USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Trabajo Fin de Grado

Computación Cuántica. Principios Matemáticos y Aplicaciones

Alfredo Chavert Sancho

Julio, 2025

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

GRADO DE MATEMÁTICAS

Trabajo Fin de Grado

Computación Cuántica. Principios Matemáticos y Aplicaciones

Alfredo Chavert Sancho

Julio, 2025

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Análise Matemática
Título: Computación cuántica. Principios matemáticos e aplicacións
Breve descrición do contido
Por unha banda, trátase de describir os principios matemáticos sobre os que se basea a computación cuántica e, por outra banda, analizar algunha aplicación práctica de interese.
Recomendacións
Outras observacións

Índice

Resumen

Este trabajo estudia las bases de la Computación Cuántica de forma íntegramente matemática, abstrayéndose de los sistemas físicos reales detrás de esta idealización. En primer lugar, se estudian los fundamentos de la Mecánica Cuántica, explorando conceptos y propiedades de los espacios de Hilbert sobre el cuerpo de los números complejos. A continuación, se definen los conceptos de cúbit y p-cúbit, así como las puertas lógicas cuánticas que actúan sobre ellos. Por último, se desarrollará una serie de algoritmos importantes con aplicaciones concretas que demuestran el interés por este tipo de lógica.

El objetivo del trabajo es ser una introducción, desde los conceptos trabajados en el Grado de Matemáticas, al mundo de la Computación Cuántica sin requerir conocimientos previos sobre Física, de forma que dé un acceso más sencillo al entendimiento de algoritmos cuánticos o a su desarrollo.

Abstract

This report studies the foundations of Quantum Computing in a fully mathematical manner, abstracting from the underlying real physical systems. Firstly, we study the fundamentals of Quantum Physics, exploring concepts and properties of Hilbert spaces over the field of complex numbers. Next, we define the concepts of qubit and p-qubit, along with the quantum logic gates that operate on them. Finally, we develop some important algorithms with specific applications that show the relevance of this kind of logic.

The aim of this document is to serve as an introduction, based on concepts covered by the Mathematics undergraduate program, to the world of Quantum Computing, without requiring any previous knowledge of Physics, in doing so, it seeks to present easier access to understanding or developing quantum algorithms.

Introducción

La computación cuántica es un área de investigación que ha crecido en popularidad en las últimas décadas. La introducción de propiedades cuánticas, como la superposición o el entrelazado, han permitido desarrollar algoritmos con costes computacionales significativamente menores que sus análogos clásicos, lo cual es de gran interés en un mundo donde la cantidad de datos que se procesan no deja de aumentar.

Aunque los comienzos de la mecánica cuántica se remontan a principios del siglo XX, la primera idea de crear un nuevo tipo de computación, basado en estas leyes, se le atribuye a Feynman [Alsing et al., 2024], a principios de los ochenta, motivado por la dificultad de los ordenadores clásicos para simular sistemas cuánticos de forma eficiente.

En los años siguientes, se empezaron a desarrollar las bases de esta nueva disciplina, por ejemplo, Deutsch [Deutsch and Penrose, 1985] formalizó los procesos y circuitos cuánticos, dando los primeros pasos en la teoría de la información cuántica. En los noventa, surgieron una gran cantidad de algoritmos y aplicaciones, sirviéndose de las nuevas reglas que introdujo la cuántica. Un ejemplo muy relevante es el algoritmo de factorización en números primos de Shor [Shor, 1994, Shor, 1997], que presenta una mejora exponencial respecto al mejor algoritmo de factorización clásico. Aunque aún no disponemos de dispositivos que puedan ejecutarlo en grandes números, se espera que este algoritmo pueda acabar rompiendo el sistema criptográfico de clave pública (RSA) en las próximas décadas, sobre el cual se basa la seguridad de las comunicaciones actuales. Esto también ha motivado recientemente el desarrollo de nuevos tipos de seguridad informática, basadas en la criptografía y comunicaciones cuánticas [Caleffi and Cacciapuoti, 2020, Bassoli et al., 2021].

En la actualidad, la computación cuántica se encuentra en la era NISQ (Noisy Intermediate-Scale Quantum) [Preskill, 2018]. Disponemos de ordenadores cuánticos *ruidosos*, sobre los que no se tiene un control perfecto sobre el estado de los cúbits y, por tanto, se obtendrán resultados con mucho ruido en la ejecución de los algoritmos (ruido entendido como resultados arbitrarios no predichos por el algoritmo). Una analogía clásica de esto sería tener bombillas que se funden con facilidad, a veces se apagarán sin habérselo ordenado y comprometerán el resultado de los

algoritmos que estemos ejecutando en ellas. La *escala intermedia* se refiere al número de cúbits, pues se predice que en los próximos años podremos disponer de computadores con hasta unos pocos centenares de estos.

En este trabajo desarrollaremos con detalle la base matemática de esta disciplina tan innovadora, que trabaja con numerosos campos como el álgebra lineal, análisis, probabilidad o teoría de grupos. Comenzaremos con una introducción a los fundamentos de la mecánica cuántica, donde se establece el marco principal de trabajo: los espacios de Hilbert de dimensión finita sobre el cuerpo de los números complejos. A continuación, introduciremos conceptos como el cúbit, las puertas o los circuitos cuánticos empleando únicamente el formalismo matemático y dejando a un lado los sistemas físicos reales que hay en los ordenadores cuánticos. Finalmente, estudiaremos algunos algoritmos cuánticos de gran interés y, en particular, nos introduciremos brevemente en el algoritmo de resolución de sistemas lineales HHL [Vazquez et al., 2022].

Capítulo 1

Fundamentos Matemáticos de la Computación Cuántica

En este capítulo se recopilan una serie de definiciones y resultados que nos permitirán establecer una formulación teórica, puramente matemática, de la computación cuántica [Bellac, 2006, Scherer, 2019, Nielsen and Chuang, 2010, Tojo et al., 2023].

1.1. Bases de la Mecánica Cuántica

Empezaremos estudiando el concepto teórico más esencial para la mecánica cuántica, los espacios de Hilbert de dimensión finita sobre el cuerpo $\mathbb{C}$.

1.1.1. Espacios de Hilbert sobre $\mathbb{C}$

Consideremos $\mathbb{H}$ un espacio vectorial sobre el cuerpo $\mathbb{C}$ y denotaremos sus elementos con la notación de Dirac: $|\psi\rangle$, llamado **"ket"**. Tenemos en $\mathbb{H}$ la operación interna **suma**:

$$\begin{aligned} + : \mathbb{H} \times \mathbb{H} &\longrightarrow \mathbb{H} \\ (|\psi\rangle, |\varphi\rangle) &\mapsto |\psi\rangle + |\varphi\rangle , \end{aligned}$$

y la operación externa **producto por escalar**:

$$\begin{aligned} \cdot : \mathbb{C} \times \mathbb{H} &\longrightarrow \mathbb{H} \\ (\alpha, |\varphi\rangle) &\mapsto \alpha \cdot |\psi\rangle , \end{aligned}$$

aunque prescindiremos de escribir explícitamente el punto. Como suponemos que $\mathbb{H}$ es un espacio vectorial, la operación suma cumple las siguientes propiedades:

1. Conmutativa: $|\psi\rangle + |\varphi\rangle = |\varphi\rangle + |\psi\rangle\,;\ \forall\, |\psi\rangle, |\varphi\rangle \in \mathbb{H}$.
2. Asociativa: $(|\psi\rangle + |\varphi\rangle) + |\phi\rangle = |\varphi\rangle + (|\psi\rangle + |\phi\rangle);\ \forall\, |\psi\rangle, |\varphi\rangle, |\phi\rangle \in \mathbb{H}$.
3. Elemento neutro: $\exists\ 0 \in \mathbb{H}$ t.q. $|\psi\rangle + 0 = 0 + |\psi\rangle = |\psi\rangle\,,\ \forall\, |\psi\rangle \in \mathbb{H}$.
4. Elemento opuesto: $\forall\, |\psi\rangle \in \mathbb{H}\ \exists\ |-\psi\rangle \in \mathbb{H}$ t.q. $|\psi\rangle + |-\psi\rangle = |-\psi\rangle + |\psi\rangle = 0$.

Además, el producto por escalar verifica las siguientes propiedades:

1. Asociativa: $\alpha(\beta\,|\psi\rangle) = (\alpha\beta)\,|\psi\rangle\,;\ \forall\, |\psi\rangle \in \mathbb{H},\ \forall \alpha\beta \in \mathbb{C}$.
2. Elemento neutro: $1 \in \mathbb{C}$ cumple que $1\,|\psi\rangle = |\psi\rangle\,,\ \forall\, |\psi\rangle \in \mathbb{H}$.
3. Distributiva respecto a la suma: $\alpha(|\psi\rangle + |\varphi\rangle) = \alpha\,|\psi\rangle + \alpha\,|\varphi\rangle\,;\ \forall\, |\psi\rangle, |\varphi\rangle \in \mathbb{H},\ \forall \alpha \in \mathbb{C}$.
4. Distributiva respecto al producto: $(\alpha + \beta)\,|\psi\rangle = \alpha\,|\psi\rangle + \beta\,|\psi\rangle\,;\ \forall\, |\psi\rangle \in \mathbb{H},\ \forall \alpha, \beta \in \mathbb{C}$.

Emplearemos la notación $|\alpha\psi\rangle \equiv \alpha\,|\psi\rangle$, con $\alpha \in \mathbb{C}$ y $|\psi\rangle \in \mathbb{H}$, para referirnos al producto por un escalar.

Definición 1.1. Un **producto escalar hermítico** es una aplicación:

$$\begin{aligned} \langle\cdot|\cdot\rangle : \mathbb{H} \times \mathbb{H} &\longrightarrow \mathbb{C} \\ (|\psi\rangle, |\varphi\rangle) &\mapsto \langle\psi|\varphi\rangle\,, \end{aligned}$$

que cumple las siguientes propiedades:

1. Linealidad: $\langle\psi|\lambda_1\varphi_1 + \lambda_2\varphi_2\rangle = \lambda_1\,\langle\psi|\varphi_1\rangle + \lambda_2\,\langle\psi|\varphi_2\rangle\,;\ \forall\, |\psi\rangle, |\varphi_1\rangle\,|\varphi_2\rangle \in \mathbb{H},\ \lambda_1, \lambda_2 \in \mathbb{C}$.
2. Hermiticidad: $\langle\psi|\varphi\rangle = \langle\varphi|\psi\rangle^*\,;\ \forall\, |\psi\rangle, |\varphi\rangle \in \mathbb{H}$, denotando por * el complejo conjugado.
3. Definido positivo: $\langle\psi|\psi\rangle \geq 0,\ \forall \psi \in \psi$ y $\langle\psi|\psi\rangle = 0 \Leftrightarrow |\psi\rangle = 0$.

Proposición 1.2. *El producto escalar hermítico definido anteriormente cumple la propiedad de antilinealidad:*

$$\langle\lambda_1\psi_1 + \lambda_2\psi_2|\varphi\rangle = \lambda_1^*\,\langle\psi_1|\varphi\rangle + \lambda_2^*\,\langle\psi_2|\varphi\rangle\,;\ \forall\, |\psi_1\rangle, |\psi_2\rangle, |\varphi\rangle \in \mathbb{H},\ \forall \lambda_1, \lambda_2 \in \mathbb{C}.$$

Demostración. Basta aplicar primero la hermiticidad, la linealidad y de nuevo la hermiticidad a ambos términos:

$$\begin{aligned} \langle\lambda_1\psi_1 + \lambda_2\psi_2|\varphi\rangle &= (\langle\varphi|\lambda_1\psi_1 + \lambda_2\psi_2\rangle)^* \\ &= (\lambda_1\,\langle\varphi|\psi_1\rangle + \lambda_2\,\langle\varphi|\psi_2\rangle)^* \\ &= \lambda_1^*\,\langle\varphi|\psi_1\rangle^* + \lambda_2^*\,\langle\varphi|\psi_2\rangle^* = \lambda_1^*\,\langle\psi_1|\varphi\rangle + \lambda_2^*\,\langle\psi_2|\varphi\rangle\,. \end{aligned}$$

□

Definición 1.3. Se define la **norma** del producto escalar hermítico como la aplicación:

$$\begin{aligned} \|\cdot\| : \mathbb{H} &\longrightarrow \mathbb{R} \\ |\psi\rangle &\mapsto \|\psi\| = \sqrt{\langle\psi|\psi\rangle}. \end{aligned}$$

Para comprobar que está bien definida, supongamos que $\langle\psi|\psi\rangle = a + ib \in \mathbb{C}$, por la propiedad hermítica se tiene que $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle^* \Leftrightarrow a + ib = a - ib$ y, por tanto, $b = 0$ y $\langle\psi|\psi\rangle = a \in \mathbb{R}$.

Proposición 1.4 (Desigualdad de Schwarz)**.** *Dados* $|\psi\rangle, |\varphi\rangle \in \mathbb{H}$. *Entonces:*

$$|\langle\psi|\varphi\rangle|^2 \leq \langle\psi|\psi\rangle\langle\varphi|\varphi\rangle = \|\psi\|^2\|\varphi\|^2. \tag{1.1}$$

Además:

$$|\langle\psi|\varphi\rangle|^2 = \|\psi\|^2\|\varphi\|^2 \Leftrightarrow \exists\ \alpha \in \mathbb{C}\ \ t.q.\ \ |\psi\rangle = \alpha\,|\varphi\rangle\,. \tag{1.2}$$

Demostración. Si $\langle\psi|\varphi\rangle = 0$, el resultado es directo. Supongamos que $\langle\psi|\varphi\rangle \neq 0$ y sea $\lambda \in \mathbb{C}$, como el producto es definido positivo:

$$\langle\varphi - \lambda\psi|\varphi - \lambda\psi\rangle \geq 0.$$

Aplicando la linealidad y antilinealidad del producto:

$$\begin{aligned} \langle\varphi - \lambda\psi|\varphi - \lambda\psi\rangle &= \langle\varphi - \lambda\psi|\varphi\rangle - \lambda\langle\varphi - \lambda\psi|\psi\rangle = \langle\varphi|\varphi\rangle - \lambda^*\langle\psi|\varphi\rangle - \lambda\langle\varphi|\psi\rangle - \lambda\lambda^*\langle\psi|\psi\rangle \\ &= \|\varphi\|^2 - \lambda^*\langle\psi|\varphi\rangle - \lambda\langle\varphi|\psi\rangle - |\lambda|^2\|\psi\|^2 \geq 0. \end{aligned}$$

Como esto se cumple para todo $\lambda \in \mathbb{C}$, podemos escoger en particular:

$$\lambda = \frac{\|\varphi\|^2}{\langle\varphi|\psi\rangle},\ \lambda^* = \frac{\|\varphi\|^2}{\langle\psi|\varphi\rangle}.$$

Tenemos entonces que $\lambda^*\langle\psi|\varphi\rangle = \lambda\langle\varphi|\psi\rangle = \|\varphi\|^2$ y la desigualdad anterior queda como:

$$\|\varphi\|^2 - 2\|\varphi^2\| + \frac{\|\varphi\|^4\|\psi\|^2}{|\langle\psi|\varphi\rangle|^2} = -\|\varphi^2\| + \frac{\|\varphi\|^4\|\psi\|^2}{|\langle\psi|\varphi\rangle|^2} \geq 0.$$

Si $\|\varphi\| = 0$, entonces la desigualdad se cumple trivialmente. Supongamos entonces que $\|\varphi\| \neq 0$, si dividimos por $\|\varphi\|^2$, obtenemos la desigualdad de Schwarz:

$$-1 + \frac{\|\varphi\|^2\|\psi\|^2}{|\langle\psi|\varphi\rangle|^2} \geq 0 \Leftrightarrow |\langle\psi|\varphi\rangle|^2 \leq \|\varphi\|^2\|\psi\|^2.$$

Supongamos ahora que $\exists\ \alpha \in \mathbb{C}$ tal que $|\psi\rangle = \alpha\,|\varphi\rangle$, tenemos que $\|\psi\|^2 = |\alpha|^2\|\varphi\|^2$, entonces:

$$|\langle\psi|\varphi\rangle|^2 = |\alpha|^2\|\varphi\|^4 = \|\psi\|^2\|\varphi\|^2.$$

Supongamos que tenemos la igualdad $|\langle\psi|\varphi\rangle|^2 = \|\psi\|^2\|\varphi\|^2$, con $\|\psi\| \neq 0$ y $\|\varphi\| \neq 0$, entonces $\|\psi\|^2 = \frac{|\langle\psi|\varphi\rangle|^2}{\|\varphi\|^2} = \frac{|\langle\psi|\varphi\rangle|^2}{\|\varphi\|^4}\|\varphi\|^2$. Consideremos ahora el número complejo:

$$\alpha = \frac{\langle\varphi|\psi\rangle}{\|\varphi\|^2} \in \mathbb{C},$$

tenemos que:

$$|\alpha\varphi\rangle = \alpha\,|\varphi\rangle = \frac{\langle\varphi|\psi\rangle}{\|\varphi\|^2}\,|\varphi\rangle \Rightarrow \langle\psi|\alpha\varphi\rangle = \frac{\langle\varphi|\psi\rangle\,\langle\psi|\varphi\rangle}{\|\varphi\|^2} = \frac{|\,\langle\psi|\varphi\rangle\,|^2}{\|\varphi\|^2} = \|\psi\|^2 = \langle\psi|\psi\rangle$$
$$\Rightarrow 0 = \langle\psi|\psi\rangle - \langle\psi|\alpha\varphi\rangle = \langle\psi|\psi - \alpha\varphi\rangle \Rightarrow |\psi - \alpha\varphi\rangle = 0 \in \mathbb{H} \Rightarrow |\psi\rangle = \alpha\,|\varphi\rangle\,.$$

□

Definición 1.5. Definimos un **espacio de Hilbert finito sobre** $\mathbb{C}$ como un espacio vectorial $\mathbb{H}$, sobre el cuerpo $\mathbb{C}$, de dimensión finita, $\dim\mathbb{H} = N \in \mathbb{N}$, con el producto escalar hermítico. Denotaremos una base ortonormal del espacio de la siguiente forma:

$$\{|n\rangle\}_{n=1}^{N} = \{|1\rangle\,, |2\rangle\,, \ldots, |N\rangle\}. \tag{1.3}$$

Por ser ortonormal, tenemos que son ortogonales con respecto al producto escalar:

$$\langle n|m\rangle = \delta_{nm},\ \forall n, m \in \{1, 2, \ldots, N\}, \tag{1.4}$$

y es un conjunto generador del espacio vectorial:

$$\forall\,|\psi\rangle \in \mathbb{H}\ \ \exists\{c_n\}_{n=1}^{N} \subset \mathbb{C} \text{ t.q. } |\psi\rangle = \sum_{i=0}^{N} c_n\,|n\rangle\,. \tag{1.5}$$

Al conjunto de coeficientes complejos $\{c_n\}_{n=1}^{N}$ se le llamará **coordenadas** del vector $|\psi\rangle$. Es trivial, por la ortogonalidad de la base, comprobar que si $|\psi\rangle = \sum_{i=0}^{N} c_n\,|n\rangle$, entonces:

$$\langle m|\psi\rangle = \left\langle m\middle|\sum_{i=0}^{N} c_n\,|n\rangle\right\rangle = \sum_{i=0}^{N} c_n\,\langle m|n\rangle = \sum_{i=0}^{N} c_n\delta_{mn} = c_m,\ \forall m \in \{1, \ldots, N\}. \tag{1.6}$$

Además, podemos expresar el producto escalar hermítico en función de estos coeficientes; consideremos $|\psi\rangle\,, |\varphi\rangle \in \mathbb{H}$ tales que:

$$|\psi\rangle = \sum_{n=0}^{N} \alpha_n\,|n\rangle \ \text{ y } \ |\varphi\rangle = \sum_{m=0}^{N} \beta_m\,|m\rangle\,,$$

entonces:

$$\begin{aligned}\langle\psi|\varphi\rangle &= \left\langle \sum_{n=0}^{N} \alpha_n n \middle| \sum_{m=0}^{N} \beta_m m \right\rangle \\ &= \sum_{m=0}^{N} \beta_m \left\langle \sum_{n=0}^{N} \alpha_n n \middle| m \right\rangle \\ &= \sum_{m=0}^{N} \beta_m \sum_{n=0}^{N} \alpha_n^* \langle n|m\rangle \\ &= \sum_{m=0}^{N}\sum_{n=0}^{N} \alpha_n^* \beta_m \delta_{n,m} = \sum_{n=0}^{N} \alpha_n^* \beta_n.\end{aligned}$$

Por tanto:

$$\langle\psi|\varphi\rangle = \sum_{n=0}^{N} \alpha_n^* \beta_n. \tag{1.7}$$

Empleando esta expresión, podemos escribir la norma de un elemento $|\psi\rangle = \sum_{n=0}^{N} \alpha_n |n\rangle \in \mathbb{H}$ como:

$$\|\psi\|^2 = \sum_{n=0}^{N} \alpha_n^* \alpha_n = \sum_{n=0}^{N} |\alpha_n|^2 \tag{1.8}$$

1.1.2. Espacio Dual

Definición 1.6. Definimos el **espacio dual** de $\mathbb{H}$, denotado por $\mathbb{H}^*$, al espacio de funciones lineales de $\mathbb{H}$ en $\mathbb{C}$, $\mathbb{H}^* = \mathcal{L}(\mathbb{H}, \mathbb{C})$. Definimos en el espacio dual la operación suma:

$$\begin{aligned} + : \mathbb{H}^* \times \mathbb{H}^* &\longrightarrow \mathbb{H}^* \\ (f, g) &\mapsto f + g, \end{aligned}$$

tal que $(f+g)(|\psi\rangle) = f(|\psi\rangle) + g(|\psi\rangle),\ \forall\, |\psi\rangle \in \mathbb{H}$, y la operación producto por escalar:

$$\begin{aligned} \cdot : \mathbb{C} \times \mathbb{H}^* &\longrightarrow \mathbb{H}^* \\ (\lambda, g) &\mapsto \lambda \cdot g \equiv \lambda g, \end{aligned}$$

tal que $(\lambda g)(|\psi\rangle) = \lambda g(|\psi\rangle)$. Con estas operaciones podemos comprobar que $\mathbb{H}^*$ también es un espacio vectorial.

Proposición 1.7. *El espacio dual $\mathbb{H}^*$ anteriormente definido, con las operaciones suma y producto por escalar, es un espacio vectorial sobre $\mathbb{C}$ isomorfo a $\mathbb{H}$.*

Demostración. Probemos primero que la suma está bien definida y cumple las propiedades del espacio vectorial, sean $f, g, h \in \mathbb{H}^*$ arbitrarias:

1. Conmutatividad: como la imagen de f y g está en $\mathbb{C}$, tenemos que $(f+g)(|\psi\rangle) = \\ = f(|\psi\rangle) + g(|\psi\rangle) = g(|\psi\rangle) + f(|\psi\rangle) = (g+f)(|\psi\rangle),\ \forall\, |\psi\rangle \in \mathbb{H}$.
2. Asociatividad: $\big[(f+g)+h\big](|\psi\rangle) = (f+g)(|\psi\rangle) + h(|\psi\rangle) = \big[g(|\psi\rangle) + f(|\psi\rangle)\big] + h(|\psi\rangle) = \\ = f(|\psi\rangle) + \big[g(|\psi\rangle) + h(|\psi\rangle)\big] = f(|\psi\rangle) + (g+h)(|\psi\rangle) = \big[f+(g+h)\big](|\psi\rangle),\ \forall\, |\psi\rangle \in \mathbb{H}$
3. Elemento neutro: definiendo la función $e(|\psi\rangle) = 0,\ \forall\, |\psi\rangle \in \mathbb{H}$ (función nula) cumple que $(e+f)(|\psi\rangle) = e(|\psi\rangle) + f(|\psi\rangle) = 0 + f(|\psi\rangle) = f(|\psi\rangle)$ por lo que $e + f = f$, por la conmutatividad se tiene que $e + f = f + e = f$.
4. Elemento opuesto: dado f, se puede definir la función $\hat{f}(|\psi\rangle) = -f(|\psi\rangle),\ \forall\, |\psi\rangle \in \mathbb{H}$ de forma que cumple que $(f+\hat{f})(|\psi\rangle) = f(|\psi\rangle) + \hat{f}(|\psi\rangle) = f(|\psi\rangle) - f(|\psi\rangle) = 0 = e(|\psi\rangle),\ \forall\, |\psi\rangle \in \mathbb{H}$. Por tanto, se tiene que $\hat{f}$ es el elemento opuesto de f, ya que $f + \hat{f} = \hat{f} + f = e$.

En segundo lugar, probaremos las propiedades del producto por un escalar, sean $f, g \in \mathbb{H}^*$ y $\alpha, \beta \in \mathbb{C}$:

1. Asociatividad: $\alpha(\beta f(|\psi\rangle)) = (\alpha\beta) f(|\psi\rangle)),\ \forall\, |\psi\rangle \in \mathbb{H}$, por tanto, $\alpha(\beta f) = (\alpha\beta) f$.
2. Elemento neutro: considerando que $1 \in \mathbb{C}$, como $1 f(|\psi\rangle) = f(|\psi\rangle),\ \forall\, |\psi\rangle \in \mathbb{H}$ tenemos que $1 f = f$.
3. Las propiedades distributivas también son triviales al provenir de las propiedades del producto en $\mathbb{C}$.

Definamos ahora la siguiente aplicación entre $\mathbb{H}$ y $\mathbb{H}^*$:

$$\begin{aligned} \theta : \mathbb{H} &\longrightarrow \mathbb{H}^* \\ |\psi\rangle &\mapsto \langle\psi| \,, \end{aligned}$$

denotando por $\langle\psi|$ al elemento de $\mathbb{H}^* = \mathcal{L}(\mathbb{H}, \mathbb{C})$ definido como:

$$\begin{aligned} \langle\psi| : \mathbb{H} &\longrightarrow \mathbb{C} \\ |\varphi\rangle &\mapsto \langle\psi|\varphi\rangle \,. \end{aligned}$$

Por la linealidad del producto escalar 1.1, sean $|\varphi\rangle, |\phi\rangle \in \mathbb{H}$:

$$\theta(\lambda_1 |\varphi\rangle + \lambda_2 |\phi\rangle) = \langle\psi| (\lambda_1 |\varphi\rangle + \lambda_2 |\phi\rangle) = \lambda_1 \langle\psi|\varphi\rangle + \lambda_2 \langle\psi|\phi\rangle = \lambda_1 \theta(|\varphi\rangle) + \lambda_2 \theta(|\phi\rangle). \quad (1.9)$$

Por tanto, θ es una aplicación lineal. Comprobemos que la aplicación θ así definida es un isomorfismo:

1. Inyectividad: dados $|\psi\rangle, |\phi\rangle \in \mathbb{H}$, con $\theta(|\psi\rangle) = \theta(|\phi\rangle)$, es decir, $\langle\psi| = \langle\phi|$. Tenemos que $\langle\phi|\psi\rangle = \langle\psi|\psi\rangle \in \mathbb{R}$ y $\langle\psi|\phi\rangle = \langle\phi|\phi\rangle \in \mathbb{R}$, como $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle = \|\psi\|^2 = \|\phi\|^2$ se verifica trivialmente la igualdad de Schwarz, entonces $\exists\ \alpha \in \mathbb{C}$ tal que $|\psi\rangle = \alpha\,|\phi\rangle$. Sin embargo, como $\alpha = \langle\psi|\phi\rangle \in \mathbb{R}$ y $\|\psi\| = \|\phi\|$ se tiene que $\alpha = 1 \in \mathbb{R}$, es decir, $|\psi\rangle = |\phi\rangle$.

2. Sobreyectividad: dada $\sigma \in \mathbb{H}^*$, σ es una aplicación lineal de $\mathbb{H}$ en $\mathbb{C}$, por tanto, dado un $|\psi\rangle = \sum_{n=1}^{N} c_n\,|n\rangle \in \mathbb{H}$ arbitrario, se tiene que:

$$\sigma(|\psi\rangle) = \sigma\Big(\sum_{n=1}^{N} c_n\,|n\rangle\Big) = \sum_{n=1}^{N} c_n\sigma(|n\rangle) = \sum_{n=1}^{N} c_n y_n^*,$$

siendo $y_n^* = \sigma(|n\rangle) \in \mathbb{C}$, $\forall n \in \{1,\dots,N\}$. Consideremos el elemento $\phi \in \mathbb{N}$ con coordenadas $\{y_n\}_{n=1}^{N}$, es decir, $|\phi\rangle = \sum_{n=1}^{N} y_n\,|n\rangle$, se tiene que $\theta(|\phi\rangle) = \langle\phi|$ es una aplicación lineal de $\mathbb{H}^*$ que verifica:

$$\langle\phi|\psi\rangle = \sum_{n=0}^{N} y_n^* c_n = \sigma(|\psi\rangle),\ \forall\,|\psi\rangle = \sum_{n=1}^{N} c_n\,|n\rangle \in \mathbb{H},$$

es decir, $\exists\ |\phi\rangle \in \mathbb{H}$ tal que $\sigma = \langle\phi| = \theta(|\phi\rangle)$.

Como θ es inyectiva y sobreyectiva, es biyectiva y, por tanto, tenemos un isomorfismo de espacios vectoriales entre $\mathbb{H}$ y $\mathbb{H}^*$. □

Definición 1.8. Denominaremos al isomorfismo entre $\mathbb{H}$ y $\mathbb{H}^*$ como **conjugación hermítica**, "†". Como se vio anteriormente, todo elemento del espacio hermítico $|\psi\rangle \in \mathbb{H}$ tiene un vector dual asociado llamado conjugado hermítico que se escribirá, según la notación de Dirac, como un **"bra"**,$(|\psi\rangle)^\dagger = \langle\psi| \in \mathbb{H}^*$.

Proposición 1.9. *Dado* $\{|n\rangle\}_{n=1}^{N} \subset \mathbb{H}$ *una base ortonormal de* $\mathbb{H}$ *y* $|\psi\rangle = \sum_{n=1}^{N} c_n\,|n\rangle \in \mathbb{H}$, *entonces:*

$$\langle\psi| = (|\psi\rangle)^\dagger = \sum_{n=1}^{N} c_n^*\,\langle n|\,.$$

Demostración. Tenemos que $|\psi\rangle = \sum_{n=1}^{N} c_n\,|n\rangle = \Big|\sum_{n=1}^{N} c_n n\Big\rangle$, por tanto, su conjugado hermítico será:

$$\langle\psi| = \left(\left|\sum_{n=1}^{N} c_n n\right\rangle\right)^\dagger = \left\langle\sum_{n=1}^{N} c_n n\right|.$$

Dado un $|\phi\rangle \in \mathbb{H}$ arbitrario, el vector dual de $|\psi\rangle$, por la propiedad antilineal del producto escalar hermítico y por la distributiva en el espacio dual, actuará sobre este de la siguiente forma:

$$\langle\psi|\phi\rangle = \left\langle\sum_{n=1}^{N} c_n n\middle|\phi\right\rangle = \sum_{n=1}^{N} c_n^*\,\langle n|\phi\rangle = \Big(\sum_{n=1}^{N} c_n^*\,\langle n|\Big)|\phi\rangle$$

□

Observación 1.10. Una consecuencia directa de 1.9 es que, dada una base ortonormal del espacio hermítico $\{|n\rangle\}_{n=1}^{N} \subset \mathbb{H}$, el conjunto de vectores duales de los anteriores, $\{\langle n|\}_{n=1}^{N} \subset \mathbb{H}^*$, es una base ortonormal del espacio dual.

Observación 1.11. Si consideramos los estados del espacio de Hilbert con notación matricial respecto a una base ortonormal $\{n\}_{n=1}^{N} \subset \mathbb{H}$:

$$|\psi\rangle = \sum_{n=1}^{N} c_n |n\rangle = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{pmatrix},$$

podemos expresar su vector dual como el transpuesto conjugado:

$$\langle\psi| = \sum_{n=1}^{N} c_n^* \langle n| = \begin{pmatrix} c_1^* & c_2^* & \dots & c_N^* \end{pmatrix}.$$

De esta forma, dados $|\psi\rangle = \sum_{n=1}^{N} c_n |n\rangle$ y $|\phi\rangle = \sum_{n=1}^{N} d_n |n\rangle$, se puede comprobar que el producto escalar coincide con la siguiente operación entre los vectores:

$$\langle\psi|\phi\rangle = \sum_{n=1}^{N} c_n^* d_n = \begin{pmatrix} c_1^* & c_2^* & \dots & c_N^* \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_N \end{pmatrix}. \tag{1.10}$$

1.1.3. Operadores lineales. Operadores Hermíticos y Unitarios

Definición 1.12. Definimos un **operador lineal en** $\mathbb{H}$ como una aplicación de la forma:

$$\begin{aligned} A : \mathbb{H} &\longrightarrow \mathbb{H} \\ |\psi\rangle &\mapsto A(|\psi\rangle) \equiv |A\psi\rangle, \end{aligned}$$

que cumple la condición de linealidad:

$$|A(\psi + \lambda\varphi)\rangle = |A\psi\rangle + \lambda |A\varphi\rangle \,;\ \forall |\psi\rangle\, |\varphi\rangle \in \mathbb{H}, \forall \lambda \in \mathbb{C}. \tag{1.11}$$

Observación 1.13. Consideremos $|\psi\rangle = \sum_{n=1}^{N} c_n |n\rangle$, entonces, la imagen de este elemento será:

$$|A\psi\rangle = \sum_{n=1}^{N} c_n |An\rangle \in \mathbb{H},$$

que, a su vez, se podrá expresar como:

$$|A\psi\rangle = \sum_{m=1}^{N} d_m |m\rangle.$$

Por tanto, se tiene la siguiente igualdad:

$$\sum_{n=1}^{N} c_n \left|An\right\rangle = \sum_{m=1}^{N} d_m \left|m\right\rangle .$$

Consideremos ahora un elemento arbitrario de la base $|l\rangle$ y hagamos el producto escalar por él en ambos lados de la ecuación:

$$\sum_{n=1}^{N} c_n \left\langle l|An\right\rangle = \sum_{m=1}^{N} d_m \left\langle l|m\right\rangle = \sum_{m=1}^{N} d_m \delta_{l,m} = d_l.$$

Definiendo ahora el **elemento de matriz de A en la base** $\{n\}_{n=1}^{N}$ como $A_{ln} = \langle l|An\rangle$. Se tiene que:

$$d_l = \sum_{n=1}^{N} A_{ln} c_n, \tag{1.12}$$

que se puede deducir de la representación matricial del operador:

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_N \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1N} \\ A_{21} & A_{22} & \cdots & A_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ A_{N1} & \cdots & \cdots & A_{NN} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{pmatrix}. \tag{1.13}$$

Notación 1.14. Es habitual denotar la aplicación de un operador escalar a un elemento del espacio vectorial como $|A\psi\rangle \equiv A\left|\psi\right\rangle$ y al producto escalar por otro elemento como $\langle\phi|A\psi\rangle \equiv \langle\phi|\, A\left|\psi\right\rangle$.

Definición 1.15. Dados dos elementos $\left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathbb{H}$, definimos el **producto de externo de** $|\psi\rangle$ **por** $|\phi\rangle$ al operador lineal $P_{\psi\varphi}$ tal que:

$$\begin{aligned} P_{\psi\varphi} : \mathbb{H} &\longrightarrow \mathbb{H} \\ \left|\phi\right\rangle &\mapsto P_{\psi\varphi}\left|\phi\right\rangle := \left\langle\varphi|\phi\right\rangle \left|\psi\right\rangle . \end{aligned}$$

Su representación en la notación de Dirac es:

$$P_{\psi\varphi} \equiv \left|\psi\right\rangle \left\langle\varphi\right| . \tag{1.14}$$

Observación 1.16. Podemos también representar el producto externo matricialmente, sean $\left|\psi\right\rangle = \sum_{n=1}^{N} a_n \left|n\right\rangle, \left|\varphi\right\rangle = \sum_{m=1}^{N} b_m \left|m\right\rangle \in \mathbb{H}$:

$$\left|\psi\right\rangle \left\langle\varphi\right| = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} \begin{pmatrix} b_1^* & b_2^* & \dots & b_N^* \end{pmatrix} = \begin{pmatrix} a_1 b_1^* & a_1 b_2^* & \dots & a_1 b_N^* \\ a_2 b_1^* & a_2 b_2^* & \dots & a_2 b_N^* \\ \vdots & \vdots & \ddots & \vdots \\ a_N b_1^* & a_N b_2^* & \dots & a_N b_N^* \end{pmatrix}. \tag{1.15}$$

Para comprobar que el producto externo equivale a la matriz anterior basta calcular el elemento de matriz l, k:

$$\langle l|\, P_{\psi\varphi}\, |k\rangle = \Big(\sum_{n=1}^{N} a_n \langle l|n\rangle\Big)\Big(\sum_{m=1}^{N} b_m^* \langle m|k\rangle\Big) = a_l b_k^*.$$

Observación 1.17. Podemos considerar también el producto externo de los vectores de una base ornotormal $\{|n\rangle\}_{n=1}^{N} \subset \mathbb{H}$, sean $m, k \in \{1, 2, \ldots, N\}$:

$$P_{mk} = |m\rangle \langle k|\,, \tag{1.16}$$

cuya matriz correspondiente tiene un único elemento de matriz no nulo, con valor la unidad, en (m, k).

Teorema 1.18. *Sea un operador lineal A, con elementos de matriz $A_{mk} \in \mathbb{C}$, en un espacio de Hilbert $\mathbb{H}$ sobre $\mathbb{C}$ con una base ortonormal $\{|n\rangle\}_{n=1}^{N} \subset \mathbb{H}$ arbitraria. Entonces A es una combinación lineal de todos los productos externos de la base ortonormal, de forma que:*

$$A = \sum_{m,k=1}^{N} A_{mk} P_{mk} = \sum_{m,k=1}^{N} A_{mk} |m\rangle \langle k|\,.$$

Demostración. Dado un $|\psi\rangle = \sum_{n=1}^{N} c_n |n\rangle \in \mathbb{H}$ arbitrario, comprobemos que $A|\psi\rangle = \Big(\sum_{m,k=1}^{N} A_{mk} |m\rangle \langle k|\Big)|\psi\rangle$:

$$\begin{aligned}
\Big(\sum_{m,k=1}^{N} A_{mk} |m\rangle \langle k|\Big)|\psi\rangle &= \sum_{m,k=1}^{N} A_{mk} \langle k|\psi\rangle |m\rangle \\
&= \sum_{m,k=1}^{N} A_{mk} \langle k| \Big(\sum_{n=1}^{N} c_n |n\rangle\Big)|m\rangle \\
&= \sum_{m,k=1}^{N} A_{mk} \Big(\sum_{n=1}^{N} c_n \langle k|n\rangle\Big)|m\rangle \\
&= \sum_{m,k=1}^{N} A_{mk} c_k |m\rangle = \sum_{m=1}^{N} \Big(\sum_{k=1}^{N} A_{mk} c_k\Big)|m\rangle\,.
\end{aligned}$$

Como $A|\psi\rangle = \sum_{m=1}^{N} d_m |m\rangle$ tal que $d_m = \sum_{k=1}^{N} A_{mk} c_k$, tenemos:

$$\sum_{m=1}^{N} \Big(\sum_{k=1}^{N} A_{mk} c_k\Big)|m\rangle = \sum_{m=1}^{N} d_m |m\rangle = A|\psi\rangle\,.$$

□

Definición 1.19. El **operador identidad**, I, es aquel que verifica que $I|\psi\rangle = |\psi\rangle\,,\ \forall |\psi\rangle \in \mathbb{H}$. Sus elementos de matriz son:

$$I_{mk} = \langle m|\, I\, |k\rangle = \langle m|k\rangle = \delta_{mk},\ \forall m, k \in \{1, \ldots, N\}. \tag{1.17}$$

Observación 1.20. El operador identidad es único, pues su expresión matricial es única.

Proposición 1.21 (Fórmula de Resolución de la Identidad)**.** *Dada una base ortonormal* $\{|n\rangle\}_{n=1}^{N} \subset \mathbb{H}$ *arbitraria, el operador identidad verifica:*

$$I = \sum_{n=1}^{N} P_{nn} = \sum_{n=1}^{N} |n\rangle \langle n| .$$

Demostración. Aplicando el Teorema 1.18 al operador identidad tenemos que:

$$I = \sum_{m,k=1}^{N} \delta_{mk} |m\rangle \langle k| = \sum_{m=1}^{N} |m\rangle \langle m| .$$

□

Proposición 1.22 (Composición de Operadores)**.** *Sean* $A \equiv (A_{mi})_{m,i=1}^{N}$ *y* $B \equiv (B_{jk})_{j,k=1}^{N}$ *dos operadores lineales en un espacio de Hilbert* H *con base ortonormal* $\{|n\rangle\}_{n=1}^{N}$*. Se tiene que la matriz del producto de operadores* AB *equivale al producto de las matrices de dichos operadores, es decir:*

$$AB = \sum_{m,k=1}^{N} (AB)_{mk} |m\rangle \langle k| \;\; t.q. \; (AB)_{mk} = \sum_{i=1}^{N} A_{mi} B_{ik}.$$

Demostración. Dado $k \in \{1, \ldots, N\}$, por la Fórmula de Resolución de la Identidad 1.21, se tiene que:

$$AB |k\rangle = AIB |k\rangle = A\Big(\sum_{i=1}^{N} |i\rangle \langle i|\Big) B |k\rangle = \sum_{i=1}^{N} A |i\rangle \langle i| B |k\rangle .$$

Calculamos ahora el elemento de matriz de AB, dado $m \in \{1, \ldots, N\}$:

$$\begin{aligned} (AB)_{mk} = \langle m| AB |k\rangle &= \langle m| \Big(\sum_{i=1}^{N} A |i\rangle \langle i| B |k\rangle\Big) \\ &= \sum_{i=1}^{N} \langle m| A |i\rangle \langle i| B |k\rangle = \sum_{i=1}^{N} A_{mi} B_{ik}. \end{aligned}$$

Que es el elemento de matriz del producto de matrices (A_{mi}) y (B_{jk}). Por el Teorema 1.18, tenemos la expresión para el operador AB:

$$\begin{aligned} AB &= \sum_{m,k=1}^{N} (AB)_{mk} |m\rangle \langle k| \\ &= \sum_{m,k=1}^{N} \Big(\sum_{i=1}^{N} A_{mi} B_{ik}\Big) |m\rangle \langle k| . \end{aligned}$$

□

Notación 1.23. Para expresar el producto de un conjunto de operadores $\{A_i\}_{i=1}^N$ se empleará la siguiente notación:

$$\prod_{i=1}^{N} A_i = A_N A_{N-1} \dots A_2 A_1, \tag{1.18}$$

nótese que el índice i indica el orden de aplicación de los mismos.

Proposición 1.24. *Dado un espacio de Hilbert* $\mathbb{H}$ *de dimensión* $\dim \mathbb{H} = N$*, el conjunto de operadores lineales en él,* $\mathcal{L}(\mathbb{H})$ *es un anillo isomorfo al conjunto de matrices* $N \times N$ *sobre* $\mathbb{C}$*, denotado por* $\mathcal{M}_{N\times N}(\mathbb{C})$*.*

Demostración. La demostración es directa a partir de las propiedades de los anillos, considerando el siguiente isomorfismo:

$$\begin{aligned} f : \mathcal{L}(\mathbb{H}) &\longrightarrow \mathcal{M}_{N\times N}(\mathbb{C}) \\ A &\longmapsto f(A) := (A_{ij}), \text{ con } A_{ij} = \langle i| A |j\rangle , \end{aligned}$$

siendo $\{|n\rangle\}_{n=1}^N$ una base ortonormal del espacio $\mathbb{H}$. □

Definición 1.25. Dado un operador A, definimos su **operador hermítico conjugado** o **adjunto**, $A^\dagger$, como aquel que verifica:

$$\left\langle \psi \middle| A^\dagger \phi \right\rangle = \langle A\psi | \phi \rangle = \langle \phi | A\psi \rangle^* , \tag{1.19}$$

equivalentemente, con la notación de Dirac:

$$\langle \psi | A^\dagger | \phi \rangle = \langle \phi | A | \psi \rangle^* . \tag{1.20}$$

Los elementos de matriz del adjunto son:

$$(A^\dagger)_{mk} = \langle m| A^\dagger |k\rangle = \langle k| A |m\rangle^* = A^*_{km}. \tag{1.21}$$

Es decir, la matriz del operador adjunto es la **transpuesta conjugada** de la matriz del operador.

Proposición 1.26. *Dados unos operadores* A *y* B*, se tienen las siguientes propiedades para el adjunto:*

1. $(AB)^\dagger = B^\dagger A^\dagger$.
2. $(A^\dagger)^\dagger = A$.

Demostración.

1. $(AB)^\dagger_{mn} = \langle m| (AB)^\dagger |k\rangle = \langle k| AB |m\rangle^* = (AB)^*_{km} = \sum_{i=1}^{N} A^*_{ki} B^*_{im} = \sum_{i=1}^{N} B^\dagger_{mi} A^\dagger_{ik} = B^\dagger A^\dagger$.
2. $(A^\dagger)^\dagger_{mk} = \langle m| (A^\dagger)^\dagger |k\rangle = \langle k| A^\dagger |m\rangle^* = (\langle m| A |k\rangle^*)^* = \langle m| A |k\rangle = A_{mk}$.

□

Definición 1.27. Un operador A se dice **hermítico** o **autoadjunto** si cumple que:

$$A^\dagger = A. \tag{1.22}$$

Un operador U se dice **unitario** si:

$$UU^\dagger = U^\dagger U = I, \tag{1.23}$$

es decir, que $U^\dagger = U^{-1}$.

Proposición 1.28. *Sea U un operador en $\mathbb{H}$, se tiene la siguiente equivalencia:*

$$U \text{ unitario } \Leftrightarrow \|U\psi\| = \|\psi\|, \ \forall\, |\psi\rangle \in \mathbb{H},$$

es decir, los operadores unitarios son aquellos que conservan la norma.

Demostración. Sea U un operador en $\mathbb{H}$:

- Supongamos U unitario y sea $|\psi\rangle \in \mathbb{H}$ un vector arbitrario, tenemos que:

$$\begin{aligned}\|U\psi\|^2 = \langle U\psi|U\psi\rangle &= \left\langle \psi \middle| U^\dagger U\psi \right\rangle \\ &= \langle\psi|\, U^\dagger U\, |\psi\rangle = \langle\psi|\, I\, |\psi\rangle \\ &= \langle\psi|\psi\rangle\, \|\psi\|^2 \Rightarrow \|U\psi\| = \|\psi\|.\end{aligned}$$

- Supongamos que $\|U\phi\| = \|\phi\|, \ \forall\, |\phi\rangle \in \mathbb{H}$. Se tiene que $\|U(\varphi + \lambda\chi)\| = \|\varphi + \lambda\chi\|$, con $|\varphi\rangle, |\chi\rangle \in \mathbb{H}$ y $\lambda \in \mathbb{C}$. Entonces:

$$\|U(\varphi + \lambda\chi)\|^2 = \|\varphi + \lambda\chi\|^2 \Leftrightarrow \langle U(\varphi + \lambda\chi)|U(\varphi + \lambda\chi)\rangle = \langle\varphi + \lambda\chi|\varphi + \lambda\chi\rangle\,. \tag{1.24}$$

  Desarrollando cada término de la igualdad por separado:

$$\begin{aligned}\langle\varphi + \lambda\chi|\varphi + \lambda\chi\rangle &= \langle\varphi|\varphi\rangle + |\lambda|^2\,\langle\chi|\chi\rangle + 2\,\mathrm{Re}(\lambda\,\langle\varphi|\chi\rangle) \\ &= \|\varphi\|^2 + |\lambda|^2\|\chi\|^2 + 2\,\mathrm{Re}(\lambda\,\langle\varphi|\chi\rangle), \\ \langle U(\varphi + \lambda\chi)|U(\varphi + \lambda\chi)\rangle &= \langle U\varphi|U\varphi\rangle + |\lambda|^2\,\langle U\chi|U\chi\rangle + 2\,\mathrm{Re}(\lambda\,\langle U\varphi|U\chi\rangle).\end{aligned}$$

  Por hipótesis, se tiene que $\|U\varphi\| = \|\varphi\|$ y $\|U\chi\| = \|\chi\|$, por lo que la expresión 1.24 se reduce a:

$$\mathrm{Re}(\lambda\,\langle U\varphi|U\chi\rangle) = \mathrm{Re}(\lambda\,\langle\varphi|\chi\rangle).$$

  Como esta expresión se verifica para todo $\lambda \in \mathbb{C}$, podemos considerar los dos siguientes casos:

$$\begin{aligned}\lambda = 1 &\Rightarrow \mathrm{Re}(\langle U\varphi|U\chi\rangle) = \mathrm{Re}(\langle\varphi|\chi\rangle), \\ \lambda = i &\Rightarrow \mathrm{Im}(\langle U\varphi|U\chi\rangle) = \mathrm{Im}(\langle\varphi|\chi\rangle).\end{aligned}$$

Por tanto, se tiene que $\langle U\varphi|U\chi\rangle = \langle\varphi|\chi\rangle$ y, en consecuencia:

$$\langle\varphi|\, U^\dagger U\,|\chi\rangle = \langle\varphi|\chi\rangle \Rightarrow U^\dagger U = I,$$

probando así que U es un operador unitario.

□

Proposición 1.29. *Sea $\mathbb{H}$ un espacio de Hilbert de dimensión N y U un operador unitario en dicho espacio. Entonces:*

$$\{|n\rangle\}_{n=1}^N \textit{ base ortonormal de } \mathbb{H} \Rightarrow \{U\,|n\rangle\}_{n=1}^N \textit{ base ortonormal de } \mathbb{H}$$

Demostración. Veamos que $\{|Un\rangle\}_{n=1}^N$ es un conjunto de vectores ortonormales:

$$\begin{aligned}\langle Um|Un\rangle &= \langle m|\, U^\dagger U\,|n\rangle \\ &= \langle m|\, I\,|n\rangle \\ &= \langle m|n\rangle = \delta_{mn}.\end{aligned}$$

Tenemos que $\{|Un\rangle\}_{n=1}^N$ es un conjunto de N vectores ortonormales en un espacio de Hilbert de dimensión N, por tanto, es una base ortonormal de dicho espacio. □

1.1.4. Autovalores y Autovectores

Definición 1.30. Sea A un operador lineal, un vector $|\psi\rangle \in \mathbb{H}$ para el cual existe un $a \in \mathbb{C}$ de forma que:

$$A\,|\psi\rangle = a\,|\psi\rangle\,, \tag{1.25}$$

se denomina **autovector** de A, el escalar a se denominará **autovalor** de A.

Observación 1.31. Consideremos un autovector $|\psi\rangle = \sum_{n=1}^N c_n\,|n\rangle \in \mathbb{H}$ con autovalor $a \in \mathbb{C}$ de un operador lineal A, podemos reescribir la expresión de la Definición 1.30 como:

$$A\,|\psi\rangle = a\,|\psi\rangle \Leftrightarrow (A - aI)\,|\psi\rangle = 0.$$

Como $(A - aI)$ es un operador lineal, podemos expresar el vector resultante de aplicarlo como:

$$\begin{aligned}(A-aI)\,|\psi\rangle &= \sum_{n=1}^N c_n(A - aI)\,|n\rangle = \sum_{n=1}^N c_n\Big(\sum_{m,k=1}^N (A-aI)_{mk}\,|m\rangle\,\langle k|\Big)|n\rangle \\ &= \sum_{n,m,k=1}^N c_n(A_{mk} - a\delta_{mk})\,|m\rangle\,\langle k|n\rangle = \sum_{n,m,k=1}^N \delta_{kn}c_n(A_{mk} - a\delta_{mk})\,|m\rangle \\ &= \sum_{m=1}^N \Big[\sum_{n=1}^N c_n(A_{mn} - a\delta_{mn})\Big]|m\rangle = 0 \Rightarrow \sum_{n=1}^N c_n(A_{mn} - a\delta_{mn}) = 0,\ \forall m \in \{1,\dots,N\}.\end{aligned}$$

Esta última expresión es un sistema de ecuaciones lineales para las componentes c_n de $|\psi\rangle$. Si definimos el **polinomio característico** como $p(a) = \det(A - aI)$, la condición de existencia de soluciones es $p(a) = 0$ y, como $p(a)$ es un polinomio de grado N, existirán N soluciones para la ecuación. Tendremos entonces N autovectores con sus respectivos autovalores salvo por degeneración, es decir, puede darse el caso de que un autovalor tenga multiplicidad mayor que uno, por lo que le corresponderá un subespacio de dimensión igual a su multiplicidad.

Teorema 1.32. *Sea A un operador hermítico, entonces sus autovalores son reales y los autovectores correspondientes son ortogonales entre sí.*

Demostración. Sea $|\psi\rangle \in \mathbb{H}$ un autovector del operador A con autovalor $a \in \mathbb{C}$ de forma que $A|\psi\rangle = a|\psi\rangle$, tenemos que:

$$\langle\psi| A |\psi\rangle = a \langle\psi|\psi\rangle = a\|\psi\|^2,$$

además, por ser A hermítico ($A = A^\dagger$), se tiene que:

$$\langle\psi| A |\psi\rangle = \langle\psi| A^\dagger |\psi\rangle = \langle A\psi|\psi\rangle = a^* \langle\psi|\psi\rangle = a^*\|\psi\|^2,$$

ya que $\langle A\psi| = (A|\psi\rangle)^\dagger = (a|\psi\rangle)^\dagger = a^* \langle\psi|$. Por tanto, $a = a^*$, es decir, $a \in \mathbb{R}$.

Sean dos autovectores $|\psi\rangle, |\phi\rangle \in \mathbb{H}$ de A, con autovalores $a_1, a_2 \in \mathbb{R}$ respectivamente, de forma que $a \neq b$. Entonces:

$$\begin{aligned}\langle\phi| A |\psi\rangle &= a \langle\phi|\psi\rangle, \\ \langle\phi| A |\psi\rangle &= \langle\phi| A^\dagger |\psi\rangle = \langle A\phi|\psi\rangle = b \langle\phi|\psi\rangle,\end{aligned}$$

por tanto, $(a - b)\langle\phi|\psi\rangle = 0$. Como $(a - b) \neq 0$ por definición, tenemos que $\langle\phi|\psi\rangle = 0$, es decir, los autovectores son ortogonales. □

Teorema 1.33 ([Bellac, 2006], pág.49)**.** *Sea A un operador hermítico de $\mathbb{H}$. Entonces existe un operador unitario U de forma que $U^\dagger AU$ es una matriz diagonal cuyos elementos son los autovalores de A, que aparecen tantas veces como su multiplicidad.*

1.1.5. Matrices de Pauli

Por la Proposición 1.24, el conjunto de operadores lineales sobre un espacio de Hilbert de dimensión 2 es un anillo isomorfo al conjunto de matrices 2×2 sobre $\mathbb{C}$, además, se tiene que el conjunto de matrices hermíticas de dicho anillo forma un espacio vectorial sobre $\mathbb{R}$. Resulta de interés encontrar una base para dicho espacio, pues nos permitirá descomponer cualquier operador hermítico como una combinación lineal de operadores de la base.

Consideremos una matriz hermítica $M \in \mathcal{M}_{2\times 2}(\mathbb{C})$ arbitraria:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

como $M = M^\dagger$, $a = a^*$, $b = c^*$ y $d = d^*$, por lo tanto, $a, d \in \mathbb{R}$. Definamos ahora los siguientes números reales:

$$c_0 = \frac{a+d}{2}, \quad c_1 = \mathrm{Re}(c) = \frac{c+c^*}{2}, \quad c_2 = Im(c) = \frac{c-c^*}{2}, \quad c_3 = \frac{a-d}{2}.$$

Podemos despejar los elementos de la matriz M en función de dichos valores:

$$a = c_0 + c_3, \quad d = c_0 - c_3, \quad c = c_1 + ic_2, \quad b = c_1 - ic_2,$$

es decir, la matriz M se puede representar de la siguiente forma:

$$\begin{aligned} M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} c_0 + c_3 & c_1 - ic_2 \\ c_1 + ic_2 & c_0 - c_3 \end{pmatrix} \\ &= c_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + c_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + c_2 \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + c_3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

Definición 1.34. Llamamos **matrices de Pauli** a las tres matrices de $\mathcal{M}_{2\times 2}(\mathbb{C})$ unitarias de la forma:

$$\sigma_x \equiv \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y \equiv \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z \equiv \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Estas matrices, junto con la identidad, forman una base del $\mathbb{R}$-espacio vectorial de matrices hermíticas 2×2.

1.1.6. Postulados de la Mecánica Cuántica

La mecánica cuántica, mediante una formulación matemática, pretende describir el comportamiento de sistemas y magnitudes físicas reales. En muchas introducciones a este campo [Bellac, 2006, Nielsen and Chuang, 2010, Scherer, 2019], se establece una serie de postulados que dan un significado físico a los conceptos teóricos que se estudiaron hasta ahora. Aunque no son estrictamente necesarios, resultan de gran ayuda para entender qué se quiere representar con la abstracción de los espacios de Hilbert, así como introducir el vocabulario habitual con el que se suele trabajar en la computación cuántica. Por ejemplo, por qué al módulo al cuadrado del producto escalar se le denomina *probabilidad* de medir un estado estando en otro.

Postulado 1 (Observables y Estados)**.** *Un* ***observable*** *es una cantidad física medible, una magnitud, que se representa mediante un operador hérmitico en un espacio de Hilbert* $\mathbb{H}$*. La*

información completa del ***estado*** *del sistema físico se representa con los vectores* $|\psi\rangle \in \mathbb{H}$ *en ese espacio de Hilbert. Estos se considerarán, por conveniencia, normalizados, es decir,* $\|\psi\|^2 = \langle\psi|\psi\rangle = 1$.

Si se consideran dos estados de un sistema como vectores en un espacio de Hilbert $\mathbb{H}$, $|\psi\rangle, |\phi\rangle \in \mathbb{H}$, una consecuencia de este postulado es que cualquier combinación lineal normalizada de estos estados:

$$|\varphi\rangle = \frac{\alpha|\psi\rangle + \beta|\phi\rangle}{\|\alpha|\psi\rangle + \beta|\phi\rangle\|},\ \alpha, \beta \in \mathbb{C}, \tag{1.26}$$

es también un estado físico del sistema. Esta propiedad es lo que se denomina **principio de superposición** de la mecánica cuántica y es una de las piezas clave para entender las reglas de la computación cuántica. Por otro lado, podemos observar que $\alpha|\psi\rangle$, $\alpha \in \mathbb{C}$ es también un estado del sistema, sin embargo, este se corresponde con el mismo que $|\psi\rangle$, ya que en el Postulado 1 se exige la normalización.

Postulado 2 (Probabilidad de Medición)**.** *Sean dos estados* $|\psi\rangle, |\phi\rangle \in \mathbb{H}$*, existe una* ***amplitud de probabilidad*** *de medir* $|\phi\rangle$ *estando en el estado* $|\psi\rangle$*,* $a(\psi \to \phi)$ *que se corresponde con el producto escalar en el espacio de Hilbert:*

$$a(\psi \to \phi) = \langle\phi|\psi\rangle \in \mathbb{C}. \tag{1.27}$$

Se define la ***probabilidad*** *de medir* $|\phi\rangle$ *en* $|\psi\rangle$ *como el cuadrado del valor absoluto de la amplitud de probabilidad:*

$$p(\psi \to \phi) = |a(\psi \to \phi)|^2 = |\langle\phi|\psi\rangle|^2. \tag{1.28}$$

Postulado 3 (Medición de un Observable)**.** *Las mediciones sobre un observable* A *siempre devuelven un valor real, el cual coincidirá con uno de los autovalores del mismo. Dado un estado del sistema* $|\psi\rangle \in \mathbb{H}$*, la probabilidad de medir un autovalor "*a*"de* A *con autoestado* $|a\rangle$ *es* $|\langle a|\psi\rangle|^2$*. La medida es un proceso instantáneo, después del cual el estado que representa al sistema es el autovector del autovalor medido* $|a\rangle$*.*

Observación 1.35. Sea $|\psi\rangle \in \mathbb{H}$ el estado del sistema y A un observable de $\mathbb{H}$ con base ortonotmal de autovectores $\{|a_n\rangle\}_{n=0}^N$, siendo $\{a_n\}_{n=0}^N$ sus autovalores asociados. El estado $|\psi\rangle$ se puede describir en función de esta base:

$$|\psi\rangle = \sum_{n=0}^{N} |a_n\rangle\langle a_n|\psi\rangle = \sum_{n=0}^{N} c_n|a_n\rangle,\ c_n = \langle a_n|\psi\rangle.$$

La probabilidad de medir el autovalor a_n en el estado ψ es $P(a_n) = |\langle a_n|\psi\rangle|^2 = |c_n|^2$, en consecuencia, para que un estado tenga un valor bien definido de un observable, es decir, $\exists\ m \in \{0, \ldots, N\}/P(a_m) = 1$ o equivalentemente, $P(a_n) = \delta_{nm}$, el estado del sistema debe corresponderse con uno de los autovectores del operador, pues se tendría que $\langle a_n|\psi\rangle = 0\ \forall n \neq m$ y entonces $|\psi\rangle = e^{i\varphi}|a_m\rangle \equiv |a_m\rangle$.

Otra consecuencia del Postulado 3 es que el estado del sistema después de la medición se corresponde con el del autovalor medido, es decir, existe una transición de estados llamada **colapso de la función de onda**:

$$|\psi\rangle \to \frac{|a_n\rangle \langle a_n|\psi\rangle}{|\langle a_n|\psi\rangle|^{1/2}}. \tag{1.29}$$

Postulado 4 (Sistemas Cuánticos Compuestos)**.** *Sean $\mathbb{H}_1^M$ y $\mathbb{H}_2^M$ dos sistemas cuánticos, para representar físicamente el sistema en conjunto, el espacio de estados de dos sistemas cuánticos independientes o interactuando, $\mathbb{H}_1^N$ y $\mathbb{H}_2^M$, es el producto tensorial de ambos espacios $\mathbb{H}_1^N \otimes \mathbb{H}_2^M$.*

1.1.7. Producto Tensorial de Espacios de Hilbert

Consideremos un sistema $\mathbb{H}$ dividido en dos subsistemas independientes $\mathbb{H}_1^N$ y $\mathbb{H}_2^M$ de dimensiones N y M respectivamente. Como ambos sistemas son independientes, el estado global del sistema, $|\psi\rangle \in \mathbb{H}$, vendrá determinado por dos estados, uno de cada subsistema, $|\varphi\rangle \in \mathbb{H}_1^N$ y $|\chi\rangle \in \mathbb{H}_2^M$. Entenderemos entonces el estado $|\psi\rangle$ como un vector $(|\varphi\rangle, |\chi\rangle)$ en un espacio de dimensión $N \times M$.

Definición 1.36. Sean dos espacios de Hilbert $\mathbb{H}_1^N$ y $\mathbb{H}_2^M$, con bases $\{|n\rangle\}_{n=1}^N \subset \mathbb{H}_1^N$ y $\{|m\rangle\}_{m=1}^M \subset \mathbb{H}_2^M$, se define su **producto tensorial** $\mathbb{H}_1^N \otimes \mathbb{H}_2^M$ como el espacio generado por los pares $\{(|n\rangle, |m\rangle) : \ n \in \{1, \ldots, N\}, \ m \in \{1, \ldots, M\}\}$. Diremos que $|n \otimes m\rangle \equiv |n\rangle \otimes |m\rangle \equiv (|n\rangle, |m\rangle)$ es el **producto tensorial de los estados** $|n\rangle$ y $|m\rangle$. Dados dos estados arbitrarios $|\varphi\rangle \in \mathbb{H}_1^N$ y $|\chi\rangle \in \mathbb{H}_2^M$, el producto tensorial de estos estados se denotará por $|\varphi \otimes \chi\rangle \equiv (|\varphi\rangle, |\chi\rangle)$.

Proposición 1.37. *En el contexto de la definición anterior, se tiene que el producto tensorial de espacios de Hilbert es un espacio de Hilbert de dimensión $N \times M$ y que $\{|n \otimes m\rangle\}_{n=1,m=1}^{N,M}$ es una base ortonormal en el producto tensorial.*

Demostración. Para comprobar que se trata de un espacio de Hilbert basta considerar el siguiente producto escalar:

$$\begin{aligned} \langle \cdot | \cdot \rangle : (\mathbb{H}_1^N \otimes \mathbb{H}_2^M) \times (\mathbb{H}_1^N \otimes \mathbb{H}_2^M) &\longrightarrow \mathbb{C} \\ (|\varphi_1 \otimes \chi_1\rangle, |\varphi_2 \otimes \chi_2\rangle) &\mapsto \langle \varphi_1 \otimes \chi_1 | \varphi_2 \otimes \chi_2 \rangle := \langle \varphi_1 | \varphi_2 \rangle_{\mathbb{H}_1^N} \langle \chi_1 | \chi_2 \rangle_{\mathbb{H}_2^M}. \end{aligned}$$

Como los productos escalares de los subsistemas son hermíticos, es fácil comprobar que el producto escalar así definido para el sistema global es también hermítico. Veamos ahora que $\{|n \otimes m\rangle\}_{n=1,m=1}^{N,M}$ es una base ortonormal del producto tensorial.

Dado $|\psi\rangle = |\varphi \otimes \chi\rangle \in \mathbb{H}_1^N \otimes \mathbb{H}_2^M$, tal que $|\psi\rangle = |\varphi \otimes \chi\rangle$. Tenemos que $\{|n\rangle\}_{n=1}^N$ y $\{|m\rangle\}_{m=1}^M$

son bases de $\mathbb{H}_1^N$ y $\mathbb{H}_2^M$, respectivamente, con lo cual $\exists\{a_n\}_{n=1}^N, \{b_m\}_{m=1}^M \subset \mathbb{C}$ tales que:

$$|\varphi\rangle = \sum_{n=1}^{N} a_n |n\rangle \text{ y } |\varphi\rangle = \sum_{m=1}^{M} b_m |m\rangle .$$

Por tanto, si definimos $c_{nm} = a_n b_m$, el estado global se puede expresar de la siguiente forma:

$$\begin{aligned} |\psi\rangle = |\varphi \otimes \chi\rangle = (|\varphi\rangle , |\chi\rangle) = (\sum_{n=1}^{N} a_n |n\rangle , \sum_{m=1}^{M} b_m |m\rangle \\ = \sum_{n=1,m=1}^{N,M} a_n b_m (|n\rangle , |m\rangle) = \sum_{n=1,m=1}^{N,M} c_{nm} |n \otimes m\rangle , \end{aligned}$$

es decir, $\{|n \otimes m\rangle\}_{n=1,m=1}^{N,M}$ genera el espacio producto tensorial. Veamos ahora si el conjunto de vectores el linealmente independiente.

Sean $\{\lambda_{nm}\}_{n=1,m=1}^{N,M} \subset \mathbb{C}$ arbitrarios, supongamos que se tiene que:

$$\sum_{n=1,m=1}^{N,M} \lambda_{n,m} |n \otimes m\rangle = 0,$$

por tanto, dado un $|\varphi \otimes \chi\rangle \in |\psi\rangle \in \mathbb{H}_1^N \otimes \mathbb{H}_2^M$ arbitrario, se tiene que:

$$\begin{aligned} \left\langle \varphi \otimes \chi \middle| \sum_{n=1,m=1}^{N,M} \lambda_{n,m} n \otimes m \right\rangle &= \sum_{n=1,m=1}^{N,M} \lambda_{n,m} \langle \varphi \otimes \chi | n \otimes m \rangle \\ &= \sum_{n=1,m=1}^{N,M} \lambda_{n,m} \langle \varphi | n \rangle \langle \chi | m \rangle = 0. \end{aligned}$$

En particular, si consideramos $|\varphi\rangle = |n'\rangle$ y $|\chi\rangle = |m\rangle$, se tiene que, para unos n', m' arbitrarios::

$$\sum_{n=1,m=1}^{N,M} \lambda_{n,m} \langle n' | n \rangle \langle m' | m \rangle = \sum_{n=1,m=1}^{N,M} \lambda_{n,m} \delta_{nn'} \delta_{mm'} = 0,$$

en consecuencia, $\lambda_{n'm'} = 0$, pero como n' y m' son arbitrarios, se tiene finalmente que $\lambda_{nm} = 0 \ \forall n \in \{1, \ldots, N\}, m \in \{1 \ldots, M\}$ y, por tanto, el conjunto $\{|n \otimes m\rangle\}_{n=1,m=1}^{N,M}$ es linealmente independiente. Como también genera el espacio, es una base del espacio producto tensorial $\mathbb{H}_1^N \otimes \mathbb{H}_2^M$. Para comprobar que es ortonormal, basta comprobar que:

$$\langle n' \otimes m' | n \otimes m \rangle = \langle n' | n \rangle \langle m' | m \rangle = \delta_{nn'} \delta_{mm'}.$$

Como $\{|n \otimes m\rangle\}_{n=1,m=1}^{N,M}$ es una base ortonormal con $N \times M$ elementos del espacio $\mathbb{H}_1^N \otimes \mathbb{H}_2^M$, entonces $\dim(\mathbb{H}_1^N \otimes \mathbb{H}_2^M) = N \times M$. □

Observación 1.38. Si consideramos dos estados no independientes, es decir, en interacción, el producto tensorial también sirve para representar sistema conjunto, como se comentaba en el Postulado 4. Una consecuencia de esto se puede ver si tomamos la forma más general de expresar un estado $|\psi\rangle \in \mathbb{H}_1^N \otimes \mathbb{H}_2^M$, empleando la base de la Proposición 1.37:

$$|\psi\rangle = \sum_{n,m} c_{nm} \, |n \otimes m\rangle \, ,$$

que podemos comprobar que sólo se puede expresar como $|\psi\rangle = |\varphi \otimes \chi\rangle$ con $|\varphi\rangle = \sum_n a_n \, |n\rangle \in \mathbb{H}_1^N$ y $|\chi\rangle = \sum_m b_m \, |m\rangle \in \mathbb{H}_2^M$ si $c_{nm} = a_n b_m$. Es decir, en el producto tensorial existen estados que no se pueden representar como producto tensorial de dos estados de los sistemas, pues existe una dependencia entre ambos, resultado de la interacción entre los sistemas, que no permite esa factorización.

Definición 1.39. Se dice que un estado del sistema es un **estado entrelazado** si no se puede expresar como producto tensorial de estados de los subsistemas. Si se puede expresar como producto de estados de los subsistemas, se dirá que es un **estado producto**.

Al igual que con los estados, será conveniente definir los operadores lineales del sistema en función de los operadores de los subsitemas.

Definición 1.40. Sean dos operadores lineales A del espacio $\mathbb{H}_1^N$ y B de $\mathbb{H}_2^M$, se define el **producto tensorial de operadores** como el operador en el espacio global que cumple la siguiente condición:

$$\begin{aligned} A \otimes B : \mathbb{H}_1^N \otimes \mathbb{H}_2^M &\longrightarrow \mathbb{H}_1^N \otimes \mathbb{H}_2^M \\ |\varphi \otimes \chi\rangle \quad &\mapsto (A \otimes B) \, |\varphi_2 \otimes \chi_2\rangle := |A\varphi \otimes B\chi\rangle = (A \, |\varphi\rangle) \otimes (B \, |\chi\rangle). \end{aligned}$$

Dado un estado arbitrario $|\psi\rangle = \sum_{n,m} c_{nm} \, |n \otimes m\rangle \in \mathbb{H}_1^N \otimes \mathbb{H}_2^M$, se puede comprobar sencillamente que el operador $A \otimes B$ actúa sobre él de la siguiente forma:

$$A \otimes B \, |\psi\rangle = \sum_{n,m} c_{nm} \, |An \otimes Bm\rangle \, . \tag{1.30}$$

Sus elementos de matriz serán:

$$\left\langle n' \otimes m' \right| A \otimes B \, |n \otimes m\rangle = A_{n'n} B_{m'm}. \tag{1.31}$$

De nuevo, no todo operador C de $\mathbb{H}_1^N \otimes \mathbb{H}_2^M$ se podrá expresar como producto tensorial de operadores $A \otimes B$, al igual que pasaba con los estados.

Proposición 1.41. *Considerando $\mathbb{C}^N$, $\mathbb{C}^M$ como espacios de Hilbert de dimensión N y M, respectivamente, se tiene que:*

$$\mathbb{C}^N \otimes \mathbb{C}^M \cong \mathbb{C}^{NM}.$$

Demostración. Sean $\{|n\rangle\}_{n=0}^{N-1} \subset \mathbb{C}^N$ y $\{|m\rangle\}_{m=0}^{M-1} \subset \mathbb{C}^M$ las respectivas bases canónicas de forma que:

$$|n\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} 0 \\ \vdots \\ n \\ \vdots \\ N-1 \end{matrix} \quad \text{y} \quad |m\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} 0 \\ \vdots \\ m \\ \vdots \\ M-1 \end{matrix},$$

en sus respectivos espacios. Consideremos una aplicación lineal que verifique:

$$\varphi : \mathbb{C}^N \otimes \mathbb{C}^M \longrightarrow \mathbb{C}^{NM}$$

$$|n \otimes m\rangle \quad \mapsto \varphi(|n \otimes m\rangle) = |N \cdot m + n\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} 0 \\ \vdots \\ N \cdot m + n, \\ \vdots \\ N \cdot M - 1 \end{matrix}$$

si la evaluamos en un estado arbitrario $|\psi\rangle = \sum_{n,m} c_{nm} |n \otimes m\rangle$, se tiene que:

$$\varphi(|\psi\rangle) = \sum_{n,m} c_{nm} \varphi(|n \otimes m\rangle) = \sum_{n,m} c_{nm} |N \cdot m + n\rangle ,$$

veamos que se trata de un isomorfismo.

- Inyectividad: sean $|\psi\rangle = \sum_{n,m} a_{nm} |n \otimes m\rangle , |\phi\rangle = \sum_{n,m} b_{nm} |n \otimes m\rangle \in \mathbb{C}^N \otimes \mathbb{C}^M$ tales que $\varphi(|\psi\rangle) = \varphi(|\phi\rangle)$, entonces:

$$\begin{aligned} \varphi(|\psi\rangle) = \varphi(|\phi\rangle) &\Leftrightarrow \sum_{n,m} a_{n,m} |N \cdot m + n\rangle = \sum_{n,m} b_{n,m} |N \cdot m + n\rangle \\ &\Leftrightarrow \sum_{n,m} (a_{nm} - b_{nm}) |N \cdot m + n\rangle = 0, \end{aligned}$$

  como $\{|N \cdot m + n\rangle\}_{n,m}$ es base de $\mathbb{C}^{NM}$, en concreto será un conjunto linealmente independiente, con lo cual:

$$a_{nm} - b_{nm} = 0, \ \forall n, m \Leftrightarrow a_{nm} = b_{nm}, \ \forall n, m \Leftrightarrow |\psi\rangle = |\phi\rangle .$$

- Sobreyectividad: sea un estado arbitrario $|\phi\rangle = \sum_{n,m} c_{nm} |N \cdot m + n\rangle \in \mathbb{C}^{NM}$, basta considerar el estado $|\psi\rangle = \sum_{n.m} c_{nm} |n \otimes m\rangle$, pues:

$$\varphi(|\psi\rangle) = \varphi\Big(\sum_{n,m} c_{nm} |n \otimes m\rangle \Big) = \sum_{n,m} c_{nm} \varphi(|n \otimes m\rangle) = \sum_{n,m} c_{nm} |N \cdot m + n\rangle .$$

  Por tanto, la aplicación lineal entre ambos espacios vectoriales es biyectiva y, en consecuencia, existe un isomorfismo entre $\mathbb{C}^N \otimes \mathbb{C}^M$ y $\mathbb{C}^{NM}$

□

1.2. El Concepto de Cúbit

Al igual que el *bit* en la computación clásica, en computación cuántica tenemos una unidad mínima de información, que denominamos *cúbit* (*qubit*, *quantum bit*). Sin embargo, a diferencia del bit, que sólo puede estar en los estados 0 (apagado) o 1 (encendido), el cúbit puede encontrarse en puntos intermedios como una superposición de dos estados denotados por $|0\rangle$ y $|1\rangle$.

Por hacernos una idea más visual, imaginemos al bit como una bombilla, esta solo puede encontrarse en dos estados *encendida* o *apagada*. El cúbit podría pensarse como una bombilla que tiene cierta probabilidad de estar encendida o apagada cuando entres en la habitación, si entras suficientes veces y registras el número de veces que te la has encontrado de cada forma, podrás deducir esa probabilidad de estar *encendida* y, por tanto, conocerás el estado de esa bombilla. Un ordenador cuántico funciona de una forma similar, si queremos saber qué estado $|\psi\rangle$ resulta de aplicar un circuito o algoritmo, deberemos repetir ese proceso y estudiar la proporción de veces que medimos $|0\rangle$ o $|1\rangle$, para deducir los coeficientes de $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$.

1.2.1. Cúbit

Consideremos $\mathbb{C}^2$ como un $\mathbb{C}$-espacio de Hilbert de dimensión 2 y denotemos los elementos de su base canónica de la siguiente forma:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ y } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.32}$$

Definición 1.42. Un **cúbit** es un sistema físico descrito por un espacio de Hilbert $\mathbb{H} = \mathbb{C}^2$, denominado **espacio del cúbit**, y a cada estado $|\psi\rangle \in \mathbb{C}^2$ tal que $\|\psi\| = 1$ se le llama **estado del cúbit** o simplemente **cúbit**. La base canónica del espacio, $\{|0\rangle, |1\rangle\}$, se dice que es la **base computacional**.

Observación 1.43. Dado un cúbit $|\psi\rangle \in \mathbb{H}$, existen $a, b \in \mathbb{C}$ tales que:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \text{ con } |a|^2 + |b|^2 = 1. \tag{1.33}$$

La observación del cúbit se realiza mediante la medida del operador σ_z, con $\sigma_z\,|0\rangle = 1\,|0\rangle$ y $\sigma_z\,|1\rangle = -1\,|1\rangle$, por tanto, por el Postulado 3, sólo seremos capaces de observar los estados de la base computacional con probabilidades:

$$P(|0\rangle) = |\langle 0|\psi\rangle|^2 = |a|^2 \text{ y } P(|1\rangle) = |\langle 1|\psi\rangle|^2 = |b|^2. \tag{1.34}$$

En consecuencia, mediante una sucesión de mediciones, no podremos determinar el estado cuántico exacto, sólo las probabilidades de cada estado computacional.

Definición 1.44 (Superposición)**.** Un cúbit $|\psi\rangle$ se dice que está en un **estado simple** si $a = 0$ o $b = 0$, es decir, si $|\psi\rangle = |1\rangle$ o $|\psi\rangle = |0\rangle$, respectivamente. Se dice que el cúbit estará en **superposición** si $a, b \neq 0$.

Observación 1.45. Estos estados en superposición son la gran diferencia respecto a la computación clásica, pues asumimos que pueden existir estados intermedios ente los elementos de la base computacional, es decir, estados que con cierta probabilidad caerán en el 0 o en el 1.

Observación 1.46. Parametricemos ahora los coeficientes de un cúbit arbitrario $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, $|a|^2 + |b|^2 = 1$, con los parámetros $\alpha, \beta \in [0, 2\pi]$ y $\theta \in [0, \pi]$ de forma que $a = \cos(\theta/2)e^{i\alpha}$ y $b = \sin(\theta/2)e^{i\beta}$. Podemos expresar el cúbit de la siguiente forma:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \cos(\theta/2)e^{i\alpha}\,|0\rangle + \sin(\theta/2)e^{i\beta}\,|1\rangle\,.$$

Si añadimos una fase global al cúbit, por el Postulado 1 sigue denotando el mismo estado físico, por tanto:

$$|\psi\rangle \equiv e^{-i\alpha}\,|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i(\beta-\alpha)}\,|1\rangle\,.$$

Finalmente, si denotamos $\phi = \beta - \alpha \in [0, 2\pi]$, se tiene la siguiente expresión:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}\,|1\rangle\,.$$

Definición 1.47 (Esfera de Bloch)**.** Dado un cúbit $|\psi\rangle \in \mathbb{H}$, se dice que los parámetros $\theta \in [0, \pi]$ y $\phi \in [0, 2\pi]$ determinan la **representación de Bloch** del cúbit:

$$|\psi(\theta, \phi)\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}\,|1\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\phi}\sin(\theta/2) \end{pmatrix}. \tag{1.35}$$

Cada cúbit se podrá representar como un punto de una esfera unitaria en $\mathbb{R}^3$, denominada **esfera de Bloch**:

$$\begin{aligned} x &= \cos(\phi)\sin(\theta), \\ y &= \sin(\phi)\sin(\theta), \\ z &= \cos(\theta). \end{aligned}$$

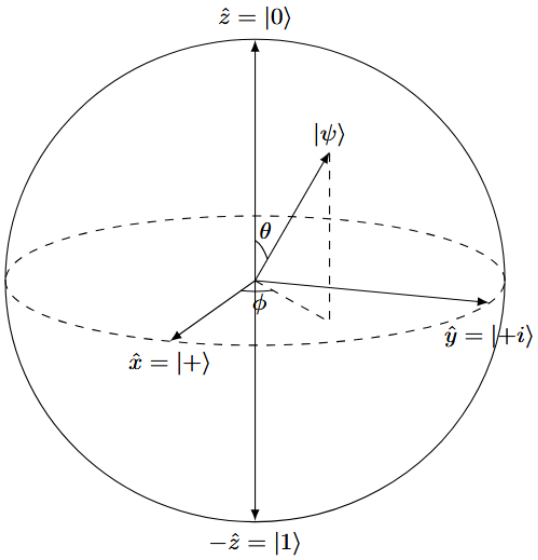

Figura 1.1: Representación de la esfera de Bloch.

Ejemplo 1.48.

1. $|0\rangle = \cos(0)\,|0\rangle + \sin(0)e^{i\phi}\,|1\rangle \equiv (0,\phi) \equiv (0,0,1)$.
2. $|1\rangle = \cos(\pi/2)\,|0\rangle + \sin(\pi/2)e^{i\phi}\,|1\rangle \equiv (\pi,\phi) \equiv (0,0,-1)$.
3. $|+x\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \cos(\pi/4)\,|0\rangle + \sin(\pi/4)e^{i0}\,|1\rangle \equiv (\pi/2,0) \equiv (1,0,0)$.
4. $|+y\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) = \cos(\pi/4)\,|0\rangle + \sin(\pi/4)e^{i\frac{\pi}{2}}\,|1\rangle \equiv (\pi/2,\pi/2) \equiv (0,1,0)$.

1.2.2. p-Cúbit

Al igual que en la computación clásica, en la mayoría de algoritmos se emplean varios cúbits simultáneamente. Los cúbits son sistemas físicos que pueden interactuar entre sí y formar estados entrelazados, donde el estado de un cúbit podrá depender del estado de otro.

Notación 1.49. Partiendo de la base computacional de $\mathbb{C}^2$, $\{|0\rangle, |1\rangle\}$, por la Proposición 1.37 se tiene que el conjunto $\{|n \otimes m\rangle\}_{n,m\in\{0,1\}}$ es una base ortogonal del espacio producto tensorial de dos cúbits, $(\mathbb{C}^2)^{\otimes 2}$. Esta base se denota de distintas formas en función de lo que sea conveniente:

- $\{|nm\rangle\}_{n,m\in\{0,1\}} = \{|00\rangle, |10\rangle, |01\rangle, |11\rangle\} = \left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}$, que se corresponde con la notación de números en binario con dos cifras, cambiando el sentido de lectura (de izquierda a derecha en este caso).
- $\{|k\rangle\}_{k=0}^{2^2-1} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$, que se obtiene de la anterior aplicando la transformación

$k = n \cdot 2^0 + m \cdot 2^1$. Esta notación es más compacta a medida que se escala con el número de cúbits, como veremos a continuación.

Proposición 1.50. *Se tiene que los espacios de Hilbert* $(\mathbb{C}^2)^{\otimes p}$ *y* $\mathbb{C}^{2^p}$ *son isomorfos.*

Demostración. Es una consecuencia directa de la Proposición 1.41, tomando sucesivamente $N = \mathbb{C}^2$ y $M = \mathbb{C}^{2^k}$ con $k = 1, \ldots, p-1$. □

Definición 1.51. Diremos que un **p-cúbit** es un sistema físico descrito por un espacio de Hilbert de la forma $\mathbb{H} = (\mathbb{C}^2)^{\otimes p}$, llamado **espacio del p-cúbit**. A cada estado $|\psi\rangle \in \mathbb{C}^{2p}$ tal que $\||\psi\|| = 1$ se le llamará **estado del p-cúbit** o simplemente **p-cúbit**.

Observación 1.52. En el contexto del resultado anterior, la Proposición 1.41 nos da también una aplicación lineal que transforma elementos de la base canónica del producto tensorial en elementos de la base canónica del espacio de dimensión producto. Empezando por $(\mathbb{C}^2)^{\otimes 2}$, se tiene que el espacio es isomorfo a $\mathbb{C}^4$ y la base canónica se relaciona con la del producto tensorial por la siguiente transformación:

$$|k\rangle_2 = |n_0 + 2 \cdot n_1\rangle_2 \equiv |n_0 n_1\rangle\,,\ n_0, n_1 \in \{0,1\}.$$

Supongamos ahora que $(\mathbb{C}^2)^{\otimes(p-1)} \cong \mathbb{C}^{2^{p-1}}$ se tiene que $|k\rangle_{p-1} = \left|\sum_{j=0}^{p-2} n_j 2^j\right\rangle \equiv |n_0 \ldots n_{p-2}\rangle$, veamos si se verifica para $(\mathbb{C}^2)^{\otimes p}$. Por la Proposición 1.41 con $N = \mathbb{C}^{2^{p-1}}$ y $M = \mathbb{C}^2$, se tiene que $\mathbb{C}^{2^{p-1}} \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^p}$ y que la base canónica de este último se relaciona con la del producto tensorial mediante la siguiente transformación:

$$|k \otimes n_{p-1}\rangle \equiv \left|\tilde{k}\right\rangle_p = \left|2^{p-1} n_{p-1} + k\right\rangle = \left|n_{p-1} 2^{p-1} + \sum_{j=0}^{p-2} n_j 2^j\right\rangle = \left|\sum_{j=0}^{p-1} n_j 2^j\right\rangle,$$

además, $|k \otimes n_{p-1}\rangle \equiv |n_0 \otimes n_{p-2} \otimes n_{p-1}\rangle \equiv |n_0 \ldots n_{p-1}\rangle$, por tanto se tiene que en general:

$$\left|\tilde{k}\right\rangle_p = \left|\sum_{j=0}^{p-1} n_j 2^j\right\rangle \equiv |n_0 \ldots n_{p-1}\rangle\,,\ n_j \in \{0,1\}.$$

Cuando trabajemos en un p-cúbit se usará la representación en el espacio $\mathbb{C}^{2^p}$ y, aunque se emplee la notación del producto tensorial $|n_0 \ldots n_{p-1}\rangle$, se estará haciendo referencia a un vector del espacio de dimensión 2^p.

Notación 1.53. Sea un p-cúbit $\mathbb{C}^{2^p}$, usaremos dos notaciones para su base canónica o computacional:

- **Notación binaria**: $\{|n_0 n_1 \ldots n_{p-1}\rangle\}_{n_j \in \{0,1\}}$.
- **Notación decimal**: $\{|k\rangle_p\}_{k=0}^{2^p-1}$.

Para las cuales se tiene la siguiente correspondencia:

$$|k\rangle_p = \left| \sum_{j=0}^{p-1} n_j 2^j \right\rangle_p \equiv |n_0 \dots n_{p-1}\rangle \,. \tag{1.37}$$

Usaremos ambas en función de cual sea la más conveniente.

Observación 1.54. Consideremos un estado arbitrario $|\psi\rangle = \sum_{k=0}^{p-1} \alpha_k |k\rangle_p \in \mathbb{C}^{2^p}$, para que sea un p-cúbit, por la Definición 1.51, debe verificar que:

$$\|\psi\| = 1 \Leftrightarrow \sum_{k=0}^{p-1} |\alpha_k|^2 = 1.$$

Definición 1.55. Sea un p-cúbit $|\psi\rangle \in \mathbb{C}^{2^p}$, se dice que es un **estado producto** si se puede expresar como producto tensorial de p 1-cúbits, es decir, $\exists \{|\psi_0\rangle, \dots, |\psi_{p-1}\rangle\} \in \mathbb{C}^2$ tales que:

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_{p-1}\rangle = \bigotimes_{k=0}^{p-1} |\psi_k\rangle \,. \tag{1.38}$$

Se dirá que el p-cúbit está **entrelazado** cuando no se pueda descomponer de esta forma.

Observación 1.56. Consideremos un 2-cúbit arbitrario $|\psi\rangle = \sum_{k=0}^{3} \alpha_k |k\rangle_2 = \alpha_0 |00\rangle + \alpha_1 |10\rangle + \alpha_2 |01\rangle + \alpha_3 |11\rangle = \alpha_{00} |00\rangle + \alpha_{10} |10\rangle + \alpha_{01} |01\rangle + \alpha_{11} |11\rangle$, supongamos que existen $|\psi_0\rangle = a_0 |0\rangle + b_0 |1\rangle, |\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle \in \mathbb{C}^2$ tales que $|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle$, entonces:

$$\begin{aligned} &\alpha_{00} |00\rangle + \alpha_{10} |10\rangle + \alpha_{01} |01\rangle + \alpha_{11} |11\rangle = a_0 a_1 |00\rangle + b_0 a_1 |10\rangle + a_0 b_1 |01\rangle + b_0 b_1 |11\rangle \\ &\Leftrightarrow (\alpha_{00} - a_0 a_1) |00\rangle + (\alpha_{10} - b_0 a_1) |10\rangle + (\alpha_{01} - a_0 b_1) |01\rangle + (\alpha_{11} - b_0 b_1) |11\rangle = 0, \end{aligned}$$

como la base computacional es un conjunto linealmente independiente:

$$\begin{aligned} \alpha_{00} = a_0 a_1,\ \alpha_{10} = b_0 a_1, \\ \alpha_{01} = a_0 b_1,\ \alpha_{11} = b_0 b_1. \end{aligned}$$

Se tiene entonces la siguiente condición necesaria y suficiente para ser estado producto, también llamada **condición de entrelazamiento**:

$$\alpha_{00}\alpha_{11} = a_0 a_1 b_0 b_1 = \alpha_{10}\alpha_{01}. \tag{1.39}$$

1.3. Puertas y Circuitos Cuánticos

1.3.1. Puertas Lógicas para un Cúbit

Ahora estudiaremos cuál es el análogo cuántico de las puertas lógicas clásicas, es decir, cómo son las transformaciones que se aplican sobre la unidad mínima de información. Estas transformaciones, denominadas **puertas lógicas cuánticas**, están descritas por operadores lineales en

el espacio de Hilbert $\mathbb{C}^2$ y, además, deben de preservar la norma, para que el estado resultante siga siendo un cúbit. Por la Proposición 1.28, sabemos que los operadores que conservan la norma son los **unitarios**.

Definición 1.57. Se define una **puerta lógica para un cúbit** como un operador unitario en el espacio de Hilbert $\mathbb{C}^2$, es decir, un operador cuya matriz asociada $U \in \mathcal{M}_{2\times 2}(\mathbb{C})$ verifica que $U^\dagger U = UU^\dagger = I_2$.

Ejemplo 1.58. Veamos ahora algunas de las puertas lógicas para un cúbit más importantes y como es su comportamiento en la esfera de Bloch:

- **Matrices de Pauli**: como vimos la Definición 1.34, las matrices de Pauli son operadores unitarios. En el contexto de puertas lógicas se emplea una nomenclatura distinta:

  1. **Puerta** $X \equiv \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Sea $|\psi\rangle \equiv (\theta, \phi)$ un estado del cúbit arbitrario, esta puerta actúa de la siguiente forma:

$$\begin{aligned} X|\psi\rangle &= X(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle) \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} e^{i\phi}\sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \equiv \begin{pmatrix} \cos\left(\frac{\pi}{2} - \frac{\theta}{2}\right) \\ e^{-i\phi}\sin\left(\frac{\pi}{2} - \frac{\theta}{2}\right) \end{pmatrix}. \end{aligned}$$

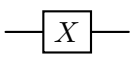

Figura 1.2: Símbolo para la puerta X.

  En la esfera de Bloch, esta transformación se corresponde con un giro del vector de 180° respecto al eje X:

$$\begin{pmatrix} \cos(\phi)\sin(\theta) \\ \sin(\phi)\sin(\theta) \\ \cos(\theta) \end{pmatrix} \xrightarrow{X} \begin{pmatrix} \cos(-\phi)\sin(\pi-\theta) \\ \sin(-\phi)\sin(\pi-\theta) \\ \cos(\pi-\theta) \end{pmatrix} = \begin{pmatrix} \cos(\phi)\sin(\theta) \\ -\sin(\phi)\sin(\theta) \\ -\cos(\theta) \end{pmatrix}.$$

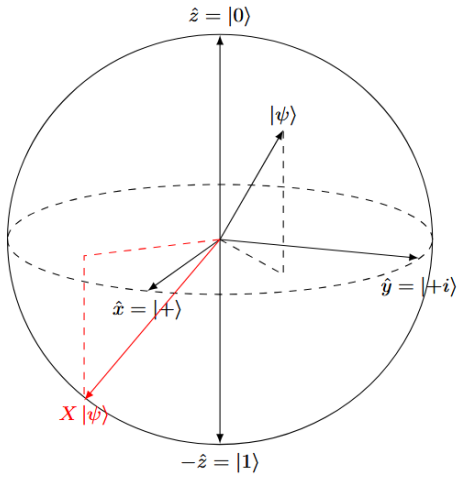

Figura 1.3: Aplicación de la puerta X en el estado $|\psi\rangle \equiv (\frac{\pi}{4}, \frac{\pi}{4})$, que pasa a $X|\psi\rangle \equiv (\frac{3\pi}{4}, -\frac{\pi}{4})$.

2. **Puerta** $Y \equiv \sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Sea $|\psi\rangle \equiv (\theta, \phi)$ un estado del cúbit arbitrario, puerta actúa de la siguiente forma:

$$\begin{aligned} Y|\psi\rangle &= Y(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle) \\ &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} e^{i(\phi-\frac{\pi}{2})}\sin\left(\frac{\theta}{2}\right) \\ e^{i\frac{\pi}{2}}\cos\left(\frac{\theta}{2}\right) \end{pmatrix} \equiv \begin{pmatrix} \cos\left(\frac{\pi}{2}-\frac{\theta}{2}\right) \\ e^{i(\pi-\phi)}\sin\left(\frac{\pi}{2}-\frac{\theta}{2}\right) \end{pmatrix}. \end{aligned}$$

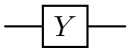

Figura 1.4: Símbolo para la puerta Y.

En la esfera de Bloch, esta transformación se corresponde con un giro del vector de 180° respecto al eje Y:

$$\begin{pmatrix} \cos(\phi)\sin(\theta) \\ \sin(\phi)\sin(\theta) \\ \cos(\theta) \end{pmatrix} \xrightarrow{Y} \begin{pmatrix} \cos(\pi-\phi)\sin(\pi-\theta) \\ \sin(\pi-\phi)\sin(\pi-\theta) \\ \cos(\pi-\theta) \end{pmatrix} = \begin{pmatrix} -\cos(\phi)\sin(\theta) \\ \sin(\phi)\sin(\theta) \\ -\cos(\theta) \end{pmatrix}.$$

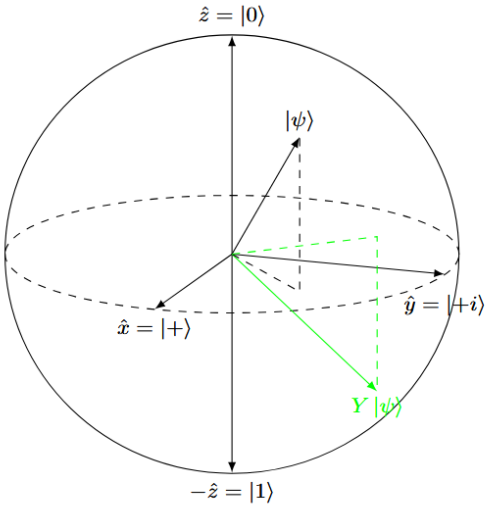

Figura 1.5: Aplicación de la puerta Y en el estado $|\psi\rangle \equiv (\frac{\pi}{4}, \frac{\pi}{4})$, que pasa a $Y|\psi\rangle \equiv (\frac{3\pi}{4}, \frac{3\pi}{4})$.

3. **Puerta** $Z \equiv \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Sea $|\psi\rangle \equiv (\theta, \phi)$ un estado del cúbit arbitrario, esta puerta actúa de la siguiente forma:

$$\begin{aligned} Z|\psi\rangle &= Z(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ -e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \equiv \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i(\phi+\pi)}\sin\left(\frac{\theta}{2}\right) \end{pmatrix}. \end{aligned}$$

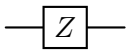

Figura 1.6: Símbolo para la puerta Z.

En la esfera de Bloch, esta transformación se corresponde con un giro del vector de 180° respecto al eje Z:

$$\begin{pmatrix} \cos(\phi)\sin(\theta) \\ \sin(\phi)\sin(\theta) \\ \cos(\theta) \end{pmatrix} \xrightarrow{Z} \begin{pmatrix} \cos(\phi+\pi)\sin(\theta) \\ \sin(\phi+\pi)\sin(\theta) \\ \cos(\theta) \end{pmatrix} = \begin{pmatrix} -\cos(\phi)\sin(\theta) \\ -\sin(\phi)\sin(\theta) \\ \cos(\theta) \end{pmatrix}.$$

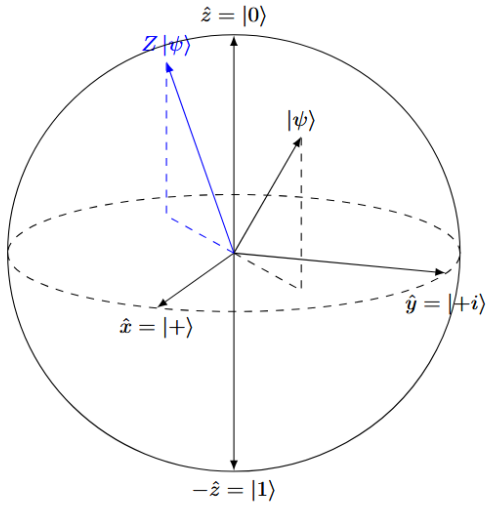

Figura 1.7: Aplicación de la puerta Z en el estado $|\psi\rangle \equiv (\frac{\pi}{4}, \frac{\pi}{4})$, que pasa a $Z|\psi\rangle \equiv (\frac{\pi}{4}, \frac{5\pi}{4})$.

- **Puerta Hadamard**: $H := \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Su mayor utilidad es poner en superposición al cúbit, por ejemplo, si este empieza en el estado $|0\rangle$ se tiene que $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) := |+\rangle$.

Figura 1.8: Símbolo para la puerta H.

- **Factor de fase**: $M(\varphi) := e^{i\varphi}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$. Añade una fase global al cúbit, no altera su estado físico.

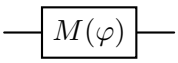

Figura 1.9: Símbolo para la puerta de factor de fase φ.

- **Desplazamiento de fase**: $P(\varphi) := |0\rangle\langle 0| + e^{i\varphi}|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$. Añade una fase parcial al cúbit, alterando el estado físico del mismo.

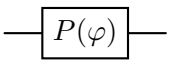

Figura 1.10: Símbolo para la puerta de desplazamiento de fase φ.

- **Puerta de rotación parametrizada**: $RT_j := P(\frac{2\pi}{2^j}) = |0\rangle\langle 0| + e^{i\frac{2\pi}{2^j}}|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^j}} \end{pmatrix}$.

Es un caso particular de la puerta de desplazamiento de fase, tiene relevancia en el algoritmo de la transformada de Fourier cuántica (QFT).

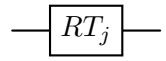

Figura 1.11: Símbolo para la puerta de rotación parametrizada.

- **Puerta de rotación-x**: $R_x(\theta) := \cos(\theta/2)I_2 - i\sin(\theta/2)\sigma_x = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$. Rota el cúbit en torno al eje x en la esfera de Bloch en un ángulo $\theta \in [0, 2\pi]$.
- **Puerta de rotación-y**: $R_y(\theta) := \cos(\theta/2)I_2 - i\sin(\theta/2)\sigma_y = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$. Rota el cúbit en torno al eje y en la esfera de Bloch en un ángulo $\theta \in [0, 2\pi]$, será relevante en el desarrollo del algoritmo HHL.

Observación 1.59 ([Scherer, 2019], Lemma 2.32). Se tiene que toda puerta unitaria puede ser representada mediante la selección adecuada de parámetros en la siguiente matriz general:

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

1.3.2. Puertas Lógicas para un p-Cúbit

Definición 1.60. Se define una **puerta lógica para un p-cúbit** como un operador unitario en el espacio de Hilbert $\mathbb{C}^{2^p}$, es decir, un operador cuya matriz asociada $U \in \mathcal{M}_{2^p \times 2^p}(\mathbb{C})$ verifica que $U^\dagger U = UU^\dagger = I_{2^p}$.

Observación 1.61. Las puertas lógicas para un p-cúbit más simples son las que se pueden descomponer como un producto tensorial de puertas para cúbits. Estas puertas tienen operadores unitarios asociados que se expresan mediante el producto tensorial de unitarios sobre $\mathbb{C}^2$, definidos en 1.40. Además, la matriz asociada al producto tensorial se puede obtener mediante el **producto de Kronecker** que, en su caso más general para un par de matrices $A \in \mathcal{M}_{m\times n}(\mathbb{C})$ y $B \in \mathcal{M}_{p\times q}(\mathbb{C})$, tiene la siguiente expresión:

$$A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix} \in \mathcal{M}_{mp\times nq}(\mathbb{C}). \tag{1.40}$$

Proposición 1.62. *Sean dos operadores unitarios $\mathcal{U} \in \mathcal{L}(\mathbb{C}^{2^p})$ y $\mathcal{V} \in \mathcal{L}(\mathbb{C}^{2^q})$ con matrices asociadas $U \in \mathcal{M}_{2^p\times 2^p}(\mathbb{C})$ y $V \in \mathcal{M}_{2^q\times 2^q}(\mathbb{C})$, respectivamente. Se tiene que $\mathcal{U}\otimes\mathcal{V}$ es un operador unitario sobre el espacio $\mathbb{C}^{2^{p+q}}$.*

Demostración. Veamos que la matriz asociada a $\mathcal{U} \otimes \mathcal{V}$ es unitaria en $\mathcal{M}_{2^{p+q}\times 2^{p+q}}(\mathbb{C})$:

$$U \otimes V = \begin{pmatrix} u_{11}V & \cdots & u_{12^{p+q}}V \\ \vdots & \ddots & \vdots \\ u_{2^{p+q}1}V & \cdots & u_{2^{p+q}2^{p+q}}V \end{pmatrix} \in \mathcal{M}_{2^{p+q}\times 2^{p+q}}(\mathbb{C}),$$

$$(U \otimes V)^\dagger = \begin{pmatrix} u_{11}V & \cdots & u_{12^{p+q}}V \\ \vdots & \ddots & \vdots \\ u_{2^{p+q}1}V & \cdots & u_{2^{p+q}2^{p+q}}V \end{pmatrix}^\dagger$$

$$= \begin{pmatrix} u_{11}^*V^\dagger & \cdots & u_{2^{p+q}1}^*V^\dagger \\ \vdots & \ddots & \vdots \\ u_{12^{p+q}}V^\dagger & \cdots & u_{2^{p+q}2^{p+q}}^*V^\dagger \end{pmatrix} = U^\dagger \otimes V^\dagger$$

Por tanto:

$$(U \otimes V)(U \otimes V)^\dagger = (U \otimes V)(U^\dagger \otimes V^\dagger) = (UU^\dagger) \otimes (VV^\dagger) = I_{2^p} \otimes I_{2^q} = I_{2^{p+q}},$$
$$(U \otimes V)^\dagger(U \otimes V) = (U^\dagger \otimes V^\dagger)(U \otimes V) = (U^\dagger U) \otimes (V^\dagger V) = I_{2^p} \otimes I_{2^q} = I_{2^{p+q}}.$$

En consecuencia, $(U \otimes V)^\dagger = (U \otimes V)^{-1}$, por lo que $U \otimes V$ es una matriz unitaria.

□

Ejemplo 1.63. Veamos algunas matrices que se pueden descomponer en productos tensoriales y sus matrices asociadas:

1. $H^{\otimes p} = \bigotimes_{i=1}^{p} H = H \otimes H^{\otimes p-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} H^{\otimes p-1} & H^{\otimes p-1} \\ H^{\otimes p-1} & -H^{\otimes p-1} \end{pmatrix}, \quad H^{\otimes 2} = \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$
2. $Z^{\otimes p} = \bigotimes_{i=1}^{p} Z = Z \otimes Z^{\otimes p-1} = \begin{pmatrix} Z^{\otimes p-1} & \mathbf{0}_{2^{p-1}} \\ \mathbf{0}_{2^{p-1}} & -Z^{\otimes p-1} \end{pmatrix}, \quad Z^{\otimes 2} = \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$
3. $Z \otimes H = \begin{pmatrix} H & \mathbf{0}_2 \\ \mathbf{0}_2 & -H \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}.$

Observación 1.64. Una utilidad interesante de la puerta Hadamard para un p-cúbit consiste en aplicarla a un estado inicial $|0\rangle^{\otimes p}$ se tiene:

$$H^{\otimes p}|0\rangle^{\otimes p} = (H|0\rangle)^{\otimes p} = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes p} = \frac{1}{\sqrt{2^p}} \sum_{\vec{k}\in\{0,1\}^p} \left|\vec{k}\right\rangle = \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} |k\rangle_p .$$

Es decir, se obtiene un estado en superposición, de forma que todos los elementos de la base computacional del p-cúbit son equiprobables. Este estado de superposición suele ser el punto de partida de muchos algoritmos cuánticos.

Proposición 1.65. *Sea $x \in \{0,1\}^p$ y $|x\rangle$ un elemento de la base computacional de un p-cúbit, se tiene que:*

$$H^{\otimes p}|x\rangle = \frac{1}{\sqrt{2^p}} \sum_{z=0}^{2^p-1} (-1)^{x\cdot z} |z\rangle , \tag{1.41}$$

donde $x \cdot z = \sum_{i=0}^{p-1} x_i z_i$, para un $z \in \{0,1\}^p$ arbitrario.

Demostración. Desarrollemos la expresión de la izquierda en 1.41:

$$\begin{aligned} H^{\otimes p}|x\rangle = H^{\otimes p}|x_0 \otimes \cdots \otimes x_{p-1}\rangle &= \bigotimes_{i=0}^{p-1} H|x_i\rangle \\ &= \bigotimes_{i=0}^{p-1} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_i}|1\rangle) = \frac{1}{\sqrt{2^p}} \sum_{z=0}^{2^p-1} \bigotimes_{i=0}^{p-1} (-1)^{x_i z_i}|z_i\rangle \\ &= \frac{1}{\sqrt{2^p}} \sum_{z=0}^{2^p-1} \prod_{i=0}^{p-1} (-1)^{x_i z_i} \bigotimes_{i=0}^{n-1} |z_i\rangle = \frac{1}{\sqrt{2^p}} \sum_{z=0}^{2^p-1} \prod_{i=0}^{p-1} (-1)^{x_i z_i}|z\rangle \\ &= \frac{1}{\sqrt{2^p}} \sum_{z=0}^{2^p-1} (-1)^{\sum_{i=0}^{p-1} x_i z_i}|z\rangle = \frac{1}{\sqrt{2^p}} \sum_{z=0}^{2^p-1} (-1)^{x\cdot z}|z\rangle . \end{aligned}$$

□

Observación 1.66. Por otro lado, existen puertas lógicas sobre p-cúbits que no pueden ser expresadas como productos tensoriales de puertas más simples, al igual que pasaba con el producto tensorial de estados y operadores. Este tipo de puertas son de especial interés, pues pueden ser usadas para obtener estados entrelazados entre cúbits.

Ejemplo 1.67. Veamos algunas de estas puertas que no se pueden descomponer:

1. Puerta $CNOT_{01} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

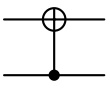

Figura 1.12: Símbolo para la puerta $CNOT$.

$$CNOT_{01}|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle ,$$

$$CNOT_{01}|10\rangle = |10\rangle ,$$

$$CNOT_{01}|01\rangle = |11\rangle ,$$

$$CNOT_{01}|11\rangle = |01\rangle .$$

En general, la puerta $CNOT_{ij}$ con $i, j \in \{0, \ldots, p-1\}$ tiene un cúbit de **control**, j, y otro **objetivo**, i. Considerando un elemento la base computacional del p-cúbit, si el dígito de control es un 1, se cambiará el dígito objetivo y si el control es 0, el objetivo se mantendrá en el que estaba.

2. Puerta $CCNOT_{012} := \left(\begin{array}{c|cc} I_6 & \mathbf{0}_{6\times 2} \\ \hline \mathbf{0}_{2\times 6} & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{array}\right)$.

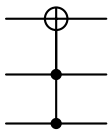

Figura 1.13: Símbolo para la puerta $CCNOT$.

$$CCNOT_{012}|000\rangle = |000\rangle , \quad CCNOT_{012}|100\rangle = |100\rangle ,$$
$$CCNOT_{012}|010\rangle = |010\rangle , \quad CCNOT_{012}|110\rangle = |110\rangle ,$$
$$CCNOT_{012}|001\rangle = |001\rangle , \quad CCNOT_{012}|101\rangle = |101\rangle ,$$
$$CCNOT_{012}|011\rangle = |111\rangle , \quad CCNOT_{012}|111\rangle = |011\rangle .$$

Para un p-cúbit con $p > 2$, la puerta $CCNOT_{ijk}$ tiene un cúbit objetivo, i, pero en este caso dos cúbits de control, j y k, de forma que solamente si en los controles tenemos 1 se cambiará el elemento del objetivo. Esta puerta es el análogo cuántico de la puerta AND clásica.

3. Puerta $SWAP_{01} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Figura 1.14: Símbolo para la puerta $SWAP$.

$$SWAP_{01}|00\rangle = |00\rangle, \quad SWAP_{01}|10\rangle = |01\rangle,$$
$$SWAP_{01}|01\rangle = |10\rangle, \quad SWAP_{01}|11\rangle = |11\rangle.$$

Para un p-cúbit, la puerta $SWAP_{ij}$ intercambia los términos de dos cúbits objetivo i y j, esta puerta se puede expresar como una composición de puertas $CNOT$:

$$\begin{aligned} CNOT_{10}CNOT_{01}CNOT_{10} &= \begin{pmatrix} 1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0 \end{pmatrix}\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}\begin{pmatrix} 1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0 \end{pmatrix} \\ &= \begin{pmatrix} 1&0&0&0\\0&0&1&0\\0&0&0&1\\0&1&0&0 \end{pmatrix}\begin{pmatrix} 1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0 \end{pmatrix} \\ &= \begin{pmatrix} 1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{pmatrix} = SWAP_{01}. \end{aligned}$$

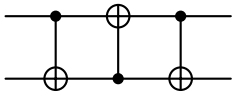

Figura 1.15: Puerta $SWAP$ en función de puertas $CNOT$s.

4. Puerta $CRT_{j,01} := \begin{pmatrix} I & \mathbf{0}_{2\times2} \\ \mathbf{0}_{2\times2} & RT_j \end{pmatrix} = \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{i\frac{2\pi}{2^j}} \end{pmatrix}$.

$$CRT_{j,01}|00\rangle = |00\rangle, \quad CRT_{j,01}|10\rangle = |10\rangle,$$
$$CRT_{j,01}|01\rangle = (RT_j|0\rangle)\otimes|1\rangle = |01\rangle,$$
$$CRT_{j,01}|11\rangle = (RT_j|1\rangle)\otimes|1\rangle = e^{i\frac{2\pi}{2^j}}|11\rangle.$$

La puerta de rotación parametrizada controlada, sólo aplica la puerta de rotación sobre el cúbit objetivo únicamente si el cúbit controlado está en el estado $|1\rangle$.

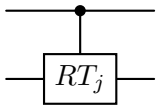

Figura 1.16: Símbolo para la puerta CRT_j.

Observación 1.68. La puerta $SWAP$ no sólo intercambia los dígitos en la base computacional de dos cúbits, si no que también puede intercambiar cuales dos estados arbitrarios haya en dichos cúbits. Por ejemplo, sea un 2-cúbit arbitrario descompuesto en función de los estadps $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ y $|\phi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ de forma que el estado del sistema total es $|\psi\rangle \otimes |\phi\rangle$, si aplicamos la puerta $SWAP_{01}$ a dicho estado se tiene que:

$$\begin{aligned} SWAP_{01}(|\psi\rangle \otimes |\phi\rangle) &= SWAP_{01}\left[(\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle)\right] \\ &= SWAP_{01}(\alpha_0\beta_0 |00\rangle + \alpha_1\beta_0 |10\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_1 |11\rangle) \\ &= \alpha_0\beta_0 |00\rangle + \alpha_1\beta_0 |01\rangle + \alpha_0\beta_1 |10\rangle + \alpha_1\beta_1 |11\rangle \\ &= \beta_0 |0\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + \beta_1 |1\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \\ &= (\beta_0 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \\ &= |\phi\rangle \otimes |\psi\rangle . \end{aligned}$$

1.3.3. Medición de un Cúbit

En un bit clásico, podemos observar directamente su estado (0 o 1) al final de las operaciones para ver el resultado de un circuito. En un cúbit, por su naturaleza cuántica, el estado resultante de observarlo tiene una naturaleza probabilística y se realiza mediante las llamadas *puertas de medición*, que colapsan el cúbit en uno de los dos estados de la base computacional ($|0\rangle$ o $|1\rangle$).

Figura 1.17: Símbolo para la puerta de medición.

Definición 1.69. Sea un p-cúbit $|\psi\rangle = \sum_{\vec{j}\in\{0,1\}^p} \alpha_{\vec{j}} \left|\vec{j}\right\rangle$, la **puerta de medición** aplicada en el cúbit k devuelve:

- $|0\rangle$ con una probabilidad:

$$P_k(|0\rangle) = \sum_{\vec{j}\in\{0,1\}^p,\ \vec{j}_k=0} \left|\alpha_{\vec{j}}\right|^2 .$$

- $|1\rangle$ con una probabilidad:

$$P_k(|1\rangle) = \sum_{\vec{j}\in\{0,1\}^p,\ \vec{j}_k=1} \left|\alpha_{\vec{j}}\right|^2 .$$

El estado resultante de aplicar esta puerta, habiendo medido $|x\rangle$, $x \in \{0,1\}$, en el cúbit k, es:

$$\left|\tilde{\psi}\right\rangle = \sum_{\vec{j}\in\{0,1\}^p,\ \vec{j}_k=x} \frac{\alpha_{\vec{j}}}{\sqrt{\sum_{\vec{j}\in\{0,1\}^p} \left|\alpha_{\vec{j}}\right|^2}} \left|\vec{j}\right\rangle .$$

Capítulo 2

Aplicaciones de la Computación Cuántica

En esta sección veremos algunos ejemplos muy conocidos de algoritmos cuánticos, que demuestran una mayor eficiencia en procesos de búsqueda o introducen algún concepto sobre comunicaciones cuánticas. Además, estudiaremos un tipo de problemas de gran interés para una gran variedad de campos, los sistemas lineales. Sus aplicaciones van desde la simulación de fluidos hasta la calibración de modelos financieros, por lo que una implementación cuántica, que mejore su eficiencia y precisión, será de gran interés cuando dispongamos de computadores cuánticos suficientemente sofisticados para ejecutarlos. En concreto, estudiaremos el algoritmo HHL (Harrow, Hassidim y Lloyd) [Vazquez et al., 2022] para sistemas lineales tridiagonales, como los que se suelen obtener al resolver la ecuación de Poisson empleando métodos numéricos como diferencias finitas [Christian Grossmann, 2007].

2.1. Algoritmos Cuánticos Relevantes

En esta sección estudiaremos varios de los algoritmos cuánticos más conocidos, algunos por ser ejemplo de las ventajas a nivel computacional que conlleva la lógica cuántica (Deustch-Jozsa, [Deutsch and Jozsa, 1992]), por tener algún uso sin análogo clásico (teletransportación cuántica, [Bennett et al., 1993]) o por ser piezas fundamentales en el desarrollo de algoritmos más complejos (QFT y QPE, [Scherer, 2019, Nielsen and Chuang, 2010]).

2.1.1. Teletransportación Cuántica

Pongámonos en la situación de que un emisor, *Alice*, quiere mandarle un mensaje a un receptor, *Bob*. Este mensaje estará codificado en el estado de un cúbit de la forma $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, donde la información relevante se puede obtener de los coeficientes de los estados de la base computacional α y β, que serán números complejos que verifican $|\alpha|^2 + |\beta|^2 = 1$. El problema está en que si *Alice* observa su estado cuántico para copiarlo y mandárselo a *Bob*, este colapsará en $|0\rangle$ o en $|1\rangle$, perdiendo la información del estado.

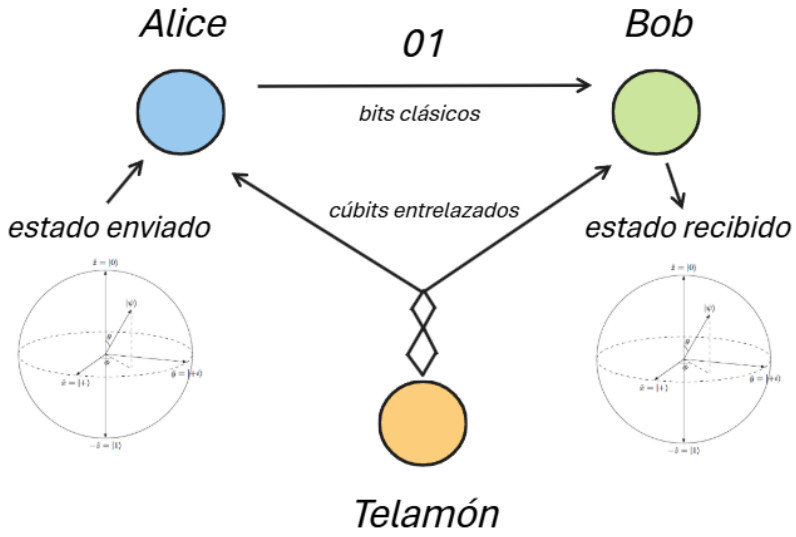

Figura 2.1: Esquema del algoritmo de teletransportación cuántica.

El **algoritmo de teletrasportación cuántica** [Bennett et al., 1993] resuelve este problema usando un sistema externo a ambos interlocutores, llamado *Telamón*, que les manda a ambos un estado entrelazado con el del otro. El término de teletransportación se usa porque, para mandar el mensaje, *Alice* debe ejecutar un circuito cuántico que destruye su estado y le manda a *Bob* cierta información clásica con la que puede reconstruir el estado original sobre su cúbit entrelazado.

$$\pi_0 : |\pi_0\rangle = |\psi\rangle \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$
$$= \frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle).$$

$$\pi_1 : |\pi_1\rangle = CNOT_{01} \otimes I_2\,|\pi_0\rangle = \frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle).$$

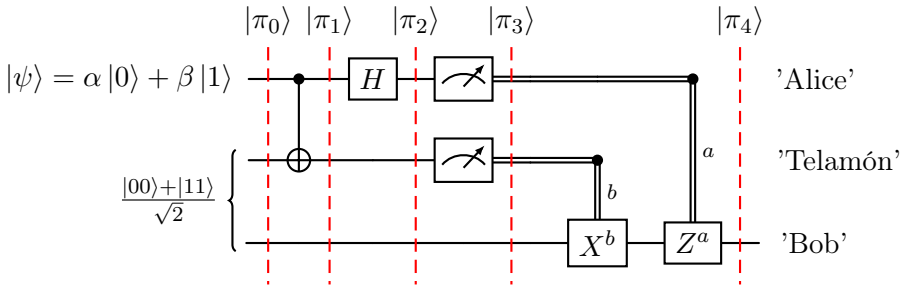

Figura 2.2: Algoritmo de teletransportación cuántica.

$$\pi_2 : |\pi_2\rangle = H \otimes I_2 \otimes I_2 |\pi_1\rangle = \frac{1}{\sqrt{2}}\Big[\frac{\alpha}{\sqrt{2}}(|000\rangle + |100\rangle) + \frac{\alpha}{\sqrt{2}}(|011\rangle + |111\rangle)$$
$$+ \frac{\beta}{\sqrt{2}}(|010\rangle - |110\rangle) + \frac{\beta}{\sqrt{2}}(|001\rangle - |101\rangle)\Big]$$
$$= \frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle) + \alpha|011\rangle + \alpha|111\rangle\,.$$

π_3 : *Alice* realiza la medición de su cúbit y la almacena en la variable clásica $a \in \{0,1\}$, destruyendo su estado cuántico. De forma análoga, el *Telamón* mide su cúbit y almacena el resultado en la variable clásica $b \in \{0,1\}$. Ambas variables son enviadas a *Bob* en la tupla (a,b), la cual tiene toda la información necesaria para recrear el estado $|\psi\rangle$ que originalmente tenía *Alice*. *Bob* aplicará una puerta X únicamente si recibe $b = 1$, a continuación, aplicará una puerta Z únicamente si recibe $a = 1$. Veamos qué ocurre para todas posibilidades de la tupla (a,b).

$(a = 0,\, b = 0)$: *Bob* no aplica ninguna puerta.

$$|\pi_3\rangle = \frac{\frac{1}{2}(\alpha|000\rangle + \beta|001\rangle)}{\sqrt{\alpha^2/4 + \beta^2/4}} = \alpha|000\rangle + \beta|001\rangle = |00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle).$$
$$|\pi_4\rangle_{Bob} = |\pi_3\rangle_{Bob} = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle\,.$$

$(a = 1,\, b = 0)$: *Bob* aplica una puerta Z.

$$|\pi_3\rangle = \frac{\frac{1}{2}(\alpha|100\rangle - \beta|101\rangle)}{\sqrt{\alpha^2/4 - \beta^2/4}} = \alpha|100\rangle - \beta|101\rangle = |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle).$$
$$|\pi_4\rangle_{Bob} = Z|\pi_3\rangle_{Bob} = Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle\,.$$

$(a = 0,\, b = 1)$: *Bob* aplica una puerta X.

$$|\pi_3\rangle = \frac{\frac{1}{2}(\alpha\,|011\rangle + \beta\,|010\rangle)}{\sqrt{\alpha^2/4 + \beta^2/4}} = \alpha\,|011\rangle + \beta\,|010\rangle = |01\rangle \otimes (\alpha\,|1\rangle + \beta\,|0\rangle).$$

$$|\pi_4\rangle_{Bob} = X\,|\pi_3\rangle_{Bob} = X(\alpha\,|1\rangle + \beta\,|0\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle = |\psi\rangle\,.$$

$(a = 1,\, b = 1)$: *Bob* aplica una puerta X y luego una puerta Z.

$$|\pi_3\rangle = \frac{\frac{1}{2}(\alpha\,|111\rangle - \beta\,|110\rangle)}{\sqrt{\alpha^2/4 + \beta^2/4}} = \alpha\,|111\rangle - \beta\,|110\rangle = |11\rangle \otimes (\alpha\,|1\rangle - \beta\,|0\rangle).$$

$$\begin{aligned}|\pi_4\rangle_{Bob} &= ZX\,|\pi_3\rangle_{Bob} = ZX(\alpha\,|1\rangle + \beta\,|0\rangle) \\ &= Z(\alpha\,|0\rangle - \beta\,|1\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle = |\psi\rangle\,.\end{aligned}$$

Como acabamos de comprobar, mediante la información clásica enviada por *Alice* y el *Telamón*, *Bob* puede recrear exactamente el mismo estado cuántico que originalmente tenía *Alice*, aplicando un circuito cuántico al estado entrelazado con el del *Telamón*.

2.1.2. Algoritmo de Deustch-Jozsa

El **problema de Deutsch** consiste en encontrar la manera más eficiente de determinar si una función $f : \{0,1\}^n \to \{0,1\}$ es **constante**, $f(x) = c \in \{0,1\}\ \forall x \in \{0,1\}^n$, o **balanceada**, $f(x) = 0$ y $f(x) = 1$ para la mitad de casos de $x \in \{0,1\}^n$. Esta eficiencia viene determinada por el número de veces que se debe aplicar la función f para determinar si es o no constante. Con cualquier método clásico, para asegurarnos de que la función es de uno de los dos tipos, debemos aplicarla un mínimo de dos veces y hasta un máximo de $2^{n-1} + 1$ veces, pues si en este último caso tenemos todos los valores iguales sabremos que es constante, ya que no estarían igualmente distribuidos.

En 1992, Deutsch y Jozsa [Deutsch and Jozsa, 1992] desarrollaron este problema y un algoritmo cuántico para resolverlo, con el que se observa un caso claro en el que la computación cuántica resulta mucho más eficiente que la clásica. En este circuito cuántico se emplea una puerta unitaria denotada por U_f que realiza la siguiente transformación:

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle\,,\ x \in \{0,1\}^n,\ y \in \{0,1\}.$$

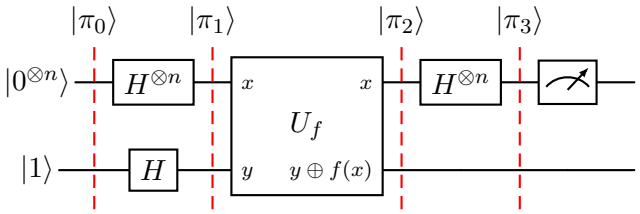

Figura 2.3: Algoritmo de Deutsch-Jozsa.

$$\pi_0 : \ |\pi_0\rangle = \left|0^{\otimes n}\right\rangle \otimes |1\rangle \, .$$

$$\pi_1 : \ |\pi_1\rangle = (H^{\otimes n} \otimes H)\,|\pi_0\rangle = (H^{\otimes n}\left|0^{\otimes n}\right\rangle) \otimes (H\,|1\rangle) = \Big[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\Big]^{\otimes n} \otimes \Big[-\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big]$$
$$= \frac{1}{\sqrt{2^{n+1}}}\Big[\sum_{x=0}^{2^n-1} |x\rangle_n \otimes (|0\rangle - |1\rangle)\Big].$$

$$\pi_2 : \ |\pi_2\rangle = U_f\,|\pi_1\rangle = \frac{1}{\sqrt{2^{n+1}}}\Big[\sum_{x=0}^{2^n-1} |x\rangle_n \otimes (|f(x)\rangle - |1 \oplus f(x)\rangle)\Big]:$$

-Si $f(x) = 0$: $|\pi_2\rangle = \dfrac{1}{\sqrt{2^{n+1}}}\Big[\displaystyle\sum_{x=0}^{2^n-1} |x\rangle_n \otimes (|0\rangle - |1\rangle)\Big]$.

-Si $f(x) = 1$: $|\pi_2\rangle = \dfrac{1}{\sqrt{2^{n+1}}}\Big[\displaystyle\sum_{x=0}^{2^n-1} |x\rangle_n \otimes (|1\rangle - |0\rangle)\Big] = -\dfrac{1}{\sqrt{2^{n+1}}}\Big[\displaystyle\sum_{x=0}^{2^n-1} |x\rangle_n \otimes (|0\rangle - |1\rangle)\Big]$.

$$|\pi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}\Big[\sum_{x=0}^{2^n-1} (-1)^{f(x)}\,|x\rangle_n \otimes (|0\rangle - |1\rangle)\Big] = \frac{1}{\sqrt{2^n}}\Big[\sum_{x=0}^{2^n-1} (-1)^{f(x)}\,|x\rangle_n\Big] \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}.$$

$$\pi_3 : \ |\pi_3\rangle = (H^{\otimes n} \otimes I_2)\,|\pi_2\rangle = H^{\otimes n}\Big[\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\,|x\rangle_n\Big] \otimes |-\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} H^{\otimes n}\,|x\rangle_n \otimes |-\rangle \, .$$

Por 1.65, se tiene que $H^{\otimes n}\,|x\rangle = \dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{z=0}^{2^n-1} (-1)^{x\cdot z}\,|z\rangle_n$, por tanto:.

$$|\pi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x\cdot z}\,|z\rangle_n \otimes |-\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{f(x)+x\cdot z}\,|z\rangle_n \otimes |-\rangle \, .$$

Omitiendo el término del último registro, correspondiente al estado $|-\rangle$, consideremos la proba-

bilidad de medir $|0^{\otimes n}\rangle$ en el estado final $|\pi_3\rangle$:

$$P(z=0) = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2.$$

Veamos que ocurre cuando la función es constante o balanceada:

-Constante:

$$P(z=0) = \left| \frac{\sum_{x=0}^{2^n-1}(-1)^{f(x)}}{2^n} \right|^2 = \left| \frac{\sum_{x=0}^{2^n-1}(-1)^{c}}{2^n} \right|^2 = \left| (-1)^c \frac{\sum_{x=0}^{2^n-1} 1}{2^n} \right|^2 = \left| (-1)^c \frac{2^n}{2^n} \right|^2 = 1.$$

-Balanceada:

$$P(z=0) = \left| \frac{\sum_{x=0}^{2^n-1}(-1)^{f(x)}}{2^n} \right|^2 = \left| \frac{\sum_{i=0}^{2^{(n-1)}-1} 1 + \sum_{i=0}^{2^{(n-1)}-1}(-1)}{2^n} \right|^2 = \left| \frac{\sum_{i=0}^{2^{(n-1)}-1}(1-1)}{2^n} \right|^2 = 0.$$

Por tanto, tras aplicar el circuito, si la función es constante, en los n primeros cúbits se medirá el estado $|0^{\otimes n}\rangle$ y, si la función es balanceada, este resultado no podrá salir. Por tanto, podemos determinar qué tipo de función es simplemente con una única ejecución del circuito y, en consecuencia, con una única aplicación de la función f, en comparación con las $2^{n-1}+1$ ejecuciones máximas que puede requerir asegurarlo en el caso clásico.

2.1.3. Transformada de Fourier Cuántica

La **transformada de Fourier Cuántica** (QFT) [Nielsen and Chuang, 2010, Scherer, 2019] es una implementación de la transformada de Fourier discreta en la computación cuántica. Es una parte fundamental de muchos algoritmos cuánticos, como el de estimación de fase, el algoritmo de Shor o el HHL. Para estudiar este algoritmo tomaremos un enfoque constructivo, partiendo de la definición de la transformada cuántica de Fourier hasta deducir la forma del circuito.

Definición 2.1 (DFT y QFT)**.** La **transformada de Fourier discreta** en un operador lineal sobre $\mathbb{C}^N$ de la forma:

$$\begin{aligned} DFT:\ \mathbb{C}^N &\longrightarrow \mathbb{C}^N \\ \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} &\longmapsto \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}, \end{aligned}$$

donde:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}, \tag{2.1}$$

siendo $\omega_N^{jk} = e^{2\pi i \frac{jk}{N}}$. Esto es,

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}.$$

La **transformada de Fourier cuántica** (QFT) es el caso particular para los cúbits, es decir, espacios de la forma $\mathbb{C}^{2^p}$. Empleando la notación de Dirac, se expresa de la siguiente forma:

$$\begin{aligned} QFT: \qquad & \mathbb{C}^{2^p} \longrightarrow \mathbb{C}^{2^p} \\ |X\rangle = \sum_{n=0}^{2^p-1} x_n \left|n\right\rangle_p \longmapsto & |Y\rangle = \sum_{k=0}^{2^p-1} y_k \left|k\right\rangle_p, \end{aligned}$$

donde y_k es el mismo que en la expresión 2.1 para $N = 2^p$.

Observación 2.2. Un caso particular es aplicar la QFT a la base computacional $\{\left|n\right\rangle_p\}_{n=0}^{2^p-1}$:

$$\begin{aligned} QFT \left|n\right\rangle_p &= \sum_{k=0}^{2^p-1} y_k \left|k\right\rangle_p \\ &= \sum_{k=0}^{2^p-1} \frac{1}{\sqrt{2^p}} \sum_{j=0}^{2^p-1} x_j \omega_{2^p}^{jk} \left|k\right\rangle_p \\ &= \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} \omega_{2^p}^{nk} \left|k\right\rangle_p \\ &= \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} e^{2\pi i \frac{nk}{2^p}} \left|k\right\rangle_p. \end{aligned} \tag{2.2}$$

De esta forma, el elemento de matriz del operador en la base computacional es:

$$\langle j| QFT \left|n\right\rangle = \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} \omega_{2^p}^{nk} \langle j|k\rangle = \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} \omega_{2^p}^{nk} \delta_{jk} = \frac{1}{\sqrt{2^p}} \omega_{2^p}^{nj},$$

por tanto, el operador QFT se podrá expresar de la siguiente forma:

$$\begin{aligned} QFT &= \frac{1}{\sqrt{2^p}} \sum_{n=0}^{2^p-1} \sum_{j=0}^{2^p-1} \omega_{2^p}^{nj} \left|j\right\rangle \langle n| \\ &= \frac{1}{\sqrt{2^p}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_{2^p}^{11} & \omega_{2^p}^{21} & \cdots & \omega_{2^p}^{2^p-1 1} \\ 1 & \omega_{2^p}^{12} & \omega_{2^p}^{22} & \cdots & \omega_{2^p}^{2^p-1 2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_{2^p}^{12^p-1} & \omega_{2^p}^{22^p-1} & \cdots & \omega_{2^p}^{2^p-1 2^p-1} \end{pmatrix}. \end{aligned} \tag{2.3}$$

Proposición 2.3. *El operador lineal QFT descrito en 2.1 es unitario.*

Demostración. Considerando la Proposición 1.28, dado $|\psi\rangle = \sum_{k=0}^{2^p-1} \alpha_k |k\rangle_p$, veamos que QFT conserva la norma:

$$\begin{aligned} |QFT\psi\rangle &= \frac{1}{\sqrt{2^p}} \sum_{n=0}^{2^p-1} \sum_{j=0}^{2^p-1} \sum_{k=0}^{2^p-1} \alpha_k \omega_{2^p}^{nj} |j\rangle \langle n|k\rangle \\ &= \frac{1}{\sqrt{2^p}} \sum_{j=0}^{2^p-1} \sum_{k=0}^{2^p-1} \alpha_k \omega_{2^p}^{kj} |j\rangle , \end{aligned}$$

por tanto:

$$\begin{aligned} \|QFT\psi\|^2 &= \langle QFT\psi | QFT\psi\rangle \\ &= \frac{1}{2^p} \sum_{j=0}^{2^p-1} \sum_{k=0}^{2^p-1} \sum_{i=0}^{2^p-1} \sum_{l=0}^{2^p-1} \alpha_l^* \omega_{2^p}^{li*} \alpha_k \omega_{2^p}^{kj} \langle i|j\rangle \\ &= \frac{1}{2^p} \sum_{j=0}^{2^p-1} \sum_{k=0}^{2^p-1} \sum_{l=0}^{2^p-1} \alpha_l^* \alpha_k \omega_{2^p}^{lj*} \omega_{2^p}^{kj} \\ &= \frac{1}{2^p} \sum_{j=0}^{2^p-1} \sum_{k=0}^{2^p-1} \sum_{l=0}^{2^p-1} \alpha_l^* \alpha_k e^{-2\pi i lj/2^p} e^{2\pi i kj/2^p} \\ &= \frac{1}{2^p} \sum_{k=0}^{2^p-1} \sum_{l=0}^{2^p-1} \alpha_l^* \alpha_k \sum_{j=0}^{2^p-1} [\exp(2\pi i(k-l)/2^p)]^j, \end{aligned}$$

si $k = l$, $\exp[2\pi i(k-l)/2^p]^j$=1. Por otro lado, si $k \neq l$:

$$\sum_{j=0}^{2^p-1} [\exp(2\pi i(k-l)/2^p)]^j = 0,$$

pues, si consideramos los términos $[\exp(2\pi i(k-l)/2^p)]^j$ como vectores en el plano complejo, se puede comprobar que en la suma anterior aparecen todos los vectores equidistantes en un ángulo $(k-l)/2^p$, hasta completar una vuelta entera de 2π radianes. En concreto, al ser un número par de vectores (2^p) equidistantes respecto al ángulo, se tendrá que, en la suma, siempre estará el opuesto de todo término. De esta forma, la suma total será nula. En consecuencia:

$$\begin{aligned} \|QFT\psi\|^2 &= \frac{1}{2^p} \sum_{k=0}^{2^p-1} \sum_{l=0}^{2^p-1} \alpha_l^* \alpha_k \delta_{lk} \\ &= \frac{1}{2^p} \sum_{k=0}^{2^p-1} \alpha_k^* \alpha_k \\ &= \|\psi\|^2 \Rightarrow \|QFT\psi\| = \|\psi\|. \end{aligned}$$

□

Ejemplo 2.4. Veamos el caso particular para un único cúbit, $p = 1$, entonces $\omega_2^{nj} = e^{2\pi i \frac{nj}{2}} = e^{i\pi nj}$, por tanto, el operador queda como:

$$\begin{aligned} QFT &= \frac{1}{\sqrt{2}} \sum_{n=0}^{1} \sum_{j=0}^{1} \omega_2^{ij} \left|j\right\rangle \left\langle n\right| \\ &= \frac{1}{\sqrt{2}} \sum_{n=0}^{1} \sum_{j=0}^{1} e^{i\pi nj} \left|j\right\rangle \left\langle n\right| \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H. \end{aligned}$$

Como hemos podido comprobar, para el caso de un único cúbit, el operador unitario del QFT coincide con la puerta de Hadamard. Veamos cómo se ven afectados los elementos de la base computacional:

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

La QFT realiza un cambio de base de la base computacional $\{\left|0\right\rangle, \left|1\right\rangle\}$ a una base transformada $\{\left|+\right\rangle, \left|-\right\rangle\}$, veamos cómo se observa esto en un cúbit $\left|\psi\right\rangle = \alpha \left|0\right\rangle + \beta \left|1\right\rangle$ arbitrario:

$$QFT \left|\psi\right\rangle = \alpha QFT \left|0\right\rangle + \beta QFT \left|1\right\rangle = \alpha \left|+\right\rangle + \beta \left|-\right\rangle.$$

Observación 2.5. Para poder construir un circuito cuántico general que realice la transformación descrita por el QFT, es conveniente expresarla en función de puertas lógicas más simples e implementables de forma directa en un ordenador cuántico. Sea $\left|n\right\rangle_p = \left|n_0 \dots n_{p-1}\right\rangle$ un estado de la base computacional del p-cúbit, de forma que $n = \sum_{i=0}^{p-1} n_i 2^i$, empleando la expresión 2.2:

$$QFT \left|n\right\rangle_p = \frac{1}{\sqrt{2^p}} \sum_{k=0}^{2^p-1} e^{2\pi i \frac{nk}{2^p}} \left|k\right\rangle_p,$$

usando la notación binaria 1.53 también para $\left|k\right\rangle_p = \left|k_0 \dots k_{p-1}\right\rangle$ con $k = \sum_{j=0}^{p-1} k_j 2^j$:

$$\begin{aligned} QFT \left|n\right\rangle_p &= \frac{1}{\sqrt{2^p}} \sum_{\vec{k} \in \{0,1\}^p} \exp\Big(\frac{2\pi i}{2^p} n \sum_{j=0}^{p-1} k_j 2^j\Big) \left|k_0 \dots k_{p-1}\right\rangle \\ &= \frac{1}{\sqrt{2^p}} \sum_{\vec{k} \in \{0,1\}^p} \exp\Big(\sum_{j=0}^{p-1} \frac{2\pi i}{2^p} n k_j 2^j\Big) \left|k_0 \dots k_{p-1}\right\rangle \\ &= \frac{1}{\sqrt{2^p}} \sum_{\vec{k} \in \{0,1\}^p} \prod_{j=0}^{p-1} \exp\Big(\frac{2\pi i}{2^{(p-j)}} n k_j\Big) \left|k_0 \dots k_{p-1}\right\rangle \\ &= \frac{1}{\sqrt{2^p}} \sum_{\vec{k} \in \{0,1\}^p} \prod_{j=0}^{p-1} \exp\Big(\frac{2\pi i}{2^{(p-j)}} n k_j\Big) \left|k_0 \dots k_{p-1}\right\rangle \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \Big[\exp\Big(\frac{2\pi i}{2^{(p-j)}} n0\Big)|0\rangle + \exp\Big(\frac{2\pi i}{2^{(p-j)}} n1\Big)|1\rangle \Big] \\
&= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \Big[|0\rangle + \exp\Big(\frac{2\pi i}{2^{(p-j)}} n\Big)|1\rangle \Big] \\
&= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \Big[|0\rangle + \exp\Big(\frac{2\pi i}{2^{(p-j)}} \sum_{i=0}^{p-1} n_i 2^i\Big)|1\rangle \Big] \\
&= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \Big[|0\rangle + \exp\Big(2\pi i \sum_{i=0}^{p-1} \frac{n_i}{2^{p-i-j}}\Big)|1\rangle \Big] \\
&= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \Big[|0\rangle + \prod_{i=0}^{p-1} \exp\Big(2\pi i \frac{n_i}{2^{p-j-i}}\Big)|1\rangle \Big]. \qquad (2.4)
\end{aligned}
$$

Nótese que en el denominador de la exponencial 2.4 aparece un término 2^{p-i-j} y el numerador es $2\pi i$ o 0 dependiendo del valor del cúbit $n_i \in \{0,1\}$. Entonces, si $p-i-j \leq 0$ se tiene que $\exp\big(2\pi i n_i/2^{p-i-j}\big) = 1$, por tanto, podremos reducir los valores de i a aquellos que verifiquen la desigualdad $i \leq p-j-1$:

$$
\begin{aligned}
QFT\,|n\rangle_p &= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \Big[|0\rangle + \prod_{i=0}^{p-1-j} \exp\Big(2\pi i \frac{n_i}{2^{(p-j-i)}}\Big)|1\rangle \Big] \\
&= \frac{\Big[|0\rangle + \prod_{i=0}^{p-1} \exp\Big(2\pi i \frac{n_i}{2^{(p-i)}}\Big)|1\rangle \Big]}{\sqrt{2}} \otimes \frac{\Big[|0\rangle + \prod_{i=0}^{p-2} \exp\Big(2\pi i \frac{n_i}{2^{(p-1-i)}}\Big)|1\rangle \Big]}{\sqrt{2}} \cdots \\
&\otimes \frac{\Big[|0\rangle + \prod_{i=0}^{1} \exp\Big(2\pi i \frac{n_i}{2^{(2-i)}}\Big)|1\rangle \Big]}{\sqrt{2}} \otimes \frac{\Big[|0\rangle + \exp\Big(2\pi i \frac{n_0}{2}\Big)|1\rangle \Big]}{\sqrt{2}}. \qquad (2.5)
\end{aligned}
$$

Ahora, buscaremos una forma de expresar cada término de esta última expresión en función de puertas lógicas conocidas. En concreto, nos centraremos en dos de ellas, la Hadamard y la de rotación controlada:

1) La puerta Hadamard, aplicada sobre los elementos de la base computacional $|x\rangle$, $x \in \{0,1\}$ de un cúbit, puede expresarse de la siguiente manera:

$$
H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \Rightarrow H\,|x\rangle = \frac{|0\rangle + (-1)^x\,|1\rangle}{\sqrt{2}} = \frac{|0\rangle + \exp\Big(2\pi i \frac{x}{2}\Big)|1\rangle}{\sqrt{2}}. \qquad (2.6)
$$

2) La puerta de rotación controlada, $CRT_{l,ji} \equiv CRT_l^{(j,i)}$, para $|x_0 x_1\rangle$, con $x_i, x_j \in \{0,1\}$, (2.7)

verifica:

$$
CRT_{l,ji}\,|0x_j\rangle = |0x_j\rangle\,,\ CRT_{l,ji}\,|1x_j\rangle = \exp\Big(2\pi i \frac{x_j}{2^l}\Big)|1x_j\rangle\,. \qquad (2.8)
$$

Denotemos por β_j cada término de 2.5 de forma que:

$$\beta_j = |0\rangle + \prod_{i=0}^{p-1-j} \exp\left(2\pi i \frac{n_i}{2^{(p-j-i)}}\right)|1\rangle\,. \tag{2.9}$$

Veamos cómo descomponer el producto de forma escalonada en estas puertas:

$$\begin{aligned}
QFT\,|n\rangle_p &= \frac{1}{\sqrt{2^p}} \bigotimes_{j=0}^{p-1} \beta_j = \frac{1}{\sqrt{2^{p-1}}} \left(\bigotimes_{j=0}^{p-2} \beta_j\right) \otimes \frac{\beta_{p-1}}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^{p-1}}} \left(\bigotimes_{j=0}^{p-2} \beta_j\right) \otimes \frac{\left[|0\rangle + \exp\left(2\pi i \frac{n_0}{2}\right)|1\rangle\right]}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^{p-1}}} \left(\bigotimes_{j=0}^{p-2} \beta_j\right) \otimes (H\,|n_0\rangle) = (I_{2^{p-1}} \otimes H) \left[\frac{1}{\sqrt{2^{p-1}}} \left(\bigotimes_{j=0}^{p-2} \beta_j\right) \otimes |n_0\rangle\right].
\end{aligned}$$

Como hemos podido comprobar, el último término del producto tensorial se corresponde con aplicar una puerta Hadamard al último cúbit. Para simplificar la notación, omitiremos la puerta $(I_{2^{p-1}} \otimes H)$ y veremos que ocurre con los términos restantes:

$$\begin{aligned}
&\frac{1}{\sqrt{2^{p-1}}} \left(\bigotimes_{j=0}^{p-2} \beta_j\right) \otimes |n_0\rangle = \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \frac{\left[|0\rangle + \prod_{i=0}^{1} \exp\left(2\pi i \frac{n_i}{2^{(2-i)}}\right)|1\rangle\right]}{\sqrt{2}} \otimes |n_0\rangle \\
&= \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \frac{\left[|0\rangle + \exp\left(2\pi i \frac{n1}{2}\right)\exp\left(2\pi i \frac{n_0}{2^2}\right)|1\rangle\right]}{\sqrt{2}} \otimes |n_0\rangle \\
&= \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \frac{\left[|0n_0\rangle + \exp\left(2\pi i \frac{n1}{2}\right)\exp\left(2\pi i \frac{n_0}{2^2}\right)|1n_0\rangle\right]}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \frac{1}{\sqrt{2}} \big[CRT_2^{(p-1,p-2)}\,|0n_0\rangle \\
&+ \exp\left(2\pi i \frac{n1}{2}\right) CRT_2^{(p-1,p-2)}\,|1n_0\rangle\big] \\
&= \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \frac{1}{\sqrt{2}} \Big[CRT_2^{(p-1,p-2)} \left(|0n_0\rangle + \exp\left(2\pi i \frac{n1}{2}\right)|1n_0\rangle\right)\Big] \\
&= \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \Big[CRT_2^{(p-1,p-2)} \frac{\left(|0\rangle + \exp\left(2\pi i \frac{n1}{2}\right)|1\rangle\right)}{\sqrt{2}} \otimes |n_0\rangle\Big] \\
&= \frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes \Big[CRT_2^{(p-1,p-2)} (H\,|n_1\rangle) \otimes |n_0\rangle\Big] \\
&= \big[CRT_2^{(p-1,p-2)} (I_{2^{p-2}} \otimes H \otimes I_2)\big] \left[\frac{1}{\sqrt{2^{p-2}}} \left(\bigotimes_{j=0}^{p-3} \beta_j\right) \otimes |n_1 n_0\rangle\right].
\end{aligned} \tag{2.10}$$

Se tiene entonces que:

$$QFT\,|n\rangle_p = (I_{2^{p-1}} \otimes H)\big[CRT_2^{(p-1,p-2)}(I_{2^{p-2}} \otimes H \otimes I_2)\big]\left[\frac{1}{\sqrt{2^{p-2}}}\left(\bigotimes_{j=0}^{p-3}\beta_j\right)\otimes|n_1 n_0\rangle\right].$$

Sea $m \geq 0$ el parámetro de inducción, hagamos la siguiente hipótesis:

$$\begin{aligned}
&\frac{1}{\sqrt{2^{p-m}}}\left(\bigotimes_{j=0}^{p-1-m}\beta_j\right)\otimes|n_{m-1}\dots n_0\rangle \\
&\qquad = \left[\prod_{l=2}^{m+1} CRT_l^{(p+1-l,p-m-1)}\right]\cdot\Big(I_{2^{(p-1-m)}} \otimes H \otimes I_{2^m}\Big) \\
&\qquad \cdot\left[\frac{1}{\sqrt{2^{p-(m+1)}}}\left(\bigotimes_{j=0}^{p-1-(m+1)}\beta_j\right)\otimes|n_m n_{m-1}\dots n_0\rangle\right],
\end{aligned} \tag{2.11}$$

por 2.10, tenemos que se verifica para $m = 1$:

$$\begin{aligned}
&\frac{1}{\sqrt{2^{p-1}}}\left(\bigotimes_{j=0}^{p-2}\beta_j\right)\otimes|n_0\rangle \\
&\qquad = \left[\prod_{l=2}^{2} CRT_l^{(p+1-l,p-2)}\right]\cdot\Big(I_{2^{p-2}} \otimes H \otimes I_2\Big) \\
&\qquad \cdot\left[\frac{1}{\sqrt{2^{p-2}}}\left(\bigotimes_{j=0}^{p-3}\beta_j\right)\otimes|n_1 n_0\rangle\right].
\end{aligned} \tag{2.12}$$

Supongamos ahora que 2.11 se verifica para m, veamos si se cumple para $m+1$:

$$\begin{aligned}
&\frac{1}{\sqrt{2^{p-(m+1)}}}\left(\bigotimes_{j=0}^{p-1-(m+1)}\beta_j\right)\otimes\big|n_{(m+1)-1}\dots n_0\big\rangle \\
&= \frac{1}{\sqrt{2^{p-[(m+1)+1]}}}\left(\bigotimes_{j=0}^{p-1-[(m+1)+1]}\beta_j\right)\otimes\frac{1}{\sqrt{2}}\beta_{p-1-(m+1)}\otimes|n_m\dots n_0\rangle \\
&= \cdots\otimes\frac{\Big[|0\rangle + \prod_{i=0}^{(m+1)}\exp\Big(2\pi i\frac{n_i}{2^{[(m+1)+1-i]}}\Big)|1\rangle\Big]}{\sqrt{2}}\otimes|n_m\dots n_0\rangle \\
&= \cdots\otimes\frac{1}{\sqrt{2}}\Big[|0n_m\dots n_0\rangle + \prod_{i=0}^{(m+1)}\exp\Big(2\pi i\frac{n_i}{2^{[(m+1)+1-i]}}\Big)|1n_m\dots n_0\rangle\Big] \\
&= \cdots\otimes\frac{1}{\sqrt{2}}\Big[|0n_m\dots n_0\rangle \\
&+ \exp\Big(2\pi i\frac{n_0}{2^{[(m+1)+1]}}\Big)\dots\exp\Big(2\pi i\frac{n_m}{2^2}\Big)\exp\Big(2\pi i\frac{n_{(m+1)}}{2}\Big)|1n_m\dots n_0\rangle\Big] \\
&= \cdots\otimes\frac{1}{\sqrt{2}}\Big[\exp\Big(2\pi i\frac{n_0}{2^{[(m+1)+1]}}\Big)\dots\exp\Big(2\pi i\frac{n_m}{2^2}\Big)|0n_m\dots n_0\rangle
\end{aligned}$$

$$
\begin{aligned}
&+ \exp\left(2\pi i \frac{n_0}{2^{[(m+1)+1]}}\right) \ldots \exp\left(2\pi i \frac{n_m}{2^2}\right) \exp\left(2\pi i \frac{n_{(m+1)}}{2}\right) |1 n_m \ldots n_0\rangle \Big] \\
&= \cdots \otimes \frac{1}{\sqrt{2}} \Big[CRT_{(m+1)+1}^{(p-1,p-1-(m+1))} \ldots CRT_2^{(p-1-m,p-1-(m+1))} |0 n_m \ldots n_0\rangle \\
&+ CRT_{(m+1)+1}^{(p-1,p-1-(m+1))} \ldots CRT_2^{(p-1-m,p-1-(m+1))} \exp\left(2\pi i \frac{n_{(m+1)}}{2}\right) |1 n_m \ldots n_0\rangle \Big] \\
&= \cdots \otimes CRT_{(m+1)+1}^{(p-1,p-1-(m+1))} \ldots CRT_2^{(p-1-m,p-1-(m+1))} \frac{1}{\sqrt{2}} \Big[|0 n_m \ldots n_0\rangle \\
&+ \exp\left(2\pi i \frac{n_{(m+1)}}{2}\right) |1 n_m \ldots n_0\rangle \Big] \\
&= \cdots \otimes CRT_{(m+1)+1}^{(p-1,p-1-(m+1))} \ldots CRT_2^{(p-1-m,p-1-(m+1))} \\
&\cdot \left[\frac{\left[|0\rangle + \exp\left(2\pi i \frac{n_{(m+1)}}{2}\right) |1\rangle \right]}{\sqrt{2}} \otimes |n_m \ldots n_0\rangle \right] \\
&= \cdots \otimes CRT_{(m+1)+1}^{(p-1,p-1-(m+1))} \ldots CRT_2^{(p-1-m,p-1-(m+1))} \left[(H |n_{m+1}\rangle) \otimes |n_m \ldots n_0\rangle \right] \\
&= \cdots \otimes \prod_{l=2}^{(m+1)+1} CRT_l^{(p+1-l,p-1-(m+1))} (I_{2^{p-1-(m+1)}} \otimes H \otimes I_{2^{(m+1)}}) |n_{m+1} n_m \ldots n_0\rangle \\
&= \prod_{l=2}^{(m+1)+1} CRT_l^{(p+1-l,p-1-(m+1))} (I_{2^{p-1-(m+1)}} \otimes H \otimes I_{2^{(m+1)}}) \\
&\cdot \left[\frac{1}{\sqrt{2^{p-[(m+1)+1]}}} \left(\bigotimes_{j=0}^{p-1-[(m+1)+1]} \beta_j \right) \otimes |n_{m+1} n_m \ldots n_0\rangle \right],
\end{aligned}
$$

que es fácil comprobar que coincide con la hipótesis 2.11 para $m+1$. Tomando $s = p-1-m$:

$$
\begin{aligned}
QFT\,|n\rangle_p &= QFT\,|n_0 \ldots n_{p-1}\rangle \\
&= \left[\prod_{s=0}^{p-1} \left(\prod_{l=2}^{p-s} CRT_l^{(p+1-l,s)} \right) \left(I_{2^s} \otimes H \otimes I_{2^{(p-1-s)}} \right) \right] |n_{p-1} \ldots n_0\rangle \,, \qquad (2.13)
\end{aligned}
$$

y haciendo un cambio de índices de la forma $s \leftrightarrow (p-1-s)$, que se corresponde con la imagen especular del circuito, obtenemos la siguiente expresión:

$$
QFT\,|n_{p-1} \ldots n_0\rangle = \left[\prod_{m=0}^{p-1} \left(\prod_{l=2}^{m+1} CRT_l^{(p+1-l,p-1-m)} \right) \left(I_{2^{(p-1-m)}} \otimes H \otimes I_{2^m} \right) \right] |n_0 \ldots n_{p-1}\rangle \,. \qquad (2.14)
$$

Además, por la Definición 2.1:

$$
QFT\,|n_0 \ldots n_{p-1}\rangle = \left(\prod_{i=0}^{\lfloor \frac{p-1}{2} \rfloor} SWAP_{i,(p-1-i)} \right) QFT\,|n_{p-1} \ldots n_0\rangle \,, \qquad (2.15)
$$

entonces:

$$QFT\,|n\rangle_p = \left(\prod_{i=0}^{\lfloor\frac{p-1}{2}\rfloor} SWAP_{i,(p-1-i)}\right) QFT\,|n_{p-1}\dots n_0\rangle$$
$$= \left(\prod_{i=0}^{\lfloor\frac{p-1}{2}\rfloor} SWAP_{i,(p-1-i)}\right)\left[\prod_{m=0}^{p-1}\left(\prod_{l=2}^{m+1} CRT_l^{(p+1-l,p-1-m)}\right)\left(I_{2^{(p-1-m)}}\otimes H\otimes I_{2^m}\right)\right]|n_0\dots n_{p-1}\rangle\,. \tag{2.16}$$

Finalmente, en esta expresión aparecen, de forma explícita, únicamente puertas H, CRT y $SWAP$. Además, por construcción, está garantizado que se corresponde con el unitario asociado a la QFT. Por tanto, 2.16 nos permite construir un circuito cuántico que realice la transformación de la QFT de forma exacta, empleando puertas aplicables en ordenadores cuánticos reales.

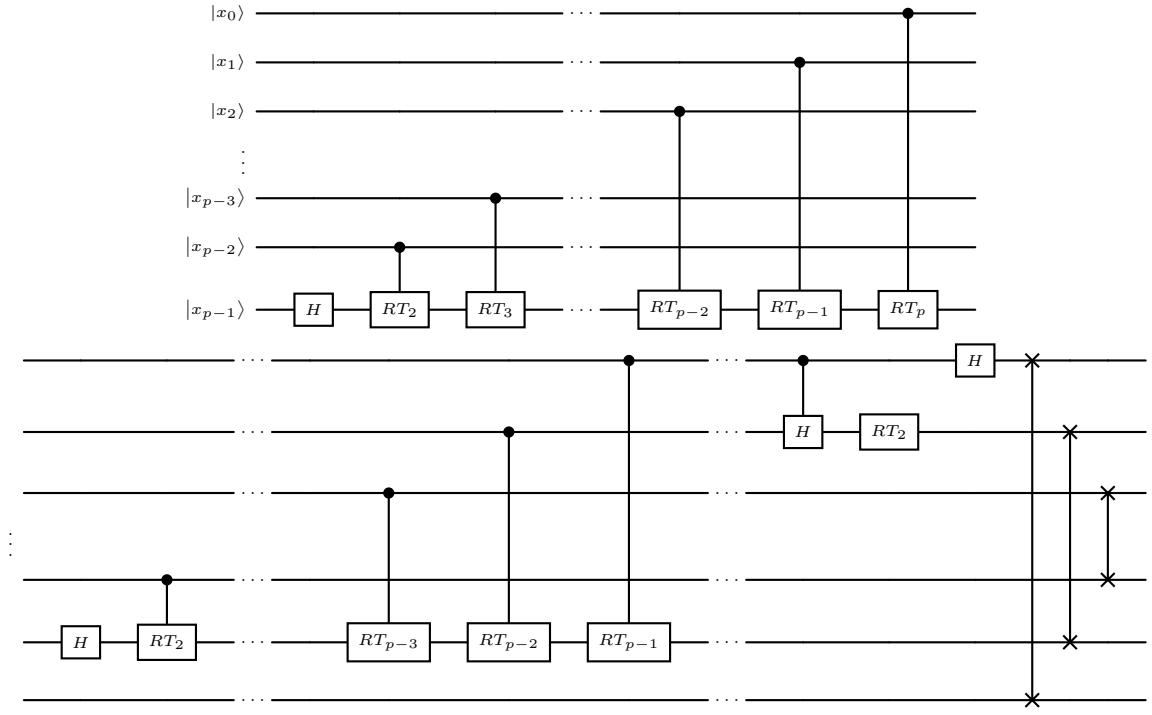

Figura 2.4: Algoritmo QFT.

2.1.4. Algoritmo de Estimación de Fase

El llamado **algoritmo de estimación de fase** [Nielsen and Chuang, 2010, Scherer, 2019] o QPE por sus siglas en inglés ("Quantum Phase Estimation") es el paso siguiente a la QFT. Dado un operador unitario U arbitrario, el algoritmo QPE estima el valor de la fase θ de un autovalor de U, de la forma $U\,|\psi\rangle = e^{i2\pi\theta}\,|\psi\rangle$, con $|\psi\rangle$ el autoestado asociado al autovalor $e^{i2\pi\theta}$.

Como U es unitario y $|\psi\rangle$ es un estado del cúbit, los autovalores del operador deben tener norma igual a 1, para preservar la norma del autoestado.

Veamos la forma del circuito:

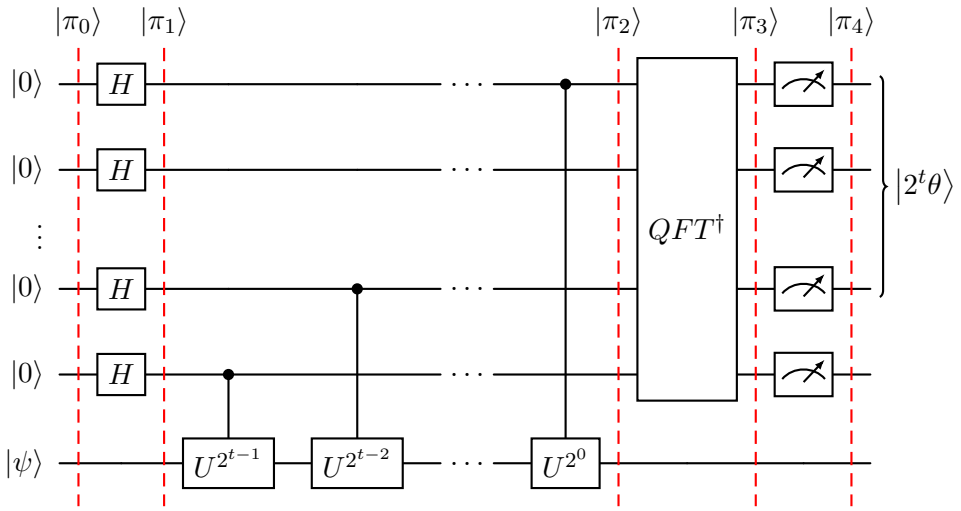

Figura 2.5: Algoritmo QPE.

$\pi_0:\ |\pi_0\rangle = |0\rangle^{\otimes t} \otimes |\psi\rangle\,.$

$\pi_1:\ |\pi_1\rangle = H^{\otimes t} \otimes I_2\,|\pi_0\rangle = (H^{\otimes t}\,|0\rangle^{\otimes t}) \otimes |\psi\rangle = \dfrac{1}{\sqrt{2^t}}(|0\rangle + |1\rangle)^{\otimes t} \otimes |\psi\rangle\,.$

$$\pi_2:\ |\pi_2\rangle = \prod_{j=0}^{t-1} CU^{2^{(t-1-j)}}_{t-1-j,t+1}\,|\pi_1\rangle = \frac{1}{\sqrt{2^t}} \bigotimes_{j=0}^{t-1}\Big[|0\rangle + (I_2 \otimes U^{2^j})\,|1\rangle\Big] \otimes |\psi\rangle$$

$$= \frac{1}{\sqrt{2^t}} \bigotimes_{j=0}^{t-1}\Big[|0\rangle + e^{i2\pi\theta 2^j}\,|1\rangle\Big] \otimes |\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} \exp\Big(i2\pi\theta \sum_{j=0}^{t-1} k_j 2^j\Big)|k_0 \ldots k_{t-1}\rangle \otimes |\psi\rangle$$

$$= \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{i2\pi\theta k}\,|k\rangle_t \otimes |\psi\rangle\,.$$

$$\pi_3:\ |\pi_3\rangle = QFT^\dagger \otimes I_2\,|\pi_2\rangle = QFT^\dagger\Big(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{i2\pi\theta k}\,|k\rangle_t\Big) \otimes |\psi\rangle$$

$$= \Big(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{i2\pi\theta k} QFT^\dagger\,|k\rangle_t\Big) \otimes |\psi\rangle = \Big(\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1}\sum_{l=0}^{2^t-1} e^{i2\pi\theta k} \frac{1}{\sqrt{2^t}} e^{-i2\pi\frac{kl}{2^t}}\,|l\rangle_t\Big) \otimes |\psi\rangle$$

$$= \Big(\frac{1}{2^t} \sum_{k=0}^{2^t-1}\sum_{l=0}^{2^t-1} e^{i2\pi k(\theta - \frac{l}{2^t})}\,|l\rangle_t\Big) \otimes |\psi\rangle = \Big(\frac{1}{2^t} \sum_{l=0}^{2^t-1}\sum_{k=0}^{2^t-1} e^{i\frac{2\pi k}{2^t}(\theta 2^t - l)}\,|l\rangle_t\Big) \otimes |\psi\rangle\,.$$

π_4 : Calculemos las probabilidades de medir cada valor de l, con $l = 0, \ldots, 2^{t-1}$:

$$P_l = \frac{1}{2^{2t}} \left| \sum_{k=0}^{2^t-1} e^{i\frac{2\pi k}{2^t}(\theta 2^t - l)} \right|^2 = \frac{1}{2^{2t}} \sum_{m=0}^{2^t-1} \sum_{k=0}^{2^t-1} e^{i\frac{2\pi k}{2^t}(\theta 2^t - l)} e^{-i\frac{2\pi m}{2^t}(\theta 2^t - l)}$$
$$= \frac{1}{2^{2t}} \sum_{m=0}^{2^t-1} \sum_{k=0}^{2^t-1} e^{i\frac{2\pi}{2^t}(\theta 2^t - l)(k-m)},$$

como $P_l \in \mathbb{R}$, sólo sumarán los términos en los que $k = m$ ó $l = 2^t\theta$. Por tanto, el estado $\left|2^t\theta\right\rangle$ será el más probable, en el caso de que $2^t\theta$ sea entero, con probabilidad:

$$P_{l=2^t\theta} = \frac{2 \cdot 2^t}{2^{2t}} = \frac{1}{2^{t-1}},$$
$$P_{l\neq 2^t\theta} = \frac{2^t}{2^{2t}} = \frac{1}{2^t}.$$

En consecuencia, si $2^t\theta$ es entero, el estado $\left|l = 2^t\theta\right\rangle$ tendrá el doble de probabilidad que cualquier otro. Para obtener la fase, bastará despejar $\theta = l/2^t$. Además, se tiene que si $2^t\theta$ no es entero, el entero más próximo a este valor también tendrá mayor probabilidad que el resto.

2.2. Resolución de Sistemas Lineales. Algoritmo HHL

La resolución de ecuaciones lineales juega un papel importante en una gran variedad de problemas, por ejemplo, en la simulación de fluidos [Christian Grossmann, 2007]. Existen múltiples métodos clásicos para su resolución, como la eliminación Gaussiana, factorización QR [Golub and Van Loan, 2013] o el método del gradiente-conjugado [Hestenes and Stiefel, 1952]. El algoritmo cuántico HHL [Vazquez et al., 2022], diseñado para matrices tridiagonales dispersas, presenta una mejora en cuanto al orden, por lo que su estudio es de gran interés.

Definición 2.6. Se dice que una matriz $A = (a_{ij}) \in \mathcal{M}_{N\times N}(\mathbb{R})$ es **tridiagonal** si:

$$a_{ij} \neq 0 \Rightarrow |i - j| \leq 1,$$

es decir, la matriz tiene todos sus elementos nulos salvo, quizá, en la diagonal principal y en las primeras subdiagonales. Además, sean $\mathbf{x}, \mathbf{b} \in \mathbb{R}^N$ dos vectores, el sistema $A \cdot \mathbf{x} = \mathbf{b}$ se denomina **sistema tridiagonal**.

Consideremos una matriz hermítica $A \in \mathcal{M}_{N\times N}(\mathbb{R})$ tridiagonal, con $N = 2^{n_b}$ y $n_b \in \mathbb{N}$; sea un vector $\mathbf{b} \in \mathbb{R}^{2^{n_b}}$ que podremos asumir normalizado, es decir, $\|\mathbf{b}\| = 1$. Podemos considerar entonces $\mathbf{b}$ como un estado n_b-cúbit en el espacio de Hilbert $\mathbb{C}^{2^{n_b}}$, escribiéndolo en la notación de Dirac como $|b\rangle$. De esta forma, el sistema lineal tridiagonal $A \cdot \mathbf{x} = \mathbf{b}$ se puede representar por:

$$A\,|x\rangle = |b\rangle\,,$$

siendo $|x\rangle$ un estado del n_b-cúbit, no necesariamente perteneciente a $\mathbb{R}^{2^{n_b}}$. Por tanto, queremos un algoritmo que obtenga un estado $|x\rangle$, que tendrá las propiedades necesarias para deducir el vector $\mathbf{x}$, para ello, deberemos obtener un circuito que realice la transformación $|x\rangle = A^{-1}|b\rangle$.

Sean $\{|u_j\rangle\}_{j=0}^{2^{n_b}-1}$ los autovectores de la matriz A con sus respectivos autovalores $\{\lambda_j\}_{j=0}^{2^{n_b}-1}$, consideremos la descomposición espectral de A:

$$A = \sum_{j=0}^{2^{n_b}-1} \lambda_j |u_j\rangle \langle u_j| ,$$

se tiene entonces que la inversa de la matriz se puede expresar de la siguiente forma:

$$A^{-1} = \sum_{j=0}^{2^{n_b}-1} \lambda_j^{-1} |u_j\rangle \langle u_j| .$$

Si consideramos el estado $|b\rangle$ en función de la base anterior de autoestados, podemos expresar el estado objetivo como sigue:

$$\begin{aligned} |\tilde{x}\rangle &= A^{-1}|b\rangle \\ &= \left(\sum_{j=0}^{2^{n_b}-1} \lambda_j^{-1} |u_j\rangle \langle u_j|\right)\left(\sum_{k=0}^{2^{n_b}-1} b_k |u_k\rangle\right) \\ &= \sum_{j=0}^{2^{n_b}-1} \lambda_j^{-1} b_j |u_j\rangle . \end{aligned} \tag{2.17}$$

Si se tiene que $\sum_{j=0}^{2^{n_b}-1} |b_j/\lambda_j|^2 = 1$, entonces la expresión 2.17 será el estado unitario que se busca.

El **algoritmo HHL** (Harrow, Hassidim y Lloyd) se puede resumir en los siguientes pasos, que desarrollaremos más adelante:

(1) Inicializar el estado $|b\rangle$ en un n_b-cúbit.

(2) Añadir un n_l-cúbit, con $n_l \in \mathbb{N}$, y aplicar el QPE con el operador unitario $U = e^{iAt}$, siendo $t \in \mathbb{R},\ t > 0$, que puede expresarse en función de los autoestados de A:

$$e^{iAt} = \sum_{j=0}^{2^{n_b}-1} e^{i\lambda_j t} |u_j\rangle \langle u_j| = \sum_{j=0}^{2^{n_b}-1} e^{2\pi i \frac{\lambda_j t}{2\pi}} |u_j\rangle \langle u_j| .$$

El estado resultante es de la forma:

$$\sum_{j=0}^{2^{n_b}-1} \beta_j \left|\tilde{\lambda}_j\right\rangle_{n_l} \otimes |u_j\rangle_{n_b} ,$$

donde $\tilde{\lambda}_j = 2^{n_l}\lambda_j t/2\pi$.

(3) Añadir un cúbit ancilla y aplicar la rotación condicionada sobre $|\lambda_j\rangle_{n_l}$, obteniendo:

$$\sum_{j=0}^{2^{n_b}-1} \beta_j \left|\tilde{\lambda}_j\right\rangle_{n_l} \otimes |u_j\rangle_{n_b} \left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}\,|0\rangle + \frac{C}{\tilde{\lambda}_j}\,|1\rangle\right),$$

siendo $C \in \mathbb{C}$ una constante de normalización.

(4) Aplicar la QPE inversa, obteniendo:

$$\sum_{j=0}^{2^{n_b}-1} \beta_j \,|0\rangle_{n_l} \otimes |u_j\rangle_{n_b} \left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}\,|0\rangle + \frac{C}{\tilde{\lambda}_j}\,|1\rangle\right).$$

(5) Medir el cúbit ancilla en la base computacional, si se mide $|1\rangle$, el estado del resto de registros será:

$$\left(\sqrt{\frac{1}{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}}\right) \sum_{j=0}^{2^{n_b}-1} \frac{\beta_j C}{\tilde{\lambda}_j}\,|0\rangle_{n_l} \otimes |u_j\rangle_{n_b}\,,$$

si el resultado es $|0\rangle$, se debe repetir el proceso desde el principio.

Se puede verificar que el estado del n_b-cúbit en una ejecución exitosa del algoritmo verifica la ecuación $A\,|x\rangle = |b\rangle$, salvo por un factor de normalización. Para comprobarlo en detalle:

$$\begin{aligned}
&A\left(\sqrt{\frac{1}{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}}\right) \sum_{j=0}^{2^{n_b}-1} \frac{\beta_j C}{\tilde{\lambda}_j}\,|u_j\rangle_{n_b} \\
&= \left(\sqrt{\frac{1}{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}}\right) \sum_{j=0}^{2^{n_b}-1} \frac{\beta_j C}{\tilde{\lambda}_j} A\,|u_j\rangle_{n_b} \\
&= \left(\sqrt{\frac{1}{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}}\right) \sum_{j=0}^{2^{n_b}-1} \frac{\beta_j C}{\tilde{\lambda}_j} \tilde{\lambda}_j\,|u_j\rangle_{n_b} \\
&= \frac{C}{\sqrt{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}} \sum_{j=0}^{2^{n_b}-1} \beta_j\,|u_j\rangle_{n_b}\,,
\end{aligned}$$

como β_j es la componente del vector $|b\rangle$ en la base de autoestados $\{|u_j\rangle_{n_b}\}$, se tiene que $\sum_{j=0}^{2^{n_b}-1} \beta_j\,|u_j\rangle_{n_b} = |b\rangle$ y, por tanto:

$$\frac{C}{\sqrt{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}} \sum_{j=0}^{2^{n_b}-1} \beta_j\,|u_j\rangle_{n_b} = \frac{C}{\sqrt{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / \left|\tilde{\lambda}_k\right|^2}}\,|b\rangle\,.$$

Suponiendo que si $\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2 / |\lambda_k|^2 = 1$, entonces se recupera el estado $|b\rangle$, como queríamos comprobar.

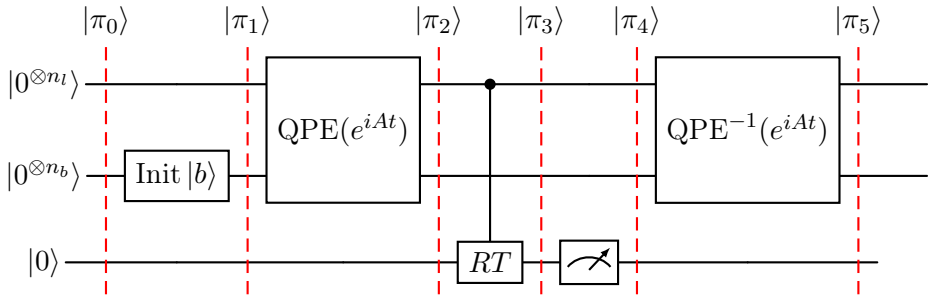

Figura 2.6: Algoritmo HHL simplificado.

$\pi_0 :\ |\pi_0\rangle = \left|0^{\otimes n_l}\right\rangle \otimes \left|0^{\otimes n_b}\right\rangle \otimes |0\rangle\,.$

$\pi_1 :\ |\pi_1\rangle = \text{Init}(|b\rangle)\,|\pi_0\rangle = \left|0^{\otimes n_l}\right\rangle \otimes |b\rangle_{n_b} \otimes |0\rangle\,.$

$\pi_2 :\ |\pi_2\rangle = \text{QPE}(e^{iAt})\big[\left|0^{\otimes n_l}\right\rangle \otimes |b\rangle_{n_b}\big] \otimes |0\rangle\,.$

Expresando $|b\rangle$ en función de la base de autoestados de A, $|b\rangle_{n_b} = \sum_{j=0}^{2^{n_b}-1} \beta_j\,|u_j\rangle_{n_b}$, se tiene:

$$\begin{aligned}
|\pi_2\rangle &= \text{QPE}(e^{iAt})\Big[\left|0^{\otimes n_l}\right\rangle \otimes \sum_{j=0}^{2^{n_b}-1} \beta_j\,|u_j\rangle_{n_b}\Big] \otimes |0\rangle \\
&= \sum_{j=0}^{2^{n_b}-1} \beta_j \text{QPE}(e^{iAt})\big[\left|0^{\otimes n_l}\right\rangle \otimes |u_j\rangle_{n_b}\big] \otimes |0\rangle \\
&= \sum_{j=0}^{2^{n_b}-1} \beta_j \big[\left|\tilde{\lambda}_j\right\rangle \otimes |u_j\rangle_{n_b}\big] \otimes |0\rangle\,,
\end{aligned}$$

donde $\tilde{\lambda}_j = 2^{n_l}\lambda_j t/2\pi$.

$$\begin{aligned}
\pi_3 :\ |\pi_3\rangle &= CRT_{0,\ldots,n_l-1;n_l+n_b} \sum_{j=0}^{2^{n_b}-1} \beta_j \big[\left|\tilde{\lambda}_j\right\rangle \otimes |u_j\rangle_{n_b} \otimes |0\rangle\big] \\
&= \sum_{j=0}^{2^{n_b}-1} \beta_j CRT_{0,\ldots,n_l-1;n_l+n_b} \big[\left|\tilde{\lambda}_j\right\rangle \otimes |u_j\rangle_{n_b} \otimes |0\rangle\big] \\
&= \sum_{j=0}^{2^{n_b}-1} \beta_j \left|\tilde{\lambda}_j\right\rangle \otimes |u_j\rangle_{n_b} \otimes \left[\sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}}\,|0\rangle + \frac{C}{\tilde{\lambda}_j}\,|1\rangle\right].
\end{aligned}$$

π_4 : Se mide el último registro, si la lectura es $|0\rangle$ se repite el proceso. Si se mide $|1\rangle$ se tiene el siguiente estado:

$$|\pi_4\rangle = \left[\sum_{j=0}^{2^{n_b}-1} \frac{1}{\sqrt{\sum_{k=0}^{2^{n_b}-1} |\beta_k|^2 |C|^2/|\lambda_k|^2}} \beta_j \frac{C}{\tilde{\lambda}_j} \left|\tilde{\lambda}_j\right\rangle \otimes |u_j\rangle_{n_b}\right] \otimes |1\rangle\,.$$

$$\begin{aligned}
\pi_5 : \ |\pi_5\rangle &= \mathrm{QPE}^{-1}(e^{iAt})\left[\frac{1}{\sqrt{\sum_{k=0}^{2^{n_b}-1}|\beta_k|^2|C|^2/|\lambda_k|^2}}\sum_{j=0}^{2^{n_b}-1}\beta_j\frac{C}{\tilde{\lambda}_j}\left|\tilde{\lambda}_j\right\rangle\otimes|u_j\rangle_{n_b}\right]\otimes|1\rangle \\
&= \left[\frac{1}{\sqrt{\sum_{k=0}^{2^{n_b}-1}|\beta_k|^2|C|^2/|\lambda_k|^2}}\sum_{j=0}^{2^{n_b}-1}\beta_j\frac{C}{\tilde{\lambda}_j}\left|0^{\otimes n_l}\right\rangle\otimes|u_j\rangle_{n_b}\right]\otimes|1\rangle \\
&= \left|0^{\otimes n_l}\right\rangle\otimes\left[\frac{1}{\sqrt{\sum_{k=0}^{2^{n_b}-1}|\beta_k|^2|C|^2/|\lambda_k|^2}}\sum_{j=0}^{2^{n_b}-1}\beta_j\frac{C}{\tilde{\lambda}_j}|u_j\rangle_{n_b}\right]\otimes|1\rangle \\
&= \left|0^{\otimes n_l}\right\rangle\otimes|\tilde{x}\rangle\otimes|1\rangle\,.
\end{aligned}$$

Este estado $|\tilde{x}\rangle$ será el candidato a solución del sistema $A|\tilde{x}\rangle = |b\rangle$.

El problema del HHL es que las puertas empleadas en este circuito no existen de forma directa, de hecho, el método que se use para implementarlas puede afectar considerablemente a las capacidades computacionales del algoritmo. En [Vazquez et al., 2022] se proponen unos métodos concretos para realizar cada paso, que mantienen la mejora exponencial del algoritmo

A continuación, veremos los tres problemas que se abordan y explicaremos brevemente las soluciones propuestas en [Vazquez et al., 2022]:

1. La inicialicación del estado $|b\rangle$ en el registro n_b-cúbit requiere de un subproceso que sólo conserva el orden sub-exponencial en algunos casos concretos. Uno de estos es considerar que el vector $\mathbf{b}$, $\{b_i\}_{i=0}^{2^{n_b}-1}$, se puede describir con una función analítica $f : [0,1] \to \mathbb{R}$ de forma que:

$$b_i = f(x_i),\ x_i = \frac{i}{2^{n_b}-1}.$$

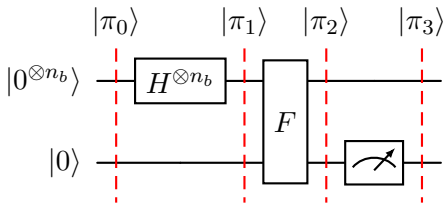

Figura 2.7: Inicialización de $|b\rangle$.

La inicialización del estado $|b\rangle$ se realiza mediante un subcircuito como el de la Figura 2.7, donde F es un operador unitario que debe realizar la siguiente transformación sobre un (n_b+1)-cúbit:

$$F(|i\rangle_{n_b}\otimes|0\rangle) := \sqrt{1-\frac{f^2(x_i)}{\|\mathbf{b}\|_\infty^2}}\,|i\rangle_{n_b}\otimes|0\rangle + \frac{f(x_i)}{\|\mathbf{b}\|_\infty}|i\rangle_{n_b}\otimes|1\rangle\,, \tag{2.18}$$

siendo $\|\mathbf{b}\|_\infty = \max\{|b_i|\}_i$. Si consideramos un polinomio de orden k que aproxime los coeficientes de 2.18, se puede comprobar que sólo hacen falta puertas de Hadamard y R_y controladas para aproximar F [Woerner and Egger, 2019].

2. La implementación del operador unitario $U = e^{iAt}$, con $A \in \mathcal{M}_{2^{n_b}\times 2^{n_b}}(\mathbb{R})$, en la QPE y su inversa, para el caso concreto de matrices simétricas de Topelitz, se realiza mediante un tipo de simulación de Hamiltonianos llamada *trotterización*, basada en la descomposición de Lie-Trotter.

   Definición 2.7. Sea $H \in \mathcal{M}_{N\times N}(\mathbb{C})$ una matriz hermítica que de la forma $H = \sum_{m=1}^{M} H_m$ y $t \in \mathbb{R}^+$, se define la fórmula de Lie-Trotter de segundo orden como:

$$S_1(t) = \prod_{j=1}^{J} e^{iH_j t/2} \prod_{j=J}^{1} e^{iH_j t/2}. \tag{2.19}$$

   De esta forma, si queremos calcular el operador unitario e^{iHt}, pueden darse dos situaciones:

   - Los operadores H_j conmutan, con lo cual:

$$e^{iHt} = e^{i\sum_{j=0}^{J} H_j t} = \prod_{j=0}^{J} e^{iH_j t}.$$

   - Los operadores H_j no conmutan, entonces se tendrá que usar la aproximación de Lie-Trotter.

   Consideremos la siguiente descomposición de $A = H_1 + H_2 + H_3$:

$$H_1 = aI_{n_b}, \tag{2.20}$$

$$H_2 = bI_{n_b-1} \otimes \sigma_x = \begin{pmatrix} 0 & b & \cdots & 0 & 0 \\ b & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b \\ 0 & 0 & \cdots & b & 0 \end{pmatrix}, \tag{2.21}$$

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & b & \cdots & 0 & 0 & 0 \\ 0 & b & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b & 0 \\ 0 & 0 & 0 & \cdots & b & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}, \tag{2.22}$$

se tiene que H_1 conmuta con H_2 y H_3, pero estos dos últimos no conmutan entre sí. Para realizar la simulación del Hamiltoniano A descompondremos el unitario en dos partes, $U = e^{iAt} = e^{i(H_1+H_2+H_3)t} = e^{iH_1t}e^{i(H_2+H_3)t}$. Para el término $e^{i(H_2+H_3)t}$ emplearemos la fórmula de Lie-Trotter 2.19, aplicando un número m de pasos de Trotter:

$$\begin{aligned} S_1^m(t/m) &= \left(e^{iH_2t/2m}e^{iH_3t/2m}e^{iH_3t/2m}e^{iH_2t/2m}\right)^m \\ &= \left(e^{iH_2t/2m}e^{iH_3t/m}e^{iH_2t/2m}\right)^m \\ &= e^{-iH_2t/2m}\left(e^{iH_2t/2m}e^{iH_3t/m}\right)^m e^{iH_2t/2m}. \end{aligned}$$

Definimos así el unitario aproximado tras m pasos de Trotter para un instante t:

$$\begin{aligned} V(t,m) :=& e^{iH_1t}S_1^m(t/m) \\ =& e^{iH_1t}e^{-iH_2t/2m}\left(e^{iH_2t/2m}e^{iH_3t/m}\right)^m e^{iH_2t/2m}, \end{aligned} \tag{2.23}$$

que, por el Teorema 4.3 en [Nielsen and Chuang, 2010], verifica:

$$\lim_{m\to\infty} V(t,m) = e^{iAt} = U. \tag{2.24}$$

Finalmente, como la expresión en puertas cuánticas de los operadores e^{iH_1t}, $e^{iH_2t/2m}$ y $e^{iH_3t/m}$ es más sencilla [Vazquez et al., 2022], se introducen en el circuito con el orden especificado en 2.23, para el número de pasos de Trotter que se quiera usar.

3. La rotación controlada, o inversión de autovalores, consiste en encontrar un unitario que realice la siguiente transformación:

$$\sum_{j=0}^{2^{n_b}-1} \beta \left|\tilde{\lambda}_j\right\rangle_{n_l} \otimes |u_j\rangle_{n_b} \otimes |0\rangle \to \sum_{j=0}^{2^{n_b}-1} \beta \left|\tilde{\lambda}_j\right\rangle_{n_l} \otimes |u_j\rangle_{n_b} \otimes \left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}\,|0\rangle + \frac{C}{\tilde{\lambda}_j}\,|1\rangle\right).$$

En [Vazquez et al., 2022] se propone un método basado en la interpolación de Chebyshev a la función $\arcsin(C/x)$. Su implementación cuántica se realiza mediante una versión cuántica del esquema de Horner, con puertas CCNOT [Häner et al., 2018, Knuth, 1962].

Bibliografía

[Alsing et al., 2024] Alsing, P. M., Cafaro, C., and Mancini, S. (2024). Feynman's "simulating physics with computers".

[Bassoli et al., 2021] Bassoli, R., Boche, H., Deppe, C., Ferrara, R., Fitzek, F., Janssen, G., and Saeedinaeeni, S. (2021). *Quantum Communication Networks*, pages 1–226. Foundations in Signal Processing, Communications and Networking. Springer Science and Business Media B.V.

[Bellac, 2006] Bellac, M. L. (2006). *Quantum Physics*. Cambridge University Press.

[Bennett et al., 1993] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899.

[Caleffi and Cacciapuoti, 2020] Caleffi, M. and Cacciapuoti, A. S. (2020). Quantum switch for the quantum internet: Noiseless communications through noisy channels. *IEEE Journal on Selected Areas in Communications*, 38(3):575–588.

[Christian Grossmann, 2007] Christian Grossmann, Hans-Gorg Roos, M. S. (2007). *Numerical Treatment of Partial Differential Equations*. Springer Berlin, Heidelberg.

[Deutsch and Jozsa, 1992] Deutsch, D. and Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558.

[Deutsch and Penrose, 1985] Deutsch, D. and Penrose, R. (1985). Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117.

[Golub and Van Loan, 2013] Golub, G. H. and Van Loan, C. F. (2013). *Matrix Computations - 4th Edition*. Johns Hopkins University Press, Philadelphia, PA.

[Hestenes and Stiefel, 1952] Hestenes, M. R. and Stiefel, E. (1952). *Methods of Conjugate Gradients for Solving Linear Systems*, volume 46, 409-435. Journal of research of the National Bureau of Standars.

[Häner et al., 2018] Häner, T., Roetteler, M., and Svore, K. M. (2018). Optimizing quantum circuits for arithmetic.

[Knuth, 1962] Knuth, D. E. (1962). Evaluation of polynomials by computer. *Commun. ACM*, 5(12):595–599.

[Nielsen and Chuang, 2010] Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.

[Preskill, 2018] Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79.

[Scherer, 2019] Scherer, W. (2019). *Mathematics of Quantum Computing: An Introduction*. Springer International Publishing.

[Shor, 1994] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.

[Shor, 1997] Shor, P. W. (1997). Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509.

[Tojo et al., 2023] Tojo, F. A. F., Fernández, F. J. F., and Brage, F. J. P. (2023). Las matemáticas en la era de la computación cuántica: nuevas fronteras. Technical report, Centro de Supercomputación de Galicia (CESGA).

[Vazquez et al., 2022] Vazquez, A. C., Hiptmair, R., and Woerner, S. (2022). Enhancing the quantum linear systems algorithm using richardson extrapolation. *ACM Transactions on Quantum Computing*, 3(1):1–37.

[Woerner and Egger, 2019] Woerner, S. and Egger, D. J. (2019). Quantum risk analysis. *npj Quantum Information*, 5(1).