Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Modelo discreto de computación cuántica con coeficientes enteros

TESIS DOCTORAL

Laura Nina Gatti Dorpich

Ingeniera en Telecomunicaciones (MSc.)

2023

Departamento de Matemática Aplicada a las TIC

Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Modelo discreto de computación cuántica con coeficientes enteros

TESIS DOCTORAL

Laura Nina Gatti Dorpich
Ingeniera en Telcomunicaciones (MSc.)

Jesús García López de Lacalle
Doctor en Ciencias Matemáticas

2023

Tribunal nombrado por el Magnífico Rector de la Universidad

Politécnica de Madrid, el día..... de..... de.....

Presidente: .....

Vocal: .....

Vocal: .....

Vocal: .....

Secretario: .....

Suplente: .....

Suplente: .....

Realizado el acto de defensa y lectura de la Tesis el día..... de.....

de 20..... en Madrid, habiendo obtenido la calificación de .....

El presidente, El secretario, Los vocales,

EL SECRETARIO

A mi familia

Agradecimientos

Quiero agradecer a la Universidad ORT Uruguay por brindarme toda la motivación y financiación necesaria para emprender el doctorado. En particular, expresar mi más sincero agradecimiento al Dr. Efraim Buskman y al Dr. André Fonseca por su inquebrantable apoyo humano y académico desde mi incorporación al grado hasta la finalización de la maestría.

Asimismo, agradezco a la Universidad Politécnica de Madrid por haberme recibido y brindarme la oportunidad de realizar este doctorado. Especialmente, agradezco al director de esta tesis, Dr. Jesús García López de Lacalle, por su transmisión de conocimientos académicos.

Mi gratitud también se extiende a la Universidad de Montevideo por recibirme a mi retorno de Uruguay y brindarme el espacio para desarrollarme en esta área y concluir esta etapa de formación. En particular, quiero agradecer al Dr. Rafael Sotelo por su constante aliento para finalizar este camino.

Por último, quiero dedicar un agradecimiento especial y personal a tres mujeres fundamentales en mi vida, quienes no solo me apoyaron en el desarrollo de mi pericia intelectual, sino que también me brindaron toda la contención emocional para enfrentar los desafíos que este camino implicó. A mi Abuela, que esperó con vida y alegría mi retorno, a mi Madre, por allanarme incondicionalmente el camino en todo momento, y a la profesora Dr. Alfonsa García, quien me adoptó como su hija postiza desde mi llegada y veló por mi bienestar en todo momento.

Resumen

Esta tesis se enmarca en el área de la computación e información cuántica y se centra en el paradigma de la computación cuántica basada en compuertas. El resultado principal es la presentación de un nuevo modelo de computación cuántica discreta basado en solo dos compuertas. Lo más novedoso y atractivo de este modelo es su simplicidad. Los coeficientes de los estados generados por estas compuertas son números complejos con coeficientes enteros, excepto un factor de $\sqrt{2}^p$. Esta característica permite una refinación acumulativa de los estados, según el parámetro p, y lo distingue de otros enfoques de computación cuántica.

A pesar de su aparente simplicidad, el modelo posee características fundamentales que hacen posible la generación de estados con superposición y entrelazamiento, dos conceptos esenciales en la computación cuántica. Además, se demuestra que el modelo presentado es un aproximador universal de cualquier compuerta cuántica. Se proporcionan caracterizaciones de las compuertas que se pueden obtener a partir del modelo, permitiendo identificar de manera inequívoca una compuerta discreta de otra que debe ser aproximada. Para un sistema de dos qubits, se presenta una forma de descomponer toda compuerta discreta como producto de compuertas del modelo más simples y con menor grado de refinamiento.

También se exploran las propiedades matemáticas subyacentes de estos estados, buscando deter -minar las propiedades geométricas que presentan. Se demuestra que, para el espacio de dos qubits, es posible completar una base de vectores propios utilizando un conjunto ortonormal de vectores pertenecientes al modelo discreto, lo cual es un resultado sumamente relevante.

Además, se ha analizado en profundidad la aplicabilidad del modelo y su relación con protocolos importantes de información cuántica, como el protocolo de teleportación y el código superdenso. Es relevante destacar que varios de los estados que se consideran de máximo entrelazamiento en diferentes sentidos son estados discretos, lo que permite el desarrollo completo de protocolos de información cuántica dentro del marco de este modelo.

Asimismo, se ha estudiado la relación entre los algoritmos cuánticos y el modelo discreto. Algunos algoritmos pueden implementarse completamente en el modelo, mientras que otros requieren aproximaciones. Sin embargo, esto no ha impedido que importantes algoritmos, como el algoritmo de búsqueda de Grover, se puedan ejecutar exactamente utilizando las compuertas del modelo, proporcionando valiosas conclusiones sobre ambos.

El modelo de computación cuántica discreta con coeficientes enteros es una propuesta innovadora y sólida que abre nuevas perspectivas en el campo de la computación cuántica. Sus características únicas y su potencial para la implementación de algoritmos importantes lo convierten en un área de investigación prometedora para futuros avances en la ciencia y la tecnología cuánticas.

Abstract

This thesis is framed in quantum computation and information and focuses on the paradigm of quantum computing based on gates. The main result is the presentation of a new model of discrete quantum computation based on only two gates. The most novel and attractive feature of this model is its simplicity. The coefficients of the states generated by these gates are complex numbers with integer coefficients, except for a factor of $\sqrt{2}^p$. This feature allows for a cumulative refinement of the states, depending on the parameter p, and distinguishes it from other quantum computing approaches.

Despite its apparent simplicity, the model possesses fundamental features that make possible the generation of states with superposition and entanglement, two essential concepts in quantum computing. Furthermore, it is shown that the model presented is a universal approximator of any quantum gate. Characterization of the gates that can be obtained from the model are provided, allowing one discrete gate to be unambiguously identified from another to be approximated. For a two-qubit system, a way of decomposing any discrete gate as a product of simpler, less refined model gates is presented.

The underlying mathematical properties of these states are also explored, seeking to determine the geometrical properties they exhibit. It is shown that, for the two-qubit space, it is possible to complete an eigenvector basis using an orthonormal set of vectors belonging to the discrete model, which is a highly relevant result.

In addition, the applicability of the model and its relation to important quantum information protocols, such as the teleportation protocol and the superdense code, have been analyzed in depth. It is relevant to note that several of the states that are maximally entangled in different directions are discrete states, which allows the complete development of quantum information protocols within the framework of this model.

The relationship between quantum algorithms and the discrete model has also been studied. Some algorithms can be fully implemented in the model, while others require approximations. However, this has not prevented important algorithms, such as Grover's search algorithm, from being accurately executed using the gates of the model, providing valuable insights into both.

The discrete quantum computing model with integer coefficients is an innovative and robust approach that opens new perspectives in the field of quantum computing. Its unique features and its potential for the implementation of important algorithms make it a promising area of research for future advances in quantum science and technology.

Índice general

Agradecimientos **VI**

Resumen **VII**

Abstract **VIII**

I Introducción y preliminares **1**

1. Introducción **2**

1.1. Motivación 2

1.2. Objetivos 4

1.2.1. Objetivo general 4

1.2.2. Objetivos específicos 4

1.3. Organización del trabajo 5

2. Introducción a la computación cuántica **7**

2.1. Principios básicos de la computación cuántica 7

2.1.1. Estructura básica de información cuántica: el *qubit* 7

2.1.2. Sistemas de múltiples *qubits* 8

2.1.3. Medidas cuánticas 8

2.1.4. Operadores de densidad 10

2.1.5. Sistemas entrelazados 10

2.1.6. Evolución de sistemas cuánticos 11

3. Modelo de circuitos cuánticos discretizados **15**

3.1. Conjuntos universales exactos: $CNOT$ y las compuertas de un *qubit*. 16

3.1.1. Caracterización de las compuertas de un *qubit*: $\Upsilon(\mathcal{H}^1)$ 16

3.1.2. Matrices controladas de dos *qubits* 17

3.1.3. Construcción de compuertas Toffolis y Toffolis generalizadas. 18

3.1.4. Matrices unitarias cualesquiera 20

3.1.5. Conclusión 22

3.2. Conjuntos discretos de compuertas universales 22

3.2.1. Conjuntos universales. 22

3.2.2. Conjuntos computacionalmente universales. 24

3.2.3. Otros modelos universales. 25

II Modelo de computación cuántica discreta **26**

4. Modelo discreto **27**

4.1. Introducción 27

4.2. Propiedades básicas del modelo 28

4.3. Estados cuánticos discretos 32

4.3.1. Definición del conjunto de estados discretos $\mathcal{E}$ 32

4.3.2. Definición del conjunto E 32

4.3.3. Los conjuntos E y $\mathcal{E}$ son iguales 33

4.3.4. $\mathcal{E} \subseteq E$ 35

4.4. Compuertas cuánticas discretas 36

4.4.1. Definición de compuerta discreta y caracterización 36

4.4.2. Demostración de la reducibilidad en el caso de dos qubits 38

4.4.3. Diferencias con el modelo de Kliuchnikov 42

4.5. Universalidad del modelo 43

4.5.1. Trabajos futuros 43

5. Completitud de bases **45**

5.1. Introducción 45

5.2. Principales resultados relacionados con el problema de los cuatro cuadrados de Lagrange 48

5.3. Versión ortogonal del teorema de los cuatro cuadrados de Lagrange 49

5.3.1. Demostración Caso 4: dos vectores $p-$ortonormales con soporte de tamaño > 2 50

5.4. Generalizaciones 58

5.4.1. Propiedades estructurales del problema 59

5.4.2. Extensiones ortogonales 59

5.4.3. Conjetura sobre estados discretos 60

III Aplicabilidad del modelo **61**

6. Entrelazamiento **63**

6.1. Importancia del entrelazamiento 64

6.1.1. Sistemas conformados por dos qubits: estados de Bell 64

6.1.2. Sistemas conformados por tres qubits: GHZ, W y sus generalizaciones 65

6.1.3. Sistemas conformados por más de tres qubits 67

6.2. Principales protocolos de información cuántica 69

6.2.1. Teleportación cuántica 69

6.2.2. Código Superdenso 71

7. Aplicación del modelo a algoritmos cuánticos **73**

7.1. Algoritmo de Deutsch-Jozsa 74

7.2. Quantum Fourier Transform 75

7.3. Algoritmo de Grover 77

7.3.1. Descripción del algoritmo de Grover 78

7.3.2. Algoritmo de Grover sobre el conjunto discreto E 79

7.3.3. Crecimiento del nivel de refinamiento y el algoritmo de Grover. 81

7.4. Interpretación 88

IV Conclusiones **90**

8. Conclusiones **91**

A. Conceptos matemáticos **94**

A.1. Espacios de Hilbert 94

A.2. Operadores en el espacio de Hilbert 95

A.3. Producto tensorial de espacios vectoriales. 99

A.4. Sistemas y su interacción con el entorno 101

A.5. Información Cuántica 104

B. Demostraciones complementarias a completitud de bases **108**

B.1. Producto de tres vectores de dimensión cuatro 108

Índice de figuras

7.1. Hiperplano correspondiente al algoritmo de Grover, formado por $|t\rangle$ y $|\bar{t}\rangle$. 79

7.2. Crecimiento del nivel de refinamiento en función del número de iteraciones del algoritmo de Grover para distintos números de qubits. 89

7.3. Nivel de refinamiento en la iteración óptima de Grover según la cantidad de qubits utilizados. . 89

Índice de tablas

5.1. Datos de forma cuasi-normal de Smith. 53

5.2. Monomios de $\det(V)c_1c_2cd$. 54

5.3. Monomios resultantes de las operaciones. 55

5.4. Monomios de $N(w_1)c_1^2c_2^2d_1^2$ y resultantes de las operaciones. 56

Parte I

Introducción y preliminares

Capítulo 1

Introducción

1.1. Motivación

Puede decirse sin equivoco que es el momento de la Computación Cuántica **QC**. Las líderes de las Big Tech, como Amazon, IBM, Google, Microsoft y Alibaba, se han adentrado en la experimentación del mundo de la **QC**. Según la consultora McKinsey & Company [1], el esfuerzo mundial en investigaciones concernientes a las tecnologías cuánticas supera los 36 mil millones entre inversiones públicas y privadas. Se espera que para 2040 el mercado global de tecnologías cuánticas alcance los 106 billones.

Los titulares sobre **QC** inundan las revistas de divulgación científica, industrial y económica. Se da cuenta de ampulosas promesas acerca de lo que se podrá alcanzar con la misma, así como las potencialmente catastróficas consecuencias de su realización. El día en que la **QC** sea suficientemente potente, el sistema de encriptación en el que sustenta el algoritmo de clave pública privada caerá. Teóricamente, las computadoras cuánticas pueden resolver en tiempos irrisorios un problema que hoy, en los mejores centros de supercomputo, aún llevaría varios miles de años: descomponer un número gigantesco en sus factores primos.

Los orígenes de la **QC** se remontan a mediados de la década de 1980, con la propuesta puramente teórica de Richard Feynman [2, 3] de utilizar la evolución de sistemas cuánticos como una herramienta de cálculo en sí misma. En ese momento, el poder de cómputo no era suficiente para simular de manera realista sistemas cuánticos mínimamente complejos. Hasta el día de hoy, y a pesar del increíble avance en la capacidad de cómputo clásico, sigue siendo imposible realizar tales simulaciones. La idea original de Feynman era unir dos mundos previamente separados: la mecánica cuántica y la ciencia de la computación junto con la teoría de la información y la criptografía. La novedad que propuso fue que la descripción y evolución de la computación estaría regida por las inusuales leyes de la física cuántica.

El desarrollo teórico de la **QC** tuvo avances significativos desde el principio. Ya en 1985, gracias a David Deutsch [4], se contaba con un marco formal completo y comprensible del concepto de Computación Cuántica. Esto permitió comprender la gran ventaja de este nuevo tipo de computación: al estar regido por las leyes de la mecánica cuántica, podría aprovechar recursos de su propia naturaleza, como la superposición de estados y el entrelazamiento. Estos dos fenómenos permitirían procesar información en paralelo [5] de una manera completamente nueva en comparación con la Computación Clásica (**CC**), obteniendo una capacidad de cómputo netamente superior a la que se puede lograr clásicamente.

Para 1997, ya se conocían dos algoritmos fundamentales que evidenciaban la supuesta ventaja cuántica. Uno de ellos es el algoritmo cuántico para implementar la Transformada Discreta de Fourier (DFT) [6, 7]. Este algoritmo, a su vez, permite implementar el algoritmo de Shor (1997) [8] para descomponer números enteros en factores primos, con una ganancia exponencial de tiempo en comparación con su contraparte clásica. El otro algoritmo fundamental es el algoritmo de búsqueda de Grover [9]. Este algoritmo de búsqueda cuántica proporciona una ganancia cuadrática en compara -ción con el mejor algoritmo de búsqueda exacta en una base desordenada que se puede implementar de manera clásica.

Esto contrastaba notablemente con las implementaciones experimentales de estos algoritmos, ya que el soporte físico necesario para la implementación de estas interacciones cuánticas presentaba importantes desafíos para la tecnología disponible. El equipo de IBM logró implementar un algoritmo de Shor utilizando técnicas de Resonancia Magnética Nuclear (RMN) en núcleos de espín 1/2, logrando factorizar el número 15 como 3 x 5 [10]. Para 2012, utilizando nuevas técnicas de RMN sobre cristal líquido, el número más grande que se había podido factorizar era 143 [11].

En 2016, IBM ofreció los primeros prototipos de computadoras cuánticas a través de acceso remoto, permitiendo su uso bajo demanda por parte de investigadores e interesados en el tema. Esto representó un soplo de aire fresco para un campo en el que el desarrollo teórico seguía expandiéndose, pero en la mayoría de los casos, carecía de la posibilidad de contrastar resultados mediante experimen -tos. El año 2016 marcó un periodo de renovada esperanza en esta tecnología, en medio de una creciente urgencia por encontrar nuevas formas de ampliar los límites de la capacidad de cómputo.

La Ley de Moore, propuesta por primera vez en 1970 [12], predijo que aproximadamente cada dos años se duplicaría el número de transistores en un circuito integrado. Esto implicaba que se debía reducir cada vez más el tamaño de los componentes integrados, lo que finalmente llevaría a un límite natural: cuando las pistas conductoras fueran del tamaño de los átomos componentes. Si bien la Ley de Moore se ha mantenido en general hasta ahora, se está haciendo evidente que la realidad de un límite físico se acerca. Los efectos cuánticos debido al tamaño de los transistores ya no pueden ser ignorados y tendrán un impacto significativo en el funcionamiento normal de la electrónica si continuamos reduciendo el tamaño de los transistores.

La Computación Cuántica representa un nuevo paradigma de cómputo que tiene el potencial de expandir significativamente los límites de la computación. Como paradigma emergente, enfrenta el desafío no solo de igualar la potencia de cálculo de las computadoras clásicas, sino también de superarla, de manera que sea justificable cuestionar el conocimiento establecido en torno a las computadoras clásicas. Estas últimas tienen un sólido marco teórico y una implementación física arraigada en nuestra vida cotidiana.

Esta tarea es enormemente desafiante. En un primer lugar, como se ha discutido previamente, el soporte físico plantea importantes desafíos tecnológicos debido a la complejidad de manipular la materia a nivel cuántico con las capacidades actuales. En segundo lugar, el desarrollo teórico de la **QC** también presenta sus propios retos. Como Shor notó en 2002 [13], encontrar algoritmos cuánticos efectivamente superiores a los clásicos es extremadamente difícil. Esto se debe a que nuestra forma de pensar está mucho más adaptada a la computación y al mundo clásico que al cuántico. Existen diferencias fundamentales entre la manipulación de información cuántica y la clásica. Ejemplos significativos de estas diferencias incluyen el teorema de no clonación para estados cuánticos, que impide operaciones de *fan-in* y *fan-out*, así como el hecho de que todas las transformaciones aplicadas a estados cuánticos deben ser reversibles, lo que hace imposible la realización de compuertas lógicas clásicas como la compuerta *AND*, a modo de ejemplo.

La obtención de resultados en algoritmos cuánticos es un proceso que conlleva sus propias dificultades. Mientras que en el mundo clásico, la perturbación causada por la medición de un sistema se puede considerar insignificante, en el mundo cuántico la situación es diferente. La operación de

medición destruye el estado cuántico y el resultado de la medición es, en general, incierto, y está asociado con la probabilidad de proyección del estado. Cualquier pequeña perturbación en el estado inicial del sistema puede dar lugar a probabilidades no nulas de obtener un resultado incorrecto al realizar la medición. Esto significa que no es posible simplemente repetir la medición para obtener el resultado correcto, ya que la medición destruye el estado medido de una forma irreparable. En cambio, es necesario comenzar el experimento desde el principio para tener la oportunidad de obtener la solución correcta. Esto subraya la sensibilidad de los sistemas cuánticos a las perturbaciones y la importancia de controlar y mitigar cualquier fuente de error en los algoritmos cuánticos.

Esta tesis propone estudiar desde un punto de vista teórico la posibilidad de desarrollar modelos simplificados de **QC** en los cuales no todas las formas de interacción estén permitidas. Las simplifica -ciones casi siempre resultan en una pérdida de amplitud y coherencia en comparación con la teoría original. Sin embargo, en ocasiones y con suerte, estas simplificaciones pueden arrojar luz sobre aspectos particulares que son difíciles de percibir en el contexto general.

1.2. Objetivos

1.2.1. Objetivo general

El objetivo general de esta tesis es proponer y desarrollar un nuevo modelo de computación cuántica discreta con coeficientes enteros que permita la generación de estados con superposición y entrelazamiento, y que sea universal para aproximarse a cualquier compuerta cuántica. El modelo busca simplificar la representación de estados cuánticos y explorar sus propiedades matemáticas subyacentes para comprender mejor su comportamiento y aplicabilidad en diversos protocolos de información cuántica.

1.2.2. Objetivos específicos

Los objetivos específicos fueron determinados de forma que posibilitaran el desarrollo de la investigación considerando el objetivo principal. Estos son:

- Presentar una introducción detallada a la computación cuántica y los fundamentos de los modelos discretos de computación cuántica basados en compuertas, estableciendo una base teórica sólida para el desarrollo del nuevo modelo propuesto.
- Diseñar y desarrollar el nuevo modelo de computación cuántica discreta con coeficientes enteros basado en solo dos compuertas, estableciendo las reglas y propiedades que definen su funciona -miento y capacidad para generar estados cuánticos con superposición y entrelazamiento.
- Demostrar la universalidad del modelo, mostrando cómo puede aproximarse cualquier compuerta cuántica estándar mediante el uso de las compuertas del modelo y proporcionando caracteriza -ciones claras de las compuertas que se pueden obtener exactamente y las que deben aproximarse.
- Investigar y analizar las propiedades matemáticas de los estados generados por el modelo, buscando determinar las propiedades geométricas y estructurales de los espacios de vectores resultantes, especialmente en el caso de dos qubits.
- Explorar la aplicabilidad del modelo en protocolos importantes de información cuántica, como el protocolo de teleportación y el código superdenso, identificando estados discretos que permitan el desarrollo completo de estos protocolos dentro del marco del modelo.

- Estudiar la relación entre los algoritmos cuánticos y el modelo discreto, analizando qué algoritmos pueden implementarse completamente en el modelo y cuáles requieren aproximaciones, con un enfoque particular en el algoritmo de búsqueda de Grover.
- Proponer posibles líneas futuras de investigación relacionadas con el modelo de computación cuántica discreta con coeficientes enteros, identificando áreas de mejora y expansión, y destacando posibles aplicaciones prácticas de este modelo en la resolución de problemas complejos en computación cuántica.

1.3. Organización del trabajo

A continuación se describe la estructura de esta tesis por capítulos, comentando las principales contribuciones realizadas:

- **Parte I. Introducción y preliminares.**
  - **Capítulo 1. Introducción.**
    Presentación del presente trabajo, objetivos y contenidos.
  - **Capítulo 2. Fundamentos de la computación e información cuántica.**
    Se realiza una introducción al tema de la computación cuántica en general. Se presentan los cuatro postulados básicos en los que se basa y se desarrolla más en profundidad las herramientas matemáticas necesarias para comprender esta tesis
  - **Capítulo 3. Fundamentos de los modelos discretos de computación cuántica.**
    En este capítulo se hace un breve resumen de las principales herramientas y resultados que se conocen para la discretización de modelos de computación cuántica basada en compuertas.
- **Parte II. Modelo de computación cuántica discreta con coeficientes enteros.**
  - **Capítulo 4. Modelo de computación cuántica discreta con coeficientes enteros.**
    En este capítulo se presenta un nuevo modelo de computación cuántica basada en dos únicas compuertas. Pese a su simplicidad este modelo permite construir estados que respetan dos de las principales características de la computación cuántica, la superposición y el entrelazamiento. La principal característica de este modelo es que los coeficientes de los estados que pueden ser generados por el mismo son todos números complejos con coeficientes enteros salvo un factor de $\sqrt{2}^p$. Se prueba que este modelo puede ser entendido como un modelo acumulativo en la refinación del mismo dependendiendo del parámetro p y finalmente se prueba la universalidad del mismo
  - **Capítulo 5. Completitud de bases.**
    Se explora aquí las propiedades matemáticas del espacio de vectores resultantes del modelo de computación cuántica discreta. Para el espacio de cuatro qubits se muestra que, dado un conjunto ortonormal de vectores $|\varphi\rangle_i$ pertenecientes al modelo discreto con $1 \leq i \leq 3$, se puede completar una base de vectores propios. Se hacen también conjeturas para dimensiones más altas.
- **Parte III. Aplicabilidad del modelo.**
  - **Capítulo 6. Entrelazamiento.** En este capítulo se exploran las principales conexiones que tiene el modelo de estados de coeficientes enteros con algunos de los protocolos más importantes de la información cuántica como el protocolo de teleportación y el

código superdenso. Es de especial relevancia que varios de los estados que se suponen de máximo entrelazamiento en alguno de todos los sentidos posibles, son estados discretos y por tanto los protocolos de información cuántico más destacados pueden desarrollarse completamente dentro del modelo.

- **Capítulo 7. Algoritmos.** Aquí se presentan los principales algoritmos de la computación cuántica y su relación con el modelo discreto. Mientras que algunos pueden desarrollarse completamente dentro del modelo, otros no. En particular el algoritmo de Shor, uno de los más importantes, para ser utilizado dentro del modelo debe aproximarse. Sin embargo otro importante algoritmo, como lo es el de búsqueda de Grover, puede implementarse exactamente utilizando compuertas del modelo. Esto permite extraer importantes conclu -siones del algoritmo y del modelo mismo.

- **Parte IV. Conclusiones.**

  - **Capítulo 8. Conclusiones.**
    En este capítulo se exponen las conclusiones del trabajo de tesis, incluyendo posibles líneas futuras de investigación.

- **Apéndices.**

  - **Apéndice A. Propiedades Matemáticas y resultados de teoría de la información.**
    En esta sección se encuentran las herramientas matemáticas y de teoría de la información cuántica que completan la descripción de los cuatro postulados de la mecánica cuántica adaptados a la computación cuántica
  - **Apéndice B. Demostraciones complementarias a completitud de bases**
    Se demuestra el caso 2: dos vectores $p-$ortonormales con soporte de tamaño 2.

Capítulo 2

Introducción a la computación cuántica

Se presenta el modelo de computación cuántica bajo el paradigma de los circuitos cuánticos basados en compuertas. Se esquematiza su marco teórico natural ya conocido, haciendo especial énfasis en la existencia de modelos universales finitos.

2.1. Principios básicos de la computación cuántica

2.1.1. Estructura básica de información cuántica: el *qubit*

Como la estructura básica de la **CC** es el bit que puede tomar los valores lógicos 0 o 1, la estructura básica de información en la **QC** es el *qubit*. Los *qubits* son vectores de un espacio vectorial bidimensional donde $\{|0\rangle, |1\rangle\}$ es una base ortonormal y se considera válido como estado lógico cualquier combinación lineal compleja normalizada de estos elementos de la base, es decir un *qubit* cualquiera $|\psi\rangle$ se representa de la forma $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1$.

En general se asocia a $\{|0\rangle, |1\rangle\}$ con los vectores de la base canónica de un espacio de Hilbert $\mathcal{H}$ (ver apéndice A.1):

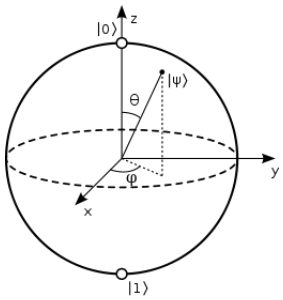
$$\text{donde } |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \; y \; |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

A esta base se la conoce como base computacional. Sin embargo la computacional no es la única base relevante, la base $\{|+\rangle, |-\rangle\}$ es otra muy utilizada, donde $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ y $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Al ser los *qubits* estados normalizados (todos de norma 1) se los puede visualizar como puntos sobre la esfera unitaria. Una notación muy útil es la esfera de Bloch:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \text{ donde } \gamma, \varphi, \theta \in \mathbb{R}$$

Al no tener efectos observables, la fase global $e^{i\gamma}$ se puede obviar. Es interesante observar que los elementos de la base computacional $\{|0\rangle, |1\rangle\}$ son el polo norte y sur de la esfera respectivamente. Estados ortogonales son antípodas en la esfera de Bloch.



2.1.2. Sistemas de múltiples *qubits*

Como en la **CC**, en la **QC** es necesario el manejo de sistemas compuestos por múltiples *qubits*. La herramienta matemática utilizada para la representación de estos sistemas es el producto tensorial, más concretamente, el producto de Kronecker para el espacio de matrices complejas que se detalla en A.3.1.

A modo de ejemplo veamos que a partir de $\{|0\rangle, |1\rangle\}$, la base computacional, podemos obtener la base computacional de $\mathcal{H} \otimes \mathcal{H} = \mathcal{H}^2$ como el conjunto de todos los posibles productos de la forma $\{|i\rangle \otimes |j\rangle\}_{\substack{0 \leq i \leq 1 \\ 0 \leq j \leq 1}}$. Por ejemplo:

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle.$$

Análogamente se obtienen $|01\rangle, |10\rangle$ y $|11\rangle$ siendo entonces $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ la base computacional de $\mathcal{H}^2$. [1]

En este punto se puede destacar las dos grandes diferencias que tiene la **QC** respecto a la **CC**. Los estados en los que se pueden encontrar un bit son el 0 o el 1, mientras que en la **QC** esencialmente un *qubit* se puede encontrar en alguno de los infinitos estados, $|0\rangle$, $|1\rangle$, o en cualquier superposición continua de los anteriores. Desde el punto de vista de teoría de la información esto implicaría que en un qubit se podría almacenar infinita información. Como se verá esto no es cierto ya que no toda la información que almacena un *qubit* es accesible. Para entender qué quiere decir esto es necesario entender qué es y qué implica medir un estado bajo el paradigma de la mecánica cuántica.

2.1.3. Medidas cuánticas

En el entorno de la mecánica cuántica medir implica colapsar el estado: debido a la interacción con el aparato de medida y el ambiente, el sistema está abierto y el proceso de medición no resulta un proceso unitario. A modo ilustrativo: dada la base en la que se medirá, el proceso de medida retornará algún estado de dicha base elegida . Esto es: dado el estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ al medirlo en la base computacional se obtendrá $|0\rangle$ con probabilidad $|\alpha|^2$ o $|1\rangle$ con probabilidad $|\beta|^2$.

Esto implica que el estado original es destruido irremediablemente. A priori se podría suponer que haciendo suficientes copias de un estado desconocido $|\psi\rangle$ se podría hacer un estudio estadístico para

[1] Aunque la dimensión del espacio de Hilbert que se está considerando tiene dimensión 2^2 se notará por simpleza $\mathcal{H}^2$. En general si se trabaja en un espacio de n qubits la dimensión del espacio de Hilbert asociado será 2^n, pero se lo notará como $\mathcal{H}^n$ haciendo referencia a la cantidad de qubits que intervienen dando por sobrentendido que la dimensión es 2^n.

obtener información sobre éste. Esto no es posible. Existe en cuántica el teorema de no clonación cuyo enunciado asegura que no existe ningún procedimiento por el cual pueda copiarse un estado cuántico desconocido arbitrario de un sistema a otro sistema idéntico (salvo el caso de que sean estados ortogonales de una base conocida). Esto es: no se pueden hacer copias de $|\psi\rangle$.

En general el proceso de medición en cuántica se modela matemáticamente mediante una colección de operadores de medida $\{M_m\}$ que actúan sobre el espacio de los estados a medir y deben cumplir $\sum_m M_m M_m^\dagger = I_d$ [2] (relación de completitud). El subíndice m refiere a los posibles resultados que se obtienen con una probabilidad p_m una vez efectuada la medida. Si el estado de un sistema cuántico es $|\psi\rangle$ inmediatamente antes de ser medido, la probabilidad de obtener el resultado m es

$$p(m) = \langle\psi|{M_m}^\dagger M_m|\psi\rangle$$

y el estado del sistema luego de la medición será

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|{M_m}^\dagger M_m|\psi\rangle}}$$

La relación de completitud asegura que las suma de las probabilidades p_m de los diferentes sucesos da 1.

Un caso particular de medida son las medidas proyectivas: dada una base ortonormal $\{|u_1\rangle, ..., |u_n\rangle\}$, se definen los proyectores:

$$\Pi_1 = |u_1\rangle\langle u_1|, ..., \Pi_n = |u_n\rangle\langle u_n|.$$

Estos proyectores son una colección de operadores de medida ya que cumplen la relación de completitud. Además son operadores hermíticos, es decir $\Pi_i = \Pi_i^\dagger$, y cumplen que $\Pi_i^2 = \Pi_i$. En este caso particular la probabilidad de obtener, después de medir en esa base, el estado $|u_m\rangle$, partiendo del estado $|\psi\rangle$ es igual a

$$p_m = \langle\psi|\Pi_m\Pi_m^\dagger|\psi\rangle = p_m = ||\Pi_m\psi||^2,$$

y el estado luego de la medida será:

$$|\psi\rangle' = \frac{\Pi_m|\psi\rangle}{\sqrt{p_m}}$$

Otro conjunto de operadores de medida importantes son los POVM, que también utilizan proyec -tores pero estos no tienen porqué ser ortogonales entre si, como ocurre en el caso de las medidas proyectivas.

En definitiva, al medir un estado cuántico éste colapsa con una determinada probabilidad a alguno de los finitos estados definidos por los operadores de medida. Ahora bien, se puede interpretar de otra manera el resultado de medir el estado. Si se realiza la medición, pero no se observa el resultado obtenido, puede suponerse que el estado se encuentra en una superposición de todos los estados de salida posibles ponderados por sus probabilidades de ocurrencia.

Este enfoque del resultado de una medición puede ser ampliado a otros escenarios en los que el estado exacto no sea conocido, escenarios que no incluyan necesariamente una medida. Por ejemplo, en la preparación de un estado se tiene que poder modelar errores, como que el estado preparado no sea exactamente el estado $|\psi\rangle$ que se quiere sino que con una cierta probabilidad el estado que en realidad se prepare sea cierto $|\varphi\rangle$. En definitiva, lo que se pretende es modelar cierto grado de incertidumbre sobre el estado. El estado no está completamente determinado, por lo tanto se lo modela mediante un conjunto de estados con una distribución de probabilidades.

[2] I_d denota a la matriz identidad del espacio de Hilbert que se este considerando. La notació † nota al vector transpuesto y conjugado, ver A.1.

2.1.4. Operadores de densidad

Para incluir esta clase de sistemas cuánticos se tiene una formulación equivalente que en vez de utilizar vectores para describir estados utiliza *operadores de densidad* o *matrices de densidad*: dado un conjunto de estados cuánticos $|\varphi_i\rangle$ y una probabilidad p_i asociada a cada estado del conjunto, se define al **estado mezcla** ρ a partir del conjunto $\{p_i, |\varphi_i\rangle\}$ como el operador

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i| \quad con \;\; p_i \geq 0 \; y \; \sum_i p_i = 1$$

Si $\#\{i\} = 1$ (se tiene un único elemento en el conjunto) utilizar una u otra representación es indistinto ya que estamos frente a un estado puro. En cualquier otro caso estamos frente a un estado mezcla. Matemáticamente para diferenciar un caso de otro se cuenta con el siguiente resultado: dado un operador de densidad se demuestra que $tr(\rho^2) \leq 1$ y $tr(\rho^2) = 1$ si y solo si ρ es el operador de densidad asociado a un estado puro.

Es importante tener en cuenta que dos conjuntos diferentes $\{p_i, |\varphi_i\rangle\}$ y $\{p_j, |\psi_j\rangle\}$ pueden tener asociada la misma matriz de densidad. Por ejemplo para los estados cuánticos $|\psi\rangle = \sqrt{\frac{3}{4}}|0\rangle + \frac{1}{2}|1\rangle$ y $|\varphi\rangle = \sqrt{\frac{3}{4}}|0\rangle - \frac{1}{2}|1\rangle$, es fácil corroborar que los conjuntos $\{(0.5, 0.5),\ (|\psi\rangle, |\varphi\rangle)\}$ y $\{(0.75, 0.25),\ (|0\rangle, |1\rangle)\}$ son el mismo estado cuántico:

$$\rho = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\varphi\rangle\langle\varphi| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| = \begin{bmatrix} 3/4 & 0 \\ 0 & 1/4 \end{bmatrix}$$

Además es fácil de chequear que $tr(\rho^2) = \frac{5}{8} < 1$.

Los conjuntos anteriores pueden provenir de dos experimentos diferentes, pero una vez que se llega al punto de modelar el sistema como esta matriz de densidad, al ser estas idénticas, es imposible determinar de qué experimento provino.

2.1.5. Sistemas entrelazados

Dados los estados $|\psi\rangle$ y $|\varphi\rangle \in \mathcal{H}^2$ ambos puros, combinación lineal de los elementos de la base computacional de $\mathcal{H}^2$, de norma unitaria

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle \quad \text{y} \quad |\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

es fácil comprobar que $|\varphi\rangle$ es el producto tensorial de los estados $|\varphi_1\rangle = |0\rangle$ y $|\varphi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ de $\mathcal{H}$, $|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$, mientras que es imposible encontrar $|\psi_1\rangle$ y $|\psi_2\rangle \in \mathcal{H}$ tal que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

Los estados que no se pueden obtener como producto tensorial de estados de un *qubit* se denominan **entrelazados**. La existencia de estados entrelazados (la inmensa mayoría) es, junto con la superposición de estados, la causante de toda la potencia de la **QC**. Por ello es importante ilustrar sus implicaciones.

Si se toman como operadores de medida en $\mathcal{H}^2$ a $\Pi_0 = |0\rangle\langle 0| \otimes I_1$ y $\Pi_1 = |1\rangle\langle 1| \otimes I_1$ (cumplen condición de completitud), al aplicarlos a $|\varphi\rangle$ se obtiene con probabilidad 1 el estado $|0\rangle \otimes |\varphi_2\rangle = |\varphi\rangle$ y con probabilidad 0 el estado $|1\rangle \otimes |\varphi_2\rangle$. En definitiva se obtiene el estado puro original. Sin embargo al aplicarlos a $|\psi\rangle$ se obtiene con probabilidad $\frac{1}{2}$ el estado $|00\rangle$ y con probabilidad $\frac{1}{2}$ el estado $|11\rangle$.

Al aplicar estos operadores de medida lo que se está haciendo es medir en la base computacional el primer *qubit* del sistema compuesto. En el primer caso como los dos *qubits* no están entrelazados medir el primero no afecta al segundo, y como el primero es efectivamente $|0\rangle$ la medida no afecta al estado. En el segundo caso la situación es radicalmente diferente, al estar entrelazado, medir el primer qubit afecta al segundo, esto es: si el resultado de medir el primero es $|0\rangle$ obliga al segundo a tomar este mismo valor, lo mismo si el primero resulta ser $|1\rangle$.

Cuando dos estados están entrelazados no pueden verse como dos sistemas separados, y toda acción que afecte a uno inevitablemente afectará al otro, ya que son un mismo sistema. Este concepto es el que en cuántica permite el fenómeno de telesportación cuántica [14], entre otros.

Para sistemas de más de dos qubits nos puede interesar que sean biseparables, triseparables o n-separables. Un concepto más general que implica todas las particiones posibles es el de **totalmente separable**. Esto ocurre cuando un estado de n-qubits se puede descomponer como el producto de n estados de un qubit: $|\psi\rangle = \bigotimes_{i=1}^{n} |q_i\rangle$ con $|q_i\rangle \in \mathcal{H}$.

Dado que los estados mezcla son una suma convexa de estados puros, una idea primaria para extender este concepto consiste en pedirle a todos los estados componentes puros que sean totalmente separables. Esta es, en definitiva, la definición de separabilidad para estados mezcla: se dice que un estado representado por su matriz de densidad ρ_0 es un estado **totalmente separable** si existe una representación tal que:

$$\rho_0 = \sum_i p_i \rho_{s_i} \text{ donde } p_i \geq 0 \ \forall i \text{ y } \sum_i p_i = 1$$

donde ρ_{s_i} son estados puros no entrelazados.

Existe otro concepto más débil que el anterior, relacionado también con la idea de separabilidad. Es el de estados **no-correlacionados**: decimos que un estado representado por su matriz de densidad $\rho_0 \in \Lambda(\mathcal{H}^n, \mathcal{H}^n)$ es un estado no-correlacionado si se puede descomponer la matriz como:

$$\rho_0 = \bigotimes_{i=1}^{n} \rho_{qi} = \rho_{q1} \otimes \rho_{q2} \otimes ... \otimes \rho_{qn} \quad \text{siendo } \rho_{qi} \text{ matriz de densidad de 1 qubit.}$$

Si bien cuando se consideran los estados puros los conceptos de estados separables y no-correlaciona -dos coinciden, no ocurre así cuando se considera estados mezcla. Que un estado sea no-correlacionado implica que es separable, pero no ocurre al revés: existen estados que son separables pero no son no-correlacionados.

2.1.6. Evolución de sistemas cuánticos

Una vez considerados la representación de los sistemas cuánticos se vuelve imperativo dar el modelo que describe la evolución de estos sistemas, ya que si se quiere computar con estos estados es necesario poder determinar su evolución para poder tener algoritmos.

La mecánica cuántica provee el mecanismo para modelar la evolución de un sistema cuando esté es cerrado (no hay interacción con el entorno). Dado el Hamiltoniano H (operador hermítico), la evolución del sistema queda determinado por la ecuación de Schrödinger

$$i\frac{d\rho}{dt} = H\rho - \rho H,$$

cuya solución dado el estado ρ_{t_1}, en un tiempo inicial t_1 evoluciona en un tiempo t al estado

$$\rho_t = e^{-i(t-t_1)H} \rho_{t_1} e^{i(t-t_1)H}$$

A partir de este resultado se pueden obtener varias conclusiones fundamentales:

- El conjunto de operadores $\{e^{itH}\}_t$ que describen la dinámica del sistema, es un grupo con la operación composición.
- Esta estructura de grupo implica que todo elemento tiene inverso, por lo que que la computación cuántica, a diferencia de la computación clásica, es reversible.
- La evolución del sistema queda descripta por una ecuación diferencial lineal, implicando que es válido el principio de superposición.
- Los operadores $\{U = e^{itH}\}_t$ son operadores unitarios ($U * U^\dagger = I_d$), se deduce directamente de que H sea hermítico.

Entonces es válido interpretar la evolución de un sistema desde un estado dado a otro cualquiera como la aplicación de una transformación unitaria al estado inicial. Este resultado es especialmente útil a la hora de hacer computación, ya que se puede ver que las transformaciones unitarias juegan el rol de las compuertas clásicas en los circuitos integrados clásicos.

Al igual que en los circuitos clásicos, la evolución de los circuitos cuánticos quedará determinada por la aplicación sucesiva de una o varias compuertas. Estas compuertas deben ser unitarias y operan sobre uno o más qubits del sistema. Si se cuenta con un sistema multiqubit, (la dimensión del espacio de Hilbert es 2^n) se notará al conjunto de todas las posibles matrices unitarias de $\mathcal{H}^n$ como $\Upsilon(\mathcal{H}^n)$.

Al igual que en los circuitos clásicos existe un set de compuertas básicas. Para sistemas de un qubit se destacan las matrices de Pauli, que se ilustran a continuación, conjuntamente con su aplicación a un estado $|\varphi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ genérico:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad I \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Y \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -ib \\ ia \end{bmatrix}$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad X \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad Z \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix}$$

La compuerta I es la matriz identidad, mientras que la compuerta X correspondería a un bit flip clásico (cambia el $|0\rangle$ por el $|1\rangle$), Z al ser un flip de fase relativa no tiene análogo clásico y finalmente Y es la aplicación conjunta de las anteriores salvo una fase global i.

Además de las matrices de Pauli existen otras compuertas importantes en sistemas de un qubit. Como pueden ser la compuerta de Hadamard H, o las compuertas de fase (o giro) generalizada $R(\theta)$, en particular los giros de $\frac{\pi}{2}$ llamada V, o de $\frac{\pi}{4}$ llamada S [3].

La matriz de Hadamard es

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

y actúa sobre un estado $|\varphi\rangle$ cualquiera como

$$H \begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} a+b \\ a-b \end{bmatrix}.$$

[3] Esta compuerta es también conocida como compuerta $\frac{\pi}{8}$ debido a su forma de construcción hitórica. Despreciando un factor de fase global de $e^{i\pi/8}$, S es igual a la compuerta que posee $e^{-i\pi/8}$ y $e^{i\pi/8}$ en sus diagonales.

En particular si se le entra el estado $|0\rangle$ devuelve el estado $|+\rangle$, es decir la superposición de los estados $|0\rangle$ y $|1\rangle$.

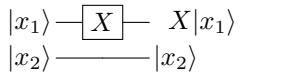
Las matrices de giro $R(\theta)$ son una generalización de Z y permiten establecer una fase relativa arbitraria.

$$R(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}.$$

Tomando $\theta = \frac{\pi}{2}$ se obtiene V, mientras que si se toma $\theta = \frac{\pi}{4}$ se obtiene S.

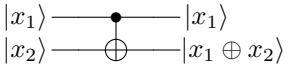
$$V = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

A partir de las compuertas para sistemas de un qubit, mediante el producto tensorial, se pueden modelar compuertas que actúan sobre sistemas de múltiples qubits. Por ejemplo $X \otimes I$ es una compuerta que aplica una compuerta X al primer qubit del sistema mientras que el segundo permanece inalterado.



Si el estado de entrada no está entrelazado tampoco lo estará a la salida.

Sin embargo existen otras transformaciones unitarias que no pueden descomponerse de la manera anterior (como producto de compuertas de un qubit), al igual que ocurre con los estados. El ejemplo más inmediato es la compuerta *CNOT*. Actúa sobre el estado $|x_1x_2\rangle$ cambiando el valor del segundo qubit utilizando el primero como control.

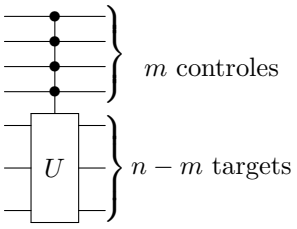


Si a la entrada se tiene el estado $|0\rangle|+\rangle$ separable a la salida se tendrá el estado $\frac{|00\rangle+|11\rangle}{2}$ que no es separable. Esta compuerta crea entrelazamiento en el sistema. Su representación matricial es

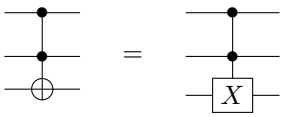
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

La idea de construcción del *CNOT* es generalizable para otras posibles compuertas para sistemas de dos qubits, $control - U$ que se denotará CU de la siguiente manera: $CU|0x\rangle = |0x\rangle$ y $CU|1x\rangle = |1\rangle \otimes U|x\rangle$. Se puede generalizar a compuertas de n qubits de entrada, utilizando m qubits de control y aplicando a los $n - m$ restantes una transformación unitaria.

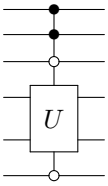
Este tipo de compuertas controladas son casos particulares de compuertas unitarias $\Upsilon(\mathcal{H}^n)$ (ver A.1), pero por su importancia en la construcción de circuitos se notarán de la forma particular $\Lambda^m(U)$, donde m hace referencia a la cantidad de controles y U es la matriz unitaria que se quiere aplicar a los $n - m$ qubits restantes.



El *CNOT* es un caso particular de estas matrices: $CNOT = \Lambda^1(X)$, se aplica la compuerta X a un qubit controlado mediante el otro. Otro caso particular de compuertas controladas es la compuerta TOFFOLI (abreviada $TOFF$): $TOFF = \Lambda^2(X)$. Esta compuerta aplica la compuerta X (negación) a un qubit dependiendo de otros dos controles.

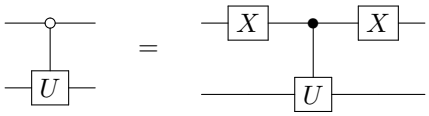


Finalmente vale mencionar que en las construcción de las compuertas $\Lambda^k(U)$ se ha tomado siempre que el valor de los controles para que se aplique efectivamente la compuerta U a los targets debe ser en todos $|1\rangle$. Esto no necesariamente debe ser así, podría pedirse que algunos de los controles por el contrario sean $|0\rangle$. Circuitalmente esto se nota con un circulo vacío en vez de uno lleno en el control. Por ejemplo el circuito dado a continuación:



Aplica la compuerta $U \in \Upsilon(\mathcal{H}^2)$ a los qubits 4 y 5, dependiendo de que los controles 1 y 2 estén en $|1\rangle$ y los qubits 3 y 6 estén en $|0\rangle$.

Vale aclarar que tomar una matriz de $\Lambda^k(U)$ modificada para que tome los controles en $|0\rangle$ en vez de $|1\rangle$ se puede obtener a partir de la matriz de $\Lambda^k(U)$ que toma todos los controles en $|1\rangle$:



Capítulo 3

Modelo de circuitos cuánticos discretizados

El modelo computacional que se propone, como se estableció en el capítulo anterior, es el de circuitos cuánticos. Esto es, representar la evolución de los sistemas de n *qubits* mediante la aplicación sucesiva de operadores unitarios sobre distintos subconjuntos de uno o más *qubits*.

A diferencia del caso clásico, donde para un sistema de n bits, la cantidad de diferentes compuertas posibles es finito, para el caso cuántico no ocurre así. Solamente inspeccionando los sistemas de un único *qubit* vemos que la cantidad de compuertas posibles a utilizar es infinita. De hecho el conjunto $\Upsilon(\mathcal{H})$ de operadores unitarios sobre $\mathcal{H}$, no es ni siquiera numerable. Las compuertas listadas antes como X, Y, Z o H son algunos ejemplos, pero toda matriz de la forma:

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ tal que } a, b, c, d \in \mathbb{C} \text{ y } U * U^{\dagger} = I_d$$

puede representar una compuerta cuántica.

Esta diferencia no es menor. En el modelo clásico se sabe que cualquier compuerta se puede construir utilizando únicamente una cantidad finita de compuertas $NAND$. Es por esto que se dice que $NAND$ es una compuerta universal (no es la única, la compuerta NOR también es universal). En los circuitos cuánticos es claro que esto no puede ocurrir, no hay un conjunto finito de compuertas unitarias que aplicándolas sucesivamente permitan obtener exactamente cualquier compuerta unitaria que se quiera.

En **QC** se busca tener un concepto paralelo al de compuertas universales, es decir un conjunto finito de compuertas que permitan hacer computación cuántica general. El concepto de **compuertas universales** en este contexto es el de un conjunto finito de compuertas que permitan aproximar con una exactitud arbitraría cualquier compuerta unitaria que se quiera. Es en este contexto en el que se habla de modelos discretos.

Por un orden histórico y de construcción es necesario comprender a fondo un primer conjunto que no es finito, pero que es un conjunto universal exacto [1]. En el trabajo de 1995 de *A. Barenco et al* [15] se establece que el $CNOT$ y el conjunto de matrices unitarias que actúan sobre un qubit son un conjunto universal exacto. En la siguiente sección se mostrarán algunos resultados intermedios para llegar a esta conclusión, que además son de interés propio para este trabajo.

[1] Toda matriz unitaria se puede obtener exactamente como un producto finito de elementos de este conjunto.

3.1. Conjuntos universales exactos: $CNOT$ y las compuertas de un *qubit*.

3.1.1. Caracterización de las compuertas de un *qubit*: $\Upsilon(\mathcal{H}^1)$

Una matriz unitaria cualquiera en la esfera de Bloch representa un giro de un ángulo θ y eje $\vec{n}$ arbitrarios [2]. Este hecho, junto a una fase global que no es observable en esta representación, permiten escribir cualquier U como $U = e^{i\alpha}R_{\vec{n}}(\theta)$.

Una matriz $U \in \Upsilon(\mathcal{H}^1)$ cualquiera, se puede expresar en función de las compuertas de un *qubit* $\{X,\ Y,\ Z,\ I_d\}$ (matrices de Pauli) cómo se verá a continuación. Por esta razón es importante destacar cómo son las matrices de giro respecto a los ejes $\vec{x}$, $\vec{y}$, $\vec{z}$ que se obtienen a partir de las matrices de Pauli:

$$R_{\vec{x}}(\theta) = e^{-i\theta X/2} \qquad R_{\vec{y}}(\theta) = e^{-i\theta Y/2} \qquad R_{\vec{z}}(\theta) = e^{-i\theta Z/2}$$

$$\cos(\theta/2)I_d - i\sin(\theta/2)X \qquad \cos(\theta/2)I_d - i\sin(\theta/2)Y \qquad \cos(\theta/2)I_d - i\sin(\theta/2)Z$$

$$\begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \quad \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \quad \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Dados un versor $\vec{n} = (n_x, n_y, n_z)$ y un valor real θ, se define la matriz de giro de eje $\vec{n}$ y ángulo θ como $R_{\vec{n}}(\theta) = e^{-i\theta\vec{n}.\vec{\sigma}/2}$ donde $\vec{n}.\vec{\sigma}$ representa la matriz $n_xX + n_yY + n_zZ$. Aplicando la definición de exponencial compleja y haciendo cuentas se llega que $R_{\vec{n}}(\theta) = \cos(\theta/2)\ I_d - i\sin(\theta/2)\ (n_xX + n_yY + n_zZ)$.

Una propiedad que será útil luego es que:

Proposición 3.1.1. *Dada cualquier $R_{\vec{n}}(\theta)$, siempre se puede obtener como $R_{\vec{z}}(\beta)R_{\vec{y}}(\gamma)R_{\vec{z}}(\delta)$.*

De hecho tomar $\vec{z}$ e $\vec{y}$ en la proposición anterior es arbitrario, se podrían tomar cualquiera dos versores $\vec{u}$ y $\vec{v}$ tal que estos no sean paralelos. Esta propiedad es bastante obvia si se la piensa geométricamente como la composición de rotaciones en la esfera unitaria.

Finalmente un resultado que tendrá una vital importancia en la sección posterior es el que se establece en el siguiente teorema:

Teorema 3.1.1. *Dada $U \in \Upsilon(\mathcal{H}^1)$ existen $A,\ B,\ C$ también pertenecientes a $\Upsilon(\mathcal{H}^1)$ tal que $ABC = I_d$ y $U = e^{i\alpha}AXBXC$*

Demostración. Tomando $A = R_{\vec{z}}(\beta)R_{\vec{y}}(\gamma/2)$, $B = R_{\vec{y}}(-\gamma/2)R_{\vec{z}}(-(\delta+\beta)/2)$ y $C = R_{\vec{z}}((\delta-\beta)/2)$ es claro que $ABC = I_d$.

Utilizando que $X^2 = I_d$, $XZX = -Z$ y que $XYX = -Y$ se tiene que:

$$XBX = XR_{\vec{y}}(-\gamma/2)XXR_{\vec{z}}(-(\delta+\beta)/2)X$$

Hay que observar que

$$XR_{\vec{y}}(-\gamma/2)X = X\left[\cos\left(-\frac{\gamma}{4}\right)I_d - i\sin\left(-\frac{\gamma}{4}\right)Y\right]X = \cos\left(-\frac{\gamma}{4}\right)I_d + i\sin\left(-\frac{\gamma}{4}\right)Y$$

[2] Una matriz unitaria cualquiera geométricamente siempre se puede interpretar como una rotación o giro respecto a un ángulo y eje determinados en el espacio donde actúa. Vale recordar que todos los autovalores de una matriz unitaria tienen módulo 1.

Dado que cos es una función par y sin impar tenemos que

$$XR_{\vec{y}}(-\gamma/2)X = \cos\left(\frac{\gamma}{4}\right)I_d - i\sin\left(\frac{\gamma}{4}\right)Y = R_{\vec{y}}(\gamma/2).$$

De la misma forma se obtiene que $XR_{\vec{z}}(-(\delta+\beta)/2)X = R_{\vec{z}}((\delta+\beta)/2)$, por tanto

$$AXBXC = R_{\vec{z}}(\beta)R_{\vec{y}}(\gamma/2)R_{\vec{y}}(\gamma/2)R_{\vec{z}}((\delta+\beta)/2)R_{\vec{z}}((\delta-\beta)/2) =$$
$$= R_{\vec{z}}(\beta)R_{\vec{y}}(\gamma)R_{\vec{z}}(\delta) = R_{\vec{n}}(\theta),$$

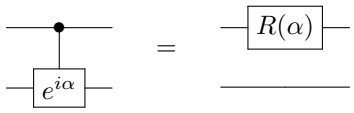
de donde $U = e^{i\alpha}R_{\vec{n}}(\theta)$. □

3.1.2. Matrices controladas de dos *qubits*

Teorema 3.1.2. *Todas las compuertas de $\Lambda^1(U)$ pueden ser implementadas utilizando unicamente compuertas $CNOT$ y compuertas de $\Upsilon(\mathcal{H}^1)$*

Para la prueba es importante el siguiente lema:

Lema 3.1.1. *Los siguientes circuitos son equivalentes:*

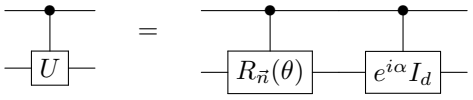


Demostración (lema): Como fácilmente se ve con sus matrices $\Lambda^1(e^{i\alpha}I_d) = R(\alpha)\otimes I_d$:

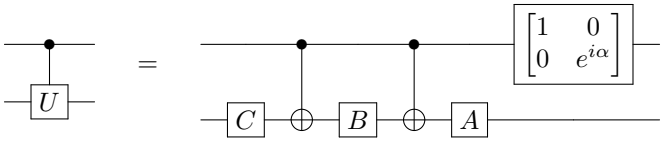
$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&e^{i\alpha}&0\\0&0&0&e^{i\alpha}\end{bmatrix} = \begin{bmatrix}1&0\\0&e^{i\alpha}\end{bmatrix}\otimes\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

Como se quería probar. □

Demostración. Desde que $U = e^{i\alpha}R_{\vec{n}}(\theta) = e^{i\alpha}I_d * R_{\vec{n}}(\theta)$ se puede plantear que $\Lambda^1(U) = \Lambda^1(e^{i\alpha}I_d) * \Lambda^1(R_{\vec{n}}(\theta))$:



Finalmente utilizando el teorema 3.1.1 (toda $U \in \Upsilon(\mathcal{H}^1)$ se descomponer como $U = e^{i\alpha}AXBXC$ tal que $ABC = I_d$ y el lema anterior(3.1.1) se ve que $\Lambda^1(U)$ se puede construir como:



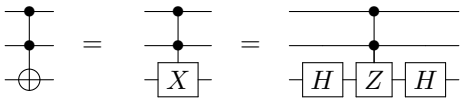
Esto es así porque si el qubit de control esta en $|0\rangle$ los $CNOT$ no actúan sobre el segundo qubit, por tanto solo se aplican las compuertas $ABC = I_d$. En cambio si qubit de control es $|1\rangle$ los $CNOT$ actúan sobre el target y en definitiva se implementa $AXBXC = R_{\vec{n}}(\theta)$. Finalmente teniendo en cuenta la identidad circuital construida, se le aplica la fase global asumiendo el control esta en $|1\rangle$. En definitiva este circuito implementa la compuerta $\Lambda^1(U)$ utilizando unicamente compuertas de un qubit y CNOT. □

3.1.3. Construcción de compuertas Toffolis y Toffolis generalizadas.

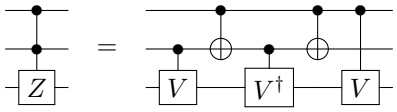
Un resultado sorprendente es que la compuerta $TOFF$ no es elemental, esto es que se puede descomponer como producto de matrices que actúan sobre espacios de uno o dos *qubits*. Este resultado presentado por [16, 17] es importante por varias razones. Dado que la compuerta $TOFF$ es suficiente para implementar toda lógica reversible [18] también lo serán entonces el conjunto de compuertas de un qubit y el $CNOT$. Por otro lado como se verá más adelante la compuerta de Toffoli es el bloque principal para la construcción de toda la familia de compuertas $\Lambda^k(X)$ con $k > 2$, es decir las compuertas Toffolis generalizadas.

Teorema 3.1.3. *La compuerta $TOFF$ ($\Lambda^2(X)$ notación utilizada en la sección 2.1.6) se puede descomponer como productos de compuertas $CNOT$ y $\Lambda^1(U)$*

Demostración. Dado que $HZH = X$, es trivial la siguiente igualdad circuital:

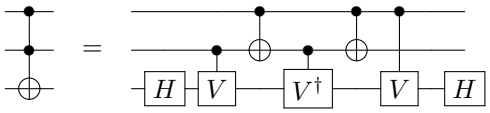


Utilizando que $V^2 = Z$, siendo V la matriz de fase $V = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$, para $\Lambda^2(Z)$ se puede plantear la siguiente descomposición:



Cuando los dos *qubits* de control son $|1\rangle$ se aplica al target $V^2 = Z$ ya que el $V^\dagger$ no se aplica (el control de $V^\dagger$ se invierte a $|0\rangle$). Si los dos qubit de control son $|0\rangle$ ninguna de las tres compuertas controladas se aplica. Finalmente si uno de los *qubits* de control es $|0\rangle$ y el otro $|1\rangle$ se aplica al target V y $V^\dagger$, o $V^\dagger$ y V, pero como V y $V^\dagger$ son unitarias se tiene que $VV^\dagger = V^\dagger V = I_d$.

Juntando ambos resultados obtenemos una descomposición para la compuerta de Toffoli que utiliza únicamente compuertas del tipo $CNOT$ y del tipo $\Lambda^1(U)$ que ya se sabe que, a su vez, se pueden descomponer en compuertas de un qubit y CNOT.



□

Con este resultado el siguiente paso será construir una compuerta Toffoli generalizada $\Lambda^k(X)$. Se verá que para esto únicamente serán necesarias compuertas del tipo $\Lambda^{k-1}(X)$, $TOFF = \Lambda^2(X)$ y un único qubit auxiliar. Por tanto la construcción de esta compuerta será recursiva, siendo el caso base $TOFF = \Lambda^2(X)$ que se obtuvo en el teorema anterior. Esta construcción de la compuerta Toffoli generalizada se puede encontrar en [19].

Antes de plantear el teorema es importante establecer la diferencia entre el uso de una ancilla y un qubit auxiliar. Un *qubit* auxiliar es un qubit que se agrega al sistema. Este puede ser manipulado por una compuerta para proveer una determinada salida pero su valor a la salida debe ser el mismo que a la entrada. La ventaja que presenta este concepto de qubit auxiliar frente al de ancilla es que es muy útil en una construcción recursiva de compuertas reversibles. Dado que el valor de la

salida debe ser igual al de la entrada, este puede ser reutilizado múltiples veces en vez de contar con ancillas en cascada.

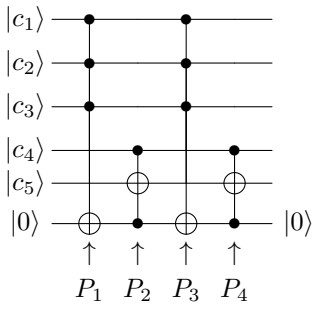
Teorema 3.1.4. *Las compuertas $\Lambda^k(X)$ (Toffoli generalizada) se pueden construir utilizando tan solo compuertas del tipo $TOFF = \Lambda^2(X)$ y un qubit auxiliar.*

La idea básica será construir de manera recursiva la compuerta $\Lambda^k(X)$ asumiendo que se dispone de $\Lambda^{k-1}(X)$ para $k > 2$. Para el caso $k = 2$ ya se dispone de $TOFF$.

Es importante recordar que el objetivo es construir una compuerta $\Lambda^k(X) \in \Upsilon(\mathcal{H}^{k+1})$ que si actúa sobre un registro de *qubits* $\{c_1, c_2, ..., c_k, c_{k+1}\}$ devuelve $\{c_1, c_2, ..., c_k, c_{k+1} \oplus \prod_{i=1}^{k} c_i\}$. Para realizar esta compuerta se implementará la siguiente compuerta en el espacio $\mathcal{H}^{k+2}$ utilizando la compuerta $\Lambda^{k-1}(X)$ de $\mathcal{H}^{k-1}$, la compuerta Toffoli y un qubit auxiliar. El esquema es el siguiente:

1. La compuerta actuará sobre un array de *qubits* de la forma $\{c_1, c_2, ..., c_k, c_{k+1}, x\}$, donde c_{k+1} será el target y x el qubit auxiliar inicializado en $|0\rangle$.
2. Se aplicará una compuerta $\Lambda^{k-1}(X)$ al registro con los $k-1$ primeros qubits como controles y el *qubit* auxiliar $|x\rangle$ como target.
3. Luego se aplica una compuerta Toffoli sobre los últimos *qubits* del registro, siendo el target, el target del registro original, o sea el c_{k+1}.
4. Se repiten los pasos 2 y 3.

Se ilustra este procedimiento para el caso $k = 4$:



Por tanto la prueba del teorema consiste en probar que este esquema funciona, es decir que implementa $\Lambda^k(X)$ y que el bit auxiliar es devuelto como se inicializó. Para esto se mostrará como evoluciona el array de *qubits* cuando se le aplican los pasos P_1, P_2, P_3 y P_4 como se muestra en la figura anterior.

Demostración. Corrección del esquema:

Paso 1. Al aplicar $\Lambda^{k-1}(X)$ a los $k-1$ primeros qubits como controles y el *qubit* auxiliar $|x\rangle$ como target, el registro a la salida de este paso será $\{c_1, c_2, ..., c_k, c_{k+1}, x \oplus \prod_{i=1}^{k-1} c_i\}$

Paso 2. Aplicar ahora al registro obtenido en el paso anterior la compuerta Toffoli sobre los ultimos 3 *qubits* del registro con el penúltimo como target devuelve $\{c_1, c_2, ..., c_k, c_{k+1} \oplus c_k(x \oplus \prod_{i=1}^{k-1} c_i), x \oplus \prod_{i=1}^{k-1} c_i\}$ que haciendo las cuentas es $\{c_1, c_2, ..., c_k, c_{k+1} \oplus c_k x \oplus \prod_{i=1}^{k} c_i, x \oplus \prod_{i=1}^{k-1} c_i\}$.

Paso 3. Al aplicar el mismo operador del paso 1 se obtiene $\{c_1, c_2, ..., c_k, c_{k+1} \oplus c_k x \oplus \prod_{i=1}^{k} c_i, x \oplus \prod_{i=1}^{k-1} c_i \oplus \prod_{i=1}^{k-1} c_i\}$. Ahora bien, es claro que $\prod_{i=1}^{k-1} c_i \oplus \prod_{i=1}^{k-1} c_i = 0$ (suma módulo dos), por lo que en definitiva se obtiene: $\{c_1, c_2, ..., c_k, c_{k+1} \oplus c_k x \oplus \prod_{i=1}^{k} c_i, x\}$. Es en este paso que el qubit auxiliar vuelve a su estado original como se requería.

Paso 4. Finalmente al aplicar la misma compuerta que en el paso 2 a la salida del paso 3 desaparece el factor $c_k x$ que sobra: a la salida se tendrá $\{c_1, c_2, ..., c_k, c_{k+1} \oplus c_k x \oplus \prod_{i=1}^{k} c_i \oplus c_k x, x\}$, que por la misma razón que en el paso anterior el resultado es $\{c_1, c_2, ..., c_k, c_{k+1} \oplus \prod_{i=1}^{k} c_i, x\}$

Este circuito es equivalente a aplicar una compuerta $\Lambda^k(X)$ a los primeros $k+1$ qubits del registro. El qubit auxiliar participa en la evolución pero es devuelto con su valor original. En definitiva esta compuerta se puede construir a partir únicamente de compuertas Toffolis, la recursión lleva al caso base que es de hecho $\Lambda^2(X) = TOFF$.

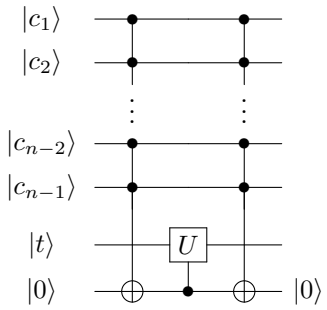
□

3.1.4. Matrices unitarias cualesquiera

Toda matriz unitaria de $\Upsilon(\mathcal{H}^n)$ se puede obtener como composición de compuertas Toffolis generalizadas y compuertas del tipo $\Lambda^1(U)$ donde $U \in \Upsilon(\mathcal{H}^1)$. Para esto, primero se verá una forma sencilla de implementar $\Lambda^{n-1}(U)$ utilizando únicamente compuertas del tipo anterior.

Teorema 3.1.5. *Dada cualquier $\Lambda^{n-1}(U)$ con $U \in \Upsilon(\mathcal{H}^1)$ se puede obtener como producto de compuertas $\Lambda^{n-1}(X)$ y $\Lambda^1(U)$, con la ayuda de un bit auxiliar inicializado en $|0\rangle$.*

Demostración. Para comprobar esto basta inspeccionar el siguiente circuito:



Aplicando un análisis similar al hecho en la parte anterior puede verificarse que este circuito implementa $\Lambda^{n-1}(U)$. Rápidamente: al aplicar $\Lambda^{n-1}(X)$ a los primeros $n-1$ *qubits* de controles y al $|0\rangle$ se devuelve $|1\rangle$ si todos los controles son $|1\rangle$, este resultado es utilizado como control para aplicar la compuerta U al target. Finalmente se aplica de nuevo $\Lambda^{n-1}(X)$ para devolver el qubit auxiliar en el valor que fue inicializado. □

Para abordar como descomponer una matriz cualquiera $U \in \Upsilon(\mathcal{H}^n)$ se hará uso de algunos resultados intermedios que no se demostrarán.

Se dice que una matriz $V_{ij} \in \Upsilon(\mathcal{H}^n)$ actúa en dos niveles si dados dos vectores distintos de la base $|i\rangle$ y $|j\rangle$, son los únicos sobre los que no actúa trivialmente. Esto es:

$$V_{ij}|k\rangle = |k\rangle \; \forall k \neq i, j \text{ y}$$

$$\begin{array}{l} V_{ij}|i\rangle = a_{11}|i\rangle + a_{21}|j\rangle \\ V_{ij}|j\rangle = a_{12}|i\rangle + a_{22}|j\rangle \end{array} \quad \text{tal que} \quad \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = v_{ij} \text{ es una matriz unitaria.}$$

Teorema 3.1.6. *toda matriz $\Upsilon(\mathcal{H}^n)$ se puede descomponer en a lo sumo $2^{n-1}(2^n-1)$ matrices de dos niveles:*

$$U = \prod_{\substack{i,j=0 \\ i>j}}^{2^n-1} V_{ij}$$

Demostración. Ver [18, 20] o, para una demostración más completa, [17]. □

Teorema 3.1.7. *Toda matriz V de $\Upsilon(\mathcal{H}^n)$ se puede obtener como productos de matrices de $\Lambda^{n-1}(U)$ con $U \in \Upsilon(\mathcal{H}^1)$ y Toffolis generalizadas.*

Demostración. Utilizando el teorema anterior esta claro que implementar cualquier V es equivalente a saber implementar a lo sumo $2^{n-1}(2^n-1)$ matrices de dos niveles. Por lo cual si se sabe implementar una compuerta de dos niveles utilizando únicamente compuertas del tipo $\Lambda^{n-1}(U)$ y Toffolis generaliza -das está resuelto el problema.

La idea básica es implementar V_{ij} a través de una compuerta del tipo $\Lambda^{n-1}(v_{ij})$[3]. Para poder hacer esto es necesario construir un camino de compuertas que mapeen el estado $|i\rangle$ en el $|j\rangle$. Si $a_{n-1}, a_{n-2}, ..., a_1, a_0$ es la representación binaria de i y $b_{n-1}, b_{n-2}, ..., b_1, b_0$ es la representación binaria de j se puede establecer una secuencia de números $i = R_1, R_2, ...R_k = j$ que conecten i con j con la condición de que la representación binaria de dos números consecutivos disten a lo sumo en 1 bit[4].

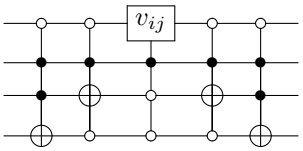
Si se toma como ejemplo $i = 0111$ y $j = 1100$ un camino posible que conecta i con j es

$$\begin{array}{rcccc} i = & 0 & 1 & 1 & 1 \quad R_1 \\ & 0 & 1 & 1 & 0 \quad R_2 \\ & 0 & 1 & 0 & 0 \quad R_3 \\ j = & 1 & 1 & 0 & 0 \quad R_4 \end{array}$$

Implementar una compuerta que transforme un elemento de la secuencia en el siguiente es trivial utilizando $\Lambda^{n-1}(X)$ (la única salvedad es que se tiene que permitir que los controles se apliquen cuando algunos de ellos estén en $|0\rangle$). Al diferir únicamente en un qubit, este será el target, mientras los demás serán los controles en $|0\rangle$ o $|1\rangle$, dependiendo del resto de los valores que se quiere conectar.

Finalmente cuando se llega al número R_{k-1} de la secuencia, este difiere de j en un solo qubit y por tanto se puede implementar v_{ij} como una rotación en ese qubit que difiere controlado por el resto en que no. Finalmente se deshace la secuencia de compuertas dejando fijos todos los estados que no sean el $|i\rangle$ y el $|j\rangle$.

Una implementación de este circuito en el ejemplo dado es:



[3] v_{ij} es la matriz de $\Upsilon(\mathcal{H}^1)$ que queda definida por la matriz de dos niveles V_{ij} de $\Upsilon(\mathcal{H}^n)$.

[4] En la bibliografía común del tema, en general, se habla de esta secuencia como el código de Gray. Esto no es cierto, ya que el código de Gray pide que sea cíclico, y aquí no es necesario. Si se utilizará el código de Gray podría ser necesaria una secuencia más larga de lo estrictamente necesaria que es $d_H(i,j)+1$ (distancia de Hamming entre i y j +1).

□

3.1.5. Conclusión

Corolario 3.1.1. *Las compuertas de un qubit y el $CNOT$ forman un conjunto universal exacto.*

Demostración. Resumiendo los resultados a los que se llegaron en un orden inverso:

1. Del teorema 3.1.7 sabemos que toda matriz de $\Upsilon(\mathcal{H}^n)$ se puede obtener como productos de matrices de $\Lambda^{n-1}(U)$ y Toffolis generalizadas.
2. Otro resultado que se tiene del teorema 3.1.5 es que $\Lambda^{n-1}(U)$ se puede descomponer en compuertas $\Lambda^k(X)$ y $\Lambda^1(U)$ utilizando un qubit auxiliar.
3. Las matrices Toffolis generalizadas son de la forma $\Lambda^k(X)$ donde algunos *qubits* de control actúan cuando valen $|0\rangle$ en vez de $|1\rangle$. Estas matrices se obtienen como productos de $\Lambda^k(X)$ y con compuertas X.
4. Utilizando el teorema 3.1.4 se tiene que las compuertas $\Lambda^k(X)$ se construyen a partir de compuertas $TOFF$, $CNOT$ y un qubit auxiliar.
5. Finalmente las compuertas $TOFF$ (bloque constructivo de $\Lambda^k(X)$) y como $\Lambda^1(U)$ pueden obtenerse como producto de compuertas $CNOT$ y $\Upsilon(\mathcal{H}^1)$ en virtud del teorema 3.1.3. Por tanto este conjunto es universal exacto como se quería probar.

□

3.2. Conjuntos discretos de compuertas universales

Del resultado anterior se deduce un corolario fundamental. Si toda matriz unitaria se puede obtener de manera exacta como productos de compuertas de un qubit y $CNOT$, entonces, si se contara con un conjunto discreto de compuertas (más que discreto finito) que permitieran aproximar con la exactitud que se quiera cualquier compuerta de un qubit, automáticamente se contaría con un conjunto finito de compuertas que permitirían aproximar cualquier compuerta unitaria.

3.2.1. Conjuntos universales.

Es necesario, brevemente, establecer con qué norma se trabajará para realizar estas aproximaciones. Diremos que la compuerta $\tilde{U}$ aproxima a la compuerta U con precisión ε si $||U - \tilde{U}|| < \varepsilon$ con la norma usual de matrices:

$$||A|| := \max_{|\psi\rangle} \frac{||A|\psi\rangle||}{|||\psi\rangle||}.$$

Además de cumplir todas las propiedades de cualquier norma también cumple las siguientes propiedades:

Prop. 1. $||XY|| \leq ||X||||Y||$.

Prop. 2. $||X^\dagger|| = ||X||$.

Prop. 3. $||X \otimes Y|| = ||X||||Y||$.

Prop. 4. $||U|| = 1$ si U es unitaria.

Para matrices unitarias se cumplen además dos propiedades especialmente interesante. La primera es que si $\tilde{U}$ aproxima a U con precisión ε entonces $\tilde{U}^{-1}$ aproxima también con precisión ε a U^{-1}. Esto es, si $||U - \tilde{U}|| < \varepsilon$ entonces $||U^{-1} - \tilde{U}^{-1}|| < \varepsilon$.

La segunda, es que si cada elemento de un circuito $U_t, ...U_2, U_1$ se aproxima por un elemento $\tilde{U}_t, ...\tilde{U}_2, \tilde{U}_1$ con precisión ε entonces el error total de aproximar el circuito total será menor a $t\varepsilon$, es decir $||U_t...U_2U_1 - \tilde{U}_t...\tilde{U}_2\tilde{U}_1|| \leq \sum_1^t \varepsilon \leq t\varepsilon$ los errores se acumulan linealmente. Esta propiedad será especialmente útil cuando se quiera aproximar circuitos utilizando únicamente compuertas de un conjunto finito.

Con esta norma se define entonces un conjunto universal como:

Se dice que un conjunto de compuertas $\mathcal{G}$ es un **conjunto universal** si el subgrupo generado por la aplicación de elementos de $\mathcal{G}$ es denso en $\Upsilon(\mathcal{H}^n)$ para todo $n \geq n_0$ con un n_0 fijo y típicamente pequeño.

La condición de que un conjunto sea denso en $\Upsilon(\mathcal{H}^m)$ es equivalente a pedir que todo elemento de $\Upsilon(\mathcal{H}^n)$ tenga arbitrariamente cerca un elemento de dicho conjunto con la norma antes establecida. Esta definición de conjunto universal puede ser llamada estricta, para permitir algunas relajaciones que se verán más adelante.

La búsqueda de estos conjuntos finitos que permitan aproximar cualquier compuerta unitaria (en general llamados bases) estuvo siempre acompañada de la búsqueda de respuestas más generales sobre estos conjuntos universales. ¿Cuál será la cantidad de compuertas necesarias para aproximar una compuerta U con precisión ε? ¿Estas construcciones pueden hacerse tolerantes a fallos? Y finalmente ¿Que característica comparten estos conjuntos? o en otras palabras ¿Cuáles son las compuertas que brindan a la **QC** de mayor potencia que la **CC**?

Un primer conjunto que se pensó podía ser universal era el conjunto compuesto por H y $CNOT$. Dado que H permite superponer estados y el $CNOT$ crear estados entrelazados parecían un conjunto prometedor. Sin embargo Gottesman y Knill [21] probaron en 1998 que todo circuito que solo involucre a estas dos compuertas puede ser simulado eficientemente por un computador clásico.

En el propio trabajo de *Barenco et all* [15] se demuestra que si se sustituye H por una compuerta R, una rotación de un ángulo múltiplo irracional de π, el conjunto que se obtiene es universal. De hecho basta que R^2 no preserve la base computacional para que lo sea.

Un ejemplo concreto de un conjunto universal es dado por *Boykin et all* en [22]. Al conjunto $\{H, CNOT\}$ le agregan la compuerta S. S es un giro respecto al eje $\vec{z}$ de ángulo $\pi/4$ ($S = e^{i\frac{\pi/4}{2}Z}$). A través de H y S logran construir giros de ángulos múltiplos irracionales de π y con eso probar (mediante una prueba independiente de la dada en [23]) la universalidad. Además se prueba que esta base de compuertas puede ser implementada tolerante a fallos.

Existen varios conjuntos que son universales [24, 25, 26] además del anterior. Una de las cuestiones que surge entonces, es comparar estos conjuntos entre sí, por ejemplo en cuestión de eficiencia. Algunos de estos conjuntos podría aproximar más rápidamente en general a un circuito cualquiera. Un teorema que da respuesta a esta cuestión es el teorema de *Solovay-Kitaev* [27] que refiere a la velocidad de aproximación de estos conjuntos.

Este teorema esencialmente muestra que si un conjunto finito genera un subconjunto denso en

$SU(2)$ (ver nota al pie [5]) entonces con este subconjunto se puede aproximar rápidamente cualquier elemento de $SU(2)$ independientemente de cual sea el conjunto finito. Formalmente:

Teorema 3.2.1 (Solovay-Kitaev)**.** *Dados dos conjuntos universales cerrados bajo su inversa, entonces un circuito compuesto por t-compuertas del primer conjunto puede ser implementado con precisión ε usando un circuito de t.poly$(log\frac{t}{\varepsilon})$ compuertas del otro conjunto.*

Demostración. Ver [27] o [28] □

3.2.2. Conjuntos computacionalmente universales.

Una versión más débil de universalidad de compuertas es la que se obtiene si se permite la utilización de ancillas. En vez de aproximar una compuerta U para aplicar a un estado $|\xi\rangle$ se aproximará esa mediante la utilización de una $\tilde{U}$ que actué en un espacio ampliado $|\xi\rangle \otimes |\phi\rangle$ como sigue:

Definición: Dado un conjunto de operadores finitos $\mathcal{G}$ pertenecientes a $\Upsilon(\mathcal{H}^k)$, si todo operador de $U \in \Upsilon(\mathcal{H}^n)$ puede ser aproximado por el operador $\tilde{U} \in \Upsilon(\mathcal{H}^k)$ mediante el estado ancilla $|\phi\rangle \in \mathcal{H}^{k-n}$ para un vector arbitrario $|\xi\rangle \in \mathcal{H}^n$ con un error ε como

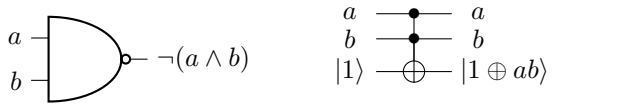
$$||\tilde{U}(|\xi\rangle \otimes |\phi\rangle) - U|\xi\rangle \otimes |\phi\rangle|| < \varepsilon |||\xi\rangle||$$

y $\tilde{U}$ es un producto finito de compuertas de $\mathcal{G}$ decimos que $\mathcal{G}$ es un conjunto **conjunto computacio -nalmente universal**

Con esta definición Shi [26] prueba que el conjunto de compuertas $\{TOFF, H\}$ es un conjunto computacional universal para $SO(4)$[6]. Valiéndose además de que toda matriz unitaria de $SU(2)$ tiene una representación real asociada en $SO(4)$ deduce que a través de $TOFF, H$ se puede obtener un conjunto computacional universal. En la prueba además se establece que esta construcción puede hacerse tolerante a fallos.

De hecho *Kitaev* había probado ya que el conjunto $\{\Lambda^1(V), H\}$ es un cojunto universal y el resultado anterior puede también deducirse de este hecho como hizo *Ahanarov* en [29].

Este resultado tiene una interpretación muy interesante: desde que la compuerta de Toffoli permite implementar toda la lógica clásica reversible. Mediante $TOFF$ se puede implementar la compuerta $NAND$:



$NAND$ clásico $NAND$ mediante $TOFF$

La compuerta $NAND$ clásica no es reversible, sin embargo la versión cuántica de ella debe serlo, para esto se replican las dos entradas a la salida y se utiliza un qubit auxiliar para codificar la salida. Dado que $NAND$ es universal para la **CC** con esta compuerta se podría replicar cualquier circuito clásico que se quiera.

[5] $SU(2)$ es el grupo de matrices unitarias especial: matrices unitarias con determinante 1 de dimensión (2x2). En esta dimensión $SU(2)$ difiere de $\Upsilon(\mathcal{H}^1)$ unicamente en un fase global que es prescindible.

[6] $SO(4)$ es el grupo de matrices ortogonales de dimensión 4x4 y con determinante 1.

Ahora bien, para espacios de dimensión mayor a $\mathcal{H}^3$ $TOFF$ es una permutación par como se verá en detalle más adelante, por lo que es necesario el uso de ancillas para poder implementar en dimensiones mayores permutaciones impares.

Entonces la compuerta $TOFF$ (ancillas mediante) permite implementar toda la lógica clásica reversible, por lo que, parece ser que si $\{TOFF, H\}$ es computacionalmente universal, es la compuerta H la que otorga la potencia a la computación cuántica. Este interpretación muestra cómo los distintos conjuntos discretos que se consideran brindan informaciones complementarias acerca de la naturaleza de la información y computación cuántica.

3.2.3. Otros modelos universales.

Existen ya varios modelos de computación cuántica discreta, que en general pretenden simplificar el modelo cuántico. En las referencias [30, 31, 32, 33] se presentan modelos que involucran conceptos modales y campos finitos para la representación de amplitudes cuánticas. Estos trabajos recuperan gran parte de la teoría cuántica convencional, pero no pueden considerarse realmente como modelos de física/computación cuántica (por ejemplo, en las teorías que involucran campos finitos no se cumple la propiedad de norma evanescente sólo para estados nulos).

Otros trabajos utilizan algún tipo de discretización como herramienta para el diseño de algoritmos, por ejemplo [34], tratando de relacionar las estructuras de la computación y los fundamentos de la física. En este sentido, Lloyd et al. [35] definen una integral de camino universal, que suma sobre todas las estructuras computables; Long et al. [36, 37, 38] introducen la dualidad computacional cuántica, permitiendo el uso de la combinación lineal de operadores unitarios para diseñar algoritmos cuánticos de forma más flexible, Gudder [39] y Long [40] establecen la teoría matemática correspondiente y Wei et al. [41] estudian dos algoritmos de simulación cuántica de dualidad; y Lomonaco [42] muestra cómo se puede utilizar la paradoja GHZ para diseñar un dispositivo de computación que no puede ser implementado físicamente en el contexto de la física clásica, pero sí en el de la física cuántica.

En el contexto de los conjuntos universales de compuertas cuánticas, los trabajos de Kitaev, Boykin, Shi, Aharonov y Kliuchnikov et al. [25, 43, 44, 45, 46] introducen cada uno de ellos diferentes conjuntos universales. El tema principal que comparten estos trabajos es la demostración de la universalidad de estos conjuntos. En el trabajo de Shi [44] se da una prueba de la universalidad del conjunto $\{H, T\}$ para operadores hermíticos y Aharonov [45] muestra que este resultado se puede extender a los operadores unitarios. Estos dos trabajos son especialmente útiles para nosotros, ya que nos permiten deducir directamente la universalidad de nuestro conjunto.

Parte II

Modelo de computación cuántica discreta

Capítulo 4

Modelo discreto

4.1. Introducción

Como se vio en la sección anterior (3.2.3) ya se han definido múltiples conjuntos de compuertas universales con diferentes características. Lo que diferencia este trabajo de los ya vistos es que el modelo está enfocado en las estados cuánticos a los que da lugar buscando la máxima simplicidad, pero sin perder las propiedades básicas de la mecánica cuántica. El conjunto resultante debe permitir representar estados que permitan expresar las principales características de la mecánica cuántica: superposición y entrelazamiento. Así mismo debe permitir aproximar cualquier otro estado fuera del modelo, es decir debe ser universal como conjunto de estados.

De todos los conjuntos posibles de estados cuánticos discretos, hay uno que, cumpliendo las tres propiedades antes mencionadas, es el más destacado en cuanto a simplicidad de los estados. Se trata del conjunto de estados de coordenadas gaussianas, que incluye todos los estados cuánticos cuyas coordenadas en la base de cálculo, salvo un factor de normalización $\sqrt{2^{-k}}$, pertenecen al anillo de enteros gaussianos:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

También necesitamos introducir un conjunto de compuertas cuánticas que verifiquen las siguientes propiedades: contiene compuertas cuánticas que transforman estados discretos en estados discretos y genera todos los estados cuánticos discretos. Nuestro modelo incluye dos puertas cuánticas elementales que verifican las propiedades anteriores, H y G. La puerta Hadamard H permite la superposición mientras que G es una puerta de tres qubits. Dos de ellos son qubits de control, mientras que el tercero es el objetivo. Si los qubits de control están en el estado $|1\rangle$ entonces la puerta V se aplica al tercer qubit:

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Esta compuerta cuántica permite la construcción de todos los estados de coordenadas gaussianas (estados discretos) y por ello la llamamos G. Por último incluimos también dos qubits auxiliares (qubits ancilla), para poder manejar adecuadamente los estados con uno y dos qubits y generar, por ejemplo, el grupo completo de permutaciones. Estos qubits juegan un papel importante en muchos algoritmos cuánticos, especialmente en implementaciones de códigos correctores, donde su uso eficiente es objeto de estudio [47].

En la primera parte del trabajo, tras establecer las propiedades básicas del modelo, demostramos

que los estados de coordenadas gaussianas pueden construirse a partir de la base computacional, aplicando sucesivamente las puertas cuánticas del modelo. El índice k en el factor de normalización proporciona un punto de vista interesante sobre los estados discretos. A saber, los estados pueden clasificarse en diferentes niveles de discretización, dependiendo de k. Estos niveles representan el grado de precisión o aproximación de los estados discretos en relación con los estados continuos.

En la segunda parte, definimos el conjunto de compuertas cuánticas discretas, como las compuertas cuánticas que dejan invariante el conjunto de estados discretos, demostramos que una compuerta cuántica es discreta si y sólo si todas sus columnas (filas) son estados discretos de niveles de la misma paridad, que se definirá oportunamente. En este sentido, el modelo más cercano al nuestro es el presentado por Kliuchnikov et al. [46], por lo que se presenta una discusión completa en la sección 4.4.3 para exponer las principales diferencias entre ambos. En este modelo, las coordenadas de los estados y los elementos de las puertas cuánticas pertenecen, salvo un factor de normalización 2^{-k}, al anillo $\mathbb{Z}[\sqrt{2}, i]$ en contraposición a nuestro anillo $\mathbb{Z}[i]$. Se discuten las consecuencias de este hecho. Para el caso de sistemas de $2-$qubits, demostramos que estas puertas cuánticas discretas pueden construirse utilizando sólo las puertas cuánticas del modelo. Conjeturamos que esta propiedad también es válida para puertas cuánticas discretas en $n-$qubits. Finalmente, se menciona la universa -lidad del modelo, como consecuencia de los trabajos citados anteriormente [25, 44].

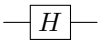
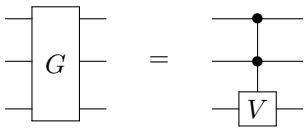
La simplicidad de este modelo es una ventaja para la investigación en ramas teóricas de la computación (teoría de la complejidad, algorítmica, etc.), en matemáticas e, incluso, en mecánica cuántica. Las propiedades de este modelo nos han permitido descubrir un teorema de completitud de bases $p-$ortonormales de estados discretos ($p = 2^k$ en el modelo introducido) que sugiere la existencia de una geometría de estados discretos [48] que se basa en una interesante generalización del teorema de los cuatro cuadrados de Lagrange [49]. Estamos estudiando este sorprendente hecho y sus posibles implicaciones en diferentes ramas de las matemáticas y la mecánica cuántica.

Nuestro modelo de computación cuántica discreta permite el uso sin restricciones de la superposi -ción cuántica y el paralelismo cuántico. Estos hechos son muy importantes para el diseño de algoritmos. Giri et al. [50] afirman que estas características tienen una ventaja significativa en términos de velocidad sobre la computación clásica, en particular en los algoritmos de búsqueda de bases de datos, que son muy importantes en la informática. Se puede comprobar fácilmente que el algoritmo de búsqueda de Grover [9] puede implementarse directamente en el modelo presentado de computación cuántica discreta, sin ninguna modificación, y, sin embargo, el algoritmo de búsqueda cuántica óptima introducido por Long [51] no se puede.

Hay muchos estados cuánticos importantes que son en realidad estados cuánticos discretos. Por ejemplo, los estados propios de las puertas cuánticas Z y Y, las columnas de las matrices que las relacionan, los principales estados utilizados en la compartición de secretos cuánticos, los estados GHZ y el estado cuántico de $6-$qubits BPB, etc. Por lo tanto, en el último de los ejemplos anteriores, la interpretación y el papel de los diferentes elementos de los protocolos de compartición de secretos cuánticos no cambian en el modelo introducido.

4.2. Propiedades básicas del modelo

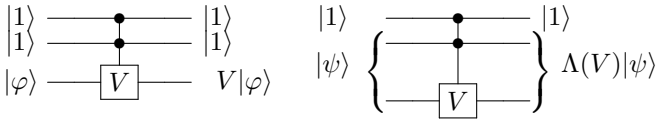
En esta sección se probará que el sistema conformado por las compuertas $\{H, G\}$, descritas abajo, permiten hacer cualquier permutación posible de la estados de la base computacional y agregar la fase relativa i en cualquier posición deseada respecto de la base computacional para un estado cuántico dado.

Representación matricial	Representación circuital
$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	
$G = diagonal\{1,1,1,1,1,1,1,i\}$	

H es la compuerta de Hadamard como hasta ahora, mientras que G es la compuerta V con dos controles. En general se utilizará la notación $\Lambda^k(U)$ para nombrar a una compuerta que actúa en un espacio de $k+1$ qubits en la cual se utilizan k controles y U es una compuerta de un qubit. Por lo tanto $G = \Lambda^2(V)$ y se utilizará cualquiera de las dos notaciones convenientemente.

Observación 4.2.1. El conjunto de compuertas componentes es cerrado bajo sus inversas con la ley de composición, ya que la inversa de H es ella misma y como se despendre de su matriz $G^4 = I_d$ de donde $G^3 = G^{-1} = G^\dagger$.

Utilizando la compuerta G se puede obtener la compuerta V y $\Lambda(V)$ que actúan en un espacio de 1 y 2 qubits respectivamente. La compuerta V multiplica por la fase i al estado $|1\rangle$ dejando al estado $|0\rangle$ inalterado. Mientras que $\Lambda(V)$ multiplica por la fase i al estado $|11\rangle$ dejando al resto de la base computacional invariante.



A partrir de las identidades circuitales

$$V^2 = Z \tag{4.1}$$

$$X = HZH \tag{4.2}$$

y de las compuertas V, $\Lambda(V)$ y G se pueden obtener los grupos de compuertas Z, $\Lambda(Z)$, y $\Lambda^2(Z)$ y X, $\Lambda(X)$ y $\Lambda^2(X)$, donde Z y X son las compuertas de Pauli usuales. En particular $\Lambda(X)$ es la compuerta $CNOT$ y $\Lambda^2(X)$ la compuerta de Toffoli.

Observando la identidad (4.1), y sin más que verificar el producto matricial, es directo verificar que V^2, $(\Lambda(V))^2$ y $(\Lambda^2(V))^2$ dan lugar a Z, $\Lambda(Z)$ y $\Lambda^2(Z)$ respectivamente.

Mientras que utilizando la identidad (4.2) y los circuitos:

se obtiene X, $\Lambda(X)$ y $\Lambda^2(X)$ como se buscaba.

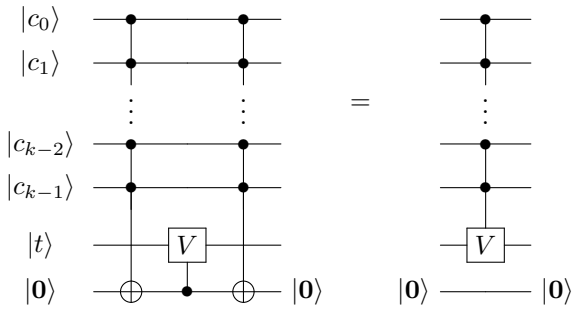
Finalmente lo que se quiere obtener es una generalización de estas compuertas de tal manera que se pueda utilizar la cantidad de controles que se quiera, es decir construir $\Lambda^k(X)$, $\Lambda^k(V)$ y $\Lambda^k(Z)$.

Está claro que pudiendo construir $\Lambda^k(X)$ ó $\Lambda^k(Z)$ la otra se obtiene inmediatamente de aplicar la identidad[1] (4.2) y circuitos análogos a los que se utilizaron para la construcción de $\Lambda(X)$ y $\Lambda^2(X)$. Por esta razón se detallará únicamente la construcción de $\Lambda^k(X)$ a partir de las compuertas con las que ya se cuenta. La construcción de $\Lambda^k(V)$ se obtiene modificando ligeramente la de $\Lambda^k(X)$.

Como se demostró en el teorema 3.1.4 las compuertas $\Lambda^k(X)$ (Toffoli generalizadas) se pueden construir utilizando tan solo compuertas $\Lambda^2(X)$ y un qubit auxiliar que será devuelto en el mismo valor que es inicializado.

Construcción de $\Lambda^k(V)$ a partir de $\Lambda^k(X)$ y $\Lambda(V)$

La generalización de la compuerta $\Lambda^2(V)$, la compuerta $\Lambda^k(V)$, se obtiene fácilmente utilizando las compuertas $\Lambda(V)$ y $\Lambda^k(X)$ y un qubit auxiliar, como queda ilustrado en el siguiente circuito:

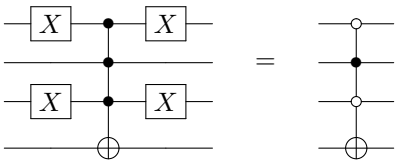


Permutación de coordenadas

Las compuertas obtenidas a partir de H y G en la subsección anterior permitirán demostrar de manera más sencilla que, en definitiva, a partir de estas compuertas y utilizando a lo sumo dos qubits auxiliares, descartables, se puede realizar cualquier permutación posible entre estados de la base computacional.

Como primer paso hay que observar que todas las compuertas controladas que se han manejado hasta el momento actúan cuando los controles se encuentran en el estado $|1\rangle$. Esto no tiene por qué ser siempre así. Puede ser útil aplicar, por ejemplo, una compuerta X cuando algunos de los controles se encuentren en $|1\rangle$ y otros en $|0\rangle$. Para realizar esto basta simplemente aplicar la compuerta X a los controles que se quiere que actúen en $|0\rangle$.

Por ejemplo supongamos que se quiere aplicar la compuerta X a un qubit si el segundo qubit de control se encuentra en $|1\rangle$ mientras que los otros dos se encuentran en $|0\rangle$, el circuito que hace esta operación sería:



Cuando los controles están dibujados con un círculo vacío se indica que el control actuará cuando ese qubit se encuentre en el estado $|0\rangle$.

[1] Como $H^2 = I_d$ esta identidad también implica que $Z = HXH$

Convenido esto, supóngase que se quiere permutar del estado $|i\rangle$ al estado $|i'\rangle$ de la base computacional, y que sus representaciones binarias son $i : a_{n-1}, a_{n-2}, ..., a_1, a_0$ e $i' : b_{n-1}, b_{n-2}, ...b_1, b_0$. La representación binaria de los números diferirá en varios a_j con $j \in 0...n-1$.

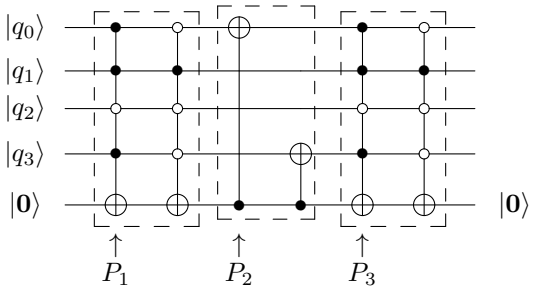
La descripción del circuito que permuta los estados $|i\rangle$ y $|i'\rangle$ es:

Paso 1. Se deben colocar dos compuertas $\Lambda^k(X)$ actuando sobre el qubit auxiliar con sus controles homologando la configuración de $|i\rangle$ e $|i'\rangle$ respectivamente. Con esta configuración de compuertas Toffolis se logra que el qubit auxiliar tome el valor 1 si y solo si a la entrada se tiene la configuración $|i\rangle$ o $|i'\rangle$. Cabe destacar que estas dos compuertas Toffoli por construcción permutan, con lo cuál su orden de aplicación no importa.

Paso 2. Controladas por el qubit auxiliar, se colocan compuertas $\Lambda(X)$ actuando sobre los qubits que se deban alterar para transformar la configuración de $|i\rangle$ a $|i'\rangle$ (que es la misma transformación para llevar $|i'\rangle$ a $|i\rangle$). Esto es, controlando por el qubit auxiliar, se deben intercambiar los 0's y 1's en los que ambas configuraciones binarias difieren.

Paso 3. Finalmente, se colocan las mismas compuertas $\Lambda^k(X)$ que en el paso 1 con el fin de devolver al valor 0 el qubit auxiliar.

El siguiente circuito muestra un ejemplo que permuta los estados $|2\rangle = |0010\rangle$ y $|11\rangle = |1011\rangle$ de la base computacional:



Introducción de la fase relativa i o -1

Con los resultados obtenidos hasta ahora, se verá que es inmediato construir una compuerta a partir de las compuertas conformantes que introduce la fase relativa i o -1 a cualquiera de los estados de la base computacional.

Esto ya se tiene hecho en el caso en el que se elija el estado $|2^n - 1\rangle$ en un espacio de n qubits, ya que es exactamente la compuerta $\Lambda^{n-1}(V)$ o $\Lambda^{n-1}(Z)$ que ya pueden ser construidas gracias al teorema 3.1.4.

Finalmente si se quiere introducir la fase relativa i o -1 en cualquier otro estado $|k\rangle$ tal que $k \neq 2^n - 1$, lo que se hace es permutar el estado $|k\rangle$ con el $|2^n - 1\rangle$ (como se vio en (4.2)) , y mediante $\Lambda^{n-1}(V)$ o $\Lambda^{n-1}(Z)$ se introduce la fase i o -1 en esta posición y luego se vuelven a permutar estos dos estados. A todo este proceso, que en sí es un circuito cuántico, se lo nombrará V_k y Z_k respectivamente indican de que se modifica la coordenada k.

Observación 4.2.2. Lo anterior son casos particulares de un resultado más general. Como es bien sabido, $\Lambda^2(X)$ (puerta de Toffoli) es universal para la computación clásica reversible. Así, como demostramos que $\Lambda^2(X)$ puede obtenerse a partir de G, toda puerta clásica reversible puede obtenerse dentro del modelo, como se mostró para $\Lambda^k(X)$ o para realizar una permutación entre dos estados cualesquiera de la base de cálculo.

4.3. Estados cuánticos discretos

El objetivo de esta sección es estudiar el conjunto de estados que se puede alcanzar, partiendo de la base computacional y utilizando únicamente las compuertas conformantes del modelo. Se verá que estos estados cumplen la condición de tener como coordenadas enteros de Gauss a menos de un factor $\sqrt{2}^{-k}$.

$$\text{Enteros de Gauss: } \mathbb{Z}[i] = \{a + bi \text{ donde } a, b \in \mathbb{Z}\}$$

Esto le otorga al modelo características propias que lo distinguen de otros modelos similares.

4.3.1. Definición del conjunto de estados discretos $\mathcal{E}$

Definición 4.3.1. Sea $\mathcal{E}$ el menor conjunto de estados cuánticos que contiene a la base computacional y que es invariante bajo la aplicación de las compuertas conformantes H y G.

Este conjunto es el conjunto de estados que se obtiene de aplicar sucesivamente las compuertas básicas H y G (utilizando, o no, los qubits auxiliares) a los estados de la base computacional del espacio generado por n qubits. Entonces, por lo visto en la sección 4.2, el conjunto será invariante por permutaciones de coordenadas y por introducción de fases relativas i o -1 donde se quiera.

4.3.2. Definición del conjunto E

El estudio del conjunto de estados discretos $\mathcal{E}$ requiere la introducción del conjunto de vectores enteros gaussianos de dimensión 2^n:

$$\mathbb{Z}[i]^{2^n} = \{(x_0 + iy_0, ..., x_{2^n-1} + iy_{2^n-1}) \mid x_i, y_i \in \mathbb{Z} \text{ for all } \ 0 \leq i < 2^n\}$$

y el conjunto de estados de coordenadas gaussianas definido a continuación.

Definición 4.3.2. Sea $|\psi\rangle$ un estado cuántico, diremos que $|\psi\rangle \in E$ sii $\exists k \in \mathbb{N}$ tal que $\sqrt{2}^k|\psi\rangle \in (\mathbb{Z}[i])^{2^n}$.

Para demostrar que $E = \mathcal{E}$, necesitaremos las siguientes propiedades del conjunto de estados de coordenadas gaussianas E.

Niveles de discretización

El conjunto de estados E se puede escribir como la unión disjunta de subconjuntos del propio E indexados por el parámetro k, a los que se llamará F_k. Estos conjuntos quedan descritos del siguiente modo:

$$F_k = \left\{ |\psi\rangle \in E \mid (\sqrt{2})^k|\psi\rangle \in (\mathbb{Z}[i])^{2^n} \text{ y } (\sqrt{2})^{k-2}|\psi\rangle \notin (\mathbb{Z}[i])^{2^n} \right\}.$$

La condición anterior establece que un estado $|\psi\rangle$ de la forma $|\psi\rangle = \frac{1}{\sqrt{2}^k}(x_0+iy_0, x_1+iy_1, ..., x_{2^n-1}+iy_{2^n-1})$ pertenece al subconjunto F_k si se cumple que:

(a) $(x_0 + iy_0, ..., x_{2^n-1} + iy_{2^n-1}) \in (\mathbb{Z}[i])^{2^n}$

(b) $x_0^2 + ... + x_{2^n-1}^2 + y_0^2 + ... + y_{2^n-1}^2 = 2^k$

(c) $2 \nmid mcd(x_0, ..., x_{2^n-1}, y_0, ..., y_{2^n-1})$

Mientras que (a) y (b) juntas establecen que $|\psi\rangle$ es efectivamente un estado cuántico (norma unitaria) y está en E, la condición (c) determina que $|\psi\rangle$ está en un determinado F_k.

Utilizando el resultado de Lagrange de ecuaciones diofánticas (ver [52]) se prueban fácilmente las siguientes proposiciones:

Proposición 4.3.1. *F_k es finito y no vacío para todo $k \geq 0$ y $n > 1$.*

Una observación interesante es que F_0 coincide con la base computacional, salvo una posible fase global -1 o $\pm i$, para todo elemento de dicha base.

Proposición 4.3.2. *F_k y F'_k son disjuntos si $k \neq k'$.*

Finalmente una conclusión importante de estas dos proposiciones es que el conjunto E tiene infinitos elementos. Está claro que

$$E = \bigcup_{k=0}^{\infty} F_k$$

La intersección entre diferentes F_k es vacía (proposición 4.3.2) por tanto es una unión disjunta. Y además como se vio en la proposición 4.3.1 $F_k \neq \emptyset$ para todo k,

$$E = \biguplus_{k=0}^{\infty} F_k$$

y se tiene que $card(E) = \infty$.

4.3.3. Los conjuntos E y $\mathcal{E}$ son iguales

$E \subseteq \mathcal{E}$

Dado un vector $|\psi\rangle \in E$, $|\psi\rangle = \frac{1}{\sqrt{2^k}}(x_0 + iy_0, x_1 + iy_1, ..., x_{2^n-1} + iy_{2^n-1})$, al hablar de la paridad del elemento $x_p + iy_p$ del vector se dirá que es par (P) si $x_p + y_p \equiv_2 0$, e impar (I) en caso contrario.

Por otro lado se hablará de la configuración de paridad del elemento $x_p + iy_p$. En este caso se hará referencia directamente a la paridades de los números enteros x_p e y_p, siendo las posibles configuraciones $[p, p]$, $[i, i]$, $[i, p]$ y $[p, i]$.

Paridad del elemento $x_p + iy_p$	configuración del elemento $x_p + iy_p$
P (pares) si $x_p + y_p \equiv_2 0$	$[p, p]$, $[i, i]$,
I (impares) si $x_p + y_p \equiv_2 1$	$[i, p]$ y $[p, i]$

Si $x_p + iy_p$ presenta las configuraciones $[p, p]$ o $[i, i]$ se estará frente a un elemento par, mientras que si presenta las configuraciones $[i, p]$ o $[p, i]$ se estará frente a un elemento impar.

Proposición 4.3.3. *Sea $|\psi\rangle$ un elemento en $F_k \subseteq E$, con $k > 0$. Entonces el número de coordenadas impares de $|\psi\rangle$ es par.*

Demostración. Como la ecuación $x_0^2 + ... + x_{2^n-1}^2 + y_0^2 + ... + y_{2^n-1}^2 = 2^k$ $(k > 0)$ debe cumplirse y 2^k es un número par, el número de sumandos impares (x_j o y_j) debe ser par. Las configuraciones pares $[p, p]$ y $[i, i]$ aportan siempre un número par de sumandos impares (0 y 2 respectivamente), mientras que las configuraciones impares $[p, i]$ y $[i, p]$ aportan exactamente un sumando impar. Por lo tanto, el número de configuraciones impares, y en consecuencia el número de coordenadas impares, es par. □

Para demostrar que $E \subseteq \mathcal{E}$ daremos un procedimiento para reducir el nivel de un estado dado $|\psi\rangle \in F_k$ con $k > 0$. Este procedimiento transforma este estado en uno nuevo $|\tilde{\psi}\rangle \in F_{k-1}$, utilizando solo las puertas permitidas en nuestro modelo.

Definición 4.3.3. Diremos que $|\psi\rangle \in F_k$ es reducible si y sólo si $H_0|\psi\rangle \in F_{k-1}$.

H_0 es la puerta cuántica H aplicada al qubit menos significativo de la matriz de qubits. En otras palabras, es la puerta $I^{\otimes n-1} \otimes H$.

Observación 4.3.1. Un estado $|\psi\rangle \in F_k$ es reducible si las coordenadas en las posiciones $2p$ y $2p+1$ tienen la misma configuración de paridad para todo $0 \leq p < 2^{n-1}$.

El siguiente procedimiento muestra que cualquier estado $|\psi\rangle \in F_k$ puede ser modificado, sin cambiar su nivel F_k, hasta alcanzar la configuración de paridad descrita en la observación 4.3.1.

Transformación de $|\psi\rangle \in F_k$ en un estado reducible del mismo nivel:

Paso 1. Utilizando las puertas V_k (ver parte final de la sección 4.2) en cada coordenada k que tenga la configuración de paridad $[p, i]$ podemos obtener la misma configuración de paridad $[i, p]$, en todas las coordenadas impares.

Paso 2. Como se estableció en la proposición 4.3.3, el número de coordenadas impares en un estado F_k es par. Utilizando este hecho, y las permutaciones de coordenadas, podemos ordenar las coordenadas del estado de forma que las coordenadas en las posiciones $2p$ y $2p + 1$ tengan la misma configuración para todo $1 \leq p < 2^{n-1}$.

$$\text{Reducible} \qquad \Big(\underbrace{[p,p],[p,p],\ldots}_{par}, \underbrace{[i,i],[i,i],\ldots}_{par}, \underbrace{[i,p],[i,p],[i,p],[i,p],\ldots}_{par} \Big)$$

$$\text{No Reducible} \qquad \Big([p,p],[i,i], \underbrace{[p,p],[p,p],\ldots}_{par}, \underbrace{[i,i],[i,i],\ldots}_{par}, \underbrace{[i,p],[i,p],\ldots}_{par} \Big)$$

Paso 3. El único problema que queda es el de las dos primeras posiciones. Si no tienen la misma configuración (es decir, $[p, p]$ y $[i, i]$) tenemos que utilizar una nueva transformación para lograr nuestro objetivo y hacer el estado reducible. Esta transformación es la puerta cuántica R que se describe a continuación.

Compuerta cuántica R

R es la puerta cuántica $V_1 H_0 V_1 H_0$, donde ya se han introducido H_0 y V_1. Recordando que la puerta V_1 multiplica la segunda coordenada por la fase i, es fácil comprobar que la acción de

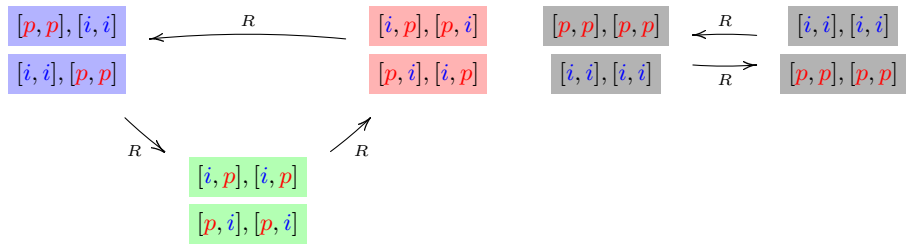
R sobre un estado discreto $|\psi\rangle = (x_j + iy_j)_{j=0,\dots,2^n-1}$ es la siguiente:

$$R|\psi\rangle = \Bigg(\frac{x_0 - y_0 + x_1 + y_1}{2} + i\frac{x_0 + y_0 - x_1 + y_1}{2},$$
$$\frac{x_0 - y_0 - x_1 - y_1}{2} + i\frac{x_0 + y_0 + x_1 - y_1}{2}, x_2 + iy_2, \dots\Bigg)$$

Observación 4.3.2. Como se puede ver en la ecuación anterior, si la cantidad de números impares en el conjunto $\{x_0, y_0, x_1, y_1\}$ es par, entonces el nivel de $|\psi\rangle$ se mantiene.

Ahora necesitamos el siguiente resultado: si p y q son enteros impares (pares) entonces $\frac{p+q}{2}$ y $\frac{p-q}{2}$ tienen paridades diferentes (la misma paridad).

Este resultado y el análisis de todas las configuraciones de paridad de x_0+iy_0 y x_1+iy_1 (las dos primeras coordenadas), que tienen una cantidad par de enteros impares, permite construir el siguiente diagrama, que muestra las transiciones entre las posibles configuraciones de paridad generadas por R:



Por tanto, si las dos primeras coordenadas tienen la configuración de paridad ($[p, p]$, $[i, i]$) o ($[i, i]$, $[p, p]$), obtendremos entonces la configuración de paridad ($[p, i]$, $[p, i]$) o ($[i, p]$, $[i, p]$), mediante R. Así, el estado obtenido permanece en el nivel original F_k, pero ahora es reducible, por observación 4.3.1.

El procedimiento anterior nos permite demostrar el siguiente teorema:

Teorema 4.3.1. *Dado un estado $|\psi\rangle \in F_k$ con $k > 0$, se puede transformar en otro estado $|\tilde{\psi}\rangle \in F_{k-1}$ dentro del modelo de computación cuántica discreta.*

Así, repitiendo este procedimiento k veces transformaremos un estado $|\psi\rangle \in F_k$ en otro $|\tilde{\psi}\rangle \in F_0$ y, aplicando una puerta cuántica más (V_j^s con $0 \leq s \leq 3$), reduciremos $|\tilde{\psi}\rangle$ a un estado $|j\rangle$ de la base de cálculo. Las puertas cuánticas utilizadas son productos de puertas H y G y, por la observación 4.2.1, sus inversas también lo son. Por lo tanto, tomando la inversa de la composición de estas puertas cuánticas, demostramos finalmente que cualquier $|\psi\rangle \in F_k$ puede obtenerse de la base computacional, aplicando H y G. De este hecho se obtiene el siguiente resultado:

Proposición 4.3.4. *Se cumple que $E \subseteq \mathcal{E}$.*

4.3.4. $\mathcal{E} \subseteq E$

Para demostrar la igualdad $\mathcal{E} = E$, tenemos que considerar la otra inclusión. A saber, todo estado que pueda construirse utilizando las puertas H y G de la base computacional es de hecho un estado

de coordenadas gaussianas (es decir, el estado tiene enteros gaussianos como coordenadas, salvo un factor $\sqrt{2}^{-k}$).

El resultado se deriva fácilmente de las dos propiedades siguientes: los estados de la base computacional pertenecen a E; y las puertas cuánticas H y G dejan invariante el conjunto E. Así, hemos obtenido el siguiente resultado:

Proposición 4.3.5. *Se cumple que $\mathcal{E} \subseteq E$.*

Finalmente, las proposiciones 4.3.4 y 4.3.5 nos permiten demostrar el resultado principal sobre los estados discretos:

Teorema 4.3.2. *El conjunto de estados discretos $\mathcal{E}$ y el conjunto de estados de coordenadas gaussianas E son iguales.*

4.4. Compuertas cuánticas discretas

4.4.1. Definición de compuerta discreta y caracterización

Definición 4.4.1. Una compuerta cuántica P pertenecerá al conjunto de compuertas discretas $\mathcal{P}$ si y solo si $\forall\ |\psi\rangle \in \mathcal{E}$ se verifica que

$$P|\psi\rangle \in \mathcal{E}$$

Teorema 4.4.1 (Caracterización del conjunto $\mathcal{P}$)**.** *$P \in \mathcal{P}$ si y solo si sus columnas son estados discretos de niveles con igual paridad.*

Demostración. ▪ Directo

Por definición una puerta P es discreta si mapea estados discretos en estados discretos. En particular los estados de la base computacional son estados discretos, por lo tanto al aplicar $P = ((p_{ij}))_{i,j=0,\dots,2^n-1}$ al estado $|k\rangle = (0,\dots,0,\underset{k}{1},\dots,0)$ se obtiene:

$$P|k\rangle = ((p_{ik}))_{i=0,\dots,2^n-1} = P_k$$

donde P_k nota a la columna $k-$ésima de P. Por lo tanto P_k debe ser un estado discreto por ser P matriz discreta y $|k\rangle$ estado discreto.

Los estados de la forma $|\phi\rangle = (|k\rangle + |k'\rangle)/\sqrt{2}$ con $k \neq k'$ son estados discretos de nivel F_1, $|\phi\rangle = (0,\dots,\underset{k}{1},0,\dots,\underset{k'}{1},\dots,0)/\sqrt{2}$. Al aplicarle P a un estado de este tipo y por ser P lineal se tiene:

$$P|\phi\rangle = \frac{P_k + P_{k'}}{\sqrt{2}}$$

donde nuevamente P_k y$P_{k'}$ notan a las columnas k y k' de P respectivamente, y por tanto son estados discretos.

Como $P_k = (x_0 + iy_0,\dots,x_{2^n-1} + iy_{2^n-1})/(\sqrt{2})^l$ y $P_{k'} = (a_0 + ib_0,\dots,a_{2^n-1} + ib_{2^n-1})/(\sqrt{2})^{l'}$ donde x_i, y_i, a_i y b_i son enteros, para que $P|\phi\rangle$ sea un estado discreto, se tiene que cumplir que a menos de un factor de $(\sqrt{2})^p$ la suma de P_k y $P_{k'}$ ponderada por un factor $\sqrt{2}$ tenga coordenadas enteras.

Suponiendo que $l \leq l'$ al sacar $(\sqrt{2})^{l'}$ como factor común en $P|\phi\rangle$ las coordenadas deberán quedar enteras:

$$P|\phi\rangle = \frac{1}{\sqrt{2}}\left(\frac{(x_0+iy_0,\ldots,x_{2^n-1}+iy_{2^n-1})}{(\sqrt{2})^l}+\frac{(a_0+ib_0,\ldots,a_{2^n-1}+ib_{2^n-1})}{(\sqrt{2})^{l'}}\right)=$$

$$\frac{1}{\sqrt{2}(\sqrt{2})^{l'}}\left((\sqrt{2})^{l'-l}(x_0+iy_0,\ldots,x_{2^n-1}+iy_{2^n-1})+(a_0+ib_0,\ldots,a_{2^n-1}+ib_{2^n-1})\right)$$

de donde se deduce que $(\sqrt{2})^{l'-l}$ debe ser un número entero y por tanto l y l' deben tener igual paridad.

- Recíproco

  Sea P una matriz unitaria cuyas filas son todos estados discretos de igual paridad, queremos mostrar que P aplicada a un estado discreto $|\psi\rangle$ devuelve un nuevo estado discreto.

  Si la coordenada j-ésima de $|\psi\rangle$ se denota por $\frac{a_j+b_ji}{\sqrt{2^l}}$ donde a_j y b_j son enteros $\forall\ j \in \{0,1,...,2^n-1\}$ y las coordendas de los estados discretos conformantes de P por $\frac{x_j^m+y_j^mi}{\sqrt{2^{k_m}}}$ para hacer rerferencia a la coordenada j-ésima de la columna m de P, donde nuevamente x_j^m y y_j^m son enteros $\forall\ j,m \in \{0,1,...,2^n-1\}$, las coordenadas de $P|\psi\rangle$ serán de la forma:

  $$(P|\psi\rangle)_m = \sum_{j=0}^{2^n-1}\left(\frac{a_j+b_ji}{\sqrt{2^l}}\right)\left(\frac{x_j^m+y_j^mi}{\sqrt{2^{k_m}}}\right)$$

  Existe un M tal que k_M es máximo. Como todos los k_m son de igual paridad si multiplicamos a $(P|\psi\rangle)_m$ por $\sqrt{2^l}\sqrt{2^{k_M}}]$ obtendremos que $(P|\psi\rangle)_m$ es un entero. Cada factor quedará multiplicado por $\sqrt{2^{k_M-k_m}}$, pero sabemos que $k_M-k_m=2p_m\geq 0$ por tanto $\sqrt{2^{k_M-k_m}}=2^{p_m}$ quedando $(P|\psi\rangle)_m$ una suma de productos de números enteros

  $$\sqrt{2^l}\sqrt{2^{k_M}}(P|\psi\rangle)_m = \sum_{j=0}^{2^n-1}2^{p_m}(a_j+b_ji)(x_j^m+y_j^mi)$$

  Finalmente como P es unitaria conserva la norma de $|\psi\rangle$ se sabe que $||P|\psi\rangle||^2=1$ de donde se deduce que $||\sqrt{2^l}\sqrt{2^{k_M}}(P|\psi\rangle)||^2=2^{l+k_M}$, con lo que se concluye que $P|\psi\rangle$ es un estado discreto.

□

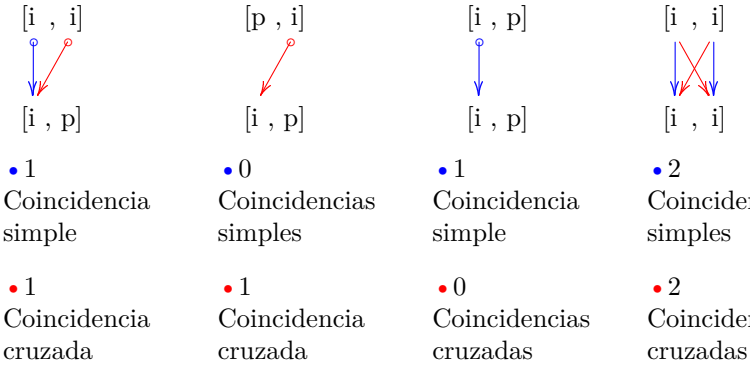
Esta caracterización de las compuertas discretas, junto al hecho de que estas deben ser transformaciones unitarias, impone las siguientes condiciones en la estructura de paridad de la matriz:

Corolario 4.4.1. *La cantidad de elementos impares de una columna es par.*

Demostración. Se deduce de que las columnas son estados discretos (ver observación 4.3.3). □

Definición 4.4.2. Coincidencias simples y cruzadas: Dadas dos columnas de cualquier compuerta discreta, diremos que hay una coincidencia simple (cruzada), cuando existen elementos en ambas columnas, correspondientes a la misma fila, con las partes reales o las partes imaginarias ambas impares (la parte real de una y la parte imaginaria de la otra ambas impares).

• Coincidencia simple	• Coincidencia cruzada
Las partes reales o las partes imaginarias de ambos son impares.	La parte real de una y la parte imaginaria de la otra son impares.



Corolario 4.4.2. *Dadas dos columnas de una matriz discreta las coincidencias tanto simples como cruzadas tienen que darse en cantidades pares.*

Demostración. Al ser las dos columnas ortogonales entre sí el producto interno entre ellas es 0. Por tanto imponiento que tanto la parte real como la imaginaria de este producto es 0 se concluye el resultado. □

Las propiedades anteriores implican a su vez una condición mucho más sencilla de comprobar:

Corolario 4.4.3. *Dadas dos columnas de una matriz discreta la coincidencia de elementos impares en las mismas coordenadas tienen que ser una cantidad par.*

Demostración. Cuando en una posición se produce una única coincidencia simple o cruzada esta debe provenir de una coincidencia de coordenadas impares (si no se produciría una y una o dos y dos). Por el corolario anterior, como debe haber una cantidad par, para compensarla, debe de haber otra coincidencia del mismo tipo, ya que si se compensa con una coincidencia proveniente de un elemento par y uno impar, se producirá otra que a su vez necesitará ser compensada. □

Finalmente es importante observar que dado que P es unitaria todas las propiedades que valen para columnas también valen para filas.

4.4.2. Demostración de la reducibilidad en el caso de dos qubits

Dada $P \in \mathcal{P}$, como todas sus columnas son estados discretos de niveles con la misma paridad, se puede definir el nivel de una matriz discreta a partir de los niveles de los estados componentes:

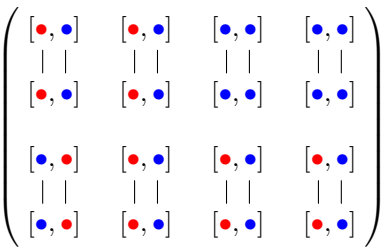
Definición 4.4.3. Dada $P \in \mathcal{P}$, decimos que P tiene nivel k, si k es el máximo de los niveles de las columnas de P. Al conjunto de matrices discretas de nivel k lo denotaremos por P_k.

Con la convención anterior es fácil definir qué es una matriz reducible:

Definición 4.4.4. Se dirá que $P \in \mathcal{P}_k$ es reducible si $H_0 P \in \mathcal{P}_{k-1}$.

En el caso de las compuertas discretas de dos qubits, los requisitos impuestos por la observación 4.4.1 nos proporcionan todas las herramientas necesarias para demostrar la reducibilidad. Aunque la idea detrás de la prueba es similar a la de la reducibilidad de los estados discretos, ahora debemos trabajar con la reducibilidad de muchos estados discretos simultáneamente. Además, tendremos que trabajar tanto con las filas como con las columnas de las compuertas discretas.

La condición de reducibilidad en el contexto de los estados discretos (observación 4.3.1) es totalmente reutilizable en este nuevo contexto. En efecto, la matriz correspondiente a la compuerta discreta H_0 actúa sobre las columnas, y la única condición que necesitamos garantizar es que en cada columna, si H_0 se aplica desde la izquierda, las posiciones $2p$ y $2p+1$ para todo $0 \leq p < 2^{n-1}$ tienen la misma configuración de paridad, como mostramos en el siguiente ejemplo.



Configuración de una matriz reducible.

Cuando queremos actuar sobre una matriz P con las compuertas permitidas en nuestro modelo, para transformar la matriz a una forma reducible, tenemos que tener en cuenta las siguientes consideraciones:

- Si la matriz P se multiplica por la izquierda por otra matriz Q, entonces Q actúa sobre las columnas de P. Así, si queremos por ejemplo intercambiar las posiciones 2 y 4 de la tercera columna, podemos utilizar la matriz de permutación que realiza esta acción. No obstante, intercambiaremos las posiciones 2 y 4 de cada columna. De hecho, al hacer esto intercambiamos las filas 2 y 4 de P.
- Por otro lado, si la matriz P se multiplica por la derecha por otra matriz Q estamos actuando sobre las filas de P. Por ejemplo si consideramos $Q = R^t$, como R actúa sobre los dos primeros elementos de un vector, entonces R^t "aplicará R" a los dos primeros elementos de cada fila. Por tanto, con R^t estamos modificando las dos primeras columnas de P.

En este contexto es útil definir un nuevo tipo de configuración de paridad, que nos permite actuar con R (por la izquierda) y R^t (por la derecha) sobre una matriz de forma que se preserve su nivel.

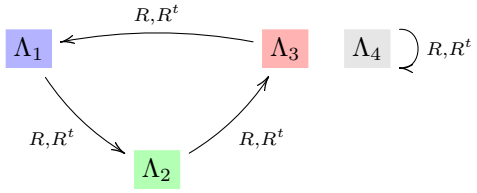
Definición 4.4.5. Una matriz $P \in \mathcal{P}$ es estándar si todos los elementos de las submatrices de la forma $\begin{pmatrix} p_{2j,2k} & p_{2j,2k+1} \\ p_{2j+1,2k} & p_{2j+1,2k+1} \end{pmatrix}$ con $0 \leq j, k < 2$ tiene igual paridad.

En el caso de dos qubits tendremos 4 submatrices que comparten paridad y, utilizando la observación 4.3.2, es fácil comprobar que R no altera el nivel de las matrices estándar de dos qubits. Por otro lado, estas matrices verifican la siguiente propiedad:

Proposición 4.4.1. *Cada matriz de dos qubits $P \in \mathcal{P}$ puede transformarse en una matriz estándar mediante matrices de permutación.*

Demostración. Si hay alguna columna con dos elementos impares, podemos ordenar las filas de forma que estos elementos ocupen las dos primeras posiciones. Aplicando la observación 4.4.3, podemos concluir que los elementos de las columnas de todas las submatrices P tienen la misma paridad. Podemos repetir este proceso por filas, y como este intercambio no afecta a la configuración de las columnas, la matriz estará en una forma estándar. □

Al igual que ocurría con los estados cuánticos, necesitamos apelar a las compuertas R y R^t, que actuarán por la izquierda y por la derecha respectivamente. Mediante la observación 4.3.2, podemos manipular una matriz discreta de dos qubits en forma estándar con los operadores, dentro del nivel de la matriz discreta. Estas compuertas actúan sobre las dos primeras filas y las dos primeras columnas respectivamente, y el siguiente diagrama muestra las transiciones entre las configuraciones de paridad generadas por R y R^t.



Los conjuntos de configuraciones de paridad en el diagrama anterior son:

R-Columnas de submatrices	R^t-Filas de submatrices

$$\Lambda_1=\left\{\begin{bmatrix}[i,i]\\[p,p]\end{bmatrix},\begin{bmatrix}[p,p]\\[i,i]\end{bmatrix}\right\} \qquad \Lambda_1=\left\{\begin{matrix}[i,i]\ ,[p,p]\\[p,p]\ ,[i,i]\end{matrix}\right\}$$

$$\Lambda_2=\left\{\begin{bmatrix}[p,i]\\[p,i]\end{bmatrix},\begin{bmatrix}[i,p]\\[i,p]\end{bmatrix}\right\} \qquad \Lambda_2=\left\{\begin{matrix}[p,i]\ ,[p,i]\\[i,p]\ ,[i,p]\end{matrix}\right\}$$

$$\Lambda_3=\left\{\begin{bmatrix}[p,i]\\[i,p]\end{bmatrix},\begin{bmatrix}[i,p]\\[p,i]\end{bmatrix}\right\} \qquad \Lambda_3=\left\{\begin{matrix}[p,i]\ ,[i,p]\\[i,p]\ ,[p,i]\end{matrix}\right\}$$

$$\Lambda_4=\left\{\begin{bmatrix}[p,p]\\[p,p]\end{bmatrix},\begin{bmatrix}[i,i]\\[i,i]\end{bmatrix}\right\} \qquad \Lambda_4=\left\{\begin{matrix}[p,p]\ ,[p,p]\\[i,i]\ ,[i,i]\end{matrix}\right\}$$

Si una matriz discreta de dos qubits está en forma estándar, las filas y columnas de sus submatrices (introducidas en la definición 4.4.5) pertenecen a los siguientes conjuntos: $\Lambda_1 \cup \Lambda_4$ en el caso de elementos pares y $\Lambda_2 \cup \Lambda_3$ en el caso de elementos impares.

Definición 4.4.6. Dada una matriz de dos qubit $P \in \mathcal{P}$ en forma estándar y una submatriz de P, $P_{j,k}$, entonces $P_{j,k}$ es par (impar) si todos sus elementos son pares (impares).

Nótese que toda submatriz de un qubit $P \in \mathcal{P}$ en forma estándar tiene que ser par o impar, debido a la forma estándar de la matriz.

Definición 4.4.7. Dada una matriz de dos qubit $P \in \mathcal{P}$ en forma estándar y una submatriz de P, $P_{j,k}$, diremos que $P_{j,k}$ es homogénea si el número de coincidencias entre sus columnas, tanto simples como cruzadas, es par. En caso contrario diremos que $P_{j,k}$ es no homogénea.

Proposición 4.4.2. *En una matriz estándar de dos qubits $P \in \mathcal{P}$, una submatriz $P_{j,k}$ es no homogénea si y sólo si tiene una columna en Λ_2 y la otra en Λ_3.*

Demostración. Toda submatriz de P es par o impar porque P es estándar. Si $P_{j,k}$ es par, es trivial comprobar que el número de coincidencias entre sus columnas, tanto simples como cruzadas, es par. Si no es así, las columnas de $P_{j,k}$ pertenecen a $\Lambda_2 \cup \Lambda_3$. Si ambas columnas pertenecen a Λ_2, o ambas pertenecen a Λ_3, siempre hay dos coincidencias simples o dos coincidencias cruzadas. El

caso restante, cuando una columna pertenece a Λ_2 y la otra a Λ_3 es el único en el que $P_{j,k}$ no es homogéneo: tiene una coincidencia simple y una coincidencia cruzada. □

Observación 4.4.1. La definición de submatriz homogénea o no homogénea es independiente de si consideramos las filas en lugar de las columnas.

Proposición 4.4.3. *Si una matriz estándar de dos qubits $P \in \mathcal{P}$ tiene una submatriz no homogénea, entonces todas sus submatrices deben ser no homogéneas.*

Demostración. Supongamos, sin pérdida de generalidad, que la submatriz no homogénea es $P_{0,0}$. Para satisfacer la observación 4.4.2 en las columnas 1 y 2, la submatriz $P_{1,0}$ debe tener una coincidencia cruzada y una coincidencia simple, porque $P_{0,0}$ es no homogénea. Entonces $P_{1,0}$ es no homogénea. Aplicando el mismo argumento a las filas 1 y 2 podemos asegurar que $P_{0,1}$ también es no homogénea, y transitivamente $P_{1,1}$ también es no homogénea. □

Definición 4.4.8. Una matriz de dos qubit $P \in \mathcal{P}$ en forma estándar es homogénea si todas sus submatrices son homogéneas.

Proposición 4.4.4. *Toda matriz de dos qubit $P \in \mathcal{P}$ en forma estándar se puede transformar en una homogénea.*

Demostración. Por la proposición 4.4.3, si una submatriz de P es no homogénea entonces todas son no homogéneas. Entonces $P_{0,0}$ y $P_{0,1}$ están conformadas por una columna de Λ_2 y otra de Λ_3. Utilizando una matriz de permutación, podemos intercambiar las columnas de P de forma que las columnas de $P_{0,0}$ pertenezcan a Λ_2 y las de $P_{0,1}$ a Λ_3. Las nuevas submatrices $P_{0,0}$ y $P_{0,1}$ son ahora homogéneas. Entonces, utilizando de nuevo la proposición 4.4.3, el resto de las submatrices deben ser homogéneas también. Por otro lado estas permutación de columnas entre elementos de Λ_2 y de Λ_3 no altera el que la matriz sea estándar. □

Proposición 4.4.5. *Toda matriz de dos qubits $P \in \mathcal{P}$ en forma estándar y homogénea se puede transformar en una matriz en la que todos sus elementos son pares.*

Demostración. La demostración puede hacerse en dos pasos.

Paso 1. Transformar $P_{0,0}$ y $P_{0,1}$ en submatrices pares.

(a) Si las filas de la submatriz $P_{0,0}$ de P pertenecen a Λ_2 (Λ_3) aplique R^t por la derecha dos veces (una vez), para que las filas de $P_{0,0}$ pertenezcan a Λ_1.
Si $P_{0,0}$ fuera una submatriz par no tenemos que hacer nada.

(b) Permutar las submatrices $P_{0,0}$ y $P_{0,1}$.

(c) Repetir el proceso (a) con la nueva submatriz $P_{0,0}$.

Paso 2. Transformar $P_{1,0}$ y $P_{1,1}$ en submatrices pares.

La configuración establecida en el paso 1 impone fuertes restricciones a las submatrices $P_{1,0}$ y $P_{1,1}$. Si analizamos las coincidencias entre columnas pertenecientes a $P_{0,0}$, $P_{0,1}$ o una a $P_{0,0}$ y la otra a $P_{0,1}$, como todos los elementos de estas submatrices son pares, las mismas columnas correspondientes a $P_{1,0}$, $P_{1,1}$ o ambas submatrices tienen que auto-satisfacer las coincidencias. Por lo tanto, las columnas de $P_{1,0}$ y $P_{1,1}$ pertenecen al conjunto $\Lambda_4 \cup \Lambda_i$ con $i \in \{1, 2, 3\}$.

En este punto la matriz P puede ser no estándar, pero esto se puede cambiar fácilmente. Utilizando el hecho de que las submatrices superiores son todas pares, podemos poner la matriz en forma estándar de nuevo mediante el intercambio de columnas. El resultado es una matriz homogénea porque las submatrices superiores son homogéneas (proposición 4.4.3).

Entonces, sólo tenemos que intercambiar las submatrices inferior y superior de P y utilizar R (R^2) si las columnas de las nuevas submatrices superiores pertenecen a Λ_3 (Λ_2). Nótese que esta operación no afecta a la configuración de las submatrices inferiores que ya hemos ajustado.

□

Obsérvese que una compuerta de dos qubits $P \in \mathcal{P}$ es reducible si la configuración de paridad de los elementos de las filas superiores (1 y 2) e inferiores (3 y 4) de P coinciden. En otras palabras, las columnas de las submatrices de P pertenecen al conjunto $\Lambda_2 \cup \Lambda_4$.

Teorema 4.4.2. *Cada compuerta de dos qubit $P \in \mathcal{P}$ puede transformarse en una reducible sin cambiar su nivel.*

Demostración. Utilizando los resultados anteriores 4.4.1, 4.4.4 y 4.4.5, ponemos la matriz en forma estándar, la hacemos homogénea y luego hacemos todos sus elementos pares.

Luego, aplicando R a la izquierda transformamos las columnas de $P_{0,0}$ y $P_{0,1}$ pertenecientes a Λ_1 en columnas del conjunto Λ_2, manteniendo las columnas que pertenecen al conjunto Λ_4. Finalmente intercambiamos las submatrices inferior y superior y hacemos lo mismo.

El resultado final es una matriz reducible que pertenece al mismo nivel que la inicial. □

Así, dada una compuerta de dos qubits $P \in \mathcal{P}_k$ con $k > 0$, se puede transformar en otra $P' \in \mathcal{P}_{k-1}$. Repitiendo este procedimiento k veces transformaremos P en otra $\tilde{P} \in \mathcal{P}_0$ y, aplicando una permutación y una compuerta cuántica $V_j^{s_j}$ $(0 \leq s_j \leq 3)$ a cada columna $0 \leq j \leq 3$, reduciremos $\tilde{P}$ a la matriz identidad. Las compuertas cuánticas utilizadas son productos de las compuertas H y G y, por la observación 4.2.1, sus inversas también lo son. Por tanto, tomando la inversa de la composición de estas compuertas cuánticas, demostramos finalmente que se pueden obtener una compuerta de dos qubits cualesquiera $P \in \mathcal{P}$ a partir de las compuertas H y G.

Teorema 4.4.3. *Cada compuerta cuántica de dos qubits puede descomponerse en un producto de compuertas cuánticas H y G.*

4.4.3. Diferencias con el modelo de Kliuchnikov

Nuestro trabajo de puertas cuánticas discretas va en la misma dirección que el trabajo de Kliuchnikov et al. [46] que se centra, como todos los modelos introducidos hasta la fecha, en el conjunto de puertas cuánticas. Nos referiremos a él como modelo KMM. Demostraron la equivalencia del conjunto de compuertas cuánticas generadas a partir del conjunto $\{H, CNOT, T = Diag(1, e^{\pi i/4})\}$ y el conjunto de compuertas cuánticas sobre el anillo $\mathbb{Z}[1/\sqrt{2}, i]$, en el caso de un solo qubit, y conjeturan que esta propiedad se mantiene para cualquier número de qubits. La conjetura fue demostrada por Giles y Selinger [53], utilizando la técnica estándar de descomposición en matrices de dos niveles [18]. En este modelo, las coordenadas de los estados y los elementos de las compuertas cuánticas pertenecen, excepto por un factor de normalización 2^{-k}, al anillo

$$\mathbb{Z}[\sqrt{2}, i] = \{a + bi + c\sqrt{2} + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Z}\}$$

El modelo que presentamos en este trabajo es más sencillo que el modelo KMM, si comparamos los respectivos anillos de escalares: $\mathbb{Z}[i]$ frente a $\mathbb{Z}[\sqrt{2}, i]$. En el modelo KMM, cada nivel de estados se divide en dos niveles de nuestro modelo:

$$\text{KMM nivel } k: \ a + bi + c\sqrt{2} + d\sqrt{2}i \ \Rightarrow \ \begin{cases} a + bi & \text{nivel } 2k \\ c + di & \text{nivel } 2k - 1 \end{cases}$$

La supresión del $\sqrt{2}$ en el anillo $\mathbb{Z}[\sqrt{2}, i]$ tiene dos consecuencias para nuestro modelo. En primer lugar, los conjuntos de estados discretos y compuertas cuánticas discretas de un qubit son finitos. En segundo lugar, no es posible utilizar la técnica estándar de descomposición en matrices de dos niveles [18], ya que $\Lambda^j H$ no es una compuerta cuántica discreta ($j \geq 1$). En consecuencia, la demostración de la caracterización de las compuertas cuánticas discretas debe ser completamente nueva, como se hizo en el trabajo para 2−qubits.

4.5. Universalidad del modelo

Finalmente en esta sección se muestra que el conjunto de compuertas que se puede alcanzar a través de las compuertas conformantes de nuestro modelo es un conjunto universal, esto es:

Definición 4.5.1 (Conjunto Universal)**.** Se dice que un conjunto de compuertas $\mathcal{G}$ es un **conjunto universal** si el subgrupo generado por la aplicación de elementos de $\mathcal{G}$ es denso en $\Upsilon(\mathcal{H}^n)$ para todo $n \geq n_0$ con un n_0 fijo y típicamente pequeño.

La condición de que un conjunto sea denso en el espacio de matrices unitarias de una dimensión dada es equivalente a pedir que todo elemento U tenga arbitrariamente cerca un elemento de dicho conjunto con alguna norma que se establezca.

En particular nosotros utilizaremos la misma que se utiliza en [25]. Diremos que la compuerta $\tilde{U}$ aproxima a la compuerta U con precisión ε si $||U - \tilde{U}|| < \varepsilon$ con la norma usual de matrices:

$$||A|| := \max_{|\psi\rangle} \frac{||A|\psi\rangle||}{|||\psi\rangle||}.$$

En [25] se define la base

$$\mathcal{Q} = \{H, V, V^{-1}, \Lambda(X), \Lambda^2(X)\}$$

y se prueba que:

Proposición 4.5.1. *Cualquier operador unitario U, para un número dado de qubits, puede ser realizado con precisión δ por un algoritmo polinomial en el número de compuertas de la base $\mathcal{Q}$ utilizando ancillas.*

De la sección 4.2 se deduce que todas las compuertas en $\mathcal{Q}$ pueden ser obtenidas exactamente a partir de las compuertas conformantes y qubits auxiliares. Por tanto se deduce inmediatamente que $\{H, G\}$ conforman un conjunto universal.

4.5.1. Trabajos futuros

Compuertas discretas en dimensiones mayores

Queda como trabajo futuro extender el resultado del último apartado de las conclusiones para matrices discretas en el espacio de más de dos qubits.

Sobre este punto se sabe que no se puede extender el mismo procedimiento que se hizo para matrices de dos qubits. En este espacio se demostró que la representación de toda compuerta discreta puede ser llevada a una matriz estándar. Una condición necesaria y suficiente para que una matriz

esté de forma estándar es que sus filas o columas repitan dos a dos paridades en sus elementos conformantes.

La matriz

$$M = \begin{pmatrix} 7 & 3 & i & i & 2 & 0 & 0 & 0 \\ -1-i & -1+i & 1-i & 1-i & 6+3i & 1-2i & -2+i & i \\ -i & -2+3i & 3+3i & -3+3i & -i & -1 & -1-i & 1+3i \\ -2-2i & 2+2i & -3+2i & -1+2i & 2+2i & -2+2i & 2-i & -3i \\ -i & 2i & -1-2i & -2+2i & -i & 6 & 2+i & -2 \\ -1-i & 4+i & -1-i & -1-2i & -1+i & -1+2i & -1+i & -2+5i \\ -i & 1+3i & -1+3i & 1-4i & -1-i & 3 & -2-i & 3-i \\ 0 & -i & -3-2i & -2+2i & -i & 0 & -6-2i & -i \end{pmatrix}$$

es una matriz discreta en el espacio de tres qubits y todos sus vectores se encuentran en el nivel F_6. Sin embargo, si se mira las paridades de sus filas:

$$M = \begin{pmatrix} I & I & I & I & P & P & P & P \\ P & P & P & P & I & I & I & I \\ I & I & P & P & I & I & P & P \\ P & P & I & I & P & P & I & I \\ I & P & I & P & I & P & I & P \\ P & I & P & I & P & I & P & I \\ I & P & P & I & P & I & I & P \\ P & I & I & P & I & P & P & I \end{pmatrix}$$

no hay dos filas con igual paridad en cada una de sus coordenadas, por tanto no es estandarizable. Sin embargo, se encontró un procedimiento en este caso para reducir la matriz, es decir bajarla de nivel.

Capítulo 5

Completitud de bases

5.1. Introducción

El modelo de computación cuántica discreta introducido en el capítulo anterior (4) se centra en los estados cuánticos discretos (en adelante estados discretos). Como se vió, su objetivo es definir un conjunto de estados discretos que verifique las siguientes propiedades: describe estados reales de física cuántica, preserva las principales características de los estados cuánticos (superposición y entrelazamiento), permite aproximar estados cuánticos generales y, sobre todo, contiene estados cuánticos simples. El conjunto de estados presentado es el más simple posible, el conjunto de estados de coordenadas gaussianas, que incluye todos los estados cuánticos cuyas coordenadas en la base computacional, salvo un factor de normalización $\sqrt{2^{-k}}$, pertenecen al anillo de los enteros de Gauss (coordenadas gaussianas)

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Para poder alcanzar estos estados se introducen un conjunto de puertas cuánticas que verifican las siguientes propiedades: contiene puertas cuánticas que transforman estados discretos en estados discretos y genera todos los estados discretos. El modelo incluye dos puertas cuánticas elementales que verifican las propiedades anteriores, H y G. La puerta de Hadamard H permite la superposición mientras que la otra, G, es una puerta de 3 qubits. Dos de ellos son qubits de control, mientras que el tercero es el objetivo. Si los qubits de control están en el estado $|1\rangle$ entonces la puerta V se aplica al tercer qubit, siendo

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

Estas puertas cuánticas permiten construir todos los estados de coordenadas gaussianas (Teorema 4.3.2) y permiten identificar estos estados con los estados discretos en los que se basa el modelo de computación cuántica discreta.

Entonces un $n-$qubit Ψ es un estado discreto si y sólo si existe un número natural k tal que

$$\Psi = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^n-1} (a_j + b_j i)|j\rangle \qquad \text{con } a_j, b_j \in \mathbb{Z} \text{ para todo } 0 \leq j < 2^n \tag{5.1}$$

Por tanto, el estado discreto Ψ está asociado a la ecuación diofántica

$$a_0^2 + b_0^2 + \cdots + a_{2^n-1}^2 + b_{2^n-1}^2 = 2^k \quad \text{con } a_j, b_j \in \mathbb{Z} \text{ para todo } 0 \leq j < 2^n \tag{5.2}$$

El índice k en el factor de normalización y proporciona un punto de vista interesante sobre los estados discretos (ver capítulo 4). Los estados pueden clasificarse en diferentes niveles de discretización en función de k. Dado un estado discreto, este pertenece al nivel k si k es el menor número natural para el que se cumple la ecuación (5.2). Estos niveles representan el grado de precisión o aproximación de los estados discretos en relación con los estados continuos.

Los resultados que presentamos en este capítulo están estrechamente ligados a las propiedades y a la conjetura sobre la generación de puertas cuánticas discretas (en adelante puertas discretas) expuesta en el capítulo (4). Recordando que las puertas discretas se definen como aquellas puertas cuánticas que dejan invariante el conjunto de estados discretos y que una puerta cuántica es una puerta discreta si y sólo si en su representación matricial, con respecto a la base computacional, sus columnas son estados discretos de niveles de la misma paridad (teorema 4.4.1). Obviamente, las filas de las puertas discretas también verifican la misma propiedad. También se demuestra una propiedad sorprendente que inicialmente no formaba parte de los objetivos del modelo de computación cuántica discreta: toda puerta discreta de dos qubits puede descomponerse en un producto de puertas H y G (Teorema 4.4.3). Finalmente se conjetura que toda puerta discreta $n-$qubit, con $n \geq 3$, también puede generarse dentro del modelo. En este capítulo se tabajará sobre está conjetura ampliandola de la siguiente manera:

Conjetura 5.1.1. Dado un conjunto de estados discretos de niveles de la misma paridad y ortogonales dos a dos, es posible construir todos ellos simultáneamente (aplicando un circuito dado a diferentes estados de la base computacional) utilizando las puertas conformadoras H y G.

Obsérvese que la conjetura también tiene sentido para $2-$qubits, ya que en el capítulo anterior sólo se ha demostrado para conjuntos de 4 estados discretos. Y nótese que la conjetura también es interesante en el caso no discreto, ya que se pregunta por la posibilidad de construir simultáneamente hasta 2^n estados cuánticos simultáneamente. En este caso la conjetura es obviamente cierta. Basta con completar la base ortonormal, por ejemplo mediante el método de Gram-Schmidt, y descomponer la matriz unitaria resultante en producto de puertas cuánticas básicas. Por tanto, tiene sentido preguntarse si lo es en el caso de la computación cuántica discreta.

Por una cuestión de simplicidad, antes de continuar, vamos a relajar la definición del nivel de un estado discreto dada en el capítulo 4 a cualquier valor de k para el cual el estado discreto verifica la Ecuación (5.2). Llamaremos a estos valores *niveles generalizados*. Nótese que si k es un nivel generalizado de un estado discreto, entonces $k+2$ también lo es. Para demostrarlo, basta con dividir el factor de normalización por 2 y multiplicar por 2 las coordenadas gaussianas de la representación del estado discreto con nivel generalizado k (en la ecuación (5.1)). Entonces, un estado discreto tiene nivel generalizado k si y sólo si es de la forma $k_0 + 2j$, donde k_0 es el nivel del estado discreto y j un número natural. Esta propiedad permite escribir todos los estados discretos (con niveles de la misma paridad) en el mismo nivel generalizado.

Veamos que, de alguna manera, construir un conjunto de estados discretos ortogonales es equivalente a completar el conjunto a una base ortonormal. Por esta razón el objetivo principal en este capítulo es dar respuesta al siguiente problema.

Problema 5.1.1. Dado un número natural k y $\Psi_1, \ldots, \Psi_j$ $n-$qubits discretos con nivel generalizado k, $1 \leq j < 2^n$, tal que $\langle \Psi_i | \Psi_m \rangle = 0$ para todo $1 \leq i < m \leq j$, entonces ¿Existe un $n-$qubit discreto con nivel generalizado k, Ψ, tal que $\langle \Psi_i | \Psi \rangle = 0$ para todo $1 \leq i \leq j$?

Basándonos en el siguiente resultado: toda puerta dicreta de $2-$qubits puede descomponerse en un producto de puertas H y G (Teorema 4.4.3); es fácil establecer la siguiente equivalencia: para $2-$qubits, la Conjetura 5.1.1 es verdadera si y sólo si el Problema 5.1.1 tiene una respuesta afirmativa.

Hemos establecido la relación entre el Problema 5.1.1, cuyo estudio es el objetivo de este capítulo, y la construcción simultánea de estados discretos de niveles de la misma paridad y ortogonales dos a dos (Conjetura 5.1.1). La resolución de este problema nos permitiría construir bases con características especiales y nos ayudaría a demostrar la conjetura de que cualquier puerta discreta de $n-$qubit, con $n \geq 3$, se puede generar con las puertas cuánticas elementales del modelo de computación cuántica discreta [54].

Es claro que el problema que se estudia en este capítulo tiene importantes conexiones con el modelo de computación cuántica discreta y, en consecuencia, con la computación cuántica. Como vamos a ver, también tiene implicaciones en campos científicos como la teoría de números, la geometría de números y la teoría de lattices. Además, creemos que los modelos discretos tendrán una gran influencia en la teoría de la información cuántica e, indirectamente, en la propia física cuántica.

Ahora, analicemos la conexión entre la computación cuántica discreta y el teorema de los cuatro cuadrados de Lagrange. El hecho que establece esta conexión es que los estados discretos tienen que satisfacer la ecuación (5.2). El teorema de los cuatro cuadrados de Lagrange [55] dice que todo número natural es una suma de cuatro números enteros al cuadrado y, en consecuencia, garantiza que existen estados discretos para cualquier nivel $k \geq 0$ y para cualquier número de qubits $n \geq 1$.

Como ya se ha comentado, el modelo de computación cuántica discreta tendría mejores propiedades si todos los sistemas ortonormales de estados discretos pudieran extenderse siempre a una base ortonormal, es decir, si el Problema 5.1.1 tuviera una respuesta afirmativa.

El problema 5.1.1 es una versión ortogonal del teorema de los cuatro cuadrados de Lagrange, es decir, el estado discreto Ψ debe verificar la Ecuación Diofantina (5.2) y las siguientes condiciones de ortogonalidad:

$$\langle \Psi_i | \Psi \rangle = 0 \quad \text{for all } 1 \leq i \leq j$$

Nótese que dado un valor de k, si la Ecuación 5.2 tiene solución para un $1-$qubit, entonces tiene solución para todo número de qubits $n \geq 2$. Sin embargo, esta generalización no es necesariamente cierta para el 5.1.1, debido a las condiciones de ortogonalidad. Por tanto, el problema tiene entidad propia para cualquier número de qubits n.

El Problema 5.1.1 resulta ser una cuestión difícil en la Teoría de Números y tiene profundas implicaciones. Por ello comenzamos con la simplificación que más se parece al problema de los cuatro cuadrados de Lagrange: $n = 2$, enteros como coordenadas en lugar de enteros gaussianos y factor de normalización $\sqrt{p}$, siendo p un número primo, en lugar de $\sqrt{2^k}$.

Problema 5.1.2. Dado un número primo p y $v_1, \ldots, v_k \in \mathbb{Z}^4$, $1 \leq k \leq 3$, tal que $\|v_i\|^2 = p$ para todo $1 \leq i \leq k$ y $\langle v_i | v_j \rangle = 0$ para todo $1 \leq i < j \leq k$, entonces, ¿existe un vector $v = (x_1, x_2, x_3, x_4) \in Z^4$ tal que $\langle v_i | v \rangle = 0$ para todo $1 \leq i \leq k$ y $\|v\|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$?

El esquema del presente capítulo es el siguiente: en primer lugar ponemos en contexto el Problema (5.1.2), discutiendo los principales resultados relacionados con el problema de los cuatro cuadrados de Lagrange en la sección 5.2. Luego demostramos el resultado principal en la seccion 5.3. En la Sección 5.4 exponemos varias generalizaciones y conjeturas relacionadas con los problemas propuestos. En la Sección 8 incluimos algunas conclusiones.

5.2. Principales resultados relacionados con el problema de los cuatro cuadrados de Lagrange

Mucho antes de que Lagrange demostrara su teorema, Diofanto se había preguntado si todo número entero positivo podía representarse como la suma de cuatro cuadrados perfectos mayores o iguales a cero. Esta cuestión se conoció más tarde como la conjetura de Bachet, por la traducción que hizo Bachet de Diofanto en 1621. Paralelamente, Fermat propuso el problema de representar cada número entero positivo como una suma de a lo sumo n números $n-$gonales. Lagrange [55] demostró el caso $n = 4$ del teorema de los números poligonales de Fermat en 1770, resolviendo también la conjetura de Bachet. Gauss [56] demostró el caso triangular en 1796 y el teorema completo de los números poligonales no se resolvió hasta que fue finalmente demostrado por Cauchy en 1813. Más tarde, en 1834, Jacobi descubrió una fórmula sencilla para el número de representaciones de un número entero como la suma de cuatro cuadrados enteros.

El mismo año en que Lagrange demostró su teorema, Waring se preguntó si cada número natural k tiene un entero positivo asociado s tal que todo número natural es la suma de como máximo s números naturales a la potencia k. Por ejemplo, todo número natural es la suma de a lo sumo 4 cuadrados, 9 cubos, o 16 cuartas potencias. La respuesta afirmativa al problema de Waring, conocida como el teorema de Hilbert-Waring, fue proporcionada por Hilbert en 1909.

Una generalización natural del problema de Lagrange es la siguiente: dados los números naturales a, b, c y d, ¿podemos resolver $n = ax_1^2+bx_2^2+cx_3^2+dx_4^2$ para todos los enteros positivos n con enteros x_1, x_2, x_3 y x_4? El teorema de los cuatro cuadrados de Lagrange respondió positivamente el caso $a = b = c = d = 1$ y la solución general fue dada por Ramanujan [57]. Demostró que si suponemos que $a \leq b \leq c \leq d$ entonces hay exactamente 54 opciones posibles para a, b, c y d tales que el problema es resoluble con enteros x_1, x_2, x_3 y x_4 para todo $n \in \mathbb{N}$. Ye [58] establece fórmulas para el número de representaciones de enteros por las formas cuadráticas $x_1^2+\cdots+x_k^2+m(x_{k+1}^2+\cdots+x_{2k}^2)$ para $m = 2, 4$ y Eum et al. [59] estudian el número de representación de un entero no negativo por la forma cuadrática cuaternaria $x_1^2 + 2x_2^2 + x_3^2 + x_4^2 + x_1x_3 + x_1x_4 + x_2x_4$. Sun [60] y Ju et al. [61] han estudiado una generalización de los problemas de Lagrange y Ramanujan, en la que x_1, x_2, x_3 y x_4 se sustituyen por números octogonales generalizados.

Otra generalización, debida a Mordel [62], trata de representar formas cuadráticas binarias enteras definidas positivas en lugar de enteros positivos. Demostró que la forma cuadrática $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ representa todas las formas cuadráticas binarias enteras definidas positivas.

Sun et al. [63, 60] ha propuesto algunos refinamientos del teorema de Lagrange como, por ejemplo, el siguiente: $n \in \mathbb{N}$ puede escribirse como $x_1^2+x_2^2+x_3^2+x_4^2$ con $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ tal que $x_1+x_2+x_3$ (o $x_1 + 2x_2$, o $x_1 + x_2 + 2x_2$) es un cuadrado (o un cubo).

La ecuación $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, para el número natural n, no siempre tiene solución si x_1, x_2, x_3 y x_4 tienen que ser números primos. A pesar de este hecho, Ching [64] demuestra que para grandes $n \equiv 4 \bmod 24$ siempre hay una solución con un primo y tres casi-primos y Harman et al. [65] definen $E_4(N)$ como el cardinal del conjunto de todos los números naturales $n \leq N$ tales que $n \equiv 4 \bmod 24$ y no pueden representarse como la suma de los cuadrados de cuatro números primos, demostrando que $E_4(N) \ll N^{7/20+\epsilon}$. Chen [66] estudia las sumas monocromáticas de cuadrados de primos: dada una $k-$partición (una partición en k subconjuntos) de la secuencia de cuadrados de los primos y $s(k)$ el menor número entero positivo tal que todo entero suficientemente grande puede escribirse como la suma de no más de s(k) elementos, que pertenecen a uno de los conjuntos de la partición, entonces demuestra que $s(k) \ll k^{2+\epsilon}$ para un número positivo suficientemente pequeño ϵ y todo $k \geq 1$.

5.3. Versión ortogonal del teorema de los cuatro cuadrados de Lagrange

En primer lugar, introduzcamos algunos conceptos básicos. Dado un número natural $1 \leq k \leq 4$ y un conjunto de vectores $v_1, \ldots, v_k \in \mathbb{Z}^4$ tal que $\|v_i\|^2 = p$ para todo $1 \leq i \leq k$ y $\langle v_i | v_j \rangle = 0$ para todo $1 \leq i < j \leq k$, diremos que $S = \{ v_1, \ldots, v_k \}$ es un *sistema $p-$ortonormal* y en el caso $k = 4$ que S es una *base $p-$ortonormal*.

Dado un *sistema $p-$ortonormal* S, llamaremos *soporte de S*, *sop*(P), al conjunto $\{ i \mid \exists j$ tal que la $i-$ésima coordenada de v_j es distinta de cero$\}$ y diremos que $|sop(P)|$ es el *tamaño del soporte de S*.

En este contexto, el problema que nos ocupa (Problema 5.1.2) se plantea como sigue: dado un número primo p y un sistema $p-$ortonormal $S = \{ v_1, \ldots, v_k \}$, $1 \leq k \leq 3$, demostrar que existe $v \in \mathbb{Z}^4$ tal que $\langle v_i | v \rangle = 0$ para todo $1 \leq i \leq k$ y $\|v\|^2 = p$.

Para demostrar el resultado, consideramos cuatro casos. Tres de ellos se resuelven con técnicas básicas de álgebra lineal. Sin embargo, el cuarto caso es mucho más difícil, y requiere el uso de lattices y algunos resultados de teoría de números. Los detalles de este caso se incluyen en la sección B.

Caso 1: sistemas de un vector $p-$ortonormal.

Si el sistema $p-$ortonormal S tiene un único vector $v_1 = (x_1, x_2, x_3, x_4)$, la solución (válida para todo $p \geq 1$) es trivial: el vector requerido es, por ejemplo, $v = (x_2, -x_1, x_4, -x_3)$.

Caso 2: dos vectores $p-$ortonormales con soporte de tamaño 2.

Si el sistema $p-$ortonormal S tiene dos vectores con $|\text{sop}(S)| = 2$, la solución (válida para todo $p \geq 1$) es también trivial. Supongamos, sin pérdida de generalidad, que $\text{sop}(S) = \{1, 2\}$, $v_1 = (x_1, x_2, 0, 0)$ y $v_2 = (y_1, y_2, 0, 0)$. Entonces, el vector requerido es, por ejemplo, $v = (0, 0, x_1, x_2)$.

Caso 3: tres vectores $p-$ortonormales.

Si el sistema $p-$ortonormal S tiene tres vectores, su producto exterior nos permite obtener el vector requerido (válido para todo $p \geq 1$).

Utilizaremos identidades entre polinomios en muchas variables cuya demostración sólo requiere probar que la expansión polinómica de la diferencia de ambos miembros de las igualdades es igual a 0. A este tipo de demostración lo llamaremos *comprobación de polinomios*.

Dadas las coordenadas de los tres vectores de S, $v_1 = (x_1, x_2, x_3, x_4)$, $v_2 = (y_1, y_2, y_3, y_4)$ y $v_3 = (z_1, z_2, z_3, z_4)$, consideramos el producto exterior $t = (t_1, t_2, t_3, t_4)$ donde

$$t_1 = -\begin{vmatrix} x_2 & x_3 & x_4 \\ y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \end{vmatrix}, \; t_2 = \begin{vmatrix} x_1 & x_3 & x_4 \\ y_1 & y_3 & y_4 \\ z_1 & z_3 & z_4 \end{vmatrix}, \; t_3 = -\begin{vmatrix} x_1 & x_2 & x_4 \\ y_1 & y_2 & y_4 \\ z_1 & z_2 & z_4 \end{vmatrix} \text{ y } \; t_4 = \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}.$$

Por ser las coordenadas de t los cofactores de una matriz formada por los vectores fila $v1, v2, v3$ y t se sabe que $\langle v_i | t \rangle = 0$ para todo $1 \leq i \leq 3$.

Para calcular $\|t\|^2$, vamos a demostrar que $t_i^2 = p^2(p - x_i^2 - y_i^2 - z_i^2)$ para todo $1 \leq i \leq 4$. Lo hacemos para t_4 ya que, por simetría, la demostración para el resto de coordenadas de t es análoga.

Considerando los vectores $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ y $z = (z_1, z_2, z_3)$ podemos demostrar, de nuevo por comprobación de polinomios (los detalles se encuentran en el anexo B), que

$$\begin{aligned} t_4^2 &= \|x\|^2 \|y\|^2 \|z\|^2 + 2\langle x|y\rangle\langle x|z\rangle\langle y|z\rangle \\ &\quad -\|x\|^2\langle y|z\rangle^2 - \|y\|^2\langle x|z\rangle^2 - \|z\|^2\langle x|y\rangle^2. \end{aligned} \tag{5.3}$$

Ahora podemos demostrar que

$$\begin{aligned} p^2(p - x_4^2 - y_4^2 - z_4^2) &= \|x\|^2 \|y\|^2 \|z\|^2 + 2\langle x|y\rangle\langle x|z\rangle\langle y|z\rangle \\ &\quad -\|x\|^2\langle y|z\rangle^2 - \|y\|^2\langle x|z\rangle^2 - \|z\|^2\langle x|y\rangle^2, \end{aligned} \tag{5.4}$$

introduciendo a la derecha de la igualdad anterior los valores

$$\begin{array}{ll} \|x\|^2 = p - x_4^2, & \langle x|y\rangle = -x_4 y_4, \\ \|y\|^2 = p - y_4^2, & \langle x|z\rangle = -x_4 z_4, \\ \|z\|^2 = p - z_4^2, & \langle y|z\rangle = -y_4 z_4 \end{array}$$

y aplicando, una vez más, la comprobación polinómica.

Uniendo las ecuaciones 5.3 y 5.4, se concluye que $t_4^2 = p^2(p - x_4^2 - y_4^2 - z_4^2)$.

Finalmente, el vector $v = t/p$ tiene las propiedades requeridas: $\langle v_i|v\rangle = 0$ para todo $1 \leq i \leq 3$ y $\|v\|^2 = p$.

Caso 4: dos vectores $p-$ortonormales con soporte de tamaño > 2.

Dado un número primo p y un sistema $p-$ortonormal $S = \{ v_1, v_2 \}$ con $|\text{sop}(S)| > 2$, existe $v \in Z^4$ tal que verifica $\langle v_1|v\rangle = \langle v_2|v\rangle = 0$ y $\|v\|^2 = p$ (ver Teorema 5.3.2).

Para la demostración de esta parte ocuparemos la subsección B entera.

5.3.1. Demostración Caso 4: dos vectores $p-$ortonormales con soporte de tamaño > 2

Notación y propiedades básicas.

Consideramos $\mathbb{Z}^4$ como una parte del espacio vectorial $\mathbb{R}^4$ provista del producto interior $\langle v|w\rangle = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, donde $v = (x_1, x_2, x_3, x_4)$ y $w = (y_1, y_2, y_3, y_4)$ son vectores de $\mathbb{R}^4$, y con la base canónica $\{e_1, \ldots, e_4\}$.

Dado un conjunto de vectores linealmente independientes $v_1, \ldots, v_k \in \mathbb{R}^4$, generan el *lattice* $\Lambda = \{ b_1v_1 + \cdots + b_kv_k \mid b_1, \ldots, b_k \in \mathbb{Z} \}$ [67] y constituyen una *base de* Λ, B. Por lo tanto, la dimensión de Λ será k. A partir de ahora sólo consideraremos bases cuyos vectores pertenezcan a $\mathbb{Z}^4$, es decir, Λ será siempre un *lattice entero*.

Dado un punto $v \in \Lambda$, descrito por sus coordenadas en B, $v = (b_i)_B$, el número $N(v) = \|v\|^2 = \langle v|v\rangle$ se llama *norma de* v y puede calcularse mediante la expresión $N(v) = b^tGb$, donde G es la

matriz de los productos escalares de los vectores de B. El determinante de G, $\det(G)$, es un invariante de Λ cuya raíz cuadrada se denota por $\det(\Lambda)$. Así pues, $\det(\Lambda) = \sqrt{\det(G)}$ y, geométricamente, se interpreta como el volumen del paralelepípedo fundamental de Λ. La matriz G es simétrica y definida positiva y está asociada a una forma cuadrática que recoge las principales propiedades de Λ.

Consideremos la *matriz de coordenadas* V, formada por los vectores de la base B de Λ colocados por filas. Si V es una matriz cuadrada, podemos calcular el determinante de Λ a partir de V, $\det(\Lambda) = |\det(V)|$, y se cumple que $\det^2(V) = \det(G)$.

Sin embargo, no estamos interesados en Λ, sino en su *lattice ortogonal*

$$\Lambda^{\perp} = \{\, v \in \mathbb{Z}^4 \mid \langle v_i | v \rangle = 0 \text{ para todo } 1 \leq i \leq k \,\}$$

El método de resolución de sistemas de ecuaciones lineales diofantinas [68] calcula una base de $\Lambda^{\perp}$ con $4-k$ vectores. Entonces la dimensión de $\Lambda^{\perp}$ será $k^{\perp} = 4-k$. Para ello tenemos que resolver el sistema lineal $VX = 0$, calculando la *forma normal de Smith* [69] de V y sus *factores invariantes* $\alpha_1, \ldots, \alpha_k$:

$$LVR = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_k \end{pmatrix} = N \quad \text{tal que} \quad \begin{array}{l} L \in GL_k(\mathbb{Z}) \\ R \in GL_4(\mathbb{Z}) \\ 0 < \alpha_1, \cdots, \alpha_k \\ \alpha_1 | \alpha_2, \ldots \alpha_{k-1} | \alpha_k \end{array}$$

Lema 5.3.1. *Dado un número $p \geq 1$ y un sistema $p-$ortonormal $S = \{\, v_1, \ldots, v_k \,\}$, $1 \leq k \leq 3$, con el lattice asociado Λ, entonces las últimas $4-k$ columnas de la matriz R, en la forma normal de Smith de V, constituyen una base de $\Lambda^{\perp}$.*

Demostración. Se cumple que $VX = 0 \Leftrightarrow LVRR^{-1}X = L\,0 = 0$ y, considerando $Y = R^{-1}X$, tenemos que $VX = 0 \Leftrightarrow NY = 0 \Leftrightarrow y_1 = \cdots = y_k = 0$. Por tanto, la base que genera las soluciones de $B^{\perp} = \{\, Re_{k+1}, \ldots, Re_4 \,\}$, es decir, el conjunto con las últimas $4-k$ columnas de R. □

Utilizaremos de nuevo la comprobación de polinomios introducida en la Sección 2 Caso 3, concretamente en las proposiciones 5.3.1 y 5.3.2 y en el lema 5.3.3.

Proposición 5.3.1. *Dado un número primo p y un sistema $p-$ortonormal $S = \{\, v_1, v_2 \,\}$, $v_1 = (x_1, \ldots, x_4)$ y $v_2 = (y_1, \ldots, y_4)$, con $|sop(S)| > 2$, entonces $mcd(x_1, \ldots, x_4) = mcd(y_1, \ldots, y_4) = 1$ y los factores invariantes de V también verifican $\alpha_1 = \alpha_2 = 1$.*

Demostración. Supongamos, por contradicción, que $\text{mcd}(x_1, \ldots, x_4) = g > 1$. Entonces $N(v_1) = g^2(x_1'^2 + \cdots + x_4'^2) = p$, donde $x_i' = \dfrac{x_i}{g}$ para todo $1 \leq i \leq 4$, y este hecho contradice la primalidad de p. Así, tenemos que $\text{mcd}(x_1, \ldots, x_4) = 1$ y de la misma manera concluimos que $\text{mcd}(y_1, \ldots, y_4) = 1$. Aplicando estos resultados, junto con la propiedad del primer factor invariante, obtenemos $\alpha_1 = 1$.

Para obtener el valor de α_2 utilizaremos la siguiente identidad, que se puede demostrar por comprobación de polinomios:

$$N(v_1)N(v_2) - \langle v_1 | v_2 \rangle^2 = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}^2 + \begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}^2 + \cdots + \begin{vmatrix} x_3 & x_4 \\ y_3 & y_4 \end{vmatrix}^2$$

Para obtener el valor de α_2 utilizaremos la siguiente identidad, que se puede demostrar por comprobación de polinomios:

$$m_{ij} = \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} \qquad \text{y} \qquad m_{ij}' = \frac{m_{ij}}{g}$$

Entonces $p^2 = g^2(m'^2_{12}+\cdots+m'^2_{34})$ y hay, al menos, dos menores diferentes de 0 porque $|\text{supp}(S)| > 2$. Estos hechos contradicen la primalidad de p. Entonces, tenemos que $\text{mcd}(m_{12},\ldots,m_{34}) = 1$ y, como este valor coincide con el segundo factor invariante, obtenemos $\alpha_2 = 1$. □

Por último, introducimos el resultado fundamental de la rama de la teoría de los números llamada geometría de números, demostrado por Minkowski en 1889.

Teorema 5.3.1 (Minkowski [67])**.** *Sea K un conjunto convexo en $\mathbb{R}^n$ que es simétrico respecto al origen. Si el volumen de K es mayor que 2^n veces el volumen del dominio fundamental (paralelepípedo) de un lattice Λ, entonces K contiene un punto del lattice no nulo.*

Dos vectores $p-$ortonormales con soporte de tamaño > 2

En primer lugar, vamos a obtener una base de $\Lambda^\perp$, $B^\perp$, mediante el cálculo de una forma cuasi-normal de Smith en la que $L \in GL_k(\mathbb{Q})$. Téngase en cuenta que en este caso el Lemma 5.3.1 también se mantiene. Sea V la matriz de coordenadas del sistema $p-$ortonormal $S = \{ v_1, v_2 \}$ con $|\text{sop}(S)| > 2$, $v_1 = (x_1, x_2, x_3, x_4)$, $v_2 = (y_1, y_2, y_3, y_4)$ y $p \geq 1$. Supongamos, reordenando las coordenadas de v_1 y v_2 si es necesario, que

$$x_1 \neq 0, \quad \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \neq 0 \quad \text{y} \quad 4 \in \text{sop}(S), \text{ i.e. } x_4 \neq 0 \text{ or } y_4 \neq 0$$

La forma cuasi-normal de Smith de S es:

$$LVR = \begin{pmatrix} c & 0 & 0 & 0 \\ 0 & cd & 0 & 0 \end{pmatrix} \quad \text{such that} \quad \begin{array}{l} L \in GL_k(\mathbb{Q}) \\ R \in GL_4(\mathbb{Z}) \\ 0 < c, d \\ R = R_1\, R_2\, R_3\, R_4\, R_5 \end{array}$$

donde las matrices L y R_i, $1 \leq i \leq 5$, y los parámetros c y d son los que aparecen en la Tabla 5.1.

Lema 5.3.2. *Dado un número $p \geq 1$ y un sistema $p-$ortonormal $S = \{ v_1, v_2 \}$ con su lattice asociado Λ, entonces $B^\perp = \{ w_1, w_2 \}$ es una base de $\Lambda^\perp$, donde*

$$\begin{aligned} w_1 &= \left(\frac{x_2\, y'_3}{c_1\, d_1} - \frac{x_3\, y'_2\, \sigma_1}{c_2\, d_1}, -\frac{x_1\, y'_3}{c_1\, d_1} - \frac{x_3\, y'_2\, \tau_1}{c_2\, d_1}, \frac{c_1\, y'_2}{c_2\, d_1}, 0 \right) \\ w_2 &= \left(\frac{y'_4(c_1\, x_3\, \sigma_1\, \tau_4 + c_2\, x_2\, \sigma_4)}{c_1\, c_2\, d} - \frac{d_1\, x_4\, \sigma_1\, \sigma_2}{c\, d}, \right. \\ &\qquad \left. \frac{y'_4(c_1\, x_3\, \tau_1\, \tau_4 - c_2\, x_1\, \sigma_4)}{c_1\, c_2\, d} - \frac{d_1\, x_4\, \sigma_2\, \tau_1}{c\, d}, -\frac{d_1\, x_4\, \tau_2}{c\, d} - \frac{c_1\, y'_4\, \tau_4}{c_2\, d}, \frac{c_2\, d_1}{c\, d} \right) \end{aligned}$$

Demostración. Obtenemos el resultado simplemente multiplicando las matrices R_1, R_2, R_3, R_4 y R_5 y aplicando el Lemma 5.3.1 a la forma cuasi-normal de Smith de S. □

Nota 5.3.1. Sean V y G_V la matriz de coordenadas y la matriz de Gram, respectivamente, del conjunto de vectores $B \cup B^\perp$ y sea G la matriz de Gram del conjunto de vectores $B^\perp$. Entonces, $\det^2(V) = \det(G_V) = p^2 \det(G)$ y, puesto que $\det^2(\Lambda^\perp) = \det(G)$, concluimos que $\det(\Lambda^\perp) = \dfrac{|\det(V)|}{p}$.

$R_1 = \begin{pmatrix} \sigma_1 & \frac{-x_2}{c_1} & 0 & 0 \\ \tau_1 & \frac{x_1}{c_1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$x_1\sigma_1 + x_2\tau_1 = c_1 = \text{ mcd}(x_1, x_2)$ $y_1' = \sigma_1 y_1 + \tau_1 y_2$ $y_2' = \frac{-x_2}{c_1} y_1 + \frac{x_1}{c_1} y_2$
$R_2 = \begin{pmatrix} \sigma_2 & 0 & \frac{-x_3}{c_2} & 0 \\ 0 & 1 & 0 & 0 \\ \tau_2 & 0 & \frac{c_1}{c_2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$c_1\sigma_2 + x_3\tau_2 = c_2 = \text{ mcd}(c_1, x_3)$ $y_1'' = \sigma_2 y_1' + \tau_2 y_3 = \sigma_2\sigma_1 y_1 + \sigma_2\tau_1 y_2 + \tau_2 y_3$ $y_3' = \frac{-x_3}{c_2} y_1' + \frac{c_1}{c_2} y_3 = \frac{-x_3}{c_2}\sigma_1 y_1 + \frac{-x_3}{c_2}\tau_1 y_2 + \frac{c_1}{c_2} y_3$
$R_3 = \begin{pmatrix} \sigma_3 & 0 & 0 & \frac{-x_4}{c} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \tau_3 & 0 & 0 & \frac{c_2}{c} \end{pmatrix}$	$c_2\sigma_3 + x_4\tau_3 = c = \text{ mcd}(c_2, x_4)$ $y_1''' = \sigma_3 y_1'' + \tau_3 y_4 = \sigma_3\sigma_2\sigma_1 y_1 + \sigma_3\sigma_2\tau_1 y_2 + \sigma_3\tau_2 y_3 + \tau_3 y_4$ $y_4' = \frac{-x_4}{c} y_1'' + \frac{c_2}{c} y_4 = \frac{-x_4}{c}\sigma_2\sigma_1 y_1 + \frac{-x_4}{c}\sigma_2\tau_1 y_2 + \frac{-x_4}{c}\tau_2 y_3 + \frac{c_2}{c} y_4$
$L = \begin{pmatrix} 1 & 0 \\ -y_1''' & c \end{pmatrix}$	
$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sigma_4 & \frac{-y_3'}{d_1} & 0 \\ 0 & \tau_4 & \frac{y_2}{d_1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$y_2'\sigma_4 + y_3'\tau_4 = d_1 = \text{ mcd}(y_2', y_3')$
$R_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sigma_5 & 0 & \frac{-y_4'}{d} \\ 0 & 0 & 1 & 0 \\ 0 & \tau_5 & 0 & \frac{d_1}{d} \end{pmatrix}$	$d_1\sigma_5 + y_4'\tau_5 = d = \text{ mcd}(d_1, y_4')$

Tabla 5.1: Datos de forma cuasi-normal de Smith.

Podemos utilizar la Nota 5.3.1 para calcular $\det(\Lambda^\perp)$ e, indirectamente, para estudiar la matriz G, considerada como una forma cuadrática simétrica definida positiva.

Proposición 5.3.2. *Dado un número $p \geq 1$ y un sistema $p-$ortonormal $S = \{ v_1, v_2 \}$, con el lattice asociado Λ, entonces $det(\Lambda^\perp) = \frac{p}{c\,d}$, donde c y d son los parámetros que aparecen en la Tabla 5.1.*

Demostración. Para obtener el resultado sólo tenemos que calcular det(V), por la Nota 5.3.1. Desarrollando la expresión del determinante de V, donde w_1 y w_2 son los vectores obtenidos en el Lema 5.3.2, obtenemos:

$$\begin{aligned}
\det(V)c_1c_2d_1cd = cy_4'(\ & c_1(x_1^2y_4 - x_1x_4y_1 + x_2(x_2y_4 - x_4y_2)) \\
& +x_3(\underline{x_1\sigma_1 + x_2\tau_1})(x_3y_4 - x_4y_3))(\underline{y_2'\sigma_4 + y_3'\tau_4}) \\
d_1(\ & +c_1^2y_2'(c_2(x_1y_2 - x_2y_1) + x_1x_4y_4\sigma_2\tau_1 - \\
& -x_4\sigma_2(x_2y_4\sigma_1 + x_4(y_1\tau_1 - y_2\sigma_1))) \\
& +c_1x_3y_2'(c_2(x_1y_3\tau_1 - x_2y_3\sigma_1 + x_3(y_2\sigma_1 - y_1\tau_1)) \\
& +x_4\tau_2(x_1y_4\tau_1 - x_2y_4\sigma_1 + x_4(y_2\sigma_1 - y_1\tau_1))) \\
& +c_2y_3'(c_2(x_1^2y_3 - x_1x_3y_1 + x_2(x_2y_3 - x_3y_2)) \\
& +x_4(x_1^2y_4\tau_2 - x_1(x_3y_4\sigma_1\sigma_2 + x_4(y_1\tau_2 - y_3\sigma_1\sigma_2)) \\
& +x_2(x_2y_4\tau_2 - x_3y_4\sigma_2\tau_1 + x_4(y_3\sigma_2\tau_1 - y_2\tau_2)))))
\end{aligned}$$

donde todos los parámetros aparecen en la Tabla 5.1.

A lo largo de la prueba sustituiremos las expresiones aplicando las igualdades de la Tabla 5.1.

1		$c_1c_2x_1^2y_2^2$	2		$c_1c_2x_1^2y_3^2$
3		$c_1c_2x_1^2y_4^2$	4		$-2c_1c_2x_1x_2y_1y_2$
5	×	$-c_1c_2x_1x_3y_1y_3$	6	×	$-c_1c_2x_1x_4y_1y_4$
7		$c_1c_2x_2^2y_1^2$	8		$c_1c_2x_2^2y_3^2$
9		$c_1c_2x_2^2y_4^2$	10	×	$-c_1c_2x_2x_3y_2y_3$
11	×	$-c_1c_2x_2x_4y_2y_4$	12		$c_1c_2x_3^2y_4^2$
13	×	$-c_1c_2x_3x_4y_3y_4$	14	×	$-c_1x_1^2x_4y_1y_4\sigma_1\sigma_2$
15	×	$-c_1x_1x_2x_4y_1y_4\sigma_2\tau_1$	16	×	$-c_1x_1x_2x_4y_2y_4\sigma_1\sigma_2$
17	×	$-c_1x_1x_3x_4y_3y_4\sigma_1\sigma_2$	18	×	$c_1x_1x_4^2y_1^2\sigma_1\sigma_2$
19	×	$c_1x_1x_4^2y_2^2\sigma_1\sigma_2$	20	×	$c_1x_1x_4^2y_3^2\sigma_1\sigma_2$
21	×	$-c_1x_2^2x_4y_2y_4\sigma_2\tau_1$	22	×	$-c_1x_2x_3x_4y_3y_4\sigma_2\tau_1$
23	×	$c_1x_2x_4^2y_1^2\sigma_2\tau_1$	24	×	$c_1x_2x_4^2y_2^2\sigma_2\tau_1$
25	×	$c_1x_2x_4^2y_3^2\sigma_2\tau_1$	26	×	$-c_1x_3^2x_4y_1y_4\sigma_1\sigma_2$
27	×	$-c_1x_3^2x_4y_2y_4\sigma_2\tau_1$	28	×	$-c_1x_3^2x_4y_3y_4\tau_2$
29	×	$c_1x_3x_4^2y_1y_3\sigma_1\sigma_2$	30	×	$c_1x_3x_4^2y_2y_3\sigma_2\tau_1$
31	×	$c_1x_3x_4^2y_3^2\tau_2$	32	×	$-c_2x_1^2x_3y_1y_3\sigma_1$
33	×	$-c_2x_1x_2x_3y_1y_3\tau_1$	34	×	$-c_2x_1x_2x_3y_2y_3\sigma_1$
35	×	$c_2x_1x_3^2y_1^2\sigma_1$	36	×	$c_2x_1x_3^2y_2^2\sigma_1$
37	×	$-c_2x_2^2x_3y_2y_3\tau_1$	38	×	$c_2x_2x_3^2y_1^2\tau_1$
39	×	$c_2x_2x_3^2y_2^2\tau_1$	40	×	$-x_1^2x_3x_4y_1y_4\sigma_1\tau_2$
41	×	$-x_1x_2x_3x_4y_1y_4\tau_1\tau_2$	42	×	$-x_1x_2x_3x_4y_2y_4\sigma_1\tau_2$
43	×	$x_1x_3^2x_4y_1y_4\sigma_1^2\sigma_2$	44	×	$x_1x_3^2x_4y_2y_4\sigma_1\sigma_2\tau_1$
45	×	$x_1x_3x_4^2y_1^2\sigma_1\tau_2$	46	×	$-x_1x_3x_4^2y_1y_3\sigma_1^2\sigma_2$
47	×	$x_1x_3x_4^2y_2^2\sigma_1\tau_2$	48	×	$-x_1x_3x_4^2y_2y_3\sigma_1\sigma_2\tau_1$
49	×	$-x_2^2x_3x_4y_2y_4\tau_1\tau_2$	50	×	$x_2x_3^2x_4y_1y_4\sigma_1\sigma_2\tau_1$
51	×	$x_2x_3^2x_4y_2y_4\sigma_2\tau_1^2$	52	×	$x_2x_3x_4^2y_1^2\tau_1\tau_2$
53	×	$-x_2x_3x_4^2y_1y_3\sigma_1\sigma_2\tau_1$	54	×	$x_2x_3x_4^2y_2^2\tau_1\tau_2$
55	×	$-x_2x_3x_4^2y_2y_3\sigma_2\tau_1^2$			

Tabla 5.2: Monomios de $\det(V)c_1c_2cd$.

Sustituyendo las expresiones subrayadas por c_1 y d_1 respectivamente, se cancelan todas las apariciones de d_1. Del mismo modo, sustituyendo c_1y_2', c_2y_3' y cy_4' por las expresiones

$$x_1y_2 - x_2y_1,$$
$$c_1y_3 - x_3(\sigma_1y_1 + \tau_1y_2) \text{ y}$$
$$c_2y_4 - x_4(\sigma_2\sigma_1y_1 + \sigma_2\tau_1y_2 + \tau_2y_3)$$

respectivamente, el parámetro c desaparece del segundo miembro de la igualdad.

La expresión $\det(V)c_1c_2cd$ es un polinomio homogéneo de grado total 6 en las variables c_1, c_2, x_1, x_2 x_3, x_4, y_1, y_2, y_3 y y_4, en los que sólo aparecen los parámetros σ_1, τ_1, σ_2 y τ_2. Los monomios de dicho polinomio se incluyen en la Tabla 5.2 y se identifican mediante índices colocados en las primeras celdas de las filas correspondientes.

Para eliminar los parámetros σ_1, τ_1, σ_2 y τ_2, agrupamos los monomios de la Tabla 5.2 por parejas para aplicar las siguientes operaciones:

(1) Sustituir $x_1\sigma_1 + x_2\tau_1$ por c_1.
(2) Sustituir $c_1\sigma_2 + x_3\tau_2$ por c_2.
(3) Anular monomios opuestos.
(4) Sumar monomios iguales.

Las operaciones aplicadas se detallan en la Tabla 5.3, donde los monomios resultantes se identifican por los índices de los primeros monomios sobre los que se opera. Cada vez que se aplica una operación,

14	×	15	$-c_1^2x_1x_4y_1y_4\sigma_2$	16	×	21	$-c_1^2x_2x_4y_2y_4\sigma_2$
17	×	22	$-c_1^2x_3x_4y_3y_4\sigma_2$	18	×	23	$c_1^2x_4^2y_1^2\sigma_2$
19	×	24	$c_1^2x_4^2y_2^2\sigma_2$	20	×	25	$c_1^2x_4^2y_3^2\sigma_2$
32	×	33	$-c_1c_2x_1x_3y_1y_3$	34	×	37	$-c_1c_2x_2x_3y_2y_3$
35		38	$c_1c_2x_3^2y_1^2$	36		39	$c_1c_2x_3^2y_2^2$
40	×	41	$-c_1x_1x_3x_4y_1y_4\tau_2$	42	×	49	$-c_1x_2x_3x_4y_2y_4\tau_2$
43	×	50	$c_1x_3^2x_4y_1y_4\sigma_1\sigma_2$	44	×	51	$c_1x_3^2x_4y_2y_4\sigma_2\tau_1$
45	×	52	$c_1x_3x_4^2y_1^2\tau_2$	46	×	53	$-c_1x_3x_4^2y_1y_3\sigma_1\sigma_2$
47	×	54	$c_1x_3x_4^2y_2^2\tau_2$	48	×	55	$-c_1x_3x_4^2y_2y_3\sigma_2\tau_1$
14	×	40	$-c_1c_2x_1x_4y_1y_4$	16	×	42	$-c_1c_2x_2x_4y_2y_4$
17	×	28	$-c_1c_2x_3x_4y_3y_4$	18		45	$c_1c_2x_4^2y_1^2$
19		47	$c_1c_2x_4^2y_2^2$	20		31	$c_1c_2x_4^2y_3^2$
26	×	43	0	27	×	44	0
29	×	46	0	30	×	48	0
5		32	$-2c_1c_2x_1x_3y_1y_3$	6		14	$-2c_1c_2x_1x_4y_1y_4$
10		34	$-2c_1c_2x_2x_3y_2y_3$	11		16	$-2c_1c_2x_2x_4y_2y_4$
13		17	$-2c_1c_2x_3x_4y_3y_4$				

Tabla 5.3: Monomios resultantes de las operaciones.

los monomios implicados se marcan con una × a la derecha del índice que identifica al monomio, para no volver a utilizarlos. Las operaciones se realizan de forma iterativa sobre los monomios de las Tablas 5.2 y 5.3 que no estén marcados, hasta que no se pueda aplicar ninguna operación más.

Todos los monomios resultantes tienen el factor c_1c_2. Por tanto, simplificando este factor se obtiene la siguiente igualdad:

$$\begin{aligned}\det(V)cd &= x_1^2y_2^2 + x_1^2y_3^2 + x_1^2y_4^2 - 2x_1x_2y_1y_2 - 2x_1x_3y_1y_3 - 2x_1x_4y_1y_4 \\ &\quad x_2^2y_1^2 + x_2^2y_3^2 + x_2^2y_4^2 - 2x_2x_3y_2y_3 - 2x_2x_4y_2y_4 + x_3^2y_4^2 \\ &\quad -2x_3x_4y_3y_4 + x_4^2y_1^2 + x_4^2y_2^2 + x_4^2y_3^2 + x_3^2y_1^2 + x_3^2y_2^2\end{aligned}$$

Por comprobación polinómica, es fácil verificar la siguiente igualdad:

$$\det(V)cd = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) - (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2$$

Por hipótesis, el segundo miembro de la igualdad anterior es igual a p^2. Por tanto, aplicando la Nota 5.3.1, concluimos que:

$$\det(\Lambda^\perp) = \frac{p}{cd}$$

□

Lema 5.3.3. *Dado un número $p \geq 1$, un sistema $p-$ortonormal $S = \{v_1, v_2\}$ y w_1 el primer vector de la base $B^\perp$ de el lattice ortogonal $\Lambda^\perp$, tenemos que $N(w_1) = \dfrac{p(p - x_4^2 - y_4^2)}{c_2^2\, d_1^2}$, donde c_2 y d_1 son los parámetros de la tabla 5.1.*

Demostración. La prueba es similar a la de la Proposición 5.3.2. Considerando el vector w_1 obtenido en el Lemma 5.3.2 y calculando $N(w_1)$, se obtiene la siguiente igualdad:

$$N(w_1)c_1^2c_2^2d_1^2 = c_1^4y_2'^2 + c_1^2x_3^2y_2'^2(\sigma_1^2 + \tau_1^2) + 2c_1c_2x_3y_2'y_3'(x_1\tau_1 - x_2\sigma_1) + c_2^2y_3'^2(x_1^2 + x_2^2)$$

1	$c_1^2x_1^2y_2^2$	
2	$c_1^2x_1^2y_3^2$	
3	$-2c_1^2x_1x_2y_1y_2$	
4	$c_1^2x_2^2y_1^2$	
5	$c_1^2x_2^2y_3^2$	
10	$x_1^2x_3^2y_1^2\sigma_1^2$	$c_1^2x_3^2y_1^2$
12	$2x_1x_2x_3^2y_1^2\sigma_1\tau_1$	
14	$x_2^2x_3^2y_1^2\tau_1^2$	

6	$-2c_1x_1^2x_3y_1y_3\sigma_1$	
7	$-2c_1x_1x_2x_3y_1y_3\tau_1$	$-2c_1^2x_1x_3y_1y_3$
8	$-2c_1x_1x_2x_3y_2y_3\sigma_1$	
9	$-2c_1x_2^2x_3y_2y_3\tau_1$	$-2c_1^2x_2x_3y_2y_3$
11	$x_1^2x_3^2y_2^2\sigma_1^2$	
13	$2x_1x_2x_3^2y_2^2\sigma_1\tau_1$	$c_1^2x_3^2y_2^2$
15	$x_2^2x_3^2y_2^2\tau_1^2$	

Tabla 5.4: Monomios de $N(w_1)c_1^2c_2^2d_1^2$ y resultantes de las operaciones.

Sustituyendo en el segundo miembro de la igualdad c_1y_2' por $-x_2y_1+x_1y_2$ y c_2y_3' por $-x_3\sigma_1y_1-x_3\tau_1y_2+c_1y_3$, se obtiene un polinomio homogéneo de grado total 6 en las variables c_1, x_1, x_2, x_3, y_1, y_2 y y_3, en los que sólo aparecen los parámetros σ_1 y τ_1.

Los monomios del mencionado polinomio se recogen en la Tabla 5.4. También se incluyen en la tabla los resultados de la siguiente sustitución: $x_1\sigma_1+x_2\tau_1$ by c_1.

Todos los monomios restantes se multiplican por el factor c_1^2. Por lo tanto, simplificando este factor, obtenemos:

$$\begin{aligned} N(w_1)c_2^2d_1^2 &= x_1^2y_2^2+x_1^2y_3^2-2x_1x_2y_1y_2+x_2^2y_1^2+x_2^2y_3^2 \\ &\quad -2x_1x_3y_1y_3-2x_2x_3y_2y_3+x_3^2y_1^2+x_3^2y_2^2 \end{aligned}$$

Por comprobación polinómica, es fácil verificar la siguiente igualdad:

$$\begin{aligned} N(w_1)c_2^2d_1^2 &= (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) \\ &\quad -(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2-x_4^2(y_1^2+y_2^2+y_3^2+y_4^2) \\ &\quad -y_4^2(x_1^2+x_2^2+x_3^2+x_4^2)+2x_4y_4(x_1y_1+x_2y_2+x_3y_3+x_4y_4) \end{aligned}$$

Por hipótesis, el segundo miembro de la igualdad anterior es igual a $p^2-px_4^2-py_4^2$. Por lo tanto, concluimos que:

$$N(w_1)=\frac{p(p-x_4^2-y_4^2)}{c_2^2d_1^2}$$

□

Lema 5.3.4. *Dado un número primo p y un sistema $p-$ortonormal $S=\{v_1,v_2\}$ con $|sop(S)|>2$, asociado al lattice Λ, entonces $c=d=1$, donde c y d son los parámetros que aparecen en la Tabla 5.1.*

Demostración. Según la Tabla 5.1 se cumple que $c=\ \mathrm{mcd}(x_1,x_2,x_3,x_4)$ y, por la Proposición 5.3.1, concluimos que $c=1$. Este resultado implica que la forma cuasi-normal de Smith descrita en la Tabla 5.1 es en realidad una forma normal, porque en este caso $L\in GL_k(\mathbb{Z})$, y en consecuencia d es el segundo factor invariante de V. Considerando una vez más la Proposición 5.3.1 concluimos que $d=1$. □

Proposición 5.3.3. *Dado un número primo p, un sistema p−ortonormal* $S = \{ v_1, v_2 \}$ *con* $|sop(S)| > 2$ *y la matriz de Gram G de la base* $B^\perp = \{ w_1, w_2 \}$ *del lattice ortogonal* $\Lambda^\perp$*, entonces se cumple que* $p|G$.

Demostración. Supongamos que la matriz de Gram $G = \begin{pmatrix} \mu & \lambda \\ \lambda & \nu \end{pmatrix}$.

Consideremos el valor de $\mu = N(w_1)$ obtenido en el Lemma 5.3.3. La factorización prima de $p(p - x_4^2 - y_4^2)$ contiene sólo un factor p, porque p es primo y $-p < p - x_4^2 - y_4^2 < p$ (recordemos que estamos suponiendo que $x_4 \neq 0$ o $y_4 \neq 0$). Entonces, la factorización en primos de $c_2^2\, d_1^2$ no contiene p, porque el número de veces que contiene cada factor primo es par. En consecuencia, $c_2^2\, d_1^2 \,|(p - x_4^2 - y_4^2)$ y esto implica que $p\,|\mu$, es decir, $\mu = p\,\mu'$. Además, $|\mu'| < p$.

Aplicando la Proposición 5.3.2, el Lema 5.3.4 y la propiedad $\det^2(\Lambda^\perp) = \det(G)$, obtenemos $p^2 = p\,\mu'\,\nu - \lambda^2$. Esto implica que $p\,|\,\lambda^2$ y, teniendo en cuenta que p es un primo, tenemos que $p\,|\,\lambda$, es decir $\lambda = p\,\lambda'$.

Reconsiderando la igualdad anterior, y anulando un factor p, obtenemos $p = \mu'\,\nu - p\,\lambda'^2$. Esto implica de nuevo que $p\,|\mu'\,\nu$ y, considerando que p es primo y $|\mu'| < p$, obtenemos $p\,|\,\nu$, es decir, $\nu = p\,\nu'$.

Llegamos a la conclusión final de que $G = p \begin{pmatrix} \mu' & \lambda' \\ \lambda' & \nu' \end{pmatrix}$, es decir, $p\,|\,G$. □

Teorema 5.3.2. *Dado un número primo p, un sistema p−ortonormal* $S = \{ v_1, v_2 \}$ *con* $|sop(S)| > 2$ *y los lattices asociados* Λ *y* $\Lambda^\perp$*, existe* $v \in \Lambda^\perp$ *tal que verifica* $N(v) = p$.

Demostración. Sea G la matriz de Gram de la base $B^\perp$ del lattice asociado $\Lambda^\perp$.

La Proposición 5.3.2, el Lema 5.3.4 y la propiedad $\det^2(\Lambda^\perp) = \det(G)$ nos permiten concluir que $\det(G) = p^2$. Aplicando ahora la Proposición 5.3.3 obtenemos que $G' = \dfrac{G}{p}$ es una matriz unimodular, es decir $G' \in GL_2(\mathbb{Z})$, y que, dado un vector $v \in \Lambda^\perp$, $N(v) = b^t\, G\, b = p$ si y sólo si $b^t\, G'\, b = 1$, siendo b el vector de coordenadas de v en la base $B^\perp$.

Sea $K = \{ x \in \mathbb{R}^2 \mid x^t\, G'\, x \leq 1 \}$ y $\{u_1, u_2\}$ una base ortonormal de vectores propios de G' con valores propios λ_1 y λ_2 respectivamente. Nótese que λ_1 y λ_2 son reales, ya que G' es simétrica, positivos, porque G' es definida positiva, y verifican $\lambda_1\,\lambda_2 = \det(G') = 1$. Entonces K es la elipse $\lambda_1 x^2 + \lambda_2 y^2 \leq 1$, con respecto al sistema de referencia determinado por u_1 y u_2, y tiene volumen $\pi \frac{1}{\sqrt{\lambda_1}} \frac{1}{\sqrt{\lambda_2}} = \pi$.

Dado un $0 < \epsilon < 1$, sea E_ϵ la elipse K escalada por un factor $f_\epsilon = \frac{2}{\sqrt{\pi}} + \epsilon$. La elipse E_ϵ tiene un volumen $\pi f_\epsilon^2 > \pi \frac{2^2}{\pi} = 2^2$. Entonces, por el Teorema 5.3.1, existe un punto b en el lattice $\mathbb{Z}^2$ (con volumen del dominio fundamental 1) tal que $b \neq 0$ y $b \in E_\epsilon$. Como el conjunto de puntos de $\mathbb{Z}^2$ que pertenecen a alguna de las elipses E_ϵ es finito, se demuestra que existe un punto b en el lattice $\mathbb{Z}^2$ tal que $b \neq 0$ y $b \in K$.

El punto b define un vector $v \in \Lambda^\perp$ que verifica $0 < b^t\, G'\, b \leq 1$. Entonces, se cumple que $b^t\, G'\, b = 1$, ya que $b^t\, G'\, b$ es entero, y, por fin, es el vector deseado de $\Lambda^\perp$, porque $N(v) = b^t\, G\, b = p$. □

El siguiente teorema es una consecuencia de los cuatro casos considerados anteriormente.

Teorema 5.3.3. *Dado un número primo p y un sistema $p-$ortonormal en Z^4, S, entonces S se puede extender a una base $p-$ortonormal.*

5.4. Generalizaciones

Hemos demostrado que todo sistema de vectores $p-$ortonormal en Z^4 puede extenderse a una base $p-$ortonormal si p es un número primo. Además, hemos verificado el resultado para cada $1 \leq p \leq 10000$. En esta sección, todas las verificaciones para valores dados de p y n se han realizado mediante la comprobación exhaustiva de todos los sistemas $p-$ortonormales en $\mathbb{Z}^n$, utilizando un programa C específico en un ordenador personal. A partir de los resultados anteriores, conjeturamos que se cumple el siguiente resultado.

Conjetura 5.4.1. Dado un número entero $p \geq 1$ y un sistema $p-$ortonormal en $\mathbb{Z}^4$, S, entonces S se puede extender a una base $p-$ortonormal.

La generalización más natural del problema es considerarlo en cualquier dimensión $n \geq 1$, es decir, estudiar el problema en $\mathbb{Z}^n$.

Problema 5.4.1. Dado un número entero $p \geq 1$ y un sistema $p-$ortonormal en $\mathbb{Z}^n$, S, ¿se puede extender S a una base $p-$ortonormal?

Una construcción análoga a la dada en la Sección 5.3, Caso 1 muestra el resultado para $n = 2$. Obsérvese que si p no puede escribirse como una suma de dos cuadrados [70] (la descomposición en primos de p contiene un primo $n = 3 \bmod 4$ elevado a una potencia impar), no hay sistemas $p-$ortonormales en $\mathbb{Z}^2$. El caso de dimensión 4 ya ha sido estudiado y, en el caso $n = 8$, hemos comprobado el resultado para $1 \leq p \leq 36$.

Para analizar el problema en otras dimensiones tratamos de encontrar contraejemplos que nos ayuden a entender en qué casos el problema tiene una respuesta positiva. Si p no es un cuadrado y existe una base $p-$ortonormal en $\mathbb{Z}^n$ entonces hay contraejemplos para p en dimensión $n+1$. En efecto, sea $\{v_1 \ldots, v_n\}$ una base $p-$ortonormal en dimensión n. Entonces $\{w_1 \ldots, w_n\}$ es un sistema $p-$ortonormal en dimensión $n+1$ que no se puede extender a una base $p-$ortonormal, siendo:

$$w_j = (v_{j,1}, \ldots, v_{j,n}, 0) \quad \text{donde} \quad v_j = (v_{j,1}, \ldots, v_{j,n}) \qquad 1 \leq j \leq n$$

Esta construcción nos permite encontrar contraejemplos para cualquier dimensión $n \not\equiv 0 \bmod 4$, $n \neq 1$ y $n \neq 2$. Dado un número entero $p \geq 1$, consideramos la base $p-$ortonormal $S_1 = \{v_1, v_2, v_3, v_4\}$ en $\mathbb{Z}^4$ y la matriz A,

$$\begin{array}{l} v_1 = (x_1, x_2, x_3, x_4) \\ v_2 = (-x_2, x_1, -x_4, x_3) \\ v_3 = (-x_3, x_4, x_1, -x_2) \\ v_4 = (x_4, x_3, -x_2, -x_1) \end{array} \quad \text{y} \quad A = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ -x_3 & x_4 & x_1 & -x_2 \\ x_4 & x_3 & -x_2 & -x_1 \end{pmatrix},$$

donde $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Si p se puede escribir como una suma de dos cuadrados, $p = y_1^2 + y_2^2$, definimos la base $p-$ortonormal $S_2 = \{u_1, u_2\}$ en $\mathbb{Z}^2$ y la matriz B,

$$\begin{array}{l} u_1 = (y_1, y_2) \\ v_2 = (-y_2, y_1) \end{array} \qquad \text{y} \qquad B = \begin{pmatrix} y_1 & y_2 \\ -y_2 & y_1 \end{pmatrix}.$$

Entonces, las filas de las siguientes matrices C_1, C_2 y C_3 definen sistemas $p-$ortonormales no extensibles para dimensiones n tales que $n \bmod 4$ es 1, 2 o 3 respectivamente:

(i) C_1 si p no es un cuadrado, $n \equiv 1 \bmod 4$ y $n \neq 1$.

(ii) C_2 si p no puede escribirse como una suma de dos cuadrados, $n \equiv 2 \bmod 4$ y $n \neq 2$.

(iii) C_3 si p no es un cuadrado y puede escribirse como una suma de dos cuadrados y $n \equiv 3 \bmod 4$.

$$C_1 = \begin{pmatrix} A & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & A & 0 \end{pmatrix} \quad C_2 = \begin{pmatrix} A & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & A & 0 & 0 \end{pmatrix} \quad C_3 = \begin{pmatrix} A & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & A & 0 & 0 \\ 0 & \cdots & 0 & B & 0 \end{pmatrix}$$

Las comprobaciones experimentales y los contraejemplos anteriores nos hacen pensar que la generalización de la Conjetura 5.4.1 debería ser la siguiente.

Conjetura 5.4.2. Dados $n \equiv 0 \bmod 4$ $(n \geq 1)$ y $p \geq 1$ y un sistema $p-$ortonormal en $\mathbb{Z}^n$, S, entonces S puede extenderse a una base $p-$ortonormal.

Pero, ¿qué ocurre si p es un cuadrado? Hemos comprobado el resultado para $n = 3, 5$ y $1^2 \leq p \leq 100^2$, $n = 6$ y $1^2 \leq p \leq 33^2$, $n = 7$ y $1^2 \leq p \leq 13^2$ y $n = 9$ y $1^2 \leq p \leq 2^2$. Sin embargo, hemos encontrado que el problema 5.4.1 tiene una respuesta negativa si $n = 9, p = 9$ y $S = \{(1, \ldots, 1)\}$. Este contraejemplo puede generalizarse como sigue: si $n = \bar{n}^2$ y $p = n\bar{p}^2$ son enteros impares, entonces el conjunto $S = \{v_1 = (\bar{p}, \ldots, \bar{p})\}$ no puede extenderse a una base $p-$ortonormal en $\mathbb{Z}^n$. En efecto, S no puede extenderse con un vector v porque, por un lado, el número de componentes impares de v debe ser impar porque $\|v\|^2 = p$ es impar y, por otro lado, el número de componentes impares de v debe ser par porque $\langle v_1|v\rangle = 0$ es par. Por lo tanto, si p es un cuadrado, nuestra conjetura es la siguiente.

Conjetura 5.4.3. Dados los números $n \geq 1$ y $p \geq 1$, de modo que o bien n es par o p es par o $n \nmid p$, y un sistema p^2-ortonormal en $\mathbb{Z}^n$, S, entonces S puede extenderse a una base p^2-ortonormal.

5.4.1. Propiedades estructurales del problema

Dado el número entero k y los vectores $u = (x_1, \ldots, x_n)$ y $v = (y_1, \ldots, y_n)$ pertenecientes a $\mathbb{Z}^n$, denotamos la *paridad de* k por $P(k) \equiv k \bmod 2$, la *paridad de* u por $P(u) \equiv (x_1 + \ldots + x_n) \bmod 2$ y la *paridad de* u *y* v por $P(u, v) \equiv \langle u|v\rangle \bmod 2$. Nótese que $P(u) = P(\|u\|^2)$.

Estas definiciones nos permiten considerar las condiciones de $p-$ortonormalidad en términos de paridades (módulo 2), demostrando el siguiente resultado.

Proposición 5.4.1. *Dado un sistema* $p-$*ortonormal en* $\mathbb{Z}^n$, $S = \{v_1, \ldots, v_k\}$, *entonces se cumple que* $P(p) = P(v_i)$, $1 \leq i \leq k$, *y* $P(v_i, v_j) = 0$, $1 \leq i < j \leq k$.

5.4.2. Extensiones ortogonales

Dado un conjunto de vectores pertenecientes a $\mathbb{Z}^n$, $S = \{v_1, \ldots, v_k\}$, tal que $\langle v_i|v_j\rangle = 0$ para todo $1 \leq i < j \leq k$, diremos que S es un *sistema ortogonal* y, si $k = n$, que S es un *base ortogonal*.

La relajación de la condición de $p-$ortonormalidad a ortogonalidad permite extender cualquier sistema ortogonal. En efecto, el Lemma 5.3.1 (Sección B) no depende de la normalización de los vectores y puede aplicarse en $\mathbb{Z}^n$, demostrando la siguiente proposición.

Proposición 5.4.2. *Dado un sistema ortogonal en $\mathbb{Z}^n$, S, entonces S se puede extender a una base ortogonal.*

Dado un conjunto ortogonal en $\mathbb{Z}^n$, $S = \{v_1, \ldots, v_k\}$ $(1 \leq k \leq n)$, denotamos la *norma de* S por $N(S) = \max\{\|v_i\|^2 \mid 1 \leq i \leq k\}$. Entonces, un problema interesante, en vista de la Proposición 5.4.2, es el siguiente:

Problema 5.4.2. Dado un sistema ortogonal en $\mathbb{Z}^n$, S, determinar la base ortogonal con la menor norma que extiende S.

5.4.3. Conjetura sobre estados discretos

Por último, también creemos que la respuesta al Problema 5.1.1 es positiva. Este hecho se recoge en la siguiente conjetura.

Conjetura 5.4.4. Dado un número natural k y $\Psi_1, \ldots, \Psi_j$ $n-$qubits discretos con nivel generalizado k, $1 \leq j < 2^n$, tal que $\langle \Psi_i | \Psi_m \rangle = 0$ para todo $1 \leq i < m \leq j$, entonces existe un $n-$qubit discreto con nivel generalizado k, Ψ, tal que $\langle \Psi_i | \Psi \rangle = 0$ para todo $1 \leq i \leq j$.

Parte III

Aplicabilidad del modelo

En el capítulo 4 se presentó el modelo central de esta tesis. La principal característica que motivó la construcción de este modelo fue su simplicidad, con sólo dos puertas, H y G (ver 4.2), se logró un modelo que mantiene las principales fortalezas de la mecánica cuántica aplicada a la computación cuántica, la superposición y el entrelazamiento. Además, los estados alcanzables por este modelo tienen la característica de tener coeficientes reales excepto un factor de normalización $\sqrt{2}^p$.

Como se ha demostrado, el modelo es interesante en sí mismo y permite explorar múltiples facetas de los estados cuánticos discretos enteros y sus propiedades matemáticas. En esta parte queremos presentar la relación de este modelo con los principales hitos y resultados de la computación cuántica.

En primer lugar, se profundizará en cómo el modelo incorpora el entrelazamiento. Para ello, se mostrará que algunos de los estados de máximo entrelazamiento conocidos forman parte de los llamados estados discretos. A continuación, se verá cómo algunas de las aplicaciones más destacadas de estos estados pueden ser modeladas únicamente con estados discretos. Entre los algoritmos computacionales cuánticos más destacados veremos que algunos pueden describirse completamente dentro del modelo sin necesidad de aproximaciones mientras que otros no. Entre los algoritmos cuánticos más sencillos se encuentra el algoritmo Deutch Jozasa, que permitió vislumbrar la potencia de la computación cuántica en comparación con la clásica en los primeros días del campo. Veremos que este algoritmo puede modelarse completamente con las puertas que componen al modelo.

Sorprendentemente, un algoritmo mucho más potente, como es el algoritmo de búsqueda de Grover, también puede modelarse sólo con las puertas del modelo. Es más, la reinterpretación de la evolución de este algoritmo en términos de estados discretos nos dará una nueva interpretación de este y nos permitirá entender aún mejor los mecanismos por los que la computación cuántica ofrece su ventaja sobre la clásica.

Al ser un modelo discreto, esperábamos que no todos los algoritmos pudieran expresarse sólo con puertas H y G. Como se verá, este es el caso del algoritmo de la transformada cuántica de Fourier (QFT), que en un espacio de más de 3 qubits no puede implementarse directamente con puertas del sistema. Por lo tanto, tampoco será posible la implementación de algoritmos tan importantes como la estimación de fase (QPE) y el algoritmo de Shor. Para implementarlos, habrá que hacer aproximaciones a las puertas componentes de estos algoritmos.

Por último, veremos que la gran mayoría de los códigos de corrección de error cuánticos pueden implementarse utilizando únicamente compuertas del modelo. Esto significa que, con este modelo, cuando se disponga de ordenadores cuánticos con un número suficiente de qubits, se podrá implemen -tar la computación cuántica tolerante a fallos.

Capítulo 6

Entrelazamiento

En la sección 2.1.5 se introdujo la noción de entrelazamiento. En sistemas compuestos existen estados que no pueden ser expresados como el producto de estados de los sistemas componentes. Una de las consecuencias más contra intuitivas de estos estados es que los resultados de las medidas de estados entrelazadas están correlacionadas, al medir uno de los estados componentes se afecta de manera irremediable a los demás sistemas. Aún en el caso de que estos se encuentren a distancia virtualmente infinita uno de otro. Einstein, descreído de la teoría cuántica y la existencia del entrelazamiento bautizó al efecto como "spooky action at a distance".

La misma existencia de estados entrelazados fue uno de los puntos de mayor controversia en los inicios de la física cuántica. En el famoso trabajo de 1935 conocido como EPR [71] Albert Einstein, Boris Podolsky y Natahan Rosen propusieron un experimento mental con el fin de probar que la mecánica cuántica era una teoría incompleta de la naturaleza. Para ellos toda teoría física sobre la realidad debía respetar ciertos elementos de la realidad (Realismo-Local):

- Realismo: Las propiedades físicas deben de existir independientemente de las observación de las mismas.
- Localidad: La perturbación de un sistema suficientemente alejado de otro no debería influir en el segundo.

La correlación de las medidas de estados entrelazados no era compatible con ambas nociones a la vez. La interpretación de los autores era que este comportamiento se debía al desconocimiento de alguna "variable oculta" asociada al modelo de Mecánica Cuántica propuesto principalmente por Niels Bohr.

El experimento mental propuesto por EPR fue reformulado múltiples veces como se recoge en [72]. Quizás la reformulación más famosa se deba a David Bohm que redujo el experimento a partículas de espín 1/2. Está formulación permitió que en 1964 John s. Bell formalizara el experimento mostrando que existe una desigualdad estricta entre las predicciones de las correlaciones que se obtienen al medir partículas entrelazadas de espín 1/2 al utilizar los postulados de la mecánica cuántica versus una teoría de variables ocultas. El experimento fue reformulado en 1969 por J. Clauser, M. Horner, A. Shimony y R. Holt [73], dando lugar a la desigualdad CHSC, que fue experimentalmente comprobada por primera vez en 1972 [74] y repetido en numerosos experimentos [75, 76, 77] zanjando finalmente la discusión a favor de la mecánica cuántica y en detrimento del realismo-local. Por estos trabajos J. Clauser, A. Aspect, y A. Zelinger ganaron el premio Nobel de Física 2023.

6.1. Importancia del entrelazamiento

Como lo atestigua la importancia de la paradoja EPR, el entrelazamiento es un recurso fundamen -tal para la mecánica cuántica y sus aplicaciones a computación y teoría de la información cuántica. Por más contra-intuitivo que este fenómeno parezca es esencial para explicar hitos de la comunicación cuántica, como puede ser la teleportación cuántica, los códigos superdensos o cualquiera de los juegos que implica telepatía cuántica como son los cuadrados de Mermin-Peres [78].

En la computación cuántica, desde los mismos inicios de la misma, se asume qu detrás de la mayor potencia de las computadoras cuánticas para realizar ciertas tareas respecto a las clásicas se encuentra justamente el entrelazamiento. Así parece indicarlo el trabajo seminal del tema publicado por Jozsa en 1997 [79] donde muestra cómo el recurso es esencial para obtener la ventaja cuántica en el caso de la QFT. A esta tesis, de que de haber una ventaja cuántica es debida al entrelazamiento, según [80] se la conoce como *'sufficiency of entanglement' thesis*. Sin embargo, al poco tiempo de este trabajo se presenta en 1999 un teorema que parece indicar lo contrario. El teorema de Gottesman-Knill [81, 82, 83] indica que utilizando únicamente compuertas de Clifford (Compuertas de Pauli, $CNOT$ y la compuerta de *Hadamard*) puede obtenerse estados entrelazados, como pueden ser los estados de Bell, y sin embargo este tipo de computo puede ser eficientemente simulado en computadoras clásicas.

Si bien el teorema de Gottesman-Knill parece contravenir la tesis propuesta por Jozsa, como remarca [80] esto es verdadero en cierto sentido y no en otro. Lo que demuestra el teorema es que la sola presencia de entrelazamiento no alcanza para obtener la ventaja cuántica. Como veremos existen muchos estados que presentan diferentes tipos de entrelazamiento, y muchos de ellos no pueden ser obtenidos con las compuertas de Clifford. En un trabajo posterior Jozsa y Linden [84] muestran exhaustivamente en todos los casos conocidos en los que se puede hablar de una ventaja cuántica, cómo es el entrelazamiento el que da lugar a tal ventaja. La pregunta respecto a si es el entrelazamiento el único recurso físico que es necesario para la obtención de una ventaja cuántica sigue sin tener una respuesta completa, como reconocen Nielsen y Chuang [18] *"¿Qué tan poderosas son las computadoras cuánticas? ¿Qué es lo que les da ese poder? Nadie sabe la respuesta aún, más allá de las suposiciones que se deducen de ejemplos concretos como el algoritmo de factorización"*, pag. 40.

Lo que sí está claro es que cualquier modelo que quiera ser útil para describir y aproximar a la capacidad de un computador cuántico debe ser capaz de generar entrelazamiento y como se verá en relación al modelo discreto de coeficientes enteros es que algunos de los principales resultados en información cuántica como puede ser la teleportación o los códigos superdensos pueden estudiarse de manera inmediata dentro del modelo y que varios (no todos) de los estados cuánticos conocidos de máximo entrelazamiento (o muy alto entrelazamiento) sorpresivamente forman parte del conjunto de estados discretos con coordenadas enteras.

6.1.1. Sistemas conformados por dos qubits: estados de Bell

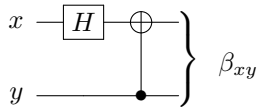
Los sistemas compuestos más sencillos son los conformados por dos qubits. En este sistema, se pueden clasificar a cualquier estado en separables o entrelazado (ver 2.1.5). Se prueba en [85] que todos los estados entrelazados de dos qubit son LOCC (*local operations and classical communication*) equivalentes, en el sentido de que mediante operaciones locales sobre cada uno de los subsistemas y comunicación clásica se puede obtener de cualquier estado entrelazado otro estado entrelazado. En

particular, cobran vital importancia los estados de Bell:

$$\beta_{00} = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \quad \beta_{01} = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$$
$$\beta_{10} = \frac{|00\rangle-|11\rangle}{\sqrt{2}} \quad \beta_{11} = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

En [86], se muestra que estos estados son los únicos de máximo entrelazamiento, sus correspondientes matrices densidad reducidas corresponden a una mezcla uniforme de los estados $|00\rangle$ y $|11\rangle$, y por tanto tienen rango de Schmidt máximo. Los estados de Bell son fundamentales en las principales aplicaciones de la información cuántica como pueden ser la teleportación cuántica y el código superdenso.

Estos cuatros estados tienen coeficientes enteros, salvo el factor $\sqrt{2}$, por tanto son estados discretos con coeficientes enteros. Además los estados de Bell forman una base orto-normal de estados gaussianos para los sistemas de dos qubits. Observando el circuito que a partir de estados de la base computacional genera estos cuatro estados



vemos que las compuertas componentes están comprendidas dentro del modelo discreto presentado. Mientras que H es una de las compuertas básicas del modelo, $\Lambda(X)$ puede obtenerse a partir de las compuertas originales del modelo (ver sección 4.2) por tanto la matriz asociada a esta transformación es una compuerta cuántica discreta de dos qubits (4.4).

6.1.2. Sistemas conformados por tres qubits: GHZ, W y sus generalizaciones

A diferencia de lo que ocurre en sistemas de dos qubits, en sistemas de mayor orden la clasificación ya no es tan clara. Además de estudiar los problemas de bi-partición de sistemas, puede querer estudiarse la multi-partición de estos, hasta llegar a la partición máxima de los mismos, que es estudiar las correspondientes matrices de densidad de cada sistema de un qubit componente. El problema de lo anterior reside en que la elección de la partición primaria que se haga determinará las subsiguientes particiones.

En tal sentido, en [85] se demuestra que en sistemas de tres qubits hay más de un tipo de equivalencia de entrelazamiento, es decir, hay estados entrelazados que no pueden ser transformados mediante LOCC de uno en otro. Aún más, aunque se descarte la imposición de certeza de alcanzar un estado respecto al otro, y se admita como clase de equivalencia que uno pueda obtenerse del otro mediante operaciones locales y comunicación clásica con una probabilidad mayor a cero SLOCC (*stochastic local operations and classical communication*) [87] estos dos tipos de estados no son equivalentes.

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \qquad \text{y} \qquad |W\rangle = \frac{|100\rangle + |010\rangle + |001\rangle}{\sqrt{3}}$$

El estado $|GHZ\rangle$ fue utilizado por primera vez en [88] al mostrar que con él se puede violar máximamente la desigualdad de Bell en un solo experimento. Lo anterior es una de las razones por las cuáles se considera que el estado $|GHZ\rangle$ es de máximo entrelazamiento [89]. Otra de las razones es que la información mutua de los resultados de la medición es máxima. Además, a partir de este estado, con operaciones locales, puede lograrse con certeza que dos de los tres sistemas pueden compartir entre ellos un estado de Bell. En general el estado $|GHZ\rangle$ es visto como una extensión natural de los estados de Bell.

Ocurre, sin embargo, que al aplicar la traza parcial a uno de los tres subsistemas del estado $|GHZ\rangle$, los dos subsistemas restantes quedan en un estado completamente separable. Esto implica que el estado $|GHZ\rangle$ es muy frágil respecto a la perdida de partículas, o en un protocolo de intercambio de información cuántica, vulnerable a que si alguna de las tres partes no colabore, los restantes no puedan hacer uso del entrelazamiento como recurso. Por el contrario, aunque el estado $|W\rangle$ no es de máximo entrelazamiento en ninguno de los sentidos que se discutió, cuando se toma la traza parcial de uno de sus subsistemas los dos restantes quedan en un estado que mantiene una gran cantidad de entrelazamiento, aunque no quede en un estado puro. En [85] se demuestra que tomando diferentes medidas de entrelazamiento, para todas las bi-particiones de un sistema de tres qubits simétrico, el estado que mantiene la mayor cantidad de entrelazamiento para su subsistema de dos qubits no trazado es el estado $|W\rangle$. Esto hace que $|W\rangle$ también sea de gran importancia en los protocolos de comunicación cuántica.

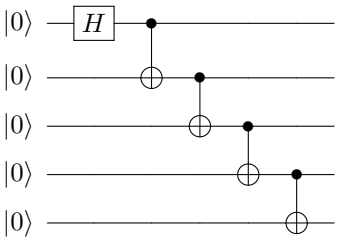
Estos dos estados son fácilmente generalizables para sistemas de n qubits:

$$|GHZ_n\rangle = \frac{|000\ldots0\rangle + |111\ldots1\rangle}{\sqrt{2}} \qquad \text{y} \qquad |W_n\rangle = \frac{|100\ldots0\rangle + |010\ldots0\rangle + \ldots + |0\ldots001\rangle}{\sqrt{n}}$$

Mientras que es inmediato que $|GHZ_n\rangle$ es un estado discreto de coeficientes enteros ($|GHZ_n\rangle \in E$), $|W_n\rangle$ no siempre lo es. En particular para $n = 3$, es claro que $|W\rangle$ no lo es. Sin embargo, cuando n es una potencia de 2, $n = 2^m$ para algún m entero, el estado $|W_{2^m}\rangle$ si será un estado discreto de coeficientes enteros y $|W_{2^m}\rangle \in F_m$. Por ejemplo, para $n = 4$:

$$|W_4\rangle = \frac{|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle}{2} \in E$$

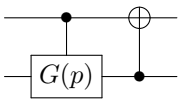
En [90] se especifican los circuitos óptimos para construir estos dos tipos de estados entrelazados multipartitos. Como es de preveer, el circuito dado para $|GHZ_n\rangle$ es claro que puede implementarse con compuertas del modelo discreto:



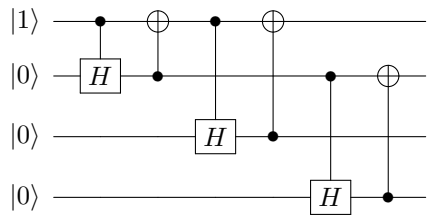
$$|GHZ_5\rangle = \frac{|00000\rangle + |11111\rangle}{\sqrt{2}}$$

Desde que este circuito está compuesto con compuertas H, que es una compuerta elemental del modelo, y $\Lambda(X)$, que se puede obtener exactamente a partir de $\{H, G\}$ y qubits auxiliares no hay más nada que agregar.

Para el caso de $|W_n\rangle$ el circuito dado se basa en la utilización reiterada del módulo

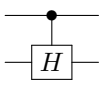


donde $G(p) = \begin{pmatrix} \sqrt{p} & -\sqrt{1-p} \\ \sqrt{1-p} & \sqrt{p} \end{pmatrix}$. Para un n cualquiera se utilizarán las compuertas $G\left(\frac{1}{i}\right)$ con $i = 2, 3...n$. En general, $G\left(\frac{1}{i}\right)$ no es una compuerta del modelo discreto. Sin embargo para el caso $n = 2^m$ que es el que interesa respecto al modelo discreto el circuito se simplifica notoriamente ya que puede construirse utilizando únicamente la compuerta $G\left(\frac{1}{2}\right) = H$ y es la única de las $G(p) \in \mathcal{P}$.



$$|W_4\rangle = \frac{|1000\rangle+|0100\rangle+|0010\rangle+|0001\rangle}{2}$$

Sin embargo, es importante notar que



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

no es una compuerta discreta, ya que es claro que sus columnas 1 y 3 son estados discretos de niveles con distinta paridad ($[1,0,0,0] \in F_0$ y $[0,0,\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}] \in F_1$) y por tanto no cumple el teorema 4.4.1. Este circuito no es válido en el contexto del modelo discreto.

Utilizando únicamente las compuertas $\{H, G\}$ y compuertas que se pueden obtener de manera de manera exacta a partir de ellas es posible construir de manera explícita un circuito que a partir del estado $|0\rangle^{\times n}$ devuelva el estado W_n para $n = 2^m$:

Paso 1. Se parte de una tira de $n = 2^m$ qubits inicializados en 0's: $|0\rangle^{\otimes n}$

Paso 2. Se les aplica la compuerta $Id^{\times n-m} \times H^{\otimes n}$, es decir, a los m qubits menos significativos se los superpone , obteniendo $|0\rangle^{\otimes 2^m-m}|+\rangle^{\otimes m}$. En la notación decimal se tendrán todos los estados de la forma $\frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|0\rangle^{\otimes 2^m-m}|i\rangle$.

Paso 3. Finalmente se aplica un circuito de cambio de base que realiza la permutación entre los estados

$$P(|0\rangle^{\otimes 2^m-m}|i\rangle) = |2^i\rangle \text{ para todo } i = 0,\ldots,n-1$$

Al cumplirse que $P_j \in F_0$, siendo P_j cualquier columna de P y por el teorema 4.4.1 se cumple que P es una puerta discreta.

6.1.3. Sistemas conformados por más de tres qubits

Al intentar generalizar los resultados obtenidos para tres qubits a sistemas multipartitos mayores [85] se concluye que habrá infinitas clases de entrelazamientos in-equivalentes (SLOCC) entre sí. Como se resume en [91] aún hoy se desconoce la geometría exacta por detrás de los estados entrelazados, en [83] se muestra que el número de tipos de entrelazamientos no equivalentes crece exponencialmente con el número de qubits. Aún más para sistemas de más de tres qubtis las medidas de entrelazamiento que se tomen [92], aún solo considerando biparticiones, dan un ordenamiento diferente de los estados respecto de su entrelazamiento. En particular, con ninguna de las 4 formas de medir el entrelazamiento utilizadas en dicho trabajo, la entropía lineal, de Von Newmann, de Renyi o la negatividad de la matriz reducida[1], dan al estado GHZ_n, como al de mayor entrelazamiento. De hecho, la posición de este estado en la distribución de entrelazamiento obtenida se va deteriorando con el aumento de la cantidad de qubits.

[1]Cantidad de valores propios negativos asociados a la matriz reducida luego de bi-partir un estado

Para el espacio de cuatro qubits Higuchi y Sudbery [93] proponen al estado HS como el de mayor entrelazamientos según la entropía de Von Newman:

$$|HS\rangle = \frac{1}{\sqrt{6}}\left(|1100\rangle + |0011\rangle + w^2(|1001\rangle + |0110\rangle) + w(|1010\rangle + |0101\rangle)\right)$$

y en [94] se prueba que este estado es un máximo local para esta medida de entrelazamiento. Este estado no es un estado del conjunto de estados discretos con coeficientes constantes, y de ser cierta la conjetura de Higuchi y Sudbery, esto implica que con este modelo no podrían alcanzarse al menos algunos estados de máximo entrelazamiento.

Brown *et al.* [95] encuentran mediante una búsqueda numérica de estados de alto entrelazamiento según la negatividad de la matriz reducida, estados para 4 y 5 qubits que según los autores están dentro de los de más alto entrelazamiento posible. Estos son:

$$|BSSB4\rangle = \frac{1}{2\sqrt{2}}\left(i|0010\rangle + (1+i)|0101\rangle + |0110\rangle + (1+i)|1000\rangle + |1011\rangle + i|1111\rangle\right)$$

$$|BSSB5\rangle = \frac{1}{2\sqrt{2}}\left(|00110\rangle + |01011\rangle + |10001\rangle + |11100\rangle + i(|00101\rangle + |01000\rangle + |10010\rangle + |11111\rangle)\right)$$

Estos estados sí pertenecen al conjunto de estados discretos y ambos pertenecen a F_3. Para obtener un circuito que permita generarlos puede utilizarse el procedimiento dado en la demostración del teorema 4.3.3.

En [92] se constata el resultado para 4 qubits ($|BSSB4\rangle$) obtenido por Brown *et al.* [95] no es óptimo: el estado HS tiene un mayor grado de entrelazamiento en todas las medidas que se elijan y este es alcanzado por su procedimiento de búsqueda. Sin embargo, para 5 qubits por Borras *et al.* no encuentran otro estado que tenga mayor entrelazamiento que el $|BSSB5\rangle$ para 5 qubits. Lo anterior parece indicar que los estados $|BSSB4\rangle$ y $|BSSB5\rangle$ no son estados de máximo entrelazamiento, pero sí tienen un alto grado de entrelazamiento, significativamente mayor respecto a la media de los estados puros de 4 y 5 qubits.

Borras *et al.* [92] además encuentran para 6 qubits el estado:

$$\begin{aligned}|BPB\rangle = \frac{1}{\sqrt{2}^5}(&|000000\rangle+|111111\rangle+|000011\rangle+|111100\rangle+|000101\rangle+|111010\rangle+|000110\rangle+|111001\rangle\\ &+|001001\rangle+|110110\rangle+|001111\rangle+|110000\rangle+|010001\rangle+|101110\rangle+|010010\rangle+|101101\rangle\\ &+|011000\rangle+|100111\rangle+|011101\rangle+|100010\rangle-|010100\rangle+|101011\rangle+|010111\rangle+|101000\rangle\\ &+|011011\rangle+|100100\rangle+|001010\rangle+|110101\rangle+|001100\rangle+|110011\rangle+|011110\rangle+|100001\rangle)\end{aligned}$$

de alto entrelazamiento. Utilizando que este estado deviene en matrices de densidad de los subsistemas reducidos de 1, 2 y 3 completamente mezcladas, este estado a sido utilizado para la construcción de múltiples protocolos de información cuántica [96, 97]. Este estado también pertenece al conjunto de estados discretos y en particular pertenece a F_5.

Estados Cluster

En ingles los estados del tipo *cluster-state* son estados cuánticos que se generan mediante arreglos de qubits dispuestos en grafos, en los que los vértices representan qubits y las aristas interacciones del tipo Ising entre los qubits conectados [98]. Su preparación puede ser resumida en dos pasos [99]:

Paso 1. Cada qubit es preparado en el estado $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$.

Paso 2. A cada par de qubits que están conectados mediante una arista se les aplica una interacción del tipo ΛZ.

Desde que el estado inicial es un estado discreto de coordenadas enteras y las interacciones entre ellos son compuertas que pueden ser obtenidas de manera exacta a partir de $\{H, G\}$, en virtud de lo visto en 4.3.3, este tipo de estados siempre serán estados comprendidos dentro del modelo de coeficientes enteros.

Estos estados son importantes, no solo porque permiten desarrollar un modelo de computación cuántica propio, basada en medidas, sino que en [100] se demuestra que estos estados son de alto entrelazamiento siempre. Se demuestra que lo son en el sentido de que si se tiene un estado de $n-$qubits, se necesitarán realizar cerca de $n/2$ medidas para obtener un estado separable completa -mente. Como se observó, esto no ocurre en el caso de los GHZ_n y ocurre de manera completa en el caso de los W_n en el que es necesario realizar $n-1$ medidas para obtener un estado separable.

La importancia de estos estados se basa en que simplifican mucho la preparación de estados de alto entrelazamiento, y por su robustez a la perdida de partículas, tienen múltiples usos en criptografía cuántica.

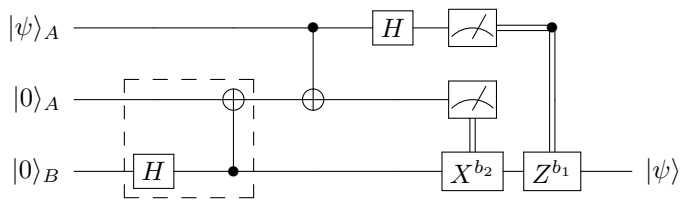
6.2. Principales protocolos de información cuántica

Presentamos aquí algunos de los protocolos de información cuántica fundamentales y las limitaciones que impone el módelo de computación cuántica con coeficientes enteros a la implementación de los mismos.

6.2.1. Teleportación cuántica

Uno de los resultados más asombrosos del entrelazamiento aplicado a la teoría de la información fue descubierto por Bennett y Wiesner [101] en 1992: la teleportación cuántica. Si dos agentes a distancias virtualmente infinitas comparten un estado de Bell (estado de máximo entrelazamiento), los autores muestran que transmitiendo dos únicos bits de información clásica, mediante un canal clásico, una de las partes puede transmitir a la otra el estado de un qubit aleatorio y desconocido por los agentes de manera *exacta*.

Una representación circuital de lo anterior es:



Luego de generar el par de Bell (circuito remarcado) $\frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$ compartido entre las partes A y B se tendrá el estado $|\psi_A\rangle \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$. Tomando el estado $|\psi_A\rangle$ de la forma genérica $\alpha|0\rangle + \beta|1\rangle$, la parte A aplicará a su subsistema de dos qubits las compuertas $CNOT$ y H, quedando el sistema

entero en el estado:

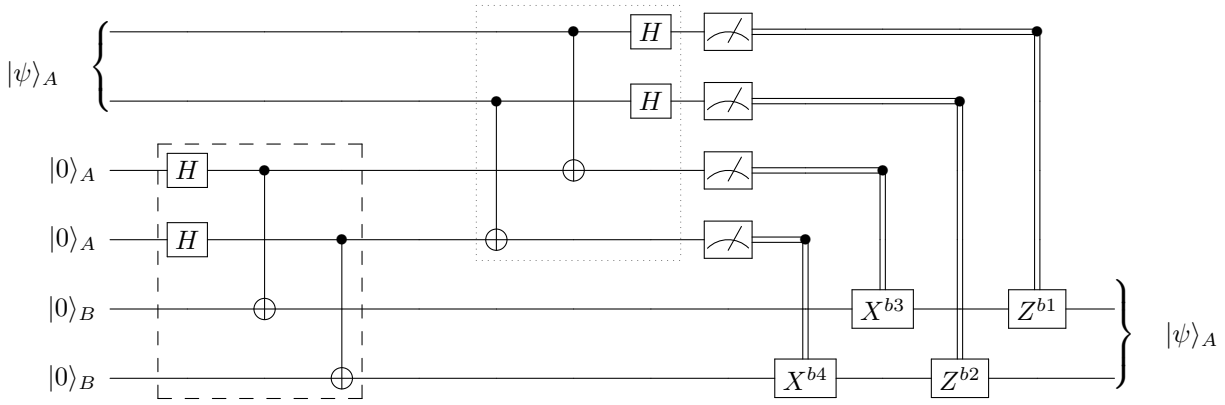
$$\frac{1}{2}\left(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)\right)$$

Luego, cuando la parte A mida sus dos qubits obtendrá dos bits de información b_2b_1 que le transmite de manera clásica a la parte B. Éste a su vez le aplica las compuertas $X^{b_2}Z^{b_1}$ a su qubit del estado de *Bell* compartido y obtendrá con 100 % de certeza el estado inicial $|\psi\rangle$.

Si el estado inicial a transmitir $\alpha|0\rangle+\beta|1\rangle$ es un estado discreto de coeficientes enteros, es inmediato de chequear que todos los estados intermedios también lo serán. Sin embargo la gran dificultad que se presenta es que estados de un qubit en el modelo que nos compete a saber hay cuatro: $|0\rangle, |1\rangle, |+\rangle$ y $|-\rangle$. Por lo cuál enviando dos bits de información se puede recuperar esta información sin ningún protocolo de teleportación.

De este protocolo original se han hecho muchas variantes. En particular, nos interesa la reformula -ción que hace Rigolin [102] del circuito original para poder transmitir mediante 4 bits de información clásica un estado correspondiente a un subsistema de 2 qubits. Esto es importante en el contexto del modelo discreto ya que existen infinitos estados discretos de dos qubits, que como se verá, pueden ser transmitidos mediante un protocolo que puede implementarse completamente dentro del modelo.

En el trabajo original [102] se da una versión bastante complicada de compactar aquí, optamos por tanto, por presentar modificaciones propias del protocolo que permiten conceptualizarlo de manera muy similar al protocolo de teleportación cuántica usual. La versión circuital que presentamos aquí tienen dos grandes ventajas. La primera es que las medidas finales que tiene que realizar una de las partes para transmitir clásicamente la información a su contraparte, puede hacerse directamente en la base computacional y por tanto obtener directamente los 4 bits de información necesaria para reconstruir el estado. La segunda ventaja tiene que ver con la interpretación mediante el modelo discreto. Como en la teleportación de un qubit puede verse que todas las compuertas que intervienen pueden obtenerse de manera exacta a partir de $\{H, G\}$, por lo tanto, si el estado $|\varphi\rangle_A$ es un estado discreto de dos qubits, todos los estados intermedios también serán estados discretos de dos qubits.



Para entender brevemente el circuito presentado arriba basta explicar el bloque recuadrado por la línea puenteada. Este bloque se encarga de generar entrelazamiento entre 2 pares de bits compartidos entre las partes A y B. La linealización de estos 4 bits en las 16 combinaciones de bits posibles dan lugar a 16 estados ortogonales 2 a 2 que los autores originales catalogan como estados de bell generalizados. Cuáles son estos queda mucho más fácil de explicar a raíz del circuito propuesto aquí.

Iniciando los 2 qubits de la parte A en $|00\rangle$, tomando las cuatro variantes de la parte B,

$|00\rangle, |01\rangle, |10\rangle$ y $|11\rangle$ se obtienen respectivamente los estados:

$$|g_{00}\rangle = |0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle$$
$$|g_{01}\rangle = |0001\rangle + |0100\rangle + |1011\rangle + |1110\rangle$$
$$|g_{02}\rangle = |0010\rangle + |0111\rangle + |1000\rangle + |1101\rangle$$
$$|g_{03}\rangle = |0011\rangle + |0110\rangle + |1001\rangle + |1100\rangle$$

Si los qubits de la parte A se inicializan en las otras 3 combinaciones binarias posibles, $|01\rangle, |10\rangle$ y $|11\rangle$, lo que se obtiene son estos mismos estados pero con fases relativas entre los estados de la base computacional respetando siempre el patrón de signo $++--, +-+-, +--+$ respectivamente a los estados iniciales dados a los estados de la parte A. A modo de ejemplo:

$$g_{32} = |0010\rangle - |0111\rangle - |1000\rangle + |1101\rangle$$

Luego, como en el caso del estado $|g_{00}\rangle$ es fácil mostrar que el estado inicial

$$|\psi_A\rangle \otimes |g_{00}\rangle = \frac{1}{2}(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle) \otimes (|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)$$

puede reescribirse como una sumatoria de estados de la forma

$$\frac{1}{8}\sum g_{mn} \otimes |\hat{\psi}_{mn}\rangle \text{ con } m, n = 0, 1, 2, 3$$

donde $|\hat{\psi}_{mn}\rangle$ es alguno de los 16 estados posibles $(Z^{b1} \otimes Z^{b2})(Z^{b3} \otimes Z^{b4})|\psi_A\rangle$, por lo que, aplicando el circuito recuadrado con puntos a los primeros 4 bits (en posesión de la parte A) se obtendrá los 16 estados en la base computacional:

$$\frac{1}{2}\sum |b1\rangle|b2\rangle|b3\rangle|b4\rangle \otimes |\hat{\psi}_{mn}\rangle$$

Midiendo los primeros 4 bits se sabrá con certeza absoluta cuál de los 16 posibles estados $|\hat{\psi}_{mn}\rangle$ tendrá en su poder la parte B y con la información clásica que le envía la parte A podrá reconstruir sin problemas el estado original $|\psi_A\rangle$

Existen otros protocolos para la teleportación cuántica que permiten teleportar uno a varios qubits. En [103] se da un protocolo de entrelazamiento utilizando estados entrelazados de tipo cluster (ver 6.1.3) para transimitir un estado de la forma

$$|\psi\rangle = \alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)$$

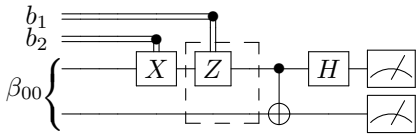
Aunque la implemetación de este protocolo puede hacerse dentro del modelo discreto sin problema, de nuevo se presenta el problema de que en el conjunto de estados discretos hay una cantidad muy limitada de estados discretos que tengan este formato. Además, en [104] se demuestra que para que el estado se pueda reconstruir con certeza absoluta, los estados cluster deben finalmente ser del tipo $|GHZ\rangle_n$. Finalmente hay protocolos [105] que utilizan como estados entrelazados los W (ver 6.1.2). Estos tipos de protocolos solo pueden implementarse exactamente si la dimensión de los estados W_n coincide con una potencia de base dos.

6.2.2. Código Superdenso

El código superdenso es un protocolo de información cuántica que en cierto modo es el inverso del de teleportación cuántica. Propuesto por primera vez por Bennett y Wiesner [101] propone

transmitir información clásica mediante un canal cuántico. Asumiendo que dos partes comparten un estado entrelazado previamente, una de las partes envía mediante el canal cuántico su qubit del par entrelazado y mediante la medición de ambos qubits puede obtener la información clásica codificada por el emisor.

En el caso óptimo el protocolo de comunicación queda determinado por el siguiente circuito



Ambas partes comparten un estado de máximo entrelazamiento, un par $|GHZ\rangle$. La parte emisora codifica sus dos 2 bits (b_1, b_2) mediante las compuertas $Z^{b_1}X^{b_2}$. Es decir, si se quiere enviar el mensaje 00 no se hace nada, el 01 se aplica una compuerta X, el 10 se aplica una compuerta Z y en caso del 11 se aplican ambas ZX. Con esto cada mensaje queda identificado con un posible estado de bell βij. Seguidamente, este primer qubit del par es enviado al receptor que con ambos qubit en su poder aplica el bloque encuadrado llevando el estado de bell βij al estado de la base computacional $|i\rangle|j\rangle$. Finalmente al medir obtiene la información clásica que se quiso transmitir.

Mediante este protocolo se logra enviar 2 bits de información cuántica utilizando el envío de un solo qubit cuántico. Es decir se logra duplicar la capacidad de un canal clásico. Dicho de otro modo, el código superdenso puede convertir un canal cuántico bidireccional con ancho de banda B en un canal clásico unidireccional con ancho de banda 2B. Durante el proceso, el entrelazamiento entre las partículas es destruido haciendo que el proceso no pueda ser repetido, a no ser que de que ambas partes compartan nuevamente un estado entrelazado.

Este tipo de protocolo, al igual que en el caso de la teleportarción, puede ser extendido para enviar más de dos bits de información. Si ambas partes comparten $n - qubits$ entrelazados previamente pueden enviarse 2n bits de información clásica. Una implementación que utiliza los mismos estados GHZ generalizados dados en el protocolo generalizado de teleportación se encuentra en [106]. Este tipo de fenómeno no viola la cota superior de información accesible de un estado cuántico conocida como cota de Holevo (ver A.5.4).

Todos las compuertas que intervienen en este protocolo pueden ser generadas de manera exacta por las compuertas del modelo discreto, por tanto, todos los estados intermedios del proceso son estados discretos. Ocurre lo mismo en su generalización para el envio de $n - qubits$.

Capítulo 7

Aplicación del modelo a algoritmos cuánticos

Fue la última década del siglo XX la más fructífera en cuánto al desarrollo de algoritmos cuánticos. Los principales algoritmos (o circuitos) cuánticos hasta el día de hoy fueron desarrollados en prácticamente 5 años. Deutsch, además de sentar las bases teóricas de la computación cuántica basada en compuertas [107] da el primer ejemplo de una tarea que una computadora cuántica podría hacer más eficientemente que una clásica

El problema de Deutsch consiste en determinar si una función definida desde el conjunto binario $\{0,1\}$ a este mismo conjunto es constante o balanceada. Una computadora clásica requiere hacer dos evaluaciones funcionales para poder concluir esto, sin embargo cuánticamente es posible haciendo una única operación equivalente a la evaluación funcional. A esta operación equivalente se la conoce como Oráculo. Posteriormente el problema fue extendido por Deutsch y Josza [108] para determinar si una función $f : \{0,1\}^n \to \{0,1\}$ es constante o balanceada manteniendo una única operación cuántica para arribar a esa conclusión frente a las $n/2 + 1$ operaciones clásicas que hay que hacer para determinarlo clásicamente en el peor de los casos. Aunque, este problema no era de interés en sí mismo, permitió vislumbrar las posibilidades de los algoritmos cuánticos.

En 1994 Shor [6] público uno de los resultados más importantes para la computación cuántica. La transformada rápida de Fourier podía implementarse utilizando aproximadamente n^2 pasos frente a los $n2^n$ clásicos necesarios para realizar la transformación de 2^n números. Aunque parezca maravilloso, debido a las múltiples aplicaciones que tiene la transformada de Fourier en procesamiento de señales, el problema es que la información de los transformados queda inaccesible mediante mediciones, ya que queda almacenada en fases relativas de los estados. Sin embargo, esta hallazgo fue usado por Shor [8] como herramienta intermedia para llegar a otros importantes resultados como ser el algoritmo de factorización y la logaritmación discreta. Una versión completa y compacta de estos algoritmos puede encontrarse en [109]. Otros algoritmos importantes posteriormente desarrolla -dos también se han apoyado en los resultados obtenidos por Shor, como pueden ser el algoritmo de Simon que resuelve una versión del problema del subgrupo oculto [110] y el algoritmo de estimación de fase [109]. Una aplicación de este último es la resolución de sistemas lineales de ecuaciones [111] mediante algoritmos cuánticos.

En 1997 Gover [9, 112] pública un nuevo algoritmo que se aparta de la estructura seguida por Shor y los trabajos que le siguieron. La funcionalidad del mismo es la búsqueda de un objeto con una determinada propiedad en un conjunto desordenado de elementos. La ventaja cuántica que se obtiene respecto al peor caso clásico es menos espectacular que en los otros casos y es de orden

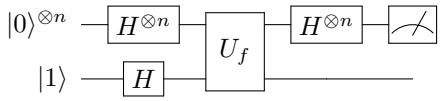
cuadrático. Como se verá (ver 7.3) varias reformas de este algoritmo se han hecho pero sin que estos hayan dado lugar a nuevos a algoritmos verdaderamente nuevos.

Como ya lo notó Shor en 2002 [13], el descubrimiento de nuevos algoritmos cuánticos se ralentizó mucho luego de estos descubrimiento. De hecho, hoy día, más de 20 años después, estos algoritmos mencionados siguen siendo los principales de la computación cuántica. Las razones pueden ser varias, entre ellas la falta de costumbre para pensar algoritmos en este tipo de estructuras, lo contra-intuitivo de los principios que subyacen a la cuántica, como al superposición, entrelazamiento e interferencia. A día de hoy, la urgencia de contar con hardware tal que permita correr en condiciones aceptables estos algoritmos hace que está tarea absorba gran parte de la masa de investigación en el área.

7.1. Algoritmo de Deutsch-Jozsa

El algoritmo de Deutsch-Josza toma el nombre de los autores que lo crearon en [108] en 1992. Consiste en determinar si una función $f : \{0,1\}^n \to \{0,1\}$, es constante o balanceada, esto es, tomar el mismo valor funcional para todas los valores de entrada (constante), o para la mitad de los valores de entrada tomar el valor funcional 1 y para la otra mitad 0 (balanceada).

La versión circuital del algoritmo que presentamos aquí es la dada en el trabajo compilatorio de algoritmos cuánticos de Ekert et al [109]. El algoritmo queda realizado mediante el algoritmo siguiente:



Donde U_f es una compuerta cuántica llamada óraculo que se comporta de la siguiente manera: $U_f|x,y\rangle \to |x, y \oplus f(x)\rangle$

El estado y es un estado auxiliar que debe inicializarse en el estado $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. A los estados correspondientes a los n primeros qubits se les aplica una compuerta $H^{\otimes n}$, obteniendo una superposición uniforme de los 2^n estados de la base computacional. Por tanto, para un estado cualquiera de los $n-$qubits de la base computacional $|x\rangle$, para el cual $f(x)$ será 0 o 1, se tiene que:

- Si $f(x) = 0$: $U_f|x,y\rangle = U_f|x,y\rangle = |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus 0\right) = |x\rangle \frac{|0\oplus 0\rangle - |1\oplus 0\rangle}{\sqrt{2}} = |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |x,y\rangle$
- Si $f(x) = 1$: $U_f|x,y\rangle = U_f|x,y\rangle = |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus 1\right) = |x\rangle \frac{|0\oplus 1\rangle - |1\oplus 1\rangle}{\sqrt{2}} = |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|x,y\rangle$

En definitiva $U_f|x,y\rangle|_x = (-1)^{f(x)}|x\rangle$. Luego

$$U_f \sum_x \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Al aplicarle finalmente la compuerta $H^{\otimes n}$ a los n primeros qubits se obtiene el estado final:

$$\sum_z \sum_x \frac{(-1)^{\langle x,z\rangle + f(x)}|z\rangle}{2^n} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Luego si $f(x)$ es constante y se mira el coeficiente correspondiente a $|z\rangle = |0\rangle^{\otimes n}$, se tendrá que $\sum_x \frac{(-1)^{\langle x,0\rangle + f(x)}}{2^n} = \sum_x \frac{(-1)^{f(x)}}{2^n} = \pm 1$. Luego todo el resto de los coeficientes deben ser 0.

Si en cambio $f(x)$ es balanceada, $|z\rangle = |0\rangle^{\otimes n}$, se tendrá que $\sum_x \frac{(-1)^{\langle x,0\rangle + f(x)}}{2^n} = \sum_x \frac{(-1)^{f(x)}}{2^n} = 0$.

Por tanto, midiendo el registro de los primeros $n-$qubits si se obtiene todos los estados 0 se puede asegurar que la función es balanceada, en cualquier otro caso, se puede asegurar que la función es constante. Todo esto haciendo una única utilización del oráculo U_f.

Como ya se adelantó, este algoritmo fue muy importante ya que fue el primero en mostrar que una computador cuántico puede realizar tareas más rápido que su contrapartida clásica. En el peor de los escenarios, un computador clásico tiene que realizar $2^n/2 + 1$ invocaciones a la función para saber si esta es constante o balanceada. Además, por su simplicidad, puede ser usado para evaluar comparativamente distintas implementaciones físicas de prototipos de computadores cuánticos [113]. Varias implementaciones físicas de este algoritmo han sido realizadas a la fecha [114, 115, 116].

En relación con el modelo discreto, este algoritmo puede ser implementado exactamente utilizando las compuertas del modelo. Las compuertas de Hadamard, están comprendidas dentro del conjunto discreto, por lo que solo resta ver que U_f puede realizarse completamente dentro del conjunto discreto. Para esto basta observar que la definición U_f en la base computacional $U_f|x, y\rangle \to |x, y \oplus f(x)\rangle$ es una permutación de los estados de dicha base. En el caso extremo $f(x) = 0$ para todo x, se tiene que es la identidad. Por tanto haciendo uso de lo ya demostrado, (ver 4.2) puede deducirse que puede implementarse de manera exacta utilizando compuertas generadas de manera exacta a partir de $\{H, G\}$.

7.2. Quantum Fourier Transform

Dado un conjunto de N números complejos $x_0, \ldots, x_{N-1}$ se define su Transformada Discreta de Fourier (DFT) como un conjunto de otros N números complejos $z_0, \ldots, z_{N-1}$ tales que:

$$z_k := \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x_l \cdot e^{\frac{2\pi i k l}{N}}$$

De a partir de esta definición, puede definirse la siguiente transformación a partir de la base computacional

$$|l\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{-\frac{2\pi i k l}{N}} |k\rangle$$

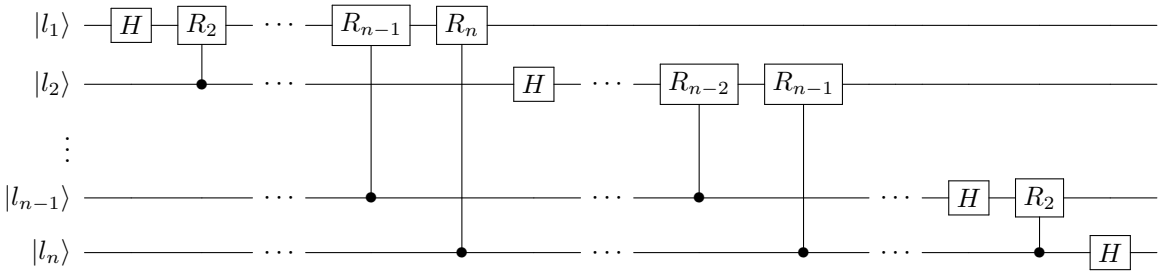
si se tiene un estado cuántico cuyas amplitudes coinciden con los x_k:

$$|x\rangle = \sum_{l=0}^{N-1} x_l |l\rangle$$

Definimos su Transformada Cuántica de Fourier QFT como:

$$QFT\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_k e^{\frac{2\pi i k l}{N}}\,|y\rangle$$

En 1994 Shor [6] hizo un hallazgo importantísimo en el área mostrando que esto podía implementarse cuánticamente utilizando el circuito



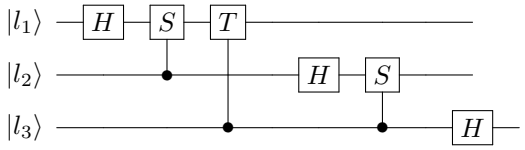
donde $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$

Está claro que para $k \geq 3$ la compuerta R_k no es una compuerta discreta, para ver esto vale observar que

$$R_3|+\rangle = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} |+\rangle = \frac{1}{2} \begin{bmatrix} \sqrt{2} \\ 1+i \end{bmatrix}$$

Utilizando la definición de compuerta discreta, vemos que partimos de un estado discreto $|+\rangle$ (ver 4.4) y no llegamos a otro estado discreto, por tanto para $k = 3$ no es una compuerta discreta y ocurre lo mismo para $k \geq 3$.

Aún en el caso de 3 qubits, donde solo se necesita utilizar hasta R_2, y donde el circuito queda reducido a



Se puede ver de una manera muy similar que la compuerta

cuya representación matricial es $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix}$

No es una compuerta discreta, ya que sus columnas no son estados discretos de igual paridad violando así el teorema 4.4.1.

Podría suponerse que puede existir otro arreglo de compuertas que no utilice estas compuertas que no se pueden generar de manera exacta con las compuertas del modelo, pero lo anterior es incongruente si se observa que la representación matricial de la transformación viene dada por la propia definición de la QFT. Así en el caso de $n = 3$ la representación matricial viene dada por

$$QFT_3 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^{2S} & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix}$$

Siendo $\omega = e^{2\pi i/2^3} = \sqrt{i}$ Por tanto la segunda columna $[1, \frac{1+i}{\sqrt{2}}, i, \frac{-1+i}{\sqrt{2}}, -1, \frac{-1-i}{\sqrt{2}}, -i, \frac{1-i}{\sqrt{2}}]^T$ puede verse que no es un estado de coeficientes enteros, por lo que no es un estado discreto.

El algoritmo que implementa la QFT no puede construirse exactamente utilizando compuertas del modelo discreto. Esto implica, que todos los algoritmos que lo toman como herramienta para alcanzar una solución, como son los algoritmos de factorización, logaritmación discreta y subgrupos ocultos, tendrán que ser aproximados, conduciendo a errores provenientes de la aproximación de querer usarse este modelo para simularlos.

7.3. Algoritmo de Grover

El algoritmo de búsqueda desarrollado por Lov K. Grover en 1997 [9, 112] es un hito en el desarrollo de algoritmos cuánticos. Resuelve el problema de hallar un elemento marcado (o varios) en un conjunto desordenado de N elementos utilizando $k_{Gr} = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ veces un sistema, denominado oráculo, que es capaz de identificar a este elemento. Presenta una mejora cuadrática en el orden en relación al clásico algoritmo de búsqueda por fuerza bruta, que requiere en el peor de los escenarios N llamadas al sistema. Se ha demostrado que el algoritmo de Grover es óptimo [117, 118] en el sentido de que dada cualquier búsqueda utilizando hasta $k_{Gr} = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ llamadas al oráculo tiene la máxima probabilidad de encontrar el elemento marcado.

Desde su publicación, múltiples estudios se han hecho sobre este algoritmo, desde sucesivas mejoras y adaptaciones hasta implementaciones en variados dispositivos físicos. El algoritmo de Grover no converge con 100 % de probabilidad al estado deseado, lo hace con una probabilidad arbitrariamente alta que depende de la relación entre soluciones y tamaño del espacio de búsqueda. Uno de las principales variantes de este algoritmo es la construido por Long [51], en la que modificará lo que más adelante llamaremos difusor para obtener con 100 % de probabilidad un elemento marcado.

El algoritmo de Grover, al ser un algoritmo de búsqueda, tiene infinidad de aplicaciones prácticas. En particular cualquier problema combinatorio NP-completo, como es el SAT, puede ser resuelto haciendo un examen exhaustivo de todas sus posibles soluciones. El algoritmo de Grover ofrece una ventaja cuadrática sobre la exploración a fuerza bruta. En el trabajo de Furer [119] se muestra que dicha ventaja se puede mantener incluso en la mayoría de algoritmos clásicos que resuelven estos problemas en una manera más sofisticada que la simple exploración por fuerza bruta. La contrapartida de este resultado es que el algoritmo de Grover facilita el ataque a los sistemas de encriptación de claves simétricas al hacer cuadráticamente más rápida la búsqueda de la clave correcta obligando a estos sistemas a duplicar el largo de sus claves para mantener el nivel de seguridad [120, 121, 122, 123].

Actualmente el algoritmo de Grover también parece ser prometedor en el área de la Inteligencia Artifical, particularmente en el modelo de redes neuronales [124, 125]. Tanto en el trabajo [125], como en otros trabajos se ha usado como soporte físico computadores cuánticos reales como ser los ofrecidos por IBM. Las limitaciones actuales de estos hacen que el desempeño del algoritmo esté seriamente limitado [126, 127]. Un factor clave para el correcto funcionamiento del mismo, en computadores ruidosos y con tiempos muy pequeños de decoherencia, es la profundidad del circuito. Minimizar la cantidad de compuertas que se utilizan en un computador real es hoy por hoy indispensable para hacer cualquier tipo de cómputo cuántico, el algoritmo de Grover no es una excepción [128].

Lo anterior pretende mostrar la importancia del algoritmo de Grover y su vigencia en el área. Por tanto es un resultado de gran importancia para esta tesis que este algoritmo en su versión original [9, 112] se puede desarrollar de manera completa utilizando las compuertas de nuestro modelo discreto (ver 4.2) y, por tanto, los estados intermedios de Grover serán estados discretos (ver 4.3). Este resultado ya fue adelantado en la tesis de maestría sobre conjuntos discretos [129].

7.3.1. Descripción del algoritmo de Grover

El problema original presentado por Grover [112] es el se describe a continuación. Sea un conjunto de $M = 2^n$ estados cuánticos en un espacio de Hilbert ($\mathcal{H}n$), siendo n la cantidad de qubits, y un estado en la base canónica desconocido marcado entre ellos (solución al problema). Dado un sistema, un operador, denominado oráculo que identifica el elemento marcado, el objetivo es hallar este elemento marcado (con alta probabilidad) utilizando la menor cantidad de pasos posible (consultas al oráculo).

Sea $|t\rangle$ el elemento marcado de la base y

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \tag{7.1}$$

el estado superposición uniforme de todos los estados de la base.

El algoritmo se puede esquematizar como:

Paso 1. Se inicializa con el estado inicial $|s\rangle$,

Paso 2. Se aplica el operador del oráculo $O = I_d - 2\,|t\rangle\,\langle t|$,

Paso 3. Se aplica el operador de difusión $D = I_d - 2\,|s\rangle\,\langle s|$,

Paso 4. Se repiten $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor - 1$ veces los pasos 2 y 3,

Paso 5. Se realiza una medición proyectiva en la base canónica en cada qubit. El estado marcado es obtenido con alta probabilidad para $N \gg 1$.

Se demuestra en [9] que k_{Gr} consultas al oráculo, es una cantidad óptima en el sentido de que es la menor cantidad de consultas que puede hacérsele para encontrar el elemento marcado con una alta probabilidad.

Al aplicar k_{Gr} veces los operadores de oráculo y difusor, el estado resultante puede ser calculado como

$$|\psi_k\rangle = G^k|\psi_0\rangle, \tag{7.2}$$

donde $Gr = DO$ es el operador de Grover. Si se definen el estado $|\bar{t}\rangle$ y el ángulo θ como sigue

$$|\bar{t}\rangle = \frac{1}{\sqrt{N-1}} \sum_{\substack{i=0 \\ i\neq t}}^{N-1} |i\rangle \;\text{ y }\; \theta = \arcsin\left(\frac{1}{\sqrt{N}}\right).$$

se puede demostrar que el estado $|\psi_k\rangle$ es de la forma

$$|\psi_k\rangle \quad = \quad \sin\left((2k+1)\theta\right)|t\rangle + \cos((2k+1)\theta)|\bar{t}\rangle,$$

Luego, la probabilidad de éxito (obtener el elemento marcado como resultado de la medición) después de k pasos es igual a

$$p(k) = \sin^2\left((2k+1)\,\theta\right). \tag{7.3}$$

Este algoritmo tiene una interpretación geométrica sencilla que permite visualizar fácilmente su funcionamiento. El estado $|\bar{t}\rangle$ es ortogonal al estado $|t\rangle$, y se puede observar que el operador de Grover Gr realiza una doble reflexión en el hiperplano formado por ambos estados, como en ilustrado en la figura 4.1

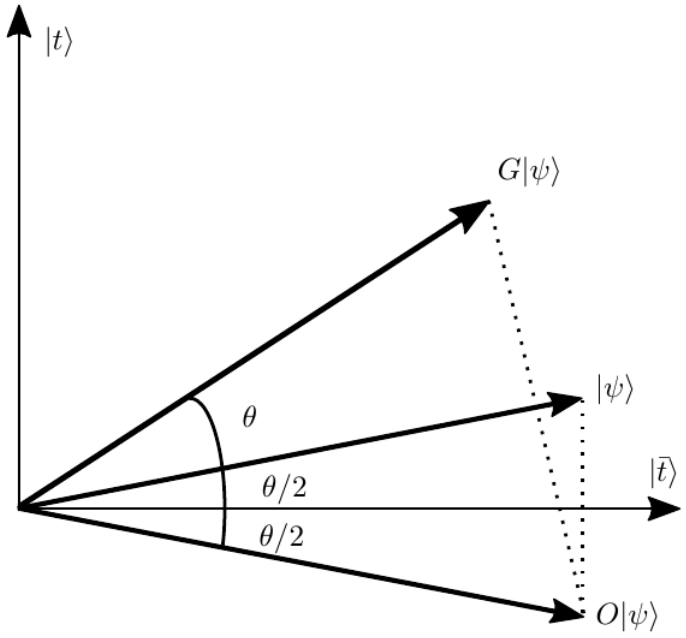


Figura 7.1: Hiperplano correspondiente al algoritmo de Grover, formado por $|t\rangle$ y $|\bar{t}\rangle$.

Es decir, si el estado $|\psi\rangle$ forma un ángulo $\theta/2$ con $|\bar{t}\rangle$, el operador del oráculo lo refleja sobre $|\bar{t}\rangle$ y el operador de difusión lo vuelve a reflejar sobre el estado original $|\psi\rangle$, obteniéndose un nuevo ángulo θ con $|\bar{t}\rangle$. Luego de una cierta cantidad de pasos, el estado es cercano a $|t\rangle$ $((2k+1)\theta/2 \approx \pi/2)$.

Una explicación más detallada y ampliada para cuando el conjunto tiene más de una solución puede encontrarse en la referencia [18].

7.3.2. Algoritmo de Grover sobre el conjunto discreto E

Como se deduce de la parte anterior el algoritmo de Grover es un algoritmo en el que se itera una cantidad dada de veces la misma aplicación de las compuertas O y D. Un resultado bastante sencillo de probar es que estas compuertas se pueden construir exactamente utilizando únicamente una cantidad polinómica, en la cantidad de qubits, de compuertas del conjunto discreto y una cantidad lineal de ancillas. Lo interesante de este resultado, es que si se parte de una superposición uniforme de los estados de la base computacional (estados discretos) todos los estados intermedios de la evolución del algoritmo son estados del conjunto de estados discretos con coeficientes enteros E.

Una prueba más compleja, pero que arroja resultados novedosos respecto a la interpretación del algoritmo de Grover bajo el paradigma del modelo discreto, es que en cada iteración (aplicación de la compuerta $Gr = DO$) los estados suben de nivel de refinación como fueron definidos en le sección 4.3.2. Este resultado reafirma dos importantes hechos del algoritmo de Grover. El primero es que no es un algoritmo cíclico, los estados nunca se repiten más halla de su comportamiento pseudo cíclico y lo segundo es que la solución nunca será exacta (salvo en casos puntuales) ya que un estado de la base computacional pertenece siempre al conjunto F_0.

Implementación del operador Gr de Grover

Implementación de O

Como paso inicial se supondrá que el target es el elemento $|M\rangle$ de la base computacional, $|M\rangle = |11111\ldots1\rangle$. En este caso se tiene que $O = I_d - 2|M\rangle\langle M|$. Este operador tiene como valor propio -1 con el vector $|M\rangle$ como vector propio asociado y valor propio 1 con todos los restantes vectores de la base computacional como vectores propios.

$$O|j\rangle = (I_d - 2|M\rangle\langle M|)|j\rangle = I_d|j\rangle - 2|M\rangle\langle M|j\rangle = \begin{cases} |j\rangle \text{ si } j \neq M \\ -|j\rangle \text{ si } j = M \end{cases}$$

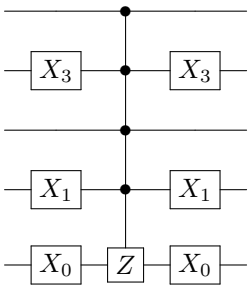
En este caso O representa la misma transformación que $\Lambda^{n-1}(Z)$. Si los primeros $M-1$ *qubits* son $|1\rangle$ aplica la compuerta Z al último *qubit*. Como $Z|0\rangle = |0\rangle$ y $Z|1\rangle = -|1\rangle$ en definitiva implementa O: multiplica por la fase -1 solo al vector $|11111\ldots1\rangle = |M\rangle$ y devuelve los demás inalterados.

Como se puede ver en la sección 4.2 la compuerta $\Lambda^{n-1}(Z)$ es fácilmente implementable teniendo en cuenta la igualdad $HXH = Z$ y la compuerta $\Lambda^{n-1}(X)$, que se implementa utilizando unicamente $T_{i,p,q}$ y un qubit auxiliar (teorema 3.1.4). Por tanto, O se puede implementar utilizando una cantidad finita de compuertas del conjunto de compuertas del modelo $\{G, H\}$.

Es posible generalizar esta construcción para cuando $|t\rangle$ no es $|M\rangle$. Dado un estado cualquiera de la base computacional $|j\rangle$ es fácil llevarlo al estado $|M\rangle$. Para esto basta con aplicarle la compuerta X_i $\forall i : c_i^j = 0$. Si se quiere deshacer el cambio basta con aplicar las compuertas X_i a los mismos *qubits* a los cuales se les aplicó.

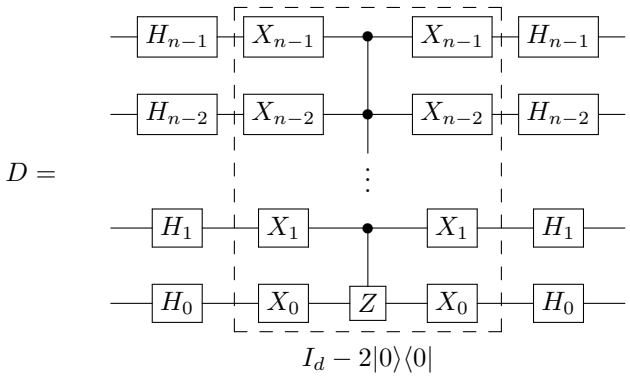
Entonces una forma general de construir $O = I_d - 2\,|t\rangle\,\langle t|$ es llevar el estado $|t\rangle$ al estado $|M\rangle$, aplicar la compuerta $\Lambda^{n-1}(Z)$ y finalmente deshacer el camino de $|M\rangle$ a $|t\rangle$. A modo de ejemplo tomando $n = 5$, se quiere implementar $O = I_d - 2\,|20\rangle\,\langle 20|$. Viendo que 20 en binario es 10100 se puede construir como sigue:

$O =$



Implementación de D

Para implementar la compuerta D del algoritmo de Grover basta observar que $D = I_d - 2\left|s\right\rangle\left\langle s\right| = H^{\otimes n}(I_d - 2\left|0\right\rangle\left\langle 0\right|)H^{\otimes n}$. Este resultado conjunto con la construcción dada anteriormente de $O = I_d - 2\left|0\right\rangle\left\langle 0\right|$ resuelven el problema:



7.3.3. Crecimiento del nivel de refinamiento y el algoritmo de Grover.

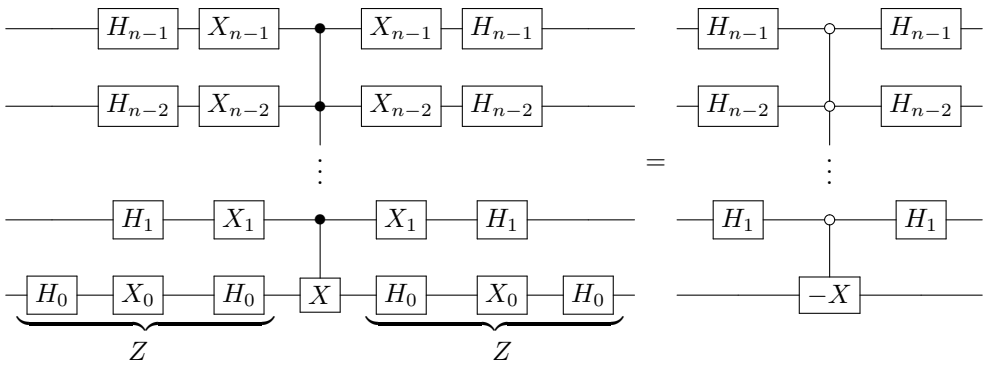
Como las compuertas pueden crearse exactamente utilizando únicamente compuertas del conjunto discreto, los estados de la evolución de Grover serán parte del conjunto de estados E (estados del modelo discreto de coeficientes enteros). Esto permite reinterpretar el funcionamiento del algoritmo de Grover en función de este modelo. La cantidad de pasos que se da en el algoritmo está directamente relacionado con el nivel de refinamiento F_k que se alcanza en los estados.

Se probará que en un sistema de n *qubits*, por cada aplicación del operador de Grover (DO), si el estado inicial está en el nivel F_k, el estado resultante estará en el nivel F_{k+2n-4}. Una aplicación de Grover aumenta el refinamiento del modelo discreto una cantidad $2n-4$.

Si se inspecciona los resultados de (7.3.2) es claro que el operador O no cambiará el nivel de refinamiento del estado. Respecto al D (ver 7.3.3), en el cual intervienen $2n$ compuertas Hadamard, a priori no es claro que todas ellas suban niveles, y de hecho no lo hacen.

Para investigar como evoluciona el estado inicial al aplicarle sucesivamente el operador de Grover, es conveniente simplificar al máximo el número de compuertas que se utilizarán para su construcción. Conviene observar entonces que en la construcción de D, se pueden simplificar algunas compuertas.

Teniendo en cuenta que $\Lambda^{n-1}(Z) = H_0\Lambda^{n-1}(X)H_0$ y las igualdades $HXH = Z$ y $ZXZ = -X$, la compuerta D se puede simplificar como sigue:



Igualmente siguen quedando $2n-2$ compuertas de Hadamard, pero es más claro ahora como actúa D. $\Lambda^{n-1}(-X)$ aplica una compuerta X al *qubit* menos significativo y lo multiplica por la fase -1 cuando el resto de los *qubits* son $|0\rangle$ (debido a esto el control aparece como un circulo no lleno en el circuito).

Para hacer la demostración de que este algoritmo siempre hace subir $2n-4$ niveles por aplicación respecto al estado previo, se tomará como target el estado $|000...0\rangle$ que se notará $|0\rangle^{\otimes}$. La demostración para el caso cuando se toma otro target es completamente análoga.

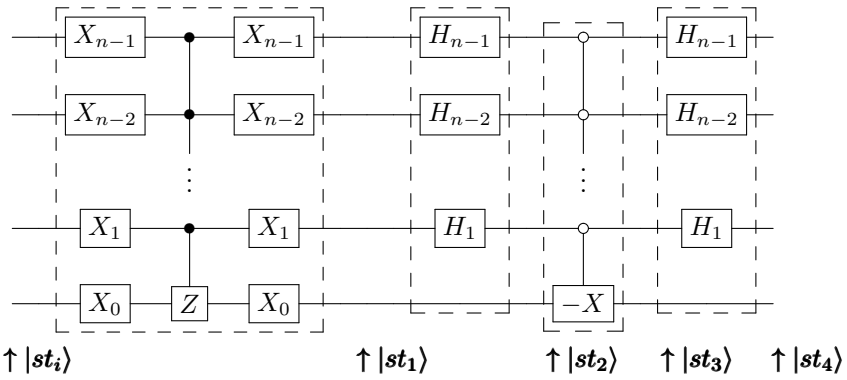
Primeramenta se estudiará cómo evoluciona el estado inicial al aplicarle una vez el algoritmo de Grover, para luego tomando como base este paso, por inducción demostrar los pasos sucesivos.

Primer paso de Grover.

El estado inicial de Grover es la superposición uniforme de todos los estados de la base computacional:

$$|st_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=1}^{2^n-1} |i\rangle$$

Para estudiar su evolución se estudiarán cuatro etapas intermedias en una aplicación completa de Grover, como se muestra a continuación:



Etapa 1. Al aplicar O a $|st_i\rangle$ se obtiene $|st_1\rangle$:

$$|st_1\rangle = O|st_i\rangle = (I_d - 2|0\rangle^{\otimes n}\langle 0|^{\otimes n})\frac{1}{\sqrt{2^n}} \sum_{i=1}^{2^n-1} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=1}^{2^n-1} |i\rangle - \frac{2}{\sqrt{2^n}}|0\rangle^{\otimes n}$$

Por un lado

$$\frac{1}{\sqrt{2^n}} \sum_{i=1}^{2^n-1} |i\rangle = \underbrace{|+\rangle \otimes \ldots \otimes |+\rangle}_{n \text{ veces}} = |+\rangle^{\otimes n}$$

y por otro se tiene que

$$\frac{2}{\sqrt{2^n}}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^{n-2}}}|0\rangle^{\otimes n}$$

Por tanto

$$|st_1\rangle = |+\rangle^{\otimes n} - \frac{1}{\sqrt{2^{n-2}}}|0\rangle^{\otimes n}$$

Etapa 2. Luego si se denota $H_{n-1} \otimes H_{n-2} \otimes \ldots \otimes H_1 \otimes I_d = H^{\otimes n-1} \otimes I_d$ se tiene que:

$$|st_2\rangle = H^{\otimes n-1} \otimes I_d |st_1\rangle = H^{\otimes n-1} \otimes I_d \left(|+\rangle^{\otimes n} - \frac{1}{\sqrt{2}^{n-2}} |0\rangle^{\otimes n} \right) =$$

$$= (H|+\rangle)^{\otimes n-1}|+\rangle - \frac{1}{\sqrt{2}^{n-2}} (H|0\rangle)^{\otimes n-1}|0\rangle = |0\rangle^{\otimes n-1}|+\rangle - \frac{1}{\sqrt{2}^{n-2}}|+\rangle^{\otimes n-1}|0\rangle$$

Luego

$$|st_2\rangle = |0\rangle^{\otimes n-1} \frac{|0\rangle + |1\rangle}{\sqrt{2}} - \frac{1}{\sqrt{2}^{n-2}}|+\rangle^{\otimes n-1}|0\rangle =$$

$$= \frac{1}{\sqrt{2}}|0\rangle^{\otimes n} + \frac{1}{\sqrt{2}}|0\rangle^{\otimes n-1}|1\rangle - \frac{1}{\sqrt{2}^{n-2}}|+\rangle^{\otimes n-1}|0\rangle$$

Observando que

$$|+\rangle^{\otimes n-1} = \frac{1}{\sqrt{2}^{n-1}} \sum_{i=1}^{2^{n-1}-1} |i\rangle$$

El estado $|+\rangle^{\otimes n-1}|0\rangle$ es una superposición de los estados de la base computacional de la forma $|q_{n-1}\rangle|q_{n-2}\rangle \ldots |q_1\rangle|0\rangle$ ponderados uniformemente por $\frac{1}{\sqrt{2}^{n-1}}$ donde $q_j = 0$ ó $q_j = 1$. Por lo cual esta superposición también contiene al termino $|0\rangle^{\otimes n}$.

El estado $|st_2\rangle$ será entonces una superposición de los estados de la base computacional con coeficientes dados como:

$$\text{Coef } |0\rangle^{\otimes n} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}^{n-2}} \frac{1}{\sqrt{2}^{n-1}} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}^{2n-3}}$$

$$\text{Coef } |0\rangle^{\otimes n-1}|1\rangle = \frac{1}{\sqrt{2}}$$

$$\text{Coef } |q_{n-1}\rangle \ldots |q_1\rangle|0\rangle = -\frac{1}{\sqrt{2}^{2n-3}} \qquad \text{(con al menos un } q_j \neq 0)$$

$$\text{Coef restantes} = 0$$

Etapa 3. El estado $|st_3\rangle$ se obtiene de aplicar $\Lambda^{n-1}(-X)$ al estado $|st_2\rangle$ cuando los primeros $n-1$ *qubits* son 0. Por tanto solo afecta a los estados de la base computacional $|0\rangle^{\otimes n}$ y $|\mathbf{0}_{n_1}\rangle|1\rangle$, intercambiando los coeficientes de ellos y multiplicándolos por una fase -1. Por tanto si

$$|st_2\rangle = \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}^{2n-3}} \right) |0\rangle^{\otimes n} + \frac{1}{\sqrt{2}}|0\rangle^{\otimes n-1}|1\rangle -$$
$$\frac{1}{\sqrt{2}^{2n-3}} \left(|q_{n-1}\rangle \ldots |q_1\rangle|0\rangle - |0\rangle^{\otimes n} \right)$$

Entonces $|st_3\rangle$ será:

$$|st_3\rangle = -\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}^{2n-3}} \right) |0\rangle^{\otimes n-1}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle^{\otimes n} -$$
$$\frac{1}{\sqrt{2}^{2n-3}} \left(|q_{n-1}\rangle \ldots |q_1\rangle|0\rangle - |0\rangle^{\otimes n} \right)$$

y reordenando los términos queda

$$|st_3\rangle = -|0\rangle^{\otimes n-1} \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}^{2n-4}}|0\rangle^{\otimes n-1} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$- \frac{1}{\sqrt{2}^{2n-3}} \left(|q_{n-1}\rangle \ldots |q_1\rangle|0\rangle \right)$$

$$= \left(-1 + \frac{1}{\sqrt{2}^{2n-4}}\right)|0\rangle^{\otimes n-1}|+\rangle - \frac{1}{\sqrt{2}^{2n-3}}\left(|q_{n-1}\rangle \dots |q_1\rangle|0\rangle\right)$$

$$= \left(-1 + \frac{1}{\sqrt{2}^{2n-4}}\right)|0\rangle^{\otimes n-1}|+\rangle - \frac{1}{\sqrt{2}^{n-2}}\left(\frac{1}{\sqrt{2}^{n-1}}\sum_{i=1}^{2^{n-1}-1}|i\rangle\right)|0\rangle$$

finalmente

$$|st_3\rangle = \left(-1 + \frac{1}{2^{n-2}}\right)|0\rangle^{\otimes n-1}|+\rangle - \frac{1}{\sqrt{2}^{n-2}}\left(|+\rangle^{\otimes n-1}\right)|0\rangle$$

Etapa 4. Escrito de esta manera $|st_3\rangle$ facilita notoriamente la obtención de $|st_4\rangle$:

$$|st_4\rangle = H^{\otimes n-1}|st_3\rangle =$$

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

$$\left(-1 + \frac{1}{2^{n-2}}\right)|+\rangle^{\otimes n-1}|+\rangle - \frac{1}{\sqrt{2}^{n-2}}\left(|0\rangle^{\otimes n-1}\right)|0\rangle =$$

$$\left(-1 + \frac{1}{2^{n-2}}\right)|+\rangle^{\otimes n} - \frac{1}{\sqrt{2}^{n-2}}|0\rangle^{\otimes n}$$

finalmente

$$|st_4\rangle = \left(-1 + \frac{1}{2^{n-2}}\right)|st_i\rangle - \frac{1}{\sqrt{2}^{n-2}}|0\rangle^{\otimes n}$$

Observación 7.3.1. Es interesante observar que $|st_2\rangle$ pertenece al nivel $2n-3$. Para ver esto basta comprobar que los coeficientes del estado por el factor $\sqrt{2}^{2n-3}$ son todos enteros y alguno es impar:

$$\begin{aligned}
(\text{Coef } |0\rangle^{\otimes n})\sqrt{2}^{2n-3} &= \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}^{2n-3}}\right)\sqrt{2}^{2n-3} \\
&= \sqrt{2}^{2n-4} - 1 = 2^{n-2} - 1 \\
(\text{Coef } |0\rangle^{\otimes n-1}|1\rangle)\sqrt{2}^{2n-3} &= \frac{1}{\sqrt{2}}\sqrt{2}^{2n-3} = 2^{n-2} \\
(\text{Coef } |q_{n-1}\rangle \dots |q_1\rangle|0\rangle)\sqrt{2}^{2n-3} &= -1 \qquad (\text{con al menos } q_j \neq 0)
\end{aligned}$$

Una explicación sencilla es que como todos los coeficientes de $|st_1\rangle$ son 1 o -1 al ser multiplicados por el factor $\sqrt{2}^n$, todos impares, una de las $n-1$ aplicaciones de H baja un nivel, mientras que todas las restantes suben un nivel, quedando el estado resultante en el nivel $n+n-1-2$.

El estado $|st_4\rangle$ es el estado resultante de aplicar un paso de Grover completo por esto lo llamaremos $|st_f\rangle$.

$$OD|st_i\rangle = |st_f\rangle = \left(-1 + \frac{1}{2^{n-2}}\right)|st_i\rangle - \frac{1}{\sqrt{2}^{n-2}}|0\rangle^{\otimes n} \tag{7.4}$$

Observación 7.3.2. $|st_f\rangle$ se encuentra en el nivel $3n-4$. Para ver esto basta observar que tiene solo dos tipos de coeficientes:

$$\begin{aligned}
\text{Coef } |0\rangle^{\otimes n} &= \frac{1}{\sqrt{2}^n}\left(-1 + \frac{1}{2^{n-2}}\right) - \frac{1}{\sqrt{2}^{n-2}} \\
\text{Coef restantes} &= \frac{1}{\sqrt{2}^n}\left(-1 + \frac{1}{2^{n-2}}\right)
\end{aligned}$$

Si multiplicamos a estos por $\sqrt{2}^{3n-4}$ obtenemos:

$$\begin{aligned}
(\text{Coef } |0\rangle^{\otimes n})\sqrt{2}^{3n-4} &= \left(\frac{1}{\sqrt{2}^{n}}\left(-1+\frac{1}{2^{n-2}}\right)-\frac{1}{\sqrt{2}^{n-2}}\right)\sqrt{2}^{3n-4} \\
&= \left(-\sqrt{2}^{2n-4}+\frac{\sqrt{2}^{2n-4}}{2^{n-2}}\right)-\sqrt{2}^{2n-2} \\
&= \underbrace{\underbrace{\left(-2^{n-2}+1\right)}_{\text{impar}}-\underbrace{2^{n-1}}_{\text{par}}}_{impar} \\
(\text{Coef restantes})\sqrt{2}^{3n-4} &= \frac{1}{\sqrt{2}^{n}}\left(-1+\frac{1}{2^{n-2}}\right)\sqrt{2}^{3n-4} \\
&= \underbrace{\left(-2^{n-2}+1\right)}_{\text{impar}}
\end{aligned}$$

Por tanto el estado final al aplicar un paso de Grover efectivamente está en el $3n-4$, esto quierer decir que el $|st_f\rangle$ subió $2n-4$ respecto a $|st_i\rangle$, ya que este estaba en el nivel n. Además los coeficientes que se obtienen son todos impares e iguales menos el estado target que tiene una probabilidad mayor que a los demás.

Resta demostrar que para los pasos sucesivos de Grover este comportamiento se mantiene.

Paso genérico de Grover.

Si se quisiera aplicar de nuevo Grover, habría que aplicar de nuevo todo lo hecho a $|st_f\rangle$ por lo que utilizando la ecuación (7.4):

$$\begin{aligned}
|st_{f2}\rangle = DO|st_f\rangle = DO\left[\left(-1+\frac{1}{2^{n-2}}\right)|st_i\rangle-\frac{1}{\sqrt{2}^{n-2}}|0\rangle^{\otimes n}\right] \\
= \left(-1+\frac{1}{2^{n-2}}\right)DO|st_i\rangle-\frac{1}{\sqrt{2}^{n-2}}DO|0\rangle^{\otimes n}
\end{aligned}$$

Ahora bien la evolución de $DO|st_i\rangle$ ya se la calculó en la parte anterior, por lo cual si se conoce $DO|0\rangle^{\otimes n}$ se conocerá los coeficientes del siguiente paso de Grover.

La evolución del estado $|0\rangle^{\otimes n}$ al aplicarle el algoritmo de Grover se puede obtener como sigue:

$$\begin{aligned}
DO|0\rangle^{\otimes n} &= D(I_d-2|0\rangle^{\otimes n}\langle 0|^{\otimes n})|0\rangle^{\otimes n} = D(-|0\rangle^{\otimes n}) \\
&= H^{\otimes n-1}\Lambda^{n-1}(-X)H^{\otimes n-1}(-|0\rangle^{\otimes n}) \\
&= H^{\otimes n-1}\Lambda^{n-1}(-X)(-|+\rangle^{\otimes n-1}|0\rangle) \\
&= H^{\otimes n-1}\left(-|+\rangle^{\otimes n-1}|0\rangle+\frac{1}{\sqrt{2}^{n-1}}|0\rangle^{\otimes n}+\frac{1}{\sqrt{2}^{n-1}}|0\rangle^{\otimes n-1}|1\rangle\right) \\
&= H^{\otimes n-1}\left(-|+\rangle^{\otimes n-1}|0\rangle+\frac{1}{\sqrt{2}^{n-2}}|0\rangle^{\otimes n-1}|+\rangle\right) \\
&= -|0\rangle^{\otimes n-1}|0\rangle+\frac{1}{\sqrt{2}^{n-2}}|+\rangle^{\otimes n-1}|+\rangle = -|0\rangle^{\otimes n}+\frac{1}{\sqrt{2}^{n-2}}|+\rangle^{\otimes n} \\
&= -|0\rangle^{\otimes n}+\frac{1}{\sqrt{2}^{n-2}}|st_i\rangle
\end{aligned} \tag{7.5}$$

Observación 7.3.3. Tanto $DO|0\rangle^{\otimes n}$ como $DO|st_i\rangle^{\otimes n}$ (ecuaciones (7.5) y (7.4) respectivamente) son combinación lineal de $\{|st_i\rangle, |0\rangle^{\otimes n}\}$ y por tanto puede obtenerse una forma recursiva de obtener la evolución para el paso *k-ésimo* de Grover.

Si $|st_{fk}\rangle$ es el estado que se obtiene al haber hecho k pasos de Grover este será de la forma $|st_{fk}\rangle = \zeta_1|st_i\rangle + \zeta_2|0\rangle^{\otimes n}$, y se puede a partir de él calcular $|st_{fk+1}\rangle$ como $|st_{fk+1}\rangle = DO|st_{fk}\rangle$ y utilizando que

$$\begin{aligned} DO|st_i\rangle &= \alpha|st_i\rangle + \beta|0\rangle^{\otimes n} \\ DO|0\rangle^{\otimes n} &= -\beta|st_i\rangle - |0\rangle^{\otimes n} \end{aligned} \tag{7.6}$$

con

$$\alpha = -1 + \frac{1}{2^{n-2}} \quad \text{y} \quad \beta = \frac{1}{\sqrt{2}^{n-2}}$$

se obtiene que:

$$\begin{aligned} |st_{fk+1}\rangle &= \zeta_1(\alpha|st_i\rangle + \beta|0\rangle^{\otimes n}) + \zeta_2(-\beta|st_i\rangle - |0\rangle^{\otimes n}) \\ &= (\alpha\zeta_1 - \beta\zeta_2)|st_i\rangle + (\beta\zeta_1 - \zeta_2)|0\rangle^{\otimes n} \end{aligned} \tag{7.7}$$

Se demostrará por inducción completa que $|st_{fk}\rangle$ está en el nivel $n + k(2n-4)$, es decir que aplicar *k-veces* el operador de grover el nivel de discretización sube $k(2n-4)$ niveles.

Proposición 7.3.1. *$|st_{fk}\rangle$ es el estado que se obtiene en el k-ésimo paso de Grover, es de la forma $\zeta_1|st_i\rangle + \zeta_2|0\rangle^{\otimes n}$, esta en el nivel $n+k(2n-4)$, todos sus coeficientes multiplicados por $\sqrt{2}^{n+k(2n-4)}$ son enteros impares y $\zeta_2\sqrt{2}^{n+k(2n-4)}$ en un número entero de la forma $2^m C$ con $m > 1$ y $C \in \mathbb{Z}$.*

Demostración. ▪ Caso Base:

El caso base se toma para $k = 1$. En esta caso ya se probó que

$$|st_{f1}\rangle = \left(-1 + \frac{1}{2^{n-2}}\right)|st_i\rangle - \frac{1}{\sqrt{2}^{n-2}}|0\rangle^{\otimes n}$$

y por tanto $|st_{f1}\rangle$ esta en el nivel $n+2n-4$ y sus coeficientes son todos impares. Falta verificar que $\zeta_2\sqrt{2}^{3n-4}$ es de la forma $2^m C$ con $m > 1$ y $C \in \mathbb{Z}$:

$$\zeta_2\sqrt{2}^{3n-4} = \frac{1}{\sqrt{2}^{n-2}}\sqrt{2}^{3n-4} = \sqrt{2}^{2n-2} = 2^{n-1}$$

y como se toma $n \geq 3$ se cumple la hipótesis.

- Hipótesis inductiva:
  $|st_{fk}\rangle = \zeta_1|st_i\rangle + \zeta_2|0\rangle^{\otimes n}$, esta en el nivel $n + k(2n-4)$, todos sus coeficientes multiplicados por $\sqrt{2}^{n+k(2n-4)}$ son enteros impares y $\zeta_2\sqrt{2}^{n+k(2n-4)}$ en un número entero de la forma $2^m C$ con $m > 1$ y $C \in \mathbb{Z}$
- Tesis inductiva:
  $|st_{fk+1}\rangle = \hat{\zeta_1}|st_i\rangle + \hat{\zeta_2}|0\rangle^{\otimes n}$, está en el nivel $n + (k+1)(2n-4)$, todos sus coeficientes multiplicados por $\sqrt{2}^{n+(k+1)(2n-4)}$ son enteros impares y
  $\hat{\zeta_2}\sqrt{2}^{n+(k+1)(2n-4)}$ en un número entero de la forma $2^m C$ con $m > 1$ y $C \in \mathbb{Z}$
- Prueba:
  De la ecuación (7.7) se sabe que

$$|st_{fk+1}\rangle = (\alpha\zeta_1 - \beta\zeta_2)|st_i\rangle + (\beta\zeta_1 - \zeta_2)|0\rangle^{\otimes n}$$

por tanto

$$\hat{\zeta_1} = \alpha\zeta_1 - \beta\zeta_2$$
$$\hat{\zeta_2} = \beta\zeta_1 - \zeta_2$$

Se empezará por probar que $\hat{\zeta_2}\sqrt{2}^{n+(k+1)(2n-4)}$ en un número entero de la forma $2^m C$ con $m > 1$ y $C \in \mathbb{Z}$. Para ver esto se tiene que:

$$\hat{\zeta_2}\sqrt{2}^{n+(k+1)(2n-4)} = (\beta\zeta_1 - \zeta_2)\sqrt{2}^{n+k(2n-4)}\sqrt{2}^{(2n-4)}$$

de lo que haciendo cuentas se obtiene:

$$\frac{\sqrt{2}^{(2n-4)}}{\sqrt{2}^{n-2}}\left(\zeta_1\sqrt{2}^{n+k(2n-4)}\right) - (\zeta_2\sqrt{2}^{n+k(2n-4)})\sqrt{2}^{(2n-4)}$$

$$= \sqrt{2}^{(n-2)}\sqrt{2}^{n}\left(\frac{\zeta_1\sqrt{2}^{n+k(2n-4)}}{\sqrt{2}^{n}}\right) - (\zeta_2\sqrt{2}^{n+k(2n-4)})2^{(n-2)}$$

Por hipótesis inductiva $\frac{\zeta_1\sqrt{2}^{n+k(2n-4)}}{\sqrt{2}^{n}}$ es un número entero al que llamaremos P y $\zeta_2\sqrt{2}^{n+k(2n-4)}$ es de la forma $2^m C$, con $m > 1$, por tanto se tiene:

$$= \sqrt{2}^{(2n-2)}P - 2^m C 2^{n-2} = 2^{n-1}P - 2^{m-1}C2^{n-1} = 2^{n-1}\underbrace{(P - 2^{m-1}C)}_{\text{entero}}$$

Como $n \geq 3$ se cumple lo que se quería probar.

Finalmente se probará que todos los coeficientes de $|st_{fk+1}\rangle$ multiplicados por $\sqrt{2}^{n+(k+1)(2n-4)}$ son enteros impares.

Como

$$|st_{fk+1}\rangle = (\alpha\zeta_1 - \beta\zeta_2)|st_i\rangle + (\beta\zeta_1 - \zeta_2)|0\rangle^{\otimes n}$$

se tienen dos tipos de coeficientes diferentes:

$$\text{Coef } |0\rangle^{\otimes n} = (\beta\zeta_1 - \zeta_2) + \frac{\alpha\zeta_1 - \beta\zeta_2}{\sqrt{2}^n}$$

$$\text{Coef restantes} = \frac{\alpha\zeta_1 - \beta\zeta_2}{\sqrt{2}^n}$$

Se empezará por probar que $\frac{\alpha\zeta_1-\beta\zeta_2}{\sqrt{2}^n}\sqrt{2}^{n+(k+1)(2n-4)}$ es un entero impar:

$$\left(-1 + \frac{1}{2^{n-2}}\right)\left(\frac{\zeta_1\sqrt{2}^{n+k(2n-4)}}{\sqrt{2}^n}\right)\sqrt{2}^{2n-4} - \frac{\zeta_2\sqrt{2}^{n+k(2n-4)}}{\sqrt{2}^{n-2}\sqrt{2}^n}\sqrt{2}^{2n-4}$$

$$= \left(-2^{n-2}+1\right)\left(\frac{\zeta_1\sqrt{2}^{n+k(2n-4)}}{\sqrt{2}^n}\right) - (\zeta_2\sqrt{2}^{n+k(2n-4)})\frac{1}{2}$$

Luego utilizando de nuevo la hipótesis inductivas se tiene que:

$$= \left(-2^{n-2}+1\right)P - 2^m C\frac{1}{2} = \underbrace{\underbrace{\left(-2^{n-2}+1\right)}_{impar}\underbrace{P}_{impar}}_{\text{impar}} - \underbrace{\underbrace{2^{m-1}}_{m>1}C}_{par}$$

por tanto el coeficiente es impar.

Finalmente el coeficiente en $|0\rangle^{\otimes n}$ multiplicado por $\sqrt{2}^{n+(k+1)(2n-4)}$ también es impar ya que se obtiene como la suma del coeficiente de los restantes términos, que se probó que por el factor de normalización es impar sumado al termino $\hat{\zeta_2}\sqrt{2}^{n+(k+1)(2n-4)}$ que ya se probó también que es par, siendo entonces esta suma impar.

□

7.4. Interpretación

Para demostrar cómo crecen los niveles de discretización se llegó a que la evolución del estado obtenido luego de k pasos de Grover siempre está en el subespacio generado por el target y por el ortogonal a él, lo que acompaña a la interpretación geométrica del algoritmo como una doble reflexión en el hiperplano formado por ambos estados.

Por otro lado se mostró que el refinamiento del estado crece linealmente con la cantidad de iteraciones o pasos de Grover. El coeficiente de crecimiento depende de la cantidad de *qubits* del sistema que se considere, y es: $2n - 4$. Esto se resume en la figura 7.2.

Una conclusión que se puede extraer de esto, es que el algoritmo de Grover no es cíclico. Al evolucionar (aumentar el número de pasos), los estados resultantes crecen estrictamente respecto a los anteriores. Esto implica que siempre estarán en un nivel F_k (utilizando la notación de la propiedad 4.3.2) diferente. Desde que los F_k no comparten estados, esta claro que nunca se repetirán los estados.

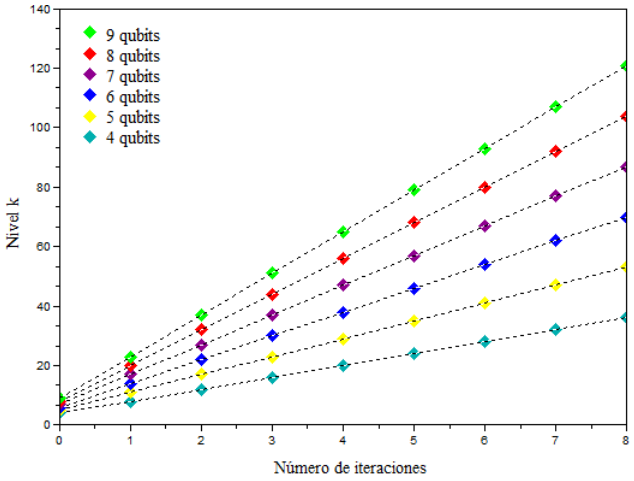


Figura 7.2: Crecimiento del nivel de refinamiento en función del número de iteraciones del algoritmo de Grover para distintos números de qubits.

De aquí que es interesante estudiar qué pasa cuando se toma la cantidad de iteraciones óptima de Grover, $p_0 = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$. Para p_0 iteraciones el nivel de refinamiento varía según la cantidad de qubits que se utilice. De hecho se puede obtener de forma exacta como $k = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor (2n-4)$. Resultado que se ilustra en la figura 7.3.

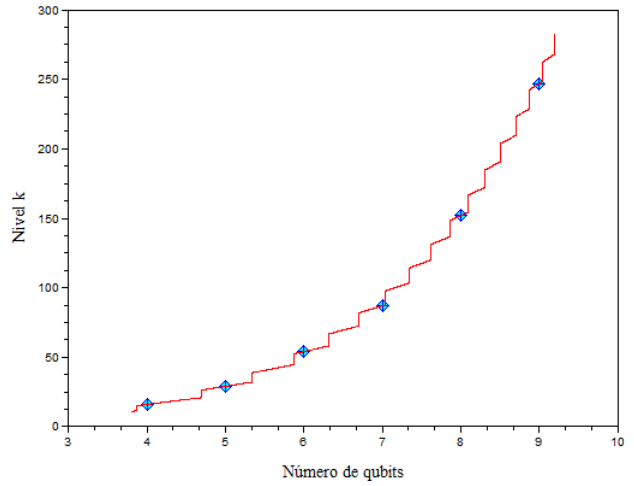


Figura 7.3: Nivel de refinamiento en la iteración óptima de Grover según la cantidad de qubits utilizados.

Parte IV

Conclusiones

Capítulo 8

Conclusiones

Esta tesis aborda un campo de estudio específico dentro del paradigma de la computación cuántica. Dada la computación cuántica basada en compuertas, se centra en el estudio de los modelos discretos, es decir, cómo se modifica el modelo de computación cuántica cuando se toma un conjunto finito de compuertas.

Para esto, en la parte I, se introducen las nociones básicas del modelo de computación cuántica, dejando el formalismo matemático que los sustenta para el Apéndice A. Seguidamente, se desarrollan brevemente los principales resultados del proceso de discretización de las compuertas, pasando primero por un conjunto infinito de compuertas para luego dar lugar a los conjuntos finitos. Los resultados expuestos son fundamentales para comprender los aportes novedosos de esta tesis que se exponen en la parte II.

El principal resultado de esta investigación es la presentación de un modelo de computación cuántica discreta conformado por únicamente dos compuertas $\{H, G\}$. Una característica excepcional del modelo es que los coeficientes de los estados generados a partir de las dos compuertas componentes y los estados de la base computacional son números complejos con coeficientes enteros, excepto por un factor de $\sqrt{2}^p$, lo que lo hace especialmente interesante desde una perspectiva teórica y práctica. Es en este sentido que se afirma que el modelo es sumamente simple, pero a pesar de su simplicidad, este modelo ha demostrado ser capaz de generar estados que cumplen con las principales características de la computación cuántica, como la superposición y el entrelazamiento.

Se ha demostrado que los estados de este modelo pueden clasificarse en niveles dependiendo del parámetro p, que representan el grado de refinamiento de los estados. Esto es, a medida que p crece, el conjunto de estados discretos se vuelve cada vez más denso, lo que permite hacer mejores aproximaciones a estados que no están dentro del modelo. Para un estado discreto de coeficientes enteros cualesquiera, se demuestra cómo puede ser obtenido a partir de las compuertas componentes.

Respecto a las compuertas que pueden obtenerse dentro del modelo, se define lo que es una compuerta cuántica discreta como aquella que es invariante respecto al conjunto de estados cuánticos discretos con coeficientes enteros. Para el caso de dos qubits, se da un procedimiento exacto de cómo descomponer estas compuertas discretas como producto de las dos compuertas elementales y derivados de ellas. Para mayores dimensiones, este resultado no es extendible de manera inmediata, pero mantenemos firmemente la convicción de que existe un procedimiento análogo para la descomposi -ción de cualquier compuerta discreta como producto de las dos compuertas elementales que conforman el modelo presentado. Es un trabajo futuro lograr esta descomposición para cualqueir dimensión, y de ser posible minimizar el número de compuertas necesario para hacerlo.

En un segundo enfoque sobre los estados discretos de coeficientes enteros, se exploraron las propiedades matemáticas del espacio de vectores resultantes del modelo de computación cuántica discreta. Se demostró que, para el espacio de cuatro qubits, es posible completar una base de vectores propios utilizando un conjunto ortonormal de vectores pertenecientes al modelo discreto. La versión ortogonal del teorema de los cuatro cuadrados de Lagrange está estrechamente relacionada con el modelo de computación cuántica discreta. Los resultados obtenidos en el análisis del problema propuesto, así como en las generalizaciones incluidas en la sección 5.4, establecen propiedades clave de este modelo. La complejidad de la prueba presentada en la sección B muestra claramente la dificultad del problema estudiado y su conexión con la teoría de números, la geometría de números y la teoría de retículos. Además, se realizaron conjeturas para dimensiones superiores, lo que sugiere posibles aplicaciones en sistemas cuánticos de mayor complejidad. Varias de las conjeturas presentadas en este trabajo fueron respondidas afirmativamente en un trabajo [130] posterior a los publicados durante esta tesis, que recoge gran parte de lo expuesto aquí.

Finalmente, en la parte III, se analizó la aplicabilidad del modelo en el contexto de la información cuántica. Se encontraron conexiones significativas entre este modelo y protocolos importantes, como el de teleportación y el código superdenso. El poder representar algunos de los estados de máximo entrelazamiento como estados discretos del modelo permitió el desarrollo completo de estos protocolos dentro de este marco, lo que podría tener implicaciones prácticas en la implementación de sistemas de comunicación cuántica.

Además, se examinaron los algoritmos cuánticos más relevantes y su relación con el modelo discreto. Mientras que algunos de estos algoritmos pueden ser implementados exactamente en el modelo, otros requieren aproximaciones. Por ejemplo, el algoritmo de Shor, crucial para la factorización de números enteros, debe aproximarse dentro de este modelo, lo que sugiere desafíos y oportunidades para futuras investigaciones. Por otro lado, el algoritmo de búsqueda de Grover puede implementarse exactamente utilizando las compuertas del modelo, lo que brinda una nueva forma de entender su funcionamiento.

A modo de cierre, dejamos unas reflexiones finales que este trabajo ha suscitado. El modelo de computación cuántica discreta, e indirectamente los resultados del presente artículo, tendrán una gran influencia en la teoría de la información cuántica y en la física cuántica. Los investigadores en computación cuántica han aprendido que el control de errores es un problema enormemente complejo, y han abandonado en su mayoría el proyecto de construir un ordenador cuántico para trabajar en la simulación cuántica.

Creemos que, con la física cuántica actual, la computación cuántica no es escalable sin sobrecostos tecnológicos. La evolución unitaria de los sistemas cuánticos impide el diseño de sistemas autocorrecti -vos basados en cuencas de atracción. Estos sistemas, que incluyen la electrónica digital, transforman automáticamente cualquier estado de la cuenca de atracción en el estado sin error que ésta representa. Obviamente, la física cuántica actual no permite hacer esto. Y los códigos cuánticos de corrección de errores no verifican ninguna de las dos hipótesis clave con las que funcionan los códigos clásicos de corrección de errores: todos los pequeños errores se corrigen y los circuitos de corrección no introducen nuevos errores. La decoherencia introduce errores no locales que, aunque son pequeños si los consideramos en intervalos de tiempo cortos, los códigos cuánticos de corrección de errores no son capaces de corregir.

Desde el punto de vista de la física, un ordenador cuántico universal es un sistema que puede evolucionar desde el estado $|0\ldots0\rangle$ de entropía cero a cualquier estado ($n-$qubit final) siguiendo cualquier camino (algoritmo) y manteniendo la entropía (error) cercana a cero. Planteado así, el segundo principio de la termodinámica pone serias dudas sobre la viabilidad de la construcción de un sistema de este tipo, más aún si tenemos en cuenta también la imposibilidad de implementar una estructura autocorrectiva efectiva.

Todas estas dificultades podrían superarse si la física cuántica, de alguna manera, pudiera ser discretizada. Las limitantes sobre los soportes físicos que presentan comportamientos determinados por la física cuántica tienen una capacidad limitada de superposición y, en consecuencia, de entrelaza -miento y paralelismo, y la superación de este hecho es irreal a corto plazo. Una segunda cuantización, presumiblemente de estados cuánticos, permitiría una física con menor capacidad de superposición, entrelazamiento y paralelismo pero más fácil de controlar. Creemos que en este contexto serán importantes los modelos de computación cuántica discreta.

Apéndice A

Conceptos matemáticos

A.1. Espacios de Hilbert

Definición A.1.1. Se llamará **espacio de Hilbert** a un espacio vectorial, $\mathcal{H}$, defiido sobre el cuerpo de los complejos, con producto interno, que es completo bajo la norma inducida del producto interno.

Definición A.1.2. Se llama **producto interno** a una función $(,) : \mathcal{H} \otimes \mathcal{H} \to \mathbb{C}$ que cumple con las siguientes propiedades:

1. $(|u\rangle, |v\rangle) = (|v\rangle, |u\rangle)^*$, $\forall |u\rangle, |v\rangle \in \mathcal{H}$, [1]
2. $(|u\rangle, \lambda|v\rangle + |w\rangle) = \lambda(|u\rangle, |v\rangle) + (|u\rangle, |w\rangle)$, $\forall |u\rangle, |v\rangle, |w\rangle \in \mathcal{H}$ y $\forall \lambda \in \mathbb{C}$
3. $(|u\rangle, |u\rangle) \geq 0$ para todo $|u\rangle \in \mathcal{H}$, además $(|u\rangle, |u\rangle) = 0$ sii $|u\rangle = 0$.

De la propiedad 2 se deduce que el producto interno es una función lineal en la segunda componente, y de las propiedades 1 y 2 se puede deducir fácilmente que es lineal conjugado en la primera componente, esto es:

$$\left(\sum_i \lambda_i |u_i\rangle, |v\rangle\right) = \left(|v\rangle, \sum_i \lambda_i |u_i\rangle\right)^* = \sum_i \lambda_i^* \left(|v\rangle, |u_i\rangle\right)^* = \sum_i \lambda_i^* \left(|u_i\rangle, |v\rangle\right) \tag{A.1}$$

Como de aquí en adelante se trabajará siempre en espacios vectoriales del tipo $\mathbb{C}^n = \mathcal{H}$, en particular de dimensión finita, se utilizará el producto usual en $\mathbb{C}^n$:

$$(|u\rangle, |v\rangle) = \sum_i^n u_i^* v_i = |u\rangle^\dagger |v\rangle = \langle u||v\rangle = \langle u|v\rangle \tag{A.2}$$

Es aquí que se ve la potencia que tiene la notación de Dirac, ya que permite escribir de manera compacta y visual operaciones básicas. Es cierto también que al escribir $\langle u||v\rangle = \langle u|v\rangle$ se comete un pequeño abuso de notación, pero que de aquí en adelante se utilizará siempre.

[1] * nota conjugado: sea $a + bi \in \mathcal{C} \Rightarrow (a + bi)^* = a - bi$

Definición A.1.3. La función $||.|| : \mathcal{H} \to \mathbb{R}$ defiida como $|||u\rangle|| = \sqrt{\langle u|u\rangle}$, $\forall |u\rangle \in \mathcal{H}$ es la **norma inducida** por el producto interno.

Como se está trabajando con espacios vectoriales de dimensión finita el par $(\mathcal{H}, (,))$ es un espacio de Hilbert, ya que $(\mathcal{H}, ||.||)$ es un espacio vectorial normado, y todo espacio vectorial finito con la norma inducida de un producto interno es completo.

Se dice que dos vectores $|u\rangle$ y $|v\rangle$ son **ortogonales** si $\langle u|v\rangle = 0$ y se dice que un vector $|u\rangle$ es **unitario** si $|||u\rangle|| = \sqrt{\langle u|u\rangle} = 1$

Decimos que un conjunto de vectores $\{|e_1\rangle, |e_2\rangle, ..., |e_n\rangle\}$ son **ortonormales** si $\langle e_i|e_j\rangle = \delta_{ij}$, para $1 \leq i \leq n,\ 1 \leq j \leq n$. Esto implica que estos vectores son ortogonales dos a dos y que todos son unitarios.

Dado un espacio de Hilbert, $\mathcal{H}$, de dimensión n, un conjunto $\{|e_j\rangle\}_j$ de n vectores ortonormales $\{|e_1\rangle, |e_2\rangle, ..., |e_n\rangle\}$ forma una base ortonormal del mismo:

$$\text{Si} \sum_{j=1}^{n} \lambda_j |e_j\rangle = 0 \ \Rightarrow\ \forall k \in [1,n],\quad (|e_k\rangle, 0) = \left(|e_k\rangle, \sum_{j=1}^{n} \lambda_j |e_j\rangle\right) = \sum_{j=1}^{n} \lambda_j \delta_{kj} = \lambda_k = 0 \tag{A.3}$$

lo que implica que son n vectores linealmente independientes, por tanto son un base de $\mathcal{H}$. Entonces cualquier vector de $\mathcal{H}$ se puede escribir de la forma:

$$|u\rangle = \sum_{j=1}^{n} u_j |e_j\rangle \text{ con } u_j = \langle e_j|u\rangle \tag{A.4}$$

A.2. Operadores en el espacio de Hilbert

Dados dos espacios de Hilbert $\mathcal{H}_1$ y $\mathcal{H}_2$, se notará $\Lambda(\mathcal{H}_1, \mathcal{H}_2)$ al conjunto de todas las aplicaciones lineales de $\mathcal{H}_1$ a $\mathcal{H}_2$.

Sean $\{|a_i\rangle\}_{i\in[1,n]}$ y $\{|b_j\rangle\}_{j\in[1,m]}$ bases ortonormales de $\mathcal{H}_1$ y $\mathcal{H}_2$ respectivamente. Dada $T \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ es sabido que tiene una representación matricial $(t_{ji})_{1\leq j\leq m,\ 1\leq i\leq n}$ asociada a las bases$\{|a_i\rangle\}_i$ y $\{|b_j\rangle\}_j$ respectivamente, dada por

$$t_{ji} = \langle b_j|T|a_i\rangle \tag{A.5}$$

Dado $|v\rangle \in \mathcal{H}_1$ se puede escribir como $|v\rangle = \sum_i v_i|a_i\rangle = \sum_i \langle a_i|v\rangle|a_i\rangle$, de donde aplicarle T a $|v\rangle$ es hacer

$$T(v) = \sum_{i}^{n} v_i T(|a_i\rangle) = \sum_{i}^{n} v_i \sum_{j}^{m} \langle b_j|T|a_i\rangle|b_j\rangle = \sum_{i}^{n} v_i \sum_{j}^{m} t_{ji}|b_j\rangle = \sum_{j}^{m} \left(\sum_{i}^{n} t_{ji} v_i\right)|b_j\rangle \tag{A.6}$$

Haciendo una cuenta similar a la anterior no es dicícil demostrar que dados $T \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ y $S \in \Lambda(\mathcal{H}_2, \mathcal{H}_3)$ y $(t_{ji})_{ji}$ y $(s_{kj})_{kj}$ sus matrices asociadas en algunas bases de $\mathcal{H}_1$, $\mathcal{H}_2$ y $\mathcal{H}_3$ respectivamente entonces la matriz asociada al operador$(S \circ T)$ en las mismas bases de $\mathcal{H}_1$ y $\mathcal{H}_3$ es $st_{ki} = (s_{kj})(t_{ji})$, o sea, el producto de ambas matrices asociadas respectivamente.

Es por esto que en general cuando se hable de matrices de aquí en adelante es importante tener en cuenta que se estará pensando en operadores entre espacios de Hilbert. Por ejemplo a todos los endomorfismos lineales en un espacio de Hilbert, $\Lambda(\mathcal{H}, \mathcal{H})$ se los puede asociar a alguna matriz cuadrada de dimensión igual a la dimensión del espacio $\mathcal{H}$, y obviamente toda matriz cuadrada puede ser pensada como un operador de este espacio.

Definición A.2.1. Dado un operador $T \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ se defie su **operador adjunto** $T^\dagger$ como el operador de $\Lambda(\mathcal{H}_2, \mathcal{H}_1)$ que cumple

$$(|u\rangle, T|v\rangle)_{\mathcal{H}_2} = (T^\dagger|u\rangle, |v\rangle)_{\mathcal{H}_1} \quad \forall |u\rangle \in \mathcal{H}_1 \text{ y } \forall |v\rangle \in \mathcal{H}_2 \tag{A.7}$$

Este operador siempre existe y es único. Además dadas dos bases ortonormales en $\mathcal{H}_1$ y $\mathcal{H}_2$ la matriz asociada al operador adjunto a otro operador es la matriz transpuesta y conjugada de la matriz asociada al operador original. Es por esta razón que se utilizará la misma notación para identificar al adjunto, que cuando se quiere indicar la matriz traspuesta y conjugada de otra, es decir aplicar a una matriz el operador †.

Proposición A.2.1. *Propiedades del operador adjunto:*

1. $(T + \alpha S)^\dagger = T^\dagger + \alpha^* S^\dagger$ *para todo* $T, S \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ *y* $\alpha \in \mathbb{C}$
2. $(TS)^\dagger = S^\dagger T^\dagger$ *para todo* $T, S \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$
3. $(T^\dagger)^\dagger = T$ *para todo* $T \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$
4. *Dado* $T \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ *, T es invertible si y solo si* $T^\dagger$ *lo es y* $(T^\dagger)^{-1} = (T^{-1})^\dagger$

Operadores normales, hermíticos y unitarios.

Considerando ahora los operadores lineales que son endomorfismos en espacios de Hilbert

Definición A.2.2. Se dice que un operador $T \in \Lambda(\mathcal{H}, \mathcal{H})$ es **Normal** si $TT^\dagger = T^\dagger T$

Proposición A.2.2. *Sea* $N \in \Lambda(\mathcal{H}, \mathcal{H})$ *un operador normal, se cumple entonces:*

- $||N^\dagger|u\rangle|| = ||N|u\rangle||$ *ya que* $||N^\dagger|u\rangle||^2 = \langle N^\dagger u|N^\dagger u\rangle = \langle N^\dagger N u|u\rangle = \langle NN^\dagger u|u\rangle = \langle Nu|Nu\rangle = ||N|u\rangle||^2$
- *De lo anterior se desprende inmediatamente que* $ker(N) = ker(N^\dagger)$
- *Sea* $|v\rangle$ *un vector propio del operador normal N asociado al valor propio* λ_v*, entonces* $|v\rangle$ *es un vector propio del operador* $N^\dagger$ *asociado al valor propio* λ_v^**. Además si* $|u\rangle$ *es un vector ortogonal a* $|v\rangle$ *entonces* $N|u\rangle$ *sigue siendo ortogonal a* $|v\rangle$ *ya que* $\langle v|N|u\rangle = \langle N^\dagger v|u\rangle = \lambda^* \langle v|u\rangle = 0$

Definición A.2.3. Un operador $T \in \Lambda(\mathcal{H}, \mathcal{H})$ es **Hermítico** si coincide con su adjunto, $T = T^\dagger$

Proposición A.2.3. *Los operadores hermíticos cumplen las siguientes propiedades:*

- *Si un operador es hermítico es normal.*
- *Las matrices asociadas a operadores hermíticos en bases ortonormales son matrices hermíticas (Si* $M \in \mathbb{M}_{n\times n}$ *M es hermítica si* $M = (M^t)^* = M^\dagger$*) , independientemente de las bases elegidas.*
- *Los valores propios de un operador* $\{\lambda_i\}$ *hermítico son valores reales,* $\lambda_i \in \mathbb{R}$*: Sea* $|u\rangle$ *un vector propio del operador hermítico T asociado al valor propio* λ_u*, por tanto* $\langle u|T|u\rangle = \langle T^\dagger u|u\rangle = \langle Tu|u\rangle \Rightarrow \langle u|\lambda_u u\rangle = \langle \lambda_u u|u\rangle \Rightarrow \lambda_u \langle u|u\rangle = \lambda_u^* \langle u|u\rangle$ *de donde* $\lambda_u^* = \lambda_u \Rightarrow \lambda_u \in \mathbb{R}$

Definición A.2.4. Un operador $T \in \Lambda(\mathcal{H}, \mathcal{H})$ es **Unitario** si es un operador biyectivo isométrico, esto es$||T|u\rangle|| = |||u\rangle||$

Proposición A.2.4. *Sea $T \in \Lambda(\mathcal{H}, \mathcal{H})$ un operador unitario, entonces:*

- *Si un operador es Unitario es normal.*
- *Los operadores unitarios preservan el producto interno, $\langle Tv|Tu\rangle = \langle v|u\rangle$*
- *Las matrices asociadas a operadores unitarios en bases ortonormales son matrices unitarias (sea $U \in \mathbb{M}_{n\times n}$ U es unitaria si $U^\dagger U = U^\dagger U = Id$) , independientemente de las bases elegidas.*
- *Los valores propios de un operador $\{\lambda_i\}$ unitarios tienen módulo uno $||\lambda_i|| = 1$: Sea $|u\rangle$ un vector propio del operador unitaria S asociado al valor propio λ_u, por tanto $\langle Su|Su\rangle = \langle u|u\rangle \Rightarrow \langle \lambda_u u|\lambda_u u\rangle = \lambda_u^* \lambda_u \langle u|u\rangle = ||\lambda_u||^2 \langle u|u\rangle = \langle u|u\rangle$ de donde se deduce que $||\lambda_u|| = 1$*

Es inmediato que si K es un operador hermítico entonces $U = e^{iK}$ es un operador unitario:

Asumiendo que $U^\dagger = \left(\mathrm{e}^{iK}\right)^\dagger = \left(\mathrm{e}^{-iK}\right)$

$$\text{Entonces } U^\dagger U = \left(\mathrm{e}^{-iK}\right)\left(\mathrm{e}^{iK}\right) = \left(\mathrm{e}^{-iK+iK}\right) = I_d \quad \text{(A.8)}$$

Definición A.2.5. Un operador $T \in \Lambda(\mathcal{H}, \mathcal{H})$ es **Positivo** si $\forall\ |u\rangle \in \mathcal{H}$, $\langle Tu|u\rangle \geq 0$, y se lo simboliza $T \geq 0$. Si además $\forall |u\rangle \in \mathcal{H}\ \langle Tu|u\rangle = 0$ sii $|u\rangle = 0$, se dice que T es defiido positivo, o que es estrictamente positivo.

Observación A.2.1. De la defiición anterior se deduce que:

1. $\forall |u\rangle \in \mathcal{H}\ |u\rangle\langle u|$ es positivo.
2. Para todo operador $T \in \Lambda(\mathcal{H}, \mathcal{H})$ se tiene que $TT^\dagger$ y $T^\dagger T$ son operadores positivos.
3. Si $T, S \in \Lambda(\mathcal{H}, \mathcal{H})$ son operadores positivos y $\alpha \in \mathbb{R} \geq 0$ entonces $T + \alpha S$ es un operador positivo

Teorema A.2.1. *Si un operador $P \in \Lambda(\mathcal{H}, \mathcal{H})$ es positivo, $P \geq 0$, entonces P es hermítico.*

Teorema A.2.2. *Dado un operador normal $N \in \Lambda(\mathcal{H}, \mathcal{H})$, si todos sus valores propios son reales no negativos entonces $N \geq 0$.*

De aquí en más se utilizará mucho un tipo de operador en particular: dados el vector $|v\rangle \in \mathcal{H}_1$ y el vector $|u\rangle \in \mathcal{H}_2$ se defie el operador $|u\rangle\langle v| \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ cuya acción a un vector $|w\rangle \in \mathcal{H}_1$ queda determinada por

$$(|u\rangle\langle v|)(|w\rangle) = \langle v|w\rangle|u\rangle \quad \forall |w\rangle \in \mathcal{H}_1 \quad \text{(A.9)}$$

De hecho obviando los paréntesis, se ve la potencia de la notación de Dirac, este operador queda claramente defiido:

$$|u\rangle\langle v||w\rangle = |u\rangle\langle v|w\rangle = \langle v|w\rangle|u\rangle \quad \forall |w\rangle \in \mathcal{H}_1 \quad \text{(A.10)}$$

Si ahora se considera $|u\rangle, |v\rangle \in \mathcal{H}$ la función $\{|v\rangle, |u\rangle\} \to |u\rangle\langle v|$ que va de $\mathcal{H} \times \mathcal{H}$ a $\Lambda(\mathcal{H}, \mathcal{H})$ se la denomina **producto externo** (en contraposición al producto interno) y es fácil de chequear que cumple las siguientes propiedades:

a. Es lineal en la primer componente y lineal conjugada en la segunda.
b. $(|u\rangle\langle v|)^\dagger = |v\rangle\langle u|$, además el operador $|u\rangle\langle u|$ siempre es hermítico.

c. Si $T \in \Lambda(\mathcal{H}, \mathcal{H})$ es otro operador se tiene que $T|u\rangle\langle v| = |Tu\rangle\langle v|$ y $|u\rangle\langle v|T = |u\rangle\langle T^\dagger v|$

La utilidad del producto externo queda de manifiesto a la hora de mostrar una importante propiedad que tienen las bases ortonormales. Si se nota $\{|i\rangle\}_{1\leq n}$ a los elementos de una base ortonormal de un espacio $\mathcal{H}$ de dimensión n, y se considera un vector $|v\rangle$ arbitrario de $\mathcal{H}$, entonces:

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle \tag{A.11}$$

y sabiendo que $|v\rangle = \sum_i v_i|i\rangle = \sum_i \langle i|v\rangle|i\rangle$ se tiene que:

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i v_i|i\rangle = v \text{ de donde} \tag{A.12}$$

$$\sum_i |i\rangle\langle i| = I_d \tag{A.13}$$

A esta relación se la conoce como relación de completitud.

Descomposición Espectral.

Definición A.2.6. Un operador $M = \Lambda(\mathcal{H}, \mathcal{H})$ es **diagonalizable** si existe una base ortonormal $|i\rangle$ de $\mathcal{H}$ conformada por vectores propios de M, asociados a los valores propios λ_i.

De ser M diagonalizable se la puede escribir como

$$M = \sum_i \lambda_i |i\rangle\langle i| \tag{A.14}$$

A los operadores $|i\rangle\langle i|$ se les llama los **proyectores** en los subespacios asociados a los valores propios λ_i y es inmediato probar que:

- $P_iP_j = \delta_{ij}P_i$ o sea $P_iP_j = 0$ si $i \neq j$ y $P_i^2 = P_i$ *si* $i = j$
- Cumplen la relación de completitud A.13, $\sum_i P_i = I_d$.

Teorema A.2.3. *Cualquier operador normal de un espacio de Hilbert es diagonalizable y recíprocamente cualquier operador diagonalizable respecto a una base ortonormal es un operador normal.*

Una demostración de este teorema se encuentra en los libros [18] o [131] citados en la blibiobrafía.

Corolario A.2.1. *Cualquier operador hermítico de un espacio de Hilbert es diagonalizable y recíprocamente cualquier operador diagonalizable respecto a una base ortonormal cuyos valores propios $\{\lambda_i\}$ son todos reales es un operador hermítico.*

Corolario A.2.2. *Cualquier operador unitario de un espacio de Hilbert es diagonalizable y recíprocamente cualquier operador diagonalizable respecto a una base ortonormal cuyos valores propios $\{\lambda_i\}$ tienen todos módulo uno es un operador unitario.*

Traza de un operador.

Definición A.2.7. Dado un operador $T \in \Lambda(\mathcal{H}, \mathcal{H})$ y su matriz asociada (t_{ij}) en alguna base ortonormal $\{|a_i\rangle\}_i$ se defie la **traza del operador** $tr : \Lambda(\mathcal{H}, \mathcal{H}) \to \mathbb{C}$ como la suma de los componentes de la diagonal de la matriz t_{ij}.

$$tr(T) = \sum_i t_{ii} \tag{A.15}$$

Para que la defiición sea consistente es necesario probar que la defiición no depende de la base elegida:

Utilizando la defiición de matriz asociada (ver en secciónA.2) $t_{ii} = \langle a_i|T|a_i\rangle$ y tomando una nueva base ortonormal $\{|b_i\rangle\}_i$, utilizando luego la relación de completitud de las bases ortonormales (ecuación A.13) tenemos que:

$$t_{ii} = \langle a_i|T|a_i\rangle = \sum_j \langle a_i|b_j\rangle\langle b_j|T|a_i\rangle = \sum_j \langle a_i|b_j\rangle\langle T^\dagger b_j|a_i\rangle = \sum_j \langle T^\dagger b_j|a_i\rangle\langle a_i|b_j\rangle \tag{A.16}$$

Entonces:

$$tr(T) = \sum_i \sum_j \langle T^\dagger b_j|a_i\rangle\langle a_i|b_j\rangle = \sum_j \sum_i \langle T^\dagger b_j|a_i\rangle\langle a_i|b_j\rangle = \sum_j \langle T^\dagger b_j|Id|b_j\rangle \tag{A.17}$$

$$tr(T) = \sum_j \langle T^\dagger b_j|b_j\rangle = \sum_j \langle b_j|T|b_j\rangle = \sum_i \langle a_i|T|a_i\rangle \tag{A.18}$$

Proposición A.2.5. *Dados los operadores T y $S \in \Lambda(\mathcal{H}, \mathcal{H})$, la función traza tiene las siguientes propiedades:*

1. $tr(T^\dagger) = tr(T)^*$
2. *La traza es cíclica:* $tr(TS) = tr(ST)$
3. *Dado U un operador invertible (unitario en particular)* $tr(T) = tr(UTU^{-1})$
4. $tr(T|u\rangle\langle v|) = \langle v|Tu\rangle \quad \forall |u\rangle, |v\rangle \in \mathcal{H}$
5. *La suma de los valores propios de un operador T, incluyendo las multiplicidades algebraicas, es igual a $tr(T)$.*

A.3. Producto tensorial de espacios vectoriales.

Proposición A.3.1. *Sean V y W dos espacios vectoriales de dimensión n y m respectivamente y el espacio vectorial $V \otimes W$ de dimensión nm, el producto tensorial es una función $\otimes : (V \times W) \to V \otimes W$* [2] *tal que al par $(|v\rangle, |w\rangle)$ le asocia el elemento $|v\rangle \otimes |w\rangle$ que cumple las siguientes propiedades:*

1. *La función $\otimes$ es una función bilineal, esto es, es lineal en ambas componentes.*
2. *Cumple las siguientes distributivas:*

[2] $\times$ denota al producto cartesiano mientras que $\otimes$ denota el producto tensorial que se está defiiendo.

- *Sean* $|v_1\rangle, |v_2\rangle \in V$ *y* $|w\rangle \in W$*, entonces* $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
- *Sean* $|v\rangle \in V$ *y* $|w_1\rangle, |w_2\rangle \in W$ *entonces* $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

y además sea $c \in \mathbb{R}$ *entonces* $c(|v\rangle \otimes |w\rangle) = (c|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$

3. *Todo elemento de* $V \otimes W$ *se puede escribir como combinación lineal de elementos* $|v_i\rangle \otimes |w_i\rangle$ *para algunos* $|v_i\rangle$ *y* $|w_i\rangle$ *de* V *y* W *respectivamente.*
4. *Sean* $\{|v_i\rangle\}_{1\leq i\leq n}$ *y* $\{|w_j\rangle\}_{1\leq j\leq m}$ *bases de* V *y* W *respectivamente entonces* $\{|v_i \otimes w_j\rangle\}_{1\leq i\leq n \text{ y } 1\leq j\leq m}$ *es una base de* $V \otimes W$
5. *Si* $|\psi\rangle$ *y* $|\varphi\rangle$ *son vectores, entonces* $|||\psi\rangle \otimes |\varphi\rangle|| = |||\psi\rangle||\ |||\varphi\rangle||$

Se obvia como se construye el espacio vectorial (para ver un desarrollo exhaustivo de esta construcción se recomienda consultar la referencia [131]) $V \otimes W$ ya que es una formalidad que no aporta a este trabajo. Además se puede demostrar que salvo isomorfismos el producto tensorial es único.

La pregunta lógica que surge, es, se tiene definido el producto tensorial entre espacios vectoriales, ¿pero qué pasa cuando se considera espacios de Hilbert?,¿se puede mantener la estructura? Sean dos espacios de Hilbert $\{\mathcal{H}_1, (,)_1\}$ y $\{\mathcal{H}_2, (,)_2\}$ y considérese en ellos $\{|a_i\rangle\}_i$ $\{|b_j\rangle\}_j$ bases ortonormales de $\mathcal{H}_1$ y $\mathcal{H}_2$ respectivamente.

Tomando ahora $|v\rangle$ y $|v'\rangle \in \mathcal{H}_1$ y $|u\rangle$ y $|u'\rangle \in \mathcal{H}_2$, se sabe que $|v\rangle = \sum_i v_i|a_i\rangle$, $|v'\rangle = \sum_i v'_i|a_i\rangle$, $|u\rangle = \sum_j u_j|b_j\rangle$ y $|u'\rangle = \sum_j u'_j|b_j\rangle$, entonces el producto $|v\rangle \otimes |u\rangle$ queda defiido en términos de los productos de las bases como $|v\rangle \otimes |u\rangle = \sum_i \sum_j v_i u_j(|a_i\rangle \otimes |b_j\rangle)$ y $|v'\rangle \otimes |u'\rangle = \sum_i \sum_j v'_i u'_j(|a_i\rangle \otimes |b_j\rangle)$

Entonces definimos el producto entre $|v\rangle \otimes |u\rangle$ y $|v'\rangle \otimes |u'\rangle$ en $\mathcal{H}_1 \otimes \mathcal{H}_2$ como:

$$(|v\rangle \otimes |u\rangle, |v'\rangle \otimes |u'\rangle)_\otimes = \left(\sum_i \sum_j v_i u_j(|a_i\rangle \otimes |b_j\rangle), \sum_i \sum_j v'_i u'_j(|a_i\rangle \otimes |b_j\rangle)\right)_\otimes = \tag{A.19}$$

$$\sum_{\substack{1\leq i,r\leq n\\ 1\leq j,k\leq m}} v_i^* u_j^* v'_r u'_k(|a_i\rangle, |a_r\rangle)_1(|b_j\rangle, |b_k\rangle)_2 \tag{A.20}$$

Se prueba directamente utilizando la formula anterior que $(,)_\otimes$ es un producto interno en $\mathcal{H}_1 \otimes \mathcal{H}_2$. Por tanto teniendo en cuenta que como $\mathcal{H}_1$ y $\mathcal{H}_2$ son finitos, por tanto $\mathcal{H}_1 \otimes \mathcal{H}_2$ también lo es, $\mathcal{H}_1 \otimes \mathcal{H}_2$ es un espacio de Hilbert.

Una propiedad importante del producto tensorial que todavía no se mencionó es la Propiedad universal del producto tensorial, ya que permite también a través del producto tensorial, crear operadores del nuevo espacio vectorial.

Proposición A.3.2. ***Propiedad universal del producto tensorial:*** *Sean* $\mathcal{H}_1$*,* $\mathcal{H}_2$ *y* $\mathcal{H}_3$ *espacios vectoriales complejos, si* $f : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathcal{H}_3$ *es una función bilineal, entonces existe una única función* F *lineal,* $F : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathcal{H}_3$ *que cumpla que* $f(|v\rangle, |w\rangle) = F(|v\rangle \otimes |w\rangle)\ \ \forall\ |v\rangle \in \mathcal{H}_1$ *y* $|w\rangle \in \mathcal{H}_2$

Esto implica que si se considera un operador cualquiera $t : \mathcal{H}_1 \times \mathcal{H}_2 \to \mathcal{H}_1 \otimes \mathcal{H}_2$ tal que $t(|v\rangle, |w\rangle) = A|v\rangle \otimes B|w\rangle$ existe una única transformación lineal T tal que $T(|v\rangle \otimes |w\rangle) = t(|v\rangle \times |w\rangle) = A|v\rangle \otimes B|w\rangle$. En otras palabras a partir de operadores en los espacios componentes se puede naturalmente construir operadores válidos en el nuevo espacio.

En dimensión finita además es equivalente a decir que todo operador $L \in \Lambda(\mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_1 \otimes \mathcal{H}_2)$ se puede escribir de la forma $\sum_i c_i A_i \otimes B_i$. Esto lo que implica fuertemente es que habrá operdores

propios del espacio $\mathcal{H}_1 \otimes \mathcal{H}_2$ que no se podrán obtener como producto de operadores de los espacios componentes. Ver en la sección 2.1.6 ejemplos de estos operadores y sus propiedades.

Es importante que todos estos resultados, repecto al producto tensorial, que se han obtenido hasta el momeno siguen siendo válidos cuando se toman una cantidad finita de operandos en vez de dos.

Proposición A.3.3. *Sean $\mathcal{H}_1$ y $\mathcal{H}_2$ espacios de Hilbert, $A \in \Lambda(\mathcal{H}_1, \mathcal{H}_1)$ y $B \in \Lambda(\mathcal{H}_2, \mathcal{H}_2)$ entonces $tr(A \otimes B) = tr(A).tr(B)$.*

Proposición A.3.4. *Sean A y $B \in \Lambda(\mathcal{H}, \mathcal{H})$, entonces si:*

- *Si A y B son operadores normales $A \otimes B$ es un operador normal.*
- *Si A y B son operadores hermíticos $A \otimes B$ es un operador hermítico.*
- *Si A y B son operadores unitarios $A \otimes B$ es un operador unitario.*

A.3.1. Producto de Kronecker

En particular de aquí en adelante se trabajará con el producto tensorial definido para el espacio vectorial de las matrices (finitas), con entradas complejas o reales, este es el producto de Kronecker:

Definición A.3.1. Dadas dos matrices $A \in \mathbb{M}_{n\times m}$ y $B \in \mathbb{M}_{p\times q}$ se defie el **producto de Kronecker** de entre A y B, como la matriz $C \in \mathbb{M}_{mp\times nq}$ y se nota como $A \otimes B = C$, donde C queda defiida por $c_{\substack{\alpha,\beta=k+p(i-1),l+q(j-1)\\ 1\leq i\leq n \quad 1\leq j\leq m\\ 1\leq k\leq p \quad 1\leq l\leq q}} = a_{ij}b_{kl}$ o de manera más visual:

$$\text{dada } A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1m} \\ a_{21} & a_{22} & ... & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & ... & a_{nm} \end{pmatrix} \text{ entonces } C = \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1m}B \\ a_{21}B & a_{22}B & ... & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & ... & a_{nm}B \end{pmatrix} \tag{A.21}$$

Observación A.3.1. Respecto al producto de Kronecker

- El producto exterior visto en A.2 es un caso particular del producto de Kronecker.
- Es asociativo $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$
- Respecto al producto mixto: supongase que A y C son matrices conformables, y B y D también, entonces $(A \otimes B)(C \otimes D) = AC \otimes BD$
- De la propiedad anterior se deduce que $(A \otimes B)$ es invertible si y solo si A y B lo son, y $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$

A.4. Sistemas y su interacción con el entorno

Hasta ahora se ha considerado que los sistemas cuánticos con los que se trata son sistemas cerrados, pero un sistema cerrado es una idealización que no coincide con la realidad de los sistemas

físicos que se pueden implementar, ya que es inevitable que en algún punto los sistemas interaccionen con su entorno.

Al considerar entonces que los sistemas reales interaccionan con el entorno, la evolución de los sistemas ya no será unitaria, ya que nuestro sistema pasa a ser parte de un sistema abierto.

En la mayoría de los casos es válida la suposición de que el sistema y el entorno inicialmente no presentan entrelazamiento[3]. El sistema global se encuentra en un estado $|u_{sis} \otimes v_{env}\rangle$ del espacio $\mathcal{H}_{sis} \otimes \mathcal{H}_{env}$, donde $\mathcal{H}_{sis}$ es el espacio de Hilbert de nuestro sistema y $\mathcal{H}_{env}$ el del ambiente (ver referencia [18], y [131]).

El sistema compuesto $\mathcal{H}_{sis} \otimes \mathcal{H}_{env}$ puede pensarse como un en sistema cerrado en sí, por tanto su evolución de este sistema quedará determinada por su Hamiltoniano:

$$H_{gl} = H_{sis} \otimes I_{env} + I_{env} \otimes H_{env} + V_{inter} \tag{A.22}$$

Los tres términos que aparecen en el Hamiltoniano se recogen la evolución del sistema por un lado, el del medio por otro y un último término que describe la interacción sistema-ambiente (extraído de [131]).

El sistema compuesto $\mathcal{H}_{sis} \otimes \mathcal{H}_{env}$ es en sí un sistema cerrado, por tanto su evolución de acuerdo tercer postulado queda descripto por la ecuación:

$$|u_{sis} \otimes v_{env}\rangle\langle u_{sis} \otimes v_{env}| = U_{gl}(t)|u_{sis} \otimes v_{env}\rangle\langle u_{sis} \otimes v_{env}|U_{gl}^{\dagger}(t) \tag{A.23}$$

donde $U_{gl}(t)$ es un operador unitario en $\mathcal{H}_{sis} \otimes \mathcal{H}_{env}$.

En general el ambiente está modelado por un sistema de Hilbert de dimensión mucho mayor que el que modela al sistema a estudiar, y en sí, saber cómo evoluciona el ambiente no es de gran interés, si no más bien, como este afecta al sistema a estudiar. Es por esto que para estudiar cómo evoluciona nuestro sistema abierto al medio, a partir del estudio de la evolución del sistema cerrado global se introduce el operador traza parcial:

$$\rho_{sis} = \Phi\rho_{sis} = tr_{env}(U_{gl}(t)\rho_{sis} \otimes \rho_{env}U_{gl}^{\dagger}(t)) \tag{A.24}$$

donde ρ_{sis} es un operador de densidad de un estado cualquiera de $\mathcal{H}_{sis}$ y ρ_{env} es un operador de densidad cualquiera de $\mathcal{H}_{env}$.

Este operador permite llegar a tener una descripción de los observables de los subsistemas de un sistema. El operador traza parcial (tr_{env}) es un operador que lleva operadores de $\mathcal{H}_{sis} \otimes \mathcal{H}_{env}$ en operadores de $\mathcal{H}_{sis}$, y para describirlo adecuadamente es necesario introducir algunos conceptos:

Definición A.4.1. Una función $\eta : \Lambda(\mathcal{H}_1, \mathcal{H}_1) \to \Lambda(\mathcal{H}_2, \mathcal{H}_2)$ (lleva operadores de un espacio $\mathcal{H}_1$ a operadores de otro espacio $\mathcal{H}_2$) es un **operador completamente positivo** si es de la forma

$$\eta(\rho) = \sum_{i=1}^{n} E_i \rho E_i^{\dagger} \tag{A.25}$$

donde $E_i \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$

A esta representación se la conoce como representación de Kraus.

Definición A.4.2. Una función lineal $\Psi : \Lambda(\mathcal{H}_1, \mathcal{H}_1) \to \Lambda(\mathcal{H}_2, \mathcal{H}_2)$ se dice que **preserva la traza** si

$$\forall \rho \in \Lambda(\mathcal{H}_1, \mathcal{H}_1) \text{ se cumple que } tr(\Psi(\rho)) = tr(\rho) \tag{A.26}$$

[3]Inicialmente el sistema está en un estado que fue preparado, por lo tanto perfectamente conocido.

Proposición A.4.1. *Un operador completamente positivo* $\Psi: \Lambda(\mathcal{H}_1, \mathcal{H}_1) \to \Lambda(\mathcal{H}_2, \mathcal{H}_2)$ *con representación de Krauss* $\sum_i^n E_i \rho E_i^\dagger$ *donde* $E_i \in \Lambda(\mathcal{H}_1, \mathcal{H}_2)$ *preserva la traza si y sólo si:*

$$\sum_i^n E_i E_i^\dagger = I_1 \tag{A.27}$$

Una demostración de esta proposición se puede encontrar en la página 38 de la referencia [132].

A.4.1. Traza Parcial

Se defie entonces traza parcial como:

Definición A.4.3. Sean $\mathcal{H}_1$ y $\mathcal{H}_2$ dos espacios de Hilbert y ρ_{12} en $\mathcal{H}_1 \otimes \mathcal{H}_2$ se defie la **traza parcial**, respecto de $\mathcal{H}_1$ del operador ρ_{12} como el operador ρ_1 de $\mathcal{H}_1$ que cumple para todo $x \in \Lambda(\mathcal{H}_1, \mathcal{H}_1)$:

$$tr(\rho_1 x) = tr(\rho_{12}(x \otimes I_2)) \tag{A.28}$$

y se nota que $tr_2(\rho_{12}) = \rho_1$

Proposición A.4.2. *La traza parcial es un operador completamente positivo que preserva la traza.*

Además se cumple que:

Proposición A.4.3. *Sea* ρ_{12} *en* $\mathcal{H}_1 \otimes \mathcal{H}_2$ *se dice que* ρ_1 *de* $\mathcal{H}_1$ *es la traza parcial, respecto de* $\mathcal{H}_1$ *del operador* ρ_{12} *si y solo si dados* $|u\rangle$ *y* $|v\rangle$ *en* $\mathcal{H}$*, y* $\{|b_j\rangle_j\}$ *una base ortonormal de* $\mathcal{H}_2$

$$\langle u|\rho_1|v\rangle = \sum_j \langle u \otimes b_j|\rho_{12}|v \otimes b_j\rangle \tag{A.29}$$

Si se toma $\{|a_i\rangle_i\}$ una base ortonormal de $\mathcal{H}_1$, recordando que $\{|a_i\rangle \otimes |b_j\rangle\}_{i,j}$ es una base ortonormal de $\mathcal{H}_1 \otimes \mathcal{H}_2$, de la definición de traza se desprende que:

$$\begin{aligned} tr(\rho_{12}(x \otimes I_2)) &= \sum_{i,j} \langle a_i \otimes b_j|\rho_{12}(x \otimes I_2)|a_i \otimes b_j\rangle = \sum_{i,j} \langle a_i \otimes b_j|\rho_{12}|xa_i \otimes b_j\rangle \\ &= \sum_i \left(\sum_j \langle a_i \otimes b_j|\rho_{12}|xa_i \otimes b_j\rangle \right) = \sum_i \langle a_i|\rho_{12}|xa_i\rangle = tr(\rho_1 x) \end{aligned} \tag{A.30}$$

De esta proposición y trabajando de manera similar para mostrar que esta proposición no depende de las bases elegidas, se demuestra que el operador traza parcial es único. Además:

Proposición A.4.4. *El operador traza parcial cumple:*

1. *La traza parcial es lineal: Sean* α_{12} *y* β_{12} *operadores de* $\mathcal{H}_1 \otimes \mathcal{H}_2$ *y* $\lambda \in \mathbb{C}$ *entonces*

$$tr_1(\alpha_{12} + \lambda\beta_{12}) = tr_1(\alpha_{12}) + \lambda tr_1(\beta_{12}) \tag{A.31}$$

2. *Si* ρ_1 *y* ρ_2 *son operadores de* $\mathcal{H}_1$ *y* $\mathcal{H}_2$ *respectivamente entonces*

$$\begin{aligned} tr_2(\rho_1 \otimes \rho_2) &= \rho_1 tr(\rho_2) \\ tr_1(\rho_1 \otimes \rho_2) &= \rho_2 tr(\rho_1) \end{aligned} \tag{A.32}$$

En particular si son operadores de densidad:

$$\begin{aligned} tr_2(\rho_1 \otimes \rho_2) &= \rho_1 \\ tr_1(\rho_1 \otimes \rho_2) &= \rho_2 \end{aligned} \tag{A.33}$$

A.5. Información Cuántica

A.5.1. Teorema de no clonación.

Proposición A.5.1. *Dado un estado $|\phi\rangle$ desconocido y otro estado conocido $|0\rangle$, ambos pertenecientes a un espacio de común de Hilbert, no existe un circuito U aplicado al sistema $|0\rangle \otimes |\phi\rangle$ que devuelva el estado $|\phi\rangle \otimes |\phi\rangle$.*

Demostración. Supongamos que existe el circuito U que clona el estado genérico $|\phi\rangle$. Tomemos dos estados $|\psi_1\rangle$ y $|\psi_2\rangle$. Por nuestra hipótesis, tenemos:

$$U|0\rangle|\psi_1\rangle = |\psi_1\rangle|\psi_1\rangle$$
$$U|0\rangle|\psi_2\rangle = |\psi_2\rangle|\psi_2\rangle$$

Multiplicando ambas ecuaciones:

$$\implies U(|0\rangle|\psi_1\rangle)^\dagger(U|0\rangle|\psi_2\rangle) = (|\psi_1\rangle|\psi_1\rangle)^\dagger(|\psi_2\rangle|\psi_2\rangle)$$
$$\langle\psi_1|\langle 0|U^\dagger U|0\rangle|\psi_2\rangle = \langle\psi_1|\langle\psi_1||\psi_2\rangle|\psi_2\rangle$$
$$\langle\psi_1|\langle 0|0|I\rangle d|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2$$
$$\langle\psi_1|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2$$

De donde se sigue que $\langle\psi_1|\psi_2\rangle = 0$ por lo que ambos estados son ortogonales. o $\langle\psi_1|\psi_2\rangle = 1$, y se tiene que $|\psi_1\rangle = |\psi_2\rangle$. Por lo que el circuito U solo puede clonar estados que sean ortogonales o iguales, y no cualquier estado arbitrario.

□

A.5.2. Entropía de von Neumann

Respecto al análogo cuántico de la entropía de Shannon (clásica) es la entropía de Von Nuemann, donde en lugar de utilizar elementos de una distribución de probabilidad se utilizan operadores densidad. La entropía de un estado cuántico con un operador ρ es

$$S(\rho) \equiv -\operatorname{tr}(\rho \log \rho)$$

Utilizando el hecho de que ρ es una matriz hermítica positiva (todos sus autovalores son no negativos) la definión anterior es equivalente a la siguiente:

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

Siendo $\{\lambda_i\}$ el conjunto de autovalores de ρ

Entropía cuántica relativa

A su vez análogamente al caso clásico se define la entropía relativa para dos operadores de densidad ρ y σ como

$$S(\rho||\sigma) \equiv \mathrm{tr}\,(\rho \log \rho) - \mathrm{tr}\,(\rho \log \sigma)$$

Teorema A.5.1. *La entropía cuántica relativa es no negativa (Desigualdad de Klein)*

$$S(\rho||\sigma) \geq 0$$

Demostración. Como ρ y σ son operadores de densidad, son hermíticos, por tanto tienen descomposición espectral. Sean entonces $\rho = \sum_i p_i |i\rangle\langle i|$ y $\sigma = \sum_j q_j |j\rangle\langle j|$, donde $\{|i\rangle\}_i$ y $\{|j\rangle\}_j$ son bases ortonormales de vectores propios de ρ y σ respectivamente. Aplicando la definición tenemos entonces:

$$S(\rho||\sigma) = \sum_i \langle i|\rho \log \rho|i\rangle - \sum_i \langle i|\rho \log \sigma|i\rangle \quad [4]$$

Además se cumple que si $\rho|i\rangle = p_i|i\rangle$ entonces $\langle i|\rho = p_i\langle i|$ ya que $(\rho|i\rangle)^\dagger = (p_i|i\rangle)^\dagger \Leftrightarrow \langle i|\rho^\dagger = p_i^*\langle i|$ pero como ρ es hermítica y por tanto p_i real tenemos que $\langle i|\rho = p_i\langle i|$ con lo cual

$$\sum_i \langle i|\rho \left(\log p_i |i\rangle\langle i|\right)|i\rangle - \sum_i p_i \langle i| \log \sigma |i\rangle$$

y utilizando que $\log \sigma = \sum_j \log q_j |j\rangle\langle j|$ tenemos que:

$$\sum_i p_i \log p_i - \sum_i p_i \langle i| \left(\sum_j \log q_j |j\rangle\langle j|\right)|i\rangle = \sum_i p_i \log p_i - \sum_i p_i \sum_j \log q_j \langle i|j\rangle\langle j|i\rangle$$

llamando $P_{i,j} = \langle i|j\rangle\langle j|i\rangle = \langle i|j\rangle\langle i|j\rangle^* = ||\langle i|j\rangle||^2 \geq 0$ tenemos que

$$S(\rho||\sigma) = \sum_i p_i \left(\log p_i - \sum_j P_{i,j} \log q_j\right)$$

Observando que $\sum_j P_{i,j} = \sum_j \langle i|j\rangle\langle j|i\rangle = \langle i|\left(\sum_j |j\rangle\langle j|\right)|i\rangle = \langle i|i\rangle = 1$ y considerando que la función log es estrictamente cóncava:

$$\sum_j P_{i,j} \log q_j \leq \log \sum_j P_{i,j} q_j$$

con lo cual

$$S(\rho||\sigma) = \sum_i p_i \left(\log p_i - \sum_j P_{i,j} \log q_j\right) \geq \sum_i p_i \left(\log p_i - \log \sum_j P_{i,j} q_j\right)$$

y finalmente llamando $r_i := \sum_j P_{i,j} q_j$ tenemos que

$$S(\rho||\sigma) \geq \sum_i p_i \left(\log p_i - \log r_i\right) = \sum_i p_i \log \frac{p_i}{r_i} = D(p||r) \geq 0$$

La no negatividad de la entropía cuántica se deduce a partir de la entropía relativa (divergencia) clásica. Además la igualdad se alcanza únicamente cuando para cada i existe un j tal que $P_{i,j} = 1$, esto es que $P_{i,j}$ es una matriz de permutación, con lo cuál escencialmente $\rho = \sigma$, ya que la única diferncia entre ellas es el orden en el que se eligió la base de vectores propios. □

[4] Observar que $\langle i|\rho|i\rangle = \lambda_i = p_i$ es el valor propio asociado al vector propio $|i\rangle$

Observación A.5.1. Respecto a la definición

1. $0 \log 0 = 0$
2. $S(\rho) \geq 0$, es decir es no negativa y $S(\rho) = 0$ si ρ es un estado puro
3. $S(\rho) \leq \log d$ y se da la igualdad únicamente si $\rho = \frac{I_d}{d}$
4. Si un sistema AB se encuentra en un estado puro $|\phi\rangle$ entonces $S(A) = S(B)$
5. $S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$
6. Si U es un operador unitario en el espacio de ρ entonces $S(\rho) = S(U\rho U^\dagger)$
7. Subaditividad de la entropía: $\begin{matrix} a) & S(A,B) \leq S(A) + S(B) \\ b) & S(A,B) \geq |S(A) - S(B)| \end{matrix}$

Para ver las demostraciones de estas propiedades se recomienda consulta [132, 131]

Algunos detalles a destacar de estas observaciones es que el estado $\rho = \frac{I_d}{d}$ se puede demostrar que es el estado más mezclado posible. Una manera de ver esto es considerando que este estado es el que se obtiene de superponer todos los estados de una b.o.n[5] con una probabilidad uniforme para todos los elementos de la b.o.n. Este estado es de todos los de $\mathcal{H}_d$ el que tiene mayor entropía lo cuál es similar al caso clásico en el cual la entropía es máxima para una distribución uniforme de los datos.

Otro observación interesante que se puede hacer es que en el caso clásico $H(X,Y) = H(Y) + H(X)$ si X e Y son independientes. En el caso cúantico esto ocurre cuando los sitemas A y B son separables:$S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$ con $\rho \in \mathcal{H}_A$ y $\sigma \in \mathcal{H}_B$

Definición A.5.1. Se define a su vez como en el caso clásico la entropía conjunta como

$$S(A,B) \equiv -\operatorname{tr}\left(\rho^{AB} \log \rho^{AB}\right)$$

Así además se define la entropía condicional y la informción mutua como

$$S(A|B) = S(A,B) - S(A)$$

$$S(A:B) = S(A) + S(B) - S(A,B)$$

Observación A.5.2.

$$S(A:B) = S(A) - S(A|B) = S(B) - S(B|A)$$

Observación A.5.3. Si consideramos el estado cuántico $|\varphi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ que es un estado compuesto de dos sistemas de un qubit AB, vemos que $S(A,B) = 0$ ya que $|\varphi\rangle$ es un estado puro. Sin embargo $|\varphi\rangle$ es un estado totalmente entrelazado (es un estado de bell) por tanto $S(A) = S(Id/2) = 1$. Por tanto $S(A,B) < S(A)$

Esto conclye que

$$S(B|A) = S(A,B) - S(A) \leq 0$$

Lo que muestra que en el caso cuántico la entropía condicional no tiene por que ser no negativo. Esta hecho es similar a lo que ocurre cuando se considera la entropía diferencial en el caso clásico. Cuando hablamos de computación cuántica pensamos en un mundo discreto, pero paradógicamente en realidad estamos en un mundo continuo, los estados son continuos. Lo que hace que esta semejanza en principio no sea tan inesperada.

[5] b.o.n: base ortonormal

A.5.3. Efecto de la medida sobre la entropía

Al aplicar una medida a un estado cuántico hay dos formas de interpretar el resultado.

Si este resultado es observado, el resultado final es un estado puro, por lo cual, desde este punto de vista, una vez efectuada una medida y visto su resultado la entropía de von neumann del estado final es 0.

Otra forma de pensar en la medida cuántica, es en vez de observar el resultado, pensar en él, como la mezcla de todos los estados finales posibles considerano sus respectivas probabilidades.

Desde este punto de vista queremos ver como afecta la medida a la entropía de un estado.

Teorema A.5.2. *Las medidas proyectivas siempre aumentan la entropía*

Supongamos que $\{P_i\}_i$ es un conjunto de proyectores ortogonales ($P_i^2 = P_i$) que cumplen la relación de completitud $\sum_i P_i = I_d$ y ρ es un operador de densidad, entonces una vez medido el estado ρ obtendremos el estado $\rho' = \sum_i P_i \rho P_i$

Bastará probar que $S(\rho') \geq S(\rho)$.

Observación A.5.4. Además de las medidas proyectivas existen otras clases de medidas. No todas las medidas aumentan la entropía, algunas pueden incluso pueden disminuir la entropía. Este es el caso cuando se utiliza como operadores de medida a los operadores $M_1 = |0\rangle\langle 0|$ y $M_2 = |0\rangle\langle 1|$[6].

Por ejemplo si consideramos el estado $\rho = \frac{I_d}{2} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ del que sabemos que su entropía es $\log(2) = 1$ y le aplicamos los operadores de medida obtenemos el nuevo estado $\rho' = M_1 \rho M_1^\dagger + M_2 \rho M_2^\dagger$:

$$\rho' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0|$$

$$\Rightarrow S(\rho') = S(|0\rangle) = 0 \leq S(\rho)$$

A.5.4. Cota de Holevo

La cota de Holevo es una cota superior sobre la información accesible de un estado cuántico.

Proposición A.5.2. *Dado un sistema preparado en un estado ρ_X, con probabilidades $p_0, \ldots, p_n$ donde $X = 0, \ldots, n$. Si a este estado se le realiza una medida descrita por los operadores de medida $\{E_0, \ldots, E_m\}$ obteniendo a la salida Y, la cota de Holevo determina que para cualquier conjunto de operadores de medida*

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$$

donde $\rho = \sum_x p_x \rho_x$.

[6]Vale resaltar que estos dos operadores cumplen la condición de completitud: $M_1^\dagger M_1 + M_2^\dagger M_2 = Id$

Apéndice B

Demostraciones complementarias a completitud de bases

B.1. Producto de tres vectores de dimensión cuatro

Dados tres vectores de $\mathcal{H}^4$ de norma p ortogonales dos a dos, definimos la matriz:

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ t_1 & t_2 & t_3 & t_4 \end{bmatrix}$$

Donde el nuevo vector Y como $y_i = M(y_i)$ donde $M(y_i)$ se refiere al menor de primer orden del elemento y_i de la matriz antes definida.

Por ejemplo se tiene que

$$t_4 = \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}$$

Se quiere probar que $Y = (t_1, t_2, t_3, t_4)$ es divisible por p^2. Para esto se probará que cada cordenada lo es, en particular la prueba se hará para t_4.

Se debe contar con que:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$$
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = p$$
$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = p$$

y que

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 = 0$$
$$x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 = 0$$
$$z_1y_1 + z_2y_2 + z_3y_3 + z_4y_4 = 0$$

Utilizaremos la notación:

$$\hat{X} = (x_1, x_2, x_3)$$
$$\hat{Y} = (y_1, y_2, y_3)$$
$$\hat{Z} = (z_1, z_2, z_3)$$

Por lo que tenemos que:

$$|\hat{X}|^2 = p - x_4^2, \quad |\hat{Y}|^2 = p - y_4^2, \quad |\hat{Z}|^2 = p - z_4^2$$

y que

$$\langle \hat{X}|\hat{Y}\rangle = -x_4 y_4, \quad \langle \hat{X}|\hat{Z}\rangle = -x_4 z_4, \quad \langle \hat{Z}|\hat{Y}\rangle = -z_4 y_4$$

A partir de aquí solo queda operar:

$$t_4 = x_1y_2z_3 + x_3y_1z_2 + z_1x_2y_3 - x_3y_2z_1 - x_1z_2y_3 - z_3y_1x_2$$

por tanto

$$\begin{aligned} t_4^2 = {} & x_1^2y_2^2z_3^2 + x_3^2y_1^2z_2^2 + z_1^2x_2^2y_3^2 + x_3^2y_2^2z_1^2 + x_1^2z_2^2y_3^2 + z_3^2y_1^2x_2^2 \\ & + 2(x_1y_2z_3x_3y_1z_2 + x_1y_2z_3z_1x_2y_3 + x_3y_1z_2z_1x_2y_3 \\ & + x_3y_2z_1x_1z_2y_3 + x_3y_2z_1z_3y_1x_2 + x_1z_2y_3z_3y_1x_2) \\ & - 2[x_1^2(y_2z_2y_3z_3) + x_2^2(y_1z_1y_3z_3) + x_3^2(y_1z_1y_2z_2) \\ & + y_1^2(x_2z_2x_3z_3) + y_2^2(x_1z_1x_3z_3) + y_3^2(x_1z_1x_2z_2) \\ & + z_1^2(x_2y_2x_3y_3) + z_2^2(x_1y_1x_3y_3) + z_3^2(x_1y_1x_2y_2)] \end{aligned}$$

Utilizando que

$$\langle \hat{X}|\hat{Y}\rangle\langle \hat{X}|\hat{Z}\rangle\langle \hat{Z}|\hat{Y}\rangle =$$

$$\begin{aligned} & x_1^2y_1^2z_1^2 + y_1^2y_2^2y_3^2 + z_1^2z_2^2z_3^2 + \\ & \quad x_1y_2z_3x_3y_1z_2 + x_1y_2z_3z_1x_2y_3 + x_3y_1z_2z_1x_2y_3 \\ & \quad + x_3y_2z_1x_1z_2y_3 + x_3y_2z_1z_3y_1x_2 + x_1z_2y_3z_3y_1x_2 \\ & \quad x_1^2(y_1z_1y_2z_2 + y_1z_1y_3z_3) + x_2^2(y_1z_1y_2z_2 + y_2z_2y_3z_3) \\ & \quad x_3^2(y_1z_1y_3z_3 + y_2z_2y_3z_3) + y_1^2(x_1z_1x_3z_3 + x_1z_1x_2z_2) \\ & \quad y_2^2(y_1z_1y_2z_2 + y_1z_1y_3z_3) + x_3^2(y_1z_1y_3z_3 + y_2z_2y_3z_3) \\ & \quad y_3^2(x_1z_1x_3y_3 + x_2z_2x_3z_3) + z_1^2(x_1y_1x_2y_2 + x_1y_1x_3y_3) \\ & \quad z_2^2(x_1y_1x_2y_2 + x_2y_2x_3y_3) + z_3^2(x_1y_1x_3y_3 + x_2y_2x_3z_3) \end{aligned}$$

se obtiene

$$\begin{aligned} t_4^2 = {} & x_1^2y_2^2z_3^2 + x_3^2y_1^2z_2^2 + z_1^2x_2^2y_3^2 + x_3^2y_2^2z_1^2 + x_1^2z_2^2y_3^2 + z_3^2y_1^2x_2^2 \\ & + 2\langle \hat{X}|\hat{Y}\rangle\langle \hat{X}|\hat{Z}\rangle\langle \hat{Z}|\hat{Y}\rangle - 2(x_1^2y_1^2z_1^2 + y_1^2y_2^2y_3^2 + z_1^2z_2^2z_3^2) + \\ & (x_1^2 + x_2^2 + x_3^2)(-\langle \hat{Z}|\hat{Y}\rangle^2 + z_1^2y_1^2 + z_2^2y_2^2 + z_3^2y_3^2) \\ & (y_1^2 + y_2^2 + y_3^2)(-\langle \hat{X}|\hat{Z}\rangle^2 + x_1^2z_1^2 + x_2^2z_2^2 + x_3^2z_3^2) \\ & (z_1^2 + z_2^2 + z_3^2)(-\langle \hat{X}|\hat{Y}\rangle^2 + x_1^2y_1^2 + x_2^2y_2^2 + x_3^2y_3^2) \end{aligned}$$

y por tanto

$$\begin{aligned} x_1^2y_2^2z_3^2 + x_3^2y_1^2z_2^2 + z_1^2x_2^2y_3^2 + x_3^2y_2^2z_1^2 + x_1^2z_2^2y_3^2 + z_3^2y_1^2x_2^2 \\ - 2(x_1^2y_1^2z_1^2 + y_1^2y_2^2y_3^2 + z_1^2z_2^2z_3^2) + \\ (x_1^2+x_2^2+x_3^2)(z_1^2y_1^2 + z_2^2y_2^2 + z_3^2y_3^2) \\ (y_1^2+y_2^2+y_3^2)(x_1^2z_1^2 + x_2^2z_2^2 + x_3^2z_3^2) \\ (z_1^2+z_2^2+z_3^2)(x_1^2y_1^2 + x_2^2y_2^2 + x_3^2y_3^2) \\ = (x_1^2+x_2^2+x_3^2)(y_1^2+y_2^2+y_3^2)(z_1^2+z_2^2+z_3^2) = |\hat{X}|^2|\hat{Y}|^2|\hat{Z}|^2 \end{aligned}$$

con lo cuál

$$t_4^2 \quad = \quad |\hat{X}|^2|\hat{Y}|^2|\hat{Z}|^2 \; + \; 2\langle\hat{X}|\hat{Y}\rangle\langle\hat{X}|\hat{Z}\rangle\langle\hat{Z}|\hat{Y}\rangle \; - \; |\hat{X}|^2\langle\hat{Z}|\hat{Y}\rangle^2 \; - \; |\hat{Y}|^2\langle\hat{X}|\hat{Z}\rangle^2 \; - \; |\hat{Z}|^2\langle\hat{X}|\hat{Y}\rangle^2$$

Finalmente, sustituyendo por los valores originales se llega a la expresión:

$$\begin{aligned} t_4^2 = (p-x_4^2)(p-y_4^2)(p-z_4^2) + 2(-x_4y_4)(-x_4z_4)(-z_4y_4) \\ - (p-x_4^2)z_4^2y_4^2 - (p-y_4^2)x_4^2z_4^2 - (p-z_4^2)x_4^2y_4^2 \\ = p^3 + p(x_4^2y_4^2 + x_4^2z_4^2 + z_4^2y_4^2) - p^2(x_4^2+y_4^2+z_4^2) - x_4^2y_4^2z_4^2 \\ - 2x_4^2y_4^2z_4^2 - p(x_4^2y_4^2 + x_4^2z_4^2 + z_4^2y_4^2) + 3x_4^2y_4^2z_4^2 \\ = p^3 - p^2(x_4^2+y_4^2+z_4^2) = p^2(p-x_4^2+y_4^2+z_4^2) \end{aligned}$$

Bibliografía

[1] M. . Company. (2023, Abril) Quantum technology monitor. Copyright © McKinsey & Company. Accedido el 04 de Junio de 2023. [Online]. Available: https://www.mckinsey.com

[2] R. P. Feynman, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6, pp. 467–488, 1982.

[3] ——, "Quantum mechanical computers," *Foundations of physics*, vol. 16, no. 6, pp. 507–531, 1986.

[4] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 400, no. 1818. The Royal Society, 1985, pp. 97–117.

[5] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 439, no. 1907. The Royal Society, 1992, pp. 553–558.

[6] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. IEEE, 1994, pp. 124–134.

[7] D. Coppersmith, "An approximate fourier transform useful in quantum factoring," *arXiv preprint quant-ph/0201067*, 2002.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[9] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Physical review letters*, vol. 79, no. 2, p. 325, 1997.

[10] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[11] N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng, and J. Du, "Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system," *Physical review letters*, vol. 108, no. 13, p. 130501, 2012.

[12] I. PRESENT, "Cramming more components onto integrated circuits," *Readings in computer architecture*, vol. 56, 2000.

[13] P. W. Shor, "Why haven't more quantum algorithms been found?" *Journal of the ACM (JACM)*, vol. 50, no. 1, pp. 87–90, 2003.

[14] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[15] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical Review A*, vol. 52, no. 5, p. 3457, 1995.

[16] V. V. Shende and I. L. Markov, "On the cnot-cost of toffoli gates," *arXiv preprint arXiv:0803.2316*, 2008.

[17] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," *Physical Review A*, vol. 51, no. 2, p. 1015, 1995.

[18] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[19] S. Xu, "Reversible logic synthesis with minimal usage of ancilla bits," *arXiv preprint arXiv:1506.03777*, 2015.

[20] G. Benenti, G. Casati, and G. Strini, *Principles of quantum computation and information: Volume I: Basic Concepts*. World scientific, 2004.

[21] D. Gottesman, "The heisenberg representation of quantum computers," *arXiv preprint quant-ph/9807006*, 1998.

[22] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis," in *Foundations of Computer Science, 1999. 40th Annual Symposium on*. IEEE, 1999, pp. 486–494.

[23] A. Barenco, "A universal two-bit gate for quantum computation," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 449, no. 1937. The Royal Society, 1995, pp. 679–683.

[24] C. H. Bennett and D. P. DiVincenzo, "Quantum information and computation," *Nature*, vol. 404, no. 6775, pp. 247–255, 2000.

[25] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and quantum computation*. American Mathematical Society Providence, 2002, vol. 47.

[26] Y. Shi, "Toffoli or control-not needs little help to do universal quantum computation," Tech. Rep., 2002.

[27] A. Y. Kitaev, "Quantum computations: algorithms and error correction," *Russian Mathematical Surveys*, vol. 52, no. 6, pp. 1191–1249, 1997.

[28] C. M. Dawson and M. A. Nielsen, "The solovay-kitaev algorithm," *arXiv preprint quant-ph/0505030*, 2005.

[29] D. Aharonov, "A simple proof that toffoli and hadamard are quantum universal," *arXiv preprint quant-ph/0301040*, 2003.

[30] B. Schumacher and M. D. Westmoreland, "Modal quantum theory," *Foundations of Physics*, vol. 42, no. 7, pp. 918–925, 2012.

[31] D. Ellerman, "Quantum mechanics over sets," *arXiv:1310.8221v1 [quant-ph]*.

[32] A. J. Hanson, G. Ortiz, A. Sabry, and Y.-T. Tai, "Geometry of discrete quantum computing," *Journal of Physics A: Mathematical and Theoretical*, vol. 46, no. 18, p. 185301, 2013.

[33] ——, "Discrete quantum theories," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 11, p. 115305, 2014.

[34] C. M. Chandrashekar, R. Srikanth, and R. Laflamme, "Optimizing the discrete time quantum walk using a su(2) coin," *Phys. Rev. A*, vol. 77, p. 032326, Mar 2008.

[35] S. Lloyd and O. Dreyer, "The universal path integral," *Quantum Information Processing*, vol. 15, no. 2, pp. 959–967, 2016.

[36] G.-L. Long, "General quantum interference principle and duality computer," *Communications in Theoretical Physics*, vol. 45, no. 5, p. 825, 2006.

[37] G.-L. Long and Y. Liu, "Duality computing in quantum computers," *Communications in Theoretical Physics*, vol. 50, no. 6, p. 1303, 2008.

[38] G.-L. Long, Y. Liu, and C. Wang, "Allowable generalized quantum gates," *Communications in Theoretical Physics*, vol. 51, no. 1, p. 65, 2009.

[39] S. Gudder, "Mathematical theory of duality quantum computers," *Quantum Information Processing*, vol. 6, no. 1, pp. 37–48, 2007.

[40] G.-L. Long, "Mathematical theory of the duality computer in the density matrix formalism," *Quantum Information Processing*, vol. 6, no. 1, pp. 49–54, 2007.

[41] S.-J. Wei and G.-L. Long, "Duality quantum computer and the efficient quantum simulations," *Quantum Information Processing*, vol. 15, no. 3, pp. 1189–1212, 2016.

[42] S. J. Lomonaco, "How to build a device that cannot be built," *Quantum Information Processing*, vol. 15, no. 3, pp. 1043–1056, 2016.

[43] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis," in *40th Annual Symposium on Foundations of Computer Science*, New York City, NY, USA, 1999.

[44] Y. Shi, "Both toffoli and controlled-not need little help to do universal quantum computing," *Quantum Information & Computation*, vol. 3, no. 1, pp. 84–92, 2003.

[45] D. Aharonov, "A simple proof that toffoli and hadamard are quantum universal," *arXiv quant-ph/0301040*, 2003.

[46] V. Kliuchnikov, D. Maslov, and M. Mosca, "Fast and efficient exact synthesis of single qubit unitaries generated by clifford and t gates," *Quantum information & computation*, vol. 13, no. 7-8, pp. 607–630, 2013.

[47] Y. S. Weinstein, D. Chai, and N. Xie, "Improving ancilla states for quantum computation," *Quantum Information Processing*, vol. 15, no. 4, pp. 1445–1453, 2016.

[48] L. N. Gatti and J. García-López, "Geometría de estados discretos en computación cuántica," in *10th Andalusian Meeting on Discrete Mathematics*, La Línea de la Concepción (Cádiz, Spain), 2017.

[49] J. Lacalle and L. N. Gatti, "Extended lagrange's four-square theorem," *Journal of the European Mathematical Society*, 2018, (submitted).

[50] P. R. Giri and V. E. Korepin, "A review on quantum search algorithms," *Quantum Information Processing*, vol. 16, no. 12, p. 315, 2017.

[51] G.-L. Long, "Grover algorithm with zero theoretical failure rate," *Physical Review A*, vol. 64, no. 2, p. 022307, 2001.

[52] E. Grosswald, *Representations of integers as sums of squares.* Springer Science & Business Media, 2012.

[53] B. Giles and P. Selinger, "Exact synthesis of multiqubit clifford+t circuits," *Physical Review A*, vol. 87, no. 3, p. 032332, 2013.

[54] L. N. Gatti and J. Lacalle, "A model of discrete quantum computation," *Quantum Information Processing*, vol. 17, no. 8, pp. 1–18, 2018.

[55] J. L. de Lagrange, "Démonstration d'un théorème d'arithmétique," 1770.

[56] C. F. Gauss, *Disquisitiones arithmeticae.* Yale University Press, 1966.

[57] S. Ramanujan, "On the expression of a number in the form axˆ 2+ byˆ 2+ czˆ 2+ duˆ 2," in *Proc. Cambridge Philos. Soc.*, vol. 19, 1917, pp. 11–21.

[58] D. Ye, "Representations of integers by certain 2k-ary quadratic forms," *Journal of Number Theory*, vol. 179, pp. 50–64, 2017.

[59] I. S. Eum, D. H. Shin, and D. S. Yoon, "Representations by x12+ 2x22+ x32+ x42+ x1x3+ x1x4+ x2x4," *Journal of Number Theory*, vol. 131, no. 12, pp. 2376–2386, 2011.

[60] Z.-W. Sun, "A result similar to lagrange's theorem," *Journal of Number Theory*, vol. 162, pp. 190–211, 2016.

[61] J. Ju and B.-K. Oh, "Universal sums of generalized octagonal numbers," *Journal of Number Theory*, vol. 190, pp. 292–302, 2018.

[62] L. J. Mordell, "A new waring's problem with squares of linear forms," *The Quarterly Journal of Mathematics*, no. 1, pp. 276–288, 1930.

[63] Y.-C. Sun and Z.-W. Sun, "Some variants of lagrange's four squares theorem," *arXiv preprint arXiv:1605.03074*, 2016.

[64] T. W. Ching, "Lagrange's equation with one prime and three almost-primes," *Journal of Number Theory*, vol. 183, pp. 442–465, 2018.

[65] G. Harman and A. Kumchev, "On sums of squares of primes ii," *Journal of Number Theory*, vol. 130, no. 9, pp. 1969–2002, 2010.

[66] G. Chen, "On monochromatic sums of squares of primes," *Journal of Number Theory*, vol. 162, pp. 180–189, 2016.

[67] J. W. S. Cassels, *An introduction to the geometry of numbers.* Springer Science & Business Media, 2012.

[68] T.-W. J. Chou and G. E. Collins, "Algorithms for the solution of systems of linear diophantine equations," *SIAM Journal on computing*, vol. 11, no. 4, pp. 687–708, 1982.

[69] H. J. S. Smith, "Xv. on systems of linear indeterminate equations and congruences," *Philosophical transactions of the royal society of london*, no. 151, pp. 293–326, 1861.

[70] G. A. Jones and J. M. Jones, *Elementary number theory.* Springer Science & Business Media, 1998.

[71] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, p. 777, 1935.

[72] D. Bohm and B. J. Hiley, *The undivided universe: An ontological interpretation of quantum theory.* Routledge, 2006.

[73] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[74] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 28, no. 14, p. 938, 1972.

[75] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of bell's inequalities using time-varying analyzers," *Physical review letters*, vol. 49, no. 25, p. 1804, 1982.

[76] J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories," *Physical review D*, vol. 10, no. 2, p. 526, 1974.

[77] A. Aspect, "Bell's inequality test: more ideal than ever," *Nature*, vol. 398, no. 6724, pp. 189–190, 1999.

[78] G. Brassard, A. Broadbent, and A. Tapp, "Quantum pseudo-telepathy," *Foundations of Physics*, vol. 35, pp. 1877–1907, 2005.

[79] R. Jozsa, "Entanglement and quantum computation," in *The Geometric Universe*. Oxford University Press, 1998.

[80] M. E. Cuffaro, "On the significance of the gottesman–knill theorem," *The British Journal for the Philosophy of Science*, 2017.

[81] D. Gottesman, "The heisenberg representation of quantum computers. group22: Proceedings of the xxii international colloquium on group theoretical methods in physics," pp. 32–43, 1999.

[82] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Phys. Rev. A*, vol. 70, p. 052328, Nov 2004. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.70.052328

[83] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of modern physics*, vol. 81, no. 2, p. 865, 2009.

[84] R. Jozsa and N. Linden, "On the role of entanglement in quantum-computational speed-up," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 459, no. 2036, pp. 2011–2032, 2003.

[85] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Physical Review A*, vol. 62, no. 6, p. 062314, 2000.

[86] A. Ekert and P. L. Knight, "Entangled quantum systems and the schmidt decomposition," *American Journal of Physics*, vol. 63, no. 5, pp. 415–423, 1995.

[87] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, "Exact and asymptotic measures of multipartite pure-state entanglement," *Physical Review A*, vol. 63, no. 1, p. 012307, 2000.

[88] D. Greenberger, M. Horne, and A. Zeilinger, "Going beyond bell's theorem bell's theorem, quantum theory and conceptions of the universe ed m kafatos," *Dordrecht: Kluwer*, vol. 69, pp. 69–72, 1989.

[89] N. Gisin and H. Bechmann-Pasquinucci, "Bell inequality, bell states and maximally entangled states for n qubits," *Physics Letters A*, vol. 246, no. 1-2, pp. 1–6, 1998.

[90] D. Cruz, R. Fournier, F. Gremion, A. Jeannerot, K. Komagata, T. Tosic, J. Thiesbrummel, C. L. Chan, N. Macris, M.-A. Dupertuis *et al.*, "Efficient quantum algorithms for ghz and w states, and implementation on the ibm quantum computer," *Advanced Quantum Technologies*, vol. 2, no. 5-6, p. 1900015, 2019.

[91] V. Vedral, "Quantum entanglement," *Nature Physics*, vol. 10, no. 4, pp. 256–258, 2014.

[92] A. Borras, A. Plastino, J. Batle, C. Zander, M. Casas, and A. Plastino, "Multiqubit systems: highly entangled states and entanglement distribution," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 44, p. 13407, 2007.

[93] A. Higuchi and A. Sudbery, "How entangled can two couples get?" *Physics Letters A*, vol. 273, no. 4, pp. 213–217, 2000.

[94] S. Brierley and A. Higuchi, "On maximal entanglement between two pairs in four-qubit pure states," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 29, p. 8455, 2007.

[95] I. D. Brown, S. Stepney, A. Sudbery, and S. L. Braunstein, "Searching for highly entangled multi-qubit states," *Journal of Physics A: Mathematical and General*, vol. 38, no. 5, p. 1119, 2005.

[96] C. Zhang, Z.-W. Sun, X. Huang, and D.-Y. Long, "Three-party quantum summation without a trusted third party," *International Journal of Quantum Information*, vol. 13, no. 02, p. 1550011, 2015.

[97] Z. Sun, C. Zhang, P. Wang, J. Yu, Y. Zhang, and D. Long, "Multi-party quantum key agreement by an entangled six-qubit state," *International Journal of Theoretical Physics*, vol. 55, pp. 1920–1929, 2016.

[98] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, "Measurement-based quantum computation," *Nature Physics*, vol. 5, no. 1, pp. 19–26, 2009.

[99] I. B. Djordjevic, *Quantum Information Processing, Quantum Computing, and Quantum Error Correction: An Engineering Approach.* Academic Press, 2021.

[100] H. J. Briegel and R. Raussendorf, "Persistent entanglement in arrays of interacting particles," *Physical Review Letters*, vol. 86, no. 5, p. 910, 2001.

[101] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states," *Physical review letters*, vol. 69, no. 20, p. 2881, 1992.

[102] G. Rigolin, "Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement," *Physical Review A*, vol. 71, no. 3, p. 032303, 2005.

[103] J. Lee, H. Min, and S. D. Oh, "Multipartite entanglement for entanglement teleportation," *Physical Review A*, vol. 66, no. 5, p. 052318, 2002.

[104] V. Verma, N. Singh, and R. S. Singh, "Improvement on quantum teleportation of three and four qubit states using multi-qubit cluster states," *International Journal of Theoretical Physics*, vol. 60, pp. 3973–3981, 2021.

[105] P. Agrawal and A. Pati, "Perfect teleportation and superdense coding with w states," *Phys. Rev. A*, vol. 74, p. 062320, Dec 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.74.062320

[106] G. Rigolin, "Superdense coding using multipartite states," *arXiv preprint quant-ph/0407193*, 2004.

[107] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[108] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.

[109] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 339–354, 1998.

[110] D. R. Simon, "On the power of quantum computation," *SIAM journal on computing*, vol. 26, no. 5, pp. 1474–1483, 1997.

[111] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Physical review letters*, vol. 103, no. 15, p. 150502, 2009.

[112] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[113] D. Collins, K. Kim, and W. Holton, "Deutsch-jozsa algorithm as a test of quantum computation," *Physical Review A*, vol. 58, no. 3, p. R1633, 1998.

[114] N. Linden, H. Barjat, and R. Freeman, "An implementation of the deutsch–jozsa algorithm on a three-qubit nmr quantum computer," *Chemical Physics Letters*, vol. 296, no. 1-2, pp. 61–67, 1998.

[115] S. Gulde, M. Riebe, G. P. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, "Implementation of the deutsch–jozsa algorithm on an ion-trap quantum computer," *Nature*, vol. 421, no. 6918, pp. 48–50, 2003.

[116] Z. Li, J. Dai, S. Pan, W. Zhang, and J. Hu, "Synthesis of deutsch-jozsa circuits and verification by ibm q," *International Journal of Theoretical Physics*, vol. 59, pp. 1668–1678, 2020.

[117] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997.

[118] C. Zalka, "Grover's quantum searching algorithm is optimal," *Physical Review A*, vol. 60, no. 4, p. 2746, 1999.

[119] M. Fürer, "Solving np-complete problems with quantum search," in *LATIN 2008: Theoretical Informatics: 8th Latin American Symposium, Búzios, Brazil, April 7-11, 2008. Proceedings 8*. Springer, 2008, pp. 784–792.

[120] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck, "Estimating the cost of generic quantum pre-image attacks on sha-2 and sha-3," in *Selected Areas in Cryptography–SAC 2016: 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers*. Springer, 2017, pp. 317–337.

[121] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying grover's algorithm to aes: quantum resource estimates," in *Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings 7*. Springer, 2016, pp. 29–43.

[122] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing grover oracles for quantum key search on aes and lowmc," in *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30*. Springer, 2020, pp. 280–310.

[123] R. Anand, S. Maitra, A. Maitra, C. S. Mukherjee, and S. Mukhopadhyay, "Resource estimation of grovers-kind quantum cryptanalysis against fsr based symmetric ciphers," *Cryptology ePrint Archive*, 2020.

[124] S. Arunachalam, "Quantum algorithms and learning theory," Ph.D. dissertation, University of Amsterdam, 2018.

[125] C. Pronin, O. Maksimychev, A. Ostroukh, A. Volosova, and E. Matukhina, "Creating quantum circuits for training perceptron neural networks on the principles of grover's algorithm," in *2022 Systems Of Signals Generating And Processing In The Field Of On Board Communications*. IEEE, 2022, pp. 1–5.

[126] Y. Wang and P. S. Krstic, "Prospect of using grover's search in the noisy-intermediate-scale quantum-computer era," *Phys. Rev. A*, vol. 102, p. 042609, Oct 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.102.042609

[127] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. Nguyen, S. X. Ng, and L. Hanzo, "Quantum error correction protects quantum search algorithms against decoherence," *Scientific reports*, vol. 6, no. 1, p. 38095, 2016.

[128] S. Arunachalam and R. de Wolf, "Optimizing the number of gates in quantum search," *Quantum Information & Computation*, vol. 17, no. 3&4, pp. 251–261, 2017.

[129] L. N. Gatti Dorpich, "Análisis de un modelo discreto para computación cuántica," 2016.

[130] F. Chamizo and J. Jiménez-Urroz, "Extendable orthogonal sets of integral vectors," *Research in the Mathematical Sciences*, vol. 9, no. 4, p. 59, 2022.

[131] L. P. Martınez, "1er coloquio del departamento de matemáticas."

[132] G. Jaeger, *Quantum information*. Springer, 2007.