



UNIVERSIDAD DE PAMPLONA

*Transformación de Fourier  
Fraccionaria Cuántica*

YESID ALEXANDER MADRID CARRILLO

FACULTAD DE CIENCIAS BÁSICAS  
DEPARTAMENTO DE FÍSICA Y GEOLOGÍA  
GRUPO DE ÓPTICA MODERNA  
PAMPLONA

2018



UNIVERSIDAD DE PAMPLONA

# *Transformación de Fourier Fraccionaria Cuántica*

YESID ALEXANDER MADRID CARRILLO

Trabajo presentado para optar al  
Título de Físico

Directores:

Sc.Dr. MARTHA MOLINA  
Universidad de Pamplona

Sc.Dr. RAFAEL TORRES  
Universidad Industrial de  
Santander

FACULTAD DE CIENCIAS BÁSICAS  
DEPARTAMENTO DE FÍSICA Y GEOLOGÍA  
GRUPO DE ÓPTICA MODERNA  
PAMPLONA

2018

*A mi familia, Mamá y Papá,  
Ustedes que son el impulso de mi camino día a día.*

# Agradecimientos

Mis agradecimientos empiezan hacia mis tutores, Rafael Torres y Martha Molina, ya que significaron un apoyo incondicional en este proceso, además de sus aportes en mi investigación, y por todas sus sugerencias y por el valioso apoyo en los resultados de mi trabajo.

Quiero dar un agradecimiento muy especial a mi tutor Rafael Torres por recibirme al interior del Grupo de Óptica y Tratamiento de Señales (GOTS) de la UIS, en donde realicé una estancia de investigación que fué de vital importancia para el desarrollo de este trabajo.

A Nestor Arias, por ser un apoyo con su participación en esta investigación, y por sus aportes al trabajo.

Agradezco a aquellos profesores que hicieron parte fundamental en mi formación académica, brindándome mas que educación y siendo formadores de mi pensamiento y contribuyentes en lo que hoy me hace un profesional.

Quiero agradecer a Nelsón Fernandez y Nidia Florez, los cuales contribuyeron a mi formación como amigos en mi proceso académico durante casi todos mis años de estudio. Y de igual manera a mis amigos y colegas Alejandra y Johan que contribuyeron en los momentos difíciles de mi formación, así como también a mis compañeros en el laboratorio de metrología óptica Darby, Juan, Sabas y Hosman.

Y por último pero no menos importante, quiero dar un agradecimiento especial a mi familia, destacando a mis padres, que han sido un apoyo y motivo de aliento en todo mi proceso de formación.

# Índice general

<b>1. Introducción</b>	<b>10</b>
<b>2. Marco de Referencia</b>	<b>13</b>
2.1. Marco Histórico . . . . .	13
2.1.1. Transformación de Fourier fraccionaria . . . . .	13
2.1.2. Computación Cuántica . . . . .	14
2.2. Marco Teórico . . . . .	15
2.2.1. Transformación de Fourier Fraccionaria . . . . .	15
2.2.2. Computación Cuántica . . . . .	17
2.2.2.1. Qubit . . . . .	17
2.2.2.2. Medida Cuántica . . . . .	19
2.2.2.3. Evolución Cuántica . . . . .	20
2.2.2.4. Paralelismo Cuántico . . . . .	20
2.2.2.5. Entrelazamiento . . . . .	22
2.2.2.6. Esfera de Bloch . . . . .	23
2.2.2.7. Compuertas y circuitos lógicos . . . . .	24
2.2.2.8. Compuertas Cuánticas . . . . .	24
2.2.3. IBM Quantum Experience . . . . .	29
2.2.3.1. Computadora QX 2 . . . . .	30
<b>3. Desarrollos Teóricos</b>	<b>33</b>
3.1. Transformación de Fourier Fraccionaria Discreta (TFfD) . . . . .	33
3.2. Transformación de Fourier Fraccionaria Cuántica (TFfC) . . . . .	35
<b>4. Compuerta Cuántica <math>\mathcal{F}_\alpha</math></b>	<b>38</b>
4.1. Definición de $\mathcal{F}_\alpha$ . . . . .	38
4.2. Aplicación de la Compuerta $\mathcal{F}_\alpha$ . . . . .	39
4.2.1. Grado de Libertad del Orden Fraccionario . . . . .	39
4.2.2. Reducción de Complejidad Computacional . . . . .	42
4.2.3. Entrelazamiento de Qubits . . . . .	45
<b>5. Aplicaciones de <math>\mathcal{F}_\alpha</math> en algunos Algoritmos Cuánticos</b>	<b>47</b>
5.1. Algoritmo de Grover . . . . .	47
5.1.0.1. Ejemplos de Circuitos Cuánticos Propuestos por IBM . . . . .	50

5.1.0.2.	Circuitos Cuánticos Propuestos por IBM usando la compuerta cuántica $\mathcal{F}_\alpha$ . . . . .	52
5.2.	Algoritmo de Shor . . . . .	53
5.2.0.1.	Ejemplos de Circuitos Cuánticos Propuestos por IBM . . . . .	56
5.2.0.2.	Circuitos Cuánticos Propuestos por IBM usando la compuerta cuántica $\mathcal{F}_\alpha$ . . . . .	57
<b>6.</b>	<b>Conclusiones</b>	<b>59</b>
<b>A.</b>	<b>Analogía Transformación de Fourier Estándar</b>	<b>61</b>
A.1.	Transformación de Fourier Estándar Discreta . . . . .	61
A.2.	Transformación de Fourier Cuántica . . . . .	62
<b>B.</b>	<b>Algoritmo de Grover</b>	<b>64</b>
B.1.	Ejemplos propuestos por IBM Experience . . . . .	64
B.1.1.	Primer Ejemplo con objetivo en el estado final $ 00\rangle$ . . . . .	64
B.1.2.	Segundo Ejemplo con objetivo en el estado final $ 01\rangle$ . . . . .	67
B.1.3.	Tercer Ejemplo con objetivo en el estado final $ 10\rangle$ . . . . .	69
B.1.4.	Cuarto Ejemplo con objetivo en el estado final $ 11\rangle$ . . . . .	71
B.2.	Aplicación de la compuerta $\mathcal{F}_\alpha$ . . . . .	73
B.2.1.	Primer Ejemplo con objetivo en el estado final $ 00\rangle$ . . . . .	73
B.2.2.	Segundo Ejemplo con objetivo en el estado final $ 01\rangle$ . . . . .	75
B.2.3.	Tercer Ejemplo con objetivo en el estado final $ 10\rangle$ . . . . .	77
B.2.4.	Cuarto Ejemplo con objetivo en el estado final $ 11\rangle$ . . . . .	79
<b>C.</b>	<b>Algoritmo de Shor</b>	<b>81</b>
C.1.	Ejemplo propuesto por IBM Experience . . . . .	81
C.2.	Aplicación de la compuerta $\mathcal{F}_\alpha$ . . . . .	82
<b>D.</b>	<b>Anexos</b>	<b>84</b>
D.1.	Productos Derivados de la Tesis . . . . .	84
D.1.1.	Ponencia The FIO+LS . . . . .	84
D.1.2.	Ponencia Quantum Optics IX . . . . .	85
D.1.3.	Proceedings Publicado en OSA Publishing . . . . .	85
D.1.4.	Artículo Sometido en Physical Review Letter . . . . .	86
D.1.5.	Premio al Autor . . . . .	86
	<b>Bibliografía</b>	<b>86</b>

# Índice de figuras

2.1. Estado Base $ 0\rangle$ . . . . .	23
2.2. Compuertas de Pauli . . . . .	25
2.3. Compuerta <b>X</b> . . . . .	26
2.4. Compuerta <b>Y</b> . . . . .	26
2.5. Compuerta <b>Z</b> . . . . .	27
2.6. Compuerta de Fase . . . . .	27
2.7. Compuerta Hadamard . . . . .	28
2.8. Compuerta Hadamard actuando sobre el estado $ 0\rangle$ . . . . .	28
2.9. Compuerta Hadamard actuando sobre el estado $ 1\rangle$ . . . . .	29
2.10. Compuerta <b>CNOT</b> . . . . .	29
2.11. Hardware de la computadora cuántica QIBM (tomado de [44]) . . . . .	30
2.12. a. Arquitectura de conexiones y b. procesador cuántico de 5-qubits superconductores, disponible en la computadora cuántica de IBM . . . . .	31
2.13. Interfaz gráfica del IBM Q denominada Quantum composer, sobre la cual es posible crear circuitos cuánticos utilizando una librería de compuertas lógicas y puntos de medición preestablecidos. (tomado de [44]) . . . . .	31
3.1. Espectro reconstruido completamente usando la rata de muestreo apropiada . . . . .	35
4.1. Superposición para la compuerta cuántica fraccionaria de orden $\alpha$ desde el estado $ 0\rangle$ . . . . .	40
4.2. Superposition for fractional Fourier quantum gate of order $\alpha$ from state $ 1\rangle$ . . . . .	41
4.3. Superposición para el estado obtenido al aplicar la compuerta $F_\alpha$ desde un estado en superposición. . . . .	42
4.4. Circuito Cuántico para mover el qubit al estado $ \odot\rangle$ . . . . .	43
4.5. Circuito Cuántico para mover el qubit al estado $ \odot\rangle$ usando la compuerta cuántica $F_\alpha$ . . . . .	44
4.6. Circuito Cuántico del estado entrelazado . . . . .	45
5.1. Algoritmo de Grover propuesto por IBM ( <a href="https://goo.gl/ppzrjR">https://goo.gl/ppzrjR</a> ) . . . . .	51
5.2. Algoritmos de factorización clásicos vs cuánticos ( <a href="https://goo.gl/ppzrjR">https://goo.gl/ppzrjR</a> ) . . . . .	54
5.3. Resultado del Circuito mostrado por Qubit. . . . .	57
5.4. Resultado del Circuito mostrado por Qubit. . . . .	58

---

D.1. Certificado de Asistencia . . . . .	84
D.2. Certificado de Asistencia . . . . .	85
D.3. Publicación . . . . .	85
D.4. Publicación . . . . .	86
D.5. Publicación . . . . .	86

# Índice de tablas

2.1. Operaciones lógicas not, and y or. . . . .	24
2.2. Operaciones lógicas nand, nor y xor. . . . .	24
4.1. Orden fraccionario aplicado al estado base $ 0\rangle$ . . . . .	40
4.2. Orden fraccionario aplicado sobre el estado base $ 1\rangle$ . . . . .	41
4.3. Resultados por cada orden fraccionario aplicado sobre el estado $(\frac{1+i}{2}  0\rangle + \frac{1-i}{2}  1\rangle)$ . . . . .	42

# Fractional Fourier Quantum Transform

Yesid Madrid

## Abstract

The Fourier transformation has been successful in different areas of science and engineering due to its multiple applications and now in quantum computing because of its utility to achieve superposition of quantum states. Our proposal consists of developing a new quantum gate associated with the fractional Fourier transformation, which allows a degree of freedom that has as a special case the standard Fourier transformation. We have tested this gate through the quantum computer simulator of IBM experience. Thus, it has been shown that the fractional order offers an additional degree of freedom in the superposition of qubit states, what allowed the reduction of the quantum volume in replacing the use of some other quantum gates according to the fractional order.

# Transformación de Fourier Fraccionaria Cuántica

Yesid Madrid

## Resumen

La transformación de Fourier ha tenido importancia en diferentes áreas de la ciencia e ingeniería debido a sus múltiples aplicaciones y recientemente en la computación cuántica debido a su utilidad para alcanzar superposición de estados cuánticos. Nuestra propuesta consiste en desarrollar una nueva compuerta cuántica asociada con la transformación de Fourier fraccionaria. Hemos probado esta compuerta a través del simulador de computador cuántico de IBM Experience. Por lo tanto, ha sido demostrado que el orden fraccionario ofrece un grado de libertad adicional en la superposición de los estados del qubit, que permite a su vez la reducción del volumen cuántico reemplazando el uso de algunas compuertas cuánticas acorde al orden fraccionario aplicado.

# Capítulo 1

## Introducción

Uno de los problemas del que se ocuparon los matemáticos del siglo XVIII es el que se conoce con el nombre del "problema de la cuerda vibrante". Este problema fue estudiado por d'Álembert y Euler (usando el método de propagación de las ondas) y un poco más tarde, concretamente en 1753, por Daniel Bernouilli. La solución dada por éste difería de la proporcionada por los anteriores y consistió básicamente en expresar la solución del problema como superposición (en general infinita) de ondas sencillas. Las ideas de Bernouilli fueron aplicadas y perfeccionadas por Fourier, en 1807, en el estudio de problemas relacionados con la conducción del calor. Estas ideas quedaron plasmadas por escrito en el libro clásico "Théorie analytique de la Chaleur" [1], publicado en 1822. Los razonamientos realizados por Fourier en este libro plantearon de manera inmediata numerosas controversias y cuestionamientos que han tenido una influencia significativa en la historia de la Matemática.

Una motivación para el estudio de la transformación de Fourier proviene de la serie de Fourier. En el estudio de las series de Fourier, las funciones complicadas pero periódicas se escriben como la suma de ondas simples representadas matemáticamente por senos y cosenos. La transformación de Fourier es una extensión de la serie de Fourier que se produce cuando el período de la función representada se alarga y se le permite acercarse al infinito. Este operador ha tenido gran relevancia en los diferentes estudios de la ciencia moderna en cuanto a la óptica y tratamiento de señales, y es hoy una de los operadores matemáticos más importantes.

La transformación de Fourier también ha sido llevada a otros campos mediante las diferentes aplicaciones que han surgido al transcurrir la historia, por ello se ve la aplicación de esta transformación en la cuántica, y más específicamente en la computación cuántica como medio de optimización en diferentes algoritmos

cuánticos[2]. Con sus diversas aplicaciones ha sido considerada una de las transformaciones matemáticas más importantes en la computación cuántica, pues ha llevado a centrar la atención de los científicos en la paralelización de los algoritmos en las computadoras cuánticas, el cual es un mecanismo que provee la oportunidad de mejorar la complejidad algorítmica [3]. Muchos algoritmos toman ventaja con la aplicación de este operador, como por ejemplo, el algoritmo de Grover, que es considerado el algoritmo de búsqueda más rápido [3–6].

Por otra parte, la transformación de Fourier estándar no ha podido demostrar aplicaciones, como lo es el caso de la difracción de Fresnel. Por esto, es necesario tener en cuenta la transformación de Fourier fraccionaria, el cual es un operador que permite describir el comportamiento del campo electromagnético a través del espacio libre, y con ello abordar la difracción de Fresnel. La transformación de Fourier Fraccionaria, fue definida por Victor Namias como una herramienta para solucionar ecuaciones diferenciales aplicadas al oscilador armónico mecánico cuántica [7], la cual en investigaciones recientes también ha demostrado ser aplicable en los teoremas de correlación y convolución [8]. En otras investigaciones, la transformación de Fourier fraccionaria es presentada como un interactivo algoritmo para calcular hologramas que permite generar patrones de difracción que no están en el plano de Fourier [9], demostrando su importancia en la holografía.

En el enfoque de señales también existe aplicación por parte de la transformación de Fourier fraccionaria, dado que existe una fórmula de interpolación que sirve para estimar una señal aleatoria a partir de una serie temporal, basándose en el teorema de muestreo fraccionario para señales aleatorias [10]. En estudios más recientes, existen aplicaciones dedicadas a temas más específicos, como lo es el método para calcular un difusor de banda limitada con un espectro uniforme en el dominio de Fresnel [11], o la formulación matemática para la propagación de fotones utilizando el formalismo de la cuantización del campo electromagnético, cuya característica principal es su similitud con una transformación de Fourier fraccionaria [12].

El interés de este trabajo está en encontrar una compuerta de la transformación de Fourier cuántica, y usar el grado de libertad adicional que provee con respecto a la transformación de Fourier estándar. En el capítulo 2 se crea un marco de referencia para establecer un pequeño resumen del estado del arte de las principales disciplinas abordadas en este trabajo, así como un marco teórico para entrar en materia con los conceptos fundamentales a tener en cuenta. En el capítulo 3

se establecen los desarrollos teóricos de este trabajo, los cuales serán base para resultados descritos en los siguientes capítulos.

En el capítulo 4 se aborda la definición de la nueva compuerta cuántica a partir de la transformación de Fourier fraccionaria cuántica obtenida previamente, luego se establecen algunos casos de aplicación de la compuerta en problemas fundamentales de la computación cuántica como la obtención de nuevos estados de superposición para los qubits, con un grado de fase libre dada por el orden fraccionario. Adicionalmente, su aplicación es orientada a la complejidad algorítmica, ya que con ésta es posible reducir el número de compuertas usadas en un circuito cuántico, y así permite reducir la complejidad del algoritmo y hacerlo más eficiente. Además, son encontradas nuevas formas de obtener estados entrelazados a partir de esta compuerta cuántica usando valores de orden fraccionarios definidos.

En el capítulo 5 son abordados algunos algoritmos cuánticos definidos y aceptados por la comunidad científica a través de la nueva compuerta cuántica, obteniendo tanto reducción del número de compuertas cuánticas aplicadas, así como la ampliación del alcance de aplicación debido al grado de libertad adicional. Para concluir en el capítulo 6 se presentan los resultados obtenidos a lo largo de este trabajo.

# Capítulo 2

## Marco de Referencia

### 2.1. Marco Histórico

#### 2.1.1. Transformación de Fourier fraccionaria

En la última década, la transformación de Fourier fraccionaria implementada por Victor Namias [7], y posteriormente justificada por McBride [13], ha tenido diversas aplicaciones en la óptica [14–17] y el procesamiento de señales [15]. Ha sido demostrado de igual manera que con un orden fraccionario  $\alpha = \frac{\pi}{2}$  la transformación de Fourier fraccionaria es equivalente a la transformación de Fourier estándar [7]. Esto se debe a que la transformación de Fourier fraccionaria de una función  $f$ , puede verse como la transformación de Fourier de la función que se obtiene al multiplicar  $f$  con una función de fase cuadrática.

Posteriormente, se demostró que la transformación de Fourier fraccionaria es equivalente a una transformación de Fresnel, cuyas expresiones matemáticas corresponden al fenómeno de difracción de Fresnel [17, 18]. Por otra parte, Ozaktas y Mendlovic desarrollan por primera vez demostraron su aplicación en la óptica experimental a través de un experimento en un medio Grin [16, 33]; posteriormente, Lohman muestra dos arquitectura ópticas en las cuales, por medio de un arreglo de lentes, se obtiene una transformación de Fourier fraccionaria en el espacio libre [15].

Sin embargo, hasta ese momento solo se habían encontrado sistemas ópticos en los cuales se demostraba que la función de distribución de campo en la salida correspondía a la aplicación de una transformación de Fourier fraccionaria aplicada a la

función de distribución del campo de entrada. Luego, el paso que se convertiría en el más importante de la óptica fraccionaria fue aquel dado por Pellat-Finet [17] donde muestran que la difracción de Fresnel se puede expresar como una transformación de Fourier fraccionaria, con lo cual se hace evidente que sistemas ópticos llevan a cabo una transformación de Fourier fraccionaria (Tff). Recientemente este operador ha tenido aplicación en la formulación matemática cuántica para la propagación de fotones [12].

### 2.1.2. Computación Cuántica

En las últimas décadas, la ciencia de la información cuántica ha surgido para considerar qué potencia y funcionalidad adicional se puede obtener en la codificación, transmisión y procesamiento de la información mediante el aprovechamiento de los efectos mecánicos cuánticos [2]. Las tecnologías anticipadas incluyen: criptografía cuántica [19], que ofrece una comunicación perfectamente segura; metrología cuántica [20], que permite mediciones más precisas de lo que podría lograrse con la mecánica clásica; y la litografía cuántica [21], que podría permitir la fabricación de dispositivos con características mucho más pequeñas que la longitud de onda de la luz. Quizás la tecnología cuántica futura más sorprendente y poderosa sea una computadora cuántica, que promete computación exponencialmente más rápida para tareas particulares [2, 22].

Los requisitos para realizar una computadora cuántica son confusos: qubits físicamente escalables (dos sistemas cuánticos de estado) que pueden estar bien aislados del entorno, pero también pueden iniciarse, medirse e interactuar de manera controlable para implementar un conjunto universal de compuertas lógicas cuánticas [23].

Las máquinas de Turing cuánticas y los circuitos cuánticos son un modelo de la computación, tal como lo son las máquinas de Turing clásicas, las funciones recursivas y el  $\lambda$ -cálculo, entre otros. Estos modelos se inscriben dentro de un área conocida como computación cuántica y, como su nombre lo indica, hacen uso de las propiedades y efectos considerados por la mecánica cuántica. Esta área fue inicialmente sugerida por Richard Feynman en los años 80, formalizada por David Deutsch (en la forma de máquinas de Turing cuánticas en 1985 [22] y en la forma de circuitos cuánticos en 1989 [24]) y resaltada su potencialidad por Peter Shor en 1994 [6].

El trabajo de Shor señaló el aspecto fundamental en el cual se diferencian la computación clásica y la computación cuántica: *la complejidad algorítmica*. Esta diferencia consiste en que es posible definir algoritmos cuánticos cuya complejidad temporal sea menor que sus análogos clásicos (conocidos hasta el momento). En particular Shor realizó la descripción de un algoritmo cuántico de complejidad temporal de tipo polinomial para la factorización de números enteros; algunos autores afirman que una máquina de Turing y una máquina de Turing cuántica son equipotentes en relación a las funciones que ellas pueden computar [22], otros autores por su parte, suponen que bajo ciertas circunstancias la computación cuántica pueda ofrecer características de “super-Turing” computación [25], pero hasta el momento todo esto es una discusión abierta.

## 2.2. Marco Teórico

### 2.2.1. Transformación de Fourier Fraccionaria

En matemáticas, en el área del análisis de armónicos, la transformación de Fourier fraccionaria o (TFf) es una familia de transformaciones lineales que generalizan la transformación de Fourier, por lo tanto, puede transformar una función en cualquier dominio intermedio entre el tiempo y la frecuencia. Sus aplicaciones abarcan desde el diseño de filtros y el análisis de señales hasta la recuperación de fases y el reconocimiento de patrones[28].

La TFf se puede utilizar para definir la convolución fraccionaria, la correlación y otras operaciones, y también se puede generalizar más en la transformación canónica lineal (LCT). Una definición temprana de TFf fue introducida por Condon[26], resolviendo la función de Green para rotaciones de espacio de fase, y también por Namias[7], generalizando el trabajo de Wiener [27] en los polinomios de Hermite.

Un significado completamente diferente para “transformación de Fourier fraccionaria” fue introducido por Bailey y Swartztrauber [28], para el caso que corresponde a una transformación discreta de Fourier desplazada por una cantidad fraccionaria en el espacio de frecuencia y evaluando en un conjunto fraccionario de puntos de frecuencia (por ejemplo, considerando solo una pequeña porción del espectro).

La transformación de Fourier fraccionaria (TFf) definida por Victor Namias como una herramienta para solucionar ecuaciones diferenciales aplicadas al oscilador

armónico mecánico cuántica [7], obteniendo un operador que es una generalización del operador transformación de Fourier estándar:

$$F^\alpha[f](x') = \frac{e^{\frac{i\pi}{4}} e^{-\frac{i\alpha}{2}}}{\sqrt{|\sin(\alpha)|}} e^{i\pi x'^2 \cot \alpha} \int_{\mathbf{R}} e^{i\pi x^2 \cot \alpha} e^{-\frac{2i\pi x x'}{\sin(\alpha)}} f(x) dx. \quad (2.1)$$

Este operador, para el valor de  $\alpha = \frac{\pi}{2}$ , se reduce al caso estándar de la transformación de Fourier.

### Propiedades

Los principales teoremas conocidos para la transformación de Fourier estándar, fueron generalizados para la Tff. Además, al igual que el caso estándar, este operador Tff, es también unitario.

- Linealidad:

$$\mathcal{F}^\alpha[af(x) + bg(x)](x') = a\mathcal{F}^\alpha[f(x)](x') + b\mathcal{F}^\alpha[g(x)](x')$$

- Inversa:

$$(\mathcal{F}^\alpha)^{-1}[f(x)](x') = \mathcal{F}^{-\alpha}[f(x')](x') \quad (2.2)$$

- Identidad:

$$\mathcal{F}^\alpha(\mathcal{F}^\alpha)^{-1} = \mathbf{I} \quad (2.3)$$

- Conmutatividad:

$$\mathcal{F}^{\alpha_1} \mathcal{F}^{\alpha_2} = \mathcal{F}^{\alpha_2} \mathcal{F}^{\alpha_1} \quad (2.4)$$

- Teorema de Parseval:

$$\int_{\mathbf{R}} f(x)g^*(x)dx = \int_{\mathbf{R}} f_\alpha(x')g_\alpha^*(x')dx' \quad (2.5)$$

- Teorema del Corrimiento:

$$\mathcal{F}^\alpha[f(x - \zeta)](x') = f_\alpha(x' - \zeta \cos(\alpha))e^{i\pi \sin(\alpha)(\zeta^2 \cos(\alpha) - 2x'\zeta)} \quad (2.6)$$

- Teorema de la Modulación:

$$\mathcal{F}^\alpha[f(x)e^{i2\pi vx}](x') = f_\alpha(x' - v \sin(\alpha))e^{-i\pi \cos(\alpha)(v^2 \sin(\alpha) - 2x'v)} \quad (2.7)$$

- Teorema del Escalamiento:

$$\mathcal{F}^\alpha[f(cx)](x') = \sqrt{\frac{\cos(\beta)}{\cos(\alpha)}} e^{\frac{1}{2}i(\alpha-\beta)} e^{i\pi x'^2 \cot(\alpha)(1-\frac{\cos^2(\beta)}{\cos^2(\alpha)})} f_\beta(x' \frac{\sin(\beta)}{c \sin(\alpha)}), \quad (2.8)$$

Donde  $\beta = c^2 \tan(\alpha)$ .

## 2.2.2. Computación Cuántica

### 2.2.2.1. Qubit

Desde la analogía de los sistemas clásicos donde conocemos que el bit es la mínima unidad de información en el cómputo, es necesario conocer la contraparte de este elemento dentro de la teoría del cómputo cuántico, denominado bit cuántico o dentro de un contexto más general “Qubit” [2]. Este objeto aunque es descrito matemáticamente con propiedades específicas, no es despreciable su realidad física y lo que implica dentro de un sistema cuántico, en el cuál su tratamiento se torna abstracto. Por lo tanto, para su correcta descripción es necesario implementar el formalismo matemático de la mecánica cuántica donde un qubit es ahora, un vector unitario en un espacio de estado bidimensional, para el cual se ha fijado una base ortonormal particular denotada por  $|0\rangle$ ,  $|1\rangle$ , que corresponden en analogía al 0 y 1 de un bit clásico.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix};$$

Los dos vectores de base  $|0\rangle$  y  $|1\rangle$  corresponden a los valores posibles que puede tomar un bit cuántico. Sin embargo, a diferencia de los bits clásicos, la potencialidad de este nuevo esquema radica en que un qubit también puede tomar muchos otros valores de los mencionados anteriormente, debido a la combinación lineal de estados [34]. En general, un qubit  $|\psi\rangle$  arbitrario se puede escribir como:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle, \quad (2.9)$$

donde  $a_0$  y  $a_1$  son números complejos que satisfacen la relación de normalización  $|a_0|^2 + |a_1|^2 = 1$ . Esta es la diferencia fundamental que distingue los bits cuánticos de los clásicos y es una aplicación directa del principio cuántico de superposición de estados. El qubit  $|\psi\rangle$  en la ecuación (2.9) está en una superposición de  $|0\rangle$  y

$|1\rangle$ , un estado en el cual no es posible decir que el qubit está definitivamente en el estado  $|0\rangle$ , o definitivamente en el estado  $|1\rangle$  [34].

Ahora, ¿cuál es el estado de un sistema que consiste no solo de un qubit sino de un conjunto de  $q$  qubits? La respuesta se presenta mediante la aplicación del producto tensorial de los  $q$  qubits individuales presentados en el sistema.

Inicialmente, se presenta la situación cuántica para  $q = 2$ , es decir, dos qubits en el sistema con una dimensión del espacio  $2^2 = 4$ . Podemos escribir la base de espacio como:

$$|u_i\rangle \otimes |v_j\rangle = |u_i, v_j\rangle, \quad (2.10)$$

donde  $i, j = 0, 1$ , y  $\otimes$  implica el producto tensorial; entonces:

$$|u_0\rangle = |0\rangle, \quad |u_1\rangle = |1\rangle, \quad |v_0\rangle = |0\rangle, \quad |v_1\rangle = |1\rangle; \quad (2.11)$$

la relaciones expresadas por las ecuaciones (2.10) y (2.11), permiten definir la base del espacio estado cuatro-dimensional como:

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}; \quad (2.12)$$

lo que puede ser escrito equivalentemente como:

$$\{|0, 0\rangle, |0, 1\rangle, |1, 0\rangle, |1, 1\rangle\}. \quad (2.13)$$

Por lo tanto, el 2 – qubit normalizado más general es

$$|x_1, x_2\rangle = \underbrace{|x_0\rangle}_{1^{er} \text{ qubit}} \otimes \underbrace{|x_1\rangle}_{2^{do} \text{ qubit}}, \quad (2.14)$$

que se puede formar en este espacio es la superposición lineal de los cuatro elementos de la base, es decir:

$$|x_1, x_2\rangle = a_0 |0, 0\rangle + a_1 |0, 1\rangle + a_2 |1, 0\rangle + a_3 |1, 1\rangle, \quad \sum_{i=0}^{2^2-1} |a_i|^2 = 1, \quad (2.15)$$

donde  $a_0, a_1, a_2, a_3 \in \mathbb{C}$ . Ahora, una convención utilizada en la computación cuántica es:

$$|x_1, x_2, \dots, x_m\rangle \equiv |x\rangle, \quad (2.16)$$

donde  $x_1, x_2, \dots, x_m$  es la representación binaria del entero  $x$ , es decir

$$x = x_1 2^{m-1} + x_2 2^{m-2} + \dots + x_{m-1} 2^1 + x_m 2^0. \quad (2.17)$$

De acuerdo con las ecuaciones (2.16) y (2.17) la base de un espacio formado por  $q$  qubits cuya dimensión es  $2^q$  está formada por

$$\{|0\rangle, |1\rangle, |2\rangle, \dots, |2^q - 1\rangle\}; \quad (2.18)$$

entonces, el  $q$  qubit normalizado más general

$$|x_1, \dots, x_q\rangle = \underbrace{|x_1\rangle}_{1^{er} \text{ qubit}} \otimes \underbrace{|x_q\rangle}_{q\text{-qubit}}, \quad (2.19)$$

usando la analogía de la ecuación (2.15), es posible ver la superposición lineal general como:

$$\sum_{i=0}^{2^q-1} |a_i|^2 = 1. \quad (2.20)$$

### 2.2.2.2. Medida Cuántica

La principal diferencia de las medidas aplicadas en elementos macroscópicos o microscópicos radica en el resultado arrojado por los procesos de medición, donde en el primer caso generan cantidades absolutas y en el segundo se obtienen probabilidades de encontrar al sistema en cierta configuración. Inmediatamente después de ser realizada la medición, la mecánica cuántica predice que el sistema evoluciona a otro estado normalizado.

Suponiendo que se desea medir cuando el sistema se encuentra en cierto estado  $|\phi\rangle = A|\psi\rangle$ , donde  $A$  implica la autofunción que describe el estado  $|\psi\rangle$ , se determina la probabilidad de encontrar el autovalor  $a_n$  de  $A$  asociado a este estado, la cual está dada por:

$$P_{a_n} = \sum_{m=1}^{g_n} |\langle \phi_n^m | \psi \rangle|^2, \quad (2.21)$$

donde  $g_n$  es el índice de degenerancia del autovalor  $a_n$ . Cuando el  $2 - qubit$  dado en la ecuación (2.15) es medido con respecto a la base, la probabilidad de encontrar un estado  $|0\rangle$  en el primer qubit del  $2 - qubit$  es:

$$P_{1|0} = |a_{00}|^2 + |a_{01}|^2, \quad (2.22)$$

de forma análoga, la probabilidad de encontrar un estado  $|1\rangle$  en el primer qubit del 2-qubit es:

$$P_{1|1\rangle} = |a_{10}|^2 + |a_{11}|^2. \quad (2.23)$$

Igualmente, para el segundo qubit es posible determinar la probabilidad de encontrar los estados  $|0\rangle$  y  $|1\rangle$  en el 2 – *qubit*, están representadas por

$$P_{2|0\rangle} = |a_{00}|^2 + |a_{10}|^2, \quad P_{2|1\rangle} = |a_{01}|^2 + |a_{11}|^2. \quad (2.24)$$

### 2.2.2.3. Evolución Cuántica

La evolución o dinámica de un  $q$  – *qubit* es determinada por un operador unitario  $\hat{U}$  sobre el espacio de Hilbert, este operador es denominado operador de evolución. Un operador es unitario si su adjunto es igual a su identidad [35], y puede expresarse como:

$$\hat{U}^\dagger \mathbf{U} = \mathbf{I} \quad (2.25)$$

Sea  $|\psi(t)\rangle = |x_1, \dots, x_q\rangle$  un estado de  $q$  – *qubit* para un tiempo  $t$  cualquiera, la evolución con base en el operador  $\hat{U}$  comprende un paso de computación, es decir, el cambio de un tiempo  $t$  a un tiempo  $t + 1$ , y está dada por

$$\mathbf{U} |\psi(0)\rangle \rightarrow \mathbf{U} |\psi(1)\rangle, \quad (2.26)$$

y en general, la evolución de  $m$  pasos de computación está dada por [22]:

$$\mathbf{U}^m |\psi(0)\rangle \rightarrow \mathbf{U} |\psi(m)\rangle. \quad (2.27)$$

En el contexto de la computación cuántica un operador de evolución que opera sobre un  $q$ -qubit, corresponde a una matriz unitaria de dimensión  $2^q$ .

### 2.2.2.4. Paralelismo Cuántico

La característica que pone en altos estándares a la computación cuántica y la convierte en una de las áreas más prometedoras, es la de poder abordar problemas que para la computación clásica resulta imposible por el tiempo de computo

necesario al intentar resolverlo. Usando un mecanismo de procesamiento de información en paralelo de manera masiva propuesto por Deutsch [22], esquematizado de la siguiente forma: Supóngase que se posee un computador cuántico que puede hacer evolucionar dos qubits cualesquiera según el operador unitario  $\hat{U}$  cuya transformación está representada por

$$\hat{U} = |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\rangle , \quad (2.28)$$

donde  $\oplus$  es la adición de modulo 2, es decir, la suma binaria. Usando la notación de la suma binaria que nos dice que  $0 \oplus 0 = 1$ ,  $1 \oplus 0 = 1$ ,  $0 \oplus 1 = 1$  y  $1 \oplus 1 = 0$ , se tiene

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

tomando  $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ , este operador cambia el segundo qubit  $|y\rangle$  a cero si  $f$  actuando en el primer qubit  $|x\rangle$  es 1, es decir, si  $f(x) = 0$  entonces  $|y \oplus f(x)\rangle = y$ , mientras que si  $f(x) = 1$  es  $|y \oplus f(x)\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|y\rangle$ . Luego,

$$\hat{U} : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) = |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) , \quad (2.29)$$

donde se ha aislado la función  $f$  en una fase dependiente de  $x$ . Si  $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  y  $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  se comprueba de inmediato que

$$\hat{U} : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}} [(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) . \quad (2.30)$$

De esta manera, con solo realizar una proyección ortogonal del primer qubit en una base  $\{|+\rangle, |-\rangle\}$ , donde

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) , \quad (2.31)$$

ya se ha resuelto con una única computación el problema planteado en la ecuación (2.28). Esto es posible debido que al utilizar un dispositivo cuántico, este no se limita a evaluar  $f(0)$  o  $f(1)$ , por el contrario, actúa sobre una superposición de los

estados  $|0\rangle$  y  $|1\rangle$  permitiendo extraer información global de la función. Este es el paralelismo cuántico [3].

### 2.2.2.5. Entrelazamiento

El entrelazamiento (entanglement), es tal vez el elemento clave con característica particular y no intuitiva de los sistemas cuánticos que crea la gran diferencia entre las teorías cuánticas y clásicas de la información. La existencia de estos estados cuánticos permiten afirmar que la descripción del estado de un sistema cuántico no puede ser siempre realizada con base en la descripción de los elementos que lo componen.

Para poder definir un estado cuántico de  $q$  qubits como entrelazado, es necesario poder expresarlo como el producto tensorial de los estados de cada uno de los  $q$  qubits que lo componen.

Sean dos qubits  $|x\rangle$  y  $|y\rangle$  dados por:

$$|x\rangle = a|0\rangle + b|1\rangle ; \quad |y\rangle = c|0\rangle + d|1\rangle ; \quad a, b, c, \in \mathbb{C} \quad (2.32)$$

el producto tensorial de estos dos qubits está dado por:

$$|x\rangle \otimes |y\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle ; \quad (2.33)$$

entonces, un estado de dos qubits es un estado entrelazado si no puede ser expresado por medio de una factorización de la forma  $|0\rangle \otimes |1\rangle$ . El análisis del comportamiento de un sistema cuántico con relación a la medida del mismo, permite observar si el sistema se encuentra o no en un estado entrelazado. Un sistema se encuentra en un estado entrelazado si la medida de uno de sus componentes afecta la medida de los otros.

Albert Einstein, Boris Podolsky y Nathan Rosen [36] fueron los primeros en percatarse de las consecuencias de la existencia de estos estados; pero, pareciéndoles del todo incompleta esta característica de “no localidad” de la Mecánica Cuántica, propusieron una teoría local de variables ocultas. Tres décadas más tarde, John Bell [37–39] consiguió probar que, mediante esquemas que supusiesen un comportamiento local de ambos subsistemas, es imposible imitar las correlaciones existentes entre los resultados obtenidos en la medida de dos subsistemas entrelazados. Los

experimentos de Alan Aspect y su grupo [40–42] confirmaron las predicciones de la teoría cuántica y demostraron, por tanto, que el comportamiento de la naturaleza es “no local”.

### 2.2.2.6. Esfera de Bloch

En mecánica cuántica, la esfera de Bloch es una representación geométrica del espacio de estados puros de un sistema cuántico de dos niveles. Su nombre alude al físico suizo Felix Bloch. Por extensión, también suele llamarse esfera de Bloch al conjunto de estados puros de sistema físico de un número finito arbitrario de niveles. En este caso, como se mostrará después, la esfera de Bloch ya no es una esfera, pero posee una estructura geométrica conocida como espacio simétrico.

Geoméricamente la esfera de Bloch puede ser representada por una esfera de radio unidad en  $\mathbf{R}^3$ . En esta representación, cada punto de la superficie de la esfera corresponde unívocamente a un estado puro del espacio de Hilbert de dimensión compleja, que caracteriza a un sistema cuántico de dos niveles.

Cada par de puntos diametralmente opuestos sobre la esfera de Bloch corresponde a dos estados ortonormales en el espacio de Hilbert, pues la distancia entre estos es 2, lo que de inmediato implica ortogonalidad. Como consecuencia forman una base del mismo espacio. Tales estados resultan ser autovectores de la proyección del operador de espín  $\frac{1}{2}$  sobre la dirección que determinan los dos puntos. Dicho operador se expresa empleando las matrices de Pauli, y todo sistema cuántico de dos niveles puede equipararse al caso de espín  $\frac{1}{2}$ .

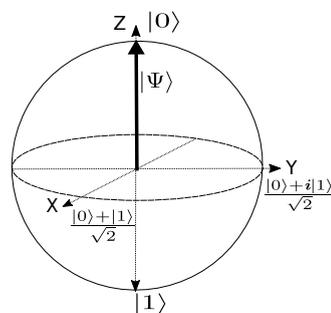


FIGURA 2.1: Estado Base  $|0\rangle$

### 2.2.2.7. Compuertas y circuitos lógicos

Las máquinas de Turing son equivalentes a circuitos lógicos en donde se le realizan procedimientos no triviales a la información. Estos procedimientos se denominan puertas lógicas. En las tablas (2.1) y (2.2), visualizamos algunas compuertas mayormente conocidas en la computación.

TABLA 2.1: Operaciones lógicas not, and y or.

x	y	NOT(-x)	AND( $x \wedge y$ )	OR( $x \vee y$ )
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

TABLA 2.2: Operaciones lógicas nand, nor y xor.

x	y	NAND( $x \uparrow y$ )	NOR( $x \downarrow y$ )	XOR( $x \otimes y$ )
0	0	0	1	0
0	1	0	0	1
1	0	0	0	1
1	1	1	0	0

Las operaciones lógicas presentadas en la tabla (2.1), pueden ser representadas por compuertas lógicas. Con estas operaciones lógicas es posible construir otras operaciones lógicas, tales como el nand ( $\uparrow$ ), xor ( $\otimes$ ) y el nor ( $\downarrow$ ) indicadas en la tabla (2.2). Estas nuevas operaciones lógicas pueden ser representadas por circuitos lógicos.

### 2.2.2.8. Compuertas Cuánticas

Una compuerta cuántica es una operación escrita por medio de una matriz unitaria que cumple la función de transformar el estado de un qubit a otro en un cierto periodo de tiempo. Con base en la descripción de la transformación que realiza

una compuerta cuántica sobre los elementos de la base del espacio, la matriz unitaria asociada a ella se obtiene a partir del siguiente procedimiento: Las filas de la matriz corresponden a los vectores base de entrada y las columnas de la matriz corresponden a los vectores base de salida; la  $(j, i)$  posición de la matriz corresponde, cuando el  $i$ -ésimo vector base es la entrada a la compuerta, al coeficiente del  $j$ -ésimo vector base en la salida de la compuerta[35]. El esquema más utilizado en computación cuántica, para representar una compuerta cuántica es el modelo circuital.

### Compuertas de Pauli

Las matrices de Pauli representan el primer conjunto de compuertas cuánticas y están representadas por operadores unitarios hermiticos. Su representación en forma matricial y circuital es:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \text{---} \boxed{I} \text{---} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \text{---} \boxed{X} \text{---}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \text{---} \boxed{Y} \text{---} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \text{---} \boxed{Z} \text{---}$$

FIGURA 2.2: Compuertas de Pauli

La compuerta de **X** equivale en computación clásica a una compuerta de negación *NOT*. Su equivalente en la esfera de Bloch es una rotación alrededor del eje  $x$  en un ángulo de  $\pi$  radianes, tal como se presenta en la figura (2.3). Al actuar esta compuerta sobre el estado  $|0\rangle$  se mapea a  $|1\rangle$  y cuando actúa en  $|1\rangle$  lo convierte en el estado  $|0\rangle$ .

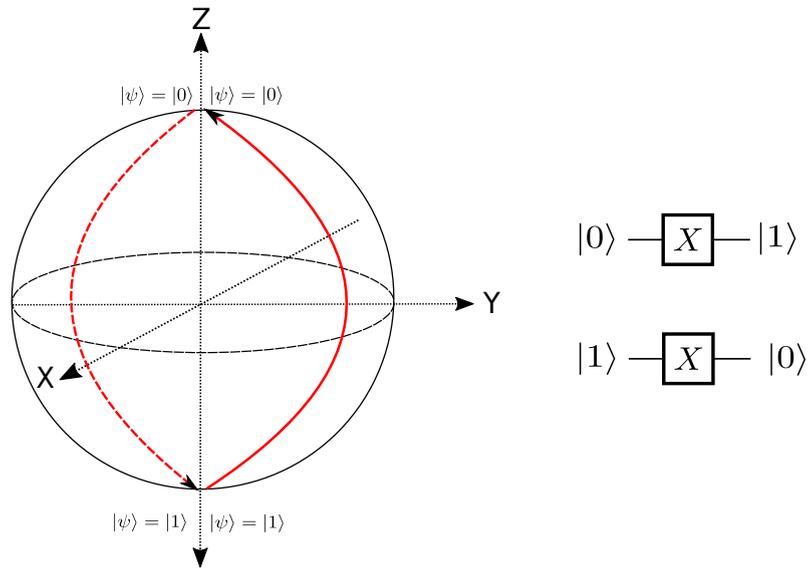


FIGURA 2.3: Compuerta **X**

La compuerta **Y** realiza una rotación de  $\pi$  radianes al estado cuántico respecto al eje  $y$  en la esfera de Bloch. El estado  $|0\rangle$  mapea a  $i|1\rangle$  y  $|1\rangle$  mapea a  $-i|0\rangle$ . Su visualización en la esfera de Bloch se muestra en la figura (2.4).

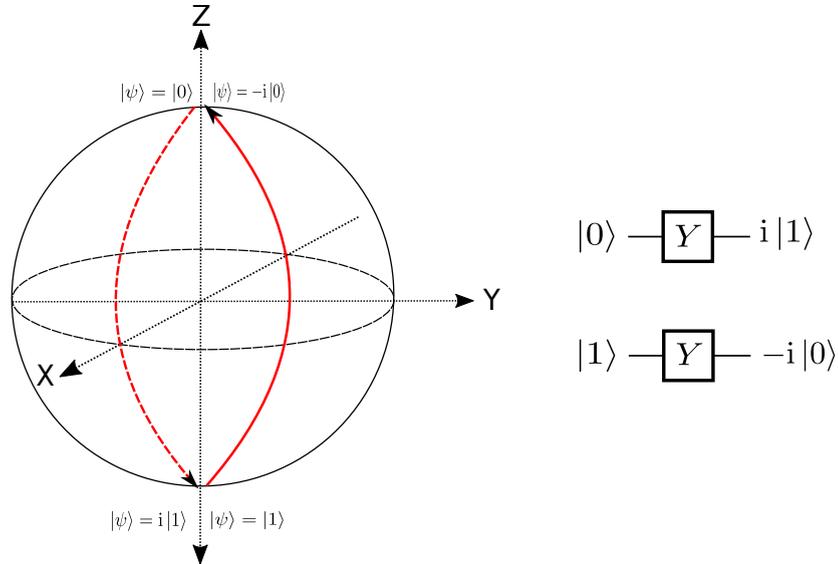


FIGURA 2.4: Compuerta **Y**

La compuerta de **Z** realiza una rotación de  $\pi$  radianes al estado cuántico respecto al eje  $z$ . El estado  $|0\rangle$  no cambia, mientras que el  $|1\rangle$  mapea  $|-1\rangle$ . En la figura (2.5) se visualiza su representación en la esfera de Bloch.

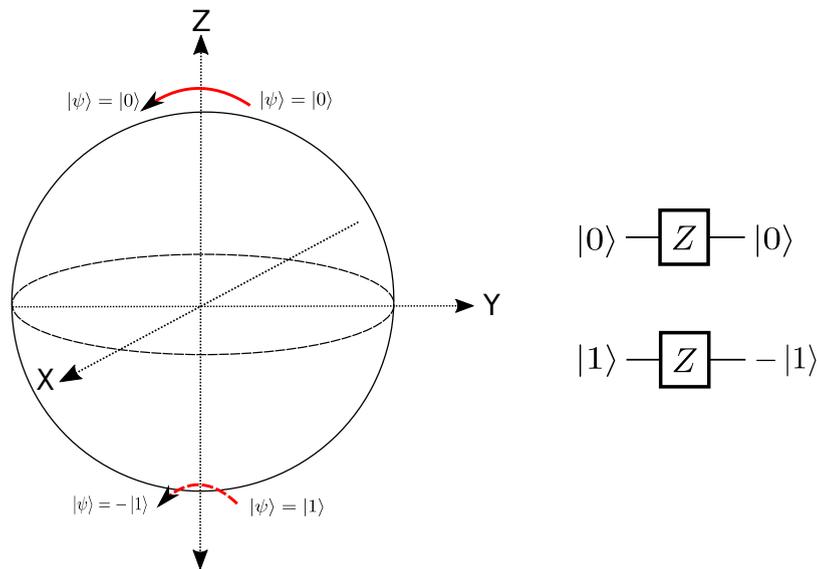


FIGURA 2.5: Compuerta Z

### Compuerta Cambio de Fase

La compuerta cambio de fase no realiza ningún cambio en el estado  $|0\rangle$ , pero  $|1\rangle$  mapea a  $e^{-i\theta} |1\rangle$ . En forma general, esta compuerta cambia la fase del estado cuántico. Su representación circuital y matricial es:

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = \text{---} \boxed{R_\theta} \text{---}$$

FIGURA 2.6: Compuerta de Fase

$R_\theta$  realiza una rotación en un ángulo  $\theta$  en la dirección contraria a las manecillas del reloj, sobre el eje  $z$  en su representación en la esfera de Bloch.

### Compuerta Hadamard

Esta compuerta, la cual es definida como la transformación de Fourier cuántica para 1 qubit [2, 34, 43], la cual es ampliamente utilizada en la construcción de circuitos cuánticos y, esta definida por el operador

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

FIGURA 2.7: Compuerta Hadamard

Una característica de esta compuerta es que  $H^2 = I$ . Cualquier operación unitaria sobre un solo qubit puede ser construida únicamente a partir de las compuertas de Hadamard y la compuerta de corrimiento de fase. Toda transformación unitaria mueve el estado de un qubit de un punto sobre la esfera de Bloch a otro punto en la misma. Esta compuerta juega un rol fundamental en la construcción de algoritmos cuánticos ya que permite crear una superposición de estados. Al actuar sobre el estado  $|0\rangle$ , se tiene:

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{2.34}$$

su representación en la esfera de Bloch se presenta en la figura (2.8).

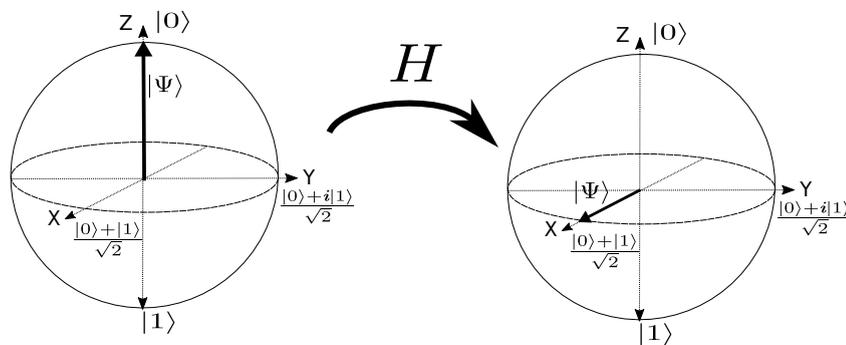


FIGURA 2.8: Compuerta Hadamard actuando sobre el estado  $|0\rangle$

Si la compuerta actúa sobre el estado  $|1\rangle$ , se tiene:

$$|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{2.35}$$

su representación en la esfera de Bloch se presenta en la figura (2.9).

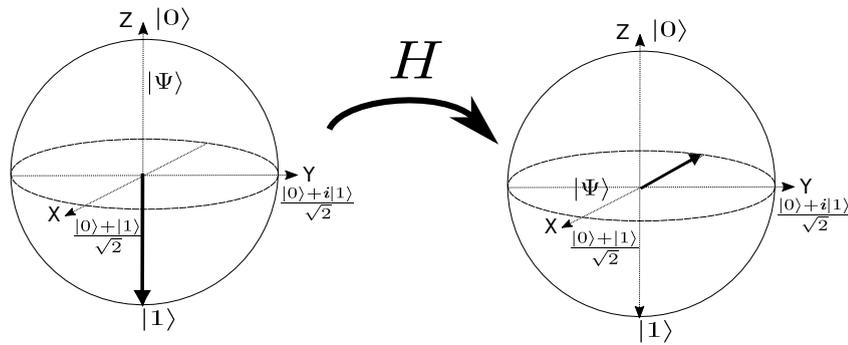


FIGURA 2.9: Compuerta Hadamard actuando sobre el estado  $|1\rangle$

### Compuerta CNOT

Esta compuerta permite generar entrelazamiento entre qubits. A diferencia de las anteriores compuertas, esta actúa sobre un sistema  $2 - qubits$ , con una base de la forma  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ . La acción de la compuerta **CNOT** sobre un qubit genérico se representa como:

$$CNOT(|x, y\rangle) = |x, x \oplus y\rangle, \tag{2.36}$$

donde  $\oplus$  indica la adición modulo 2. La representación matricial y circuital de esta compuerta se presenta a continuación:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

FIGURA 2.10: Compuerta **CNOT**

### 2.2.3. IBM Quantum Experience

En el mes de mayo de 2016, IBM anunció el lanzamiento de IBM Q [44], su primera computadora cuántica de 5 qubits de acceso libre a cualquier persona dispuesta a interactuar con el mundo cuántico. Este puede ser considerado el primer paso hacia una masificación de la computación cuántica a través de la nube.



FIGURA 2.11: Hardware de la computadora cuántica QIBM (tomado de [44])

Un año después, en mayo de 2017 [44], IBM anunció la introducción de dos nuevos procesadores en su computador cuántico: uno de 16 qubit que permitiría realizar experimentos de mayor complejidad que en el procesador de 5 qubit disponible anteriormente. Su uso está enfocado a desarrolladores, programadores e investigadores, quienes busquen ejecutar algoritmos cuánticos de mayor complejidad.

### 2.2.3.1. Computadora QX 2

Esta es una computadora cuántica que opera con un procesador  $QX2$  de 5 qubits superconductores (2.11), inmersa en un refrigerador de dilución. Esta localizada en los cuarteles generales de IBM, en el Thomas J. Watson Research Center, Yorktown Heights, New York. A diferencia de proyectos similares, el acceso que provee IBM a su computadora es libre y para todo el público. El procesador cuántico de IBM se basa en una red cuadrada de cinco qubits superconductores en un chip, como se presenta en la figura (2.12). Los qubits 0,1,3 y 4 se encuentran acoplados al qubit 2. Al realizar una operación con compuertas cuánticas de 2-qubits, estas

involucran al qubit 2 de este circuito. De igual forma, en la compuerta CNOT, el qubit 2 actúa como target.

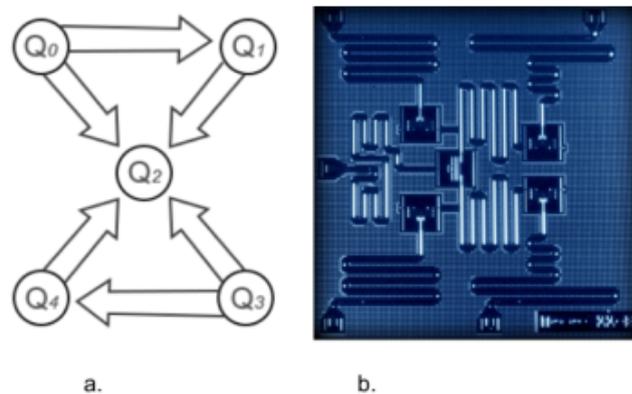


FIGURA 2.12: a. Arquitectura de conexiones y b. procesador cuántico de 5-qubits superconductores, disponible en la computadora cuántica de IBM (tomado de [44])

Toda operación en un computador cuántico, se ve afectada por errores que pueden ocurrir en los estados de superposición del qubit. Uno de ellos se denomina error de inversión del qubit, que simplemente invierte un qubit del estado  $|0\rangle$  al estado  $|1\rangle$  y viceversa. Para llevar a acabo una corrección de errores cuánticos, es necesario considerar adicionalmente los errores de cambio de fase (*phase – flip*), los cuales invierten el signo de la relación de fase entre  $|0\rangle$  y  $|1\rangle$  en un estado de superposición. La geometría cuadrada del circuito propuesto por IBM, permite detectar de forma simultánea estos errores [45]. En este circuito fue posible implementar protocolos de corrección de errores, permitiendo que esta arquitectura sea físicamente escalable a un sistema con un mayor número de qubits [45].



FIGURA 2.13: Interfaz gráfica del IBM Q denominada Quantum composer, sobre la cual es posible crear circuitos cuánticos utilizando una librería de compuertas lógicas y puntos de medición preestablecidos. (tomado de [44])

La interfaz de trabajo de esta computadora es llamada IBM Q experience [46] y ofrece una programación gráfica, empleando la representación del circuito cuántico. La figura (2.13) muestra el Quantum Composer, que es la interfaz gráfica sobre la cual se construye el circuito cuántico a estudiar.

Las mediciones posibles que ofrece el computador cuántico son dos: La representación en la esfera de Bloch y la medición estándar  $Z$ . En la primera, se indica el estado final del qubit al ser proyectado en  $X, Y$  y  $Z$ , el cual se representa como un vector al interior de una esfera. La segunda opción de medición es una proyección sobre el eje  $Z$  de la esfera de Bloch, la cual es representada como un gráfico de barras, indicando la probabilidad normalizada de que el resultado colapse en un cierto estado cuántico.

# Capítulo 3

## Desarrollos Teóricos

Para lograr comprender mejor nuestro trabajo y los resultados que de él derivan, es posible realizar la analogía de las demostraciones presentadas en esta sección con los resultados de la transformación de Fourier estándar ubicados en el apéndice (A).

### 3.1. Transformación de Fourier Fraccionaria Discreta (TFfD)

Tomando la fórmula de Namias (2.1) la TFf de orden  $\alpha$  de una función  $f(x)$  es

$$f_\alpha(x') = F_\alpha[f(x)] = C_\alpha e^{-i\pi x'^2 \cot(\alpha)} \int_{\text{Re}} f(x) e^{-i\pi x^2 \cot(\alpha)} e^{\frac{i2\pi x x'}{\sin(\alpha)}} dx, \quad (3.1)$$

donde,  $C_\alpha = \frac{e^{i(\frac{\pi}{4} - \frac{\hat{\alpha}}{2})}}{\sqrt{|\sin(\alpha)|}}$  y  $\hat{\alpha} = \text{sgn}(\sin(\alpha))$ . Asumiendo que  $\alpha$  es real en  $[-\pi, \pi]$  (ver [13]).  $F_\alpha[f(x)]$  es llamado el espectro fraccionario de orden  $\alpha$ . Teniendo en cuenta la función anterior es posible asociar  $N$  muestras en uno de los dominios con  $N$  muestras en el otro, usando  $\zeta$  y  $\xi$  como los soportes de las funciones  $f_\alpha(x')$  y  $f(x)$  en los dominios fraccionarios, respectivamente

$$N = \frac{\zeta \xi}{\sin(\alpha)}. \quad (3.2)$$

Ya que  $N$  se interpreta como el *número de grados de libertad o dimensionalidad de la función  $f(x)$* , ésta se define a su vez como una medida de la cantidad de

información contenida en la función. Ahora, para discretizar (2.9) es necesario usar una apropiada rata de muestreo, para esto se propone el siguiente cambio de variables:

$$x = n\Delta_x, \quad x' = k\Delta_{x'}, \quad (3.3)$$

donde acorde al teorema de muestreo propuesta por Torres en la referencia [47], las ratas de muestreo en terminos de  $x$  y  $x'$  respectivamente, son:

$$\Delta_x = \frac{\sin(\alpha)}{\zeta}, \quad \Delta_{x'} = \frac{\sin(\alpha)}{\xi}, \quad (3.4)$$

si delimitamos el rango de muestreo al intervalo  $0 < n < N - 1$ , donde  $N$  es el número de muestras en la función, se tiene

$$f_\alpha(k\Delta_{x'}) = C_\alpha e^{-i\pi(k\Delta_{x'})^2 \cot(\alpha)} \sum_{n=0}^{N-1} f(n\Delta_x) e^{-i\pi(n\Delta_x)^2 \cot(\alpha)} e^{\frac{i2\pi\Delta_x\Delta_{x'}}{\sin(\alpha)}nk}. \quad (3.5)$$

Reescribiendo los soportes de las funciones con respecto a  $\alpha$ , tal que  $\xi = \zeta = \sqrt{N \sin(\alpha)}$  en la cual su validez se puede demostrar por medio de la ecuación (3.2), es posible definir una rata de muestreo con respecto a  $\alpha$ :

$$\Delta_x = \Delta_{x'} = \frac{\sqrt{\sin(\alpha)}}{\sqrt{N}}. \quad (3.6)$$

Sustituyendo (3.6) en (3.5), obtenemos

$$F(k) = \overbrace{\frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{N}} e^{\frac{-i\pi k^2}{N} \cos(\alpha)} \sum_{n=0}^{N-1} e^{\frac{-i\pi n^2}{N} \cos(\alpha)} e^{\frac{i2\pi kn}{N}} f(n)}^{F_\alpha}. \quad (3.7)$$

la cual corresponde a la versión discretizada de la transformación de Fourier fraccionaria (TFf) para  $N$  entradas. Escrita la transformación de forma completa:

$$F_\alpha = \frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{N}} e^{\frac{-i\pi k^2}{N} \cos(\alpha)} \sum_{n=0}^{N-1} e^{\frac{-i\pi n^2}{N} \cos(\alpha)} e^{\frac{i2\pi kn}{N}} f(n). \quad (3.8)$$

Esta definición asocia  $N$  muestras en el dominio directo, con  $N$  muestras en el dominio fraccionario, pero además con la condición que se cumpla la rata de muestreo

óptimo en los dos dominios, dada por el teorema de muestreo.

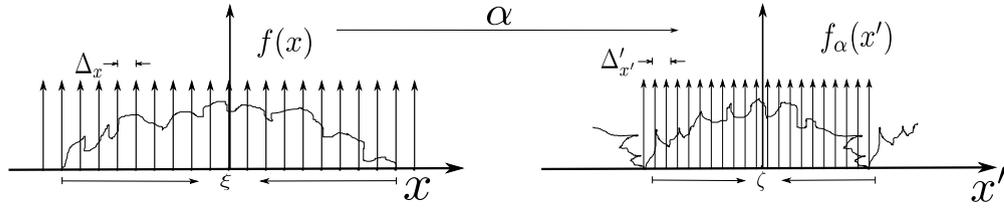


FIGURA 3.1: Espectro reconstruido completamente usando la tasa de muestreo apropiada

En resumen y tal como se muestra en la figura (3.1), el teorema de muestreo con el cual se obtiene la definición de la TFfD resulta adecuado. En algunas funciones más complejas, como por ejemplo con la función Chirp, se evidencia la necesidad de una dependencia de  $\alpha$  en la tasa de muestreo, y en consecuencia la aplicabilidad de esta nueva definición.

### 3.2. Transformación de Fourier Fraccionaria Cuántica (TFfC)

Tomando la TFfD definida en la sección anterior, la cual usando la notación Bra-ket desde la mecánica cuántica se puede expresar como un operador actuando sobre una combinación lineal de números

$$|F_\alpha[f]_k\rangle \rightarrow \frac{e^{i(\frac{\pi}{4} - \frac{\hat{\alpha}}{2})}}{\sqrt{\sin(\alpha)}} e^{\frac{-i\pi k^2}{2^q} \cos(\alpha)} \sum_{n=0}^{2^q-1} e^{\frac{-i\pi n^2}{2^q} \cos(\alpha)} e^{\frac{i2\pi}{2^q} kn} \left| \frac{n\sqrt{\sin(\alpha)}}{\sqrt{2^q}} \right\rangle, \quad (3.9)$$

con  $N = 2^q$ , la cual es la misma equivalencia usada en la transformación de Fourier estándar cuántica [2], donde  $q$  es el número de qubits, y adoptando la analogía de la mecánica cuántica usada en la ecuación (2.16) es posible reescribir la combinación lineal,

$$\left| \frac{n\sqrt{\sin(\alpha)}}{\sqrt{2^q}} \right\rangle = \frac{\sqrt{\sin(\alpha)}}{\sqrt{2^q}} |n\rangle.$$

Ahora, definiendo las variables  $\vartheta = e^{\frac{-i\pi}{2^q}}$  y  $\omega = e^{\frac{2i\pi}{2^q}}$ , la ecuación (3.9) se reduce a

$$|F_\alpha[f]_k\rangle \rightarrow \frac{e^{i(\frac{\pi}{4}-\frac{\hat{\alpha}}{2})}}{\sqrt{2^q}} \vartheta^{k^2 \cos(\alpha)} \sum_{n=0}^{2^q-1} \vartheta^{n^2 \cos(\alpha)} \omega^{kn} |n\rangle. \quad (3.10)$$

Escribiendo este operador de manera matricial,

$$W = \sum_{k,n=0}^{2^q-1} \omega^{kn} \quad V = \sum_{k,n=0}^{2^q-1} \vartheta^{k^2 \cos(\alpha)} \vartheta^{n^2 \cos(\alpha)}, \quad (3.11)$$

donde  $W$  es conocida como la matriz de Vandermonde (ver [48]) y  $V$  es definida como:

$$V = \begin{bmatrix} 1 \\ \vartheta^{\cos(\alpha)} \\ \vartheta^{4 \cos(\alpha)} \\ \dots \\ \vartheta^{k^2 \cos(\alpha)} \end{bmatrix} \begin{bmatrix} 1 & \vartheta^{\cos(\alpha)} & \vartheta^{4 \cos(\alpha)} & \dots & \vartheta^{n^2 \cos(\alpha)} \end{bmatrix}, \quad (3.12)$$

aplicando el producto matricial a (3.12), se tiene

$$V = \begin{bmatrix} 1 & \vartheta^{\cos(\alpha)} & \dots & \vartheta^{n^2 \cos(\alpha)} \\ \vartheta^{\cos(\alpha)} & \vartheta^{2 \cos(\alpha)} & \dots & \vartheta^{(n^2+1) \cos(\alpha)} \\ \vartheta^{4 \cos(\alpha)} & \vartheta^{5 \cos(\alpha)} & \dots & \vartheta^{(n^2+4) \cos(\alpha)} \\ \vdots & \vdots & \vdots & \ddots \\ \vartheta^{k^2 \cos(\alpha)} & \vartheta^{(k^2+1) \cos(\alpha)} & \dots & \vartheta^{(k^2+n^2) \cos(\alpha)} \end{bmatrix}. \quad (3.13)$$

Por lo tanto, la transformación de Fourier fraccionaria cuántica (TFfC) es definida a través de un producto Hadamard,

$$F_\alpha^q = \frac{e^{i(\frac{\pi}{4}-\frac{\alpha}{2})}}{\sqrt{2^q}} [V_N \circ W_N], \quad (3.14)$$

donde  $\circ$  es el producto Hadamard. Teniendo en cuenta que  $\alpha$  esta en un rango de  $[0, \pi]$ , entonces  $\alpha = \hat{\alpha}$ . Aplicando el producto Hadamard,

$$F_{\alpha}^q = \frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{2^q}} \begin{bmatrix} 1 & \vartheta^{\cos(\alpha)} & \dots & \vartheta^{n^2 \cos(\alpha)} \\ \vartheta^{\cos(\alpha)} & \vartheta^{2 \cos(\alpha)} \omega & \dots & \vartheta^{(n^2+1) \cos(\alpha)} \omega^{2^q-1} \\ \vartheta^{4 \cos(\alpha)} & \vartheta^{5 \cos(\alpha)} \omega^2 & \dots & \vartheta^{(n^2+4) \cos(\alpha)} \omega^{2(2^q-1)} \\ \vdots & \vdots & \vdots & \ddots \\ \vartheta^{k^2 \cos(\alpha)} & \vartheta^{(k^2+1) \cos(\alpha)} \omega^{2^q-1} & \dots & \vartheta^{(k^2+n^2) \cos(\alpha)} \omega^{(2^q-1)^2} \end{bmatrix}, \quad (3.15)$$

y reescribiendo (3.15) en términos de las variables originales, tenemos la TFfC generalizada para  $q$  qubits en el sistema.

$$F_{\alpha}^q = \frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{2^q}} \begin{bmatrix} 1 & e^{\frac{-i\pi}{2^q} \cos(\alpha)} & \dots & e^{\frac{-i\pi}{2^q} n^2 \cos(\alpha)} \\ e^{\frac{-i\pi}{2^q} \cos(\alpha)} & e^{\frac{-i\pi}{2^q} 2 \cos(\alpha)} e^{\frac{2i\pi}{2^q}} & \dots & e^{\frac{-i\pi}{2^q} (n^2+1) \cos(\alpha)} e^{\frac{2i\pi}{2^q} (2^q-1)} \\ e^{\frac{-i\pi}{2^q} 4 \cos(\alpha)} & e^{\frac{-i\pi}{2^q} 5 \cos(\alpha)} e^{\frac{2i\pi}{2^q} (2)} & \dots & e^{\frac{-i\pi}{2^q} (n^2+4) \cos(\alpha)} e^{\frac{2i\pi}{2^q} 2(2^q-1)} \\ \vdots & \vdots & \vdots & \ddots \\ e^{\frac{-i\pi}{2^q} k^2 \cos(\alpha)} & e^{\frac{-i\pi}{2^q} (k^2+1) \cos(\alpha)} e^{\frac{2i\pi}{2^q} (2^q-1)} & \dots & e^{\frac{-i\pi}{2^q} (k^2+n^2) \cos(\alpha)} e^{\frac{2i\pi}{2^q} (2^q-1)^2} \end{bmatrix}. \quad (3.16)$$

Esta compuerta representa la transformación aplicada a un sistema de  $q$  qubits para cambiar su estado de superposición, teniendo en cuenta el grado de libertad obtenido con el orden fraccionario que brinda la TFfC. No obstante, esta definición permite observar la aplicabilidad de la transformación en la computación cuántica, puesto que el orden fraccionario aplicado representa un desfase que no es posible obtener con las compuertas hasta ahora definidas.

# Capítulo 4

## Compuerta Cuántica $\mathcal{F}_\alpha$

### 4.1. Definición de $\mathcal{F}_\alpha$

Para un caso específico de  $q = 1$  (un qubit),  $2^1 = 2$ , se puede escribir (3.14) en la siguiente forma ,

$$F_\alpha = \frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{2}} \begin{bmatrix} 1 & \vartheta^{\cos(\alpha)} \\ \vartheta^{\cos(\alpha)} & \vartheta^{2\cos(\alpha)} \end{bmatrix} \circ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (4.1)$$

y reescribiendo (4.1)

$$F_\alpha = e^{i(\frac{\pi}{4} - \frac{\alpha}{2})} \begin{bmatrix} 1 & \vartheta^{\cos(\alpha)} \\ \vartheta^{\cos(\alpha)} & \vartheta^{2\cos(\alpha)} \end{bmatrix} \circ \underbrace{\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}}_{\mathbf{H}}, \quad (4.2)$$

donde la matriz de la derecha, corresponde a la compuerta Hadamard denotada como  $\mathbf{H}$ . Aplicando nuevamente el producto Hadamard como en la sección anterior y usando la definición de la TFfC como  $F_\alpha$  se tiene,

$$F_\alpha = \frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{2}} \begin{bmatrix} 1 & \vartheta^{\cos(\alpha)} \\ \vartheta^{\cos(\alpha)} & -\vartheta^{2\cos(\alpha)} \end{bmatrix}, \quad (4.3)$$

y por lo tanto, es definida la compuerta cuántica  $F_\alpha$  para un qubit como,

$$F_\alpha = \frac{e^{i(\frac{\pi}{4} - \frac{\alpha}{2})}}{\sqrt{2}} \begin{bmatrix} 1 & e^{-\frac{i\pi}{2}\cos(\alpha)} \\ e^{-\frac{i\pi}{2}\cos(\alpha)} & -e^{-i\pi\cos(\alpha)} \end{bmatrix}. \quad (4.4)$$

Es posible ver que para  $F_\alpha^q$ , es decir,  $F_\alpha$  aplicada a un número de  $q$  qubits definidos, basta con aplicar el producto tensorial  $F_\alpha \otimes F_\alpha^{q-1}$ , y se tiene la ecuación (3.16) nuevamente, la cual es la forma generalizada de la compuerta.

De acuerdo con la ecuación (2.25),  $F_\alpha$  puede ser una compuerta cuántica sí y solo sí, es un operador unitario. Para probar esto, se toma la condición y se evalúa matemáticamente como se muestra a continuación:

$$\begin{aligned}
 F_\alpha F_\alpha^\dagger &= \frac{e^{i(\frac{\pi}{4}-\frac{\alpha}{2})}}{\sqrt{2}} \frac{e^{-i(\frac{\pi}{4}-\frac{\alpha}{2})}}{\sqrt{2}} \\
 &\times \begin{bmatrix} 1 & e^{-\frac{i\pi}{2} \cos(\alpha)} \\ e^{-\frac{i\pi}{2} \cos(\alpha)} & -e^{-i\pi \cos(\alpha)} \end{bmatrix} \begin{bmatrix} 1 & e^{\frac{i\pi}{2} \cos(\alpha)} \\ e^{\frac{i\pi}{2} \cos(\alpha)} & -e^{i\pi \cos(\alpha)} \end{bmatrix} \\
 F_\alpha F_\alpha^\dagger &= \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I},
 \end{aligned} \tag{4.5}$$

y

$$\begin{aligned}
 F_\alpha^\dagger F_\alpha &= \frac{e^{-i(\frac{\pi}{4}-\frac{\alpha}{2})}}{\sqrt{2}} \frac{e^{i(\frac{\pi}{4}-\frac{\alpha}{2})}}{\sqrt{2}} \\
 &\times \begin{bmatrix} 1 & e^{\frac{i\pi}{2} \cos(\alpha)} \\ e^{\frac{i\pi}{2} \cos(\alpha)} & -e^{i\pi \cos(\alpha)} \end{bmatrix} \begin{bmatrix} 1 & e^{-\frac{i\pi}{2} \cos(\alpha)} \\ e^{-\frac{i\pi}{2} \cos(\alpha)} & -e^{-i\pi \cos(\alpha)} \end{bmatrix} \\
 F_\alpha^\dagger F_\alpha &= \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}.
 \end{aligned} \tag{4.6}$$

La principal característica de esta compuerta cuántica es el grado de libertad adicional ganado en la obtención de estados nuevos de los qubits siendo que esta permite rotaciones a diferentes estados de superposición del qubit, algunos ejemplos de esta ventaja son mostrados en la siguiente sección.

## 4.2. Aplicación de la Compuerta $\mathcal{F}_\alpha$

### 4.2.1. Grado de Libertad del Orden Fraccionario

El grado de libertad adicional mencionado anteriormente permite rotaciones de cualquier estado base hasta estados de superposición reales y/o complejos, con solo cambiar el orden fraccionario  $\alpha$  en un rango  $[0, \pi]$ .

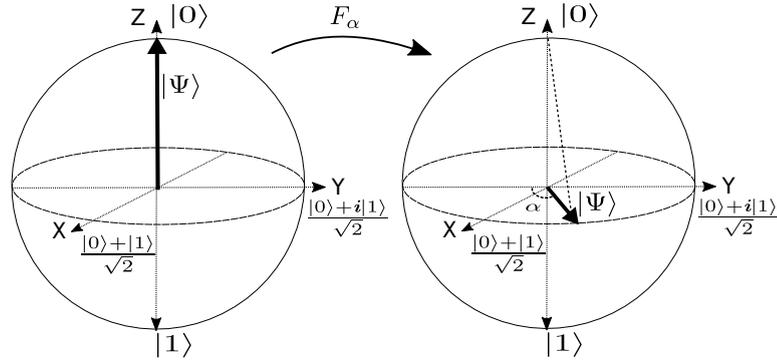


FIGURA 4.1: Superposición para la compuerta cuántica fraccionaria de orden  $\alpha$  desde el estado  $|0\rangle$ .

En el primer caso (Fig. 4.1), el grado de libertad es aplicado al estado inicial  $|0\rangle$ , y son obtenidos estados de superposición complejos del qubit, localizados entre los ejes  $-Y$  y  $Y$ , algunos ejemplos para diferentes ordenes fraccionarios se muestran en la tabla (4.1).

Estado Inicial	Orden Fraccionario	Estado Final
$ 0\rangle$	$F_0$	$\frac{1+i}{2}  0\rangle + \frac{1-i}{2}  1\rangle$
$ 0\rangle$	$F_{0,17\pi}$	$(0,61 + 0,35i)  0\rangle + (0,47 - 0,52i)  1\rangle$
$ 0\rangle$	$F_{\frac{\pi}{4}}$	$(0,65 + 0,27i)  0\rangle + (0,53 - 0,46i)  1\rangle$
$ 0\rangle$	$F_{0,35\pi}$	$(0,69 + 0,16i)  0\rangle + (0,63 - 0,32i)  1\rangle$
$ 0\rangle$	$F_{\frac{\pi}{2}}$	$\frac{1}{\sqrt{2}}  0\rangle + \frac{1}{\sqrt{2}}  1\rangle$
$ 0\rangle$	$F_{0,65\pi}$	$(0,69 - 0,16i)  0\rangle + (0,63 + 0,32i)  1\rangle$
$ 0\rangle$	$F_{\frac{3\pi}{4}}$	$(0,65 - 0,27i)  0\rangle + (0,53 + 0,46i)  1\rangle$
$ 0\rangle$	$F_{0,85\pi}$	$(0,60 - 0,37i)  0\rangle + (0,47 + 0,53i)  1\rangle$
$ 0\rangle$	$F_\pi$	$\frac{1-i}{2}  0\rangle + \frac{1+i}{2}  1\rangle$

TABLA 4.1: Orden fraccionario aplicado al estado base  $|0\rangle$

En el segundo caso (Fig. 4.2), se muestra cuando el estado inicial es  $|1\rangle$ , donde son obtenidos estados de superposición complejos del qubit nuevamente, algunos ejemplos se muestran en la tabla (4.2).

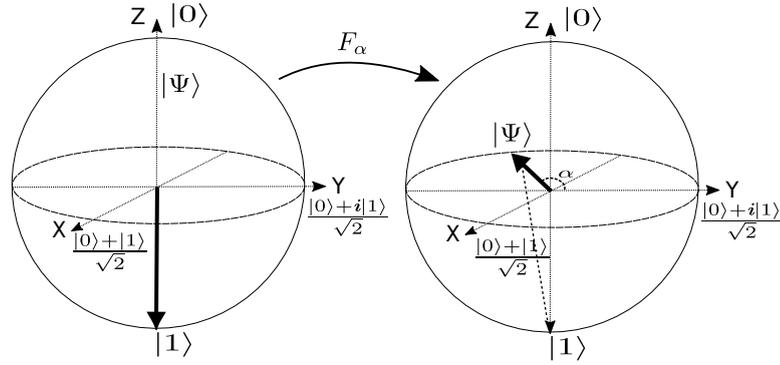


FIGURA 4.2: Superposición for fractional Fourier quantum gate of order  $\alpha$  from state  $|1\rangle$ .

Estado Inicial	Orden Fraccionario	Estado Final
$ 1\rangle$	$F_0$	$\frac{1-i}{2}  0\rangle + \frac{1+i}{2}  1\rangle$
$ 1\rangle$	$F_{0,17\pi}$	$(0,47 - 0,52i)  0\rangle + (0,41 + 0,58i)  1\rangle$
$ 1\rangle$	$F_{\frac{\pi}{4}}$	$(0,53 - 0,46i)  0\rangle + (0,18 + 0,68i)  1\rangle$
$ 1\rangle$	$F_{0,35\pi}$	$(0,63 - 0,32i)  0\rangle + (-0,41 + 0,66i)  1\rangle$
$ 1\rangle$	$F_{\frac{\pi}{2}}$	$\frac{1}{\sqrt{2}}  0\rangle - \frac{1}{\sqrt{2}}  1\rangle$
$ 1\rangle$	$F_{0,65\pi}$	$(0,63 + 0,32i)  0\rangle - (0,26 + 0,66i)  1\rangle$
$ 1\rangle$	$F_{\frac{3\pi}{4}}$	$(0,53 - 0,46i)  0\rangle + (0,18 - 0,68i)  1\rangle$
$ 1\rangle$	$F_{0,85\pi}$	$(0,53 - 0,47i)  0\rangle + (0,18 - 0,68i)  1\rangle$
$ 1\rangle$	$F_\pi$	$\frac{1+i}{2}  0\rangle + \frac{1-i}{2}  1\rangle$

TABLA 4.2: Orden fraccionario aplicado sobre el estado base  $|1\rangle$

En el último caso (Fig. 4.3), la compuerta es aplicada en un qubit localizado en un estado de superposición, donde el grado de libertad muestra sus ventajas de mover un qubit a diferentes estados en cualquier lugar de la esfera, los ejemplos con algunos ordenes fraccionarios se muestran en la tabla (4.3).

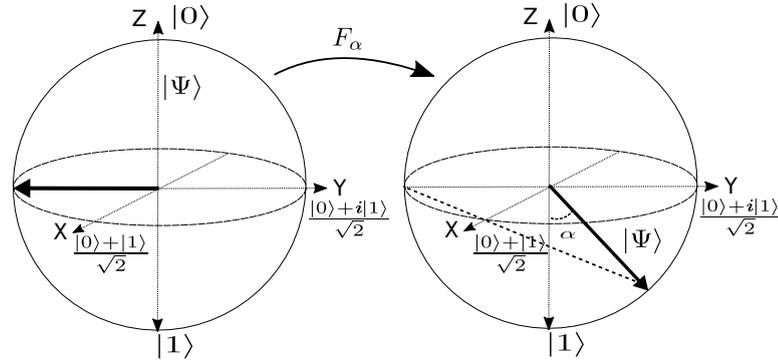


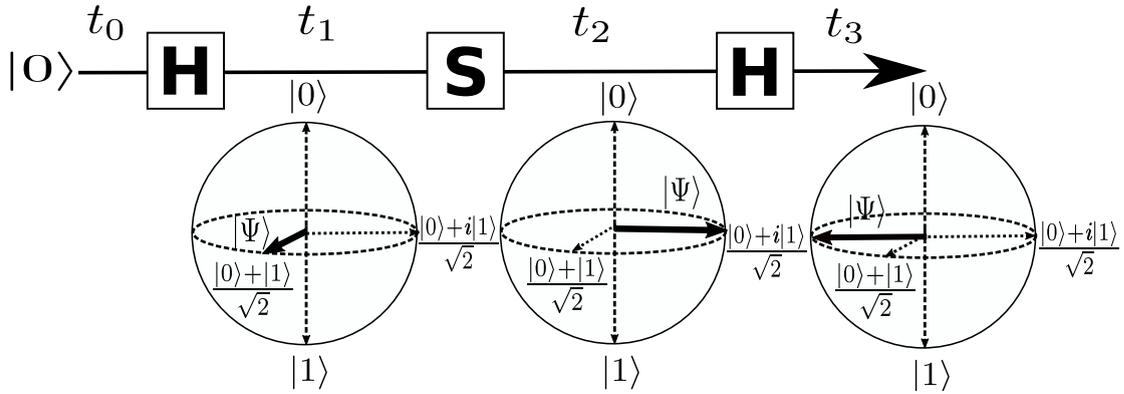
FIGURA 4.3: Superposición para el estado obtenido al aplicar la compuerta  $F_\alpha$  desde un estado en superposición.

Estado Inicial	Orden Fraccionario	Estado Final
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_0$	$\frac{1+i}{\sqrt{2}}  0\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{0,17\pi}$	$(0,80 + 0,58i)  0\rangle - (0,07 + 0,08i)  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{\frac{\pi}{4}}$	$(0,79 - 0,56i)  0\rangle - (0,10 + 0,20i)  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{0,35\pi}$	$(0,71 + 0,56i)  0\rangle - (0,02 + 0,41i)  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{\frac{\pi}{2}}$	$\frac{1+i}{2}  0\rangle + \frac{1-i}{2}  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{0,65\pi}$	$(0,26 + 0,33i)  0\rangle + (0,91 + 0,04i)  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{\frac{3\pi}{4}}$	$(0,13 + 0,18i)  0\rangle + (0,86 - 0,45i)  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_{0,85\pi}$	$(0,05 + 0,07i)  0\rangle + (0,72 + 0,69i)  1\rangle$
$\frac{1}{\sqrt{2}}  0\rangle + \frac{i}{\sqrt{2}}  1\rangle$	$F_\pi$	$\frac{1+i}{\sqrt{2}}  1\rangle$

TABLA 4.3: Resultados por cada orden fraccionario aplicado sobre el estado  $(\frac{1+i}{2} |0\rangle + \frac{1-i}{2} |1\rangle)$

### 4.2.2. Reducción de Complejidad Computacional

En la computación cuántica, al hablar de algoritmos cuánticos se considera que un circuito cuántico es menos costoso computacionalmente si existe una reducción considerable de las compuertas cuánticas requeridas para ejecutar el trabajo [3]. Como un ejemplo, un procedimiento usual que consiste en llevar al qubit a un estado de superposición complejo  $|\odot\rangle = |0\rangle - i|1\rangle$ , se muestra en la figura (4.4) a través del circuito cuántico


 FIGURA 4.4: Circuito Cuántico para mover el qubit al estado  $|0\rangle$ 

Donde  $\mathbf{S}$  es la compuerta de fase usada para tener superposiciones complejas, definida como:  $\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ .

El paso a paso para lograr describir el circuito matemáticamente es:

$$\begin{aligned}
 t_0 &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \\
 t_1 &= \mathbf{H}|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
 &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 t_2 &= \mathbf{SH}|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, \\
 &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \\
 t_3 &= \mathbf{HSH}|0\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+i \\ 1-i \end{bmatrix} \\
 &= \frac{1}{\sqrt{2}}((1+i)|0\rangle + (1-i)|1\rangle)
 \end{aligned} \tag{4.7}$$

resultando en un estado de superposición compleja ubicada en la base circular izquierda  $|0\rangle$ . Ahora, para ilustrar la eficiencia de la compuerta cuántica  $\mathbf{F}_\alpha$ , se muestra a continuación como este estado final se obtiene después de aplicar esta nueva compuerta, a través del circuito cuántico mostrado en la figura (4.5).

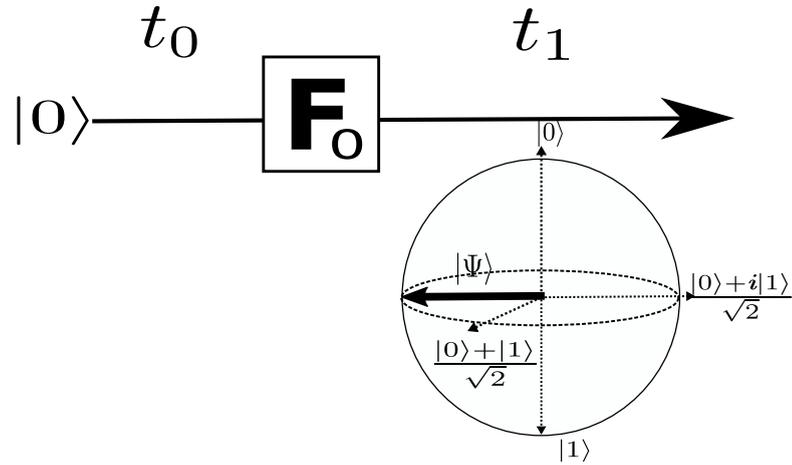


FIGURA 4.5: Circuito Cuántico para mover el qubit al estado  $|0\rangle$  usando la compuerta cuántica  $\mathbf{F}_\alpha$

El procedimiento matemático respectivo es:

$$\begin{aligned}
 t_0 &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \\
 t_1 &= \mathbf{F}_0 |0\rangle = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}} \begin{bmatrix} 1 & e^{-i\frac{\pi}{2}} \\ e^{-i\frac{\pi}{2}} & -e^{-i\pi} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\
 &= \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+i \\ 1-i \end{bmatrix} \\
 &= \frac{1}{2} ((1+i)|0\rangle + (1-i)|1\rangle).
 \end{aligned} \tag{4.8}$$

Entonces, la optimización consiste en reducir el número de compuertas cuánticas, dependiendo únicamente del orden fraccionario  $\alpha$ . Unificando las tres transformaciones a una se obtiene,

$$\mathbf{HSH} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \mathbf{F}_0. \tag{4.9}$$

Por lo tanto, el efecto de la simplificación en el circuito está dado por la característica de la compuerta  $\mathbf{F}_\alpha$  de simplificar el número de compuertas cuánticas utilizadas en un algoritmo para llevar a cabo cierto trabajo utilizando un determinado orden  $\alpha$ . Ya que con esta nueva compuerta es posible obtener el mismo efecto de aplicar diversas rotaciones en conjunto al qubit, la cual constituye una reducción significativa de la complejidad cuántica y por lo tanto una reducción en el volumen cuántico de los algoritmos.

### 4.2.3. Entrelazamiento de Qubits

A continuación se muestra la aplicación de la compuerta  $\mathbf{F}_\alpha$  en un caso de más de un qubit, en donde el resultado presenta un entrelazamiento entre dos qubits con el efecto del orden fraccionario (ver Fig. 4.6).

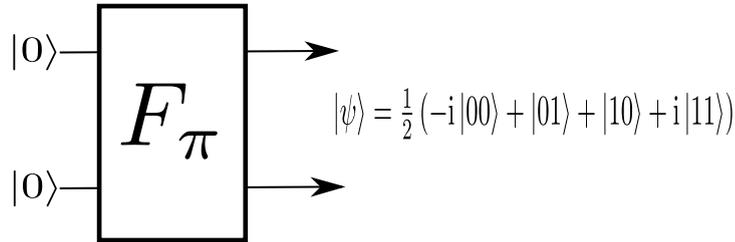


FIGURA 4.6: Circuito Cuántico del estado entrelazado

La descripción matemática para el circuito cuántico mostrado en la figura (4.6) es,

$$\begin{aligned}
 |\Psi\rangle &= (\mathbf{F}_\pi \otimes \mathbf{F}_\pi) |00\rangle \\
 &= \left( \frac{1-i}{2} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \otimes \frac{1-i}{2} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \right) |00\rangle \\
 &= \frac{1}{2} \begin{bmatrix} -i & 1 & 1 & i \\ 1 & -i & i & 1 \\ 1 & i & -i & 1 \\ i & 1 & 1 & -i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -i \\ 1 \\ 1 \\ i \end{bmatrix} \\
 &= \frac{1}{2} (-i|00\rangle + |01\rangle + |10\rangle + i|11\rangle)
 \end{aligned} \tag{4.10}$$

Si se calcula la matriz de densidad reducida  $\rho$  del estado obtenido, para un estado  $|\Psi\rangle = |\psi\rangle |\phi\rangle$  se verifica la condición de entrelazamiento del estado si el rango de  $\rho$  es diferente de uno [2].

$$\rho_A = Tr_B(|\Psi\rangle \langle\Psi|) = |\psi\rangle \langle\psi|, \tag{4.11}$$

y

$$Tr(\rho_A^2) = Tr(|\psi\rangle \langle\psi| \cdot |\psi\rangle \langle\psi|) \neq 1, \tag{4.12}$$

con el estado  $|\Psi\rangle = \frac{1}{2}(-i|00\rangle + |01\rangle + |10\rangle + i|11\rangle)$  aplicando la ecuación (4.12) es obtenido  $Tr(\rho_A^2) = \frac{1}{4}$ , por lo tanto se concluye que  $|\Psi\rangle$  es un estado entrelazado y que la compuerta  $\mathbf{F}_\alpha$  puede ser aplicada para obtener estados entrelazados específicos usando el orden fraccionario. Similarmente, el grado de libertad aplicado al sistema con más de un qubit ha sido demostrado con un ejemplo elemental, donde nuevos estados entrelazados son obtenidos basados en el orden fraccionario.

# Capítulo 5

## Aplicaciones de $\mathcal{F}_\alpha$ en algunos Algoritmos Cuánticos

### 5.1. Algoritmo de Grover

Muchos problemas, que se pueden denominar problemas de búsqueda, se pueden plantear de la siguiente forma: "Hallar  $x$  en un conjunto de posibles soluciones tal que la sentencia  $P(x)$  sea cierta".

Por ejemplo, el problema de buscar un factor para un número entero  $q$  se puede tratar con un algoritmo de búsqueda en un lista que contenga a todos los enteros entre 2 y  $\sqrt{q}$ , buscando uno que verifique la propiedad  $P(x) : q \bmod x = 0$ .

Un problema de búsqueda no estructurada es aquel para cuya resolución no se puede usar ninguna hipótesis relativa a la estructura del espacio de soluciones o a la sentencia  $P$ .

Por ejemplo, una búsqueda en una lista alfabetizada, como la búsqueda del número de un usuario en la guía telefónica, es un problema de búsqueda estructurada, mientras que la búsqueda en la misma guía del titular de un número concreto sería una búsqueda no estructurada. En una búsqueda estructurada, se puede usar la estructura ordenada de la lista para construir algoritmos eficientes, pero en una búsqueda no estructurada lo habitual es testear aleatoriamente la veracidad de la sentencia. En el modelo de computación clásico, para un espacio de búsqueda de tamaño  $N$ , sería necesario evaluar  $P$  un promedio de  $N/2$  veces y  $N$  veces en el peor de los casos. Los algoritmos clásicos de búsqueda no estructurada requieren  $O(N)$  evaluaciones de  $P$ .

Grover (ver [4]) probó en 1996 que, con computación cuántica, un problema de búsqueda no estructurada, con solución única, se puede resolver, con probabilidad acotada, con  $O(\sqrt{N})$  evaluaciones de  $P$ .

Probablemente una de las muchas ventajas que tiene una computadora cuántica sobre una computadora clásica es su base de datos de búsqueda de velocidad superior. El algoritmo de Grover demuestra esta capacidad [4]. Este algoritmo puede acelerar un problema de búsqueda no estructurada de forma cuadrática, pero sus usos se extienden más allá de eso. Puede servir como un truco general o subrutina para obtener mejoras de tiempo de ejecución cuadráticas para una variedad de otros algoritmos. Esto se llama el truco de amplificación de amplitud. Pero antes de comenzar las simulaciones, veamos el problema de la búsqueda no estructurada.

### Descripción del Algoritmo

Partimos de una lista de tamaño  $N$ . Suponiendo, que  $N = 2^q$  para algún  $q$ . Trabajaremos con los índices de los elementos de la lista, es decir con  $x = 0..2^q - 1$  y se quiere localizar aquellos  $x$  tales que  $f(x) = 1$ , para una cierta función booleana  $f$ .

La computación cuántica permite evaluar  $f$  simultáneamente sobre todos los posibles *inputs*, sin más que construir el estado  $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ , que se obtiene, a partir de  $|00\dots,0\rangle$ , con la compuerta Hadamard. El problema es que no puede leer el resultado obtenido sin destruir el estado.

Se parte del estado  $|\psi\rangle$  y se ira modificando de modo que se vaya incrementando la amplitud de los  $x$  tales que  $f(x) = 1$  y disminuyendo la de aquellos que no verifican la propiedad. Así se conseguira, al medir el registro resultante, tener un acierto con probabilidad alta. Para conseguir este efecto, en un estado cuántico  $\sum_{j=0}^{N-1} a_j |x_j\rangle$ , primero se invierte la amplitud, es decir se cambia  $a_j$  por  $-a_j$  para los  $x_j$  tales que  $f(x_j) = 1$  y después se lleva a cabo la operación denominada inversión sobre el promedio, que transforma  $\sum_{j=0}^{N-1} a_j |x_j\rangle$  en  $\sum_{j=0}^{N-1} (2A - a_j) |x_j\rangle$ , donde  $A$  es el promedio de los  $a_j$ .

Es notable que si los  $a_j$  son números reales, después de realizar estas operaciones se tendrá un estado cuyas amplitudes sean también números reales. A continuación se puede observar como llevar a cabo cada una de estas operaciones:

1. Cambio de signo de la amplitud

Se trata de implementar la transformación,

$$U : |x\rangle \rightarrow (-1)^{f(x)} |x\rangle , \quad (5.1)$$

que no modifica los  $|x\rangle$  tales que  $f(x) = 0$  y pone un coeficiente  $-1$  a los que verifican  $f(x) = 1$ .

Se sabe que la compuerta cuántica  $U_f$  implementa la evaluación de la función booleana  $f$  del siguiente modo:

$$U_f : |x, b\rangle \rightarrow |x, b \oplus f(x)\rangle , \quad (5.2)$$

donde  $\oplus$  es la suma módulo 2. Cuando sólo se quiere evaluar  $f$  sobre un estado  $|x\rangle$  se aplica  $U_f$  con  $b = 0$ , pero en este caso se considera el estado  $|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ . Nótese que si  $f(x) = 0$ , entonces  $|b \oplus f(x)\rangle = |b\rangle$ , mientras que si  $f(x) = 1$  es  $|b \oplus f(x)\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|b\rangle$ , luego:

$$U_f(|x, b\rangle) = (-1)^{f(x)} |x, b\rangle . \quad (5.3)$$

Con esta transformación se realiza simultáneamente la evaluación de  $f$  y la inversión de las amplitudes de los  $|x_j\rangle$  que satisfacen la propiedad.

A continuación se muestra a detalle la actuación de  $U_f$  sobre un estado cualquiera  $\phi = \sum_{j=0}^{N-1} a_j |x_j\rangle$ .

Sean  $X_0 = x : f(x) = 0$  y  $X_1 = x : f(x) = 1$ . Entonces:

$$\begin{aligned} U_f(|\phi, b\rangle) &= U_f \left( \sum_{x_j \in X_0} a_j |x_j, b\rangle + \sum_{x_j \in X_1} a_j |x_j, b\rangle \right) \\ &= \left( \sum_{x_j \in X_0} a_j |x_j, b\rangle - \sum_{x_j \in X_1} a_j |x_j, b\rangle \right) \\ &= \left( \sum_{x_j \in X_0} a_j |x_j, b\rangle - \sum_{x_j \in X_1} a_j |x_j, b\rangle \right) \otimes |b\rangle . \end{aligned} \quad (5.4)$$

Por tanto el efecto de  $U_f$  es el cambio de signo de las amplitudes. Nótese que en la salida de  $U_f$  no se modifica el estado de  $b$ , por lo tanto se puede omitir al escribir y en lo que sigue es posible referirse a esta transformación, que en la literatura especializada se suele denominar “oráculo”, como:

$$U : |x\rangle \rightarrow (-1)^{f(x)} |x\rangle . \quad (5.5)$$

## 2. Inversión sobre el Promedio

Dado  $\psi = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ , se puede ver que la transformación  $G = 2|\psi\rangle\langle\psi| - I$  cuya matriz asociada es:

$$G = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \dots & \frac{2}{N} \\ \vdots & \vdots & \dots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} - 1 \end{bmatrix} \quad (5.6)$$

transforma  $\sum_{j=0}^N a_j |x_j\rangle$  en  $\sum_{j=0}^N (2A - a_j) |x_j\rangle$ , donde  $A$  es el promedio de los  $a_j$ .

Grover propuso una implementación eficiente de esta transformación con  $O(\log(N))$  compuertas elementales. Para ello basta probar que  $G = W_n R W_n$ , donde  $W_n$  es la transformación de Walsh-Hadamard ( $W_n = H \otimes H^n$  y  $R = (r_{ij})$ ) es una matrix diagonal tal que  $r_{11} = 1$  y  $r_{ii} = -1$  para  $i = 2 \dots N$ .

La matriz  $R$  se puede escribir como  $R = R' - I$  donde  $R' = 2|0\rangle\langle 0|$  es una matriz con todos sus elementos iguales a 0 menos el de la primera fila y primera columna que es  $r'_{11} = 2$ . Entonces:

$$W_n R W_n = W_n (2|0\rangle\langle 0| - I) W_n = W_n 2|0\rangle\langle 0| W_n - I, \quad (5.7)$$

y como  $W_n |0\rangle = |\psi\rangle$ , se concluye que:

$$W_n R W_n = 2|\psi\rangle\langle\psi| - I = G. \quad (5.8)$$

La transformación  $R$  se puede implementar con  $n = \log(N)$  compuertas CNOT y el costo de  $W_n$  también es  $\log(N)$ . El algoritmo de Grover consiste en aplicar sucesiva y reiteradamente las transformaciones  $U$  (5.5) y  $G$  (5.6).

### 5.1.0.1. Ejemplos de Circuitos Cuánticos Propuestos por IBM

A continuación se definen 4 ejemplos de IBM donde el objetivo principal es ubicar el ganador en las 4 principales combinaciones de  $|0\rangle$  y  $|1\rangle$ . El algoritmo esta conformado por tres partes como se muestra en la figura (5.1). Para empezar el algoritmo toma dos qubits en su proceso, ubicados como  $q[1]$  y  $q[2]$ , primero se tiene la fase *Save*, la cual consiste en encriptar el estado del sistema complicando la forma de conocer el estado final de los qubits. Luego, la sección *Oracle* hace referencia a la

aplicación de la función “Óráculo” que permite la búsqueda avanzada del estado final del sistema. Por último, se establece la medición del estado final del sistema abarcando las probabilidades de encontrar el sistema en cada combinación lineal dada por los estados  $|0\rangle$  y  $|1\rangle$ .

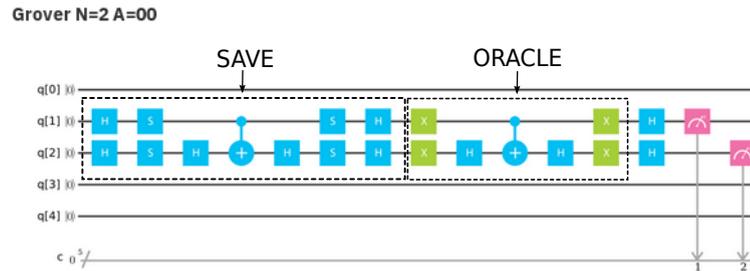
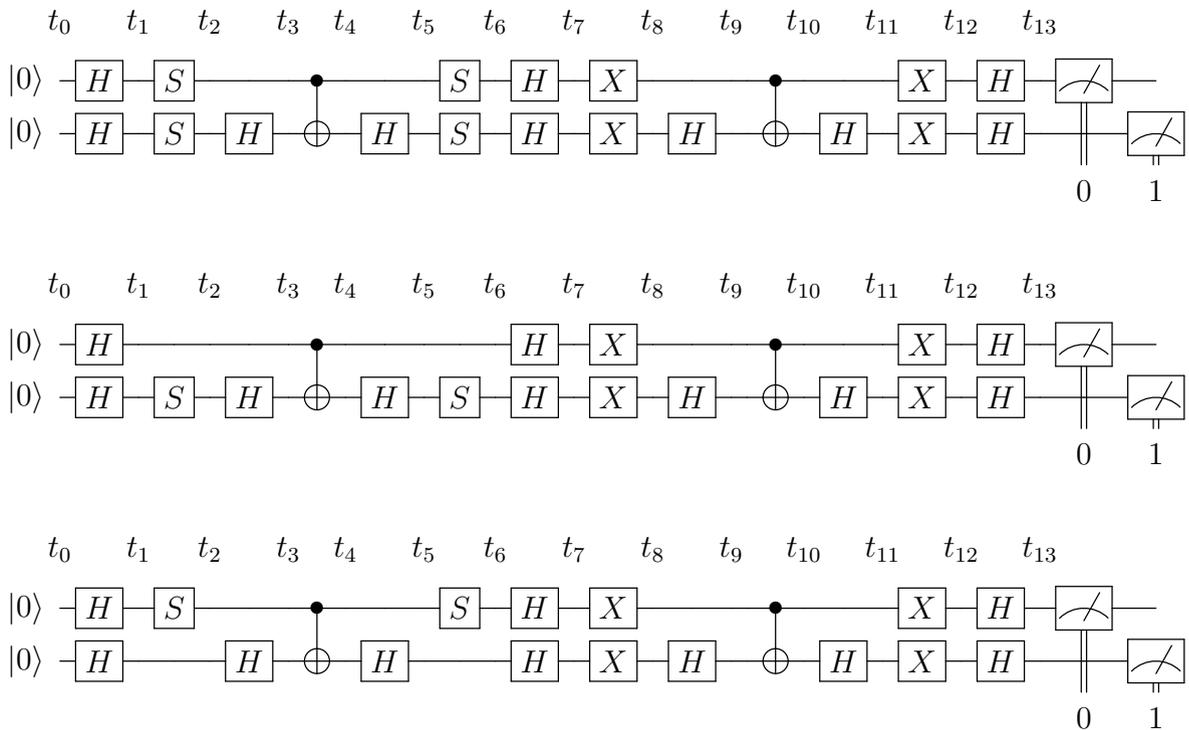
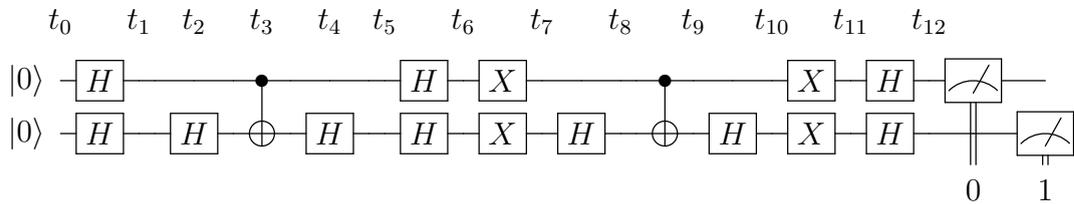


FIGURA 5.1: Algoritmo de Grover propuesto por IBM (<https://goo.gl/ppzrjR>)

Los algoritmos establecidos por IBM como un ejemplo básico para entender el funcionamiento del algoritmo de Grover se presentan en los siguientes circuitos cuánticos (Figura 5.1). La descripción matemática de estos ejemplos se encuentra en el apéndice (B).





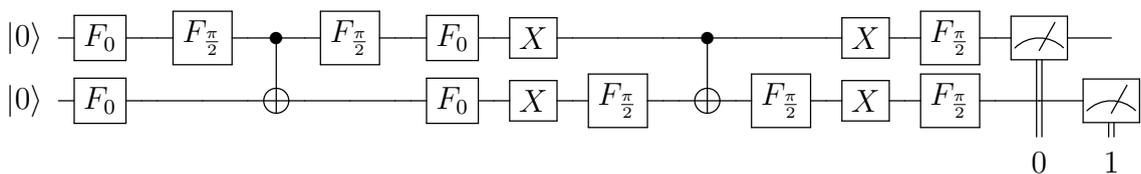
**Figura 5.1:** Circuitos cuánticos definidos como ejemplo para el algoritmo de Grover por IBM Q Experience.

La diferencia de estos cuatro ejemplos es la manera en que el qubit ha sido encriptado, y por lo tanto es modificado el estado final del sistema luego de terminar cada algoritmo, obteniendo así diferentes combinaciones de los estados base  $|0\rangle$  y  $|1\rangle$ .

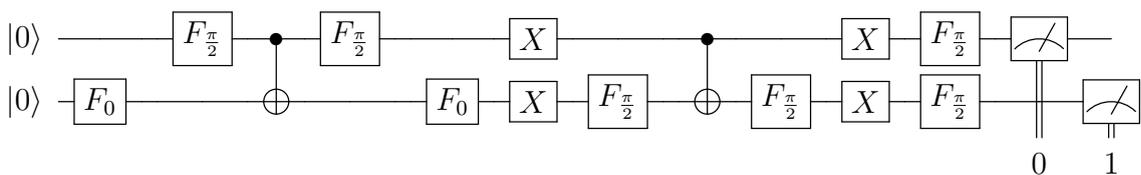
### 5.1.0.2. Circuitos Cuánticos Propuestos por IBM usando la compuerta cuántica $\mathcal{F}_\alpha$

En este algoritmo se presenta la aplicación de la nueva compuerta  $\mathcal{F}_\alpha$  en el uso de optimización de los circuitos cuánticos, ya que como fue explicado anteriormente, al reducir el número de compuertas cuánticas usadas en un algoritmo, inmediatamente es reducida su complejidad algorítmica, y por ende es obtenido un menor tiempo de cómputo para el algoritmo. Además, al hablar de algoritmos cuánticos es notable por medio de los siguientes circuitos cuánticos la aplicación del grado de libertad adicional proporcionada por esta compuerta, al llevar inmediatamente el qubit a un estado de superposición compleja para así, emplear un nuevo estado en los diferentes circuitos (Figura 5.2). La descripción matemática de estos ejemplos se encuentra en el apéndice (B).

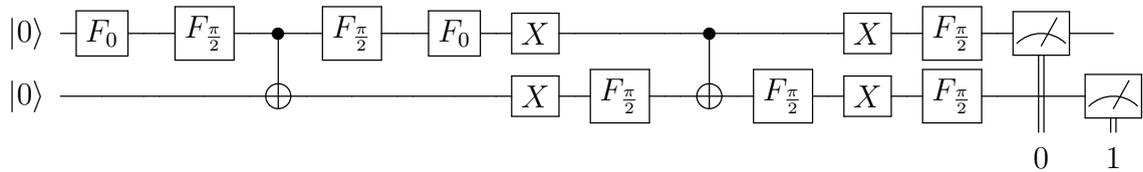
#### Grover N=2 A=00



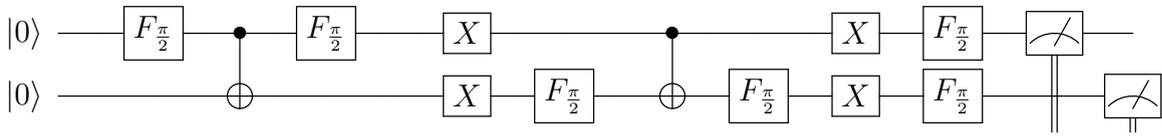
#### Grover N=2 A=01



**Grover N=2 A=10**



**Grover N=2 A=11**



**Figura 5.2:** Aplicación de la compuerta  $F_\alpha$  en los circuitos cuánticos definidos como ejemplo para el algoritmo de Grover por IBM Q Experience.

## 5.2. Algoritmo de Shor

Aunque cualquier número entero tiene una descomposición única en un producto de números primos, se dice que encontrar los factores primos es un problema difícil [5]. De hecho, la seguridad de nuestras transacciones online se basa en el supuesto de que factorizar enteros con mil dígitos o más es prácticamente imposible. Esta suposición ha sido cuestionada en 1995 cuando Peter Shor propuso un algoritmo cuántico de tiempo polinómico para el problema de la factorización [5, 6].

### Complejidad de Factorizar

Supongamos que nuestra tarea es factorizar un entero  $N$  con  $d$  dígitos decimales. El algoritmo de fuerza bruta recorre todos los números primos  $p$  hasta  $\sqrt{N}$  y verifica si  $p$  divide  $N$ . En el peor de los casos, esto tomaría un tiempo aproximado de  $\sqrt{N}$  lo cual es exponencial en el número de dígitos  $d$ . Un algoritmo más eficiente conocido como el quadratic sieve intenta construir los enteros  $a, b$  de modo que  $a^2 - b^2$  es un múltiplo de  $N$ . Una vez que se encuentra  $a, b$  se comprueba si  $a \pm b$  tiene factores comunes con  $N$ . El método quadratic sieve tiene un tiempo de ejecución asintótico exponencial en  $\sqrt{d}$ . El algoritmo de factorización clásico más eficiente conocido como *general number field sieve* logra un exponencial de tiempo de ejecución asintótico en  $d^{\frac{1}{3}}$ . La escala de tiempo de ejecución exponencial limita la aplicabilidad de los algoritmos de factorización clásicos a números con unos

pocos cientos de dígitos, con el registro mundial siendo  $d = 232$  (que toma aproximadamente 2000 años para ejecutarse). En contraste, el algoritmo de factorización de Shor tiene un polinomio de tiempo de ejecución en  $d$ . La versión del algoritmo que se describe a continuación debido a Alexey Kitaev requiere aproximadamente  $10d$  qubits y tiene un tiempo de ejecución de aproximadamente  $d^3$  [46].

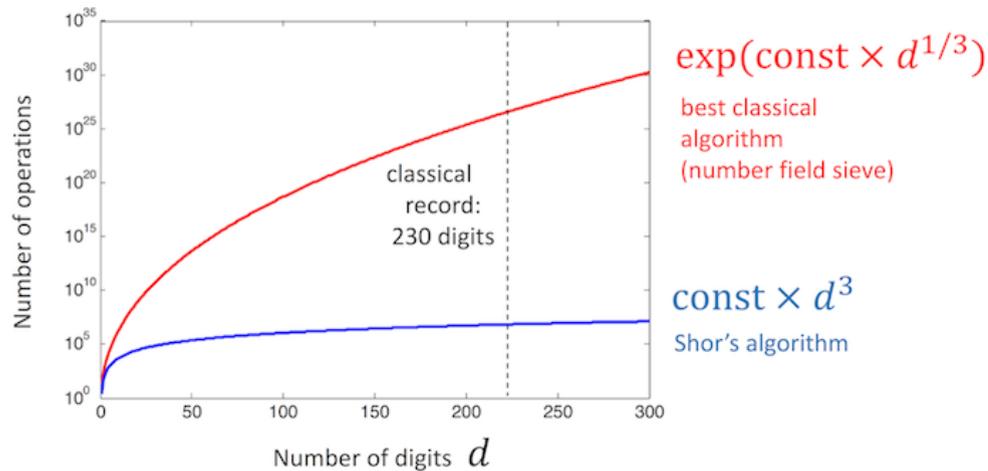


FIGURA 5.2: Algoritmos de factorización clásicos vs cuánticos (<https://goo.gl/ppzrjR>)

### Descripción del Algoritmo

Demostremos ahora que una computadora cuántica puede simular eficientemente la máquina de búsqueda de períodos. Explotaremos el paralelismo cuántico y la interferencia constructiva para determinar si una función complicada tiene una cierta propiedad global que no puede aprenderse evaluando la función solo en algunos puntos. Sin embargo, en lugar de detectar la propiedad de ser una función balanceada, buscamos detectar y medir la periodicidad de la función de exponenciación modular. El hecho de que la interferencia facilite la medición de la periodicidad no debería ser una gran sorpresa. Después de todo, utilizamos habitualmente la dispersión de las ondas electromagnéticas y las mediciones de interferencia para determinar la periodicidad de los objetos físicos, como las celosías de cristal. Del mismo modo, el algoritmo de Shor explota la interferencia para medir la periodicidad de los objetos aritméticos[46].

Supongamos que se nos dan enteros primos comunes  $a, N$ . Nuestro objetivo es calcular el período de un módulo  $N$ , es decir, el entero positivo más pequeño  $r$  tal que  $a^r = 1(\text{mod}N)$ . La idea básica es construir un operador unitario  $U_a$  que implemente la función de multiplicación modular  $x \rightarrow ax(\text{mod}N)$ . Se puede demostrar que los valores propios de  $U_a$  están estrechamente relacionados con el

período de  $a$ . Es decir, cada valor propio de  $U_a$  tiene una forma  $e^{i\gamma}$ , donde  $\gamma = \frac{2\pi k}{r}$  para algún entero  $k$ . Además, los valores propios de ciertos operadores unitarios se pueden medir de manera eficiente utilizando el algoritmo de estimación de fase. Desafortunadamente, inferir  $r$  a partir de los valores propios medidos de  $U_a$  solo es posible si los valores propios se miden exactamente (o con una precisión exponencialmente pequeña). Por ejemplo, factorizar un número de 1000 dígitos requeriría medir el valor propio de  $U_a$  con una precisión de  $10^{-2000}$ . Dicha precisión no se puede lograr mediante una aplicación directa del algoritmo de estimación de fase, ya que esto requeriría un sistema de puntero demasiado grande. Aquí viene el truco principal: estimaremos el valor propio de  $U_a$  aplicando el algoritmo de estimación de fase a una familia de operadores unitarios  $U_b$  con  $b = a, a^2, a^4, a^8, \dots$ . Nos detendremos en  $b = a^{2^p}$  con  $2^p \approx N^2$ [46].

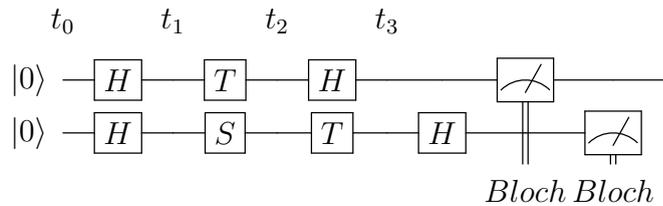
¿Por qué funciona? La primera observación es que todos los operadores  $U_b$  son potencias enteras de  $U_a$ . Sabiendo, si  $b = a^t$  entonces  $U_b = (U_a)^t$ . Esto implica que los operadores  $U_b$  tienen los mismos vectores propios. En particular, los valores propios de la familia  $U_b$  se pueden medir simultáneamente. En segundo lugar, implementar  $U_b$  es tan fácil como implementar  $U_a$ : solo hay que calcular previamente las potencias  $b = a, a^2, a^4, a^8, \dots \pmod{N}$  mediante el método de cuadratura repetida. Finalmente, incluso si los valores propios de  $U_b$  se miden con una precisión pobre (por ejemplo, 10%), cada cuadratura de  $a$  reduce el error en el valor propio estimado de  $U_a$  en un factor  $\frac{1}{2}$ . De hecho, considere un vector propio de  $U_a$  con un valor propio  $e^{2i\gamma}$ . Si  $b = a^2$ , el valor propio de  $U_b$  es  $e^{2i\gamma}$ . Si  $b = a^4$ , entonces el valor propio de  $U_b$  es  $e^{4i\gamma}$ , etc. Por lo tanto, podemos estimar  $\gamma, 2\gamma, 4\gamma, \dots, 2^p\gamma$  con una precisión constante (por ejemplo, 10%). Veremos que esto es suficiente para estimar  $\gamma$  con una precisión de aproximadamente  $2 - p$ . Por ejemplo, uno puede lograr una precisión  $10^{-2000}$  mediante una secuencia de menos de 106 mediciones pésimas de  $U_b$  con un error del 10%. Además, se puede demostrar que la estimación de unos pocos valores propios seleccionados aleatoriamente  $\gamma = 2\pi k/r$  con una precisión inferior a  $\frac{1}{N^2}$  es suficiente para determinar el período  $r$  exactamente (la idea es encontrar la mejor aproximación racional a la estimación de  $\frac{k}{r}$  utilizando fracciones continuas)[46].

Para utilizar el algoritmo de estimación de fase necesitamos construir un circuito cuántico implementando el operador de multiplicación modular. Por analogía con los algoritmos clásicos que pueden vincular funciones de biblioteca estándar, un algoritmo cuántico puede llamar subrutinas clásicas, por ejemplo una subrutina para calcular la multiplicación modular. Es importante destacar que, antes de que

dichas subrutinas clásicas se incorporen a un circuito cuántico, deben transformarse en una forma reversible. Más precisamente, un algoritmo cuántico puede llamar una subrutina clásica solo si se compila en una secuencia de puertas lógicas reversibles como compuerta **CNOT** o **Toffoli** (en particular, el número de cables de entrada y salida en cada puerta debe ser el mismo). Se permite que la subrutina utilice una memoria virtual similar a las variables locales utilizadas por las funciones de biblioteca estándar. Sin embargo, una vez que se completa la subrutina, la memoria virtual debe estar totalmente limpia (por ejemplo, todos los ceros). La razón es que un algoritmo cuántico opera sobre superposiciones coherentes de diferentes estados clásicos. Dejar información sobre las entradas o las salidas en la memoria virtual podría potencialmente destruir la coherencia cuántica y evitar que el algoritmo vea interferencias entre diferentes estados[46].

### 5.2.0.1. Ejemplos de Circuitos Cuánticos Propuestos por IBM

En este caso IBM hace énfasis en el ejemplo de estimación de fase por medio del siguiente circuito cuántico. No obstante, la diferencia radica ahora en el último operador utilizado en el algoritmo, que en realidad es la medición del qubit individualmente sobre la esfera de Bloch. La descripción matemática de estos ejemplos se encuentra en el apéndice (C).



**Circuito cuántico propuesto por IBM** (<https://goo.gl/ppzrjR>)

La aplicación de este algoritmo consiste en la obtención de diferentes estados de superposición para los dos qubits utilizados, con el fin de simular el proceso de factorización en diferentes alternativas con ayuda de la computación cuántica. A continuación en la figura (5.3), se muestra el resultado obtenido en la esfera de Bloch para cada qubit.

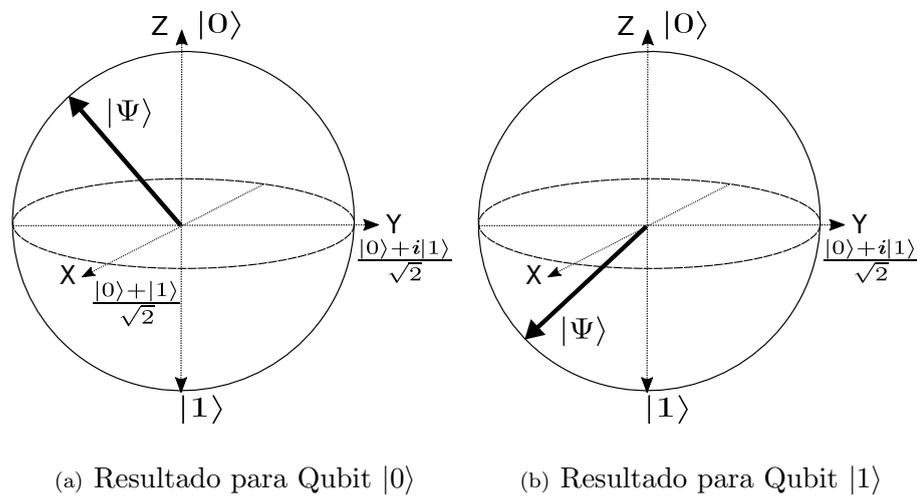
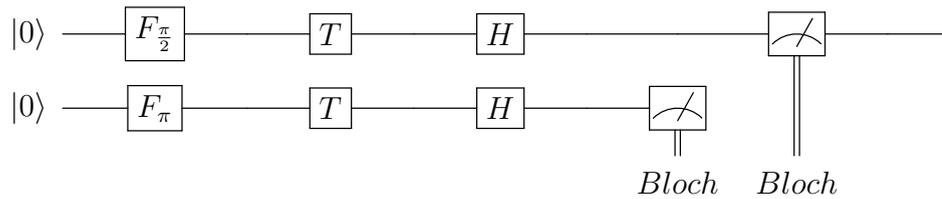


FIGURA 5.3: Resultado del Circuito mostrado por Qubit.

**5.2.0.2. Circuitos Cuánticos Propuestos por IBM usando la compuerta cuántica  $\mathcal{F}_\alpha$**

En este caso es la nueva compuerta  $\mathcal{F}_\alpha$  al circuito cuántico descrito anteriormente, ya que es posible visualizar tanto la aplicación de la reducción de compuertas cuánticas estándar por medio de un orden fraccionario definido, así como también la generalización de la Tff al reemplazar la compuerta Hadamard. La descripción matemática de estos ejemplos se encuentra en el apéndice (C).



**Aplicación de  $F_\alpha$  al circuito cuántico propuesto por IBM**

Nuevamente ha sido demostrado la reducción de complejidad algorítmica en este ejemplo, debido a que el número de compuertas cuánticas han sido reducidas gracias al grado de libertad adicional brindado por el orden fraccionario de la nueva compuerta cuántica. El resultado de esta algoritmo sigue siendo el mismo como se muestra en la figura (5.4), obteniendo diferentes estados de superposición para cada qubit, y así demostrando la efectividad de la computación cuántica en algoritmos complejos.

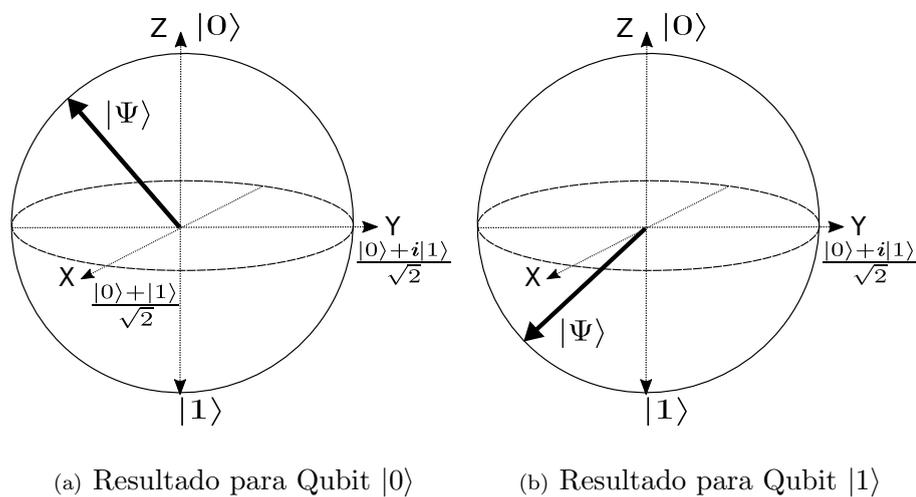


FIGURA 5.4: Resultado del Circuito mostrado por Qubit.

# Capítulo 6

## Conclusiones

Se presenta a continuación los resultados obtenidos en este trabajo, incluyendo los resultados teóricos en materia de la computación cuántica. Se mencionan los que a criterio del autor son considerados los resultados más originales del trabajo:

- Se obtuvo una nueva versión de la transformación de Fourier fraccionaria discreta a partir de la transformación continua propuesta por Namias, utilizando el teorema del muestreo definido por R. Torres junto con el soporte de la función definido en este trabajo.
- Se encontró una nueva compuerta cuántica a partir de la transformación de Fourier fraccionaria cuántica obtenida en este trabajo.
- Se halló la generalización de la compuerta Hadamard en la computación cuántica aplicando la nueva compuerta cuántica.
- Se obtuvo un grado de libertad adicional (estados superpuestos fuera del eje) en la rotación del qubit usando la nueva compuerta cuántica obtenida.
- Se aplicó la nueva compuerta cuántica obtenida en el mejoramiento de la complejidad del algoritmo cuántico: Algoritmo de Grover.
- Se encontró que la nueva compuerta cuántica permite obtener estados entrelazados (entanglement).
- Se analizó la aplicación de la nueva compuerta cuántica en algunos algoritmos cuánticos propuestos en la teoría, encontrando gran adaptabilidad y en algunos casos mejoras a dichos algoritmos gracias al orden fraccionario obtenido con la nueva compuerta cuántica.

- Se reprodujo cada uno de los resultados en un simulador de computador cuántico ofrecido por IBM Experience.

La computación cuántica es, ante muchos investigadores, un tema de estudio completamente nuevo. La importancia de este trabajo radica en la complementación de las teorías referentes al campo de investigación, así como la apropiación de los conceptos para llevar a cabo la aplicabilidad de la nueva compuerta en los diferentes aspectos estudiados. El hecho de poder encontrar nuevos estados de superposición del qubit, así como la reducción de operaciones dentro de un algoritmo cuántico, y por ende la reducción de la complejidad algorítmica determina un avance significativo en la investigación, dado que genera un foco hacia la nueva era de la computación.

# Apéndice A

## Analogía Transformación de Fourier Estándar

### A.1. Transformación de Fourier Estándar Discreta

Partiendo de la transformación de Fourier continua estándar :

$$F^{\frac{\pi}{2}} f(x') = \int_{\mathbf{R}} f(x) e^{-2i\pi x x'} dx, \quad (\text{A.1})$$

y usando un cambio de variable adecuado

$$x = n\Delta_x, \quad x' = k\Delta_{x'}, \quad (\text{A.2})$$

entonces, si delimitamos el rango de muestreo al intervalo  $0 < n < N - 1$ , donde  $N$  es el número de muestras en la función, tenemos

$$F^{\frac{\pi}{2}} f(k) = \sum_{n=0}^{N-1} f(n\Delta_x) e^{i2\pi\Delta_x\Delta_{x'}nk}, \quad (\text{A.3})$$

donde las ratas de muestreos usadas corresponden al teorema de muestreo de Nyquist,

$$\Delta_x = \frac{1}{\zeta}, \quad \Delta_{x'} = \frac{1}{\xi} \quad (\text{A.4})$$

usando el soporte de la función propuesto por Nyquist  $\xi = \zeta = \sqrt{N}$ , en la ecuación (A.3) se obtiene la transformada de Fourier discreta (TFD)

$$F_{\frac{\pi}{2}} f(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{\frac{i2\pi kn}{N}} f(n). \quad (\text{A.5})$$

Este operador puede ser escrito como una matriz transformación usando la expresión  $F(k) = Wf(n)$ , donde  $W$  es la matriz cuadrada  $N - \text{por} - N$  de la transformada de Fourier discreta, conocida como matriz Vandermonde [48]. La matriz transformación  $W$  puede ser definida como  $W = \left(\frac{\omega^{kn}}{\sqrt{N}}\right)$  donde  $\omega = e^{\frac{2\pi i}{N}}$  y  $k, n = 0, \dots, N - 1$

$$W = \frac{1}{\sqrt{N}} \begin{bmatrix} \omega^{00} & \omega^{01} & \dots & \omega^{0(N-1)} \\ \omega^{10} & \omega^{11} & \dots & \omega^{1(N-1)} \\ \omega^{20} & \omega^{21} & \dots & \omega^{2(N-1)} \\ \dots & \dots & \dots & \dots \\ \omega^{(N-1)0} & \omega^{(N-1)1} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix}, \quad (\text{A.6})$$

donde para un caso específico de  $N=2$  la ecuación (A.6) queda descompuesta como:

$$\begin{aligned} F(0) &= \frac{1}{\sqrt{2}}(f(0) + f(1)), \\ F(1) &= \frac{1}{\sqrt{2}}(f(0) + f(1)e^{i\pi}). \end{aligned} \quad (\text{A.7})$$

Teniendo en cuenta que  $\exp(-i\pi) = (-1)$ , y tomando la forma de la ecuación (A.6) de manera matricial daría:

$$\begin{bmatrix} F(0) \\ F(1) \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} f(0) \\ f(1) \end{bmatrix}. \quad (\text{A.8})$$

Se observa que la transformada de Fourier es igual al producto de la matriz  $\mathbf{W}$  con un vector con la evaluación de los valores en la función inicial.

## A.2. Transformación de Fourier Cuántica

En el caso cuántico, la ecuación (A.5) puede ser vista como:

$$TFC : |k\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{\frac{i2\pi kn}{N}} |n\rangle, \quad (\text{A.9})$$

donde  $|k\rangle$  es un estado base, y tomando en consideración  $N := 2^q$  y  $\omega = e^{\frac{2\pi i}{2^q}}$  para  $q$  qubits, la TFC es escrita como

$$W = \frac{1}{\sqrt{2^q}} \begin{bmatrix} \omega^{00} & \omega^{01} & \dots & \omega^{0(N-1)} \\ \omega^{10} & \omega^{11} & \dots & \omega^{1(N-1)} \\ \omega^{20} & \omega^{21} & \dots & \omega^{2(N-1)} \\ \dots & \dots & \dots & \dots \\ \omega^{(N-1)0} & \omega^{(N-1)1} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix}; \quad (\text{A.10})$$

para el caso de 1 qubit,  $N = 2^1 = 2$  se obtiene la matriz  $\mathbf{W}$  mostrada en la ecuación (A.8) que es conocida en computación cuántica como la compuerta Hadamard  $\mathbf{H}$ ,

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (\text{A.11})$$

Dicho esto, se puede demostrar que la compuerta  $\mathbf{H}$  es un operador unitario:

$$\mathbf{H}\mathbf{H}^* = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}_n$$

Ahora, se supone se tiene el estado del qubit simple  $a_0 |0\rangle + a_1 |1\rangle$ . Si se aplica la operación Hadamard a este estado se obtiene el nuevo estado:

$$\frac{1}{\sqrt{2}}(a_0 + a_1) |0\rangle + \frac{1}{\sqrt{2}}(a_0 - a_1) |1\rangle = \bar{a} |0\rangle + \bar{b} |1\rangle \quad (\text{A.12})$$

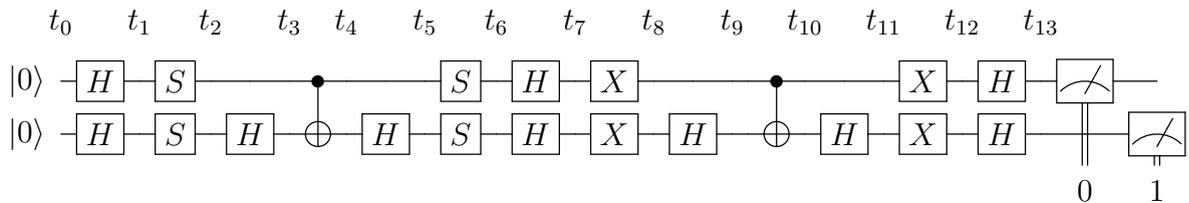
# Apéndice B

## Algoritmo de Grover

En el capítulo 5 (Figura 5.2), fue abordada la descripción teórica del algoritmo de Grover, presentado como una promesa de la computación cuántica. Por medio de este apéndice se establece la descripción matemática detallada del comportamiento de los sistemas en cada ejemplo propuesto por IBM Experience para el algoritmo de Grover, para así aportar una más alta comprensión al lector del procesamiento de los circuitos cuánticos presentados.

### B.1. Ejemplos propuestos por IBM Experience

#### B.1.1. Primer Ejemplo con objetivo en el estado final $|00\rangle$



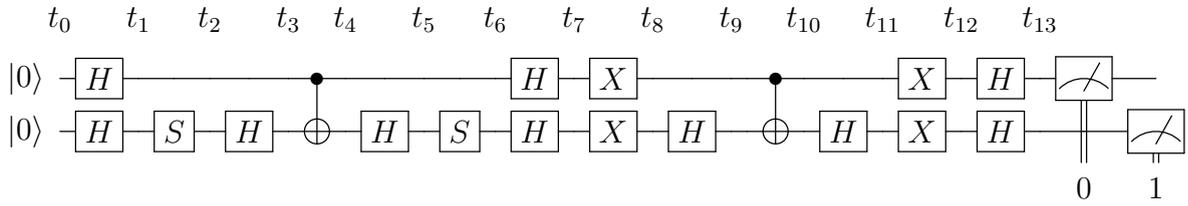
$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{H} \otimes \mathbf{H}) |00\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{aligned}
 t_2 &= (\mathbf{S} \otimes \mathbf{S})t_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ i \\ -1 \end{bmatrix} \\
 t_3 &= (\mathbf{I} \otimes \mathbf{H})t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ i \\ i \\ -1 \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ -1+i \\ 1+i \end{bmatrix} \\
 t_4 &= (\mathbf{CNOT})t_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ -1+i \\ 1+i \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1+i \\ -1+i \end{bmatrix} \\
 t_5 &= (\mathbf{I} \otimes \mathbf{H})t_4 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1+i \\ -1+i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ i \\ 1 \end{bmatrix} \\
 t_6 &= (\mathbf{S} \otimes \mathbf{S})t_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ i \\ i \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \\
 t_7 &= (\mathbf{H} \otimes \mathbf{H})t_6 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\
 t_8 &= (\mathbf{X} \otimes \mathbf{X})t_7 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
 t_9 &= (\mathbf{I} \otimes \mathbf{H})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \\
 t_{10} &= (\mathbf{CNOT})t_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}
 \end{aligned}$$

$$\begin{aligned}
 t_{11} &= (\mathbf{I} \otimes \mathbf{H})t_{10} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\
 t_{12} &= (\mathbf{X} \otimes \mathbf{X})t_{11} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\
 t_{13} &= (\mathbf{H} \otimes \mathbf{H})t_{12} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle
 \end{aligned}$$

**B.1.2. Segundo Ejemplo con objetivo en el estado final  $|01\rangle$**



$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

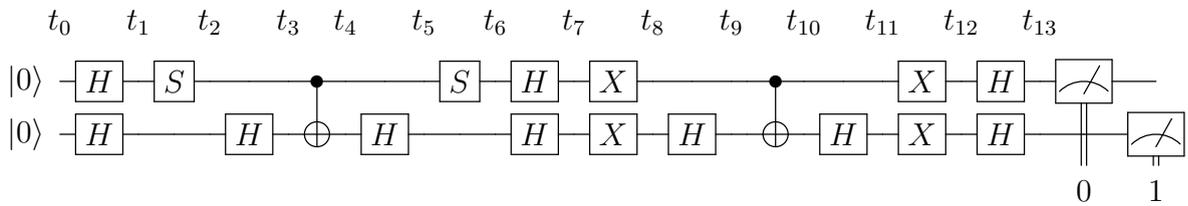
$$t_1 = (\mathbf{H} \otimes \mathbf{H}) |00\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$t_2 = (\mathbf{I} \otimes \mathbf{S})t_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ 1 \\ i \end{bmatrix}$$

$$\begin{aligned}
 t_3 &= (\mathbf{I} \otimes \mathbf{H})t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ i \\ 1 \\ i \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1+i \\ 1-i \end{bmatrix} \\
 t_4 &= (\mathbf{CNOT})t_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1+i \\ 1-i \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1-i \\ 1+i \end{bmatrix} \\
 t_5 &= (\mathbf{I} \otimes \mathbf{H})t_4 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1-i \\ 1+i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ 1 \\ -i \end{bmatrix} \\
 t_6 &= (\mathbf{I} \otimes \mathbf{S})t_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ i \\ 1 \\ -i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \\
 t_7 &= (\mathbf{H} \otimes \mathbf{H})t_6 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \\
 t_8 &= (\mathbf{X} \otimes \mathbf{X})t_7 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \\
 t_9 &= (\mathbf{I} \otimes \mathbf{H})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \\
 t_{10} &= (\mathbf{CNOT})t_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}
 \end{aligned}$$

$$\begin{aligned}
 t_{11} &= (\mathbf{I} \otimes \mathbf{H})t_{10} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \\
 t_{12} &= (\mathbf{X} \otimes \mathbf{X})t_{11} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \\
 t_{13} &= (\mathbf{H} \otimes \mathbf{H})t_{12} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix} = -|01\rangle
 \end{aligned}$$

### B.1.3. Tercer Ejemplo con objetivo en el estado final $|10\rangle$



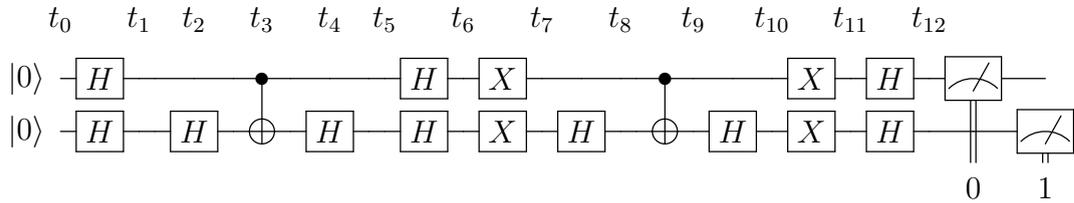
$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{H} \otimes \mathbf{H})|00\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{aligned}
 t_2 &= (\mathbf{S} \otimes \mathbf{I})t = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ i \\ i \end{bmatrix} \\
 t_3 &= (\mathbf{I} \otimes \mathbf{H})t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ i \\ i \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ i \\ 0 \end{bmatrix} \\
 t_4 &= (\mathbf{CNOT})t_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ i \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ i \end{bmatrix} \\
 t_5 &= (\mathbf{I} \otimes \mathbf{H})t_4 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ i \\ -i \end{bmatrix} \\
 t_6 &= (\mathbf{S} \otimes \mathbf{I})t_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ i \\ -i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \\
 t_7 &= (\mathbf{H} \otimes \mathbf{H})t_6 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \\
 t_8 &= (\mathbf{X} \otimes \mathbf{X})t_7 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \\
 t_9 &= (\mathbf{I} \otimes \mathbf{H})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} \\
 t_{10} &= (\mathbf{CNOT})t_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}
 \end{aligned}$$

$$\begin{aligned}
 t_{11} &= (\mathbf{I} \otimes \mathbf{H})t_{10} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \\
 t_{12} &= (\mathbf{X} \otimes \mathbf{X})t_{11} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \\
 t_{13} &= (\mathbf{H} \otimes \mathbf{H})t_{12} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} = -|10\rangle
 \end{aligned}$$

**B.1.4. Cuarto Ejemplo con objetivo en el estado final  $|11\rangle$**



$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{H} \otimes \mathbf{H})|00\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

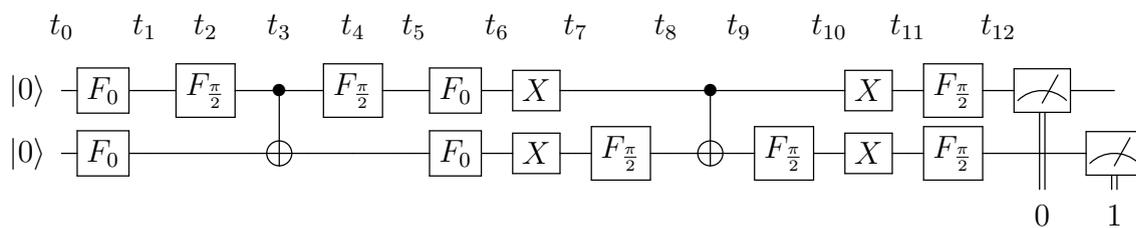
$$t_2 = (\mathbf{I} \otimes \mathbf{H})t_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{aligned}
 t_3 &= (\mathbf{CNOT})t_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \\
 t_4 &= (\mathbf{I} \otimes \mathbf{H})t_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
 t_5 &= (\mathbf{H} \otimes \mathbf{H})t_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
 t_6 &= (\mathbf{X} \otimes \mathbf{X})t_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\
 t_7 &= (\mathbf{I} \otimes \mathbf{H})t_6 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \end{bmatrix} \\
 t_8 &= (\mathbf{CNOT})t_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \end{bmatrix} \\
 t_9 &= (\mathbf{I} \otimes \mathbf{H})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
 t_{10} &= (\mathbf{X} \otimes \mathbf{X})t_9 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
 t_{11} &= (\mathbf{H} \otimes \mathbf{H})t_{10} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} = -|11\rangle
 \end{aligned}$$

## B.2. Aplicación de la compuerta $\mathcal{F}_\alpha$

Ahora, es presentanda la descripción matemática del procesamiento de los circuitos cuánticos propuestos por IBM Experience para el algoritmo de Grover usando la compuerta  $F_\alpha$  obtenida en el trabajo, en los cuales es notable la reducción del número de procesos ejecutados a comparación de los circuitos anteriores.

### B.2.1. Primer Ejemplo con objetivo en el estado final $|00\rangle$



$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{F}_0 \otimes \mathbf{F}_0)t_0 = \frac{1}{2} \begin{bmatrix} i & 1 & 1 & -i \\ 1 & i & -i & 1 \\ 1 & -i & i & 1 \\ -i & 1 & 1 & i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} i \\ 1 \\ 1 \\ -i \end{bmatrix}$$

$$t_2 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} i \\ 1 \\ 1 \\ -i \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ -1+i \\ 1+i \end{bmatrix}$$

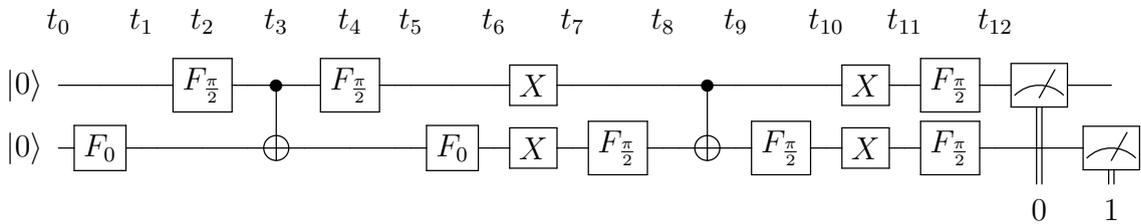
$$t_3 = (\mathbf{CNOT})t_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ -1+i \\ 1+i \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1+i \\ -1+i \end{bmatrix}$$

$$t_4 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1}{2\sqrt{2}} \begin{bmatrix} 1+i \\ 1-i \\ 1+i \\ -1+i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+i \\ 0 \\ 0 \\ 1-i \end{bmatrix}$$

$$t_5 = (\mathbf{F}_0 \otimes \mathbf{F}_0)t_4 = \frac{1}{2} \begin{bmatrix} i & 1 & 1 & -i \\ 1 & i & -i & 1 \\ 1 & -i & i & 1 \\ -i & 1 & 1 & i \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1+i \\ 0 \\ 0 \\ 1-i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{aligned}
 t_6 &= (\mathbf{X} \otimes \mathbf{X})t_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
 t_7 &= (\mathbf{I} \otimes \mathbf{F}_{\frac{\pi}{2}})t_6 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \\
 t_8 &= (\mathbf{CNOT})t_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \\
 t_9 &= (\mathbf{I} \otimes \mathbf{F}_{\frac{\pi}{2}})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\
 t_{10} &= (\mathbf{X} \otimes \mathbf{X})t_9 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\
 t_{11} &= (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{F}_{\frac{\pi}{2}})t_{10} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle
 \end{aligned}$$

**B.2.2. Segundo Ejemplo con objetivo en el estado final  $|01\rangle$**



$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{I} \otimes \mathbf{F}_0)t_0 = \frac{1+i}{2} \begin{bmatrix} 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1+i}{2} \begin{bmatrix} 1 \\ -i \\ 0 \\ 0 \end{bmatrix}$$

$$t_2 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1+i}{2} \begin{bmatrix} 1 \\ -i \\ 0 \\ 0 \end{bmatrix} = \frac{1+i}{2\sqrt{2}} \begin{bmatrix} 1 \\ -i \\ 1 \\ -i \end{bmatrix}$$

$$t_3 = (\mathbf{CNOT})t_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1+i}{2\sqrt{2}} \begin{bmatrix} 1 \\ -i \\ 1 \\ -i \end{bmatrix} = \frac{1+i}{2\sqrt{2}} \begin{bmatrix} 1 \\ -i \\ -i \\ 1 \end{bmatrix}$$

$$t_4 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1+i}{2\sqrt{2}} \begin{bmatrix} 1 \\ -i \\ -i \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ i \\ -i \end{bmatrix}$$

$$t_5 = (\mathbf{I} \otimes \mathbf{F}_0)t_4 = \frac{1+i}{2} \begin{bmatrix} 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ i \\ -i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$$

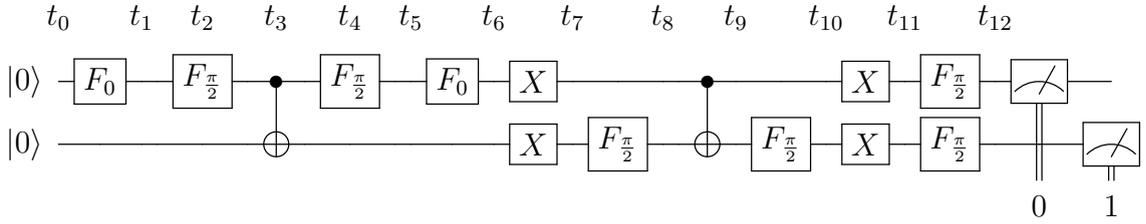
$$t_6 = (\mathbf{X} \otimes \mathbf{X})t_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix}$$

$$t_7 = (\mathbf{I} \otimes \mathbf{F}_{\frac{\pi}{2}})t_6 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$t_8 = (\mathbf{CNOT})t_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{aligned}
 t_9 &= (\mathbf{I} \otimes \mathbf{F}_{\frac{\pi}{2}})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \\
 t_{10} &= (\mathbf{X} \otimes \mathbf{X})t_9 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \\
 t_{11} &= (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{F}_{\frac{\pi}{2}})t_{10} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix} = -|01\rangle
 \end{aligned}$$

### B.2.3. Tercer Ejemplo con objetivo en el estado final $|10\rangle$



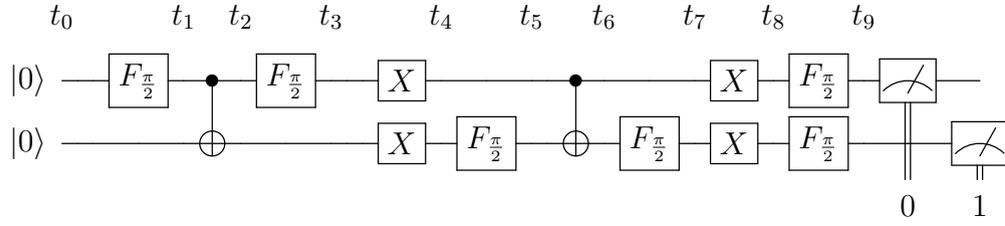
$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{F}_0 \otimes \mathbf{I})t_0 = \frac{1+i}{2} \begin{bmatrix} 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i \\ -i & 0 & 1 & 0 \\ 0 & -i & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1+i}{2} \begin{bmatrix} 1 \\ 0 \\ -i \\ 0 \end{bmatrix}$$

$$t_2 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1+i}{2} \begin{bmatrix} 1 \\ 0 \\ -i \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ i \\ 0 \end{bmatrix}$$

$$\begin{aligned}
 t_3 &= (\mathbf{CNOT})t_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ i \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ i \end{bmatrix} \\
 t_4 &= (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ 1 \\ -i \end{bmatrix} \\
 t_5 &= (\mathbf{F}_0 \otimes \mathbf{I})t_4 = \frac{1+i}{2} \begin{bmatrix} 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i \\ -i & 0 & 1 & 0 \\ 0 & -i & 0 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ i \\ 1 \\ -i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \\
 t_6 &= (\mathbf{X} \otimes \mathbf{X})t_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \\
 t_7 &= (\mathbf{I} \otimes \mathbf{F}_{\frac{\pi}{2}})t_6 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} \\
 t_8 &= (\mathbf{CNOT})t_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} \\
 t_9 &= (\mathbf{I} \otimes \mathbf{F}_{\frac{\pi}{2}})t_8 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \\
 t_{10} &= (\mathbf{X} \otimes \mathbf{X})t_9 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \\
 t_{11} &= (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{F}_{\frac{\pi}{2}})t_{10} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} = -|10\rangle
 \end{aligned}$$

**B.2.4. Cuarto Ejemplo con objetivo en el estado final  $|11\rangle$**



$$t_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$t_1 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$t_2 = (\mathbf{CNOT})t_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$t_3 = (\mathbf{F}_{\frac{\pi}{2}} \otimes \mathbf{I})t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$$

$$t_4 = (\mathbf{X} \otimes \mathbf{X})t_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$t_5 = (\mathbf{I} \otimes \mathbf{H})t_4 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \end{bmatrix}$$

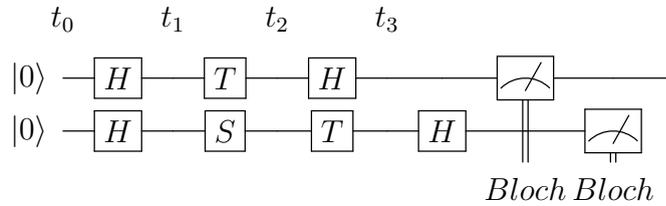
$$\begin{aligned}
t_6 &= (\mathbf{CNOT})t_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \end{bmatrix} \\
t_7 &= (\mathbf{I} \otimes \mathbf{H})t_6 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
t_8 &= (\mathbf{X} \otimes \mathbf{X})t_7 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \\
t_9 &= (\mathbf{H} \otimes \mathbf{H})t_8 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} = -|11\rangle
\end{aligned}$$

# Apéndice C

## Algoritmo de Shor

En este caso se presenta el ejemplo propuesto por IBM Experience para el algoritmo de Shor, el cual hace énfasis en el ejemplo de estimación de fase, mostrando la descripción matemática del procesamiento del circuito cuántico establecido.

### C.1. Ejemplo propuesto por IBM Experience



**Qubit 1**

$$t_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$t_1 = \mathbf{H}|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$t_2 = \mathbf{T}t_1 = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \frac{1+i}{\sqrt{2}} \end{bmatrix}$$

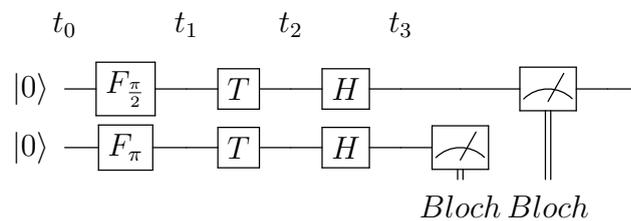
$$t_3 = \mathbf{H}t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \frac{1+i}{\sqrt{2}} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 + \frac{1+i}{\sqrt{2}} \\ 1 - \frac{1+i}{\sqrt{2}} \end{bmatrix}$$

**Qubit 2**

$$\begin{aligned}
 t_0 &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \\
 t_1 &= \mathbf{H}t_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
 t_2 &= \mathbf{S}t_1 = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} \\
 t_3 &= \mathbf{T}t_2 = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \frac{-1+i}{\sqrt{2}} \end{bmatrix} \\
 t_3 &= \mathbf{H}t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \frac{-1+i}{\sqrt{2}} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 + \frac{-1+i}{\sqrt{2}} \\ 1 - \frac{-1+i}{\sqrt{2}} \end{bmatrix}
 \end{aligned}$$

**C.2. Aplicación de la compuerta  $\mathcal{F}_\alpha$**

A continuación se muestra la descripción matemática de la aplicación de la compuerta cuántica  $F_\alpha$  sobre el circuito cuántico del algoritmo de Shor mostrado anteriormente.



**Qubit 1**

$$\begin{aligned}
t_0 &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \\
t_1 &= \mathbf{F}_{\frac{\pi}{2}} |0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
t_2 &= \mathbf{T}t_1 = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \frac{1+i}{\sqrt{2}} \end{bmatrix} \\
t_3 &= \mathbf{F}_{\frac{\pi}{2}} t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \frac{1+i}{\sqrt{2}} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 + \frac{1+i}{\sqrt{2}} \\ 1 - \frac{1+i}{\sqrt{2}} \end{bmatrix}
\end{aligned}$$

## Qubit 2

$$\begin{aligned}
t_0 &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \\
t_1 &= \mathbf{F}_{\pi} t_0 = \frac{1+i}{2} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1+i}{2} \begin{bmatrix} 1 \\ i \end{bmatrix} \\
t_2 &= \mathbf{T}t_1 = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \frac{1+i}{2} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1+i}{2} \begin{bmatrix} 1 \\ \frac{-1+i}{\sqrt{2}} \end{bmatrix} \\
t_3 &= \mathbf{F}_{\frac{\pi}{2}} t_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1+i}{2} \begin{bmatrix} 1 \\ \frac{-1+i}{\sqrt{2}} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 + \frac{1+i}{\sqrt{2}} \\ 1 + \frac{1+i}{\sqrt{2}} \end{bmatrix}
\end{aligned}$$

# Apéndice D

## Anexos

### D.1. Productos Derivados de la Tesis

#### D.1.1. Ponencia The FIO+LS

El trabajo fue presentado por medio de un Poster en la conferencia The FIO+LS desarrollada en la ciudad de Washington-USA, que fue llevada a cabo desde el 16 hasta el 20 de septiembre del 2018.



FIGURA D.1: Certificado de Asistencia

El autor agradece a OSA por el apoyo para poder asistir a la conferencia.

### D.1.2. Ponencia Quantum Optics IX

El trabajo fue presentado por medio de un Poster en la conferencia Quantum Optics IX desarrollada en la ciudad de Cartagena-Colombia, que fue llevada a cabo desde el 21 hasta el 26 de octubre del 2018.



FIGURA D.2: Certificado de Asistencia

El autor agradece al comite organizador por el apoyo para poder asistir a la conferencia.

### D.1.3. Proceedings Publicado en OSA Publishing

El trabajo fue publicado en la revista de OSA Publishing por medio del abstract llevado a la conferencia The FIO+LS.



FIGURA D.3: Publicación

### D.1.4. Artículo Sometido en Physical Review Letter

El trabajo fue sometido a publicación en la revista de Physical Review Letter, donde actuacmente sen cuenta con la aprobación del editor.

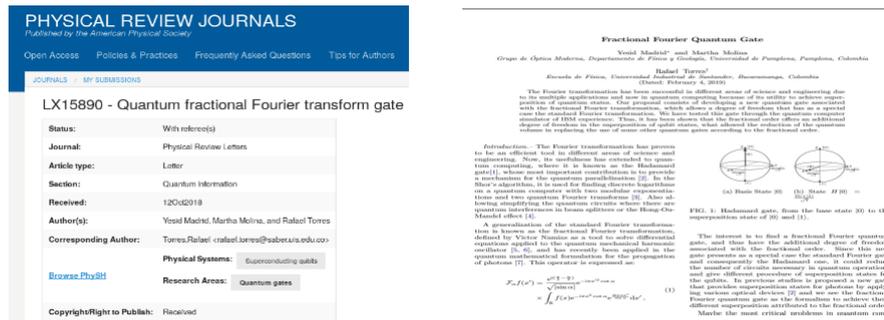


FIGURA D.4: Publicación

### D.1.5. Premio al Autor

Gracias a los resultados obtenidos por el trabajo, el departamento de Ingeniería Elctrica, Electrónica, Sistemas y Telecomunicaciones DEEST otorga al autor un premio como Mejor Docente Investigador durante el año 2018.



FIGURA D.5: Publicación

# Bibliografía

- [1] Joseph Fourier. *Theorie analytique de la chaleur, par M. Fourier*. Chez Firmin Didot, père et fils, 1822.
- [2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2010.
- [3] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A*, 439(1907):553–558, 1992.
- [4] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.
- [5] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994.
- [6] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.
- [7] Victor Namias. The fractional order fourier transform and its application to quantum mechanics. *IMA Journal of Applied Mathematics*, 25(3):241–265, 1980.
- [8] Rafael Torres, Pierre Pellat-Finet, and Yezid Torres. Fractional convolution, fractional correlation and their translation invariance properties. *Signal processing*, 90(6):1976–1984, 2010.
- [9] R Torres, Pierre Pellat-Finet, and Yezid M Torres Moreno. Numerical holography computing by using the fractional fourier transform: a ping-pong-pang algorithm. In *5th Iberoamerican Meeting on Optics and 8th Latin American Meeting on Optics, Lasers, and Their Applications*, volume 5622, pages 1457–1463. International Society for Optics and Photonics, 2004.

- 
- [10] Rafael Torres, Zandra Lizarazo, and Edmanuel Torres. Fractional sampling theorem for alpha-bandlimited random signals and its relation to the von neumann ergodic theorem. *IEEE Trans. Signal Processing*, 62(14):3695–3705, 2014.
- [11] Alberto Patiño-Vanegas, Pierre-Emmanuel Durand, Pierre Pellat-Finet, and Rafael Torres. Diffuser in fractional fourier optics. In *Latin America Optics and Photonics Conference*, pages LTu3A–2. Optical Society of America, 2016.
- [12] Elkin A Santos, Ferney Castro, and Rafael Torres. Huygens-fresnel principle: Analyzing consistency at the photon level. *Physical Review A*, 97(4):043853, 2018.
- [13] AC McBride and FH Kerr. On namias’s fractional fourier transforms. *IMA Journal of applied mathematics*, 39(2):159–175, 1987.
- [14] T Alieva, Vicente Lopez, F Agullo-Lopez, and LB Almeida. The fractional fourier transform in optical propagation problems. *Journal of modern optics*, 41(5):1037–1044, 1994.
- [15] Adolf W Lohmann. Image rotation, wigner rotation, and the fractional fourier transform. *JOSA A*, 10(10):2181–2186, 1993.
- [16] Haldun M Ozaktas and David Mendlovic. Fractional fourier transforms and their optical implementation. ii. *JOSA A*, 10(12):2522–2531, 1993.
- [17] Pierre Pellat-Finet and Georges Bonnet. Fractional order fourier transform and fourier optics. *Optics communications*, 111(1-2):141–154, 1994.
- [18] Pierre Pellat-Finet. Fresnel diffraction and the fractional-order fourier transform. *Optics Letters*, 19(18):1388–1390, 1994.
- [19] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.
- [20] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.
- [21] Agedi N Boto, Pieter Kok, Daniel S Abrams, Samuel L Braunstein, Colin P Williams, and Jonathan P Dowling. Quantum interferometric optical lithography: exploiting entanglement to beat the diffraction limit. *Physical Review Letters*, 85(13):2733, 2000.

- 
- [22] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400(1818):97–117, 1985.
- [23] David P DiVincenzo and Daniel Loss. Quantum information is physical. *Superlattices and Microstructures*, 23(3-4):419–432, 1998.
- [24] David Deutsch. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425(1868):73–90, 1989.
- [25] Mike Stannett. X-machines and the halting problem: Building a super-turing machine. *Formal Aspects of Computing*, 2(1):331–341, 1990.
- [26] EU Condon. Immersion of the fourier transform in a continuous group of functional transformations. *Proceedings of the National Academy of Sciences*, 23(3):158–164, 1937.
- [27] Norbert Wiener. Hermitian polynomials and fourier analysis. *Studies in Applied Mathematics*, 8(1-4):70–73, 1929.
- [28] David H Bailey and Paul N Swarztrauber. The fractional fourier transform and applications. *SIAM review*, 33(3):389–404, 1991.
- [29] Ronald Newbold Bracewell and Ronald N Bracewell. *The Fourier transform and its applications*, volume 31999. McGraw-Hill New York, 1986.
- [30] Athanasios Papoulis and AA Maradudin. The fourier integral and its applications. *Physics Today*, 16:70, 1963.
- [31] Yigal Bitran, Zeev Zalevsky, David Mendlovic, and Rainer G Dorsch. Fractional correlation operation: performance analysis. *Applied optics*, 35(2):297–303, 1996.
- [32] Zeev Zalevsky, David Mendlovic, and John H Caulfield. Fractional correlator with real-time control of the space-invariance property. *Applied optics*, 36(11):2370–2375, 1997.
- [33] David Mendlovic and Haldun M Ozaktas. Fractional fourier transforms and their optical implementation: I. *JOSA A*, 10(9):1875–1881, 1993.
- [34] Marius Nagy and Selim G Akl. Quantum computation and quantum information. *The International Journal of Parallel, Emergent and Distributed Systems*, 21(1):1–59, 2006.

- 
- [35] Andrés Sicard. Algunos elementos introductorios acerca de la computación cuántica. *Memorias VII Encuentro ERM, Universidad de Antioquia, Medellín, agosto, 23, 1999.*
- [36] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.
- [37] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.
- [38] John S Bell. On the problem of hidden variables in quantum mechanics. In *John S Bell On The Foundations Of Quantum Mechanics*, pages 1–6. World Scientific, 2001.
- [39] Colin Jack. Sherlock holmes investigates the epr paradox. *Physics World*, 8(4):39, 1995.
- [40] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Physical review letters*, 49(25):1804, 1982.
- [41] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell's theorem. *Physical review letters*, 47(7):460, 1981.
- [42] Alain Aspect. Testing bell's inequalities. *Europhysics News*, 22(4):73–75, 1991.
- [43] Henry O. Kunz. On the equivalence between one-dimensional discrete walsh-hadamard and multidimensional discrete fourier transforms. *IEEE Transactions on Computers*, (3):267–268, 1979.
- [44] C Vu. Ibm makes quantum computing available on ibm cloud to accelerate innovation. *IBM News Room*, 2016.
- [45] Antonio D Córcoles, Easwar Magesan, Srikanth J Srinivasan, Andrew W Cross, Matthias Steffen, Jay M Gambetta, and Jerry M Chow. Demonstration of a quantum error detection code using a square lattice of four superconducting qubits. *Nature communications*, 6:6979, 2015.
- [46] HE Caicedo-Ortiz, E Santiago-Cortés, and DA Mantilla-Sandoval. Construyendo compuertas cu anticlas con ibm's cloud quantum computer. *Journal de Ciencia e Ingeniería*, 9(1):42–56, 2017.

- 
- [47] Rafael Torres, Pierre Pellat-Finet, and Yezid Torres. Sampling theorem for fractional bandlimited signals: A self-contained proof. application to digital holography. *IEEE Signal Processing Letters*, 13(11):676–679, 2006.
- [48] Ake Björck and Victor Pereyra. Solution of vandermonde systems of equations. *Mathematics of Computation*, 24(112):893–903, 1970.