aplicación autoadjunta de un endomorfismo* A *de* $\mathcal{H}$ *es* $A^* = \bar{A}^t$*, es decir, la matriz traspuesta conjugada de* A*.*

Definición 1.8 (Aplicación Autoadjunta)**.** *Sea V un $\mathbb{K}$-espacio vectorial con un producto escalar $\langle \cdot, \cdot \rangle$. Un endomorfismo $A : V \to V$ se dice que es autoadjunto si su aplicación adjunta coincide con sí mismo, es decir, $A^* = A$.*

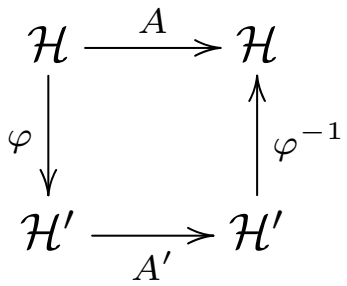


Figura 1.1: Diagrama conmutativo que relaciona el operador A con su dual A' mediante la biyección φ entre $\mathcal{H}$ y su dual $\mathcal{H}'$. Si se cumple que $A = \varphi^{-1} \circ A' \circ \varphi$, A es autoadjunta o hermítica.

Proposición 1.3 (Matriz Hermítica)**.** *En el caso $\mathbb{K} = \mathbb{C}$, A es autoadjunta si y solo si $A = A^* = \bar{A}^t$. En ese caso, A se dice hermítica.*

Teorema 1.3. *Sea $\mathcal{H}$ un $\mathbb{C}$-espacio vectorial y $A \colon \mathcal{H} \longrightarrow \mathcal{H}$ hermítica. Son ciertas las siguientes afirmaciones:*

1. *Existe una base de vectores propios de A ortonormal.*
2. *Los valores propios de A son reales.*

Matrices Unitarias

Definición 1.9. *Sea $\mathcal{H}$ un $\mathbb{C}$-espacio vectorial dotado de un producto escalar $\langle \cdot, \cdot \rangle$. Sea $f : \mathcal{H} \to \mathcal{H}$. f se dice unitaria si*

$$\langle f(u), f(v) \rangle = \langle u, v \rangle$$

Proposición 1.4. *Sea $\mathcal{H}$ un $\mathbb{C}$-espacio vectorial dotado de un producto escalar $\langle \cdot, \cdot \rangle$. Sea $f : \mathcal{H} \to \mathcal{H}$ unitaria. Entonces:*

1. *$||f(u)|| = ||u||$ para todo $u \in \mathcal{H}$.*
2. *u y v son ortogonales si y solo $f(u)$ y $f(v)$ también son ortogonales con $u, v \in \mathcal{H}$.*

3. *f es biyectiva.*

4. *Si k es un valor propio de f, entonces $|k| = 1$.*

5. *Dados dos vectores propios de f con valores propios distintos, los vectores son ortogonales.*

Proposición 1.5. *$A \in End(\mathcal{H})$ define un endomorfismo unitario si y solo si $A^*A = AA^* = \mathbb{I}$. En ese caso la matriz se llama unitaria.*

Proposición 1.6. *$A \in End(\mathcal{H})$ es un endomorfismo unitario si y solo si $||Ax|| = ||x||$ para todo $x \in \mathcal{H}$.*

Proposición 1.7. *Las aplicaciones unitarias de un $\mathbb{C}$-espacio vectorial $\mathcal{H}$ dotado de un producto escalar $\langle \cdot, \cdot \rangle$ forman un grupo llamado grupo unitario $U(n)$ con la operación de composición, donde n es la dimensión de $\mathcal{H}$.*

1.3. Mecánica Cuántica

Notación de Dirac

En mecánica cuántica, es habitual utilizar la notación bra-ket de Dirac. Se trabaja con $\mathbb{C}$-espacios de Hilbert $(\mathcal{H}, \langle \cdot, \cdot \rangle)$, de forma que cada vector se denomina **ket** y se escribe $|\psi\rangle$, donde ψ hace referencia a cada vector.

Definición 1.10. *Un ket $|\psi\rangle$ es un vector en un $\mathbb{C}$-espacio de Hilbert.*

Por el Teorema 1.1, a cada ket $|\psi\rangle$ le corresponde un elemento en el dual $\mathcal{L}(\mathcal{H}, \mathbb{K})$. Ese operador se denomina **bra** y se expresa $\langle\psi|$.

Definición 1.11. *Un bra $\langle\psi|$ asociado a un ket $|\psi\rangle$ es un operador del espacio dual:*

$$\begin{aligned} \langle\psi| : \mathcal{H} &\longrightarrow \mathbb{K} \\ |\rho\rangle &\longmapsto \langle\psi|\rho\rangle = \langle |\psi\rangle, |\rho\rangle \rangle \end{aligned}$$

Nota 1.2. *Pese al orden de los argumentos, el Teorema 1.1 se puede aplicar en este caso.*

Se puede definir también la siguiente operación:

$$\begin{aligned} |\phi\rangle\langle\psi| : \mathcal{H} &\longrightarrow \mathcal{H} \\ |\rho\rangle &\longmapsto |\phi\rangle\langle\psi|\rho\rangle \end{aligned}$$

donde finalmente se tiene un ket $|\phi\rangle$ multiplicado por un escalar $\langle\psi|\rho\rangle$, que es una operación bien definida en espacios vectoriales.

Espacios de Hilbert de N qubits

En mecánica cuántica, no siempre se tienen espacios de Hilbert de dimensión finita. La posición es un ejemplo de magnitud continua. Sin embargo, al trabajar con qubits se utilizan $\mathbb{C}$-espacios de Hilbert $\mathcal{H}$ de dimensión finita $n = 2^N$, siendo N el número de qubits en el sistema. Por el Teorema 1.2, $\mathcal{H} \cong \mathbb{C}^n$.

Por el Postulado 1.4 de la Mecánica Cuántica, se ha de tener en cuenta que un estado válido es aquel de norma 1, por lo que $\mathbb{C}^n$ se restringe a $\mathbb{C}^n|_{S_{\mathbb{C}^n}}$, donde:

$$S_{\mathbb{C}^n} = \{x \in \mathbb{C}^n \colon \|x\|_2 = 1\}$$

con $n \in \mathbb{N}$. A este conjunto se le llama también esfera de radio 1. Es un conjunto cerrado de $\mathbb{C}^n$, lo cual implica que toda sucesión convergente en $S_{\mathbb{C}^n}$ converge a un punto de $S_{\mathbb{C}^n}$.

Nota 1.3. *La condición de que los estados de un qubit o un sistema de qubits tengan norma 1 se llama condición de normalización. Si no se impone, sí que se tiene un isomorfismo con $\mathbb{C}^n$. Sin embargo, dejarían de representar estados de un qubit. Es por esta razón que a veces se habla de isomorfismo con $\mathbb{C}^n$, mientras que los vectores que representan estados reales habitan en la esfera de radio 1. Se sobreentiende entonces que el isomorfismo se restringe a $\mathbb{C}^n|_{S_{\mathbb{C}^n}}$.*

El producto escalar en estos casos se escoge de forma que $(\mathcal{H}, \langle\cdot,\cdot\rangle) \cong (\mathbb{C}^n, \langle\cdot,\cdot\rangle_{\mathbb{C}^n})$, siendo $\langle\cdot,\cdot\rangle_{\mathbb{C}^n}$ el producto escalar usual en $\mathbb{C}^n$ definido por:

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i^* y_i \quad x, y \in \mathbb{C}^n.$$

Para ello, se define el operador $\mathcal{T}$ lineal y continuo:

$$\begin{aligned} \mathcal{T} \colon \mathcal{H} &\longrightarrow \mathbb{C}^n|_{S_{\mathbb{C}^n}} \\ |\psi_i\rangle &\longmapsto e_i \end{aligned}$$

con $\{|\psi_i\rangle\}_{i=1}^n$ una base ortonormal en $\mathcal{H}$ y $\{e_i\}_{i=1}^n$ la base canónica en $\mathbb{C}^n$.

Así, se asocia cada ket a un vector columna x y el bra $x^\dagger$ correspondiente a un vector fila que es el vector adjunto de x. Por tanto, la operación $|\phi\rangle\langle\psi|$ es una operación

lineal que se puede expresar como una matriz de tamaño $n \times n$.

Nota 1.4. *La norma inducida por el producto escalar usual se denota* $\|\cdot\|_2$.

Al trabajar con sistemas de más de 1 qubit ($N > 1$), es necesario definir el producto tensorial.

Definición 1.12. *Sean dos espacios de Hilbert* $\mathcal{H}_n$ *de dimensión* n *y* $\mathcal{H}_m$ *de dimensión* m*. Se define el producto tensorial* $\otimes$ *como:*

$$\begin{aligned} \otimes \colon \mathcal{H}_n \times \mathcal{H}_m &\longrightarrow \mathcal{H}_{n\times m} \\ (a, b) &\longmapsto a \otimes b \end{aligned}$$

siendo

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \\ a_2 \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \\ \vdots \\ a_n \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \end{pmatrix}$$

donde $\mathcal{H}_{n\times m}$ *hace referencia al* $\mathbb{C}$*-espacio de Hilbert de dimensión* $n \times m$ *(restringido a la esfera de radio 1).*

Se extiende el concepto para operadores de la siguiente manera:

$$\begin{aligned} \otimes \colon \mathcal{L}(\mathcal{H}_n, \mathcal{H}_n) \times \mathcal{L}(\mathcal{H}_m, \mathcal{H}_m) &\longrightarrow \mathcal{L}(\mathcal{H}_{n\times m}, \mathcal{H}_{n\times m}) \\ (A, B) &\longmapsto A \otimes B \end{aligned}$$

siendo

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}.$$

En el caso de sistemas de N qubits (dimensión finita), se puede extender de forma natural el producto tensorial para admitir un número n finito de entradas ($a_1 \otimes a_2 \cdots \otimes a_n$), teniendo en cuenta la siguiente propiedad:

Proposición 1.8. *El producto tensorial $\otimes$ es asociativo.*

Sin embargo, este operador no es exhaustivo, es decir, existen vectores en $\mathcal{H}_{n\times m}$ y operadores en $\mathcal{L}(\mathcal{H}_{n\times m}, \mathcal{H}_{n\times m})$ que no se construyen a partir del producto tensorial de elementos de espacios de menor dimensión. Nacen así los conceptos de **estados producto** y **estados entrelazados**. Se definen a continuación, y se expondrán los ejemplos a la hora de llevarlo a la práctica más adelante. Son conceptos fundamentales para la computación cuántica. El entrelazamiento es un fenómeno característico de la mecánica cuántica.

Definición 1.13 (Estado producto)**.** *Dado un espacio de Hilbert de dimensión $n > 1$, un ket $|\psi\rangle$ se dice estado producto si existen $|\psi_1\rangle$ y $|\psi_2\rangle$ tal que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.*

Definición 1.14 (Estado entrelazado)**.** *Dado un espacio de Hilbert de dimensión $n > 1$, un ket $|\psi\rangle$ es un estado entrelazado si no es un estado producto.*

A continuación, se prueba un resultado útil para trabajar con bases de espacios de mayor dimensión a partir de bases de espacios de menor dimensión. Es común en computación cuántica trabajar con la base canónica, también llamada **base computacional**.

Proposición 1.9. *Sean dos espacios de Hilbert $\mathbb{C}^n$ de dimensión n con base canónica $\{e_i^n\}_{i=1}^n$ y $\mathbb{C}_n$ de dimensión m con base canónica $\{e_j^m\}_{j=1}^m$. Entonces $\{e_i^n \otimes e_j^m\}$ con $i = 1, ..., n$ y $j = 1, ..., m$ es la base canónica de $\mathbb{C}^{n\times m}$.*

Demostración. Fijados $i = 1, ..., n$ y $j = 1, ..., m$, se ve que

$$e_i^n \otimes e_j^m = e_{m(i-1)+j}^{nm}$$

donde $e_{m(i-1)+j}^{nm}$ hace referencia al vector columna nulo excepto en la componente $m(i-1)+j$. □

Por último, se expresa una propiedad para trabajar con productos tensoriales en notación de Dirac.

Proposición 1.10. *Sean $\{\mathcal{H}_i\}_{i=1}^n$ espacios de Hilbert, $\{|\psi_i\rangle\}_{i=1}^n$ kets en $\mathcal{H}_i$ respectivamente y $\{\langle\phi_i|\}_{i=1}^n$ bras en el dual $\mathcal{H}_i'$. Se cumple que*

$$(\langle\phi_1| \otimes \cdots \otimes \langle\phi_n|)(|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle) = \langle\phi_1|\psi_1\rangle \ldots \langle\phi_n|\psi_n\rangle \,.$$

Postulados de la Mecánica Cuántica

La mecánica cuántica es una teoría física que surge para describir la mecánica de sistemas atómicos y subatómicos, al comprobar que la mecánica clásica no explicaba ciertos fenómenos como la radiación de cuerpo negro o el efecto fotoeléctrico. Los postulados que rigen la mecánica cuántica son los siguientes:

Postulado 1.1. *El estado cuántico de un sistema físico se describe por un vector de estado $|\psi\rangle$ en un espacio de Hilbert.*

Postulado 1.2. *A cualquier observable físico le corresponde un operador A hermítico.*

En mecánica cuántica, la operación $\langle bra| A |ket\rangle$ está relacionada con la probabilidad de medir $\langle bra|$ al observar A en el estado $|ket\rangle$. Sin embargo, es importante que esta operación sea simétrica, así $\langle bra| A$ es el bra que corresponde a $A|ket\rangle$ [6]. Esto se consigue si A es hermítico:

$$\langle\psi| A^* |\rho\rangle = \langle\rho| A |\psi\rangle^*$$

Postulado 1.3. *La medición de un observable cuántico da como resultado uno de los valores propios a_i del operador A asociado al observable.*

De esta forma, por el Teorema 1.3, se tiene que los valores propios de A son reales.

Postulado 1.4. *Cuando se mide un observable cuántico asociado con un operador A, la probabilidad de obtener el valor propio a_i es dada por*

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

donde $|\psi\rangle$ es el estado cuántico del sistema y $|a_i\rangle$ es el estado propio correspondiente a a_i.

La mecánica cuántica es de naturaleza probabilística, al contrario que la mecánica clásica, que es determinista. Esto significa que, en mecánica cuántica, al repetir un experimento en idénticas condiciones se puede obtener un resultado distinto al original.

Postulado 1.5. *Cuando se realiza una medición en un sistema cuántico y se obtiene el valor propio a_i de un observable, el estado cuántico $|\psi\rangle$ colapsa instantáneamente a la proyección normalizada del estado original en el estado de la medición, es decir, a*

$$|\psi'\rangle = \frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}},$$

donde P_i es el operador de proyección ortogonal del subespacio fundamental de vectores propios de a_i.

Postulado 1.6. *La evolución temporal de un sistema cuántico está gobernada por el Hamiltoniano $H(t)$ mediante la ecuación de Schrödinger, que corresponde a la expresión*

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle ,$$

con $\hbar = \frac{h}{2\pi}$, siendo h la constante de Planck.

Nota 1.5. *El Hamiltoniano H es el operador que corresponde al observable energía en un sistema cuántico.*

Capítulo 2

Modelo Cuántico de Circuitos

En este capítulo se formaliza el concepto de qubit y se expone el modelo cuántico de circuitos. Para ello se introducen las puertas cuánticas, y se dan ejemplos de circuitos cuánticos. Se incluyen también ejemplos de algoritmos cuánticos.

2.1. Introducción

Un qubit es la unidad mínima de información en computación cuántica. A diferencia de un bit clásico, un qubit puede estar en superposición de dos estados denominados $|0\rangle$ y $|1\rangle$.

Definición 2.1. *Un qubit es un sistema cuántico que es superposición de dos estados propios:* $|0\rangle$ *y* $|1\rangle$*. Su estado puede expresarse de forma genérica como* $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$*, con* $a, b \in \mathbb{C}$ *tal que* $|a|^2 + |b|^2 = 1$*.*

Los estados $|0\rangle$ y $|1\rangle$ son ortonormales, lo que implica que $\langle i|j\rangle = \delta_{i,j}$ con $i, j = \{0, 1\}$.

En la sección 1.3, se vio que un sistema de N qubits forma un espacio de Hilbert de dimensión finita $n = 2^N$, que se identifica con $\mathbb{C}^n|_{S_{\mathbb{C}^n}}$ con el producto escalar usual.

Nota 2.1. *Se recuerda que el isomorfismo es en realidad con* $\mathbb{C}^n$*, pero cada vector en* $\mathbb{C}^n$ *se normaliza para que represente el estado de un qubit.*

Nota 2.2. *En adelante, para simplificar notación, se denota* $\mathcal{H}$ *al espacio de Hilbert de dimensión dos de los estados de un qubit. Cuando se trabaje con más qubits se especificará la notación empleada.*

Los estados $|0\rangle$ y $|1\rangle$ forman una base ortonormal de $\mathcal{H}$ por construcción. Dicha base se llama base computacional. La ortogonalidad se da por definición.

Nota 2.3. *Es importante destacar que la condición* $|a|^2+|b|^2=1$ *se llama condición de normalización, y significa que, dado* A *un observable con vectores propios* $\{a_i\}_{i=1}^n$*, la suma de las probabilidades de los posibles sucesos verifica* $\sum_{i=1}^n \mathcal{P}(a_i)=1$*. En otras palabras, la norma de un qubit* $|\psi\rangle$ *es igual a 1.*

Por el Teorema 1.2, es posible asociar

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

y trabajar con notación matricial. Tanto la notación matricial como la notación de Dirac son equivalentes en este caso. Por tanto, se tienen las siguientes igualdades:

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

En notación matricial, se tienen las siguientes igualdades:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \qquad \langle\phi| = c^*\,\langle 0| + d^*\,\langle 1| = \begin{pmatrix} c^* & d^* \end{pmatrix}$$

$$\langle\phi|\psi\rangle = (c^*\,\langle 0| + d^*\,\langle 1|)(a\,|0\rangle + b\,|1\rangle) = \begin{pmatrix} c^* & d^* \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = c^*a + d^*b$$

En las igualdades previas se supone que $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$.

Toma de mediciones

En cada proceso computacional, se involucran tres elementos: los datos, las operaciones y los resultados. En el contexto del modelo de circuitos cuánticos, los datos son los estados de los qubits, las operaciones son puertas cuánticas, y los resultados son las mediciones. Al realizar una observación del estado de un qubit, la función de onda colapsará a uno de los estados fundamentales de la base en la que se efectúa dicha medición. Es importante destacar que esta medición tiene un carácter probabilístico, conforme a los postulados de la mecánica cuántica.

Dado un qubit en un estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, se ha visto que

$$\mathcal{P}_0 = |\langle 0|\psi\rangle|^2 = |a|^2$$

$$\mathcal{P}_1 = |\langle 1|\psi\rangle|^2 = |b|^2$$

donde $\mathcal{P}_0$ y $\mathcal{P}_1$ son la probabilidad de obtener los valores propios asociados a $|0\rangle$ y $|1\rangle$ respectivamente. Se puede extender el cálculo para n qubits.

Proposición 2.1. *Dado* $|\psi\rangle = \sum_{j=1}^{n} c_j |a_j\rangle$, $\mathcal{P}(a_i) = |c_i|^2$, *siendo* a_i *el valor propio asociado a* a_i.

Demostración. La probabilidad se escribe tal que:

$$\mathcal{P}(a_i) = |\langle a_i|\psi\rangle|^2$$

Por un lado, se tiene que:

$$\langle a_i|\psi\rangle = \sum_{j=1}^{n} c_j \langle a_i|a_j\rangle = c_i$$

por lo que:

$$\mathcal{P}(a_i) = |c_i|^2$$

□

De este hecho se deduce que la probabilidad de encontrar cada valor propio dependerá exclusivamente de la diferencia de fase relativa entre los coeficientes c_i. Se define a continuación una fase global y se prueba que es físicamente irrelevante.

Definición 2.2 (Fase Global)**.** *Se considera una fase global a una constante* $c \in \mathbb{C}$ *con* $|c| = 1$ *que multiplica al estado del qubit.*

Proposición 2.2. *Una fase global es físicamente irrelevante, es decir, no afecta a las probabilidades de obtener cada valor propio. En lenguaje matemático, dado* $|\psi\rangle = \sum_{j=1}^{n} c_j |a_j\rangle$ *y* $c \in \mathbb{C}$ *con* $|c| = 1$, $\mathcal{P}(a_i)$ *es igual para* $|\psi\rangle$ *que para* $c|\psi\rangle$.

Demostración. Para $|\psi\rangle$:

$$\mathcal{P}(a_i) = |c_i|^2$$

Para $c|\psi\rangle$:

$$\mathcal{P}(a_i) = |\langle a_i|c|\psi\rangle|^2 = |c|^2|\langle a_i|\psi\rangle|^2 = |c|^2|c_i|^2 = |c_i|^2$$

□

2.2. Esfera de Bloch

En esta sección se expone el concepto de esfera de Bloch, una forma gráfica de visualizar el estado de un solo qubit.

Proposición 2.3. *Un qubit $|\psi\rangle$ se puede expresar de la siguiente manera en coordenadas esféricas:*

$$|\Psi\rangle = cos(\theta/2)\,|0\rangle + sen(\theta/2)e^{i\phi}\,|1\rangle$$

de forma que solo se han de especificar los ángulos polar $\theta \in [0, \pi]$ y azimutal $\phi \in [0, 2\pi]$ para cada estado.

Demostración. Sea $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Un estado queda descrito por dos números complejos a y b, o equivalentenmente, cuatro números reales. Sin embargo, debido a que solo la diferencia relativa de fases entre a y b determina la probabilidad de obtener cada valor propio a la hora de realizar una observación (Proposición 2.2), los grados de libertad se reducen a tres, de forma que $a = r_a$ y $b = r_b e^{i\phi}$, $r_a, r_b \in R^+, \phi \in [0, 2\pi]$. De esta manera, y sin pérdida de generalidad, se supone que a es real para simplificar los cálculos.

A continuación se impone la condición de normalización, es decir, $\|\psi\|^2 = \langle\psi|\psi\rangle = 1$, por lo que se llega a que $\langle\psi|\psi\rangle = (a^*\,\langle 0| + b^*\,\langle 1|)(a\,|0\rangle + b\,|1\rangle) = a^*a + b^*b = |a|^2 + |b|^2 = 1$. En coordenadas cartesianas esta expresión se convierte en $r_a^2 + r_b^2$.

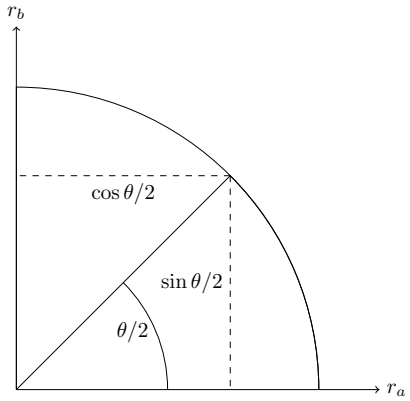


Figura 2.1: Arco de circunferencia de radio 1 con ejes r_a y r_b.

Se define por conveniencia $\theta/2$ como en la Figura 2.1, de tal forma que $\theta \in [0, \pi]$. Así, por trigonometría, $cos(\theta/2) = r_a$ y $sen(\theta/2) = r_b$ y el qubit queda descrito por $|\Psi\rangle = cos(\theta/2)\,|0\rangle + sen(\theta/2)e^{i\phi}\,|1\rangle$. □

Así, el estado $|0\rangle$ corresponde con $\theta = 0$, es decir, el polo norte de la esfera. El estado

$|1\rangle$ corresponde con el ángulo $\theta = \pi$, es decir, el polo sur. Los dos estados aparecen representados en la esfera de Bloch en la Figura 2.2.

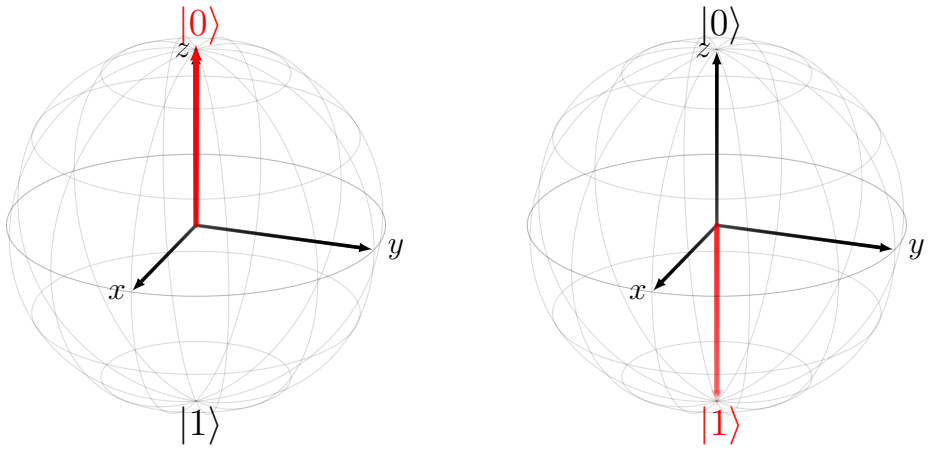


Figura 2.2: Representación en la esfera de Bloch de los estados $|0\rangle$ (izquierda) y $|1\rangle$ (derecha).

Esta representación resulta efectiva para visualizar un qubit, pero resulta menos adecuada para la representación de sistemas compuestos por múltiples qubits que se encuentran entrelazados.

2.3. Puertas Cuánticas de un Qubit

Existen distintos modelos matemáticos de computación cuántica. Entre ellos, el modelo de circuitos es el más conocido y empleado. Este modelo se basa en secuencias de operaciones lógicas llamadas puertas cuánticas, que se unen formando un circuito. Al igual que en ordenadores clásicos, son necesarias las puertas lógicas para realizar operaciones, construir circuitos y así implementar algoritmos. Es decir, una puerta cuántica cambia el estado de los qubits.

Puertas Lógicas Cuánticas

Las puertas lógicas cuánticas son el equivalente a las puertas lógicas de los ordenadores clásicos digitales. En el contexto de los qubits, es necesario que sean definidas como endomorfismos del espacio de Hilbert. Esto significa que si se aplica una puerta a un qubit en un estado $|\psi_0\rangle$, necesariamente se ha de obtener un qubit en otro estado $|\psi_1\rangle$.

Se ha visto que un qubit habita en un espacio de Hilbert que se identifica con $\mathcal{H} = \{w \in \mathbb{C}^2 \colon \|w\|_2 = 1\} \subset \mathbb{C}^2$. Es por tanto necesario que, dado $A \colon \mathcal{H} \longrightarrow \mathbb{C}^2$, $\|Ax\|_2 = 1$ para todo $x \in \mathcal{H}$. Dicho de otra forma, el operador ha de conservar la norma.

Se concluye, por la Proposición 1.6, que A ha de ser unitaria. Las puertas cuánticas no son observables físicos, sino que describen la evolución del sistema de qubits.

Gracias a la representación de la esfera de Bloch, se puede interpretar cada puerta cuántica de un qubit como una aplicación que a cada punto de una esfera le asigna otro punto en la esfera.

Operaciones sobre un Qubit

A continuación, se introducen las puertas cuánticas más importantes, empezando por aquellas que actúan sobre uno y dos qubits y posteriormente generalizando a un sistema de N qubits. Sin embargo, se verá que para cualquier operación unitaria, se puede construir un circuito equivalente empleando únicamente puertas de uno y dos qubits. De esta forma se extiende el concepto de universalidad a la computación cuántica.

El caso más sencillo es la puerta I o identidad. Para construir puertas más complejas, se ha de tener en cuenta que los autovalores asociados a los vectores de la base computacional son de módulo 1 al tratarse de una matriz unitaria.

Así, la **puerta $\boldsymbol{Z}$** se escribe

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

Su acción sobre los estados de la base computacional es

$$Z\,|0\rangle = |0\rangle\,, \qquad\qquad Z\,|1\rangle = -\,|1\rangle\,.$$

Otro ejemplo muy importante es la **puerta $\boldsymbol{X}$** o puerta NOT, dada por

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

.

Su acción sobre los estados de la base computacional es

$$X\left|0\right\rangle = \left|1\right\rangle, \qquad X\left|1\right\rangle = \left|0\right\rangle.$$

Esta puerta niega cada estado, de forma equivalente a la puerta NOT clásica.

La **puerta Hadamard *H*** sirve para crear una superposición entre los estados de la base, y viene dada por

$$H = \frac{X+Z}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Su acción sobre los estados de la base computacional es la siguiente:

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) = \left|+\right\rangle,$$
$$H\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) = \left|-\right\rangle,$$

de forma que el nuevo estado se encuentra en superposición de $|0\rangle$ y $|1\rangle$. Se han definido dos nuevos estados $|+\rangle$ y $|-\rangle$. Estos dos estados forman una base. En la Figura 2.3 se representan estos dos estados en la esfera de Bloch.

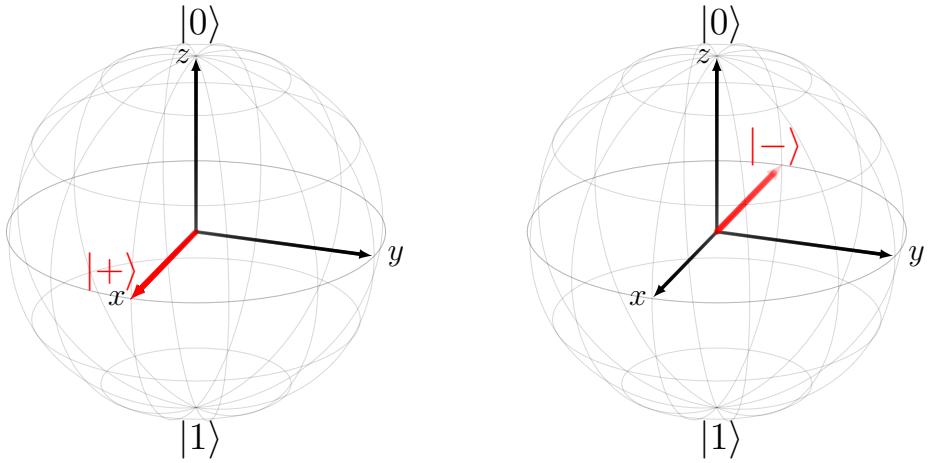


Figura 2.3: Representación en la esfera de Bloch de los estados $|+\rangle$ y $|-\rangle$.

La **puerta $\boldsymbol{Y}$** se escribe

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

e induce un cambio de fase con respecto de la puerta NOT.

El nombre de las puertas X, Y y Z coinciden con los nombres de los ejes cartesianos. Esta notación no es arbitraria, sino que se da debido a que cada puerta es una rotación de π radianes alrededor de su eje correspondiente en la esfera de Bloch. Esto implica que se pueden generalizar las tres puertas para que dependan de un ángulo θ, de la siguiente forma:

$$R_x(\theta) = e^{-i\frac{\theta}{2}X} = \cos\frac{\theta}{2}\mathbb{I} - i\sin\frac{\theta}{2}X = \begin{pmatrix} cos(\frac{\theta}{2}) & -isin(\frac{\theta}{2}) \\ -isin(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{pmatrix},$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\frac{\theta}{2}\mathbb{I} - i\sin\frac{\theta}{2}Y = \begin{pmatrix} cos(\frac{\theta}{2}) & -sin(\frac{\theta}{2}) \\ sin(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{pmatrix},$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\frac{\theta}{2}\mathbb{I} - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix},$$

donde $\equiv$ indica que son equivalentes salvo una fase global.

Se recuperan las puertas X, Y, Z si se sustituye θ por π en cada puerta respectivamente. Son importantes también los casos donde $\theta = \pi/2$ y $\theta = \pi/4$ alrededor del eje Z. Se obtienen así la **puerta $\boldsymbol{S}$**, dada por

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix},$$

y la **puerta $\boldsymbol{T}$**, definida por

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

En la Figura 2.4, se encuentra una tabla resumiendo las expresiones matriciales de las puertas cuánticas de un qubit más empleadas.

Es también importante conocer las relaciones entre las puertas cuánticas a la hora

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Figura 2.4: Puertas cuánticas de un qubit más comunes.

de operar. Por ejemplo, la puerta Hadamard intercambia los ejes x y z. Por tanto, si se aplica dos veces, se deduce que esa acción es similar a no aplicar ninguna puerta. Se puede ver operando matricialmente.

Equivalencia. $H^2 = I$

Las matrices de Pauli son un conjunto de matrices destacado tanto en computación cuántica como en física cuántica.

Definición 2.3. *El conjunto* $\{I, X, Y, Z\}$ *se le conoce como matrices de Pauli y forman una base del espacio vectorial* $\mathcal{M}_{2\times 2}(\mathbb{C})$ *de las matrices* 2×2.

En el caso de las matrices de Pauli, puesto que son rotaciones de π radianes alrededor de un eje, ocurre lo mismo que en el caso de la puerta Hadamard. Puesto que rotar 2π radianes es lo mismo que no rotar, se deduce que aplicar dos veces seguidas una matriz de Pauli es equivalente a no aplicar ninguna puerta. Se puede comprobar mediante el producto matricial que son ciertas las siguientes equivalencias:

Equivalencia. $X^2 = Y^2 = Z^2 = I$

además de las relaciones entre ellas:

Equivalencia.

$$ZX = iY = -XZ$$

Es necesario para este trabajo definir bases alternativas a la computacional. En este caso, se ve que dos vectores antipodales en el plano ecuatorial de la esfera de Bloch forman una base de $\mathcal{H}$.

Los estados $|+\rangle_\alpha$ y $|-\rangle_\alpha$ forman una base ortonormal de $\mathcal{H}$ siendo

$$|+\rangle_\alpha = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle),$$
$$|-\rangle_\alpha = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle),$$

con $\alpha \in [0, 2\pi]$.

Equivalencias entre Puertas Cuánticas de un Qubit

Para cerrar la sección de puertas cuánticas de un qubit, es importante destacar distintas equivalencias que son útiles a la hora de simplificar los cálculos de las operaciones unitarias.

Equivalencia. *Sea $\theta \in [0, 2\pi]$. Entonces se cumple $HR_x(\theta)H = R_z(\theta)$*

Demostración. Se sigue del hecho de que

$$HR_x(\theta)H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}cos(\frac{\theta}{2}) & -isin(\frac{\theta}{2})\\ -isin(\frac{\theta}{2}) & cos(\frac{\theta}{2})\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}e^{-i\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{pmatrix} = R_z(\theta).$$

□

Es común ver este resultado cuando $\theta = 0$, en cuyo caso

$$HXH = Z. \tag{2.1}$$

Se puede obtener otra equivalencia basándose en este resultado previo.

Equivalencia. *Sea $\theta \in [0, 2\pi]$. Entonces se cumple que*

$$R_z(\theta)X = XR_z(-\theta).$$

Demostración. Se tiene que

$$XR_x(\theta)X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}e^{-i\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}e^{i\frac{\theta}{2}} & 0\\ 0 & e^{-i\frac{\theta}{2}}\end{pmatrix} = R_z(-\theta),$$

de donde se obtiene el resultado multiplicando por X a la izquierda. □

Con estas equivalencias se demuestra el siguiente resultado, útil para secciones posteriores.

Proposición 2.4. *Sea $m = \{0, 1\}$. Entonces $HR_z(\theta)X^mH = Z^mR_x((-1)^m\theta)$.*

Demostración.

- Si $m = 0$, es la ecuación vista anteriormente

$$HR_z(\theta)H = R_x(\theta).$$

- Si $m = 1$, se parte de

$$R_z(\theta)X = XR_z(-\theta).$$

Se multiplica por H a ambos lados

$$HR_z(\theta)XH = HXR_z(-\theta)H.$$

Se concluye, por las equivalencias previas que

$$HR_z(\theta)XH = HXHR_x(-\theta)H^2,$$
$$HR_z(\theta)XH = ZR_x(-\theta).$$

□

Universalidad en Puertas de un Qubit

Por último, es importante recalcar que, a la hora de llevar a la práctica la computación, se priorizan las puertas universales, ya que abaratan los costes. En el caso de puertas cuánticas, se da el siguiente resultado:

Proposición 2.5. *Para toda puerta cuántica de un qubit U, existen tres ángulos α, β, γ de forma que $U \equiv R_z(\alpha)R_y(\beta)R_z(\gamma)$. Este resultado también es cierto para todo par de ejes de rotación no paralelos.*

De la Proposición 2.5, se puede derivar la siguiente descomposición de una puerta unitaria U cualquiera.

Proposición 2.6 (Descomposición de U unitaria)**.** *Sea U puerta cuántica de un qubit, por tanto, una matriz unitaria 2×2. Entonces existen A, B, C matrices unitarias 2×2 tal que $ABC = I$ y una fase $\theta \in [0, 2\pi]$ tal que*

$$U = e^{i\theta} AXBXC.$$

Es posible describir una puerta universal en función de tres ángulos. De hecho, empresas como IBM las usan en sus ordenadores cuánticos. La **puerta universal** $\boldsymbol{U}$ depende de tres ángulos y se escribe como

$$U(\theta, \varphi, \lambda) = \begin{pmatrix} cos(\frac{\theta}{2}) & -e^{i\lambda} sin(\frac{\theta}{2}) \\ e^{i\varphi} sin(\frac{\theta}{2}) & e^{i(\varphi+\lambda)} cos(\frac{\theta}{2}) \end{pmatrix}.$$

La universalidad hace refencia a que esta puerta engloba cualquier puerta cuántica de un qubit.

2.4. Puertas Cuánticas de dos Qubits

En la sección 1.3, se expusieron los fundamentos teóricos para trabajar con sistemas de más de un qubit ($N > 1$). Se estableció un isomorfismo con $\mathbb{C}^n$ con el producto escalar usual $\langle \cdot, \cdot \rangle_{\mathbb{C}^n}$ y se definió el producto tensorial, además de la distinción entre estados producto y estados entrelazados.

Para el caso de $N = 2$, se trabaja con un espacio de Hilbert de dimensión $n = 2^2 = 4$. A partir de la Proposición 1.9 para el caso concreto $n = m = 2$, se obtiene una nueva base, dada por

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

Estos vectores o kets son ejemplos de estados producto, ya que se construyeron a partir de qubits individuales. A continuación se muestra un ejemplo de estado de dos qubits entrelazado.

Nota 2.4. *Se usa la notación $|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$ salvo que esta notación lleve a*

confusión. En ese caso, se indicará.

Ejemplo 2.1. *Uno de los ejemplos más simples de un estado entrelazado de dos qubits es el estado de Bell* $|\Psi^+\rangle$*, que se define como*

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Para ver que el estado de Bell es un estado entrelazado se prueba que no es un estado producto. Se supone, por reducción al absurdo, que $|\Psi^+\rangle$ *se puede expresar como un producto tensorial de dos estados, en la forma*

$$\left|\Psi^+\right\rangle = (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle\,,$$

siendo $a, b, c, d \in \mathbb{C}$*.*

Igualando las ecuaciones, se deduce que $ad = 0$ *y que* $bc = 0$*. Así, si se emplea la segunda igualdad, se tiene que* $b = 0$ *o* $c = 0$*. En cualquier caso se halla una contradicción puesto que no se puede obtener* $|\Psi^+\rangle$ *bajo estas condiciones. Se prueba así que* $|\Psi^+\rangle$ *no es un estado producto y sí es un estado entrelazado.*

Es importante observar que en este estado $|\Psi^+\rangle$*, si se realiza una medición en uno de los qubits y se obtiene, por ejemplo, el valor propio de* $|0\rangle$*, inmediatamente se conoce que el otro qubit también colapsará en el estado* $|0\rangle$*, independientemente de la distancia física entre ellos. Esto fue motivo de controversia en la física, ya que la información viaja como máximo a la velocidad de la luz.*

El concepto de colapsar tras realizar una medición se expone más adelante en la Proposición 2.7.

Existen otros tres estados de Bell que forman una base del espacio de Hilbert de dos qubits. Son los siguientes:

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Al trabajar con dos qubits, al medir uno el otro colapsará a un nuevo estado ket $|\psi\rangle$

de un qubit.

Proposición 2.7. *Sea* $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ *un estado genérico de dos qubits.*

- *Si al medir el primer qubit se obtiene* $|0\rangle$*, el sistema colapsa al estado*

$$|\psi_0\rangle = \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}.$$

- *Si se mide* $|1\rangle$ *en el primer qubit, el estado pasará a ser*

$$|\psi_1\rangle = \frac{a_{10}|10\rangle + a_{11}|11\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}}.$$

El resultado es análogo si se mide el segundo qubit, solo cambian los estados de la base.

Los qubits entrelazados permiten conocer el estado del segundo qubit tras medir el primero. En términos de computación cuántica, la propiedad de entrelazamiento de estados cuánticos es una de las más importantes a la hora de construir circuitos que implementen algoritmos. Se aprovecha el hecho de que se conocen los posibles estados en los que colapsará la función de onda tras haber realizado una medición. Esta propiedad es básica en el modelo basado en medidas.

De forma análoga a los kets producto y entrelazados, existen puertas cuánticas que se pueden escribir a partir de las puertas de un qubit y otras que no. Para un estado producto, aquellas puertas que se descomponen en puertas de un qubit actúan de forma individual en cada qubit, de acuerdo a

$$(U_1 \otimes U_2)(|\psi_1\psi_2\rangle) = U_1|\psi_1\rangle \otimes U_2|\psi_2\rangle.$$

Sin embargo, al igual que con estados entrelazados, existen matrices unitarias de dimensión 4 con coeficientes en $\mathbb{C}$ que no pueden ser descompuestas en productos tensoriales. Estas matrices son puertas cuánticas que actúan de forma conjunta sobre todos los qubits del sistema.

La **puerta *SWAP*** es un ejemplo de puerta cuántica de dos qubits.

$$SWAP = \frac{I \otimes I + X \otimes X + Y \otimes Y + Z \otimes Z}{2}.$$

Su expresión matricial es

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

y su acción sobre los estados de la base computacional es:

$$SWAP\,|00\rangle = |00\rangle\,, \quad SWAP\,|01\rangle = |10\rangle\,, \quad SWAP\,|10\rangle = |01\rangle\,, \quad SWAP\,|11\rangle = |11\rangle\,.$$

La puerta SWAP intercambia el estado de los dos qubits. Si el primero está en $|0\rangle$ o $|1\rangle$, lleva $|0\rangle$ o $|1\rangle$ al segundo qubit. Ocurre lo mismo para el segundo qubit.

Otro ejemplo de puertas destacable son las **puertas de control** o **controladas**. En ellas, un qubit sirve como controlador, y en el otro se aplica U si el primer qubit se halla en el estado $|1\rangle$.

En su forma más general, una **puerta controlada *CU*** con el primer qubit de control es:

$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix},$$

donde

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

es una puerta cuántica de un qubit.

Esta puerta aplica la puerta U al segundo qubit si el estado del primer qubit es $|1\rangle$, del siguiente modo:

$$CU\,|00\rangle = |00\rangle\,, \quad CU\,|01\rangle = |01\rangle\,, \quad CU\,|10\rangle = |1\rangle\,U\,|0\rangle\,, \quad CU\,|11\rangle = |1\rangle\,U\,|1\rangle\,.$$

Los casos concretos más comunes y más importantes son cuando $U = X$ y $U = Z$. Cuando $U = X$, se conocen como la **puerta *CNOT*** o **puerta *CX***. Su expresión

matricial es

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

Su acción sobre los estados de la base computacional es invertir el estado del segundo qubit si el del primero es $|1\rangle$. En notación de Dirac, se tiene que:

$$CNOT\,|00\rangle = |00\rangle\,, \quad CNOT\,|01\rangle = |01\rangle\,, \quad CNOT\,|10\rangle = |11\rangle\,, \quad CNOT\,|11\rangle = |10\rangle\,.$$

La expresión matricial de la **puerta CZ** es

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

y su acción sobre los estados de la base computacional es:

$$CZ\,|00\rangle = |00\rangle\,, \quad CZ\,|01\rangle = |01\rangle\,, \quad CZ\,|10\rangle = |10\rangle\,, \quad CZ\,|11\rangle = -\,|11\rangle\,.$$

Si se analiza en detalle la acción de CZ, se ve que es independiente del qubit que sea el controlador ya que solo cambia el estado de $|11\rangle$. También se conoce esta puerta como puerta $CPhase$ o $CFase$.

Equivalencias en Puertas Cuánticas de dos Qubits

Una equivalencia importante es la siguiente.

Equivalencia. *Se cumple que:*

$$(I \otimes H)CZ(I \otimes H) = CNOT$$

Demostración. Se verifica que

$$(I \otimes H)CZ(I \otimes H) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} =$$

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

□

2.5. Universalidad de las Puertas Cuánticas

En computación clásica, existen puertas universales con las que es posible realizar cualquier otra operación. Esto es importante por distintos motivos, entre ellos económicos, ya que se reducen el número de puertas diferentes a implementar físicamente.

Es, por tanto, importante buscar puertas cuánticas universales. Si se pretende demostrar la equivalencia de dos modelos de computación cuántica, se podrá probar que se pueden llevar a cabo las puertas universales en lugar de probarlo para toda operación unitaria. En consecuencia se proponen a continuación distintos conjuntos que actúan como puertas universales para toda operación unitaria de cualquier dimensión finita.

En una dimensión, se vio en la Proposición 2.5 que cualquier puerta cuántica de un qubit se puede escribir usando R_z y R_y. Para dimensión n, se obtiene el siguiente resultado:

Teorema 2.1 (Universalidad de las Puertas de 1 y 2 Qubits)**.** *Cualquier operación unitaria de dimensión n se puede implementar con puertas de un qubit y la puerta CNOT. Es decir, se puede construir un circuito equivalente a cualquier operación unitaria empleando únicamente puertas de un qubit y la puerta CNOT.*

Por último, se propone un conjunto concreto de tres puertas que actúan como conjunto universal. Este conjunto será importante a la hora de probar la equivalencia de los dos modelos de computación cuántica considerados en este trabajo.

Proposición 2.8. *El conjunto de puertas $\{H, T, CNOT\}$ sirve para aproximar cualquier operación U unitaria hasta cualquier grado de precisión, en el sentido de que la norma de la diferencia tiende a 0 [12].*

La Proposición 2.8 indica que, dado un $\epsilon > 0$, existirá un circuito que, a partir de $\{H, T, CNOT\}$, implemente una operación unitaria U_ϵ tal que $||U - U_\epsilon|| < \epsilon$. Este conjunto no es único, sino que existen diferentes conjuntos que pueden servir como conjuntos universales.

2.6. Puertas Cuánticas de N qubits

Trabajar con sistemas de N qubits requiere extender de forma análoga los conceptos previos a un espacio de Hilbert de dimensión $2^N = n$. La base computacional se extiende de igual forma que para el caso $N = 2$. En este caso, no es cómodo trabajar con kets $|\psi_1\psi_2 \dots \psi_n\rangle$, sino que los estados de la base se nombran por el número decimal que corresponde al número binario $\psi_1\psi_2 \dots \psi_n$, donde el bit más significativo es, como se ha trabajado hasta ahora, ψ_1.

Nota 2.5. *Se recuerda que la notación para espacios de Hilbert de dimensión n que representen un sistema de qubits es $\mathcal{H}_n$, donde el subíndice se omite en caso de $n = 1$.*

De esta manera se obtiene una base

$$|0\rangle, |1\rangle, \dots |2^n - 1\rangle$$

que se asocia a la base canónica de $\mathbb{C}^n$ de forma que $e_i = |i - 1\rangle$ con $i = 1, ..., n$.

Ejemplo 2.2. *Para el caso $N = 2$, la base computacional se escribe con esta notación, de forma que*

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

$$|2\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |3\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Se extiende también la Proposición 2.7 para el caso de N qubits.

Proposición 2.9. *Sea $\sum_{i=1}^{n} = a_i |i\rangle$ un estado genérico de un sistema de N qubits en $\mathcal{H}_n$. Entonces:*

- *Si al medir el qubit j con $j = 1, ..., N$ se obtiene $|0\rangle$, el estado colapsa al estado*

$$\frac{\sum_{l \in J_0} a_l |l\rangle}{\sqrt{\sum_{l \in J_0} |a_l|^2}},$$

  con $J_0 = \{|\psi_1 \psi_2 \dots \psi_n\rangle \in \mathcal{H}_n \colon \psi_j = 0\}$. La probabilidad de medir $|0\rangle$ es

$$\sum_{l \in J_0} |a_l|^2$$

- *Si al medir el qubit j con $j = 1, ..., N$ se obtiene $|1\rangle$, el estado colapsa a*

$$\frac{\sum_{l \in J_1} a_l |l\rangle}{\sqrt{\sum_{l \in J_1} |a_l|^2}},$$

  con $J_1 = \{|\psi_1 \psi_2 \dots \psi_n\rangle \in \mathcal{H}_n \colon \psi_j = 1\}$. La probabilidad de medir $|1\rangle$ es

$$\sum_{l \in J_1} |a_l|^2$$

Antes de exponer distintas puertas comunes para $N > 2$, de forma similar a los casos $N = 1$ y $N = 2$, se recuerda el resultado el Teorema 2.1 de universalidad de las puertas de 1 y 2 qubits. Por tanto no es necesario exponer ningún ejemplo en concreto en esta introducción, ya que se las puertas de más de dos qubits se pueden implementar mediante un circuito que utilice solo puertas de 1 y 2 qubits.

Hay un caso en concreto de puerta que sí es importante para $N = 3$ y es el caso de la **puerta Toffoli** o ***CCNOT***. Es importante ya que $\{H, CCNOT\}$ es también un conjunto de puertas universales [12]. Sin embargo, no se empleará en este trabajo. De hecho se verá una descomposición de $CCNOT$ en función de $\{H, T, CNOT\}$.

La puerta Toffoli actúa sobre 3 qubits y transforma la base computacional de la siguiente forma:

$$CCNOT\,|x\rangle\,|y\rangle\,|z\rangle = |x\rangle\,|y\rangle\,|z \oplus (x \wedge y)\rangle$$

con $\oplus$ la función XOR clásica (suma mód 2) y $\wedge$ el símbolo de la función AND (producto de los dos bits). Se recuerdan las dos funciones clásicas:

$$XOR(0,0) = 0, \quad , XOR(0,1) = 1, \quad XOR(1,0) = 1, \quad XOR(1,1) = 0.$$

$$AND(0,0) = 0, \quad AND(0,1) = 0, \quad AND(1,0) = 0, \quad AND(1,1) = 1.$$

De forma más simple, la función $CCNOT$ aplica la puerta NOT al tercer qubit si los dos qubits controladores (el primero y el segundo) están en $|1\rangle$. Extiende la puerta $CNOT$ a un qubit más.

Antes de concluir, ha de tenerse en cuenta la siguiente aclaración sobre notación.

Nota 2.6. *En un sistema de N qubits, es común que se aplique una puerta a un qubit j con $j = 1, ..., N$ o a varios $j_1, ..., j_m$ con $m < N$, mientras que al resto de qubits no se le aplica ninguna puerta. En esos casos los subíndices de la puerta en concreto harán referencia a los qubits a los que se aplica. Por ejemplo, U_{12} es una puerta de dos qubits que se aplica al qubit 1 y al 2. Los primeros números hacen referencia a los controladores, en el caso de que existan más de uno. Así, $CNOT_{21}$ tiene el segundo qubit como controlador, mientras que $CNOT_{12}$ tiene el primer qubit como controlador.*

En lugar de escribir $(I \otimes ... \otimes U_{j_1...j_m} \otimes .... \otimes I)$, se escribe solo $U_{j_1...j_m}$. Se sobreentenderá que al resto de qubits no se le aplica ninguna puerta.

Como ejemplo, sea $N = 4$, sea CZ_{23} y $|\psi\rangle$ el estado del sistema. Se puede escribir, de forma equivalente, $CZ_{23}\,|\psi\rangle$ en lugar de $(I \otimes CZ_{23} \otimes I)\,|\psi\rangle$.

Si aparece CU cualquiera sin subíndices (como $CNOT$ o CZ) y el contexto deja dudas (existen más de dos qubits), siempre se entenderá que se refiere a CU_{12}.

Concluye así la exposición de las puertas cuánticas más importantes.

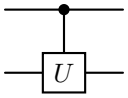
2.7. Modelo Cuántico de Circuitos

Ya se han expuesto los conceptos de qubits y de puertas cuánticas. Es decir, ya se han expuesto los dos componentes esenciales para la computación cuántica: los datos

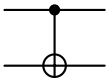
y las posibles operaciones que se pueden realizar sobre ellos. Es hora de concretar estos conceptos en un modelo que permita realizar cualquier operación unitaria sobre los qubits y computar algoritmos para obtener aplicaciones útiles en el mundo real. El modelo más estudiado y empleado es el modelo cuántico de circuitos [12].

Un circuito tiene los siguientes componentes:

- Cada qubit es representado por un **cable**.
- Cada puerta cuántica de 1 qubit se representa como una **caja** cuadrada con el nombre de la puerta correspondiente dentro. Los cables que atraviesa son los qubits a los cuales se aplica esa puerta en concreto.
- Las puertas controladas se representan como en el siguiente circuito, donde el punto del qubit superior significa que ese qubit es el controlador.

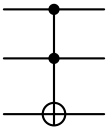


  Es común que la notación cambie para $CNOT$ y para CZ. En esos casos se representan de la siguiente manera respectivamente:

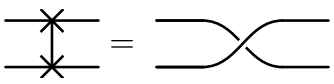


  La notación para CZ tiene sentido ya que CZ actúa de forma equivalente siendo cualquiera de los dos qubits el controlador.

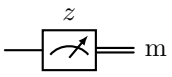
  La puerta $CCNOT$ se representa a partir se de la extensión de la puerta $CNOT$ a tres qubits, del siguiente modo:



  La puerta SWAP también tiene notación propia:



- Las mediciones se representan con el símbolo

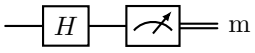


  donde z, o el eje que corresponda, hace referencia a la base con la respecto a la que se mide. z se refiere a la base computacional y x a la base $|\pm\rangle$. Si no aparece z, entonces la medición se hace en la base computacional. El resultado de la medición es m. El doble cable significa que es un cable clásico, ya que tras la medición el qubit ha colapsado a un bit clásico.

Estos son los elementos que forman un circuito. A continuación se verán ejemplos para ilustrar cómo se implementan al llevarlo a la práctica.

Ejemplos de Circuitos

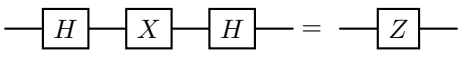
Ejemplo 2.3. *Un circuito básico que se puede construir consiste en implementar H y medir en la base computacional.*



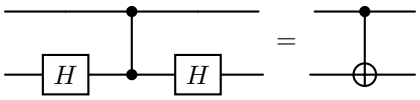
Si el estado inicial es $|0\rangle$, entonces $H|0\rangle = |+\rangle$, por lo que $\mathcal{P}_0 = 1/2$. Si el estado inicial es $|+\rangle$, entonces $H|+\rangle = |0\rangle$, por lo que $\mathcal{P}_0 = 1$.

Los siguientes ejemplos se exponen con doble finalidad: comprender la notación del modelo de circuitos y exponer algunas equivalencias entre puertas cuánticas que son útiles a la hora de computar.

Ejemplo 2.4. *La equivalencia de la Ecuación 2.1 escrita en circuitos es*

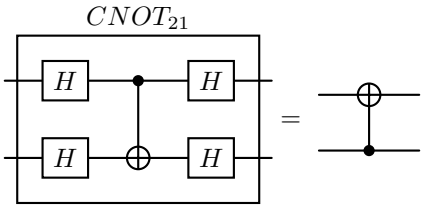


Ejemplo 2.5. *Como ya fue probado, $CNOT$ se puede escribir a partir de CZ y H de la siguiente forma:*

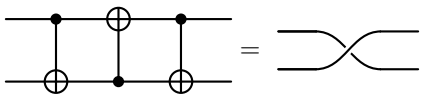


En este caso $(I \otimes H)$ se representa con una puerta H en el qubit inferior, ya que I es equivalente a no transformar el estado del qubit.

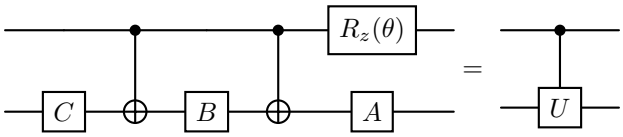
Ejemplo 2.6. *El siguiente circuito muestra la equivalencia para una puerta $CNOT_{21}$ con el segundo qubit como controlador. Se puede comprobar matricialmente que se da la igualdad.*



Ejemplo 2.7. *La puerta $SWAP$ es equivalente a usar tres puertas $CNOT$ dispuestas como en este ejemplo. Se puede comprobar matricialmente que se da la igualdad.*

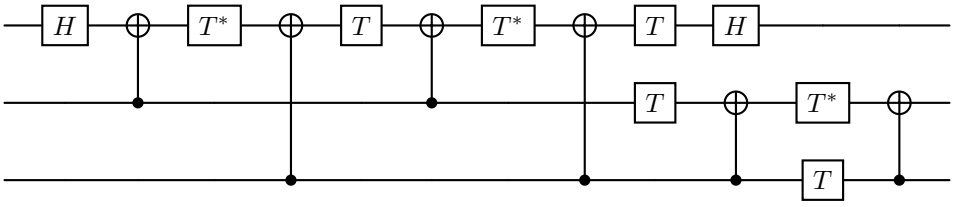


Ejemplo 2.8. *A partir de la Proposición 2.6, que hace referencia a una descomposición matricial de una matriz U unitaria, se deriva el siguiente circuito para una descomposición de una puerta controlada CU:*



con A, B, C tal que $ABC = I$ y $e^{i\theta} \in [0, 2\pi]$ de forma que $U = e^{i\theta}AXBXC$.

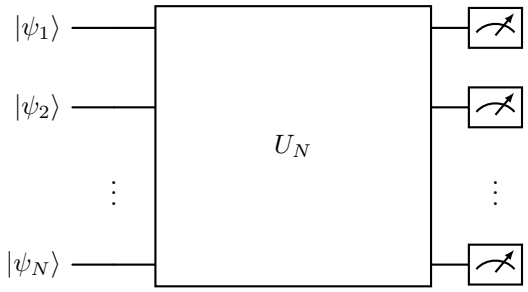
Ejemplo 2.9. *La puerta Toffoli se puede implementar a partir del conjunto de puertas universal $\{H, T, CNOT\}$. Una posible descomposición es [12]*



Pese a que T^* y $CNOT_{21}$ no pertenecen explícitamente a $\{H, T, CNOT\}$, sí se pueden formar a partir de ellas:

- *$T^* = T^{-1}$ por ser T unitaria. Como $T^8 = I$, entonces $T^* = T^{-1} = T^7$.*
- *Se ha visto una equivalencia de $CNOT_{21}$ a partir de $CNOT$ y H.*

Vistos estos ejemplos se ha ilustrado el modelo de circuitos. De forma genérica, un circuito de N qubits tiene la siguiente forma:



donde las mediciones no han de estar presentes necesariamente. Puesto que las matrices unitarias forman un grupo $U(N)$, se puede escribir el producto de todas como U_N. Así, se obtiene un circuito que implementa U_N sobre N qubits.

2.8. Algoritmos Cuánticos

Toda la teoría desarrollada acerca de la computación cuántica nace con el fin de fundamentar un área con aplicaciones en el mundo real. En esta sección se verá cómo se pueden implementar algoritmos cuánticos a partir del modelo de circuitos presentado. Para más información se remite a [1].

Algoritmo de Deutsch Jozsa

El algoritmo de Deutsch Jozsa es el ejemplo más fácil para comprender cómo un algoritmo cuántico supera con creces a su análogo clásico en términos de eficiencia computacional. Su punto débil es que no tiene aplicación real conocida, sino que sirve únicamente para ilustrar el poder de la computación cuántica.

El problema que se intenta resolver es el siguiente: Sea f una función definida en un conjunto de N bits tal que

$$\begin{aligned} f\colon \mathbb{Z}_2^N &\longrightarrow \mathbb{Z}_2 \\ x &\longmapsto f(x) \end{aligned}$$

donde $\mathbb{Z}_2 = \{0, 1\}$. f no es cualquier función, sino que se sabe que f pertenece a una de las dos opciones siguientes:

- f es constante, i.e., $f(x) = 0$ o $f(x) = 1$ para todo $x \in \mathbb{Z}_2^N$.

- f es balanceada, i.e., $f(x) = 0$ para la mitad de los elementos de $\mathbb{Z}_2^N$ y $f(x) = 1$ para la otra mitad.

El objetivo del algoritmo es determinar el tipo de la función f, es decir, si es balanceada o constante.

Un algoritmo clásico evaluaría distintos valores de la función hasta encontrar dos distintos (función balanceada) o, en el peor de los casos, $2^{n-1}+1$ valores, es decir, la mitad más 1. Esto corresponde a que la función fuese constante, o que la función fuese balanceada y se obtuviesen un único valor de f para los primeros 2^{n-1} elementos.

La eficiencia del algoritmo cuántico es evidente ya que este resuelve el problema en una sola evaluación. El circuito para dimensión n se representa en la Figura 2.5.

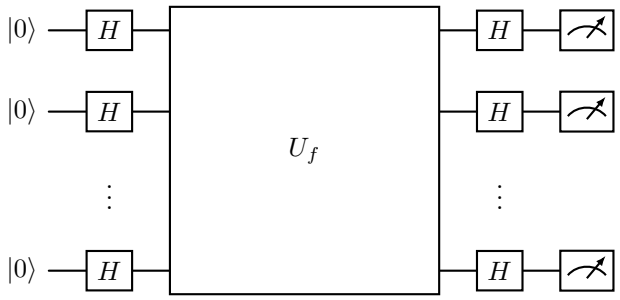


Figura 2.5: Circuito que implementa el algoritmo de Deutsch Jozsa.

La puerta U_f actúa de la siguiente forma sobre la base computacional:

$$U_f \left|i\right\rangle = (-1)^{f(i)} \left|i\right\rangle$$

U_f se le suele referir con el nombre de oráculo. En este caso se expone su acción sobre los estados, y se puede interpretar como una caja negra. Así no es necesario conocer la lógica interna de la puerta, sólo su acción.

Teorema 2.2. *Sea f una función de n entradas en las condiciones de Deutsch Jozsa. Si se mide $|0\rangle$ en el circuito de la Figura 2.5, entonces f es constante. En otro caso f es balanceada.*

Demostración. Sea $|0\ldots0\rangle = |0\rangle = |\psi_0\rangle$ el estado inicial. Se asume $n = 2^N$ por simplicidad. Si se aplica H a cada qubit, el nuevo estado será

$$H\left|\psi_0\right\rangle = \left|\psi_1\right\rangle = \left|+\cdots+\right\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} \left|i\right\rangle,$$

i.e., una superposición de estados uniforme.

Si f es **constante**, U_f introducirá una fase global idéntica $(-1)^{f(i)}$ en cada estado puesto que $f(i)$ es constante para todo ket i de la base. Es decir:

$$U_f \left|\psi_1\right\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{f(i)} \left|i\right\rangle \equiv \left|\psi_1\right\rangle$$

Finalmente, se aplica H y se obtiene de nuevo el estado $|0\rangle$. Por tanto al medir en la base computacional se obtendrá $|0\rangle$.

Si f es **balanceada**, U_f introducirá una fase relativa (-1) en la mitad de los estados de la base. Esto ocurre ya que la mitad de los estados tendrán imagen 0 y la otra mitad 1. Es decir:

$$U_f \left|\psi_1\right\rangle = \frac{1}{\sqrt{n}} \left[\sum_{i \in f^{-1}(0)} \left|i\right\rangle + \sum_{i \in f^{-1}(1)} (-1)^{f(i)} \left|i\right\rangle \right]$$

Veamos el producto escalar de $U_f \left|\psi_1\right\rangle$ con $\left|\psi_1\right\rangle$.

$$\langle + \cdots + | U_f | \psi_1 \rangle = \frac{1}{\sqrt{n}} \left[n/2 - n/2 \right] = 0$$

Por tanto, son ortogonales, y al aplicar H a cada estado lo seguirán siendo, pues H es unitaria. Se concluye que es imposible medir $|0\rangle$ a partir de $HU_f \left|\psi_1\right\rangle$ si f es balanceada.

□

Transformada de Fourier Cuántica

La transformada de Fourier Cuántica es la análoga de la transformada de Fourier discreta y es una parte importante de algoritmos cuánticos como el de Shor, que es el fundamento cuántico para la factorización de números enteros.

Se define la transformada de Fourier discreta como:

$$\begin{aligned} \mathcal{F}_n \colon \mathbb{C}^n &\longrightarrow \mathbb{C}^n \\ x &\longmapsto \mathcal{F}(x) \end{aligned}$$

de forma que:

$$\mathcal{F}_n \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} \sum_{j=0}^{n-1} x_j e^{\frac{2\pi i}{n} j0} \\ \vdots \\ \sum_{j=0}^{n-1} x_j e^{\frac{2\pi i}{n} j(n-1)} \end{pmatrix}$$

Se define $\omega = e^{\frac{2\pi i}{n}}$. Se puede escribir $\mathcal{F}_n$ en forma matricial del siguiente modo:

$$\mathrm{F}_n = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(n-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

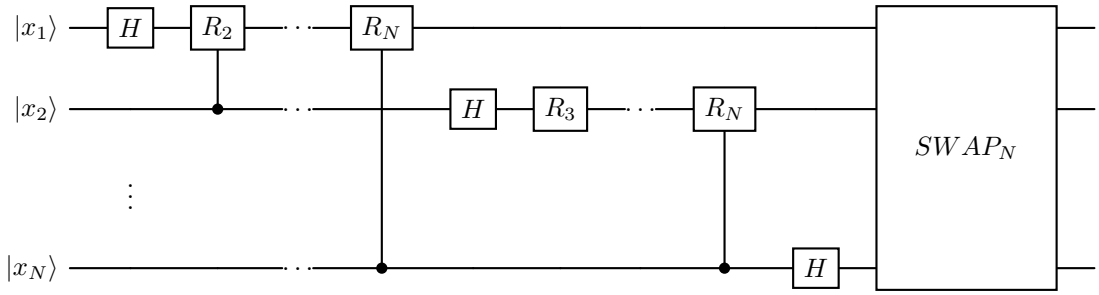


Figura 2.6: Circuito para implementar la transformada cuántica de Fourier con N qubits. La puerta SWAP intercambia los qubits $(i, N-i)$ para todo $i \in \{0, N/2-1\}$.

En esta sección se mostrará el circuito para implementar $\mathcal{F}_4$. Para ello se define $\omega = e^{\frac{\pi}{2}} = i$. Se tiene que

$$\mathcal{F}_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Si se define

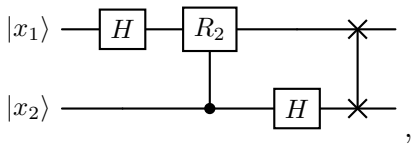
$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^k}} \end{pmatrix} \equiv R_z(\frac{2\pi}{2^k})$$

con $k = 2, ..., N$, se tiene que el circuito de la Figura 2.6 implementa $\mathcal{F}_n$. Se recuerda que $n = 2^N$.

En este caso, los qubits se nombran de 1 a N para facilitar la notación con respecto a las rotaciones R_k. El algoritmo QFT consta de los siguientes pasos:

- Para cada qubit i con $i = 1, ..., N$, por ese orden, se implementa H y después la puerta CR_k con $k = i + 1, ..., N$ con controlador el qubit k.
- Finalmente la puerta SWAP intercambia los qubits $(i, N - i)$ para todo $i \in \{0, N/2 - 1\}$.

El caso concreto con dos qubits corresponde a $n = 4$, la dimensión del espacio de Hilbert. El circuito que implementa $\mathcal{F}_4$ es



,

donde $R_2 = R_z(\pi/2) = S$.

Capítulo 3

Measurement Based Quantum Computing

La computación cuántica basada en medidas (Measurement Based Quantum Computing o MBQC) es un modelo de computación alternativo al modelo de circuitos. Se vio en el capítulo 2 que el modelo de circuitos combina puertas cuánticas para realizar operaciones unitarias U sobre un estado inicial de N qubits, para posteriormente medir el estado final.

El modelo MBQC emplea un enfoque distinto. Para ello, comienza con un estado entrelazado de qubits, al que posteriormente se van realizando medidas en diferentes bases que se determinan según los resultados previos, para llegar a un estado final equivalente a haber realizado una operación unitaria sobre esos qubits finales.

3.1. Teleportación Cuántica

El modelo MBQC es posible gracias a una propiedad cuántica llamada **teleportación**. Esta propiedad se basa a su vez en el entrelazamiento cuántico. No existe un equivalente clásico, pero se puede encontrar un ejemplo para ilustrar tal fenómeno [13]. Si se introducen dos papeles de distintos colores (como rojo y verde) en dos sobres y se barajan, al abrir uno de ellos se sabrá el color del papel que contienen el otro. Esto ocurre de forma instantánea e independientemente de la distancia entre los dos sobres.

Paradoja EPR

Este fenómeno de teleportación fue motivo de controversia tras la creación de la teoría de la mecánica cuántica, de naturaleza probabilística, en la primera mitad del siglo XX. Albert Einstein nunca se sintió cómodo con la mecánica cuántica. Pronunció la famosa frase "Dios no juega a los dados" para expresar su descontento con la naturaleza no determinista de la mecánica cuántica. Pero su oposición iba más allá. Creía que las propiedades de los objetos físicos tienen una realidad objetiva independiente de su medición. La mecánica cuántica deduce que al colapsar la función de onda se pierde información. Esto deriva de la no conmutatividad de los observables. La precisión con la que es posible conocer ciertas propiedades de una partícula, como su posición y momento, está sujeta a límites fundamentales debido al principio de indeterminación de Heisenberg. Cuando se realiza una medición de una magnitud, como la posición, la función de onda colapsa en un estado propio de esa magnitud, lo que significa que la información sobre su magnitud conjugada, en este caso, el momento, se pierde. Esta pérdida de información es inherente a la naturaleza misma de la mecánica cuántica. Debido a estas aparentes deficiencias, Einstein creía que la mecánica cuántica era una descripción incompleta de la realidad.

En 1935, Einstein, Boris Podolsky y Nathan Rosen publicaron un artículo presentando un experimento mental diseñado para exponer las deficiencias de la mecánica cuántica. La Paradoja EPR (Einstein-Podolsky-Rosen) intenta exponer el comportamiento absurdo de la teoría. Aunque las implicaciones de la paradoja EPR han sido debatidas durante décadas, la evidencia experimental ha demostrado la existencia real del entrelazamiento cuántico, además del Teorema de Bell que rechaza la teoría de variables ocultas.

Para entenderlo es importante conocer que las partículas de espín $1/2$ se pueden describir, de forma análoga a un qubit, como un $\mathbb{C}-$espacio de Hilbert de dimensión dos. En este experimento hay dos partículas, por lo que la situación es similar a un sistema de dos qubits.

Una partícula inestable con espín 0 se desintegra en dos partículas con espín $1/2$, que por conservación del momento angular deben tener componentes de espín opuestas y por conservación del momento lineal deben viajar en direcciones opuestas. Por ejemplo, un mesón pi neutro se desintegra en un electrón y un positrón según $\pi^0 \to e^- + e^+$. El estado cuántico de este sistema tras la desintegración de dos partículas es

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle_1|-\rangle_2 - |-\rangle_1|+\rangle_2), \tag{3.1}$$

donde los subíndices etiquetan las partículas y el signo menos relativo asegura que este es un estado de espín 0. Este estado en la base computacional se expresa como el estado $|\Phi^-\rangle$ de los estados de Bell. Así, el resultado de medir el espín de la primera partícula revela el resultado de medir el espín de la segunda partícula, que será el opuesto. Por tanto, si las partículas están alejadas lo suficiente y la información viaja como mucho a la velocidad de la luz, es previsible suponer que la información ya estaba en la segunda partícula. Los autores de la paradoja suponían que existían variables ocultas o desconocidas que contenían esa información.

Teleportación de un qubit

En la Figura 3.1 se representa la teleportación de un qubit. Se parte de un estado genérico de un qubit $|\psi\rangle$ que se quiere trasladar a otro qubit auxiliar que se encuentra en el estado $|+\rangle$. Para ello se entrelazan los dos qubits con la puerta CZ, y se realiza una medición del qubit original en el plano ecuatorial o plano $X-Y$ con un ángulo θ. Esto se consigue aplicando primero la puerta $R_z(\theta)$ y después la puerta H, para finalmente medir respecto a la base $\{|0\rangle, |1\rangle\}$, es decir, el eje z.

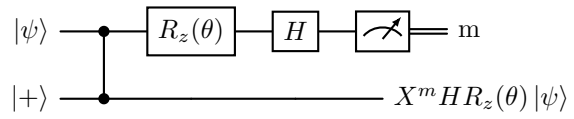


Figura 3.1: Circuito cuántico de teleportación de un qubit.

Teorema 3.1 (Teleportación de un qubit)**.** *La salida del circuito de la Figura 3.1 para una entrada $|\psi\rangle\otimes|+\rangle$ es $X^m H R_z(\theta)|\psi\rangle$, siendo $m=\{0,1\}$ el resultado de medir el primer qubit (medición ecuatorial con un ángulo θ) y $|\psi\rangle$ un estado genérico de un qubit.*

Demostración. El estado inicial es

$$|\psi_0\rangle = |\psi\rangle \otimes |+\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |+\rangle = \alpha|0+\rangle + \beta|1+\rangle$$

Se aplica primero la puerta CZ para entrelazar los dos qubits, obteniendo

$$CZ|\psi_0\rangle = CZ(\alpha|0+\rangle + \beta|1+\rangle) = \alpha|0+\rangle + \beta|1-\rangle =: |\psi_1\rangle .$$

Posteriormente se aplica la puerta $R_z(\theta)$ al primer qubit para conseguir

$$(R_z(\theta)\otimes\mathbb{I})|\psi_1\rangle = (R_z(\theta)\otimes\mathbb{I})(\alpha|0+\rangle + \beta|1-\rangle) = (\alpha|0+\rangle + \beta e^{i\theta}|1-\rangle) =: |\psi_2\rangle ,$$

y, a continuación, la puerta H, dando lugar a

$$(H \otimes \mathbb{I})(\alpha |0+\rangle + \beta e^{i\theta} |1-\rangle) = \alpha |++\rangle + \beta e^{i\theta} |--\rangle =: |\psi_3\rangle .$$

Finalmente, se mide el qubit en la base computacional. Para ello, se expresa el primer qubit de $|\psi_3\rangle$ en la base $\{|0\rangle, |1\rangle\}$, obteniendo

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle \otimes \left(\alpha |+\rangle + \beta e^{i\theta} |-\rangle \right) + |1\rangle \otimes \left(\alpha |+\rangle - \beta e^{i\theta} |-\rangle \right) \right] .$$

Esta expresión es equivalente a

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle \otimes X^0 H R_z(\theta) |\psi\rangle + |1\rangle \otimes X^1 H R_z(\theta) |\psi\rangle \right] ,$$

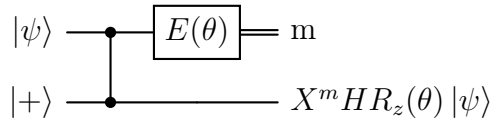
ya que

$$\begin{aligned} X^m H R_z(\theta) |\psi\rangle &= X^m H(\alpha |0\rangle + \beta e^{i\theta} |1\rangle) = X^m (a |+\rangle + b e^{i\theta} |-\rangle) \\ &= \begin{cases} \alpha |+\rangle + \beta e^{i\theta} |-\rangle & \text{si } m = 0 \\ \alpha |+\rangle - \beta e^{i\theta} |-\rangle & \text{si } m = 1. \end{cases} \end{aligned}$$

□

Se ha conseguido, mediante el circuito de teleportación, teleportar el estado de un qubit a otro auxiliar. Este principio es la base del modelo MBQC.

Nota 3.1. *De forma equivalente y para reducir notación, el circuito de teleportación puede ser representado de la siguiente forma [13]:*



donde θ es el ángulo con el que se realiza la medición en el plano ecuatorial.

Nota 3.2. *Se dice que se realiza una medición en el plano $X - Y$ con un ángulo θ ya que, con las puertas aplicadas, las probabilidades de medir 0 y 1 son las mismas que si se mide en la base $|\theta_\pm\rangle = \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$. Se puede también referir a esta medición como medición ecuatorial con ángulo θ.*

A continuación se justifica esta forma de nombrar a la operación que se realiza al qubit original en la Proposición 3.1. Por simplicidad y sin pérdida de generalidad,

se toma $\theta = 0$.
Sea $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \frac{1}{\sqrt{2}}(\alpha+\beta)\,|+\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)\,|-\rangle$.

- *Si se mide en la base computacional,* $\mathcal{P}_0 = |\alpha|^2$ *y* $\mathcal{P}_1 = |\beta|^2$.
- *Si se mide en la base* $|\theta_\pm\rangle = |\pm\rangle$, $\mathcal{P}_0 = \frac{1}{2}|\alpha+\beta|^2$ *y* $\mathcal{P}_1 = \frac{1}{2}|\alpha-\beta|^2$.

Sin embargo, si se mide $H\,|\psi\rangle$, *los ejes* x *y* z *se intercambian, por lo que las probabilidades de medir en cada base se intercambian.*
Sea $H\,|\psi\rangle = \alpha\,|+\rangle + \beta\,|-\rangle = \frac{1}{\sqrt{2}}(\alpha+\beta)\,|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)\,|1\rangle$. *Entonces:*

- *Si se mide en la base* $|\theta_\pm\rangle = |\pm\rangle$, $\mathcal{P}_0 = |\alpha|^2$ *y* $\mathcal{P}_1 = |\beta|^2$.
- *Si se mide en la base computacional,* $\mathcal{P}_0 = \frac{1}{2}|\alpha+\beta|^2$ *y* $\mathcal{P}_1 = \frac{1}{2}|\alpha-\beta|^2$.

Por tanto, medir en la base $|\pm\rangle$ *es equivalente a aplicar la puerta* H *y medir en la base computacional.*

3.2. Measurement Based Quantum Computing

En esta sección se introducen los conceptos necesarios, además de la notación para comprender el modelo de computación cuántica basada en medidas.

Notación

Como los enfoques del modelo de circuitos y el modelo MBQC son distintos, se ha de adaptar la notación a la filosofía del segundo modelo, basada en el empleo de grafos. En el caso MBQC, las reglas que se siguen son las siguientes:

- Cada nodo del grafo representa la medición de un qubit en el plano $X-Y$ con un ángulo θ.
- Las mediciones se realizan de izquierda a derecha.
- Los nodos que aparecen conectados mediante un cable están entrelazados por una puerta CZ y se inicializan en el estado $|+\rangle$, a menos que se indique lo contrario. En ese caso, se especificará el estado inicial de los nodos situados a la izquierda (los primeros en ser medidos).

- Los nodos circulares representan los qubits que son medidos, mientras que los cuadrangulares son los qubits que representan el output de la computación.

Nota 3.3. *Se recuerda que existen diferentes enfoques para el modelo de mediciones, pero en este trabajo se usan medidas en el plano $X-Y$. Cualquier otro enfoque es equivalente.*

Ejemplo 3.1. *Como ejemplo, se representa en la Figura 3.2 el circuito de teleportación de un qubit de la Proposición 3.1. El nodo circular representa el qubit original que es medido en el plano X-Y con un ángulo θ.*

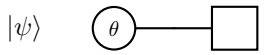


Figura 3.2: Notación MBQC para el circuito de teleportación de un qubit, donde $|\psi\rangle$ es el estado genérico que se quiere teleportar.

Mallas

A continuación se exponen las opciones más comunes a la hora de distribuir y entrelazar los qubits.

Definición 3.1 (Cluster State)**.** *Un estado clúster de tamaño $n \times m$ se construye de forma que*

- *Se inicializa cada qubit (i,j) en el estado $|+\rangle$ con $i \in \{1,...,n\}$ y $j \in \{1,...,m\}$.*
- *Se aplica la puerta CZ entre los qubits de cada fila $1 \leq i \leq n$, es decir, entre los qubits (i,j) y $(i,j+1)$ con $1 \leq j \leq m-1$.*
- *Se aplica la puerta CZ entre los qubits de cada columna $1 \leq j \leq m$, es decir, entre los qubits (i,j) y $(i+1,j)$ con $1 \leq i \leq n-1$.*

Se puede definir también un estado similar pero con los qubits de salida sin entrelazar.

Definición 3.2 (Open Cluster State)**.** *Un estado clúster abierto de tamaño $n \times m$ se construye de forma que*

- *Se inicializa cada qubit (i,j) en el estado $|+\rangle$ con $i \in \{1,...,n\}$ y $j \in \{1,...,m\}$.*
- *Se aplica la puerta CZ entre los qubits de cada fila $1 \leq i \leq n$, es decir, entre los qubits (i,j) y $(i,j+1)$ con $1 \leq j \leq m-1$.*

- *Se aplica la puerta CZ entre los qubits de cada columna $1 \leq j \leq m-1$, es decir, entre los qubits (i,j) y $(i+1,j)$ con $1 \leq i \leq n-1$.*

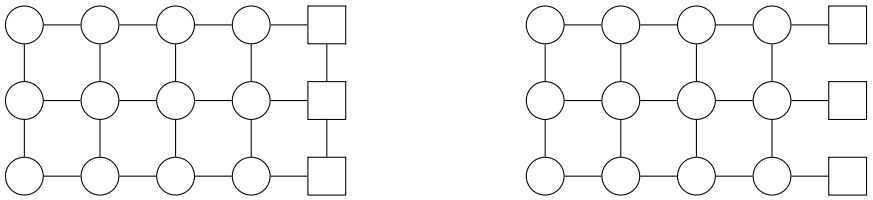


Figura 3.3: Estado clúster y estado clúster abierto de dimensiones $n = 3 \times m = 5$.

En la Figura 3.3 se representan los grafos de un estado clúster y un estado clúster abierto de dimensiones $n = 3 \times m = 5$.

Existe un tipo de distribución concreta que es empleado en modelos de computación cuántica ciega, y que es útil a la hora de probar la equivalencia entre los dos modelos en el capítulo 4 [14].

Definición 3.3 (Brickwork State)**.** *Un estado brickwork (ladrillo) de tamaño $n \times m$ donde $m \equiv 5$ (mód 8), es un estado entrelazado construido de la siguiente manera:*

- *Se inicializan todos los qubits en el estado $|+\rangle$.*
- *Para cada fila $i = \{1, ..., n\}$, se aplica el operador CZ en los qubits (i,j) y $(i,j+1)$ donde $1 \leq j \leq m-1$.*
- *Para cada columna $j \equiv 3$ (mód 8) y cada fila impar i, se aplica el operador CZ en los qubits (i,j) y $(i+1,j)$ y también en los qubits $(i,j+2)$ y $(i+1,j+2)$.*
- *Para cada columna $j \equiv 7$ (mód 8) y cada fila par i, se aplica el operador CZ en los qubits (i,j) y $(i+1,j)$ y también en los qubits $(i,j+2)$ y $(i+1,j+2)$.*

En la Figura 3.4 se representa un estado brickwork para una dimensión concreta ($n = 4$ y $m = 13$).

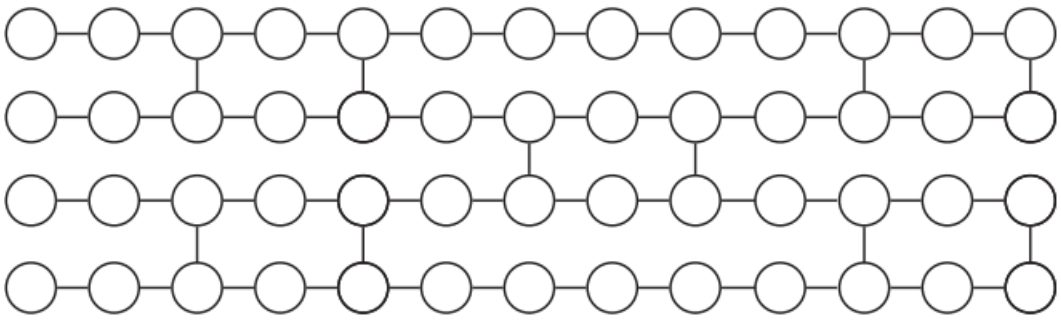


Figura 3.4: Estado brickwork con $n = 4$ y $m = 13$.

Nota 3.4. *En el caso de que sea necesario hacer referencia a un qubit en concreto, se asigna a cada qubit un índice* (i, j)*, donde* i *es una columna* $(i = \{1, ..., n\})$ *y* j *es una fila* $(j = \{1, ..., m\})$*.*

Grafo Lineal

Se consideran en esta sección los grafos lineales tal como el de la Figura 3.5. Un grafo lineal es un estado clúster con $n = 1$. El objetivo es comprender mejor el modelo MBQC, para ello se usa en un comienzo grafos unidimensionales.

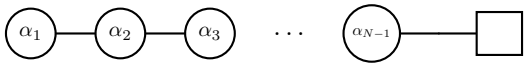


Figura 3.5: Grafo lineal con N *qubits.*

Proposición 3.1. *El estado del qubit de salida tras medir un estado clúster de* $n = 1 \times m = 3$ *es*

$$|\psi_3\rangle = X^{m_2} Z^{m_1} R_x((-1)^{m_1}\alpha_2) R_z(\alpha_1) |+\rangle$$

con $m_1, m_2 = \{0, 1\}$ *los resultados de medir el primer y el segundo qubit respectivamente.*

Demostración. El Teorema 3.1 se aplica para casos en los que exista un qubit objeto de medición y un qubit auxiliar para completar la teleportación. En este caso, no se cumplen esas condiciones. Sea $|G\rangle$ el estado inicial entrelazado.

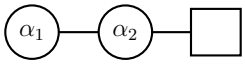


Figura 3.6: Grafo lineal con $n = 1 \times m = 3$ *que representa el estado* $|G\rangle$*.*

Sin embargo, sí se puede aplicar al grafo $|G'\rangle = CZ_{23} |G\rangle$.

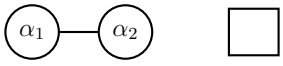


Figura 3.7: Grafo del estado $|G'\rangle$*.*

Si se realiza por tanto la medición del primer qubit se obtiene que $|\psi_2\rangle = X^{m_1} H R_z(\alpha) |+\rangle$. La medición del segundo qubit se realiza posteriormente.

Figura 3.8: Grafo del estado $|G'\rangle$ tras la medición del primer qubit.

Se aplica CZ_{23} de nuevo a $|G'\rangle$, de forma que $CZ_{23}\,|G'\rangle = CZ_{23}^2\,|G\rangle = |G\rangle$.

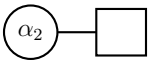
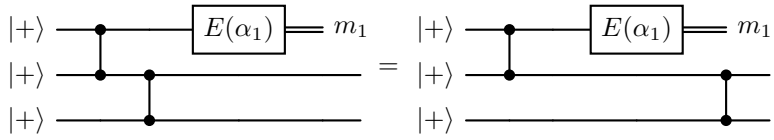


Figura 3.9: Grafo lineal equivalente a haber medido el primer qubit de $|G\rangle$. Ahora el segundo qubit se encuentra en el estado $|\psi_2\rangle$.

Esta forma de operar se puede visualizar en el modelo de circuitos.



De esta forma se puede aplicar el Teorema 3.1 a los dos qubits de la Figura 3.6. Así, el tercer qubit se encontrará en el estado $|\psi_3\rangle = X^{m_2}HR_z(\alpha_2)X^{m_1}HR_z(\alpha_1)\,|+\rangle$.

Usando la Proposición 2.4, se llega a que

$$|\psi_3\rangle = X^{m_2}Z^{m_1}R_x((-1)^{m_1}\alpha_2)R_z(\alpha_1)\,|+\rangle$$

□

Matrices de Corrección

Del grafo lineal de $N = 3$ de la Proposición 3.1 se han de destacar dos particularidades:

- La rotación alrededor del eje x es de $-\alpha_2$ radianes y no α_2.
- Hay dos matrices de Pauli que dependen de los resultados de la medición. Se las denomina matrices de corrección.

El primer hecho tiene solución fácil, puesto que las mediciones se pueden modificar previamente. Si se obtiene $m = 1$ en la medición previa, entonces se cambia el ángulo de medición θ por $-\theta$. Se cancela así el signo negativo.

Ahora se verán las consecuencias de la presencia de las matrices de corrección. Supongamos que $m = 1$, entonces $Z^m = Z$. Sin embargo, Z no afecta las probabilidades de medir $|0\rangle$ o $|1\rangle$ (medida en base computacional), ya que sólo introduce una fase global a $|1\rangle$, dejando igual a $|0\rangle$.

Si $X^m = X$, las probabilidades de medir $|0\rangle$ o $|1\rangle$ se intercambian y se pueden obtener las originales multiplicando el estado por X.

Estas correcciones no son por tanto definitivas sino que se pueden subsanar, siempre que estén al final de la operación unitaria. Se ve que siempre se pueden colocar al final, tras demostrar los dos siguientes lemas:

Lema 3.1. *Se cumple la siguiente relación:*

$$CZ_{ij}R_{z_i}(\theta) = R_{z_i}(\theta)CZ_{ij}$$

Demostración. Se escribe primero $R_{z_i} \otimes I$ y luego se realizan las operaciones pertinentes:

$$R_{z_i} \otimes I = \begin{pmatrix} e^{-i\theta/2} & 0 & 0 & 0 \\ 0 & e^{-i\theta/2} & 0 & 0 \\ 0 & 0 & e^{i\theta/2} & 0 \\ 0 & 0 & 0 & e^{i\theta/2} \end{pmatrix}.$$

Operando se puede ver la siguiente relación:

$$CZ_{ij}(R_{z_i} \otimes I) = \begin{pmatrix} e^{-i\theta/2} & 0 & 0 & 0 \\ 0 & e^{-i\theta/2} & 0 & 0 \\ 0 & 0 & e^{i\theta/2} & 0 \\ 0 & 0 & 0 & -e^{i\theta/2} \end{pmatrix} = (R_{z_i} \otimes I)CZ_{ij}.$$

□

Lema 3.2. *Se cumple la siguiente relación:*

$$CZ_{ij}X_i = X_iZ_jCZ_{ij}$$

Demostración. Primero se escribe $X_i \otimes I$:

$$X_i \otimes I = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Operando se cumple que:

$$CZ_{ij}(X_i \otimes I) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} = X_i Z_j CZ_{ij}$$

□

Se demuestra así que X y Z se pueden posponer si viene sucedido de CZ. Esto no es aislado ya que se verá que X y Z se pueden posponer siempre.

Proposición 3.2. *Existe siempre una expresión equivalente a multiplicar por la izquierda las matrices X y Z por el conjunto $\{H, R_z(\theta), R_x(\theta), CZ\}$, donde el control de CZ es en el qubit donde se aplican X y Z y $\theta \in [0, 2\pi]$.*

Demostración. Se verá paso a paso cada multiplicación:

- X y Z conmutan con $R_x(\theta)$ y $R_z(\theta)$ respectivamente al ser rotaciones alrededor del mismo eje.
- X y Z se pueden posponer si se aplica H posteriormente. Se ve gracias a la Ecuación 2.1: $HZ = XH$ y $HX = ZH$.
- X y Z se pueden posponer si $R_z(\theta)$ y $R_x(\theta)$ se aplican posteriormente. Si son dos rotaciones sobre ejes distintos se emplea la equivalencia:

  $$R_z(\theta)X = XR_z(-\theta).$$

  De igual forma, se tiene que

  $$R_x(\theta)Z = HR_z(\theta)HZ = HR_z(\theta)XH = HXR_z(-\theta)H = ZHR_z(-\theta)H = ZR_x(-\theta).$$

- Por último, ya se vio que X y Z se pueden posponer si van seguidas de la puerta CZ por el Lema 3.1 y el Lema 3.2.

□

Las matrices de Pauli siempre se pueden poner al final del resto de las operaciones y, además, se puede subsanar su contribución. Es por ello que en los modelos teóricos, salvo en el contexto de la computación cuántica ciega, se suelen obviar las correcciones y trabajar omitiéndolas. De forma general, en la literatura consultada el convenio establecido ha sido ese, ya que el hecho de evitar arrastrar las correcciones en cada paso simplifica el entendimiento y los cálculos para la computación basada en medidas.

Sin embargo, se ha de tener en cuenta que sí son importantes en la práctica, ya que pueden suponer un intercambio en las probabilidades de obtener cada valor en la medición.

Con estas dos nuevas pautas, el estado $|\psi_3\rangle$ del grafo lineal de la Proposición 3.1 pasaría de,

$$|\psi_3\rangle = X^{m_2} Z^{m_1} R_x((-1)^{m_1}\alpha_2) R_z(\alpha_1) |+\rangle$$

a

$$|\psi_3\rangle = R_x(\alpha_2) R_z(\alpha_1) |+\rangle .$$

Esto es equivalente a

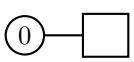
$$|\psi_3\rangle = H R_z(\alpha_2) H R_z(\alpha_1) |+\rangle ,$$

que es el resultado de aplicar dos veces el resultado del Teorema 3.1 de teleportación sin tener en cuenta la corrección X^m.

Ejemplos de Grafos Lineales

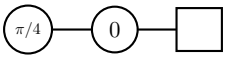
Se verán ahora dos ejemplos de cómo construir ciertas puertas de un qubit con estas pautas.

Ejemplo 3.2. *La puerta Hadamard es sencilla de aplicar. Basta con usar el siguiente grafo lineal:*



Ya que $R_z(0) = I$, el segundo qubit se encuentra en $|\psi_2\rangle = H |+\rangle$.

Ejemplo 3.3. *La otra puerta de un qubit que se utiliza en el conjunto de puertas universales es* T

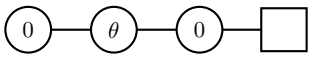


ya que $R_z(\pi/4) = T$*. El segundo qubit se encuentra en* $|\psi_2\rangle = H^2T\,|+\rangle = T\,|+\rangle$.

Una característica del modelo basado en medidas es que depende del input, en este caso, $|+\rangle$. ¿Y si se requiere que la puerta H se aplique a otro estado, como por ejemplo $R_x(\theta)\,|+\rangle$? ¿O a $R_y(\theta)\,|+\rangle$?

En el primer caso es sencillo puesto que es conocido las relaciones entre las rotaciones alrededor de x y de z. En el segundo es necesario conocer esa equivalencia para poder representarla. Sin embargo, no es un problema de existencia, sino de desconocimiento. Si se consigue implementar H, T y $CNOT$, se han de poder implementar todas las puertas.

Para aplicar H a $R_x(\theta)\,|+\rangle$, es posible hacerlo con medidas empleando 4 qubits:



Así, $|\psi_4\rangle = HHR_z(\theta)H\,|+\rangle = HR_x(\theta)\,|+\rangle$.

El hecho de que se preparen por convenio los qubits iniciales en el estado $|+\cdots+\rangle$ no interfiere con la demostración de la universalidad del modelo basado en medidas. Esto ocurre ya que cualquier otro estado inicial puede obtenerse a partir de $|+\cdots+\rangle$. Esta operación se añade a la operación original, dando lugar a una nueva que es producto de ambas. Por la universalidad del conjunto de puertas universales, esta nueva operación también se puede descomponer en esas puertas básicas.

Ejemplos de Grafos con $n > 1$

Si se aumenta el número de filas, aparece una dificultad nueva, puesto que el Teorema 3.1 toma un estado $|\psi\rangle$ de un qubit, pero en este nuevo caso aparece un estado entrelazado. Sin embargo, el resultado es análogo al aumentar la dimensión del estado original. Esto sucede ya que un estado entrelazado de n qubits (se toma n porque corresponde al número de filas) se puede escribir en coordenadas de la base computacional del espacio de Hilbert de dimensión 2^n. Se procede entonces de forma análoga a la teleportación de un qubit.

Nota 3.5. *En este caso n es el número de filas del grafo. En este capítulo se toma $N = 2^n$ por simplicidad. Esta notación de n y N no es la del capítulo 2.*

Teorema 3.2 (Teleportación de un qubit entrelazado)**.** *Sea una columna de n qubits entrelazados de un estado de MBQC y sea $|\psi\rangle$ el estado entrelazado que lo describe. Su expresión en la base computacional es*

$$|\psi\rangle = a_0 |0 \dots 0\rangle + \cdots + a_{N-1} |1 \dots 1\rangle ,$$

con $N = 2^n$. Se mide el primer qubit con un ángulo θ. Este qubit está previamente entrelazado con el qubit de su fila en la columna 2. Entonces el estado que describe los qubits que restan en la columna y el qubit $(1, 2)$ (suponiendo orden de izquierda a derecha y de arriba a abajo) es

$$(I \otimes \cdots \otimes X^m H R_z(\theta)) |\psi\rangle$$

siendo $m = \{0, 1\}$ el resultado de medir el primer qubit (medición ecuatorial).

Demostración. Por comodidad se define $N = 2^n$ (solo en esta demostración). El estado inicial, sin haber entrelazado el qubit de la segunda columna, es

$$|\psi_0\rangle = |\psi\rangle \otimes |+\rangle = (a_0 |0 \dots 0\rangle + \cdots + a_{N-1} |1 \dots 1\rangle) \otimes |+\rangle$$

Se definen ahora dos conjuntos:

$$S_0 = \{|\psi_0 \dots \psi_{N-1}\rangle \in \mathcal{H}_N \colon \psi_0 = 0\}$$

$$S_1 = \{|\psi_0 \dots \psi_{N-1}\rangle \in \mathcal{H}_N \colon \psi_0 = 1\}$$

Es decir S_0 son los estados de la base computacional tal que el primer qubit es 0. Se tiene además que $|S_0| = N/2 = 2^{n-1} =: M$. Es también necesario definir una biyección:

$$\begin{aligned} \varphi_0 \colon S_0 &\longrightarrow B(m) \\ |\psi_0 \dots \psi_{N-1}\rangle &\longmapsto |\psi_1 \dots \psi_{N-1}\rangle \end{aligned}$$

donde

$$B(m) = \{|\psi_1 \dots \psi_{N-1}\rangle \in \mathcal{H}_M\}$$

es la base canónica del espacio de Hilbert de dimensión M. En otras palabras, son los kets de S_0 tras eliminar la coordenada que corresponde al primer qubit.

Se puede establecer otra biyección φ_1 de S_1 a $B(m)$ análoga a φ_0. Sin embargo, se denotará $\varphi_1(S_1) = B'(m)$. $B(m)$ es el mismo conjunto que $B'(m)$, pero tienen orígenes distintos. Esto es importante porque el objetivo es asociar cada coordenada que acompaña a un ket de S_0 y S_1 con la imagen de ese ket mediante φ_0 y φ_1.

Dado $|\psi_0\rangle$, se aplica entonces la puerta CZ para entrelazar los dos qubits de la primera fila.

$$|\psi_1\rangle = (CZ_{1(N+1)} \otimes I \cdots \otimes I)\,|\psi_0\rangle = (a_0\,|0\ldots0\rangle + \cdots +$$
$$+a_{N/2-1}\,|0\ldots1\rangle) \otimes |+\rangle + (a_{N/2}\,|1\ldots0\rangle + \cdots + a_{N-1}\,|1\ldots1\rangle) \otimes |-\rangle$$

Posteriormente se aplica la puerta $R_z(\theta)$ al primer qubit. A los elementos de S_0 esta rotación no les afecta (se toma la equivalencia por fase global de la puerta $R_z(\theta)$ de la definición). A los elementos de S_1 esta rotación les introduce una fase de $e^{i\theta}$. El nuevo estado es $|\psi_2\rangle$:

$$|\psi_2\rangle = (R_z(\theta) \otimes I \cdots \otimes I)\,|\psi_1\rangle = (a_0\,|0\ldots0\rangle + \cdots +$$
$$+a_{N/2-1}\,|0\ldots1\rangle) \otimes |+\rangle + (a_{N/2}e^{i\theta}\,|1\ldots0\rangle + \cdots + a_{N-1}e^{i\theta}\,|1\ldots1\rangle) \otimes |-\rangle$$

Por último se aplica la puerta H. Para los elementos de S_0 el estado del primer qubit será $|+\rangle$ y $|-\rangle$ para los elementos de S_1.

$$|\psi_3\rangle = (R_z(\theta) \otimes I \cdots \otimes I)\,|\psi_2\rangle = (a_0\,|+\ldots0\rangle + \cdots +$$
$$+a_{N/2-1}\,|+\ldots1\rangle) \otimes |+\rangle + (a_{N/2}e^{i\theta}\,|-\ldots0\rangle + \cdots + a_{N-1}e^{i\theta}\,|-\ldots1\rangle) \otimes |-\rangle$$

Finalmente se mide el primer qubit en la base computacional. Para ello, se expresa el primer qubit de $|\psi_3\rangle$ en la base $\{|0\rangle, |1\rangle\}$. Se opera de forma análoga a la demostración del caso del circuito de teleportación, por lo que se tiene

$$\begin{aligned}|\psi_3\rangle =& \frac{1}{\sqrt{2}}\left[|0\rangle \otimes \left(\left(\sum_{i\in B(m)} a_i\,|i\rangle\right) \otimes |+\rangle + e^{i\theta}\left(\sum_{i\in B'(m)} a_i\,|i\rangle\right) \otimes |-\rangle\right)\right] + \\ &+\frac{1}{\sqrt{2}}\left[|1\rangle \otimes \left(\left(\sum_{i\in B(m)} a_i\,|i\rangle\right) \otimes |+\rangle - e^{i\theta}\left(\sum_{i\in B'(m)} a_i\,|i\rangle\right) \otimes |-\rangle\right)\right],\end{aligned}$$

donde a_i hace referencia al escalar que multiplicaba a $\varphi_0^{-1}(|i\rangle)$ si $i \in B(m)$ o a

$\varphi_1^{-1}(|i\rangle)$ si $i \in B'(m)$.

Esto es más sencillo de lo que aparenta. Por ejemplo, el ket $|0\rangle$ o $|0\dots0\rangle$ que aparece en la base al expresar $|\psi_0\rangle$ está multiplicado por a_0 y el ket $|M\rangle$ o $|100\dots0\rangle$ está multiplicado por a_M. La imagen de cada ket por su respectiva biyección es la misma, pero cada uno lleva asociado una coordenada diferente.

La última expresión es equivalente a la siguiente

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle \otimes (I \otimes \cdots \otimes X^m H R_z(\theta))\,|\psi\rangle + |1\rangle \otimes (I \otimes \cdots \otimes X^m H R_z(\theta))\,|\psi\rangle\,,\right]$$

y así se prueba el resultado. □

En este teorema se toma el qubit de la fila 1 por comodidad, pero se aplica a toda fila $i = 1, ..., n$. El objetivo es demostrar que es posible aplicar la teleportación con un estado más general. La puerta $X^m H R_z(\theta)$ se aplica al final porque es el orden que se estableció al entrelazar los dos qubits. Tras realizar la medición, la primera coordenada de los vectores de la base hace referencia al qubit $(2, 1)$ y la última al qubit $(1, 2)$. Lo relevante del teorema es que se puede aplicar directamente $X^m H R_z(\theta)$. Se escribe en el siguiente corolario cómo sería medir los n qubits de la columna.

Corolario 3.1. *Sea una columna j de n qubits entrelazados de un estado de MBQC con $j = 1, ..., m-1$ y sea $|\psi\rangle$ un estado entrelazado de n qubits. Su expresión en la base computacional es*

$$|\psi\rangle = a_0\,|0\dots0\rangle + \cdots + a_{N-1}\,|1\dots1\rangle$$

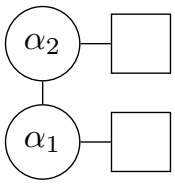
con $N = 2^n$. Se miden los n qubits con un ángulo θ_n respectivamente (se supone orden de arriba a abajo). Cada qubit (i, j) está entrelazado con el qubit de su fila en la columna $j + 1$ con $i = 1, ..., n$. Entonces el nuevo estado entrelazado que representa la columna $j + 1$ es

$$(X^{m_1} H R_z(\theta_1) \otimes \cdots \otimes X^{m_n} H R_z(\theta_n))\,|\psi\rangle$$

siendo $m_i = \{0, 1\}$ el resultado de medir el qubit (i, j) (medición ecuatorial).

Se ve a continuación un caso sencillo para ilustrar este hecho, fundamental en el modelo MBQC.

Ejemplo 3.4. *Un caso sencillo es cuando $n = 2$. Se tiene entonces un grafo como el siguiente.*



Se procede a medir el qubit $(1,1)$ con el ángulo indicado. Sea $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ un estado que describe un entrelazamiento general entre los dos qubits de la primera columna. Por tanto el estado inicial teniendo en cuenta el qubit $(1,2)$ es

$$|\psi_0\rangle = |\psi\rangle \otimes |+\rangle .$$

Si se entrelaza el qubit $(1,1)$ con el qubit $(1,2)$ mediante CZ, se obtiene

$$|\psi_1\rangle = (a_{00}|00\rangle + a_{01}|01\rangle) \otimes |+\rangle + (a_{10}|10\rangle + a_{11}|11\rangle) \otimes |-\rangle .$$

Posteriormente se aplica $HR_z(\alpha_2)$ y se obtiene:

$$|\psi_3\rangle = (a_{00}|+0\rangle + a_{01}|+1\rangle) \otimes |+\rangle + e^{i\alpha_2}(a_{10}|-0\rangle + a_{11}|-1\rangle) \otimes |-\rangle .$$

Se realiza el cambio de base del primer qubit del estado entrelazado, se llega a

$$\begin{aligned} |\psi_3\rangle =& \frac{1}{\sqrt{2}}\left[|0\rangle \otimes \left((a_{00}|0\rangle + a_{01}|1\rangle) \otimes |+\rangle + e^{i\alpha_2}((a_{10}|0\rangle + a_{11}|1\rangle) \otimes |-\rangle)\right] + \\ &+ \frac{1}{\sqrt{2}}\left[|1\rangle \otimes \left(((a_{00}|0\rangle + a_{01}|1\rangle) \otimes |+\rangle - e^{i\alpha_2}(a_{10}|0\rangle + a_{11}|1\rangle) \otimes |-\rangle\right)\right] . \end{aligned}$$

Ahora se ve la acción de $(I \otimes X^m HR_z(\alpha_2))$ sobre $|\psi\rangle$, que es

$$\begin{aligned} &a_{00}|0+\rangle + (-1)^m a_{01} e^{i\alpha_2}|0-\rangle + a_{10}|1+\rangle + (-1)^m a_{11} e^{i\alpha_2}|1-\rangle = \\ &= (a_{00}|0\rangle + a_{10}|1\rangle) \otimes |+\rangle + (-1)^m e^{i\alpha_2}(a_{01}|0\rangle + a_{11}|1\rangle) \otimes |-\rangle . \end{aligned}$$

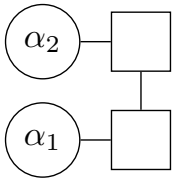
Se han seguido los pasos de la demostración del Teorema 3.2. Aplicando directamente el Corolario 3.1, se obtiene que los dos qubits de salida se encuentran entrelazados en el estado:

$$(X^{m_2} HR_z(\alpha_2) \otimes X^{m_1} HR_z(\alpha_1))|\psi\rangle$$

si m_2 es el resultado de medir el qubit $(1,1)$ y m_1 el $(2,1)$.

El último caso novedoso es el siguiente ejemplo, ya que el resto son extensiones de los ejemplos ya vistos.

Ejemplo 3.5. *Sea el grafo de la figura y sea* $|\psi\rangle$ *un ket que describe el estado en el que se hallan los qubits* $(1,1)$ *y* $(2,1)$*. Generalmente* $|\psi\rangle = |{+}{+}\rangle$*.*



En este caso, los dos qubits de salida se encontrarán en el estado:

$$CZ(X^{m_2}HR_z(\alpha_2) \otimes X^{m_1}HR_z(\alpha_1))\,|\psi\rangle$$

si m_2 *es el resultado de medir el qubit* $(1,1)$ *y* m_1 *el* $(2,1)$*.*

Nota 3.6. *Se recuerda que en general no se arrastran las matrices de Pauli, sino que se omiten.*

Celda Universal del estado Brickwork

En un estado brickwork los entrelazamientos entre filas no son arbitrarios, sino que forman celdas como la de la Figura 3.10. Se denominará en adelante celda universal del estado brickwork. No es una celda base o unidad porque el patrón general no se forma a partir de ellas, sino de una celda un poco más grande (2 filas y 8 columnas). Sin embargo, esta celda sirve para aplicar una puerta concreta, mientras que los qubits que restan en la celda unidad actúan como la identidad. Más adelante se aclarará este concepto, ya que es importante para probar la universalidad del MBQC.

Los ángulos especificados tienen su razón de ser. A continuación se verá la acción sobre los dos qubits de salida, es decir, la operación unitaria que actúa sobre ellos.

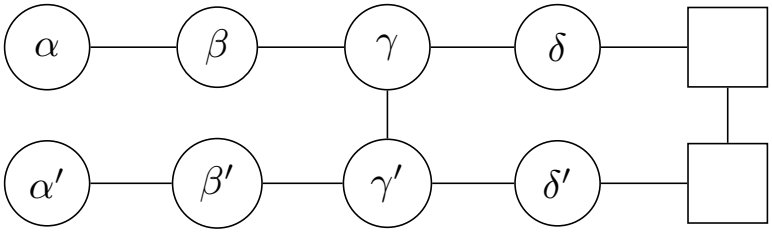
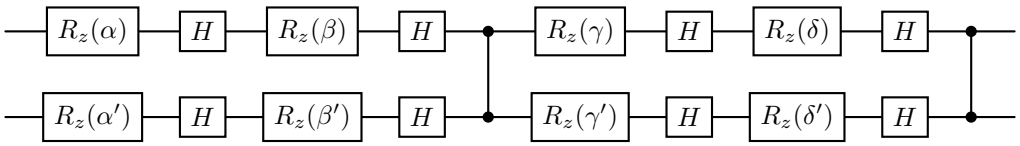


Figura 3.10: Celda universal de un estado brickwork.

Proposición 3.3. *La operación unitaria equivalente al circuito de la Figura 3.10 es*

$$CZ\,(HR_z(\delta)HR_z(\gamma)) \otimes (HR_z(\delta')HR_z(\gamma'))\,CZ\,(HR_z(\beta)HR_z(\alpha)) \otimes (HR_z(\beta')HR_z(\alpha'))$$

Demostración. Por el Teorema 3.1 y el Corolario 3.1, el circuito de la Figura 3.10 es equivalente a



□

Nota 3.7. *En realidad tendría que aparecer que el estado inicial es el estado en superposición $|{+}{+}\rangle$. Sin embargo, como ya se expuso previamente, si se prueba la universalidad, cualquier otro estado se puede obtener a partir de $|{+}{+}\rangle$ mediante el modelo basado en medidas. Es por ello que en el circuito equivalente al grafo de la Figura 3.10 no se especifica el estado inicial de los dos qubits. Este hecho también se aplica en casos posteriores donde se trate las equivalencias concretas con puertas de un conjunto universal.*

3.3. Algoritmos Cuánticos en MBQC

Algoritmo de Deutsch Jozsa

En esta sección se verá la forma equivalente de aplicar el algoritmo de Deutsch-Jozsa en MBQC para el caso $n = 2$ (con la notación usada para este algoritmo en el caso del modelo de circuitos).

La mayor diferencia entre los dos modelos ocurre con el carácter del oráculo U_f. En el modelo de circuitos se trata como una caja negra, pero en el modelo MBQC se han de especificar los ángulos a usar, y eso dependerá del carácter de la función f. Por tanto en el modelo MBQC se ha de adaptar el oráculo a la función f específica, no se puede tratar de modo genérico. Esto implica que este algoritmo no tiene ningún sentido práctico en la realidad en el modelo MBQC, porque para poder implementarlo habría que conocer la solución del problema de antemano (el carácter de f). Sin embargo, se expone para continuar mostrando ejemplos y comprendiendo el modelo basado en medidas.

Para $n = 2$, existen 8 variantes posibles de la función f: dos constantes y seis balanceadas. En el caso de las balanceadas, si se mira las combinaciones para la antiimagen del 0 se tienen un total de

$$\binom{4}{2} = 6$$

posibilidades distintas.

En general, el número de variantes de f balanceada con n entradas son:

$$\binom{2^n}{2^{n-1}}.$$

Es por esta razón que se escoge el caso $n = 2$. Las variantes se hallan en la tabla de la Figura 3.11.

	i	ii	iii	iv	v	vi	vii	$viii$
$f(0,0)$	0	1	0	0	0	1	1	1
$f(0,1)$	0	1	0	1	1	0	0	1
$f(1,0)$	0	1	1	0	1	0	1	0
$f(1,1)$	0	1	1	1	0	1	0	0

Figura 3.11: Tabla con las 8 variantes de f cuando $n = 2$. Las dos primeras corresponden a f constante.

El oráculo se implementará en cada caso según la Figura 3.12.

Ejemplo 3.6. *Con este ejemplo se ilustra cómo funcionan las equivalencias de la Figura 3.12. Se toma la variante (vi) de la función f, que corresponde al caso balanceado. Por la definición de oráculo U_f, su acción sobre la base es:*

$$U_f |i\rangle = (-1)^{f(x)} |i\rangle$$

Su acción sobre $|{+}{+}\rangle$ es entonces

$$U_f |{+}{+}\rangle = \frac{1}{2} [|01\rangle + |10\rangle - |00\rangle - |11\rangle] .$$

Se ve ahora que $U_f \equiv (Y \otimes Y)$, ya que

$$(Y \otimes Y) |{+}{+}\rangle = \frac{1}{2} \left[i^2 |00\rangle - i^2 |01\rangle - i^2 |10\rangle + i^2 |11\rangle \right] = \frac{1}{2} [|01\rangle + |10\rangle - |00\rangle - |11\rangle] .$$

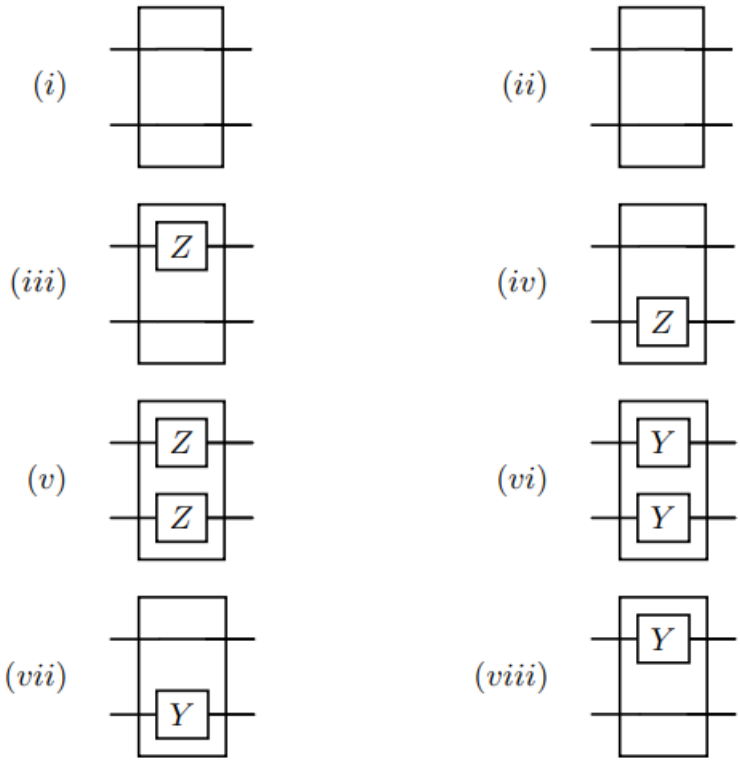
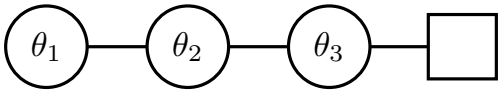


Figura 3.12: Implementación del oráculo U_f para $n = 2$ para las 8 variantes de f [8].

Se puede operar de forma análoga para el resto de variantes.

Se aprecia en la Figura 3.12 que no existe entrelazamiento entre los dos qubits, sino que se consigue el resultado gracias a la superposición de estados. Si el estado inicial es $|{+}{+}\rangle$, que es el convenio en el modelo MBQC, entonces solo es necesario aplicar la puerta Hadamard tras el oráculo para implementar el algoritmo.

A partir de las diferentes construcciones del oráculo se puede ejecutar el algoritmo en el modelo MBQC a partir de dos grafos lineales con 4 qubits como el siguiente:



Por el Corolario 3.1, este grafo produce la operación unitaria

$$HR_z(\theta_3)HR_z(\theta_2)HR_z(\theta_1).$$

Teorema 3.3. *El grafo de la Figura 3.13 implementa el algoritmo de Deutsch Jozsa*

con los ángulos especificados en la Figura 3.14.

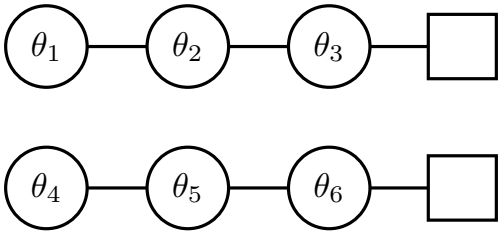


Figura 3.13: Grafo que implementa el el algoritmo de Deutsch Jozsa de 2 entradas en el modelo MBQC.

Demostración. Se tiene que:

- H se consigue si $\theta_i = 0$ con $i = 1, 2, 3$ ya que

$$H^3 = H.$$

- HZ se consigue si $\theta_1 = \pi$ y el resto de ángulos 0 ya que

$$H^2HZ = HZ.$$

- HY se consigue si $\theta_2 = \pi = \theta_3$ y $\theta_1 = 0$, puesto que

$$HZHZH = HZX = iHY \equiv HY.$$

  Se ha de tener en cuenta que $ZX = iY$.

La Figura 3.14 registra las combinaciones de ángulos necesarias para cada variante de la función f. □

	i	ii	iii	iv	v	vi	vii	viii
θ_1	0	0	π	0	π	0	0	0
θ_2	0	0	0	0	0	π	0	π
θ_3	0	0	0	0	0	π	0	π
θ_4	0	0	0	π	π	0	0	0
θ_5	0	0	0	0	0	π	π	0
θ_6	0	0	0	0	0	π	π	0

Figura 3.14: Tabla con los ángulos requeridos para implementar el algoritmo de Deutsch Jozsa de 2 entradas en el modelo MBQC.

Capítulo 4

Universalidad del modelo MBQC

En el modelo de circuitos se vio que se puede descomponer cualquier operación unitaria en el conjunto de puertas universales $\{H, T, CNOT\}$. El objetivo de esta sección es probar que el modelo de computación cuántica basada en medidas o MBQC es equivalente al modelo de circuitos. Para ello, se prueba que se puede construir una malla en la que es posible aplicar H, T y $CNOT$ a cualquier qubit.

Si fuese posible construir tal malla, entonces los dos modelos serían equivalentes. En ese caso se concluiría que el modelo MBQC es universal.

4.1. Equivalencia del Modelo MBQC con el Modelo de Circuitos

Teorema 4.1 (Equivalencia del modelo MBQC sobre un estado brickwork con el modelo de circuitos)**.** *Dado un circuito que utilice las puertas del conjunto universal $\{H, T, CNOT\}$, se puede construir un estado brickwork que implemente una operación unitaria equivalente.*

El objetivo de esta sección es demostrar este teorema. Una vez se pruebe su veracidad, se prodrá probar el siguiente teorema que establece la universalidad del modelo MBQC.

Teorema 4.2 (Universalidad del modelo MBQC)**.** *El modelo MBQC es universal en el sentido de que se puede aproximar cualquier operación unitaria con cualquier precisión requerida.*

En esta demostración se da por cierto el Teorema 4.1.

Demostración. Sea U una operación unitaria de dimensión arbitraria (finita). Por la Proposición 2.8, dado $\epsilon > 0$, se puede construir un circuito empleando el conjunto de puertas $\{H, T, CNOT\}$ que realice una operación unitaria U' de forma que $\|U' - U\| < \epsilon$. Ahora, por el Teorema 4.1, existe un estado brickwork equivalente al circuito que implementa U'. Se concluye que el modelo MBQC es universal. □

4.2. Estado Brickwork

La distribución de entrelazamientos en un estado brickwork no es arbitraria, sino que tiene su razón de ser. En la Figura 4.1, cada color representa una celda universal como la de la Figura 3.10.

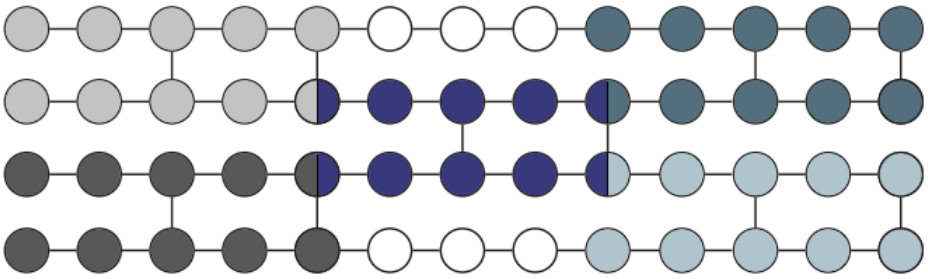


Figura 4.1: Estado brickwork con $n = 4$ y $m = 13$. Cada color representa una celda universal.

Los pasos a seguir para probar la equivalencia del modelo MBQC con el modelo de circuitos son los siguientes:

- Se prueba que una celda universal puede implementar las puertas del conjunto $\{H, T, CNOT\}$.
- Se prueba que la secuencia de tres qubits que se hallan entre celda y celda en la fila superior e inferior no produce ninguna operación unitaria si son medidos con un ángulo 0 en el plano ecuatorial.
- Se intrepreta cada celda como una operación unitaria de dos qubits tal como se ve en la Figura 4.2.

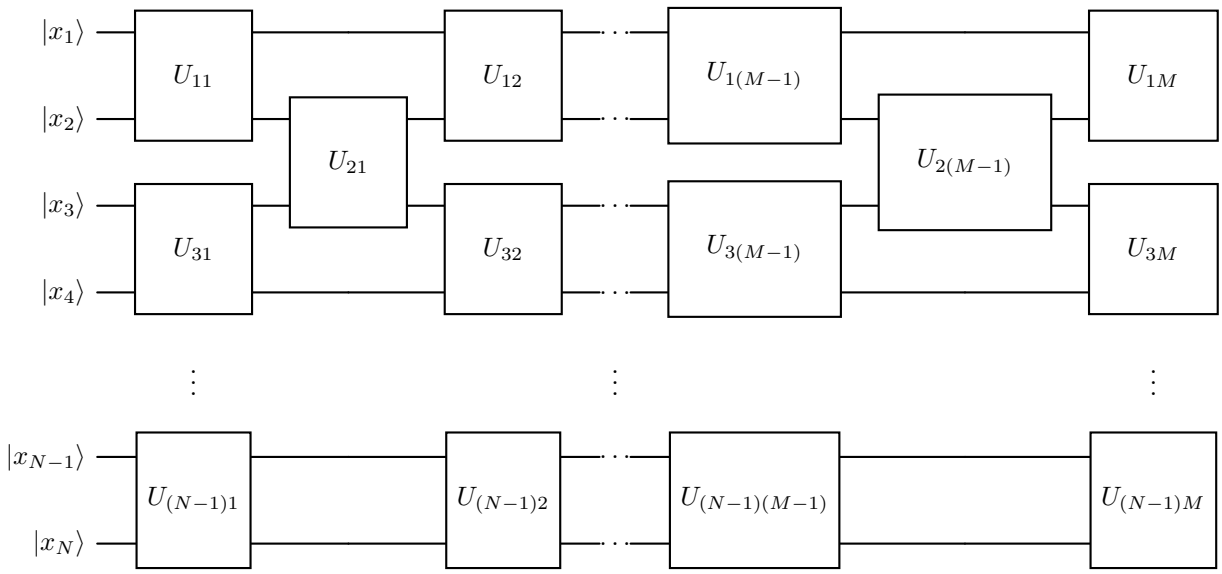


Figura 4.2: Equivalencia del estado brickwork con el modelo de circuitos. Cada celda universal se intrepreta como una puerta cuántica de dos qubits. No aparecen explícitamente las puertas $U_{(N-2)1}$ ni $U_{(N-2)(M-1)}$.

Con estos pasos se prueba la equivalencia ya que cualquier circuito que utilice las puertas del conjunto universal $\{H, T, CNOT\}$ se puede construir mediante un estado brickwork.

Ejemplo 4.1. *Como ejemplo se muestra en la Figura 4.3 la equivalencia del grafo de la Figura 4.1 en el modelo de circuitos.*

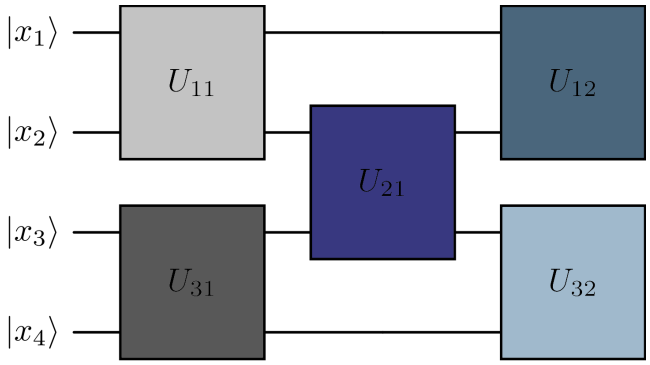


Figura 4.3: Equivalencia del estado brickwork con $n = 4$ y $m = 13$ en el modelo de circuitos.

Paso 1: Equivalencia de la Celda Universal con H,T y CNOT.

Se comienza probando que se puede implementar las puertas H,T y CNOT en una celda universal.

Puerta Hadamard

Proposición 4.1. *El grafo de la Figura 4.4 implementa la puerta H en el qubit superior y no actúa sobre el inferior. Es decir, el grafo es equivalente a realizar la operación $H \otimes I$.*

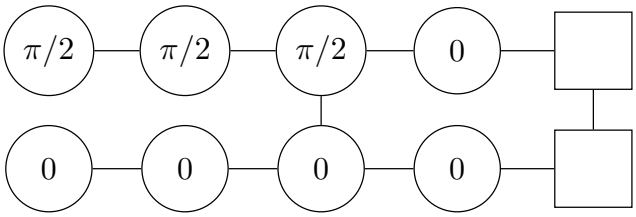
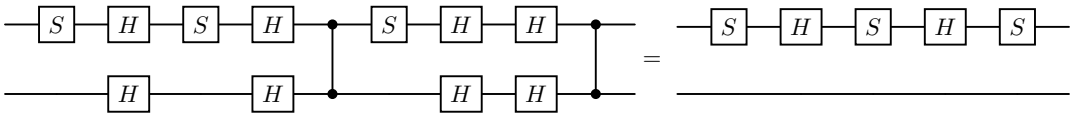


Figura 4.4: Celda universal del estado brickwork que implementa H en el qubit superior.

Demostración. La Proposición 3.3 trató el caso general. Se han de sustituir los siguiente ángulos:

- $\alpha = \beta = \gamma = \pi/2$.
- $\alpha' = \beta' = \gamma' = \delta = \delta' = 0$.

Por tanto el circuito equivalente al grafo de la Figura 4.4 es



donde se tuvo en cuenta que $H^2 = CZ^2 = I$ y que CZ conmuta con $R_z(\theta)$.

Se ha de ver ahora que $SHSHS$ es equivalente a la puerta H. Se tiene

$$SHSHS = \frac{1}{2}\begin{pmatrix} 1+i & 1+i \\ 1+i & -(1+i) \end{pmatrix} = \frac{1}{2}(1+i)\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Por la Proposición 2.2, esta puerta es equivalente a multiplicarla por una fase global $c \in \mathbb{C}$ con $|c| = 1$. Sea $c = \frac{\sqrt{2}}{1+i}$.

$$|c| = \left|\frac{\sqrt{2}}{1+i}\right| = \frac{\sqrt{2}}{\sqrt{2}} = 1$$

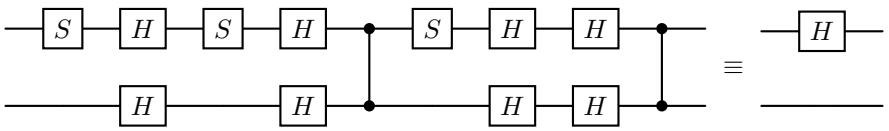
Además, se ve que

$$\frac{1}{2}c(1+i) = \frac{\sqrt{2}}{1+i}\frac{1}{2}(1+i) = \frac{1}{\sqrt{2}}.$$

Por tanto

$$SHSHS = \frac{1}{2}(1+i)\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \equiv \frac{1}{2}c(1+i)\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = H.$$

Se concluye que es cierto la siguiente equivalencia:



□

Puerta T

Proposición 4.2. *El grafo de la Figura 4.5 implementa la puerta T en el qubit superior y no actúa sobre el inferior. Es decir, el grafo es equivalente a realizar la operación $T \otimes I$.*

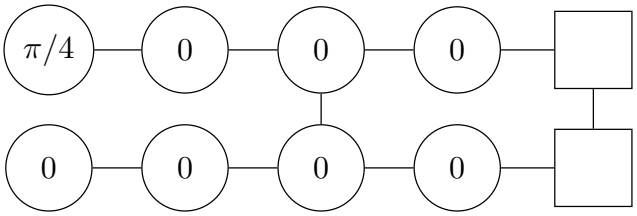
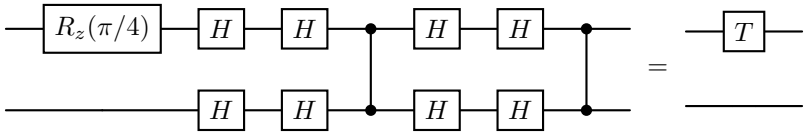


Figura 4.5: Celda universal del estado brickwork que implementa T en el qubit superior.

Demostración. Se han de sustituir los siguiente ángulos en el caso genérico tratado en la Proposición 3.3 :

- $\alpha = \pi/4$.
- $\alpha' = \beta = \beta' = \gamma = \gamma' = \delta = \delta' = 0$.

Por tanto el circuito equivalente al grafo de la Figura 4.4 es



donde se tuvo en cuenta que $H^2 = CZ^2 = I$. □

Puerta CNOT

Proposición 4.3. *El grafo de la Figura 4.6 implementa la puerta CNOT siendo el qubit superior el controlador.*

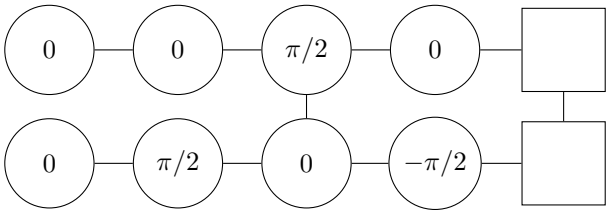
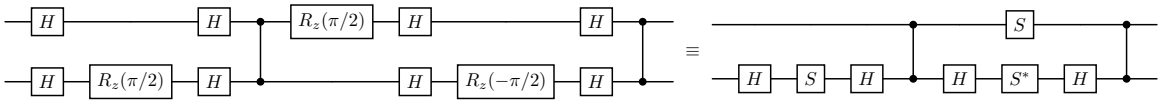


Figura 4.6: Celda universal del estado brickwork que implementa CNOT siendo el qubit superior el controlador.

Demostración. Se han de sustituir los siguiente ángulos en el caso genérico tratado en la Proposición 3.3 :

- $\beta' = \gamma = \delta' = \pi/4$.
- $\alpha = \alpha' = \beta = \gamma' = \delta = 0$.

Por tanto el circuito equivalente al grafo de la Figura 4.6 es



donde se tuvo en cuenta que $H^2 = I$.

La expresión matricial de la operación unitaria del circuito es

$$(I \otimes HSH)CZ(S \otimes HS^*H)CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = CNOT.$$

□

Puerta SWAP a partir de la puerta CNOT.

La demostración del Teorema 4.2 se basa en la premisa de que el conjunto de puertas $\{H, T, CNOT\}$ es universal, proposición que se expuso sin demostración en el Capítulo 2.

Este conjunto universal es solo un caso concreto del Teorema 2.1, que señala que toda puerta unitaria se puede descomponer en puertas de uno y dos qubits. Ese conjunto incluye también las puertas $CNOT_{ij}$ cuando i y j no son consecutivos. Se ha de probar también cómo implementarla. Para ello es importante tener en cuenta el siguiente lema.

Lema 4.1 (SWAP con CNOT)**.** *Sean dos qubits en un estado general $|\psi\rangle$. La operación $CXCX_{21}CX$ es equivalente a cambiar el estado de los dos qubits. Es decir,*

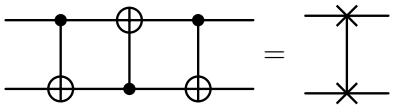
$$CXCX_{21}CX \equiv SWAP$$

Demostración. Se comparan las expresiones matriciales siguientes:

$$CXCX_{21}CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = SWAP.$$

□

A continuación se muestra la representación de la equivalencia anterior:



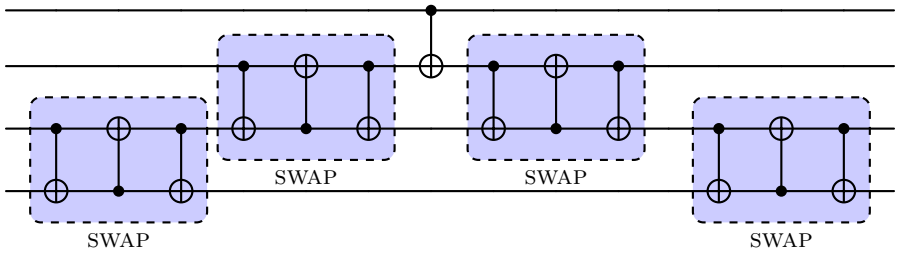
Puerta CNOT no Adyacente

El objetivo es construir una puerta $CNOT_{ij}$ entre los qubits i y j cuando no son consecutivos. Una forma sencilla de implementarlo es utilizando la puerta $SWAP$ [18]. La siguiente proposición sin demostración muestra una forma de implementarla.

Proposición 4.4 (CNOT con SWAP)**.** *Los siguientes pasos implementan la puerta* $CNOT_{ij}$ *con* $i < j$ $(i, j = 1, ...n)$*:*

- *Se emplea la puerta SWAP mediante la descomposición del Lema 4.1 entre los qubits* k *y* $k+1$ *para* $k = j-1, ..., i+1$ *empezando por la última fila y subiendo de una en una.*
- *Se emplea* $CNOT_{i(i+1)}$*.*
- *Se revierte el primer paso, es decir, se emplea la puerta SWAP mediante la descomposición del Lema 4.1 entre los qubits* k *y* $k+1$ *para* $k = i+1, ..., j-1$ *empezando por la segunda fila y bajando de una en una.*

En la siguiente imagen se ve el caso concreto en el que $j - i = 3$:



Nota 4.1. *Se observa que la construcción de la puerta* $CNOT_{21}$ *es tan directa como intercambiar los ángulos de medición de la fila superior e inferior en la celda universal que implementa CNOT. Esto cambiaría el qubit controlador al segundo.*

Esta última observación acerca de cómo construir la puerta $CNOT_{i,j}$ cuando i, j no son consecutivos evidencia que esta forma de probar la equivalencia del modelo MBQC con el modelo de circuitos (a partir de la celda universal del estado brick-work) no es eficiente. Se trata simplemente de una herramienta para demostrar la equivalencia. Más adelante se apuntan unas observaciones acerca de este hecho.

Paso 2: Grafo Lineal con 5 Qubits y $\theta_i = 0$

El segundo paso es probar que la medición de los qubits que no pertenenecen a ninguna celda universal (que se hallan en la primera y última fila) no afecta a la operación global si se miden con un ángulo de 0 radianes.

Proposición 4.5. *El grafo de la Figura 4.7 no modifica el estado inicial* $|\psi\rangle$*.*

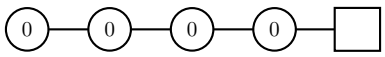


Figura 4.7: Grafo Lineal con 5 Qubits y $\theta_i = 0$.

Demostración. Sea $|\psi\rangle$ el estado inicial. Por el Corolario 3.1, el qubit de salida se halla en el estado

$$H^4 |\psi\rangle = |\psi\rangle$$

□

Se demuestra así que los qubits que no se hallan en ninguna celda universal no transforman el estado cuántico.

Paso 3: Universalidad de un Estado Clúster

Tras las dos últimos pasos, a partir de la Figura 4.2 se ve que el modelo de circuitos y el modelo MBQC son equivalentes. Basta con encontrar la descomposición de cualquier puerta unitaria en el conjunto $\{H, T, CNOT\}$ y sustituir esa descomposición por su correspondiente estado brickwork equivalente, fijando los ángulos de cada celda universal de forma que replique la puerta que se desee.

En algunos casos será preferible implementar la puerta I, pese a que $H^2 = I$. Esto permite reducir el número de qubits auxiliares empleados.

Proposición 4.6. *El grafo de la Figura 4.8 implementa la puerta I identidad en los dos qubits.*

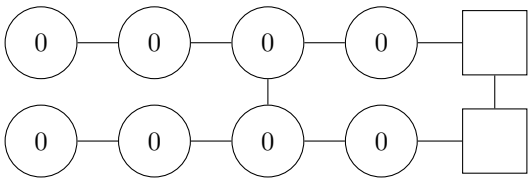
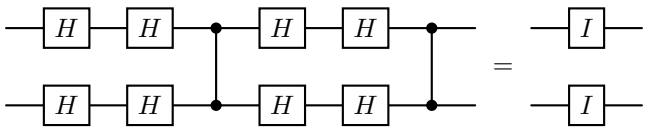


Figura 4.8: Celda del estado brickwork que implementa I en los dos qubits.

Demostración. Se han de sustituir los siguiente ángulos en el caso genérico tratado en la Proposición 3.3 :

- $\alpha = \alpha' = \beta = \beta' = \gamma = \gamma' = \delta = \delta' = 0$.

Por tanto el circuito equivalente al grafo de la Figura 4.8 es



donde se tuvo en cuenta que $H^2 = CZ^2 = I$. □

4.3. Observaciones acerca de la Universalidad del Estado Brickwork

Es necesario apuntar unos comentarios acerca del modelo MBQC. La forma de probar la equivalencia con el modelo de circuitos tiene un carácter genérico, por lo que se evidencian una serie de problemas.

- Un estado brickwork es un estado muy concreto, en el que los entrelazamientos ocurren en columnas que son múltiplos de ciertos números. A la hora de construir físicamente un sistema de qubits, es preferible encontrar disposiciones **simétricas**, como las que se pueden hallar en las disposiciones de átomos en sólidos.

  Es por ello que también existe una demostración de universalidad para estados **clúster**, realizando únicamente mediciones ecuatoriales.

  Originalmente se probó la universalidad para un estado clúster con mediciones en dos planos. Esto no es lo preferible, ya que ciertos protocolos de computación cuántica ciega se basan en mediciones en el plano ecuatorial. Se ahondará en ello en el capítulo 5.

- No es **eficiente** utilizar las equivalencias para cada celda universal. Por ejemplo, dado un qubit en un estado $|\psi\rangle$ al que se le ha de aplicar H, la demostración de la universalidad del estado brickwork requiere el uso de 10 qubits, 8 de ellos auxiliares. Lo más sencillo es realizar una medición en el eje x, de forma que solo se empleen dos qubits. Este caso se vio en el Ejemplo 3.2.

  Otro caso es la puerta $S = T^2$. Es más fácil implementarla con una cadena lineal de 3 qubits que empleando dos celdas para replicar T.

Por ello, más adelante, se verá la equivalencia de la puerta QFT_2 en el modelo MBQC sin usar una distribución fija de los qubits.

4.4. Universalidad de un Estado Clúster

Los qubits no son solo una entidad matemática, sino que se estudian ya que existen sistemas en la vida real que pueden actuar como tales. Para construir un qubit, se emplean distintas estrategias: exiten qubits superconductores, qubits fotónicos, qubits que aprovechan la estructura cristalina de los átomos en un sólido... En general, una malla rectangular como la de un estado clúster es más común en la naturaleza o más sencilla de replicar en un laboratorio que otras mallas gracias a su simetría.

Además, es recomendable limitar las mediciones a un solo plano, tal como se expuso previamente. Esto simplifica el diseño y la aplicación de protocolos de privacidad.

En [7], se demuestra la universalidad de un estado clúester limitando las mediciones al plano ecuatorial. Los detalles se pueden consultar en el documento original. Se utiliza el siguiente conjunto universal:

Lema 4.2. *El conjunto* $\{R_z(\theta), R_x(\theta), R_{z\otimes x}(\theta)\}$ *con* $\theta = [0, 2\pi]$ *es un conjunto de puertas universal.*

Nota 4.2. *Se recuerda la equivalencia* $R_U(\theta) = e^{-i\theta/2U} = \cos\frac{\theta}{2}\mathbb{I} - i\sin\frac{\theta}{2}U$ *aplicable a toda operación unitaria* U *de dimensión arbitraria.*

La demostración de la universalidad se basa en la siguiente proposición [14]:

Proposición 4.7. *Sea un estado clúster abierto de* $n \times (n+2)$ *qubits. Entonces, las siguientes afirmaciones son verdaderas:*

1. *Cuando se mide el qubit* i*-ésimo de la primera columna con un ángulo* θ *en el plano* (X, Y)*, y todos los demás qubits se miden en la base* X *(*$\theta = 0$*), se implementa una rotación* $R_z(\theta)$ *en el qubit* $(n+1-i)$*-ésimo del estado inicial.*

2. *Cuando se mide el qubit* i*-ésimo de la columna* $(n+1)$ *con un ángulo genérico* θ *en el plano* (X, Y)*, y todos los demás qubits se miden en la base* X*, se implementa una rotación* $R_x(\theta)$ *en el qubit* $(n+1-i)$*-ésimo del estado inicial.*

3. *Cuando se mide el qubit* i*-ésimo de la columna* p*-ésima con* $i = 1$ *y* $1 < p < n+1$ *con un ángulo genérico* θ *en el plano* (X, Y)*, y todos los demás qubits se miden en la base* X*, se implementa la puerta* $R_{z\otimes x}$ *en los qubits* $(n-p+1)$*-ésimo y* $(n-p+2)$*-ésimo en el estado inicial. De manera análoga, si* $i = n$*, se implementa la puerta* $R_{z\otimes x}$ *en los qubits* p*-ésimo y* $(p-1)$*-ésimo de entrada.*

Esta proposición se prueba para $m = n + 2$. Este estado se puede entender como una celda, de forma análoga a la celda universal en el estado brickwork. Así, se tiene la universalidad del estado clúster:

Teorema 4.3. *La familia de grafos de estados clúster abiertos de dimensión arbitraria pero finita es universal en el modelo MBQC si se emplean mediciones en el plano ecuatorial. Es decir, toda operación unitaria se puede implementar realizando medidas en el plano $X - Y$ en un estado clúster.*

Además, se puede suponer que el estado inicial es $|+\cdots+\rangle$, ya que cualquier otro estado inicial puede obtenerse a partir de $|+\cdots+\rangle$, y esta operación se puede concatenar con la operación original. De igual forma, se puede suponer que los estados clúster tienen todas las conexiones de entrelazamiento. No ha de ser necesariamente abierto.

Lema 4.3. *La universalidad de los estados clúster abiertos implica la universalidad de los estados clúster.*

Demostración. Sea U operación unitaria de dimensión arbitraria. Por la universalidad de los estados clúster abiertos existen dos grafos (estados clúster abiertos) G_1 y G_2 tal que G_1 implemente $(CZ_{12} \otimes \cdots \otimes CZ_{(n-1)n})U$ y G_2 implemente $CZ_{12} \otimes \cdots \otimes CZ_{(n-1)n}$ en un estado lineal de dimensión el número de filas de G_1. Así, $G_1 \cup G_2$ implementa U, y se puede escribir de forma equivalente como G_1 con la última columna entrelazada. □

Se recogen en un corolario las dos últimas observaciones:

Corolario 4.1. *La familia de grafos de estados clúster abierto de dimensión arbitraria pero finita es universal en el modelo MBQC con las siguientes condiciones:*

- *Se emplean mediciones en el plano ecuatorial.*
- *El estado inicial es $|+\cdots+\rangle$, superposición uniforme de los estados de la base computacional.*

Un ejemplo que incluye el documento [7] es el caso donde el número de filas $n = 2$:

Ejemplo 4.2. *Como ejemplo de aplicación de la Proposición 4.7 se tiene los circuitos de la Figura 4.9.*

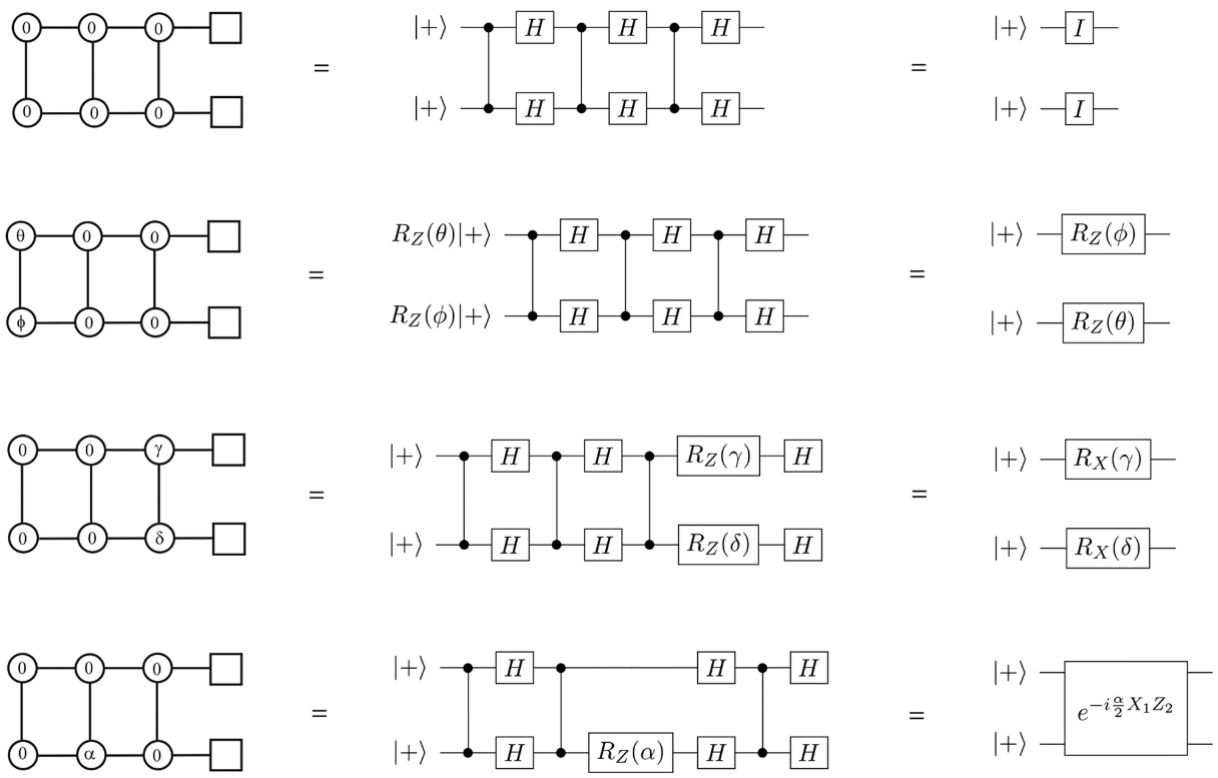


Figura 4.9: Implementación de distintas puertas en un estado clúster abierto de tamaño 2×4 *cuando el input es* $|{+}{+}\rangle$ *[7]*

.

Nota 4.3. *Una de las razones por las que se expone en más detalle la universalidad de los estados brickwork que de los estados clúster es la claridad a la hora de concretar y de ejemplificar en la documentación consultada. En la Figura 4.9, el primer circuito no corresponde a la identidad, sino a la puerta SWAP. Como en este caso* $|{+}{+}\rangle$ *es el ket inicial, SWAP sí actúa como I. Por tanto, tal grafo no valdría para concatenarlo con otro que devolviese un estado* $|\psi\rangle$ *arbitrario.*

4.5. Transformada de Fourier Cuántica

El capítulo se cierra con un ejemplo para ilustrar la universalidad del modelo MBQC. Para ello, se toma el algoritmo QFT. Se verá para el caso concreto $N = 2$, donde el circuito es el de la Figura 4.10. No se empleará ninguna distribución fija (malla concreta), sino que se intenta reducir el número de qubits auxiliares empleados.

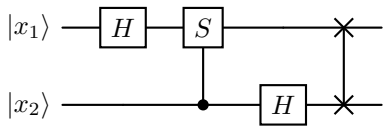


Figura 4.10: Algoritmo QFT con $N = 2$.

Para construir un grafo equivalente en el modelo MBQC, es importante descomponer las puertas utilizadas en aquellas que se puedan implementar de forma directa mediante mediciones. Estas son $R_z(\theta), H$ y CZ.

El primer caso es la puerta CS. Para descomponer CS_{21} es necesario tener en cuenta el Ejemplo 2.8, que muestra la descomposición de una puerta CU. Se ha de buscar A, B, C tal que $ABC = I$ y $e^{i\theta}$ de forma que $S = e^{i\theta}AXBXC$.

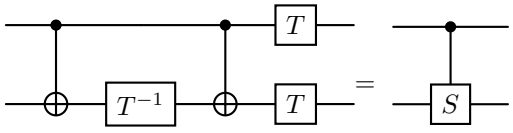
Proposición 4.8. *La descomposición de CS en las condiciones anteriores es $A = T$, $B = T^{-1}$, $C = I$ y $\theta = \pi/4$.*

Demostración. Matricialmente, se tiene que

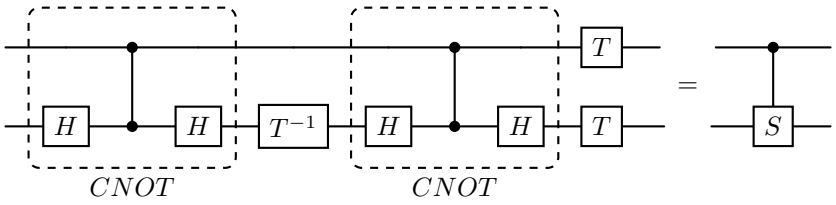
$$e^{i\pi/4}TXT^{-1}X = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = S.$$

□

Con la puerta CS, ocurre un caso similar al de la puerta CZ. Si se invierte el qubit controlador, la expresión matricial es idéntica. Esto ocurre ya que CS solo cambia el estado de la base $|11\rangle$. Por tanto, se tiene la siguiente descomposición:



Aplicar la puerta $CNOT$ mediante el uso de celdas universales no es eficiente, pues se usan 10 qubits en total. Es deseable descomponer $CNOT$ en H y CZ usando la descomposición del Ejemplo 2.5. Así, se da la siguiente equivalencia:



El segundo caso es la puerta $SWAP$, que se puede descomponer en $CNOT$, por tanto, ya se tienen todas las descomposiciones para implementar QFT_2 con $R_z(\theta), H$ y CZ. Así, se podrá obtener un grafo que realice la operación QFT_2 basándose en medidas, de manera que el número de qubits auxiliares no crezca desproporcionadamente.

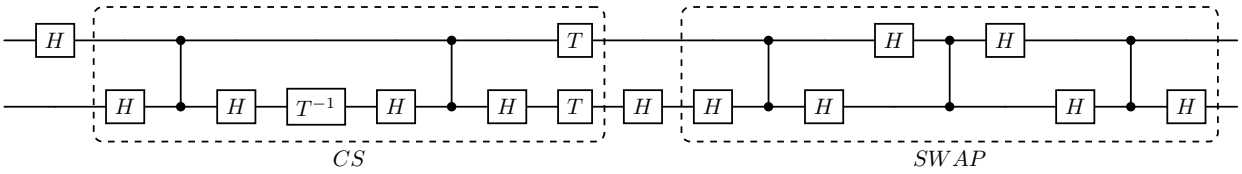


Figura 4.11: Circuito equivalente al de la Figura 4.10 empleando puertas $R_z(\theta), H$ y CZ.

En este punto se han dado todos los pasos para encontrar un grafo equivalente, de forma que la computación sea más eficiente que si se utilizase un estado brickwork o clúster fijo.

Proposición 4.9 (Equivalencia de la puerta QFT_2 en el modelo MBQC.)**.** *La puerta QFT_2 se puede implementar empleando el modelo MBQC mediante el grafo de la Figura 4.12.*

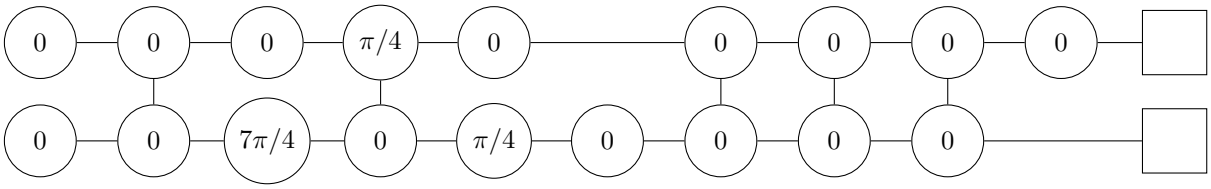
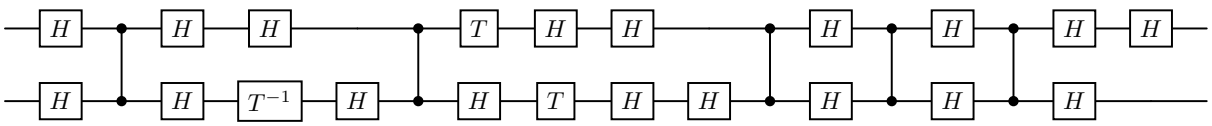


Figura 4.12: Grafo que implementa la puerta QFT_2 con medidas en el plano ecuatorial.

Demostración. Por el Teorema 3.1 y el Corolario 3.1, el circuito equivalente al grafo de la Figura 4.12 es



donde si se simplifican las puertas $H^2 = I$ en aquellos casos en los que es posible, se llega a un circuito equivalente al de la Figura 4.11.

□

Se ha de destacar que en general, al construir un ordenador cuántico, sí se emplean **mallas** o distribuciones fijas. Un ordenador cuántico tendrá los qubits distribuidos de una cierta manera, y una vez constuido, será díficil modificar la estructura. El grafo de la Figura 4.12 no tiene una disposición simétrica, ni tampoco periódica. Es por ello que en la práctica debería de implementarse en una malla rectangular o clúster o en un estado brickwork.

Capítulo 5

Blind Quantum Computing

Se prevé que un futuro, si se consigue construir un ordenador cuántico universal, estos serán limitados en número y no llegarán al público general. Un motivo será el coste de mantenimiento de los mismos. Por ejemplo los transmones, que son qubits basados en la superconductividad, necesitan temperaturas en torno a las centésimas de Kelvin para que se observen efectos superconductores.

En este capítulo, se presenta un protocolo de actuación para que un cliente realice, de forma privada, una operación MBQC en los servidores de un poseedor de un ordenador cuántico. De ahí el nombre de computación cuántica ciega (BQC) o computación cuántica ciega universal (UBQC), puesto que se ha probado que el modelo MBQC es universal. Otro requisito del protocolo es que el cliente no posea acceso a ningún dispositivo de computación cuántica, sino únicamente a ordenadores clásicos.

En este capítulo se expondrá un protocolo concreto, pero se ha de notar que existen variaciones más complejas, con inputs cuánticos e incluso para otros modelos de computación como el modelo de circuitos. También se recuerda que existe una teoría que define con rigor el concepto de privacidad. Para más información se remite a [14] y [17].

5.1. Protocolo de BQC

Sean dos usuarios: un cliente Alice (A) y un servidor Bob (B). Alice quiere realizar una computación MBQC de dimensiones $n \times m$, que se caracteriza por unos ángulos ϕ_{xy} para cada $x \in 1, ..., n$ e $y \in 1, ..., m$ en el plano X-Y, es decir, mediciones respecto al plano ecuatorial. Ya se conoce de capítulos previos que esta configuración

es universal.

El objetivo es realizar esa operación en los qubits de Bob sin que Bob pueda obtener los ángulos concretos de medición, de forma que desconozca la operación concreta. La única información respecto a la operación que Bob conocerá será el tamaño del estado $n \times m$. Esto no supone un problema puesto que la dimensión puede variar añadiendo operaciones que se cancelen mutuamente. Es decir, si se añaden operaciones unitarias equivalentes a la identidad a la operación original se aumenta el tamaño de la malla sin variar el resultado. El protocolo presupone que la distribución de los qubits de Bob es un estado brickwork.

Protocolo de BQC

- **Preparación de Alice:**
  - Para cada columna $x = 1, \ldots, n$ y cada fila $y = 1, \ldots, m$: Alice prepara $|\psi_{x,y}\rangle \in \{|+_{\theta_{x,y}}\rangle = \sqrt{\frac{1}{2}}(|0\rangle + (-1)^{r_{x,y}} e^{i\theta_{x,y}}|1\rangle) : \theta_{x,y} = 0, \frac{\pi}{4}, \ldots, \frac{7\pi}{4}, r_{x,y} = 0, 1\}$, y envía los qubits a Bob.

    Estos estados son escogidos de forma aleatoria por Alice (su ordenador).
- **Preparación de Bob:**
  - Bob crea un estado entrelazado a partir de todos los qubits recibidos, de acuerdo con sus índices, aplicando CZ entre los qubits para crear un estado brickwork.
- **Interacción y Medición:**
  - Para cada columna $x = 1, \ldots, n$ y cada fila $y = 1, \ldots, m$:

1. Alice calcula $\phi'_{x,y}$, que es el ángulo en el que se quiere medir teniendo en cuenta las correcciones por los resultados previos y el valor inicial $\phi_{x,y}$.
2. Alice calcula $\delta_{x,y} = \phi'_{x,y} - \theta_{x,y}$.
3. Alice envía $\delta_{x,y}$ a Bob.
4. Bob mide en la base $\{|+_{\delta_{x,y}}\rangle, |-_{\delta_{x,y}}\rangle\}$.
5. Bob envía el resultado $s_{x,y} \in \{0, 1\}$ a Alice.
6. Si $r_{x,y} = 1$, Alice invierte $s_{x,y}$; de lo contrario, no hace nada.

Proposición 5.1. *El protocolo anterior realiza la operación correcta, es decir, cada qubit (x, y) con $x = 1, \ldots, n$ e $y = 1, \ldots, m$ se mide con respecto a $\phi'_{x,y}$ en el plano ecuatorial.*

Demostración. En la operación original de MBQC, los qubits se inicializan a $|+\rangle$. En este caso, se les aplica una rotación $R_z(\theta_{x,y})Z^{r_{x,y}}$ a cada qubit (x, y). Por el Lema 3.1, esta rotación conmuta con CZ, que se usa para entrelazar los estados previamente.

Por tanto, se tiene que

$$R_z(\theta_{x,y})Z^{r_{x,y}} |+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{r_{x,y}} e^{i\theta_{x,y}} |1\rangle\right).$$

Al medir en la base $\{\left|+_{\delta_{x,y}}\right\rangle, \left|-_{\delta_{x,y}}\right\rangle\}$, se aplica una rotación $R_z(\delta_{x,y})$. Se tiene por tanto que

$$R_z(\delta_{x,y})R_z(\theta_{x,y})Z^{r_{x,y}} |+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{r_{x,y}} e^{i\delta_{x,y}} e^{i\theta_{x,y}} |1\rangle\right) = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{r_{x,y}} e^{i\phi'_{x,y}} |1\rangle\right).$$

Se ha visto que

$$HR_z(\phi'_{x,y})Z^{r_{x,y}} = HR_z(\delta_{x,y})R_z(\theta_{x,y})Z^{r_{x,y}}.$$

Para que sea equivalente a medir en la base $\{\left|+_{\phi'_{x,y}}\right\rangle, \left|-_{\phi'_{x,y}}\right\rangle\}$, si $r_{x,y} = 1$ se ha de cambiar el resultado, o de forma equivalente,

$$s'_{x,y} = s_{x,y} \oplus r_{x,y}$$

siendo $\oplus$ la suma módulo 2 y $s'_{x,y}$ el resultado de la medición corregido. □

Proposición 5.2. *La única información acerca de la operación de Alice de la que Bob está seguro es el tamaño (n, m) del estado. Es decir, la operación de Alice es privada y segura.*

Demostración. Bob recibe para cada (x, y) dos ángulos $\theta'_{x,y}$ y $\delta_{x,y}$, donde $\theta'_{x,y} = (-1)^{r_{x,y}}\theta_{x,y}$. Los dos ángulos pertenecen al conjunto $0, \frac{\pi}{4}, \ldots, \frac{7\pi}{4}$, puesto que $\phi'_{x,y}$ se asume que también pertenece (MBQC es universal con ese conjunto de ángulos). Pero Bob no puede hallar $\phi'_{x,y} = \delta_{x,y} + \theta_{x,y}$, puesto que desconoce $r_{x,y}$. □

En el siguiente ejemplo se ilustra la seguridad del protocolo.

Ejemplo 5.1. *Como ejemplo, dado (x, y) con $x = 1, \ldots, n$ e $y = 1, \ldots, m$, se toma $\phi'_{x,y} = \frac{\pi}{4}$, $\theta_{x,y} = \frac{3\pi}{4}$, $r_{x,y} = 1$. El primero es el ángulo con respecto al que se quiere medir (corregido), los dos últimos fueron elegidos al azar.*

Por tanto, Bob recibe únicamente $\theta'_{x,y} = -\frac{3\pi}{4} = \frac{5\pi}{4}$ *(una rotación de* 2π *es equivalente a no rotar), y* $\delta_{x,y} = \phi'_{x,y} - \theta_{x,y} = \pi$.

Bob sabe que $\delta_{x,y} = \phi'_{x,y} - \theta_{x,y}$ *y que* $\theta'_{x,y} = (-1)^{r_{x,y}}\theta_{x,y}$.

Si intenta hallar $\phi'_{x,y} = \delta_{x,y} + (-1)^{1-r_{x,y}}\theta'_{x,y}$ *se encuentra con dos posibilidades, una para cada* $r_{x,y}$*, que son:*

$$\phi'_{x,y} = \frac{\pi}{4}$$

$$\phi'_{x,y} = \frac{7\pi}{4}$$

Al haber sido escogidas de forma aleatoria hay 2 opciones para $n \times m$ *qubits, es decir,* $2^{n \cdot m}$ *posibles combinaciones de ángulos. Para un estado brickwork del tamaño de* $n = 4$ *y* $m = 13$*, como el de la Figura 4.1, se tiene que:*

$$2^{4 \cdot 13} \simeq 4.5 \cdot 10^{15}$$

Nota 5.1. *La seguridad o privacidad de la operación se obtiene debido a las mínimas posibilidades de hallar la combinación correcta que empleó Alice.*

Conclusiones

El objetivo del trabajo era estudiar la equivalencia del modelo de circuitos con el modelo MBQC. Se han presentado en detalle las características de ambos modelos. Se ha probado además que son equivalentes, y que, por tanto, los dos son universales para computación cuántica. Se concluye por ende que los dos modelos sirven como fundamento para la construcción de algoritmos para computación cuántica. Algoritmos que, gracias a la superposición de estados, podrán modelar sistemas con un número muy elevado de variables; cuya utilidad varía desde problemas de transporte a la simulación del comportamiento de átomos en una batería.

Se añadió además una breve introducción a la computación cuántica ciega o blind quantum computing (BQC) como posible aplicación de lo expuesto en el trabajo. Estos protocolos pueden llegar a ser importantes en un futuro si se construye un ordenador cuántico universal.

En general, se ha intentado exponer los resultados con rigurosidad y justificación, sin dar nada por supuesto, además de añadir múltiples ejemplos para facilitar la comprensión. El más destacable fue la equivalencia del algoritmo QFT en el modelo MBQC. Para la equivalencia del algoritmo de Deutsch Jozsa se utilizó [8].

Dificultades y Aprendizaje

La mayor dificultad a la hora de escribir el trabajo ha sido la consulta de la literatura científica existente con respecto al modelo MBQC. Las fuentes empleadas han sido listadas en la bibliografía.

No se sigue una misma notación ni un mismo criterio en los distintos documentos. En algunos se trasladan las correcciones de Pauli, pero solo para casos concretos [13]. En otros, se omiten sin justificar la razón [7]. No se encuentra un algoritmo genérico para arrastrar estas matrices. Solo en [14] sí se encuentra una explicación de cómo tratar las correcciones. Por eso fue una dificultad entender la razón por la

cual se pueden omitir, y se decidió presentar el trabajo con ese enfoque.

Por otro lado, toda la documentación consultada expone el caso de teleportación de un qubit, pero ninguna trata el caso genérico en el que se tenga un estado entrelazado. Es más, en una malla rectangular (estado clúster) están entrelazados todos los qubits con sus vecinos. El teorema de teleportación de un qubit no tiene aplicación directa para esos casos, pero no se justificaba su uso en mayores dimensiones. En el Teorema 3.2 y su Corolario 3.1 se justifica la teleportación para una columna entrelazada de qubits. Esta justificación es de elaboración propia.

Otra dificultad que se halló fue en la prueba de la universalidad de una malla rectangular, basada en la documentación [7]. Como se comentó en la Nota 4.3, los ejemplos que se hallan en la documentación no sirven para un estado input aleatorio. Sí es verdad que se prueba para cualquier input, pero para unas dimensiones muy concretas y sin aportar ningún ejemplo. Se comenta que se prueba para esas dimensiones sin pérdida de generalidad. Sin embargo, un objetivo que se propuso al pensar el trabajo fue poder escribir la equivalencia de algún algoritmo entre los dos modelos. Al final se hizo con la transformada de Fourier cuántica (QFT). Ese objetivo quizás no se hubiera conseguido si el trabajo se hubiera basado en [7].

También fue necesario aprender a manejar programas de diseño de circuitos como Tikz y CircuiTikz para crear las figuras tanto del modelo de circuitos como del MBQC.

Programas Utilizados

El documento fue escrito en LaTeX. Todas las figuras que no están citadas son de elaboración propia mediante paquetes de LaTeX (Tikz y QuanTikz) [10].

Bibliografía

[1] Michael A Nielsen e Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010.

[2] Evan Jeffrey et al. «Fast accurate state measurement with superconducting qubits». En: *Physical review letters* 112.19 (2014).

[3] David P DiVincenzo. «The physical implementation of quantum computation». En: *Fortschritte der Physik: Progress of Physics* 48.9-11 (2000), págs. 771-783.

[4] M. Castellet e I. Llerena. *Álgebra lineal y geometría*. Reverté, 1991. ISBN: 9788429150094.

[5] *Introductory Functional Analysis with Applications*. Wiley classics library. Wiley India Pvt. Limited, 2007. ISBN: 9788126511914.

[6] D.H. McIntyre et al. *Quantum Mechanics: A Paradigms Approach*. Always learning. Pearson, 2012. ISBN: 9780321798527.

[7] Mantri A., Demarie T. y Fitzsimons J. «Universality of quantum computation with cluster states and (X, Y)-plane measurements.» En: *Sci Rep* 7 42861 (2017). DOI: https://doi.org/10.1038/srep42861.

[8] M Schwetz y RM Noack. «Three-qubit Deutsch-Jozsa in Measurement-Based quantum computing». En: *arXiv preprint arXiv:2306.13372* (2023).

[9] Arute F., Arya K. y Babbush R. et al. «Quantum Supremacy using a Programmable Superconducting Processor». En: *Nature* 574 (2019), págs. 505-510. DOI: https://doi.org/10.1038/s41586-019-1666-5.

[10] Alastair Kay. «Tutorial on the quantikz package». En: *arXiv preprint arXiv:1809.03842* (2018).

[11] Morten Kjaergaard et al. «Superconducting qubits: Current state of play». En: *Annual Review of Condensed Matter Physics* 11 (2020), págs. 369-395.

[12] E.F. Combarro, S. Gonzalez-Castillo y A. Di Meglio. *A Practical Guide to Quantum Machine Learning and Quantum Optimization: Hands-on Approach to Modern Quantum Algorithms*. Packt Publishing, 2023. ISBN: 9781804618301.

[13] Robert B. Griffiths. *Measurement-Based Quantum Computation*. Oxford Research Encyclopedia of Physics. 2021.

[14] Anne Broadbent, Joseph Fitzsimons y Elham Kashefi. «Universal blind quantum computation». En: (2009), págs. 517-526.

[15] Richard Jozsa. «An introduction to measurement based quantum computation». En: *NATO Science Series, III: Computer and Systems Sciences. Quantum Information Processing-From Theory to Experiment* 199 (2006), págs. 137-158.

[16] Michael A Nielsen. «Cluster-state quantum computation». En: *Reports on Mathematical Physics* 57.1 (2006), págs. 147-161.

[17] Joseph F Fitzsimons. «Private quantum computation: an introduction to blind quantum computing and related protocols». En: *npj Quantum Information* (2017), pág. 23.

[18] Beatrice Nash, Vlad Gheorghiu y Michele Mosca. «Quantum circuit optimizations for NISQ architectures». En: *Quantum Science and Technology* (2020).