Universidad de San Carlos de Guatemala
Escuela de Ciencias Físicas y Matemáticas
Departamento de Física

IMPLEMENTACIÓN DE COMPUERTAS CUÁNTICAS USANDO ÓPTICA CUÁNTICA

Eduardo Alberto Bardales España
Asesorado por Dr. Giovanni Ramírez García

Guatemala, julio de 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICAS

IMPLEMENTACIÓN DE COMPUERTAS CUÁNTICAS USANDO ÓPTICA CUÁNTICA

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JEFATURA DEL
DEPARTAMENTO DE FÍSICA
POR

EDUARDO ALBERTO BARDALES ESPAÑA
ASESORADO POR DR. GIOVANNI RAMÍREZ GARCÍA

AL CONFERÍRSELE EL TÍTULO DE
LICENCIADO EN FÍSICA APLICADA

GUATEMALA, JULIO DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICAS

CONSEJO DIRECTIVO

DIRECTOR	M.Sc. Jorge Marcelo Ixquiac Cabrera
SECRETARIO ACADÉMICO	M.Sc. Edgar Anibal Cifuentes Anléu

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

EXAMINADOR	Ph.D. María Eugenia Cabrera
EXAMINADOR	Ph.D. Ángel Giovanni Ramírez
EXAMINADOR	M.Sc. Juan Diego Chang

ÍNDICE GENERAL

ÍNDICE DE FIGURAS III

ÍNDICE DE TABLAS V

LISTA DE SÍMBOLOS VII

OBJETIVOS IX

INTRODUCCIÓN XI

1. COMPUTACIÓN CUÁNTICA Y CONJUNTO UNIVERSAL DE COMPUERTAS CUÁNTICAS 1

1.1. Introducción . . . 1
1.1.1. El qubit . . . 1
1.1.2. Generalidades de las computadoras cuánticas . . . 4
1.2. Compuertas cuánticas . . . 6
1.2.1. Compuertas de un qubit . . . 7
1.2.2. Compuertas de dos qubits . . . 10
1.3. Conjuntos universales de compuertas . . . 14
1.4. Algoritmos . . . 20
1.4.1. Evaluación de funciones . . . 20
1.4.2. El sumador cuántico . . . 23
1.4.3. Algoritmo de Deutsch y algoritmo de Deutsch-Jozsa . . . 26
1.4.4. Transformada de Fourier cuántica . . . 29
1.5. Aplicaciones . . . 32
1.5.1. Búsqueda cuántica: Algoritmo de Grover . . . 32
1.5.1.1. Ejemplo: búsqueda entre 4 elementos . . . 36
1.5.1.2. El oráculo . . . 38
1.5.2. El algoritmo de Shor . . . 38
1.5.2.1. El período de una función . . . 40

1.5.2.2. Máximo común divisor: el algoritmo de Euclides 42
1.5.3. Complejidad computacional 43
1.5.4. Errores cuánticos y su corrección 45
1.5.4.1. Errores unitarios 45
1.5.4.2. Código de tres qubits para inversión del bit 47
1.5.4.3. Código de tres qubits para inversión de fase 48
1.5.4.4. Código de nueve qubits de Shor 49

2. ÓPTICA CUÁNTICA 55
2.1. Introducción 55
2.2. Diferencia entre óptica clásica y cuántica 56
2.3. Cuantización escalar del campo electromagnético 57
2.4. Efectos cuánticos de la luz 63
2.4.1. Fluctuaciones cuánticas de un campo de modo único 63
2.4.2. Operadores de cuadratura 65
2.4.3. Estados coherentes 66
2.5. Aplicaciones 74
2.5.1. Divisores de haz 74
2.5.2. Interacción Kerr 80
2.5.3. Computación cuántica 84

3. IMPLEMENTACIÓN DE COMPUERTAS CUÁNTICAS EN ÓPTICA CUÁNTICA 87
3.1. Introducción 87
3.2. Implementaciones 89
3.2.1. Compuertas de un qubit 89
3.2.1.1. Compuerta NOT 89
3.2.1.2. Desplazador de fase 90
3.2.1.3. Compuerta de Hadamard 91
3.2.1.4. Compuerta σ_y 92
3.2.1.5. Compuerta $R_y(\theta)$ 92
3.2.1.6. Compuerta $R_x(\theta)$ 93
3.2.2. Compuertas de dos qubits 94
3.2.2.1. Compuerta CPHASE 94
3.2.2.2. Compuerta CNOT 95
3.2.2.3. Compuertas CNOT generalizadas 95
3.2.2.4. Compuerta SWAP 96

3.2.2.5. Compuerta C-U 96
3.2.3. Compuertas de múltiples qubits 99
3.2.3.1. Compuerta de Tiffoli 99
3.2.3.2. Compuerta C^3-U 99
3.2.4. Algoritmos 99
3.2.4.1. Sumador cuántico 102
3.2.4.2. Algoritmo de Deutsch 102
3.2.4.3. Transformada de Fourier cuántica 104
3.2.4.4. Algoritmo de Grover: ejemplo 106
3.2.4.5. Algoritmo de Shor: ejemplo 106
3.2.5. Materiales 107
3.3. Manejo de error 110
3.3.1. Incertezas de procesos computacionales 110
3.3.2. Transmisión por canales ruidosos 113

CONCLUSIONES **117**

TRABAJO A FUTURO Y RECOMENDACIONES **119**

BIBLIOGRAFÍA **121**

ÍNDICE DE FIGURAS

1.1. Esfera de Bloch 2
1.2. Diagrama de circuito para un qubit 6
1.3. Diagrama de circuito para n qubits 7
1.4. Diagrama de circuito para compuertas lógicas cuánticas 7
1.5. Diagrama de circuito para compuerta **NOT** 7
1.6. Diagrama de circuito para compuerta σ_y 8
1.7. Diagrama de circuito para compuerta **CNOT** 10
1.8. Diagrama de circuito para base de Bell 11
1.9. Diagrama de circuito para compuertas **CNOT** generalizadas 11
1.10. Diagrama de circuito para compuerta **CNOT** invertida 12
1.11. Diagrama de circuito para compuerta **CPHASE** 13
1.12. Diagrama de circuito para compuerta **C-U** 14
1.13. Diagrama de circuito para compuerta de Tiffoli 15
1.14. Diagrama de circuito para compuerta C^k**-U** 16
1.15. Diagrama de circuito para compuerta C^2**-U** 17
1.16. Diagrama de circuito para código de Gray 18
1.17. Diagrama de circuito para compuerta **CNOT** negada 19
1.18. Diagrama de circuito para evaluación de función ejemplo 21
1.19. Diagrama de circuito para evaluación de función cuadrática 22
1.20. Diagrama de circuito para suma cuántica 24
1.21. Diagrama de circuito para acarreo de suma cuántica 25
1.22. Diagrama de circuito para sumador cuántico 25
1.23. Diagrama de circuito para algoritmo de Deutsch 27
1.24. Diagrama de circuito para transformada de Fourier cuántica 31
1.25. Visualización geométrica de la iteración de Grover 34
1.26. Diagrama de circuito para iteración de Grover 36
1.27. Diagrama de circuito para algoritmo de Grover $N = 4$ 37
1.28. Diagrama de circuito para período de una función 41

1.29. Diagrama de circuito contra inversión del qubit 47
1.30. Diagrama de circuito para síndrome de error 48
1.31. Diagrama de circuito para corregir inversión del qubit 49
1.32. Diagrama de circuito de código de Shor 51
1.33. Diagrama de circuito de de síndrome de error código de Shor 52

2.1. Cavidad unidimensional 57
2.2. Incertidumbre del vacío 70
2.3. Incertidumbre de estados coherentes 71
2.4. Divisor de haz 74
2.5. Interferómetro de Mach-Zehnder 79
2.6. Interferómetro de Mach-Zehnder acoplado a un medio Kerr 83

3.1. Representación de doble riel 88
3.2. Compuerta **NOT** 90
3.3. Compuerta **PHASE** 90
3.4. Compuerta de Hadamard 91
3.5. Compuerta σ_y 92
3.6. Compuerta $R_y(\theta)$ 92
3.7. Compuerta $R_x(\theta)$ 93
3.8. Compuerta **CPHASE** 94
3.9. Compuerta **CNOT** 96
3.10. Compuerta **CNOT** negada 97
3.11. Compuerta **CNOT** invertida 97
3.12. Compuerta **SWAP** 97
3.13. Compuerta **C-U**, parte 1 98
3.14. Compuerta **C-U**, parte 2 98
3.15. Compuerta de Tiffoli, parte 1 99
3.16. Compuerta de Tiffoli, parte 2 100
3.17. Compuerta C^3**-U**, parte 1 100
3.18. Compuerta C^3**-U**, parte 2 101
3.19. Compuerta C^3**-U**, parte 3 101
3.20. Compuerta C^3**-U**, parte 4 102
3.21. **S** del sumador cuántico 103
3.22. **C** del sumador cuántico, parte 1 103
3.23. **C** del sumador cuántico, parte 2 104
3.24. Algoritmo de Deutsch 104

3.25. Transformada de Fourier cuántica, parte 1 105
3.26. Transformada de Fourier cuántica, parte 2 105
3.27. Transformada de Fourier cuántica, parte 3 106
3.28. Algoritmo de Grover para $N = 4$ 107
3.29. Algoritmo de Shor, parte 1 108
3.30. Algoritmo de Shor, parte 2 108
3.31. Algoritmo de Shor, parte 3 109
3.32. Construcción de divisor de haz 109
3.33. Código de tres qubits para inversión del bit, parte 1 113
3.34. Código de tres qubits para inversión del bit, parte 2 114
3.35. Código de tres qubits para inversión del bit, parte 3 114
3.36. Código de tres qubits para inversión del bit, parte 4 115
3.37. Código de tres qubits para inversión de fase 115

ÍNDICE DE TABLAS

1.1. Ejemplo de función binaria 21
1.2. Función cuadrática 22
1.3. Suma y acarreo 24

LISTA DE SÍMBOLOS

Símbolo	Significado
$\delta(x - x_0)$	medida de Dirac, función δ de Dirac o δ-función
δ_{ij}	delta de Kronecker
$\|\psi\rangle$	vector *ket*, notación de Dirac
$\langle\psi\|$	funcional *bra*, notación de Dirac
$\langle\varphi\|\psi\rangle$	*braket*, producto interno en notación de Dirac
σ_μ	elemento del grupo de Pauli
$A \otimes B$	producto tensorial
$a \oplus b$	suma módulo 2, residuo de $(a + b)/2$
$O(f(n))$	crecimiento de orden $f(n)$
$A^{\otimes n}$	producto tensorial de n veces el objeto A
$\left\|\tilde{\psi}\right\rangle$	estado real con incerteza respecto a estado ideal teórico $\|\psi\rangle$
$\left[\hat{A}, \hat{B}\right]$	conmutador de operadores $\hat{B}$
$\mathrm{Re}(z)$	parte real del número complejo z
$\mathrm{Im}(z)$	parte imaginaria del número complejo z
$\chi^{(n)}$	susceptibilidad de orden n a la polarización eléctrica
$R_i(\theta)$	rotaciones alrededor del eje $i = x, y, z$ por un ángulo θ
U	operador unitario
H	operador de compuerta de Hadamard
K	material con susceptibilidad Kerr o $\chi^{(3)}$
NOT	compuerta de negación de un solo qubit
C-U	compuerta de operador U controlada por un qubit
C^k**-U**	compuerta de operador U controlada por k qubits

OBJETIVOS

General

Estudiar un conjunto universal de compuertas de computación cuántica y su implementación en el contexto de la óptica cuántica.

Específicos

1. Explicar los conceptos fundamentales de la computación cuántica, su historia y su importancia en el desarrollo tecnológico.

2. Comprender el funcionamiento de las compuertas lógicas cuánticas y su agrupamiento en un Conjunto universal de compuertas.

3. Explicar los conceptos fundamentales de la óptica cuántica, su desarrollo histórico, y el comportamiento de aparatos ópticos lineales y medios Kerr desde ese enfoque.

4. Explicar los mecanismos ópticos a través de los cuales se construyen físicamente las compuertas cuánticas en la representación de doble riel óptico de la computación cuántica.

INTRODUCCIÓN

Desde mediados del siglo pasado, la mecánica cuántica ha permitido hacer más eficientes los componentes de las computadoras, pero manteniéndose siempre dentro de los parámetros lógicos de la computación clásica. Sin embargo, el hecho de que el mundo cuántico funcione con una lógica diferente al clásico, específicamente en lo referente a superposición de estados y entrelazamiento, permite concebir un nuevo tipo de computación abstracta, la computación cuántica, y su materialización: las computadoras cuánticas [7]. Los fenómenos cuánticos suponen la capacidad de una computadora cuántica para realizar el equivalente a múltiples procesos clásicos en un solo proceso, dada la indeterminación de los estados cuánticos [7]. Además, la invertibilidad de los procesamientos cuánticos permite evitar pérdidas de información inevitables en la computación clásica [9].

La unidad básica de la computación cuántica es el *bit cuántico* o *qubit* [7]. El bit clásico puede estar en uno de dos estados, 0 y 1, pero el qubit puede estar en cualquier superposición de sus estados base, $\{|0\rangle, |1\rangle\}$, dando un conjunto continuo de posibles estados [9]. La medición de un qubit arrojará solamente uno de los dos estados base con cierta probabilidad para cada uno, pero previo a la medición el qubit está en un estado superpuesto que puede ser manipulado y transformado para alterar indirectamente los resultados de las mediciones, resultando en consecuencias experimentales reales [9]. Una operación de computación cuántica consta de tres pasos básicos: preparación de un estado de entrada, transformación unitaria de este estado, y medición del estado de salida; una computadora cuántica es un conjunto de múltiples qubits siendo sometidos a este proceso [7].

La transformación unitaria del estado del qubit es lo que se conoce como *compuerta cuántica*, y al igual que en la computación clásica, hay un conjunto universal de unas pocas compuertas con las cuales se pueden construir todas las posibles transformaciones necesarias para una computadora cuántica [9]. Las compuertas clásicas

no son invertibles, lo que significa que un bit operado no puede devolverse a su estado anterior, provocando una pérdida de información [9]. Por el contrario, las compuertas cuánticas siempre son invertibles, evitando esta pérdida de información [9].

La óptica cuántica tiene su base en la cuantización escalar de los campos eléctrico y magnético de la luz [12]. Esta cuantización resulta en una base ortonormal de eigenestados $|n\rangle$ del número de fotones y de cantidad de energía, que coincide con los niveles de energía del oscilador armónico cuántico [12]. Dada esta cuantización, los eigenestados fotónicos están sometidos a la superposición de estados cuánticos y, por tanto, al entrelazamiento cuántico [12]. Estas características cuánticas de la luz cuentan con varias confirmaciones experimentales, de manera que la óptica cuántica resulta en un campo fértil para el desarrollo experimental de la computación cuántica.

Existe una diversidad de métodos actuales y en desarrollo que permiten la manipulación de los estados cuánticos de la luz, lo que se traduce en la posibilidad real de elaborar compuertas cuánticas para construir los algoritmos que manipulan los qubits ópticos [12]. En el siguiente trabajo se presenta una de estas posibles implementaciones físicas de computación cuántica, conocida como representación de doble riel óptico. En el primer capítulo se exploran las ideas básicas sobre compuertas lógicas en computación cuántica, haciendo énfasis en los requerimientos mínimos que hacen universal a la computación cuántica. El segundo capítulo explora la óptica cuántica para entender como evolucionan los fotones con el paso a través de medios ópticos lineales y medios Kerr (no lineales). El tercer capítulo introduce la representación de doble riel de la computación cuántica; en esta implementación, un qubit puede representarse con el producto de estados fotónicos o modos $|n = 0\rangle$ de vacío y $|n = 1\rangle$ de fotón único. Las operaciones de compuertas cuánticas se pueden realizar sobre estos estados con espejos, divisores de haz, desplazadores de fase óptica, y materiales de alta susceptibilidad Kerr que permitan interacción Kerr cruzada entre los modos de distintos qubits. Este último capítulo también explica las dificultades asociadas a este modelo de computación cuántica, y algunas posibilidades para superar dichos impedimentos.

1. COMPUTACIÓN CUÁNTICA Y CONJUNTO UNIVERSAL DE COMPUERTAS CUÁNTICAS

1.1. Introducción

1.1.1. El qubit

La mínima unidad de contenido de información clásica es el bit; el equivalente del bit clásico en la computación cuántica es el bit cuántico o *qubit* [15]. Un qubit consiste en un sistema de dos niveles o estados, los cuales se pueden representar como la base $\{|0\rangle, |1\rangle\}$ con

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1.1}$$

que se conocen como *base computacional*, son ortonormales $\langle i|j\rangle = \delta_{ij}$ y complejos $|i\rangle \in \mathbb{C}^2$ [15]. Sistemas de múltiples qubits se pueden representar con esta notación a través del producto tensorial [15]: por ejemplo, para dos qubits se tiene $|i\rangle \otimes |j\rangle = |i\rangle\,|j\rangle = |ij\rangle$ para el estado total del sistema.

La superioridad de la computación cuántica sobre la computación clásica radica en el hecho de que, previo a una medición, el qubit no se encuentra en uno de sus dos estados, sino en una superposición de ambos estados $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, con $a, b \in \mathbb{C}$ y $|a|^2 + |b|^2 = 1$ [9]. Un sistema de múltiples qubits se encuentra en un producto tensorial de los estados superpuestos de los qubits individuales, creando un estado superpuesto para el sistema total. Debido a esta propiedad de los qubits, cuando estos son procesados en una operación computacional, no se está procesando sólo un eigenestado $|i\rangle$ hacia otro $|j\rangle$, sino que se está procesando la superposición completa hacia otra superposición [9]. Esto se traduce en un equivalente a múltiples procesos clásicos realizándose paralelamente [9]. Sin embargo, los postulados de la mecánica cuántica demandan que una medición colapse un estado cuántico general hacia un

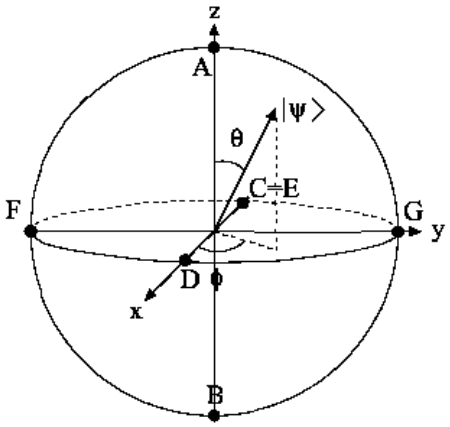

Figura 1.1. Esfera de Bloch, elaborado por Benenti, Casati y Strini [7].

eigenestado, perdiéndose la información paralela; la extracción de la información es uno de los principales problemas que un algoritmo cuántico debe resolver [9].

Un qubit genérico puede escribirse como

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}, \tag{1.2}$$

cuya forma permite una representación geométrica conocida como *Esfera de Bloch* [7], una esfera unitaria donde ϕ es el ángulo azimutal y θ es el polar en coordenadas polares, como se puede observar en la figura 1.1.

En coordenadas cartesianas de la esfera de Bloch, el qubit genérico toma la forma

$$|\psi\rangle = \begin{pmatrix} \sqrt{\frac{1+z}{2}} \\ \frac{x+iy}{\sqrt{2(1+z)}} \end{pmatrix},$$

con la conversión $x = \sin\theta\cos\phi$, $y = \sin\theta\sin\phi$ y $z = \cos\theta$, que implica $x^2+y^2+z^2 = 1$. Los valores de estas coordenadas cartesianas se obtienen de los valores esperados de las matrices de Pauli respecto del qubit genérico en (1.2)

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.3}$$

de lo que se obtiene

$$\langle\sigma_x\rangle_\psi = \sin\theta\cos\phi = x,$$

$$\langle\sigma_y\rangle_\psi = \sin\theta\sin\phi = y,$$

$$\langle \sigma_z \rangle_\psi = \cos\theta = z.$$

Para obtener el valor esperado de un operador, se deben realizar múltiples mediciones del observable y calcular el promedio, y la precisión depende de la cantidad de mediciones realizadas sobre qubits preparados en el mismo estado [7].

El espacio de Hilbert de un sistema cuántico es el espacio generado por el conjunto de eigenestados del sistema, y posee un producto interno entre estados [9]. El espacio de Hilbert total de un sistema es el producto tensorial de los espacios de Hilbert de los subsistemas: los estados totales son productos tensoriales de los estados de los subsistemas, los estados de un subsistema sólo tienen producto interno entre sí, y los operadores de un subsistema solo afectan a los estados de dicho subsistema [9].

Cuando un sistema consiste en múltiples qubits, el espacio de Hilbert total es el producto del espacio de cada qubit [9]. En esta situación, la superposición de estados del sistema total puede producir entrelazamiento cuántico [16] [17] [18], en el que los estados de los subsistemas están correlacionados entre sí más fuertemente de lo que es posible en cualquier situación clásica, lo cual fue demostrado matemáticamente por J. Bell en 1964 [5] [6] y probado experimentalmente por A. Aspect en 1981 [2] [3] [4]. Estos fenómenos ya se pueden observar con tan solo dos qubits; en esta situación, el estado más general del sistema está dado por

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

donde los estados base son el producto tensorial $|ij\rangle = |i\rangle \otimes |j\rangle$ de los estados base de cada qubit, y se tiene la condición de normalización $\sum_{ij} |\alpha_{ij}|^2 = 1$ para las probabilidades $|\alpha_{ij}|^2$ que cada estado tiene de aparecer ante una medición [9]. Al realizar una medición sobre un qubit del sistema solamente, el estado total colapsa en un estado con un valor definido para el qubit medido y una superposición respecto a los valores del otro qubit: por ejemplo, si se mide que el primer qubit tiene valor $|1\rangle$, el estado total resultante de la medición, con su nueva normalización, queda

$$|\psi\rangle = \frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{11}|^2 + |\alpha_{10}|^2}}.$$

Por otro lado, el fenómeno de entrelazamiento cuántico se puede observar con los

llamados *estados de Bell* [5] [6]

$$|\psi\rangle_1 = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \qquad |\psi\rangle_2 = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right), \tag{1.4}$$

en los cuales el estado total del sistema es independiente de las separaciones físicas y temporales de los subsistemas (los qubits individuales), condición que ha sido probada usando pares de fotones entrelazados con una separación de hasta 1203 km de distancia sobre la Tierra, utilizando satélites para la distribución de los fotones, lo que resulta en un camino de longitud total variable entre 1600 y 2400 km [20]. De esta manera, la medición sobre un qubit colapsa el estado total del sistema hacia el estado base correspondiente a la medición realizada, colapsando a su vez el estado del otro qubit [9]. La característica más importante de los estados entrelazados es que no pueden ser factorizados como el producto tensorial de estados de los subsistemas [9]. Para $|\psi\rangle_1$ específicamente, si una medición sobre el primer qubit arroja $|0\rangle$, una medición sobre el segundo arrojará necesariamente $|0\rangle$ también. Este fenómeno es la correlación entre sistemas (los qubits) que es mucho más fuerte que cualquier correlación clásica, como establecen los estudios de Bell [5] [6].

La superposición de estados y el entrelazamiento cuántico son las características fundamentales que diferencian el mundo cuántico del clásico, y que implican que la computación cuántica tiene una capacidad de procesamiento de información superior a la de la computación clásica [9].

1.1.2. Generalidades de las computadoras cuánticas

Una computadora clásica se puede describir como un registro finito de n bits, sobre los cuales se efectúan operaciones elementales (o se aplican compuertas lógicas) individualmente o en conjuntos [7]. El estado de tal registro se etiqueta con un número entero

$$i = \sum_{k=0}^{n-1} i_k 2^k,$$

con $i_k \in \{0, 1\}$ [7]. Entre estas operaciones elementales, existen conjuntos de unas pocas compuertas lógicas que se pueden combinar para efectuar todas las operaciones posibles [7].

Esta definición, el modelo de circuito, es aplicable a la computación cuántica:

una computadora cuántica es un registro de n qubits, sobre los cuales se aplican operaciones elementales, o compuertas lógicas cuánticas, individualmente o en conjuntos [7]. El estado total genérico de este registro cuántico es una superposición de los 2^n eigenestados del espacio de Hilbert total de la computadora

$$|\psi\rangle = \sum_{i=0}^{2^{n-1}} c_i \, |i\rangle = \sum_{i_{n-1}=0}^{1} \cdots \sum_{i_0=0}^{1} c_{i_{n-1},\cdots,i_0} \, |i_{n-1}\rangle \otimes \cdots \otimes |i_0\rangle \, ,$$

con la normalización $\sum_{i=0}^{2^{n-1}} |c_i|^2 = \sum_{i_{n-1}=0}^{1} \cdots \sum_{i_0=0}^{1} \left|c_{i_{n-1},\cdots,i_0}\right|^2 = 1$ [7]. Es útil la notación $|i_{n-1}\rangle \otimes \cdots \otimes |i_0\rangle = |i_{n-1} \cdots i_0\rangle$.

El estado total de un registro de n bits clásicos corresponde solamente a un número entero; por otro lado, la superposición de estados del registro cuántico se puede asociar con hasta 2^n estados base del conjunto de qubits, es decir, almacena paralelamente un equivalente de hasta 2^n registros clásicos [7]. La capacidad de extraer toda o parte de esta información, más allá de un solo eigenestado, es una de las cualidades no triviales de los algoritmos cuánticos [9].

Es importante notar que en física clásica existen múltiples instancias de superposición de diferentes aspectos físicos, pero estas superposiciones son fundamentalmente diferentes a la superposición de estados cuánticos: la superposición clásica es un constructo matemático para describir la totalidad de un aspecto físico medible (la superposición es la medición), pero la superposición cuántica trata sobre estados que se excluyen mutuamente ante una medición (la superposición desaparece ante la medición) [7]. Además, la superposición de estados clásicos solo existe para estados de un solo sistema, mientras que los estados cuánticos de múltiples sistemas separados (qubits) se superponen entre sí, permitiendo la aparición de entrelazamiento [7].

El entrelazamiento cuántico le da a la computación cuántica una importante ventaja sobre la computación clásica respecto al uso de recursos [7]. Para representar la superposición de 2^n niveles clásicamente, estos niveles deben pertenecer al mismo sistema [7]. Entonces, si la separación de energía entre cada nivel es Δ, el costo computacional de realizar la representación será proporcional a $\Delta 2^n$, un crecimiento exponencial de recursos respecto a n [7]. Sin embargo, un conjunto de solamente n qubits puede encontrarse en una superposición de hasta 2^n estados, es decir, puede

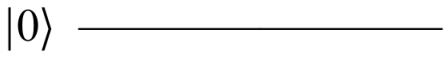

Figura 1.2. Representación de un qubit en un diagrama de circuito, elaborado por Hidary [15].

realizar la representación con un costo computacional lineal respecto de n [7].

1.2. Compuertas cuánticas

Un registro cuántico es un sistema cuántico, por lo que su evolución está determinada por la ecuación Schrödinger, y la descripción de esta evolución se realiza con operadores lineales unitarios [7]. En la base computacional, para n qubits, estos operadores se representan como matrices de $2^n \times 2^n$, las cuales a su vez se pueden descomponer en el producto tensorial de matrices unitarias de 2×2 o 4×4, cada una actuando sobre uno solo o dos qubits, respectivamente [7].

El modelo de circuito de una computadora cuántica se representa a través diagramas de circuitos con la siguiente simbología: una línea (o cable) representa un qubit, se puede etiquetar según el estado del qubit, como se observa en la figura 1.2, y se le puede poner una etiqueta en cada extremo para qubits que han sido modificados [15]. En la figura 1.3 se observa una representación condensada de n qubits; esto solamente es notación, no tiene ningún significado físico particular. Por otro lado, en la figura 1.4 se puede ver la representación visual de una compuerta lógica cuántica genérica U (letra elegida por la palabra 'unitaria'), que puede afectar uno o múltiples qubits simultáneamente [15].

En mecánica cuántica, la evolución de estados preserva el producto interno del espacio del Hilbert, de manera que en computación cuántica las compuertas que evolucionan el estado de los qubits son operadores unitarios y, por tanto, reversibles por medio del operador adjunto [15]. Las mediciones realizadas sobre qubits se describen con operadores hermíticos, que son auto-adjuntos, y sus eigenvalores son reales y corresponden a resultados de medición [15].

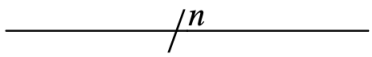

Figura 1.3. Representación condensada de n qubits en un diagrama de circuito, elaborado por Hidary [15].

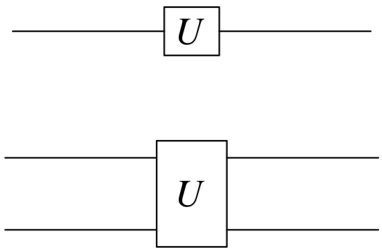

Figura 1.4. Representación de compuertas lógicas cuánticas en un diagrama de circuito, elaborado por Hidary [15].

1.2.1. Compuertas de un qubit

La compuerta lógica más simple, tanto en computación clásica como en la computación cuántica, es la que cambia el valor de un bit o qubit, la compuerta de la negación o **NOT** [15]. Para un qubit genérico, esto se observa como [15]

$$\mathbf{NOT}\left(\alpha\left|0\right\rangle+\beta\left|1\right\rangle\right)=\beta\left|0\right\rangle+\alpha\left|1\right\rangle.$$

En la base computacional que se define en (1.1), esta compuerta corresponde a la matriz de Pauli para el eje x

$$\mathbf{NOT}=\sigma_x=X=\begin{pmatrix}0&1\\1&0\end{pmatrix}, \tag{1.5}$$

y se ilustra en diagrama de circuitos según la figura 1.5. La acción de esta compuerta también puede expresarse como

$$\mathbf{NOT}\left|j\right\rangle=\left|j\oplus 1\right\rangle \tag{1.6}$$

donde $a\oplus b$ representa el residuo de $(a+b)/2$, y se le llama *Suma módulo-2* [15].

Figura 1.5. Representación de compuerta **NOT** cuántica en un diagrama de circuito, elaborado por Hidary [15].

Figura 1.6. Representación de compuerta Y o σ_y de Pauli en un diagrama de circuito, elaborado por Hidary [15].

Los otros operadores del grupo de Pauli también son compuertas válidas [15]. El operador del eje y se representa en un diagrama según la figura 1.6 y tiene un efecto [15]

$$Y\left|j\right\rangle = (-1)^j i\left|j \oplus 1\right\rangle.$$

El operador σ_z o Z tiene como efecto un cambio de fase condicionado al valor del qubit

$$Z\left|j\right\rangle = (-1)^j\left|j\right\rangle,$$

y tiene una representación de circuito idéntica a la de Y, pero con la letra correspondiente [15]. En general, el grupo de Pauli actúa como rotaciones de valor fijo sobre la esfera de Bloch, alrededor del eje correspondiente al operador, tomando en cuenta que cuando un $|0\rangle$ queda con un coeficiente imaginario, este último se factoriza del estado total y se trata como fase global (irrelevante) [15].

A partir del grupo de Pauli se pueden obtener rotaciones generales en la esfera de Bloch [7]. Para llegar a esto, se utiliza el hecho de que al hacer la expansión de Taylor del exponencial de operadores $\hat{O}$ que cumplen $\hat{O}^2 = \hat{I}$, se obtiene

$$e^{-i\alpha\hat{O}} = \cos(\alpha)\,\hat{I} - i\sin(\alpha)\,\hat{O}. \tag{1.7}$$

Usando esta ecuación, las rotaciones alrededor del eje x son

$$R_x(\delta) = e^{-i\frac{\delta}{2}\sigma_x} = \begin{pmatrix} \cos\frac{\delta}{2} & -i\sin\frac{\delta}{2} \\ -i\sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{pmatrix}; \tag{1.8}$$

y similarmente para el eje y

$$R_y(\delta) = e^{-i\frac{\delta}{2}\sigma_y} = \begin{pmatrix} \cos\frac{\delta}{2} & -\sin\frac{\delta}{2} \\ \sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{pmatrix}. \tag{1.9}$$

El procedimiento se repite para el eje z, pero el resultado que se obtiene recibe el

nombre de desplazamiento de fase [7]

$$R_z(\delta) = e^{-i\frac{\delta}{2}\sigma_z} = e^{-i\frac{\delta}{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}. \tag{1.10}$$

Ignorando la fase global del operador, lo que se tiene es un cambio de fase condicional: el estado $|0\rangle$ no es afectado, mientras que el estado $|1\rangle$ recibe un cambio de fase de magnitud δ (tomando sus definiciones en (1.1)) [7]. Si se tiene un operador $\hat{n}|n\rangle = n|n\rangle$ con $n = 0, 1$, el desplazamiento de fase se puede expresar como

$$e^{i\delta\hat{n}}|n\rangle = e^{i\delta n}|n\rangle. \tag{1.11}$$

Una rotación general es solamente el producto de rotaciones al rededor de cada eje: para una rotación infinitesimal al rededor de un eje dado por el vector unitario $\vec{n}$, se tiene

$$R_n(\epsilon) \approx R_x(n_x\epsilon)R_y(n_y\epsilon)R_z(n_z\epsilon),$$

con $\epsilon \ll 1$, de manera que

$$R_n(\epsilon) \approx \hat{I} - i\frac{\epsilon}{2}\vec{n}\cdot\vec{\sigma},$$

por lo que la rotación finita es [7]

$$R_n(\delta) = e^{-i\frac{\delta}{2}\vec{n}\cdot\vec{\sigma}},$$

Otra compuerta importante es la de Hadamard, que al actuar sobre estados base los convierte en estados superpuestos con la misma probabilidad para cada eigenestado [7]. Esta compuerta, en la base computacional, tiene forma matricial

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1.12}$$

que provoca

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

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

resumible en

$$H|j\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^j|1\rangle\right], \tag{1.13}$$

y cumple que $H^2 = \hat{I}$ y $H^\dagger = H$ [7].

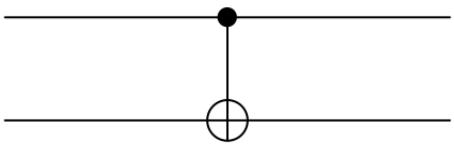

Figura 1.7. Representación de compuerta **CNOT** cuántica en un diagrama de circuito, elaborado por Hidary [15].

Es importante enfatizar que cualquier compuerta cuántica que actúa sobre un qubit es, necesariamente, algún tipo de rotación en la esfera de Bloch del qubit, y puede descomponerse en tales términos [7].

1.2.2. Compuertas de dos qubits

Como se mencionó en la sección 1.1.2, el entrelazamiento cuántico es una de las propiedades y ventajas fundamentales de la computación cuántica, y sólo se puede presentar en sistemas con dos o más qubits [7]. Para obtener entrelazamiento, se utiliza la compuerta **CNOT** cuántica, también llamada negación controlada, cuyo diagrama de circuito está en la figura 1.7 y trabaja con dos qubits, denomidados *control* y *objetivo*, realizando la acción

$$\mathbf{CNOT}\,|x\rangle\,|y\rangle = |x\rangle\,|x \oplus y\rangle\,, \tag{1.14}$$

lo que significa que la compuerta cambia el valor del qubit objetivo $|y\rangle$, si y sólo si el qubit control $|x\rangle$ es $|1\rangle$ [7]. Utilizando la notación $|00\rangle = |0\rangle$, $|01\rangle = |1\rangle$, $|10\rangle = |2\rangle$ y $|11\rangle = |3\rangle$, se pueden obtener los elementos de matriz de la compuerta en base computacional: $(\mathbf{CNOT})_{ab} = \langle a|\,\mathbf{CNOT}\,|b\rangle$, quedando [7]

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.15}$$

Se puede observar que el bloque de 2×2 derecho inferior de la matriz corresponde al operador **NOT**. La generación de entrelazamiento a partir de esta compuerta se realiza [7]

$$\mathbf{CNOT}\,(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle = \alpha\,|00\rangle + \beta\,|11\rangle\,,$$

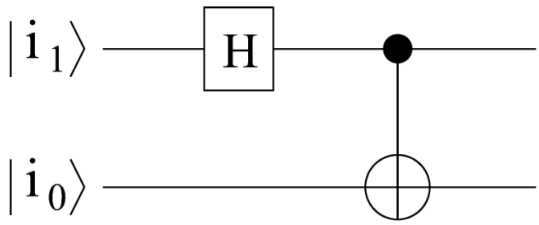

Figura 1.8. Representación de la combinación de compuertas que produce la base de Bell en un diagrama de circuito, elaborado por Benenti, Casati y Strini [7].

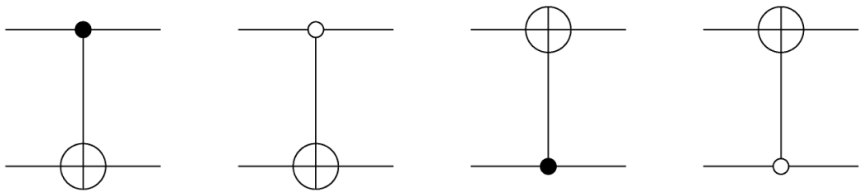

Figura 1.9. Representación de las compuertas cuánticas **CNOT** generalizadas en un diagrama de circuito, elaborado por Benenti, Casati y Strini [7].

$$\mathbf{CNOT}\left(\alpha\left|0\right\rangle+\beta\left|1\right\rangle\right)\left|1\right\rangle=\alpha\left|01\right\rangle+\beta\left|10\right\rangle.$$

Si se parte de alguno de los eigenestados de dos qubits, la acción combinada de la compuerta de Hadamard sobre el qubit control y la **CNOT** produce la llamada *Base de Bell* de estados entrelazados [7]

$$\left|00\right\rangle\rightarrow\left|\phi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right), \tag{1.16}$$

$$\left|10\right\rangle\rightarrow\left|\phi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right), \tag{1.17}$$

$$\left|01\right\rangle\rightarrow\left|\psi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right), \tag{1.18}$$

$$\left|11\right\rangle\rightarrow\left|\psi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right). \tag{1.19}$$

El diagrama de circuito de este proceso se puede observar en la figura 1.8.

La compuerta **CNOT** se puede generalizar hacia otras variantes, en las cuales se intercambian los papeles de qubit control y qubit objetivo, o se cambia la condición para realizar la negación [7]. Los diagramas de estas compuertas se presentan en la figura 1.9, donde el círculo negro significa que la condición para el cambio es que el control sea $|1\rangle$, y el círculo blanco representa la condición de control $|0\rangle$ [7]. La combinación de **CNOT** estándar, luego una invertida (la tercera desde la izquierda en la figura 1.9) y al final otra estándar, produce un intercambio $|xy\rangle\rightarrow|yx\rangle$, lla-

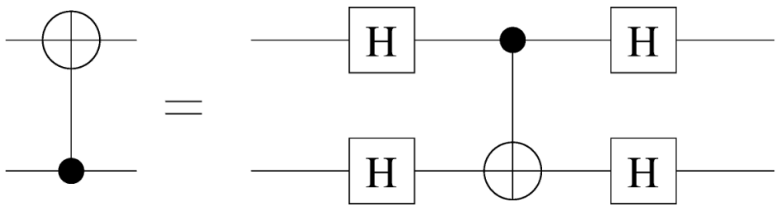

Figura 1.10. Diagrama de circuito de la combinación que produce la tercera compuerta de la figura 1.9, elaborado por Benenti, Casati y Strini [7].

mado compuerta **SWAP** [7]. La tercera compuerta **CNOT** mencionada se puede obtener a partir de la estándar y compuertas de Hadamard en la combinación presente en la figura 1.10 [7].

Otra compuerta cuántica binaria importante es la de desplazamiento de fase controlado o **CPHASE**, la cual es la aplicación controlada de la compuerta descrita por (1.10), con el primer qubit como control [7]. Utilizando la notación de la ecuación (1.11), la acción de esta compuerta es

$$e^{i\delta \hat{n}_c \hat{n}_t} |n_c n_t\rangle = e^{i\delta n_c n_t} |n_c n_t\rangle , \tag{1.20}$$

de manera que la compuerta sólo se aplica al qubit objetivo si el control es $|1\rangle$, y la aplicación sólo es efectiva si el qubit objetivo es también $|1\rangle$, tal como sucede para el desplazamiento de fase de un solo qubit [7]. La representación matricial de **CPHASE** en la base computacional tiene la forma

$$\mathbf{CPHASE}(\delta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{pmatrix} , \tag{1.21}$$

y es posible obtenerla a partir de compuertas **CNOT** y $R_z\left(\pm\frac{\delta}{2}\right)$ (esta última de un solo qubit) combinadas en la forma mostrada en la figura 1.11.

En general, es posible construir una compuerta cuántica unitaria controlada genérica **C-U**, de efecto

$$\mathbf{C-U} |a\rangle |b\rangle = |a\rangle U^a |b\rangle , \tag{1.22}$$

a partir de rotaciones y desplazamientos de fase de un solo qubit, en combinación con compuertas **CNOT** [9]. Para demostrar esto, primero se debe iniciar mostrando

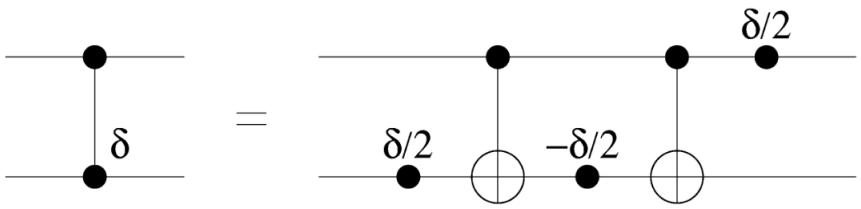

Figura 1.11. Diagrama de circuito de la combinación que produce **CPHASE**, elaborado por Benenti, Casati y Strini [7].

que una operación unitaria genérica $\mathbf{U}$ consiste en una combinación de rotaciones y fases: dado que $\mathbf{U}$ es unitaria, su representación matricial computacional tiene filas y columnas ortonormales, por lo que existen $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ tal que

$$\mathbf{U} = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)} \sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos\frac{\gamma}{2} \end{bmatrix},$$

lo cual se puede expresar como

$$\mathbf{U} = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Esta descomposición se puede reformular utilizando el hecho de que $\sigma_x\sigma_y\sigma_x = -\sigma_y$ y $\sigma_x\sigma_z\sigma_x = -\sigma_z$, lo que al aplicarse con la ecuación (1.7), usando $j = y, z$, da [9]

$$\sigma_x R_j(\theta)\sigma_x = \cos(\theta)\,\sigma_x\hat{I}\sigma_x - i\sin(\theta)\,\sigma_x\sigma_j\sigma_x$$

$$= \cos(\theta)\,\hat{I} + i\sin(\theta)\,\sigma_j = \cos(-\theta)\,\hat{I} - i\sin(-\theta)\,\sigma_j$$

$$= R_j(-\theta).$$

Con esto, se puede tomar la descomposición de $\mathbf{U}$, aplicarle las propiedades de transformación de σ_x sobre rotaciones, y reescribirla como

$$\mathbf{U} = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) = e^{i\alpha} R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta+\beta}{2}\right) R_z\left(\frac{\delta-\beta}{2}\right)$$

$$= e^{i\alpha} R_z(\beta) R_y\left(\frac{\gamma}{2}\right) \sigma_x R_y\left(-\frac{\gamma}{2}\right) \sigma_x\sigma_x R_z\left(-\frac{\delta+\beta}{2}\right) \sigma_x R_z\left(\frac{\delta-\beta}{2}\right)$$

$$= e^{i\alpha} R_z(\beta) R_y\left(\frac{\gamma}{2}\right) \sigma_x R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right) \sigma_x R_z\left(\frac{\delta-\beta}{2}\right),$$

que se puede escribir como

$$\mathbf{U} = e^{i\alpha} A\sigma_x B\sigma_x C, \tag{1.23}$$

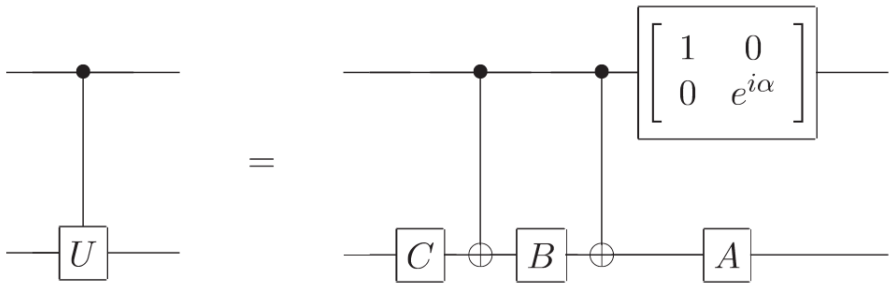

Figura 1.12. Diagrama de circuito de la combinación que produce **C-U**, elaborado por Nielsen y Chuang [9].

donde las matrices de la descomposición son

$$A = R_z(\beta)R_y\left(\frac{\gamma}{2}\right),$$

$$B = R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right),$$

$$C = R_z\left(\frac{\delta-\beta}{2}\right),$$

y cumplen que $ABC = I$ [9].

Es importante notar que aunque la fase $e^{i\alpha}$ se asocie a un qubit en particular, en realidad es un factor multiplicando a todo el estado base en el que está incluido el qubit en cuestión [9]. Ahora, con la descomposición universal (1.23) para un solo qubit, se puede extender a una compuerta **C-U** general: tomando que **U** actúe sobre el qubit objetivo, si los operadores σ_x se condicionan al estado de un qubit de control, pasando de ser compuertas **NOT** a ser **CNOT**, entonces el qubit control determinará si lo que se aplica sobre el qubit objetivo es $ABC = I$ o $A\sigma_x B\sigma_x C = e^{-i\alpha}\mathbf{U}$ [9]. Para completar, el operador de fase se aplica sobre el control en forma $R_z(\alpha)$, de manera que si este es $|0\rangle$, no habrá efecto alguno sobre el sistema [9]. Si el control es $|1\rangle$, el efecto total sobre el sistema será el efecto **C-U** deseado [9]. Todo este proceso puede visualizarse en la figura 1.12.

1.3. Conjuntos universales de compuertas

En computación clásica existen conjuntos de operaciones lógicas elementales llamados *Conjuntos Universales de Compuertas*; uno (cualquiera) de estos conjuntos

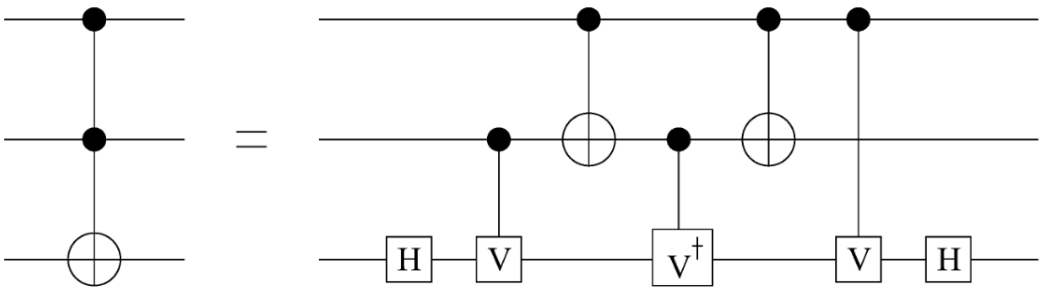

Figura 1.13. Diagrama de circuito de la combinación que produce la compuerta de Tiffoli, elaborado por Benenti, Casati y Strini [7].

universales (como $\{\mathbf{NAND}, \mathbf{COPY}\}$) contiene una cantidad limitada de compuertas lógicas que se pueden combinar para realizar procesos arbitrariamente complejos [7]. Este resultado también aparece en la computación cuántica: cualquier operación unitaria sobre el espacio de Hilbert de un registro de tamaño n puede descomponerse en una combinación de compuertas **CNOT** estándar y compuertas de un solo qubit [7].

Primero, es necesario definir y construir la compuerta de *Tiffoli*, que es el nombre especial que recibe $C^2 - \mathbf{NOT}$, la cual cambia el valor de un qubit objetivo solamente si los *dos* qubits de control son $|1\rangle$ [7]. Esta compuerta está constituida por compuertas **CNOT**, de Hadamard, compuertas controladas **C-V** y su adjunto $\mathbf{C} - \mathbf{V}^\dagger$ (recordando *Unitario: el adjunto de un operador es su inverso*), donde $\mathbf{V}$ de un solo qubit es un desplazamiento de fase

$$R_z\left(\frac{\pi}{2}\right) = \mathbf{V} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

de manera que **C-V** es realmente un caso especial de **CPHASE**, la cual se ha mostrado previamente que se puede construir solamente con **CNOT** y compuertas de un solo qubit [7]. A partir de estas compuertas, la de Tiffoli se construye como se observa en la figura 1.13. Es evidente que una compuerta de Tiffoli es su propio inverso [7].

Ya se tiene la compuerta de Tiffoli construida, en última instancia, a partir de compuertas de un solo qubit (rotaciones sobre la esfera de Bloch) y **CNOT**, además de la descomposición en los mismos términos de la compuerta **C-U** según la ecuación (1.23) y la figura 1.12. Ahora se puede hallar la descomposición de una compuerta general $C^k{-}\mathbf{U}$, la aplicación de $\mathbf{U}$ sobre un qubit objetivo condicionada a k qubits

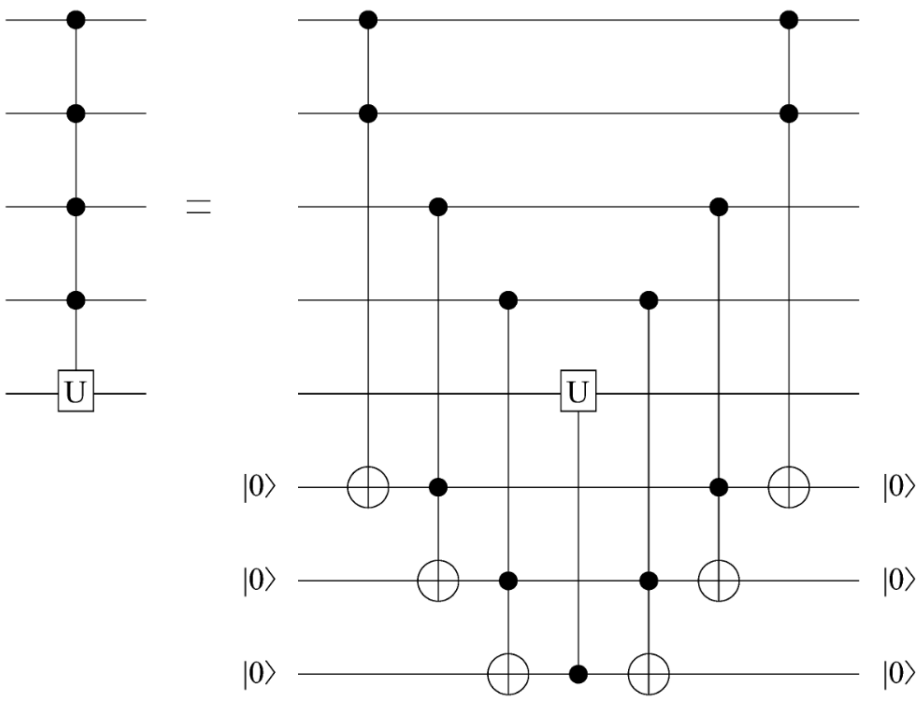

Figura 1.14. Diagrama de circuito de la combinación que produce la compuerta $C^k-\mathbf{U}$, para el caso especial $k = 4$, elaborado por Benenti, Casati y Strini [7].

de control, en términos de compuertas de Tiffoli y **C-U**, lo que a su vez significa que puede considerarse una combinación únicamente de compuertas **CNOT** y rotaciones de un qubit [7]. Dicha descomposición, de k qubits de control con un qubit objetivo, requiere el uso de $k - 1$ qubits auxiliares inicializados en estados $|0\rangle$ [7].

El razonamiento se puede visualizar en la figura 1.14, donde está el caso especial $k = 4$: las compuertas de Tiffoli condicionan un cambio de valor de un qubit auxiliar a un qubit de control y a un auxiliar afectado previamente por otra Tiffoli (el primer qubit auxiliar es condicionado por dos de control) [7]. Este proceso continúa iterando hasta agotar los k qubits de control y llegar al último qubit auxiliar, cuyo cambio $|0\rangle \rightarrow |1\rangle$ queda para todo propósito condicionado por los k qubits de control originales. Este último qubit auxiliar funciona como control para una compuerta **C-U** que actúa sobre el qubit objetivo [7]. De esta manera, la aplicación total es una aplicación de **U** condicionada por k qubits de control, con apoyo de los auxiliares [7]. Tras esto, se aplican las compuertas de Tiffoli en orden reverso para regresar a los qubits auxiliares a su estado original [7].

Se puede hacer la descomposición de $C^k-\mathbf{U}$ sin qubits auxiliares, tal como el

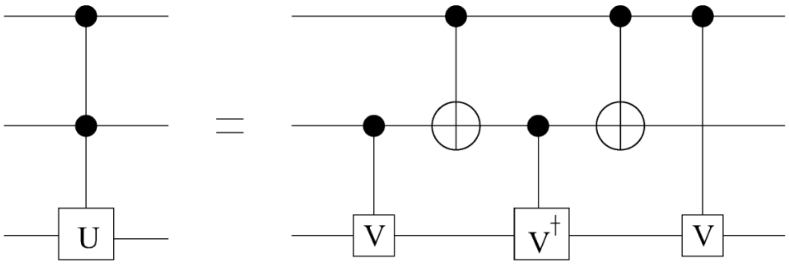

Figura 1.15. Diagrama de circuito de la combinación que produce la compuerta $C^2-\mathbf{U}$, sin qubits auxiliares, elaborado por Benenti, Casati y Strini [7].

ejemplo de $C^2-\mathbf{U}$ en la figura 1.15, pero en este caso la cantidad de compuertas usadas aumenta como $O(k^2)$, donde k son los qubits de control, frente al aumento $O(k)$ con el uso de auxiliares [7].

La otra parte de esta demostración de universalidad es la descomposición del operador unitario $U^{(n)}$ que actúa sobre un conjunto n de qubits [7]. En primer lugar, se expresa el operador como el producto de rotaciones

$$U^{(n)} = \prod_{i=1}^{2^n-1} \prod_{j=0}^{i-1} V_{ij}, \tag{1.24}$$

donde cada V_{ij} produce una rotación sólo de los eigenestados $|i\rangle$ y $|j\rangle$ del espacio de Hilbert de 2^n dimensiones, es decir, actúa sobre sólo dos componentes de un estado genérico $|\psi\rangle$ de los n qubits [7]. El siguiente paso es expresar V_{ij} como una combinación de compuertas $C^{(n-1)}-\mathbf{NOT}$ generalizadas y la rotación controlada de un solo qubit [7].

Esta descomposición requiere de la implementación de un *Código de Gray*, en el cual se parte del estado $|i\rangle$ y se le aplica una sucesión de compuertas $C^{(n-1)}-\mathbf{NOT}$ generalizadas que cambien sus valores de qubits hasta llegar a un estado $|i_f\rangle$ que difiere de $|j\rangle$ en el valor de un único qubit [7]. En ese punto, se aplica V_{ij} como una rotación sobre ese único qubit, controlada por todos los otros qubits [7]. Luego de eso las compuertas $C^{(n-1)}-\mathbf{NOT}$ generalizadas del código de Gray se aplican en orden reverso para regresar $|i_f\rangle$ a $|i\rangle$ [7]. De esta manera, V_{ij} ha actuado solamente sobre $|i\rangle$ y $|j\rangle$.

A manera de ejemplo, se pueden usar los estados base $|i\rangle = |00111010\rangle$ y

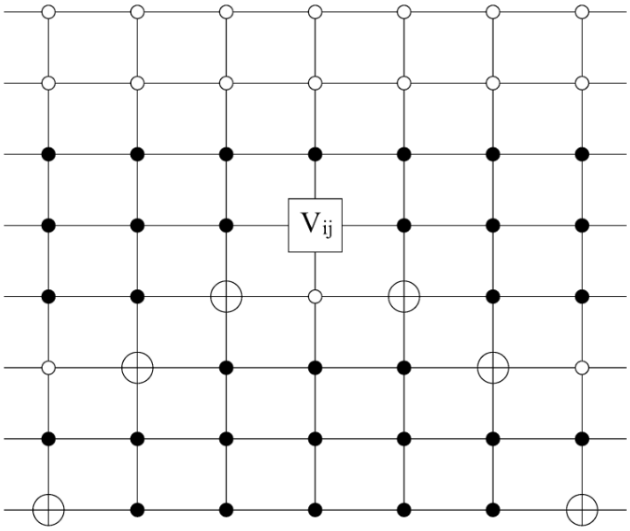

Figura 1.16. Diagrama de circuito del proceso del código de Gray y la aplicación de V_{ij}, para el ejemplo dado en el texto, elaborado por Benenti, Casati y Strini [7].

$|j\rangle = |00100111\rangle$ [7]. El código de Gray se implementa como

$$\begin{aligned} |i\rangle &= |00111010\rangle \\ &\rightarrow |00111011\rangle \\ &\rightarrow |00111111\rangle \\ \rightarrow |i_f\rangle &= |00110111\rangle \\ |j\rangle &= |00100111\rangle\,, \end{aligned}$$

usando las compuertas $C^{(7)}-\mathbf{NOT}$ generalizadas, donde las condiciones de control son los valores de todos los qubits excepto el qubit que se quiere cambiar en la iteración particular [7]. Una vez completado el código de Gray, se aplica V_{ij} sobre el cuarto qubit como una compuerta $C^7-\mathbf{V_{ij}}$ generalizada, donde las condiciones de aplicación son todos los qubits donde $|i_f\rangle$ y $|j\rangle$ tienen los mismos valores (de manera que sólo puede afectar a esos dos estados) [7]. Tras esto se aplican las compuertas $C^{(7)}-\mathbf{NOT}$ generalizadas en orden reverso. Todo este proceso está ilustrado en la figura 1.16.

La aplicación sucesiva de los múltiples V_{ij}, incluyendo sus procesos de código de Gray, producen la compuerta unitaria $U^{(n)}$, según la ecuación (1.24).

Como un punto aparte importante para la completitud de la demostración de la

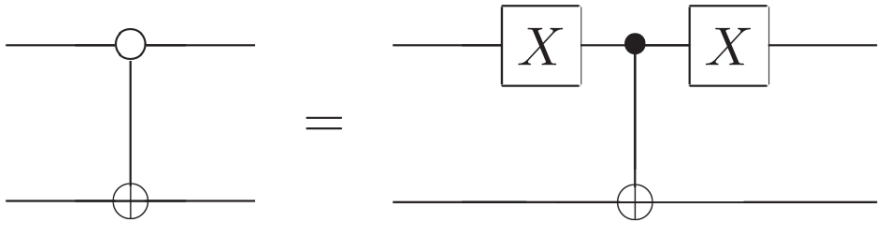

Figura 1.17. Diagrama de circuito del cambio de condición de control para **CNOT**, elaborado por Nielsen y Chuang [9].

universalidad del conjunto las compuertas de un solo qubit y compuerta **CNOT**, es necesario explicar que una compuerta $C^{(m)}-\mathbf{NOT}$ generalizada se puede conseguir de una $C^m-\mathbf{NOT}$ estándar, pero en los qubits donde se quiere que la condición de aplicación sea $|0\rangle$ se aplica una compuerta **NOT** previo a la aplicación de la estándar, y otra **NOT** después para regresar el qubit a su estado original [9]. Un ejemplo de este proceso se ilustra en la figura 1.17. Lo misma idea es válida para la $C^m-\mathbf{V_{ij}}$ generalizada respecto de una estándar armada según el molde de $C^m-\mathbf{U}$ [9].

Entonces, ha quedado demostrado que la compuerta genérica $U^{(n)}$ se puede construir, en última instancia, solamente con compuertas **CNOT** y rotaciones de un qubit, de manera que estos dos tipos de compuerta son un Conjunto Universal de compuertas cuánticas, con las cuales se puede realizar cualquier operación de computación cuántica sin importar su complejidad [7].

Combinando las conclusiones de ambas partes de la demostración, se tiene que a partir de este conjunto universal se puede armar también una compuerta $C^n-U^{(m)}$, donde hay n qubits de control y m qubits objetivo, y las condiciones de control se pueden generalizar con algunas compuertas de un solo qubit [9].

Que sea posible armar cualquier operación unitaria sólo con compuertas **CNOT** y rotaciones de un qubit, no significa que este sea el procedimiento más eficiente [7]. Si se puede obtener una compuerta más compleja que esos dos tipos sin hacer combinaciones de otras compuertas, será más eficiente que realizar la combinación [7]. La posibilidad de obtener un conjunto universal de compuertas cuánticas es la prueba de la universalidad de la computación cuántica, que significa que no está intrínsecamente limitada para resolver algún tipo de problemas, sólo la limitan los recursos disponibles [7].

Las compuertas clásicas reversibles de uno y dos bits no son universales [7]. Por otro lado, dado que la compuerta de Tiffoli es universal para la computación clásica, y la versión cuántica del operador se puede construir con un conjunto universal cuántico, la computación clásica está contenida dentro de la computación cuántica basada en rotaciones de un qubit y compuertas **CNOT**, las cuales son reversibles [7]. Además, la irreversibilidad de las operaciones lógicas clásicas conlleva un gasto de energía intrínseco que no afecta a los operadores reversibles cuánticos [7].

1.4. Algoritmos

1.4.1. Evaluación de funciones

La tarea básica de una computadora es la evaluación de funciones lógicas, donde el dominio consiste en n bits y la imagen es un solo bit

$$f : \{0,1\}^n \to \{0,1\}\,,$$

lo que significa que f toma una entrada $(x_{n-1}, \ldots, x_1, x_0) = x$, donde cada $x_i \in \{0,1\}$, y proporciona un valor de salida 0 o 1 [7]. A partir de estas funciones binarias se puede armar cualquier función más compleja [7]. En computación clásica, una función binaria f se puede evaluar reversiblemente si se usa un bit auxiliar para almacenar el resultado $f(x)$; las compuertas lógicas cuánticas son operadores unitarios reversibles, por lo que siempre usan qubits auxiliares

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle ,$$

donde x son los qubits de entrada y y es el qubit auxiliar [7]. De esta manera, aunque múltiples entradas x tengan la misma salida, el estado total de entrada con resultado es único [7].

Una función binaria genérica $f(x)$ de n bits (o qubits) de entrada se puede expresar en *mintérminos*: para un $x^{(a)}$ tal que $f\left(x^{(a)}\right) = 1$, un mintérmino se define como [7]

$$f^{(a)}(x) = \begin{cases} 1, & x = x^{(a)} \\ 0, & x \neq x^{(a)}. \end{cases} \tag{1.25}$$

x_2	x_1	x_0	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Tabla 1.1. Ejemplo de función binaria [7].

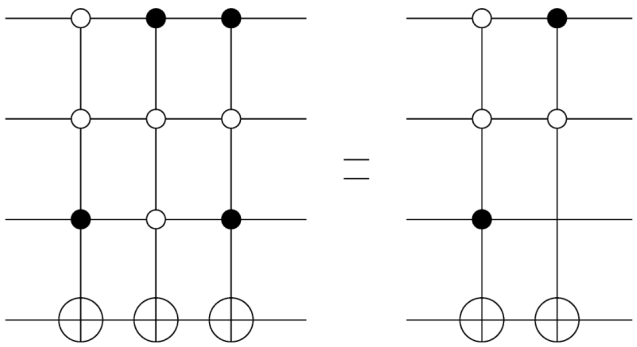

Figura 1.18. Diagrama de circuito para la evaluación de la función en la Tabla 1.1, elaborado por Benenti, Casati y Strini [7].

La función total se escribe como la disyunción de todos sus mintérminos

$$f(x) = f^{(1)}(x) \vee f^{(2)}(x) \vee \cdots \vee f^{(m)}(x), \tag{1.26}$$

con $0 \leq m \leq 2^n$ [7]. En computación cuántica, cada mintérmino se puede expresar como una compuerta $C^n - \mathbf{NOT}$ generalizada; es importante notar que la cantidad de mintérminos de una función genérica sin estructura crece con 2^n (exponencialmente), por lo que la cantidad de compuertas elementales necesarias para evaluar la función crece de la misma manera [7].

Un ejemplo simple de uso de mintérminos es la función definida según la tabla de verdad 1.1, de donde se tiene que los mintérminos corresponden a las configuraciones de entrada $x_1 = (0, 0, 1)$, $x_2 = (1, 0, 0)$ y $x_3 = (1, 0, 1)$ [7]. Cada mintérmino se implementa con una compuerta $C^3-\mathbf{NOT}$ generalizada, donde la condición de aplicación es el valor del x_i correspondiente, como se puede ver en la figura 1.18, y donde la disyunción de los mintérminos es la aplicación de las compuertas se-

x_1	x_0	x	x^2	x^2
0	0	0	0	0000
0	1	1	1	0001
1	0	2	4	0100
1	1	3	9	1001

Tabla 1.2. Tabla de verdad de $f(x) = x^2$ con dos qubits de entrada [7].

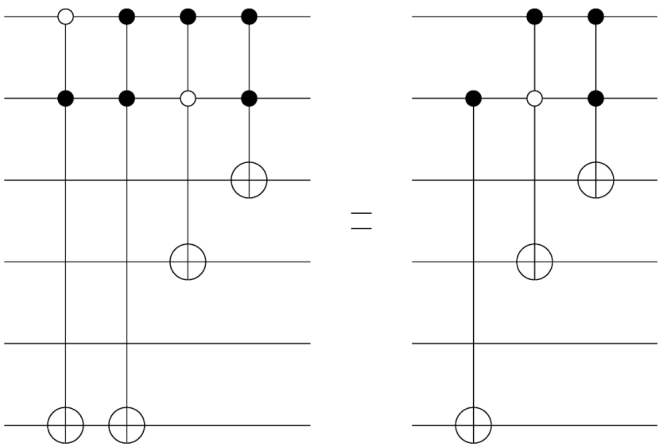

Figura 1.19. Diagrama de circuito para la evaluación de la función $f(x) = x^2$, elaborado por Benenti, Casati y Strini [7].

cuencialmente [7]. En esa misma figura se puede observar la simplificación de dos compuertas C^n-**NOT** generalizadas cuando solamente difieren en la condición de un qubit de control [7].

Otro ejemplo de evaluación de funciones es la implementación de $f(x) = x^2$ con entrada de 2 qubits [7]. Si un número entero $x \in [1, N]$ se puede almacenar en $n = \log_2 N$ qubits, en general el cuadrado del número se puede almacenar en $2n = \log_2 N^2$ qubits [7]. De esta manera, la tabla de verdad de la función es la tabla 1.2, por lo que se requieren 4 qubits auxiliares (preparados inicialmente como $|0\rangle$) para almacenar el resultado [7]. Tomando x^2 como una función diferente para cada qubit auxiliar, todas dependientes de los qubits de entrada, se pueden observar en la Tabla 1.2 los mintérminos de cada función: $(1, 1)$ para el primer qubit auxiliar, $(1, 0)$ para el segundo, ninguno para el tercero, y $(0, 1)$ y $(1, 1)$ para el cuarto [7]. Con esta información se puede armar el diagrama de circuitos de la figura 1.19, donde se utiliza la misma simplificación de circuitos que en la figura 1.18.

El paralelismo de la computación cuántica se puede observar con este ejemplo de x^2: si se ingresa el estado superpuesto

$$|\psi\rangle_{in} = \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)|0\rangle\,,$$

y se le aplica el circuito en la figura 1.19, se obtiene el resultado para todos los posibles valores de entrada [7]

$$|\psi\rangle_{out} = \frac{1}{2}\left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle + |2\rangle\,|4\rangle + |3\rangle\,|9\rangle\right).$$

En términos más generales, este paralelismo es

$$U_f \sum_{x=0}^{2^n-1} |x\rangle\,|y\rangle = \sum_{x=0}^{2^n-1} |x\rangle\,|y \oplus f(x)\rangle\,, \tag{1.27}$$

gracias a la linealidad de los operadores cuánticos [7].

1.4.2. El sumador cuántico

Una computadora debe ser capaz de realizar operaciones aritméticas elementales para poder llevar a cabo funciones avanzadas [7]. Una de estas funciones es la suma usual de dos números enteros a y b de n bits cada uno, que en notación binaria se escriben $a = a_{n-1}a_{n-2}\cdots a_1a_0$ y $b = b_{n-1}b_{n-2}\cdots b_1b_0$, $a_i, b_i \in \{0,1\}$ [7]. La suma se puede hacer como

$$|a,b\rangle \to |a,a+b\rangle\,, \tag{1.28}$$

donde b en la entrada es $b = 0b_{n-1}b_{n-2}\cdots b_1b_0$ para evitar desborde, y se utilizan qubits auxiliares para almacenar el acarreo [7]. La suma se realiza qubit por qubit, empezando por el qubit menos significativo (etiquetado con un 0) de cada registro: se inicia con un acarreo c_i determinado por la suma anterior, un a_i, un b_i y un $c_{i+1} = 0$ para almacenar el nuevo acarreo; la suma deja intactos c_i y a_i, almacena la suma $b_i \to s_i$ y el acarreo c_{i+1} para ser usado en la suma del siguiente conjunto de qubits [7]. La tabla de verdad 1.3 corresponde a este proceso, de donde se puede ver que las operaciones lógicas para cada parte del resultado son

$$s_i = a_i \oplus b_i \oplus c_i, \tag{1.29}$$

c_i	a_i	b_i	s_i	c_{i+1}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Tabla 1.3. Tabla de verdad de proceso de suma y su acarreo [7].

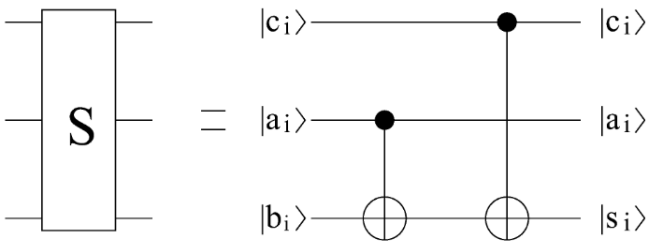

Figura 1.20. Diagrama de circuito para la evaluación de s_i de la Tabla 1.3, elaborado por Benenti, Casati y Strini [7].

y

$$c_{i+1} = (a_i \wedge b_i) \vee (c_i \wedge a_i) \vee (c_i \wedge b_i)\,. \tag{1.30}$$

La suma s_i, almacenada sobre $|b_i\rangle$, se puede construir solamente con compuertas **CNOT** entre esos tres qubits [7]. Por otro lado, el acarreo se define con las operaciones irreversibles de disyunción y conjunción, por lo que requiere un qubit auxiliar $|c_{i+1}\rangle$ (lo cual la vuelve una operación reversible) [7]. Las compuertas de suma **S** y de acarreo **C** se pueden observar en las figuras 1.20 y 1.21, respectivamente.

La construcción de la suma total requiere que el sumador aplique las compuertas **C** primero para obtener todos los c_i que requieren las compuertas **S**, aplicándolas sucesivamente desde el qubit *menos* significativo [7]. Una vez se completa la obtención de todos los acarreos se empiezan a aplicar las sumas sucesivamente, partiendo de los qubits *más* significativos, e intercalando con compuertas $\mathbf{C}^\dagger$ que reviertan la acción de las **C** tras el uso de c_i correspondiente [7]. Esta reversión permite que las compuertas **S** se apliquen con los datos esperados según la figura 1.20, y que los qubits auxiliares regresen a su estado original $|0\rangle$ [7]. En la figura 1.22 se puede observar este proceso en un diagrama de circuito.

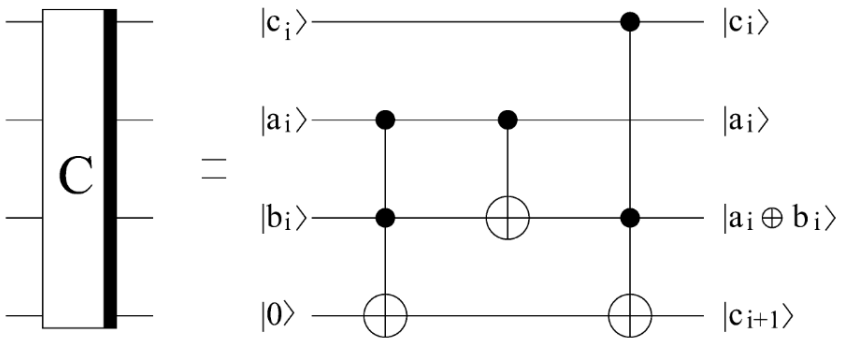

Figura 1.21. Diagrama de circuito para la evaluación de c_{i+1} de la Tabla 1.3, elaborado por Benenti, Casati y Strini [7].

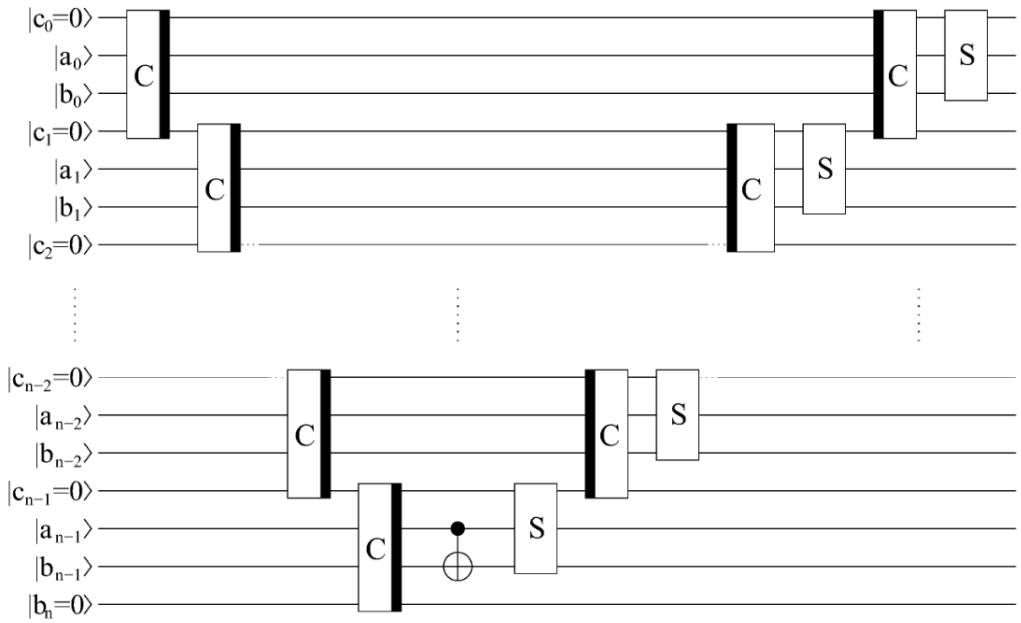

Figura 1.22. Diagrama de circuito para el sumador cuántico (de suma usual), elaborado por Benenti, Casati y Strini [7].

1.4.3. Algoritmo de Deutsch y algoritmo de Deutsch-Jozsa

El problema de Deutsch consiste en determinar si una función booleana,

$$f : \{0,1\} \to \{0,1\},$$

es constante (mismo valor de salida para todas las entradas) o balanceada (varía la salida según la entrada) [15]. El operador que aplica la función en cuestión se le llama oráculo, y se le trata como una caja negra [15]. La versión clásica de este problema requiere que el oráculo sea usado dos veces, una vez para cada posible valor de entrada [15]. El algoritmo de Deutsch permite realizar la determinación con una sola evaluación del oráculo [15].

El oráculo se aplica sobre dos qubits, actuando como

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle,$$

con $|x\rangle$ como principal y $|y\rangle$ como auxiliar [15]. Para poder determinar el tipo de función con una sola evaluación, se debe usar la propiedad de interferencia cuántica, lo cual requiere utilizar compuertas de Hadamard [15]. El qubit auxiliar se prepara en el estado inicial $|1\rangle$ y se le aplica una compuerta de Hadamard

$$|x\rangle (H |1\rangle) = |x\rangle |-\rangle = \frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle).$$

Al ser evaluado por el oráculo, este estado evoluciona a

$$U_f |x\rangle |-\rangle = \frac{1}{\sqrt{2}} |x\rangle [|f(x)\rangle - |1 \oplus f(x)\rangle],$$

por lo que el estado $|-\rangle$ puede conservar su signo o cambiarlo dependiendo del valor de $f(x)$

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

de manera que la fase del qubit auxiliar se ha *propagado hacia atrás*, hacia el qubit principal [15]. Si el qubit principal es preparado inicialmente en $|0\rangle$, y se le aplica una compuerta de Hadamard, este llega al oráculo como $|+\rangle$ [15]. De esta manera, la acción del oráculo es

$$U_f |+\rangle |-\rangle = \frac{1}{2} U_f (|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2} \left[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle\right](|0\rangle - |1\rangle),$$

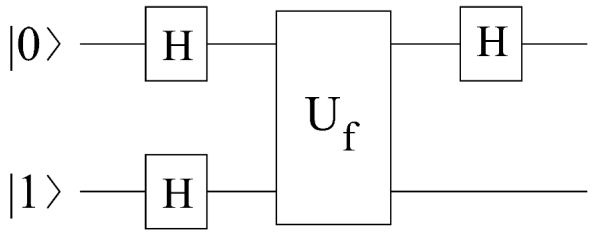

Figura 1.23. Diagrama de circuito para el algoritmo de Deutsch, elaborado por Benenti, Casati y Strini [7].

con lo que, ignorando una fase global, hay dos opciones: si la función es constante, el qubit principal quedará $|+\rangle$; si es balanceada, quedará $|-\rangle$ [15]. Aplicando una compuerta de Hadamard sobre el primer qubit, esto se transforma a la base computacional en la que se realizará la medición: $|0\rangle$ para una función constante, y $|1\rangle$ para una función balanceada [15]. El diagrama de circuito en este algoritmo se puede apreciar en la figura 1.23.

El problema de Deutsch y su solución son un caso particular del problema de Deutsch-Jozsa, que es el mismo problema, pero con una función cuyo dominio es un registro de n qubits

$$f : \{0,1\}^n \to \{0,1\},$$

y se debe determinar si la función es constante, o si es balanceada (produce una salida 0 para la mitad de las entradas, y 1 para la otra mitad) con una sola evaluación en el oráculo que aplica la función [9]. Aquí, como en el algoritmo de Deutsch, se requiere de un bit auxiliar preparado en el estado $|1\rangle$, y el registro principal debe iniciar en el estado $|0\rangle^{\otimes n}$, donde el exponente $\otimes n$ denota un producto tensorial de n estados iguales [9]. Esta misma notación es aplicable a operadores, donde $U^{\otimes n}$ significa el operador U aplicado de la misma manera sobre cada uno de los estados individuales de un producto tensorial de n estados [9]. Ahora, para iniciar se aplica una compuerta de Hadamard H sobre el qubit auxiliar y una $H^{\otimes n}$ sobre el registro principal, con lo que se obtiene

$$\left(H^{\otimes n}|0\rangle^{\otimes n}\right)(H|1\rangle) = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

donde $x \in \{0,1\}^n$ significa que x toma todos los posibles valores de eigenestados del espacio de Hilbert total del registro principal (equivalente a la notación $\sum_{x=0}^{2^n-1}$) [9].

Ahora, como en el problema de Deutsch, el oráculo ejecuta la acción

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle ,$$

donde x es el registro principal de n qubits y y es el qubit auxiliar [9]. Entonces, como con $n = 1$, se tiene que el qubit auxiliar en estado $|-\rangle$ puede conservar su signo o cambiar, dependiendo del valor que tome x y de la naturaleza de $f(x)$ [9]. Entonces, la aplicación de U_f sobre el estado total del sistema tras las compuertas de Hadamard produce una propagación hacia atrás del signo final de $|-\rangle$ hacia el eigenestado $|x\rangle$ específico que provocó la aparición de dicho signo

$$U_f \sum_{x\in\{0,1\}^n} \frac{\left|x\right\rangle}{\sqrt{2^n}} \left(\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right) = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)} \left|x\right\rangle}{\sqrt{2^n}} \left(\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right).$$

El siguiente paso es aplicar otra compuerta $H^{\otimes n}$ sobre el registro principal [9]. Esta compuerta, actuando sobre un solo eigenestado del registro provoca

$$H^{\otimes n} \left|x\right\rangle = \sum_{z\in\{0,1\}^n} \frac{(-1)^{x_0 z_0 \oplus \ldots \oplus x_{n-1} z_{n-1}} \left|z\right\rangle}{\sqrt{2^n}} = \sum_{z\in\{0,1\}^n} \frac{(-1)^{x\cdot z} \left|z\right\rangle}{\sqrt{2^n}}.$$

La acción de esta compuerta sobre el estado total tras aplicar el oráculo es

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

En este punto se debe analizar únicamente el estado del registro principal

$$\sum_{x,z\in\{0,1\}^n} \frac{(-1)^{x\cdot z + f(x)} \left|z\right\rangle}{\sqrt{2^n}}.$$

Si se toma el estado $|z\rangle = |0\rangle^{\otimes n}$ (fijar el valor de z, con una sumatoria sobre x), se observa que el factor de signo es $(-1)^{x\cdot z + f(x)} = (-1)^{f(x)}$, dependiente únicamente de la función que se está investigando [9]. Una función constante causaría que el estado $|0\rangle^{\otimes n}$ se sumara 2^n veces con el mismo signo, de manera que se tendría que el coeficiente de $|0\rangle^{\otimes n}$ es ± 1, es decir, su probabilidad de ser medido es del 100 % [9]. Por otro lado, si la función es balanceada, el estado $|0\rangle^{\otimes n}$ se sumará con un signo en la mitad de la sumatoria, y se sumará con el signo opuesto la otra mitad, efectivamente borrándose del resultado, es decir, un 0 % de probabilidades de aparecer [9].

De esto se tiene que, para un registro de n qubits principales con un qubit auxiliar, el algoritmo de Deutsch-Jozsa arroja una medición final del registro principal con exactamente dos posibilidades: si se obtiene el estado $|0\rangle^{\otimes n}$, la función es constante; cualquier otro resultado implica que la función es balanceada [9]. El diagrama de circuito del algoritmo solución es idéntico al que se encuentra en la figura 1.23, pero todo lo referente al qubit principal pasa a corresponder a un registro de n qubits [9]. La única forma en la que un algoritmo clásico puede determinar la naturaleza de $f(x)$ con total certeza requiere de $2^{n-1}+1$ evaluaciones del oráculo [9].

Los algoritmos de Deutsch y de Deutsch-Jozsa fueron los primeros en demostrar una clara ventaja de la computación cuántica sobre la clásica [15].

1.4.4. Transformada de Fourier cuántica

La transformada de Fourier es una transformación lineal unitaria que cambia la representación de un vector [9]. En el caso de un vector definido por componentes, la transformación es discreta y se define como

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i}{N} jk} x_j, \tag{1.31}$$

en donde se está realizando la transformación de un vector de longitud N y de componentes complejas $(x_0, \ldots, x_{N-1})$ hacia uno de la misma longitud y componentes $(y_0, \ldots, y_{N-1})$, obteniéndose cada componente por separado [9]. La versión cuántica de esta transformación realiza lo mismo sobre vectores de estado cuántico [9]. Sobre un elemento de la eigenbase $\{|0\rangle, ..., |N-1\rangle\}$, la transformada de Fourier realiza

$$F\left(|j\rangle\right) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle, \tag{1.32}$$

y sobre un vector arbitrario en esa misma base, realiza

$$F\left(\sum_{j=0}^{N-1} x_j |j\rangle\right) = \sum_{k=0}^{N-1} y_k |k\rangle$$

donde y_k está definida según la ecuación (1.31) [9].

Trabajando con n qubits, se tiene que $N = 2^n$, y los números enteros en notación binaria son $j = j_1 j_2 \dots j_n$, con j_n el dígito menos significativo [9]. Los números decimales en notación binaria se expresan como

$$0.j_l j_{l+1} \dots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \dots + \frac{j_m}{2^{m-l+1}}. \tag{1.33}$$

Usando esta notación, se puede factorizar la transformada de Fourier de un eigenestado $|j\rangle$ (lo cual implica que no produce estados entrelazados) [9]

$$F(|j\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i}{2^n} jk} |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1,\dots,k_n=0}^{1} e^{2\pi i\left(j \sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \dots k_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1,\dots,k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i\left(j k_l 2^{-l}\right)} |k_l\rangle$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi i\left(j k_l 2^{-l}\right)} |k_l\rangle$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle\right)$$

$$F(|j\rangle) = \frac{\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n} |1\rangle\right)}{\sqrt{2^n}}. \tag{1.34}$$

Esta factorización permite ver que la transformada de Fourier se puede aplicar con compuertas de Hadamard y **CPHASE**, donde la rotación condicionada está dada por [9]

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}. \tag{1.35}$$

Aplicando la compuerta de Hadamard sobre el qubit más significativo $|j_1\rangle$, se tiene el estado

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.j_1} |1\rangle\right) |j_2 \dots j_n\rangle .$$

Sobre este mismo estado se aplica una compuerta **CPHASE** dependiente de j_2 y

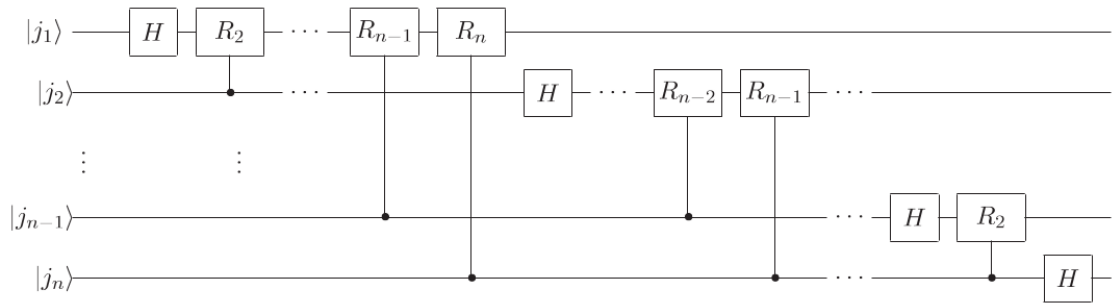

Figura 1.24. Diagrama de circuito para la transformada de Fourier cuántica, elaborado por Nielsen y Chuang [9].

rotación R_2 según lo definido en la ecuación (1.35), dando

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}\,|1\rangle\right)|j_2 \ldots j_n\rangle\,.$$

Este proceso continúa con compuertas **CPHASE**, cada una dependiente del siguiente qubit y aumentando de uno en uno el k en R_k, hasta llegar a una rotación R_n dependiente del qubit menos significativo $|j_n\rangle$ [9]. El siguiente qubit, $|j_2\rangle$, se le aplica H y luego se le aplican sucesivamente rotaciones condicionadas, empezando por R_2 condicionada a $|j_3\rangle$ hasta llegar a R_{n-1} condicionada a $|j_n\rangle$ [9]. Todo este proceso se aplica secuencialmente a cada qubit, hasta llegar a los qubits menos significativos: a $|j_{n-1}\rangle$ se le aplica H y R_2 condicionada a $|j_n\rangle$, y a $|j_n\rangle$ sólo se le aplica H [9]. La aplicación de las compuertas en el orden detallado se ilustra como diagrama de circuito en la figura 1.24.

El algoritmo de la figura 1.24 arroja el estado final

$$\frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}\,|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}\,|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_n}\,|1\rangle\right),$$

que está multiplicado (como tensores) en el orden inverso al resultado deseado de la ecuación (1.34), de manera que el resultado tiene invertido el orden de significancia de los qubits [9]. Esto se corrige con compuertas **SWAP** descritas en la sección 1.2.2, una compuerta entre cada par de qubits $|j_l\rangle$ y $|j_{n-l+1}\rangle$ [9].

Los mejores algoritmos clásicos para calcular la transformada de Fourier discreta utiliza compuertas cuyo número aumenta según $O\left(n^2 2^n\right)$ [9]. La transformada de Fourier cuántica, contando las compuertas **SWAP** como combinaciones de com-

puertas **CNOT**, aumenta con el tamaño n del registro según $O(n^2)$, que es una mejora exponencial respecto del algoritmo clásico [9]. Sin embargo, se debe notar que el resultado de la transformada de Fourier cuántica produce un estado superpuesto, por lo que no es posible obtener toda la información de la transformación con una medición del registro [9].

1.5. Aplicaciones

1.5.1. Búsqueda cuántica: Algoritmo de Grover

El problema de búsqueda consiste en identificar un elemento marcado dentro de una base de datos sin estructura con $N = 2^n$ elementos [7]. Esto se puede replantear como el problema del oráculo: con los elementos de la base de datos etiquetados $\{0, 1, \ldots, N-1\}$, el elemento marcado es x_0 y el oráculo aplica una función

$$f : \{0,1\}^n \to \{0,1\},$$

tal que

$$f(x) = \begin{cases} 1, & x = x_0 \\ 0, & x \neq x_0 \end{cases}. \tag{1.36}$$

Lo que se quiere es encontrar el elemento etiquetado con x_0 con el menor número de evaluaciones posibles al oráculo [7]. Clásicamente, para encontrar x_0 con una probabilidad de éxito p, se requieren $pN = O(N)$ evaluaciones del oráculo [7].

El algoritmo de Grover para resolver este problema en computación cuántica inicia con el registro de entrada preparado en el estado base $|0\rangle$ de N qubits, y un qubit auxiliar en $|1\rangle$ [7]. Como en el algoritmo de Deutsch-Jozsa, se utilizan compuertas de Hadamard para que la aplicación del oráculo se almacene en la propagación hacia atrás de la fase global del qubit auxiliar [7]. Entonces, se comienza aplicando las compuertas de Hadamard

$$H^{\otimes n+1} |0\rangle |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |-\rangle .$$

Al aplicar el oráculo sobre este estado, actúa la propagación hacia atrás de la fase

y se obtiene

$$O\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\,|-\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\,|x\rangle\,|-\rangle\,,$$

donde $f(x)$ corresponde a lo definido en la ecuación (1.36).

En general, este problema no se puede resolver con una sola evaluación del oráculo; se requiere entonces realizar, sobre el mismo registro, múltiples aplicaciones de la *iteración de Grover*

$$G = DO,$$

donde O es el operador asociado al oráculo, y D es

$$D = H^{\otimes n}\left(-I + 2\,|0\rangle\langle 0|\right)H^{\otimes n} = H^{\otimes n}D'H^{\otimes n}. \tag{1.37}$$

Ese operador D' entre las compuertas de Hadamard es una especie de desplazamiento de fase condicionado, que aplica un -1 a todos los estados excepto $|0\rangle$ [7]. La búsqueda cuántica consiste en aplicar la iteración de Grover hasta que una medición aplicada sobre el registro tenga una alta probabilidad de resultar en x_0 [7].

Para entender como funciona el algoritmo, se debe realizar una visualización geométrica: el operador del oráculo actúa como

$$O : |x\rangle \to (-1)^{f(x)}\,|x\rangle\,,$$

con la función $f(x)$ definida en (1.36), de manera que el operador se expresa como

$$O = I - 2\,|x_0\rangle\langle x_0| = R_{|x_0\rangle}, \tag{1.38}$$

esto es, una reflexión respecto del hiperplano perpendicular a $|x_0\rangle$ [7]. Si se toma un vector bidimensional $|\psi\rangle = \alpha\,|x_0\rangle + \beta\left|x_0^{\perp}\right\rangle$ (donde $\left|x_0^{\perp}\right\rangle$ es el vector total formado por la superposición de todos los eigenestados que no son $|x_0\rangle$), el oráculo produce $O\,|\psi\rangle = -\alpha\,|x_0\rangle + \beta\left|x_0^{\perp}\right\rangle$, es decir, ha reflejado a $|\psi\rangle$ respecto del eje $\left|x_0^{\perp}\right\rangle$, es decir, el plano perpendicular a $|x_0\rangle$ [7].

Ahora, tomando en cuenta que la compuerta de Hadamard es hermítica, el operador D queda como

$$D = H^{\otimes n}\left(-I + 2\,|0\rangle\langle 0|\right)H^{\otimes n} = -I + 2\,|S\rangle\langle S| = -R_{|S\rangle}, \tag{1.39}$$

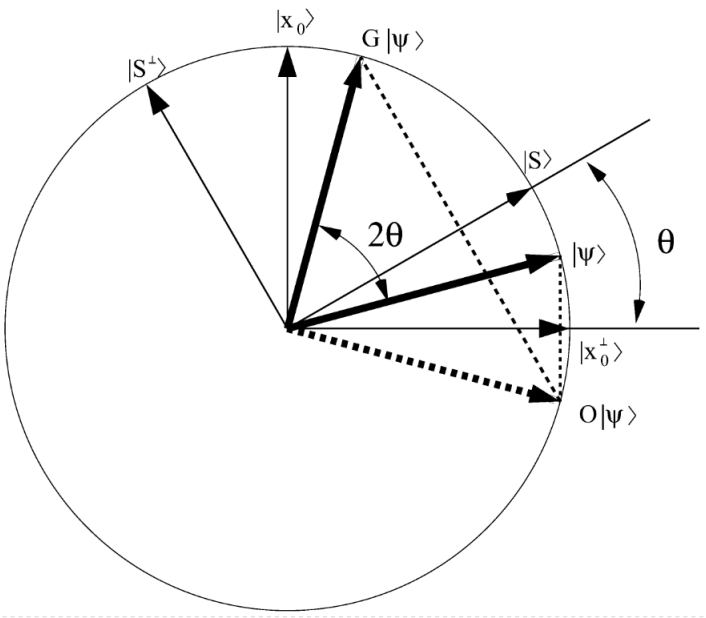

Figura 1.25. Visualización geométrica de la iteración de Grover, elaborado por Benenti, Casati y Strini [7].

el negativo de una reflexión respecto del hiperplano perpendicular a $|S\rangle$, con

$$|S\rangle = H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle .$$

De esta manera, la iteración de Grover es

$$G = DO = -R_{|S\rangle} R_{|x_0\rangle}.$$

Se define el vector $|u\rangle = \mu|S\rangle + \nu\left|S^{\perp}\right\rangle$ [7]. Entonces, se aplica la reflexión

$$-R_{|S\rangle}|u\rangle = -\left(-\mu|S\rangle + \nu\left|S^{\perp}\right\rangle\right) = \mu|S\rangle - \nu\left|S^{\perp}\right\rangle = R_{\left|S^{\perp}\right\rangle}|u\rangle$$

de modo que $-R_{|S\rangle} = R_{\left|S^{\perp}\right\rangle}$ [7]. Usando este resultado, se tiene la iteración de Grover como

$$G = -R_{|S\rangle} R_{|x_0\rangle} = R_{\left|S^{\perp}\right\rangle} R_{|x_0\rangle}. \tag{1.40}$$

Si se tiene que el ángulo entre $\left|x_0^{\perp}\right\rangle$ y $|S\rangle$ es θ, entonces el efecto de G sobre un vector genérico en este plano es rotarlo un ángulo 2θ, lo cual es representado visualmente en la figura 1.25.

Tras la primera aplicación de $H^{\otimes n}$, el registro se encuentra en un estado que

puede escribirse con la base $\left\{|x_0\rangle, \left|x_0^{\perp}\right\rangle\right\}$

$$|\psi_0\rangle = |S\rangle = \sin\theta\,|x_0\rangle + \cos\theta\left|x_0^{\perp}\right\rangle,$$

de manera que la aplicación sucesiva de la iteración de Grover produce el estado

$$|\psi_j\rangle = G^j\,|\psi_0\rangle = \sin\left[(2j+1)\theta\right]|x_0\rangle + \cos\left[(2j+1)\theta\right]\left|x_0^{\perp}\right\rangle.$$

Entonces, se puede ver que la cantidad j de iteraciones de Grover necesarias para que medir $|x_0\rangle$ sea altamente probable, son las que cumplen $\sin\left[(2j+1)\theta\right] \approx 1$ (o tan cerca como sea posible), es decir

$$(2j+1)\theta \approx \frac{\pi}{2},$$

por lo que la cantidad j de iteraciones de Grover, redondeando al número entero más cercano, que se requieren para completar la búsqueda es [7]

$$j \approx \frac{\pi}{4\theta} - \frac{1}{2}. \tag{1.41}$$

Como el estado $|\psi_0\rangle$ es la superposición uniforme $|S\rangle$, donde cada estado base tiene la misma probabilidad de ser medido, se puede determinar que

$$\sin\theta = \langle\psi_0|x_0\rangle = \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}}.$$

Si N es muy grande,

$$\sin\theta \approx \theta \approx \frac{1}{\sqrt{N}},$$

y la cantidad requerida de iteraciones de Grover es entonces

$$j \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2},$$

que implica $O\left(\sqrt{N}\right)$ evaluaciones del oráculo, una mejora cuadrática respecto a las $O(N)$ requeridas por el algoritmo clásico [7]. Al terminar de aplicar G^j, se realiza una medición del registro $|x\rangle$ en la base computacional, lo cual arrojará la medida $\bar{x}$ [7]. El estado colapsado $|\bar{x}\rangle$ es pasado por el oráculo una vez más: si este arroja $f(\bar{x}) = 1$, la búsqueda fue exitosa. Si la función se evalúa a 0, entonces falló [7]. La probabilidad de fracaso del algoritmo se reduce proporcionalmente a $1/N$, por lo que el éxito es altamente probable [7].

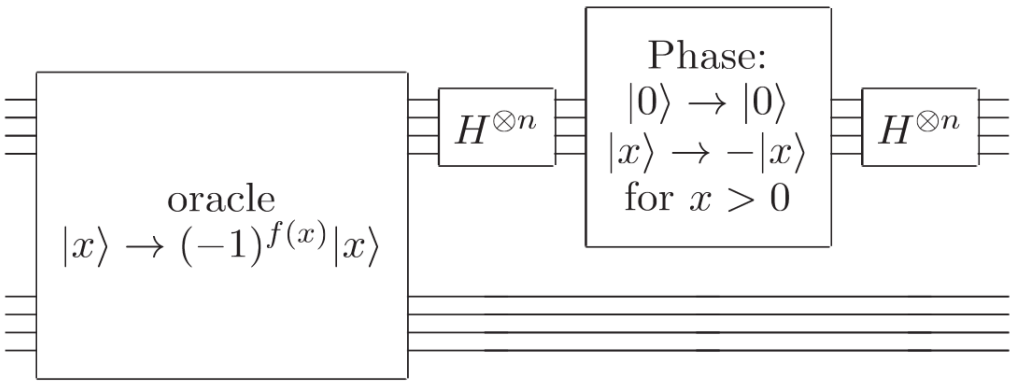

Figura 1.26. Diagrama de circuito de una iteración de Grover general, elaborado por Nielsen y Chuang [9].

En la figura 1.26 se presenta un diagrama de circuito para una iteración de Grover general.

1.5.1.1. Ejemplo: búsqueda entre 4 elementos

De lo visto en la explicación previa, la búsqueda entre $N = 4$ elementos se hace con dos qubits principales, donde los elementos entre los que se busca son los 4 estados base del espacio de Hilbert total de este registro, en la base computacional; también se utiliza un qubit auxiliar [7]. Según lo determinado para el caso general, para el estado $|\psi_0\rangle$ se tiene que $\sin\theta = 1/\sqrt{4} = 1/2$, de manera que

$$\theta = \frac{\pi}{6}.$$

Insertando este resultado en la ecuación (1.41), se tiene que para esta búsqueda se requiere realizar solamente $j = 1$ iteración de Grover [7]. El operador D de la matriz de Grover está dado por

$$D = H^{\otimes 2}\left(-I_{4\times 4} + 2\,|00\rangle\langle 00|\right) H^{\otimes 2} = H^{\otimes 2} D' H^{\otimes 2},$$

de manera que

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

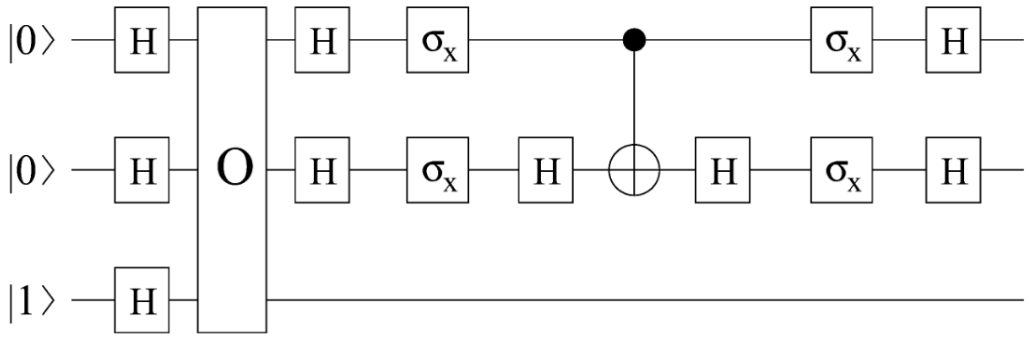

Figura 1.27. Diagrama de circuito del algoritmo de Grover para el caso $N = 4$, elaborado por Benenti, Casati y Strini [7].

lo cual se construye con compuertas universales como

$$D' = \sigma_x^{\otimes 2} (I \otimes H) \, \mathbf{CNOT} \, (I \otimes H) \, \sigma_x^{\otimes 2}.$$

La reflexión D completa queda con la representación matricial [7]

$$D = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix},$$

El estado al iniciar el circuito, incluyendo el qubit auxiliar, es $|00\rangle\,|1\rangle$. A este estado se le aplica $H^{\otimes 3}$, quedando [7]

$$\frac{1}{2} \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right) |-\rangle = \frac{1}{2} \left(|0\rangle + |1\rangle + |2\rangle + |3\rangle \right) |-\rangle .$$

El oráculo, aplicando la función (1.36), pondrá un signo $(-)$ frente a uno de los estados base del registro principal, $|x_0\rangle$ [7]. El efecto del operador D, sobre este registro es entonces

$$D \frac{1}{2} \begin{bmatrix} (-1)^{f(0)} \\ (-1)^{f(1)} \\ (-1)^{f(2)} \\ (-1)^{f(3)} \end{bmatrix} = \begin{bmatrix} \delta_{f(x_0)f(0)} \\ \delta_{f(x_0)f(1)} \\ \delta_{f(x_0)f(2)} \\ \delta_{f(x_0)f(3)} \end{bmatrix}.$$

De esta manera, esa única iteración de Grover ha dejado el registro en el estado correspondiente al elemento buscado, y se tiene un 100 % de probabilidad de éxito [7]. El diagrama de circuito de este algoritmo está en la figura 1.27.

1.5.1.2. El oráculo

El uso del oráculo como una caja negra tiene la apariencia de un atajo para evitar hacer el trabajo de analizar una parte importante del problema de búsqueda; de primera impresión, pareciera que el oráculo *sabe* cuál es la solución, y el algoritmo de búsqueda queda reducido a una caja negra [9]. Sin embargo, como se puede observar en la discusión sobre el algoritmo de Grover, aun con un oráculo de caja negra el problema no es trivial: una vez el oráculo marcó el elemento que se busca, es necesario realizar un algoritmo para *saber* cuál es el elemento marcado [9]. El oráculo en realidad no tiene la capacidad de *saber* la respuesta al problema de búsqueda, solamente tiene la capacidad de *reconocer* la respuesta correcta y marcarla [9].

Como ejemplo, un método obvio para buscar factores primos de un número m que sea producto de sólo dos primos es dividirlo entre todos los números enteros en el intervalo $\left[2, m^{1/2}\right]$, de manera que en algún punto se obtendrá el factor primo más pequeño, que a su vez permitirá encontrar el otro factor (hay algoritmos clásicos más eficientes que eso, pero eso es irrelevante para este ejemplo) [9]. Un oráculo se puede construir de manera que divida m entre todos los números x que son ingresados como estados de un registro cuántico, y que aplique un desplazamiento de fase sobre el eigenestado que no produce residuo de división [9]. En ese punto todavía es necesario extraer esta información del registro, a través de la conversión este desplazamiento de fase en algo mensurable [9].

De esta manera se entiende que en el algoritmo de Grover el oráculo sólo se trabaja como una caja negra, ya que este puede ser la resolución de un problema en sí mismo en el que la respuesta queda marcada dentro de un estado superpuesto, necesitando del algoritmo de búsqueda para poder conocer la solución de dicho problema [9].

1.5.2. El algoritmo de Shor

Una de las principales formas de encriptación moderna es la RSA (en honor a Rivest, Shah y Adelman), que está basada en la conjetura de que la factorización de números muy grandes hacia sus factores primos no se puede realizar con recursos clásicos humanamente disponibles, y estos factores son necesarios para descifrar la información encriptada [15]. Hasta ahora, esta conjetura no ha sido refutada [15]. Sin embargo, las propiedades de la computación cuántica abren la posibilidad de

realizar muchas tareas computacionales con recursos mucho menores respecto a la computación clásica; en el caso del problema de los factores primos, la reducción de recursos es exponencial (de $O\left(e^{n^{1/3}(\log n)^{2/3}}\right)$ para el mejor algoritmo clásico hacia $O\left(n^2 \log n \log\log n\right)$ para el cuántico [7]), y el algoritmo que realiza esta tarea es el *algoritmo de Shor*, creado por el matemático aplicado Peter Shor [15].

El problema de factorizar un número se puede reducir a encontrar uno de sus factores [15]. Con un factor del número, el número original se divide, y se vuelve a tener el problema de factorización, pero con un número más pequeño [15]. Para encontrar un factor de un número N, el algoritmo de Shor busca el período r de la función

$$f(x) = a^x \mod N, \tag{1.42}$$

que significa, el residuo de la división entera a^x/N. De la teoría clásica de números se sabe que con r se pueden obtener dos factores primos de N [15]. En términos generales, los pasos del algoritmo de Shor son [15]

1. Elegir al azar un número entero a tal que $a < N$.

2. Calcular $\gcd(a, N)$, el máximo común divisor de ambos números.

3. Si $\gcd(a, N) \neq 1$, a y N no son *relativamente primos*, y a es un factor no trivial de N, lo que resuelve el problema.

4. De otra manera, se debe encontrar el período r de la función (1.42) con a y N los números que se usaron en los pasos anteriores.

5. Si r es impar, o si se cumple $a^{r/2} = -1 \pmod N$ (que significa $a^{r/2} \mod N = -1 \mod N$), el algoritmo falló y se debe empezar de nuevo.

6. Si no es así, la teoría clásica de números estipula que $\gcd\left(a^{r/2}+1, N\right)$ y $\gcd\left(a^{r/2}-1, N\right)$ son factores no triviales de N.

La definición de r es la definición común de período, $f(x) = f(x+kr)$ con $k \in \mathbb{Z}$ [15]. Por ejemplo, en la función $f(n) = 2^n \mod 91$, el primer valor es $f(0) = 1$; este valor se repite en $f(12) = 1$, a partir de donde se vuelven a repetir los valores para $n = 1, 2, 3, \ldots$. Entonces, el período de dicha función es 12 [15].

1.5.2.1. El período de una función

Para encontrar el período, se requieren dos registros, uno para almacenar una superposición igualitaria de estados que provee los valores x y otro para almacenar los valores tomados por la función $f(x)$ cuyo período se quiere encontrar (se asume que existe un r tal que $f(x + kr) = f(x)$ con $k \in \mathbb{Z}$) [7]. Por simplicidad se asume $2^n/r = m \in \mathbb{Z}$ con n el tamaño del primer registro (el caso general agrega algunas complicaciones que no invalidan las ideas generales al respecto del algoritmo) [7].

Utilizando compuertas de Hadamard y las transformaciones unitarias condicionadas apropiadas, se produce el estado

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

donde $f(x)$ es la función cuyo período se está buscando, y que corresponde a (1.42) en el algoritmo de Shor [7]. En este estado ambos registros han quedado entrelazados, de manera que al realizar una medición sobre el segundo registro se obtiene un resultado $f(x_0)$, y un estado total

$$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle \, |f(x_0)\rangle \,,$$

donde el segundo registro se puede factorizar e ignorar [7]. Ahora se realiza aplica la transformada de Fourier cuántica sobre el primer registro

$$\frac{1}{\sqrt{m2^n}} \sum_{j=0}^{m-1} \sum_{k=0}^{2^n-1} e^{2\pi i(x_0+jr)k/2^n} \, |k\rangle \,,$$

lo cual, tras eliminación de términos por sumas y restas, queda

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i x_0 k/r} \left| k\frac{2^n}{r} \right\rangle . \tag{1.43}$$

Aquí la interferencia de estados cuánticos ha seleccionado un conjunto de frecuencias específicas. Sobre este último estado se realiza una medición, que arrojará un valor $k2^n/r = c$ [7]. Entonces, se tiene

$$\frac{c}{2^n} = \frac{\lambda}{r},$$

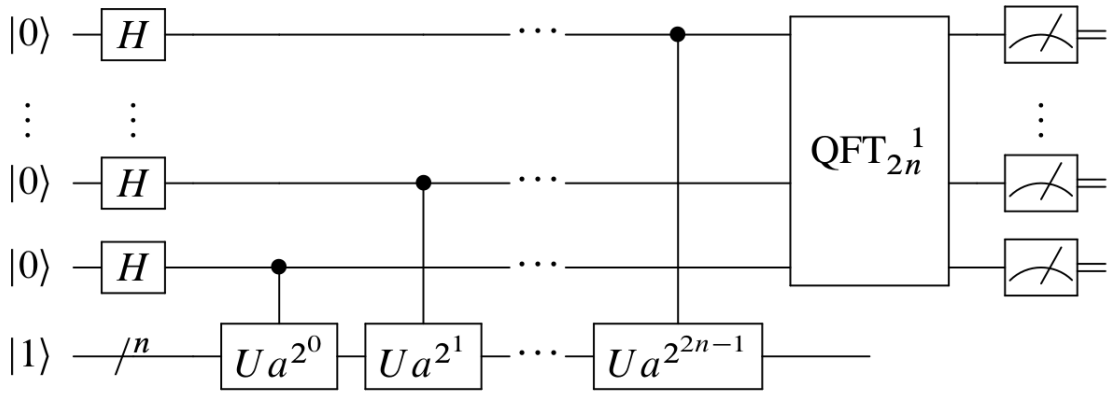

Figura 1.28. Diagrama de circuito de algoritmo de período de una función del algoritmo de Shor, elaborado por Hidary [15].

con $\lambda \in \mathbb{Z}$ desconocido [7]. Existe una probabilidad de al menos $1/\log\log r$ de que λ y r no tengan factores comunes, en cuyo caso la fracción irreducible de c/N provee los valores de λ y r. Si no es así, el algoritmo fracasa [7]. La probabilidad de éxito del algoritmo crece hacia 1 tras un número $O(\log\log n)$ de ejecuciones [7].

En la figura 1.28 aparece un diagrama de circuito para el proceso de determinación de período del algoritmo de Shor. En ella se incluye una representación de la aplicación de $f(x)$ sobre el registro auxiliar como operaciones unitarias condicionadas al registro principal.

Como ejemplo, se tiene la función

$$f(x) = \frac{1}{2}\left[\cos(\pi x) + 1\right],$$

cargada en un registro de 3 qubits ($2^n = 2^3 = 8$) [7]. Esta función solo arroja 0 para x par, y 1 para x impar, por lo que el resultado se puede almacenar en un solo qubit [7]. Se inicia con el estado $|000\rangle|0\rangle$, que tras pasar por las compuertas $H^{\otimes 3}$ y por la evaluación de la función, arroja

$$\frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x\rangle|f(x)\rangle.$$

Al realizar la medición del segundo registro, si este da $|0\rangle$ el estado total colapsa a

$$\frac{1}{2}\left(|1\rangle + |3\rangle + |5\rangle + |7\rangle\right)|0\rangle.$$

La transformada de Fourier realiza

$$|x\rangle \rightarrow \frac{1}{\sqrt{8}} \sum_{k=0}^{7} e^{2\pi i x k/8} |k\rangle ,$$

y en el estado total se eliminan por interferencia todos los estados base excepto

$$\frac{1}{\sqrt{2}} (|0\rangle - |4\rangle) .$$

Ahora se realiza la medición del registro. Si se obtiene $|0\rangle$, el algoritmo falla y hay que repetirlo [7]. Si se obtiene $|4\rangle$, entonces $c/2^n = 4/8 = 1/2 = \lambda/r$, y se ha obtenido el período de la función $r = 2$ [7].

1.5.2.2. Máximo común divisor: el algoritmo de Euclides

Para encontrar el máximo común divisor de dos números existe un algoritmo diseñado por Euclides [9]. Para utilizarlo, primero se requiere saber que

$$\gcd(a, b) = \gcd(b, r), \tag{1.44}$$

donde $r = a \mod b$ [9]. Usando este conocimiento, el algoritmo de Euclides con los números enteros a y b es como sigue: [9]

1. Ordenar los números de manera que $a > b$.
2. Hacer la división a/b con resultado entero k_1 y residuo r_1, de manera que $a = k_1 b + r_1$.
3. Realizar b/r_1, para obtener $b = k_2 r_1 + r_2$.
4. Realizar r_1/r_2 para obtener $r_1 = k_3 r_2 + r_3$.
5. Repetir hasta que el residuo obtenido sea 0, de manera que $\gcd(r_m, r_{m+1}) = r_{m+1}$.
6. Dada la propiedad descrita en (1.44), se tiene

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_m, r_{m+1}) = r_{m+1}. \tag{1.45}$$

Computacionalmente, este algoritmo tiene un costo de recursos de $O(n^3)$, donde n es el tamaño en bits de a [9]. De esta manera, una vez se ha hallado cuánticamente

el período r de la función $f(x)$ del algoritmo de Shor, se pueden ejecutar clásicamente en tiempo polinomial las operaciones $\gcd\left(a^{r/2}+1, N\right)$ y $\gcd\left(a^{r/2}-1, N\right)$, obteniéndose factores no triviales de N [15].

1.5.3. Complejidad computacional

El planteamiento teórico que define y delimita la computación clásica respecto de la Máquina Universal de Turing es la tesis de Church-Turing, que en su planteamiento original estipula [15]

> Si un algoritmo puede ejecutarse en alguna pieza de hardware, entonces existe un algoritmo equivalente para una Máquina Universal de Turing (MUT) que ejecuta exactamente el mismo algoritmo.

Para tomar en cuenta la eficiencia de los algoritmos, esta proposición se modificó hacia la versión fuerte de la tesis, que establece [15]

> Cualquier proceso algorítmico puede simularse eficientemente en una MUT.

Esto quiere decir que la MUT puede simular en tiempo polinomial cualquier máquina que ejecute algoritmos [9]. Esta versión de la tesis resulta refutada por algoritmos que utilizan números aleatorios para obtener soluciones; algunos de estos algoritmos realizan tareas más rápido que sus contrapartes deterministas, y tienen altas probabilidades de éxito [15]. Por estas razones, se propuso la versión extendida de la tesis de Church-Turing: [15]

> Cualquier proceso algorítmico puede ser simulado eficientemente en una Máquina de Turing Probabilística.

La capacidad de la computación cuántica de resolver problemas exponencialmente más rápido que cualquier computadora cuántica rompe con esta versión extendida [15]. Entonces se arriba a la versión cuántica extendida de la tesis de Church-Turing, que dice [15]

> Cualquier aparato computacional realista puede ser eficientemente simulado por una computadora cuántica tolerante a fallos.

La existencia de la computación cuántica y las propiedades que la diferencian de la computación clásica ampliaron el estudio de la complejidad computacional, llevando a la creación de nuevas categorías de complejidad y al ajuste de la tesis de Church-Turing [15]. Las principales clases de complejidad computacional que se relacionan con ambos tipos de computación son [15]

- **P -** Tiempo polinomial: problemas que pueden ser resueltos en tiempo polinomial, es decir, que conforme crece el tamaño de la entrada del problema, el tiempo de resolución máximo para el peor escenario no supera un crecimiento polinomial.

- **NP -** Tiempo polinomial no-determinista: ante la solución de un problema, un algoritmo puede verificar si la respuesta es correcta o incorrecta en un tiempo polinomial. Determinar si la clases **P** y **NP** son equivalentes entre sí es uno de los *Problemas del Milenio* establecidos por el Instituto Clay de Matemáticas, 7 problemas matemáticos de los cuales 6 siguen sin ser resueltos (sólo la conjetura de Poincaré ha sido probada) y cuyas soluciones serán premiadas con 1 millón de dólares americanos cada una [10].

- **PSPACE -** Espacio polinomial: problemas que pueden ser resueltos haciendo uso de un espacio de memoria cuyo tamaño no crece más rápido que una función polinomial. Todas las otras clases de problemas mencionadas en esta lista están contenidas en esta clase. Por otro lado, **PSPACE** está contenido en **EXPTIME**, problemas resolubles en tiempo exponencial, que a su vez está contenido en **EXPSPACE**, problemas resolubles en espacio exponencial.

- **BPP -** Tiempo polinomial probabilístico de error limitado: problemas de decisión (respuesta Sí o No) que un algoritmo aleatorio de tiempo polinomial puede resolver con una probabilidad de éxito de 2/3. A veces un algoritmo aleatorio puede resolver un problema más rápido que uno determinista. Problemas de esta clase caen en dos categorías: resolubles con un algoritmo determinista en tiempo polinomial, o resolubles con un algoritmo probabilístico que fallará no más de 1/3 de las veces. La clase **P** está contenida en **BPP**, y se conjetura que **P**=**BPP**.

- **BQP -** Tiempo polinomial cuántico de error limitado: equivalente cuántico de **BPP**; problemas de decisión cuya resolución tiene una alta probabilidad de éxito. Se cree que esta clase contiene problemas intratables en el régimen clásico pero resolubles en tiempo polinomial en una computadora cuántica de error limitado. Sin embargo, no se tiene claridad acerca de la relación de **BPQ** respecto de **P**, **NP** y **PSPACE**.

- **EQP -** Tiempo polinomial cuántico exacto: similar a **BPQ**, pero con probabilidad de éxito 1, es decir, equivalente cuántico a **P**. La mecánica cuántica

no hace tratables a todos los problemas **NP**, solamente a los que tienen una estructura que se pueda aprovechar con la superposición de estados cuánticos y el entrelazamiento.

- **QMA -** Merlin-Arthur cuántico: equivalente cuántico a la clase **NP**; verifica respuestas con al menos 2/3 de probabilidad de éxito.

1.5.4. Errores cuánticos y su corrección

En esta sección se explican algunas formas básicas de errores en computación cuántica y métodos de corrección. Se inicia con los errores unitarios, producto de la incerteza en la construcción de las compuertas cuánticas y las cotas superiores para las desviaciones introducidas respecto a resultados ideales. El siguiente punto son los errores introducidos en la transmisión de información cuántica a través de canales ruidosos. En primer lugar se explican dos tipos simples de errores de transmisión, la inversión del bit y la inversión de fase, y los códigos que protegen la información cuántica y corrigen los errores introducidos por el ruido. Al final, se explica el código de 9 qubits de Shor, que permite proteger un qubit contra errores arbitrarios introducidos por canales ruidosos.

1.5.4.1. Errores unitarios

Si el estado inicial de un registro de qubits es $|\psi_0\rangle$, tras la implementación de un circuito (sucesión de compuertas cuánticas) el estado final está dado por

$$|\psi_n\rangle = \prod_{i=1}^{n} U_i \, |\psi_0\rangle \, ,$$

donde U_i representan las transformaciones unitarias aplicadas a los qubits en un algoritmo, y cuyo efecto individual es

$$|\psi_i\rangle = U_i \, |\psi_{i-1}\rangle \, .$$

Sin embargo, este modelo matemático asume que las compuertas aplicadas realizan perfectamente la operación U_i [7]. Físicamente, una compuerta incluye un error respecto del ideal U_i, de manera que la compuerta realmente aplica una transformación V_i tal que

$$V_i \, |\psi_{i-1}\rangle = |\psi_i\rangle + |E_i\rangle \, ,$$

donde [7]

$$|E_i\rangle = (V_i - U_i)\,|\psi_{i-1}\rangle\,.$$

Partiendo del estado $|\psi_0\rangle$, la evolución del registro cuántico incluyendo los errores unitarios de las compuertas cuánticas, tiene la forma

$$\left|\tilde{\psi}_1\right\rangle = V_1\,|\psi_0\rangle = |\psi_1\rangle + |E_1\rangle\,,$$

de manera que el estado final del registro, en vez de $|\psi_n\rangle$, resulta ser

$$\left|\tilde{\psi}_n\right\rangle = |\psi_n\rangle + |E_n\rangle + V_n\,|E_{n-1}\rangle + \ldots + V_nV_{n-1}\ldots V_2\,|E_1\rangle\,.$$

El peor escenario posible para estos errores es que estén alineados y se sumen linealmente, por lo que la desigualdad del triángulo da un límite superior para el error del estado final

$$\left\|\left|\tilde{\psi}_n\right\rangle - |\psi_n\rangle\right\| \leq \sum_{k=1}^{n} \||E_k\rangle\|\,,$$

donde se ha asumido una evolución total unitaria, de manera que $\|V_i\,|E_{i-1}\rangle\| = \||E_{i-1}\rangle\|$ [7]. El valor de cada error individual $\||E_i\rangle\|$ está limitado por

$$\||E_i\rangle\| = \|(V_i - U_i)\,|\psi_{i-1}\rangle\| \leq \|V_i - U_i\|_{\sup}\,.$$

La notación $\|U\|_{\sup}$ indica el eigenvalor del máximo módulo del operador U [7]. Si esta norma superior tiene un límite superior uniforme

$$\|V_i - U_i\|_{\sup} < \epsilon,$$

entonces el error unitario del vector final para el peor caso posible está dado por

$$\left\|\left|\tilde{\psi}_n\right\rangle - |\psi_n\rangle\right\| < n\epsilon, \tag{1.46}$$

mientras que el caso de errores aleatorios presentan un crecimiento más favorable de $\sqrt{n}$ [7]. Al realizar una medida proyectiva, la probabilidad de obtener el eigenestado $|i\rangle$ está dada por $p_i = |\langle i|\psi_n\rangle|^2$ para el caso de evolución unitaria ideal [7]. Tomando en cuenta el error unitario, la probabilidad de medición $\tilde{p}_i = \left|\left\langle i|\tilde{\psi}_n\right\rangle\right|^2$, y el error total entre ambos casos está limitado según

$$\sum_i |p_i - \tilde{p}_i| \leq 2\left\|\left|\tilde{\psi}_n\right\rangle - |\psi_n\rangle\right\|. \tag{1.47}$$

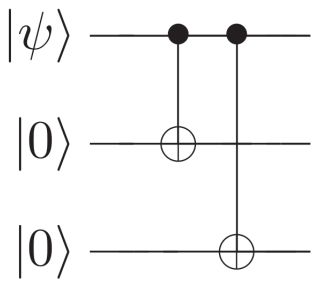

Figura 1.29. Diagrama de circuito para codificación de protección contra inversión del qubit, elaborado por Nielsen y Chuang [9].

1.5.4.2. Código de tres qubits para inversión del bit

Se requiere enviar un qubit en estado $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ a través de un canal ruidoso [8]. Se considera un escenario en el que el efecto del ruido es invertir el qubit, es decir, que aplica el operador σ_x de manera que $|\psi\rangle \to \beta\,|0\rangle + \alpha\,|1\rangle$ con una probabilidad ϵ, la cual se requiere que cumpla $\epsilon < 1/2$ [8].

En computación clásica, para proteger un bit contra el ruido en un canal de transmisión se realizan dos copias adicionales del bit; dado que el ruido altera el bit con una pequeña probabilidad solamente, se espera que sólo uno de los tres bits idénticos sea alterado, y al final de la transmisión se aplica votación de mayoría para decidir el valor correcto del bit [8]. Los estados cuánticos no se pueden copiar, pero se puede obtener una redundancia similar a la clásica realizando una operación

$$|\psi\rangle\,|00\rangle \to \alpha\,|000\rangle + \beta\,|111\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle \neq |\psi\rangle\,|\psi\rangle\,|\psi\rangle\,,$$

donde el subíndice L corresponde a la nomenclatura de estados $|0\rangle$ *lógico* y $|1\rangle$ *lógico*, también conocidos como *palabras clave* [8]. La codificación de tales estados se consigue mediante el circuito en la figura 1.29. Tras esta preparación inicial, cada qubit es enviado por una copia del mismo canal ruidoso.

Para obtener información sobre si un qubit ha sido invertido, y cuál de los tres, no se puede realizar mediciones directas sobre le registro, ya que esto destruiría el estado cuántico almacenado [8]. Se utilizan entonces dos qubits auxiliares cuyo valor se altera de acuerdo los valores de pares de qubits del registro según

$$|\psi_c\rangle\,|00\rangle \to |\psi_c\rangle\,|x_0x_1\rangle\,,$$

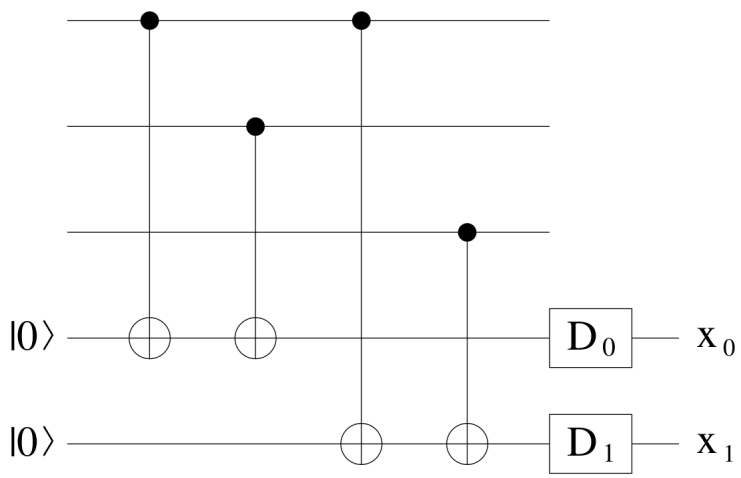

Figura 1.30. Diagrama de circuito para medición del síndrome de error de la inversión de qubit, elaborado por Benenti, Casati y Strini [8].

donde $|\psi_c\rangle$ es el estado del registro corrompido por el ruido, y a los valores de x_0 y x_1 se les conoce como *síndrome de error*, y almacenan las mediciones colectivas $\sigma_z^{(1)}\sigma_z^{(2)}$ y $\sigma_z^{(1)}\sigma_z^{(3)}$ respectivamente [8]. En la figura 1.30 se puede observar la asignación y medición del síndrome de error, de manera que el valor final de x_0 es 0 cuando los qubits primero y segundo son iguales $\sigma_z^{(1)}\sigma_z^{(2)} = 1$, y es 1 cuando son diferentes $\sigma_z^{(1)}\sigma_z^{(2)} = -1$; la misma relación se aplica para el valor de x_1 respecto de los qubits primero y tercero. Estos qubits auxiliares se usan como qubits de control de compuertas C^2**-NOT** generalizadas para corregir el qubit invertido, de la manera en la que se ilustra en la figura 1.31. En esta figura las últimas dos compuertas sirven para que el registro regrese al estado original $|\psi\rangle|00\rangle = (\alpha|0\rangle + \beta|1\rangle)|00\rangle$ [8].

Este código falla si el ruido ha alterado a más de un qubit, lo cual sucede con probabilidad $\epsilon^2(1-\epsilon)$ para dos qubits corrompidos y ϵ^3 para tres [8].

1.5.4.3. Código de tres qubits para inversión de fase

El error de inversión de fase consiste en la aplicación del operador σ_z con probabilidad ϵ, de manera que un estado inicial $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ se transforma a $\sigma_z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$ [8]. Para lidiar con este tipo de error se hacen las mismas dos *copias* adicionales que con la inversión de bit $|\psi\rangle|00\rangle \rightarrow |\psi_L\rangle$, y luego se realiza un cambio de base $\{|0\rangle, |1\rangle\} \rightarrow \{|+\rangle, |-\rangle\}$ utilizando compuertas de Hadamard [8]. Con este cambio de base se tiene $|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|+++\rangle + \beta|---\rangle$, y la inversión de fase se convierte en una inversión de bit $|+\rangle \leftrightarrow |-\rangle$ [8].

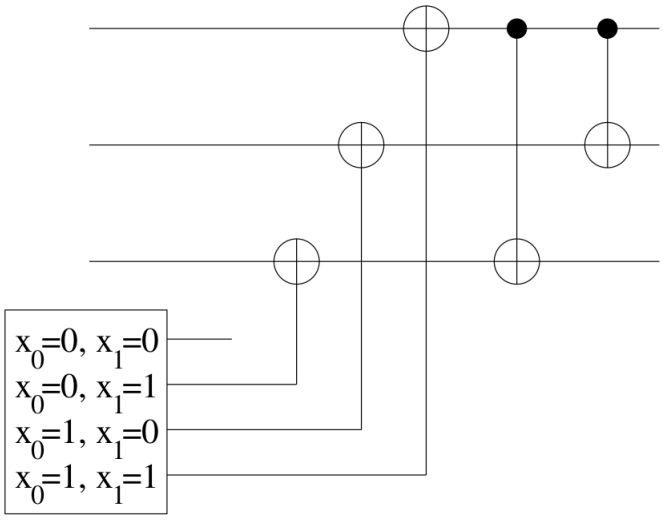

Figura 1.31. Diagrama de circuito de corrección de la inversión de qubit, elaborado por Benenti, Casati y Strini [8].

Tras pasar por el canal ruidoso, se utilizan compuertas de Hadamard para revertir el cambio de base $\{|+\rangle, |-\rangle\} \rightarrow \{|0\rangle, |1\rangle\}$ [8]. Una vez se realiza este cambio, la inversión de bit en la base $\{|+\rangle, |-\rangle\}$ se mantiene como inversión de bit en $\{|0\rangle, |1\rangle\}$ [8]. Como ejemplo de esto: se inicia con la codificación

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|+++\rangle + \beta|---\rangle,$$

cuyo paso por el canal ruidoso provoca el cambio

$$\alpha|+++\rangle + \beta|---\rangle \rightarrow \alpha|-++\rangle + \beta|+--\rangle,$$

y al pasar de nuevo por $H^{\otimes 3}$ se convierte en

$$\alpha|-++\rangle + \beta|+--\rangle \rightarrow \alpha|100\rangle + \beta|011\rangle.$$

Teniendo un error de inversión de bit, se aplica el mismo método de medición del síndrome de error y de corrección que en el apartado anterior, y se aplican las mismas condiciones respecto a la probabilidad de error y efectividad de la corrección [8]. Finalmente se revierte la codificación para regresar al estado original $|\psi\rangle|00\rangle$ [8].

1.5.4.4. Código de nueve qubits de Shor

Este código puede corregir un error arbitrario sobre un solo qubit; para esto aprovecha el hecho de que el ruido se puede parametrizar como la combinación

lineal de 4 tipos de errores, y al medir el síndrome de error el estado total del sistema colapsa hacia un estado con uno solo de los tipos de errores [8]. Esta parametrización se observa de la siguiente manera: asumiendo que al inicio el entorno de un qubit está en un estado puro $|0\rangle_E$, la evolución conjunta más general de qubit y entorno está dada por

$$U|0\rangle|0\rangle_E = |0\rangle|e_0\rangle_E + |1\rangle|e_1\rangle_E\,,$$

$$U|1\rangle|0\rangle_E = |0\rangle|e_2\rangle_E + |1\rangle|e_3\rangle_E\,,$$

donde $\{|e_i\rangle_E\}$ son estados del entorno, no necesariamente normalizados ni ortogonales [8]. Sobre un estado inicial de qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, esta evolución toma la forma

$$\begin{aligned} U|\psi\rangle|0\rangle_E &= \alpha\left(|0\rangle|e_0\rangle_E + |1\rangle|e_1\rangle_E\right) + \beta\left(|0\rangle|e_2\rangle_E + |1\rangle|e_3\rangle_E\right) \\ &= \frac{1}{2}\left(\alpha|0\rangle + \beta|1\rangle\right)\left(|e_0\rangle_E + |e_3\rangle_E\right) + \frac{1}{2}\left(\alpha|0\rangle - \beta|1\rangle\right)\left(|e_0\rangle_E - |e_3\rangle_E\right) \\ &+ \frac{1}{2}\left(\alpha|1\rangle + \beta|0\rangle\right)\left(|e_1\rangle_E + |e_2\rangle_E\right) + \frac{1}{2}\left(\alpha|1\rangle - \beta|0\rangle\right)\left(|e_1\rangle_E - |e_2\rangle_E\right) \\ &= I|\psi\rangle|e_I\rangle_E + \sigma_z|\psi\rangle|e_z\rangle_E + \sigma_x|\psi\rangle|e_x\rangle_E + \sigma_x\sigma_z|\psi\rangle|e_{xz}\rangle_E\,. \end{aligned}$$

De esta manera, el ruido que afecta al qubit por interacción con el entorno queda parametrizado en la base del grupo de Pauli, cuyos elementos producen cuatro tipos de errores: I para qubit sin error, σ_z para inversión de fase, σ_x para inversión de bit, y $\sigma_x\sigma_z = -i\sigma_y$ para inversión de fase seguida de inversión de bit [8]. La medición del síndrome de error es una medición sobre el estado $|e_\mu\rangle_E$ (con $\mu = I, 1, 2, 3$), de manera que el estado total en esa última ecuación colapsa hacia uno solo de las cuatro posibilidades de error, conservando intacto $|\psi\rangle$ con un error específico [8].

La forma en la que el código de Shor permite detectar y corregir estos errores empieza por la codificación

$$|0\rangle \to |0_L\rangle = \left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right),$$

$$|1\rangle \to |1_L\rangle = \left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right),$$

que se efectúa con el circuito presente en la figura 1.32, haciendo que el estado inicial genérico se transforme como $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \to \alpha|0_L\rangle + \beta|1_L\rangle$, y el estado total se puede visualizar en 3 bloques de 3 qubits cada uno.

En la figura 1.33 se puede apreciar como se mide el síndrome de error de inver-

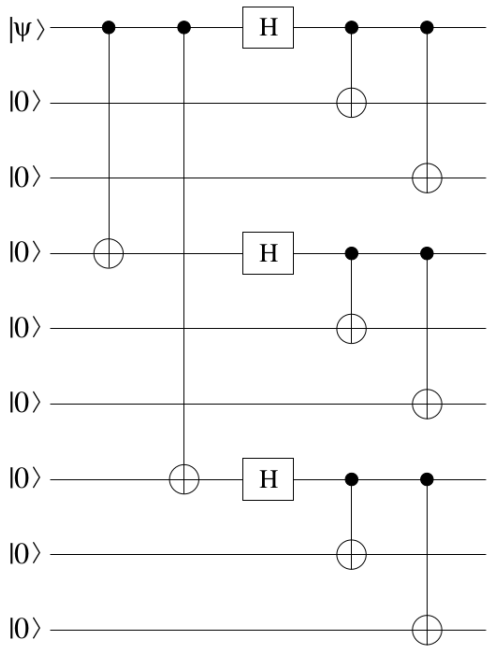

Figura 1.32. Diagrama de circuito de la codificación del qubit en el código de Shor, elaborado por Benenti, Casati y Strini [8].

sión de bit en cada bloque individual de qubits. En la misma imagen se presenta la medición para un error de inversión de fase en alguno de los bloques (no es necesario saber el qubit específico) $|000\rangle \pm |111\rangle \rightarrow |000\rangle \mp |111\rangle$, donde a través de compuertas de Hadamard y compuertas C^6-**NOT** se aplican las mediciones colectivas

$$y_0 = \sigma_x^{(1)}\sigma_x^{(2)}\sigma_x^{(3)}\sigma_x^{(4)}\sigma_x^{(5)}\sigma_x^{(6)},$$

$$y_1 = \sigma_x^{(1)}\sigma_x^{(2)}\sigma_x^{(3)}\sigma_x^{(7)}\sigma_x^{(8)}\sigma_x^{(9)},$$

que actúa como

$$\sigma_x^{(1)}\sigma_x^{(2)}\sigma_x^{(3)}\left(|000\rangle \pm |111\rangle\right) = \pm\left(|000\rangle \pm |111\rangle\right),$$

de manera que los casos (y_0, y_1) indican errores de la siguiente manera: $(1,1)$ para ningún error, $(-1,-1)$ para error en el primer bloque, $(-1,1)$ para el segundo, y $(1,-1)$ para el tercero [8]. Para corregir este error se deben aplicar $\sigma_z^{(1+3j)}\sigma_z^{(2+3j)}\sigma_z^{(3+3j)}$, con $j = 0, 1, 2$ dependiendo del bloque con error, debido a que estas compuertas efectúan [8]

$$\sigma_z^{(1)}\sigma_z^{(2)}\sigma_z^{(3)}\left(|000\rangle \pm |111\rangle\right) = \left(|000\rangle \mp |111\rangle\right).$$

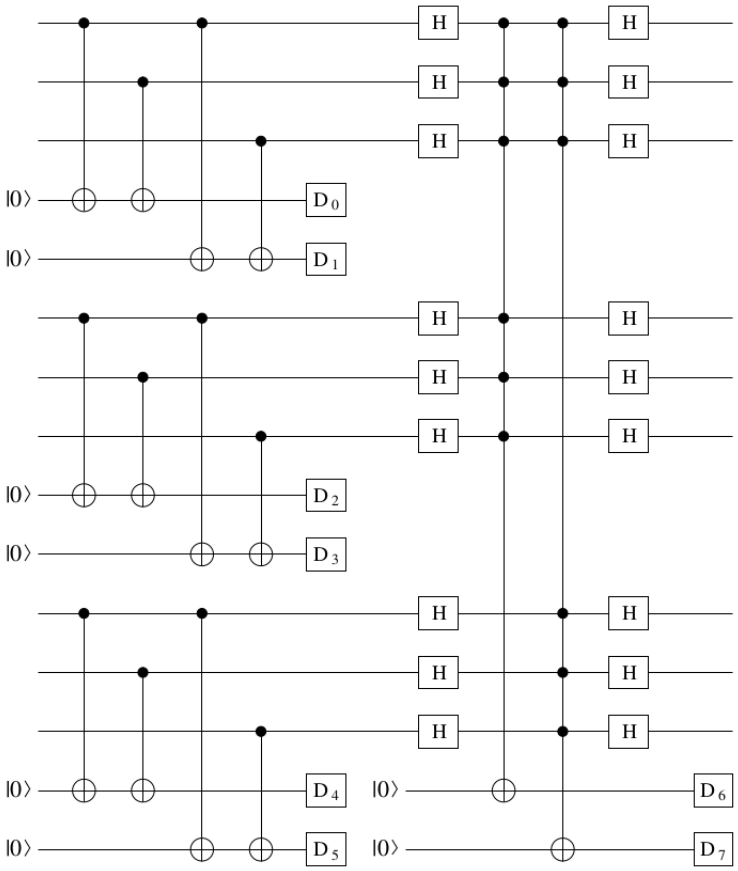

Figura 1.33. Diagrama de circuito de medición del síndrome de error en el código de Shor, elaborado por Benenti, Casati y Strini [8].

Un error más general es, por ejemplo, una rotación sobre el primer qubit

$$U_\epsilon^{(1)} = \cos(\epsilon) I^{(1)} + i \sin(\epsilon) \sigma_x^{(1)},$$

que actúa sobre el primer bloque de qubits como

$$U_\epsilon^{(1)} \left(|000\rangle + |111\rangle \right) = \cos(\epsilon) \left(|000\rangle + |111\rangle \right) + i \sin(\epsilon) \left(|100\rangle + |011\rangle \right),$$

cuya medición colectiva de $\sigma_z^{(1)} \sigma_z^{(2)}$ arroja un estado intacto con probabilidad $\cos^2 \epsilon$, o un estado con el primer qubit invertido con probabilidad $\sin^2 \epsilon$, efectivamente reduciendo un error de rotación de magnitud arbitraria a una inversión de bit, o ningún error en absoluto [8].

2. ÓPTICA CUÁNTICA

2.1. Introducción

El problema que dio el impulso inicial al desarrollo de la teoría cuántica fue la radiación de cuerpo negro, que trata sobre la forma en la que un cuerpo incandescente absorbe y emite energía a través de radiación electromagnética, y que sólo pudo ser resuelto por Plank considerando que estos procesos ocurren de manera discreta [12]. Esta idea fue generalizada por Eintein al proponer que estos cuantos de radiación no eran exclusivos del problema de cuerpo negro, sino una propiedad intrínseca de toda la luz [12]. Einstein utilizó esta generalización para explicar el efecto fotoeléctrico, y para proponer la emisión estimulada como producto del proceso de equilibrio entre materia y radiación, dando origen a los emisores láser y máser (láser de microondas) [12]. Fue también el trabajo de Eintein sobre movimiento molecular el que dejó en firme ante la comunidad científica la naturaliza atómica y molecular de la materia [11].

Tras los avances sobre la dualidad onda-partícula de la luz, de Broglie propuso que esta característica de la luz era generalizable a toda la materia, y en la década de 1920 se establecieron las bases de la teoría cuántica con los trabajos de Schrödinger, Heisenberg y Dirac [12]. Fue este último quién, en la década de 1930, trabajó en la teoría cuántica de la luz con el nuevo formalismo [1]. En el avance sobre la naturaleza de la radiación electromagnética se llegó a la Electrodinámica Cuántica en los años 40 y 50, que fue la primera teoría cuántica de campos desarrollada, y permitió la descripción teórica de fenómenos sin explicación previa [12].

Por otro lado, en la década de 1960 Glauber estableció la óptica cuántica en su sentido moderno, y aplicó este formalismo a aparatos ópticos clásicos [1]. Glauber también introdujo el concepto de estados cuasi-clásicos de la luz, que permite entender por qué las fuentes disponibles al momento emitían luz explicable a partir

de un enfoque semi-clásico, pero también dio inicio a los avances que llevaron a descubrir fenómenos ópticos puramente cuánticos, a su vez llevando a la construcción de fuentes de luz no clásica [1].

En el área de fundamentos cuánticos e información cuántica, Einstein, Podolsky y Rosen (EPR) mostraron las peculiaridades de las correlaciones cuánticas (inicialmente como objeción a la teoría cuántica); dichas correlaciones cuánticas fueron separadas de sus pares clásicos por los estudios de Bell y Bohm, y finalmente demostradas experimentalmente por Aspect utilizando fotones [12]. Las correlaciones cuánticas y su diferencia respecto a las correlaciones clásicas son el fundamento del procesamiento de información en computación cuántica [12].

2.2. Diferencia entre óptica clásica y cuántica

La óptica clásica consiste en la descripción de la luz como una onda electromagnética, campos eléctricos y magnéticos que se propagan a través del espacio gobernados por las ecuaciones de Maxwell [13]. La descripción de estos campos electromagnéticos es determinista y continua, y todos los fenómenos asociados a la luz se describen asumiendo estas propiedades clásicas, tanto en el vacío como en presencia de materia [13]. Desde este punto de vista clásico, la ausencia de campo electromagnético en el vacío implica ausencia de energía [13].

La óptica cuántica se erige sobre una cuantización escalar del campo electromagnético [12]. Esto quiere decir que el campo electromagnético consiste en estados discretos de energía conocidos como fotones [12]. Un fotón es una excitación discreta de energía de magnitud $\hbar\omega$, donde $\hbar$ es la constante de Plank que surge del estudio de la radiación de cuerpo negro; al llevar el campo cuantizado al límite clásico, la cantidad ω se convierte en la frecuencia angular de la onda electromagnética [12]. Otra de las propiedades más significativas del campo electromagnético cuantizado es que da lugar a una energía de vacío, que existe aún en ausencia total de fotones y cuyos efectos se han comprobado experimentalmente [12].

También es importante resaltar las diferencias entre la teoría corpuscular de la luz y la óptica cuántica. La teoría corpuscular, pieza introductoria de la mecánica cuántica, considera a los fotones como partículas de luz; por otro lado, en la óptica

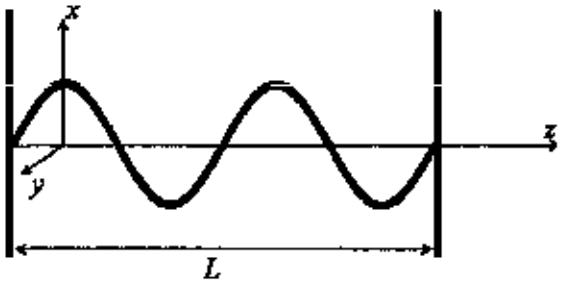

Figura 2.1. Diagrama de la cavidad unidimensional, elaborada por Gerry y Knight [12].

cuántica los fotones surgen como excitaciones discretas de energía, no-localizados y esparcidos sobre el espacio [12].

2.3. Cuantización escalar del campo electromagnético

Para realizar la cuantización requerida, se parte de un caso simple y limitado: una cavidad unidimensional a lo largo del eje z, con paredes perfectamente conductoras en $z = 0$ y $z = L$, sin fuentes de carga ni materiales [12]. En el interior de dicha cavidad, como se observa en la figura 2.1, hay un campo electromagnético cuyo componente de campo eléctrico está polarizado linealmente (sólo hay una componente cartesiana del campo) en el eje x [12]

$$\vec{E}(\vec{r}, t) = \vec{e}_x E_x(z, t).$$

Dadas las características de la cavidad, se tienen las condiciones de frontera

$$E_x(0, t) = E_x(L, t) = 0, \tag{2.1}$$

las cuales implican que el campo dentro de la cavidad es una onda estacionaria [12].

El campo electromagnético obedece a las ecuaciones de Maxwell, que en el vacío y en ausencia de fuentes de campo tienen la forma

$$\vec{\nabla} \cdot \vec{E} = 0, \tag{2.2}$$

$$\vec{\nabla} \cdot \vec{B} = 0, \tag{2.3}$$

$$\vec{\nabla} \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}, \tag{2.4}$$

$$\vec{\nabla} \times \vec{B} = \mu_0 \epsilon_0 \frac{\partial \vec{E}}{\partial t}, \tag{2.5}$$

donde $\vec{E}$ es el campo eléctrico, $\vec{B}$ es el campo magnético, ϵ_0 es la permitivad eléctrica del vacío, y μ_0 es la permeabilidad magnética del vacío [12].

Una función $\vec{E}$ de un solo modo (cuyo significado se discute más adelante) que cumple con las condiciones de frontera y las ecuaciones de Maxwell tiene

$$E_x(z,t) = \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} q(t)\sin(kz), \tag{2.6}$$

donde ω es la frecuencia angular de la onda, $k = \omega/c$ es el número de onda y V es el volumen efectivo de la cavidad [12]. Tomando la masa como elemento unitario ($[m] = 1$) y un volumen tridimensional, $q(t)$ queda con dimensional de longitud. De las condiciones de frontera en la Ecuación (2.1) se deduce que solamente hay ciertos valores permitidos para k y ω

$$k_m = \frac{m\pi}{L},$$

$$\omega_m = c\frac{m\pi}{L},$$

donde $m = 1, 2, 3\ldots$, con cada posible k_m, ω_m correspondiente a un *modo* de la onda electromagnética [12].

Aplicando la Ecuación (2.5) sobre el $\vec{E}(\vec{r},t)$ propuesto, se obtiene un campo magnético $\vec{B}(\vec{r},t) = \vec{e}_y B_y(z,t)$ con

$$B_y(z,t) = \left(\frac{\mu_0\epsilon_0}{k}\right)\left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \dot{q}(t)\cos(kz), \tag{2.7}$$

en el cual, tomando una masa unitaria, se puede igualar $\dot{q}(t) = p(t)$, donde p es una variable de momentum [12].

La energía total H de un campo electromagnético clásico en el vacío está dada por

$$H = \frac{1}{2}\int \left(\epsilon_0 \vec{E}^2 + \frac{1}{\mu_0}\vec{B}^2\right) dV,$$

que, con los campos de la cavidad trabajada, toma la forma [12]

$$H = \frac{1}{2}\int \left(\epsilon_0 E_x^2 + \frac{1}{\mu_0} B_y^2\right) dz.$$

Integrando cada término por separado, a lo largo de la cavidad, se tiene

$$\int_0^L \epsilon_0 E_x^2 = \frac{2\omega^2}{V} q^2 \int_0^L \sin^2(kz) dz = \frac{\omega^2}{L} q^2 \int_0^L \left[1 - \cos\left(2\frac{m\pi}{L} z\right)\right] dz = \omega^2 q^2,$$

$$\int_0^L \frac{1}{\mu_0} B_y^2 = \frac{\dot{q}^2}{L} \int_0^L \sin^2(kz) dz = \dot{q}^2 = p^2,$$

de manera que la energía total es

$$H = \frac{1}{2}\left(p^2 + \omega^2 q^2\right), \tag{2.8}$$

que corresponde al hamiltoniano del oscilador armónico simple para una masa unitaria [12].

En este punto se introduce la cuantización canónica, con las variables de posición y momentum, q y p, tomando el papel de operadores hermíticos, $\hat{q}$ y $\hat{p}$, que cumplen con la relación de conmutación [12]

$$[\hat{q}, \hat{p}] = i\hbar. \tag{2.9}$$

De esta manera, los campos eléctrico y magnético se convierten también en operadores (esencialmente los mismos $\hat{q}$ y $\hat{p}$):

$$\hat{E}_x(z,t) = \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \hat{q}(t)\sin(kz), \tag{2.10}$$

$$\hat{B}_y(z,t) = \left(\frac{\mu_0\epsilon_0}{k}\right)\left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \hat{p}(t)\cos(kz), \tag{2.11}$$

y la energía total pasa a ser el operador hamiltoniano del oscilador armónico cuántico en una dimensión [12]

$$\hat{H} = \frac{1}{2}\left(\hat{p}^2 + \omega^2 \hat{q}^2\right). \tag{2.12}$$

El siguiente paso es darle a este hamiltoniano el tratamiento algebraico típico para el oscilador armónico cuántico. Se empieza definiendo los operadores escalera,

o de creación ($\hat{a}^\dagger$) y aniquilación ($\hat{a}$), que son el adjunto uno de otro [12]

$$\hat{a} = (2\hbar\omega)^{-1/2}(\omega\hat{q} + i\hat{p}), \tag{2.13}$$

$$\hat{a}^\dagger = (2\hbar\omega)^{-1/2}(\omega\hat{q} - i\hat{p}). \tag{2.14}$$

Partiendo de la relación de conmutación (2.9), estos operadores resultan en la relación

$$[\hat{a}, \hat{a}^\dagger] = 1, \tag{2.15}$$

y permiten reescribir los operadores de campo como

$$\hat{E}_x = \mathcal{E}_0(\hat{a} + \hat{a}^\dagger)\sin(kz), \tag{2.16}$$

$$\hat{B}_y = -i\mathcal{B}_0(\hat{a} - \hat{a}^\dagger)\cos(kz), \tag{2.17}$$

con $\mathcal{E}_0 = (\frac{\hbar\omega}{\epsilon_0 V})^{1/2}$ y $\mathcal{B}_0 = \frac{\mu_0}{k}(\frac{\epsilon_0\hbar\omega^3}{V})^{1/2}$. El hamiltoniano toma la forma [12]

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right). \tag{2.18}$$

Las relaciones de conmutación entre el hamiltoniano y los operadores escalera están dadas por

$$[\hat{H}, \hat{a}] = [\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right), \hat{a}] = \hbar\omega[\hat{a}^\dagger\hat{a}, \hat{a}] = \hbar\omega(\hat{a}^\dagger[\hat{a}, \hat{a}] + [\hat{a}^\dagger, \hat{a}]\hat{a}),$$

simplificándose a

$$[\hat{H}, \hat{a}] = -\hbar\omega\hat{a}, \tag{2.19}$$

y

$$[\hat{H}, \hat{a}^\dagger] = \hbar\omega\hat{a}^\dagger, \tag{2.20}$$

obtenidas utilizando (2.15). Si se propone una eigenvector $\hat{H}\psi = E\psi$, y se le aplican los operadores de estas relaciones de conmutación, resulta que

$$\hat{H}(\hat{a}\psi) = (E - \hbar\omega)(\hat{a}\psi),$$

$$\hat{H}(\hat{a}^\dagger\psi) = (E + \hbar\omega)(\hat{a}^\dagger\psi),$$

demostrando que $\hat{a}\psi$ y $\hat{a}^\dagger\psi$ son también eigenvectores de $\hat{H}$, respectivamente aniquilando y creando un cuanto $\hbar\omega$ de energía al ser aplicados a algún eigenvector de

$\hat{H}$. De esto se deduce que el estado fundamental del oscilador armónico cuántico es aquel que cumple con

$$\hat{a}\,|0\rangle = 0,$$

lo cual implica

$$\hat{H}\,|0\rangle = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|0\rangle = \frac{1}{2}\hbar\omega\,|0\rangle\,,$$

obteniéndose la energía de punto cero o de vacío $E_0 = \hbar\omega/2$ [12]. Conociéndose el efecto de $\hat{a}^\dagger$, se hace claro que

$$\hat{H}(\hat{a}^\dagger)^n\,|0\rangle = \hbar\omega\left(n + \frac{1}{2}\right)(\hat{a}^\dagger)^n\,|0\rangle\,,$$

de manera que es razonable etiquetar los eigenvectores del hamiltoniano (que es un operador hermítico) como

$$(\hat{a}^\dagger)^n\,|0\rangle = c_n\,|n\rangle\,,$$

con c_n una constante de normalización, $n = 0, 1, 2\ldots$, condición de normalización

$$\langle n|m\rangle = \delta_{nm}, \tag{2.21}$$

y condición de completitud [12]

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = 1. \tag{2.22}$$

Entonces n corresponde al número de cuantos o excitaciones discretas de energía de tamaño $\hbar\omega$ presentes en un estado; en otras palabras, n es el número de fotones, cada uno con la energía $\hbar\omega$ conocida desde los albores de la teoría cuántica [12]. Es importante notar que, en ausencia de fotones, queda una energía de vacío E_0 encontrada previamente, cuyos efectos predichos se han demostrado experimentalmente y son: el efecto Cassimir, el desplazamiento de Lamb y la emisión espontánea de luz [12].

Conociéndose estas propiedades, se puede introducir a la nomenclatura el operador número

$$\hat{a}^\dagger\hat{a} = \hat{n}, \tag{2.23}$$

que por definición es hermítico, y cumple con

$$\hat{n}\,|n\rangle = n\,|n\rangle\,, \tag{2.24}$$

lo que permite reescribir el hamiltoniano como [12]

$$\hat{H} = \hbar\omega\left(\hat{n} + \frac{1}{2}\right).$$

Para normalizar el efecto de los operadores escalera, se hace

$$\langle \hat{a}n|\hat{a}n\rangle = \langle n|\,\hat{a}^\dagger\hat{a}\,|n\rangle = \langle n|\,\hat{n}\,|n\rangle = n,$$

a la vez que

$$\langle \hat{a}n|\hat{a}n\rangle = |c_{n-1}|^2\,\langle n-1|n-1\rangle = |c_{n-1}|^2\,,$$

resultando que [12]

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{2.25}$$

Y para el operador de creación

$$\left\langle \hat{a}^\dagger n|\hat{a}^\dagger n\right\rangle = \langle n|\,\hat{a}\hat{a}^\dagger\,|n\rangle = \langle n|\,\hat{a}^\dagger\hat{a}+1\,|n\rangle = n+1,$$

donde se usó el conmutador de la Ecuación (2.15). Ahora

$$\left\langle \hat{a}^\dagger n|\hat{a}^\dagger n\right\rangle = |c_{n+1}|^2\,\langle n+1|n+1\rangle = |c_{n+1}|^2\,,$$

quedando [12]

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,. \tag{2.26}$$

Gracias a esto, se puede escribir cualquier estado $|n\rangle$ a partir del estado de vacío [12]

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}\,|0\rangle\,. \tag{2.27}$$

En la descripción de Heisenberg de la mecánica cuántica, la evolución temporal de un operador está dada por

$$\frac{d\hat{O}}{dt} = \frac{i}{\hbar}[\hat{H},\hat{O}], \tag{2.28}$$

que para los operadores escalera es

$$\frac{d\hat{a}}{dt} = -i\omega\hat{a},$$

$$\frac{d\hat{a}^\dagger}{dt} = i\omega\hat{a}^\dagger,$$

ecuaciones cuyas soluciones son [12]

$$\hat{a}(t) = \hat{a}(0)e^{-i\omega t}, \tag{2.29}$$

$$\hat{a}^\dagger(t) = \hat{a}^\dagger(0)e^{i\omega t}. \tag{2.30}$$

Otra forma de obtener estos resultados, la cual es útil para trabajar con interacciones no lineales, es utilizando el operador propagador (o de evolución temporal)

$$\hat{O}(t) = e^{i\hat{H}t/\hbar}\hat{O}(0)e^{-i\hat{H}t/\hbar}, \tag{2.31}$$

y aplicando el lema de Baker-Hausdorf, que puede tomarse como una expansión de Taylor para $\hat{O}(t)$ donde las derivadas se reemplazan con conmutadores según (2.28)

$$\hat{O}(t) = \hat{O} + \frac{it}{\hbar}[\hat{H},\hat{O}] + \frac{1}{2!}\left(\frac{it}{\hbar}\right)^2[\hat{H},[\hat{H},\hat{O}]] + \frac{1}{3!}\left(\frac{it}{\hbar}\right)^3[\hat{H},[\hat{H},[\hat{H},\hat{O}]] + \ldots, \tag{2.32}$$

usando $\hat{O}(0) = \hat{O}$; de esta manera un operador escalera queda [12]

$$\hat{a}(t) = \hat{a}(0)\left(1 - i\omega t - \frac{\omega^2t^2}{2!} + i\frac{\omega^3t^3}{3!} + \ldots\right) = \hat{a}(0)e^{-i\omega t}. \tag{2.33}$$

2.4. Efectos cuánticos de la luz

2.4.1. Fluctuaciones cuánticas de un campo de modo único

Un estado $|n\rangle$ de número definido de fotones, está asociado a una energía E_n bien definida, pero no a un campo eléctrico bien definido [12], como se puede ver utilizando (2.16)

$$\left\langle \hat{E}_x \right\rangle = \langle n|\, \hat{E}_x(z,t)\, |n\rangle = \mathcal{E}_0 \sin(kz)(\langle n|\, \hat{a}\, |n\rangle + \langle n|\, \hat{a}^\dagger\, |n\rangle) = 0.$$

Sin embargo, el valor esperado del cuadrado del campo no se anula, dado que

$$\left\langle \hat{E}_x^2 \right\rangle = \mathcal{E}_0^2 \sin^2(kz) \left\langle n \right| (\hat{a}^\dagger)^2 + \hat{a}^2 + \hat{a}^\dagger \hat{a} + \hat{a}\hat{a}^\dagger \left| n \right\rangle ,$$

que se simplifica para dar [12]

$$\left\langle \hat{E}_x^2 \right\rangle = \mathcal{E}_0^2 \sin^2(kz) \left\langle n \right| 2\hat{a}^\dagger \hat{a} + 1 \left| n \right\rangle = 2\mathcal{E}_0^2 \sin^2(kz) \left(n + \frac{1}{2} \right) .$$

Con estos valores, se pueden obtener las fluctuaciones cuánticas o incerteza del campo eléctrico ΔE_x utilizando la varianza

$$(\Delta x)^2 = \left\langle x^2 \right\rangle - \left\langle x \right\rangle^2 , \tag{2.34}$$

con lo que se consigue [12]

$$\Delta E_x = \sqrt{2}\mathcal{E}_0 \sin(kz) \left(n + \frac{1}{2} \right)^{1/2} . \tag{2.35}$$

Entonces, estas fluctuaciones persisten aun en el vacío $n = 0$ [12].

Este resultado coincide con el principio de incertidumbre de Heisenberg, que estipula que para dos operadores complementarios,

$$[\hat{A}, \hat{B}] = \hat{C} \neq 0,$$

se cumple que [12]

$$\Delta A \Delta B \geq \frac{1}{2} \left| \left\langle \hat{C} \right\rangle \right| \tag{2.36}$$

A partir de esto, se tiene para los operadores de número y de campo eléctrico

$$[\hat{n}, \hat{E}_x] = \mathcal{E}_0 \sin(kz)(\hat{a}^\dagger - \hat{a}),$$

con lo que se obtiene la desigualdad [12]

$$\Delta n \Delta E_x \geq \frac{1}{2} \mathcal{E}_0 \left| \sin(kz) \right| \left| \left\langle \hat{a}^\dagger - \hat{a} \right\rangle \right| . \tag{2.37}$$

Para un estado de número definido de fotones $|n\rangle$, se tiene $\Delta n = 0$ y $\left\langle \hat{a}^\dagger - \hat{a} \right\rangle = 0$, por lo que el campo eléctrico queda con incerteza $\Delta E_x \neq 0$. [12]

Existe una conexión entre el campo eléctrico y la fase del campo, de manera que el operador de número y un operador de fase son complementarios y relacionados por el principio de incertidumbre [12]. No es posible describir esta relación a detalle, dado que la definición de un operador de fase cuántico es un problema abierto de la física [12].

2.4.2. Operadores de cuadratura

Definiendo $\hat{a}(0) = \hat{a}$ y $\hat{a}^\dagger(0) = \hat{a}^\dagger$, y reemplazando con (2.29) y (2.30), el operador de campo eléctrico se escribe [12]

$$\hat{E}_x = \mathcal{E}_0(\hat{a}e^{-i\omega t} + \hat{a}^\dagger e^{i\omega t})\sin(kz). \tag{2.38}$$

Los operadores de cuadratura se definen como

$$\hat{X}_1 = \frac{1}{2}(\hat{a} + \hat{a}^\dagger), \tag{2.39}$$

$$\hat{X}_2 = \frac{1}{2i}(\hat{a} - \hat{a}^\dagger), \tag{2.40}$$

y el campo eléctrico pasa a ser

$$\hat{E}_x = 2\mathcal{E}_0 \sin(kz)\left[\hat{X}_1\cos(\omega t) + \hat{X}_2\sin(\omega t)\right], \tag{2.41}$$

donde se puede observar a $\hat{X}_1$ y $\hat{X}_2$ como amplitudes de oscilaciones en desfase de $\pi/2$, es decir, en cuadratura [12].

De su definición, es claro que los operadores de cuadratura son esencialmente los operadores de posición $\hat{x}$ y momentum $\hat{p}$, y conservan su conmutador (2.9)

$$[\hat{X}_1, \hat{X}_2] = \frac{i}{2}, \tag{2.42}$$

que, según el principio de Heisenberg en (2.36), impone [12]

$$\Delta\hat{X}_1 \Delta\hat{X}_2 \geq \frac{1}{4}. \tag{2.43}$$

Esto se puede obtner a partir de que

$$\langle n|\,\hat{X}_1\,|n\rangle = \langle n|\,\hat{X}_2\,|n\rangle = 0$$

y

$$\langle n|\,\hat{X}_1^2\,|n\rangle = \langle n|\,\hat{X}_2^2\,|n\rangle = \frac{1}{4}(2n+1),$$

lo que, para $n = 0$, arroja el valor mínimo de la desigualdad (2.43) [12].

2.4.3. Estados coherentes

Como ya se ha visto, los estados número fotónicos no producen un valor definido de campo eléctrico [12]. Entonces, si se quiere asociar la cuantización del campo electromagnético con su contraparte clásica, se requieren tener estados que produzcan valores definidos de campo eléctrico a partir del operador correspondiente; dada la definición de dicho operador en la ecuación (2.16), la condición requerida es que los estados en cuestión sean eigenestados de $\hat{a}$ para obtener $\langle\hat{a}\rangle \neq 0$ [12]. Se establecen los requerimientos

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.44}$$

$$\langle\alpha|\,\hat{a}^\dagger = \alpha^*\,\langle\alpha|\,. \tag{2.45}$$

donde $|\alpha\rangle$ es el estado buscado [12].

Dado que los estados fotónicos $\{|n\rangle\}$ forman una eigenbase completa, se puede escribir

$$|\alpha\rangle = \sum_{n=0}^{\infty} C_n\,|n\rangle\,,$$

al que al aplicarle el operador de aniquilación produce

$$\hat{a}\,|\alpha\rangle = \sum_{n=0}^{\infty} C_n\sqrt{n}\,|n-1\rangle = \alpha\sum_{n=0}^{\infty} C_n\,|n\rangle\,,$$

de manera que hay una relación de recursión

$$C_n\sqrt{n} = \alpha C_{n-1},$$

que extendiendo hasta $n = 0$ da

$$C_n = \frac{\alpha^n}{\sqrt{n!}}C_0,$$

por lo que el estado total es [1]

$$|\alpha\rangle = C_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle .$$

Para normalizar y completar la definición, se hace el producto interno

$$\langle\alpha|\alpha\rangle = 1 = |C_0|^2 \sum_{m,n}^{\infty} \frac{\alpha^m \alpha^n}{\sqrt{m!n!}} \langle m|n\rangle = |C_0|^2 \sum_{n}^{\infty} \frac{|\alpha|^{2n}}{n!} = |C_0|^2 e^{|\alpha|^2},$$

de donde se obtiene la constante de normalización $C_0 = e^{-\frac{1}{2}|\alpha|^2}$ y el eigenestado buscado queda con la forma [12]

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.46}$$

El operador de campo eléctrico, generalizado a una dependencia espacial general, tiene la forma

$$\hat{E}_x(\vec{r}, t) = i \left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2} \left[\hat{a} e^{i\left(\vec{k}\cdot\vec{r}-\omega t\right)} - \hat{a}^\dagger e^{-i\left(\vec{k}\cdot\vec{r}-\omega t\right)}\right],$$

cuyo valor esperado es [1]

$$\langle\alpha| \hat{E}_x |\alpha\rangle = i \left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2} \left[\alpha e^{i\left(\vec{k}\cdot\vec{r}-\omega t\right)} - \alpha^* e^{-i\left(\vec{k}\cdot\vec{r}-\omega t\right)}\right].$$

Si se toma la forma polar del eigenvalor $\alpha = |\alpha| e^{i\theta}$, el valor esperado del campo eléctrico queda como

$$\left\langle \hat{E}_x \right\rangle = 2|\alpha| \left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2} \sin(\omega t - \vec{k}\cdot\vec{r} - \theta), \tag{2.47}$$

que es la forma clásica de una componente de campo eléctrico de una onda electromagnética de modo único [12]. El estado $|\alpha\rangle$ da paso a un valor definido del operador de campo eléctrico, que coincide con el campo eléctrico clásico; de ahí el nombre de *estado coherente* para $|\alpha\rangle$, pues está asociado al campo eléctrico de luz coherente. La incertidumbre asociada a los estados coherentes requiere hallar

$$\hat{E}_x^2 = -\frac{\hbar\omega}{2\epsilon_0 V} \left[\hat{a}^2 e^{2i\left(\vec{k}\cdot\vec{r}-\omega t\right)} + \left(\hat{a}^\dagger\right)^2 e^{-2i\left(\vec{k}\cdot\vec{r}-\omega t\right)} - \hat{a}^\dagger\hat{a} - \hat{a}\hat{a}^\dagger\right],$$

y usando la relación de conmutación

$$\hat{E}_x^2 = -\frac{\hbar\omega}{2\epsilon_0 V}\left[\hat{a}^2 e^{2i\left(\vec{k}\cdot\vec{r}-\omega t\right)} + \left(\hat{a}^\dagger\right)^2 e^{-2i\left(\vec{k}\cdot\vec{r}-\omega t\right)} - 2\hat{a}^\dagger\hat{a} - 1\right]$$

para obtener [12]

$$\langle\alpha|\,\hat{E}_x^2\,|\alpha\rangle = -\frac{\hbar\omega}{2\epsilon_0 V}\left[\alpha^2 e^{2i\left(\vec{k}\cdot\vec{r}-\omega t\right)} + (\alpha^*)^2\, e^{-2i\left(\vec{k}\cdot\vec{r}-\omega t\right)} - 2\,|\alpha|^2 - 1\right],$$

pasando a forma polar

$$\langle\alpha|\,\hat{E}_x^2\,|\alpha\rangle = -\frac{\hbar\omega}{2\epsilon_0 V}\left\{|\alpha|^2\left[e^{2i\left(\omega t-\vec{k}\cdot\vec{r}-\theta\right)} + e^{-2i\left(\omega t-\vec{k}\cdot\vec{r}-\theta\right)} - 2\right] - 1\right\},$$

con la definición de sin

$$\langle\alpha|\,\hat{E}_x^2\,|\alpha\rangle = -\frac{\hbar\omega}{2\epsilon_0 V}\left[|\alpha|^2\,(2i)^2\sin^2(\omega t - \vec{k}\cdot\vec{r} - \theta) - 1\right],$$

y simplificando

$$\langle\alpha|\,\hat{E}_x^2\,|\alpha\rangle = \frac{\hbar\omega}{2\epsilon_0 V}\left[1 + 4\,|\alpha|^2\sin^2(\omega t - \vec{k}\cdot\vec{r} - \theta)\right].$$

Con estas cantidades se puede calcular la incertidumbre, ruido o fluctuaciones en el campo eléctrico del estado coherente [12], utilizando la ecuación (2.34),

$$\Delta E_x = \left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2}. \tag{2.48}$$

Este valor de incertidumbre es constante, y coincide con el valor de ΔE_x en (2.35) para el vacío $n = 0$, es decir, los estados coherentes minimizan las fluctuaciones cuánticas de vacío [12]. Estos estados, con su ruido mínimo y su valor esperado de campo eléctrico oscilante, son los estados cuánticos más *clásicos* posibles de la luz, y por ello también son llamados *estados cuasi-clásicos* [1]. La propiedad de mínima incertidumbre también se evidencia en los operadores de cuadratura (2.39) y (2.40), donde se tiene

$$\langle\alpha|\,\hat{X}_1\,|\alpha\rangle = \frac{1}{2}(\alpha + \alpha^*),$$

$$\langle\alpha|\,\hat{X}_2\,|\alpha\rangle = \frac{1}{2i}(\alpha - \alpha^*),$$

$$\langle\alpha|\,\hat{X}_1^2\,|\alpha\rangle = \frac{1}{4}\,\langle\alpha|\,\hat{a}^2 + \left(\hat{a}^\dagger\right)^2 + 2\hat{a}^\dagger\hat{a} + 1\,|\alpha\rangle = \frac{1}{4}\left[\alpha^2 + (\alpha^*)^2 + 2\,|\alpha|^2 + 1\right],$$

$$\langle\alpha|\,\hat{X}_2^2\,|\alpha\rangle = -\frac{1}{4}\left[\alpha^2 + (\alpha^*)^2 - 2\,|\alpha|^2 - 1\right],$$

con lo que se obtiene la incertidumbre de los operadores de cuadratura para el estado del vacío, $|0\rangle$,

$$\Delta X_1 = \Delta X_2 = \frac{1}{2}, \tag{2.49}$$

correspondiente al valor mínimo de (2.43) [12]. Así, los estados coherentes también minimizan el ruido en los operadores de cuadratura [12].

Como se puede ver en el valor esperado del campo eléctrico, el ángulo θ en $\alpha = |\alpha|\,e^{i\theta}$ está asociado a la fase de las oscilaciones del campo. Para hallar el significado físico de la norma de α, se opera con $\hat{n} = \hat{a}^\dagger\hat{a}$

$$\bar{n} = \langle\hat{n}\rangle = |\alpha|^2, \tag{2.50}$$

es decir, el cuadrado de la norma del eigenvalor de $\hat{a}$ es el número promedio de fotones en la onda electromagnética [1]. La incerteza asociada está dada por

$$\left\langle\hat{n}^2\right\rangle = \langle\alpha|\,\hat{a}^\dagger\hat{a}\hat{a}^\dagger\hat{a}\,|\alpha\rangle = \langle\alpha|\,\hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a} + \hat{a}^\dagger\hat{a}\,|\alpha\rangle = \bar{n}^2 + \bar{n},$$

de manera que el número de fotones en la luz de estado coherente fluctúa con amplitud de [1]

$$\Delta n = \bar{n}^{1/2} \tag{2.51}$$

La distribución de probabilidad para cada estado número $|n\rangle$, utilizando la definición en (2.46) está dada por

$$P_n = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!} = e^{-\bar{n}}\frac{\bar{n}^n}{n!}, \tag{2.52}$$

que es la distribución de Poisson, la cual se aproxima a la distribución normal al crecer $\bar{n}$ [1].

La evolución temporal de los estados coherentes está dada por la acción del operador propagador sobre el estado

$$|\alpha, t\rangle = e^{-i\hat{H}t/\hbar}\,|\alpha\rangle = e^{-i\omega t/2}e^{-i\omega t\hat{n}}\,|\alpha\rangle\,,$$

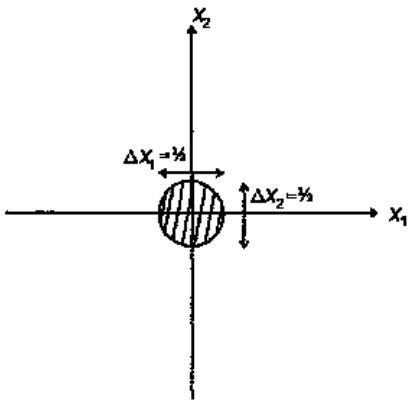

Figura 2.2. Incertidumbre en el espacio de fases para el vacío, elaborada por Gerry y Knight [12].

y usando (2.46)

$$e^{-i\omega t\hat{n}}\left|\alpha\right\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}e^{-i\omega t\hat{n}}\left|n\right\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\left(\alpha e^{-i\omega t}\right)^n}{\sqrt{n!}}\left|n\right\rangle,$$

por lo que un estado coherente se mantiene coherente con el paso del tiempo

$$\left|\alpha,t\right\rangle = e^{-i\omega t/2}\left|\alpha e^{-i\omega t}\right\rangle \tag{2.53}$$

con una fase que cambia según ωt y un número promedio de fotones $|\alpha|^2$ constante [1].

Si se usan los operadores de cuadratura como ejes de un espacio de fases, el área limitada por la incertidumbre de $\hat{X}_1$ y $\hat{X}_2$ crea la gráfica observada en la figura 2.2. Los estados coherentes provocan esta misma área de incertidumbre, pero desplazada una distancia $|\alpha|$ y un ángulo θ, de la manera en la que se presenta en la figura 2.3.

El *desplazamiento* que produce los estados coherentes desde el estado de vacío $|0\rangle$ está detallado en el operador de desplazamiento [12]

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}. \tag{2.54}$$

Para trabajar con este operador, se requiere el teorema de desenredamiento

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-\frac{1}{2}\left[\hat{A}+\hat{B}\right]} = e^{\hat{B}}e^{\hat{A}}e^{\frac{1}{2}\left[\hat{A},\hat{B}\right]}, \tag{2.55}$$

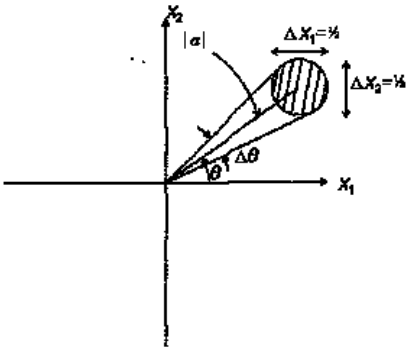

Figura 2.3. Incertidumbre en el espacio de fases para estados coherentes, elaborada por Gerry y Knight [12].

para $\left[\hat{A},\hat{B}\right] \neq 0$ y $\left[\hat{A},\left[\hat{A},\hat{B}\right]\right] = \left[\hat{B},\left[\hat{A},\hat{B}\right]\right] = 0$ [12]. Así, el operador de desplazamiento queda

$$\hat{D}(\alpha) = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}},$$

cuyo efecto sobre el estado de vacío, operador por operador, es

$$e^{-\alpha^*\hat{a}}\,|0\rangle = \sum_{n=0}^{\infty} \frac{(-\alpha^*\hat{a})^n}{n!}\,|0\rangle = |0\rangle$$

gracias a que $\hat{a}^0 = 1$ [12]. Luego, usando (2.26),

$$e^{\alpha\hat{a}^\dagger}\,|0\rangle = \sum_{n=0}^{\infty} \frac{(\alpha^n)}{n!}\left(\hat{a}^\dagger\right)^n |0\rangle = \sum_{n=0}^{\infty} \frac{(\alpha^n)}{\sqrt{n!}}\,|n\rangle\,.$$

Entonces, comparando con la ecuación (2.46), resulta que [12]

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,. \tag{2.56}$$

Tomando la forma *desenredada* del operador de desplazamiento, se tiene que el adjunto de este como

$$\hat{D}^\dagger(\alpha) = \left(e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}\right)^\dagger = e^{-\frac{1}{2}|\alpha|^2} \left(e^{-\alpha^*\hat{a}}\right)^\dagger \left(e^{\alpha\hat{a}^\dagger}\right)^\dagger,$$

y haciendo por separado

$$\left(e^{-\alpha^*\hat{a}}\right)^\dagger = \sum_{n=0}^{\infty} \frac{\left(-\alpha\hat{a}^\dagger\right)^n}{n!} = e^{-\alpha\hat{a}^\dagger},$$

$$\left(e^{\alpha\hat{a}^\dagger}\right)^\dagger = \sum_{n=0}^{\infty} \frac{(\alpha^*\hat{a})^n}{n!} = e^{\alpha^*\hat{a}},$$

de manera que [12]

$$\hat{D}^\dagger(\alpha) = e^{-\frac{1}{2}|\alpha|^2} e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}}.$$

Con la otra forma desenredada de $\hat{D}(\alpha)$

$$\hat{D}(\alpha) = e^{\frac{1}{2}|\alpha|^2} e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger},$$

se puede hacer

$$\hat{D}(\alpha)\hat{D}^\dagger(\alpha) = e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger} e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}},$$

y utilizando el Teorema de desenredamiento (2.55) con el hecho de que cualquier operador conmuta consigo mismo, se obtiene entonces [12]

$$\hat{D}(\alpha)\hat{D}^\dagger(\alpha) = \hat{D}^\dagger(\alpha)\hat{D}(\alpha) = 1. \tag{2.57}$$

Es decir, el operador de desplazamiento es unitario [12].

Los posibles operadores de desplazamiento del vacío forman un semigrupo [12]. Tomando de nuevo el teorema de desenredamiento (2.55), y usando $\hat{A} = \alpha\hat{a}^\dagger - \alpha^*\hat{a}$ y $\hat{B} = \beta\hat{a}^\dagger - \beta^*\hat{a}$ con $\left[\hat{A}, \hat{B}\right] = \alpha\beta^* - \alpha^*\beta = 2i\mathrm{Im}\,(\alpha\beta^*)$, se tiene el producto

$$\hat{D}(\alpha)\hat{D}(\beta) = e^{\hat{A}} e^{\hat{B}} = e^{i\mathrm{Im}(\alpha\beta^*)} e^{(\alpha+\beta)\hat{a}^\dagger - (\alpha+\beta)^*\hat{a}},$$

que fácilmente se simplifica

$$\hat{D}(\alpha)\hat{D}(\beta) = e^{i\mathrm{Im}(\alpha\beta^*)}\hat{D}(\alpha+\beta), \tag{2.58}$$

donde el factor de fase es físicamente irrelevante [12].

Es importante notar que los estados coherentes no son ortogonales, y solo son completos sobre el plano complejo de α [12]. La no-ortogonalidad se observa como

$$\langle\beta|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2} \sum_{n,m=0}^{\infty} \frac{\beta^{*n}\alpha^m}{\sqrt{n!m!}} \langle n|m\rangle = e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2} \sum_{n=0}^{\infty} \frac{(\beta^*\alpha)^n}{n!},$$

de forma que

$$\langle\beta|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2 + \beta^*\alpha},$$

y se simplifica hacia

$$\langle\beta|\alpha\rangle = e^{\frac{1}{2}(\beta^*\alpha-\beta\alpha^*)}e^{-\frac{1}{2}|\beta-\alpha|^2}, \tag{2.59}$$

donde el primer exponencial es una fase compleja [12]. Entonces, la probabilidad de medir $|\beta\rangle$ como proyección del estado $|\alpha\rangle$ es

$$|\langle\beta|\alpha\rangle|^2 = e^{-|\beta-\alpha|^2},$$

lo cual solo presenta ortogonalidad aproximada cuando la diferencia entre α y β es muy grande [12].

La completitud en el plano complejo se observa de la siguiente manera

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha|\, d^2\alpha = \frac{1}{\pi}\int e^{-|\alpha|^2}\sum_{n,m}\frac{\alpha^n\alpha^{*m}}{\sqrt{n!m!}}\,|n\rangle\langle m|\, d^2\alpha,$$

tomando $d^2\alpha = d\mathrm{Re}(\alpha)d\mathrm{Im}(\alpha)$ [12]. Esto permite pasar a coordenadas polares con $\alpha = re^{i\theta}$ y $d^2\alpha = rdrd\theta$ [12]

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha|\, d^2\alpha = \sum_{n,m}\frac{|n\rangle\langle m|}{\sqrt{n!m!}}\int_0^\infty e^{-r^2}r^{n+m+1}dr\int_0^{2\pi}e^{i(n-m)\theta}d\theta.$$

La última integral es la definición integral de la delta de Kronecker [12]

$$\int_0^{2\pi}e^{i(n-m)\theta}d\theta = 2\pi\delta_{nm}.$$

Reemplazando esto, y haciendo el cambio de variables $r^2 = y$ y $2rdr = dy$ se tiene

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha|\, d^2\alpha = \sum_n\frac{|n\rangle\langle n|}{n!}\int_0^\infty e^{-y}y^n dy,$$

y como

$$\int_0^\infty e^{-y}y^n dy = \Gamma(n+1) = n!,$$

en total se tiene

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha|\, d^2\alpha = \sum_n |n\rangle\langle n| = 1,$$

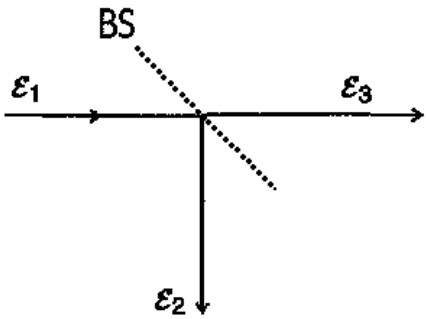

Figura 2.4. Diagrama de un divisor de haz en acción, elaborada por Gerry y Knight [12].

mostrando la completitud. Un vector en general se puede expresar [12]

$$|\psi\rangle = \frac{1}{\pi}\int |\alpha\rangle \langle\alpha|\psi\rangle \, d^2\alpha.$$

Para un estado coherente, esto da [12]

$$|\beta\rangle = \frac{1}{\pi}\int |\alpha\rangle \, e^{-\frac{1}{2}|\alpha|^2-\frac{1}{2}|\beta|^2+\beta^*\alpha} d^2\alpha,$$

Es decir, el conjunto de estados coherentes no es linealmente independiente; además, son *sobrecompletos*, lo que significa que hay más que suficientes elementos para expresar cualquier estado en términos de los estados coherentes [12].

2.5. Aplicaciones

2.5.1. Divisores de haz

Clásicamente, un divisor de haz sin pérdidas es un elemento óptico en el que al ingresar un haz de luz, emite un haz transmitido y un haz reflejado, y las intensidades de los haces transmitido y reflejado suman la intensidad del haz incidente [12]. La figura 2.4 provee una representación gráfica de dicho elemento. Matemáticamente, se tiene que la amplitud compleja $\mathcal{E}_1$ del haz incidente está asociada con las amplitudes reflejada y transmitida $\mathcal{E}_2$ y $\mathcal{E}_3$ de acuerdo a

$$\mathcal{E}_2 = r\mathcal{E}_2, \qquad \mathcal{E}_3 = t\mathcal{E}_1, \tag{2.60}$$

donde los coeficientes r y t son complejos [12]. Considerando que no hay pérdidas de energía, las intensidades $|\mathcal{E}|^2$ cumplen con

$$|\mathcal{E}_1|^2 = |\mathcal{E}_2|^2 + |\mathcal{E}_3|^2 , \tag{2.61}$$

que a su vez impone [12]

$$|r|^2 + |t|^2 = 1. \tag{2.62}$$

Para un divisor $50:50$, que divide el haz incidente en dos haces de exactamente la misma intensidad, se requiere que [12]

$$|r| = |t| = \frac{1}{\sqrt{2}}.$$

Para hacer la cuantización del efecto del divisor de haz, en primera instancia podría pensarse en reemplazar las amplitudes complejas de los haces con operadores de aniquilación, haciendo analogía con el modelo clásico [12]

$$\hat{a}_2 = r\hat{a}_1, \qquad\qquad \hat{a}_3 = t\hat{a}_1.$$

Estos operadores deben cumplir con las relaciones de conmutación (2.15)

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{ij},$$

$$[\hat{a}_i, \hat{a}_j] = \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger\right] = 0,$$

para $i, j = 1, 2, 3$ correspondientes a los haces incidente, reflejado y transmitido [12]. Sin embargo, las relaciones de conmutación de los operadores a partir de sus definiciones por la analogía clásica son

$$\left[\hat{a}_2, \hat{a}_2^\dagger\right] = |r|^2 \left[\hat{a}_1, \hat{a}_1^\dagger\right] = |r|^2 ,$$

$$\left[\hat{a}_3, \hat{a}_3^\dagger\right] = |t|^2 \left[\hat{a}_1, \hat{a}_1^\dagger\right] = |t|^2 ,$$

$$\left[\hat{a}_2, \hat{a}_3^\dagger\right] = rt^* \neq 0,$$

es decir, no se conservan las relaciones de conmutación y, por tanto, no es una descripción cuántica adecuada del divisor de haz [12].

La inefectividad de la analogía entre clásico y cuántico surge del estado de

vacío, que a nivel clásico siempre se ignora [12]. El divisor de haz tiene dos puertos de incidencia, pero por lo general solo se usa uno, como se ve en la figura 2.4; el otro, colineal a $\mathcal{E}_2$, se deja vacío y sin efecto clásico sobre los haces reflejado y transmitido [12]. Cuánticamente, el vacío es un eigenestado de energía con efectos físicos reales, de manera que el otro puerto de incidencia tiene una entrada $|0\rangle$, y afecta los estados de salida del divisor [12]. Entonces, esta incidencia de vacío tiene asociados un operador $\hat{a}_0$ y coeficientes de reflexión y transmisión [12]. Tomando en cuenta que la reflexión de $\mathcal{E}_1$ es la transmisión de $|0\rangle$, y viceversa, los operadores de campo para los haces de salida quedan [12]

$$\hat{a}_2 = r\hat{a}_1 + t'\hat{a}_0, \qquad \hat{a}_3 = t\hat{a}_1 + r'\hat{a}_0. \tag{2.63}$$

Las relaciones de conmutación son ahora [12]

$$\left[\hat{a}_2, \hat{a}_2^\dagger\right] = \left[r\hat{a}_1 + t'\hat{a}_0, r^*\hat{a}_1^\dagger + t'^*\hat{a}_0^\dagger\right] = |r|^2 + |t'|^2,$$

$$\left[\hat{a}_3, \hat{a}_3^\dagger\right] = |r'|^2 + |t|^2,$$

$$[\hat{a}_2, \hat{a}_3] = [r\hat{a}_1 + t'\hat{a}_0, t\hat{a}_1 + r'\hat{a}_0] = 0,$$

$$\left[\hat{a}_2^\dagger, \hat{a}_3^\dagger\right] = 0,$$

$$\left[\hat{a}_2, \hat{a}_3^\dagger\right] = \left[r\hat{a}_1 + t'\hat{a}_0, t^*\hat{a}_1^\dagger + r'^*\hat{a}_0^\dagger\right] = rt^* + t'r'^*,$$

$$\left[\hat{a}_3, \hat{a}_2^\dagger\right] = \left[t\hat{a}_1 + r'\hat{a}_0, r^*\hat{a}_1^\dagger + t'^*\hat{a}_0^\dagger\right] = tr^* + r't'^*.$$

Se requiere que $|r|^2 + |t'|^2 = |r'|^2 + |t|^2 = 1$ y $tr^* + r't'^* = 0$ [12]. De esta última se tiene que $|r|\,|t| = |r'|\,|t'|$, con lo que se puede hacer

$$|r|^2 + \left(\frac{|r|\,|t|}{|r'|}\right)^2 = |r'|^2 + |t|^2,$$

y factorizando

$$\left(\frac{|r|}{|r'|}\right)^2 \left(|r'|^2 + |t|^2\right) = |r'|^2 + |t|^2,$$

de manera que

$$|r| = |r'|,$$

que a su vez implica

$$|t| = |t'|,$$

y por tanto [12]

$$|r|^2 + |t|^2 = 1.$$

Dado que un divisor de haz es una capa de material que refleja y transmite luz, los estados fotónicos reflejados y los transmitidos están desfasados [12]. Si el divisor consiste en una sola capa de dieléctrico, el desfase es de $e^{\pm i\pi/2} = \pm i$ [12]. Entonces, para un divisor $50:50$ con un desfase de $\pi/2$, las relaciones en (2.63) y sus condiciones de conmutación arrojan [12]

$$\hat{a}_2 = \frac{1}{\sqrt{2}}\left(\hat{a}_0 + i\hat{a}_1\right), \qquad \hat{a}_3 = \frac{1}{\sqrt{2}}\left(i\hat{a}_0 + \hat{a}_1\right). \tag{2.64}$$

Como cualquier estado fotónico $|n\rangle$ se puede construir con operadores de creación actuando sobre el vacío $|0\rangle$, entonces se pueden hallar los estados de salida del divisor correspondientes a sus estados de entrada, partiendo del hecho de que una entrada de vacío produce una salida vacía $|0\rangle_0 |0\rangle_1 \to |0\rangle_2 |0\rangle_3$ [12]. Para el caso en el hay un solo fotón en la entrada

$$|0\rangle_0 |1\rangle_1 = \hat{a}_1^\dagger |0\rangle_0 |0\rangle_1,$$

despejando

$$\hat{a}_1^\dagger = \frac{1}{\sqrt{2}}\left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger\right), \tag{2.65}$$

y partiendo de la relación entrada-salida con vacíos, se tiene [12]

$$|0\rangle_0 |1\rangle_1 \to \frac{1}{\sqrt{2}}\left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger\right)|0\rangle_2 |0\rangle_3,$$

que provocan

$$|0\rangle_0 |1\rangle_1 \to \frac{1}{\sqrt{2}}\left(i\,|1\rangle_2 |0\rangle_3 + |0\rangle_2 |1\rangle_3\right). \tag{2.66}$$

En la formulación de Heisenberg, esta transformación está dada por el operador unitario [12]

$$U_{BS} = e^{i\frac{\pi}{4}\left(\hat{a}_0^\dagger \hat{a}_1 + \hat{a}_0 \hat{a}_1^\dagger\right)} \tag{2.67}$$

Como es de esperarse, el divisor de haz $50:50$ le da a un solo fotón incidente un $50\,\%$ de probabilidades de reflejarse y $50\,\%$ de transmitirse [12]. Además, el estado de salida *es un estado entrelazado* [12].

Para un estado en el que hay un fotón en cada puerto de incidencia, $|1\rangle_0 |1\rangle_1$,

usando

$$\hat{a}_0^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}_2^\dagger + i\hat{a}_3^\dagger\right), \tag{2.68}$$

lleva a

$$|1\rangle_0 |1\rangle_1 \to \frac{1}{2}\left(\hat{a}_2^\dagger + i\hat{a}_3^\dagger\right)\left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger\right)|0\rangle_2 |0\rangle_3 = \frac{i}{2}\left[\left(\hat{a}_2^\dagger\right)^2 + \left(\hat{a}_3^\dagger\right)^2\right]|0\rangle_2 |0\rangle_3 ,$$

que se opera como [12]

$$|1\rangle_0 |1\rangle_1 \to \frac{i}{\sqrt{2}}\left(|2\rangle_2 |0\rangle_3 + |0\rangle_2 |2\rangle_3\right). \tag{2.69}$$

Cuando entra un fotón en cada puerto de incidencia, los dos fotones pasan juntos a uno solo de los puertos de salida [12]. Esto sucede debido a que, como se ve al hacer la multiplicación de (2.68) y (2.65), los dos posibles estados $|1\rangle_2 |1\rangle_3$ interfieren destructivamente entre sí y desaparecen del estado total [12].

Cuando en un puerto de entrada incide un estado coherente, el efecto del divisor de haz es el esperado para luz clásica: se toma $|0\rangle_0 |\alpha\rangle_1 = \hat{D}_1(\alpha)|0\rangle_0 |0\rangle_1$ con $\hat{D}_1(\alpha)$ definido en (2.54), de manera que

$$|0\rangle_0 |\alpha\rangle_1 \to e^{\frac{\alpha}{\sqrt{2}}\left(i\hat{a}_2^\dagger + \hat{a}_3^\dagger\right) - \frac{\alpha^*}{\sqrt{2}}(\hat{a}_3 - i\hat{a}_2)}|0\rangle_2 |0\rangle_3 ,$$

expandiendo

$$|0\rangle_0 |\alpha\rangle_1 \to e^{\frac{i\alpha}{\sqrt{2}}\hat{a}_2^\dagger + \frac{\alpha}{\sqrt{2}}\hat{a}_3^\dagger - \frac{\alpha^*}{\sqrt{2}}\hat{a}_3 + \frac{i\alpha^*}{\sqrt{2}}\hat{a}_2}|0\rangle_2 |0\rangle_3 ,$$

y reagrupando

$$|0\rangle_0 |\alpha\rangle_1 \to \hat{D}_2\left(\frac{i\alpha}{\sqrt{2}}\right)\hat{D}_3\left(\frac{\alpha}{\sqrt{2}}\right)|0\rangle_2 |0\rangle_3 ,$$

para resultar en

$$|0\rangle_0 |\alpha\rangle_1 \to \left|\frac{i\alpha}{\sqrt{2}}\right\rangle_2 \left|\frac{\alpha}{\sqrt{2}}\right\rangle_3 , \tag{2.70}$$

donde en cada puerto de salida está la mitad de la intensidad del puerto de entrada, $|\alpha|^2/2$ [12].

El interferómetro de Mach-Zehnder (MZI, por sus siglas en inglés) es un aparato óptico que utiliza dos divisores de haz $50:50$ para provocar interferencia entre estados cuánticos con un solo fotón [12]. El esquema básico del MZI está dado en la figura 2.5. En este diagrama, los componentes M corresponden a espejos y los

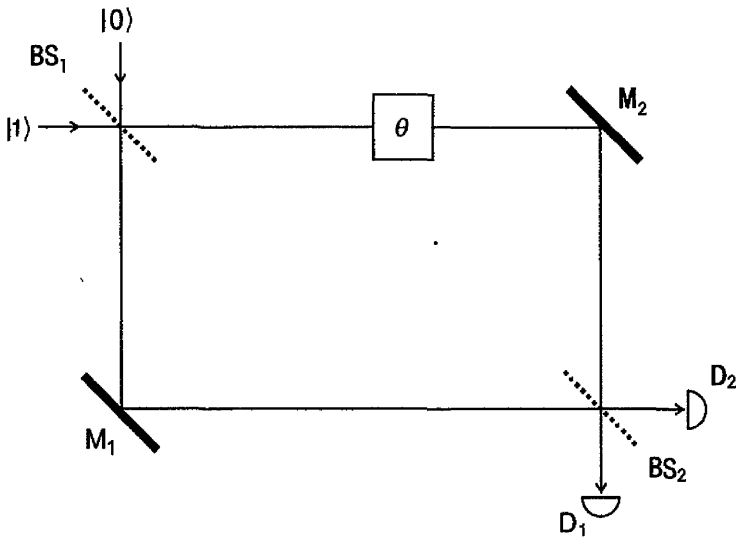

Figura 2.5. Diagrama de interferómetro de Mach-Zehnder con un solo fotón, elaborada por Gerry y Knight [12].

componentes D corresponden a detectores al final de cada posible trayectoria del fotón [12]. El componente etiquetado con θ es un desplazador de fase óptica, que puede consistir en un tramo de fibra óptica cuya longitud determina θ, y está matemáticamente representado por el operador unitario $e^{i\theta\hat{n}}$; el desfase θ es relativo entre las dos trayectorias [12].

El estado de entrada al MZI es el estado producto $|0\rangle|1\rangle$, usándose que el primer estado factor es el de la trayectoria en sentido antihorario, y el segundo es el de la horaria [12]. El efecto del primer divisor de haz está dado por (2.66)

$$|0\rangle|1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + i|1\rangle|0\rangle\right).$$

Cada espejo provoca un desfase de $\pi/2$, pero ambas trayectorias tienen un espejo, así que este desfase es irrelevante [12]. El desplazador de fase está en la trayectoria horaria, así que solo afectará el componente donde el fotón tome esa trayectoria [12]

$$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + i|1\rangle|0\rangle\right) \to \frac{1}{\sqrt{2}}\left(e^{i\theta}|0\rangle|1\rangle + i|1\rangle|0\rangle\right).$$

Usando (2.68) y (2.65), se halla la transformación causada por el segundo divisor de haz [12]. Manteniendo la regla de que la trayectoria antihoraria (terminando en

D_1) precede a la trayectoria horaria (terminando en D_2), se tiene [12]

$$|0\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + i|1\rangle|0\rangle\right),$$

$$|1\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|1\rangle|0\rangle + i|0\rangle|1\rangle\right).$$

De esta manera, la transformación del estado total por el segundo divisor es [12]

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

Entonces, el MZI produce una transformación total

$$|0\rangle|1\rangle \rightarrow \frac{1}{2}\left[\left(e^{i\theta}-1\right)|0\rangle|1\rangle + i\left(e^{i\theta}+1\right)|1\rangle|0\rangle\right], \tag{2.71}$$

donde D_2 sería activado por el estado $|0\rangle|1\rangle$, mientras D_1 detectaría $|1\rangle|0\rangle$, con probabilidades $P_{01} = \frac{1}{2}(1-\cos\theta)$ y $P_{10} = \frac{1}{2}(1+\cos\theta)$, respectivamente [12].

2.5.2. Interacción Kerr

La forma más simple de polarización dieléctrica corresponde a la forma lineal

$$\vec{P}(\vec{r},t) = \epsilon_0 \chi^{(1)} \vec{E}(\vec{r},t)$$

para un medio isotrópico, donde $\chi^{(1)}$ es la susceptibilidad lineal del dieléctrico [1]. Para un medio no-isotrópico, la susceptibilidad pasa a ser un tensor de rango 2, y cada componente del vector de polarización está dada por [1]

$$P_i(\vec{r},t) = \epsilon_0 \chi^{(1)}_{ij} E_j(\vec{r},t).$$

La polarización lineal es una aproximación para un campo eléctrico externo débil [1]. Al crecer el campo eléctrico, la polarización entra en régimen no-lineal descrito por

$$P_i = \epsilon_0 \chi^{(1)}_{ij} E_j + \epsilon_0 \chi^{(2)}_{ijk} E_j E_k + \epsilon_0 \chi^{(3)}_{ijkl} E_j E_k E_l,$$

o, en un medio isotrópico,

$$\vec{P}(\vec{r},t) = \epsilon_0 \chi^{(1)} \vec{E}(\vec{r},t) + \epsilon_0 \chi^{(3)} \left|\vec{E}\right|^2 \vec{E}(\vec{r},t),$$

ecuación que proviene de una expansión de Taylor de la susceptibilidad en términos de intensidad de campo eléctrico en un modelo de átomos de dos niveles [1]. La polarización de tercer orden es conocida como *efecto Kerr* [1]. Por otro lado, muchos medios que exhiben un efecto Kerr significativo tienen una $\chi^{(2)}$ despreciable [1].

Es posible clasificar el efecto Kerr en dos variantes. La primera es el efecto Kerr electro-óptico, en el cual un potente campo eléctrico estable se utiliza para modificar las propiedades ópticas de un medio dieléctrico [1]. La otra variante es el efecto Kerr óptico, en el cual una luz incidente produce el efecto Kerr a su paso a través del material [1]. Una de las consecuencias del efecto Kerr óptico es el efecto o interacción Kerr cruzada: cuando dos ondas electromagnéticas entran en un medio Kerr, la propagación de estas con una susceptibilidad no-lineal produce un acoplamiento no-lineal entre las ondas [1].

Cuánticamente, el efecto Kerr puede modelarse como una *auto-interacción* (sin campos paramétricos que provoquen el efecto) de la luz con hamiltoniano

$$\hat{H}_I = \hbar K \left(\hat{a}^\dagger \hat{a}\right)^2 = \hbar K \hat{n}^2, \tag{2.72}$$

donde K es proporcional a la susceptibilidad no-lineal de tercer orden, $\chi^{(3)}$ [12]. Sobre un estado coherente, la evolución unitaria bajo este hamiltoniano puede producir un tipo de estado entrelazado conocido como estado de Yurke-Stoler [12]. La evolución temporal es [12]

$$e^{i\hat{H}_I t/\hbar} |\alpha\rangle = e^{iK\hat{n}^2 t} |\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} e^{iKn^2 t} |n\rangle = |\psi(t)\rangle .$$

Si se usa una interacción de duración $t = \frac{\pi}{2K}$, se tiene un estado de salida [12]

$$\left|\psi\left(\frac{\pi}{2K}\right)\right\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} e^{i\pi n^2/2} |n\rangle .$$

Los valores de $e^{i\pi n^2/2}$, dado que $n \in \mathbb{Z}$, solo son dos, 1 para n par, y $-i$ para n impar [12]. Así, el estado de salida queda

$$\left|\psi\left(\frac{\pi}{2K}\right)\right\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \left(\frac{\alpha^{2n}}{\sqrt{(2n)!}} |2n\rangle - i \frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}} |2n+1\rangle \right),$$

y agregando términos que suman 0 entre sí

$$\left|\psi\left(\frac{\pi}{2K}\right)\right\rangle = \frac{e^{-\frac{1}{2}|\alpha|^2}}{2}\sum_{n=0}^{\infty}\left(\frac{\alpha^{2n}}{\sqrt{(2n)!}}\left|2n\right\rangle + \frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}\left|2n+1\right\rangle - i\frac{\alpha^{2n}}{\sqrt{(2n)!}}\left|2n\right\rangle\right.$$

$$-i\frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}\left|2n+1\right\rangle + i\frac{\alpha^{2n}}{\sqrt{(2n)!}}\left|2n\right\rangle - i\frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}\left|2n+1\right\rangle$$

$$\left.+\frac{\alpha^{2n}}{\sqrt{(2n)!}}\left|2n\right\rangle - \frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}\left|2n+1\right\rangle\right),$$

que se resumen en

$$\left|\psi\left(\frac{\pi}{2K}\right)\right\rangle = \frac{1-i}{2}\left(\left|\alpha\right\rangle + i\left|-\alpha\right\rangle\right),$$

o bien

$$\left|\psi\left(\frac{\pi}{2K}\right)\right\rangle = \frac{1}{\sqrt{2}}e^{-i\pi/4}\left(\left|\alpha\right\rangle + i\left|-\alpha\right\rangle\right), \tag{2.73}$$

el cual, independientemente de la fase global, es el estado entrelazado conocido como Yurke-Stoler [12].

Una forma más realista de interacción Kerr cuántica está dada por el hamiltoniano

$$\hat{H}_I = \hbar K\left(\hat{a}^\dagger\right)^2\hat{a}^2 = \hbar K\left(\hat{n}^2 - \hat{n}\right), \tag{2.74}$$

que, tomando en cuenta el teorema (2.55) y el procedimiento de (2.53), provoca una evolución de forma [12]

$$\left|\psi(t)\right\rangle = e^{-iKt\left(\hat{n}^2-\hat{n}\right)}\left|\alpha\right\rangle = e^{-iKt\hat{n}^2}\left|\alpha e^{iKt}\right\rangle.$$

Tomando $t = \frac{\pi}{2K}$, se puede usar el resultado (2.73) para obtener que

$$\left|\psi\left(\frac{\pi}{2K}\right)\right\rangle = \frac{1}{\sqrt{2}}e^{-i\pi/4}\left(\left|\beta\right\rangle + i\left|-\beta\right\rangle\right),$$

donde la amplitud del estado coherente se ha rotado hacia $\beta = i\alpha$ [12]. Entonces, se vuelve a obtener el estado de Yurke-Stoler [12].

En la figura 2.6, se puede observar una forma de aplicar el efecto Kerr cruzado para acoplar estados cuánticos de la luz, en este caso, con un MZI [12]. Como se puede ver, en los modos b y c del interferómetro entran estados número o fotónicos; por otro lado, hay un modo a externo al interferómetro, que se acopla a este a través

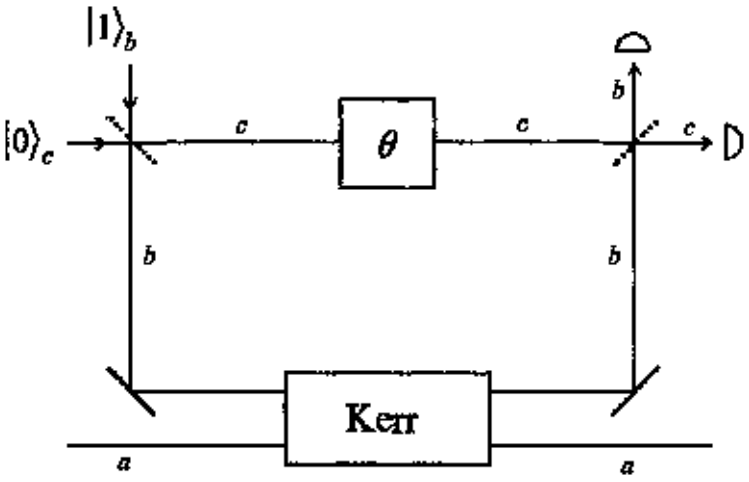

Figura 2.6. Diagrama de interferómetro de Mach-Zehnder acoplado a un medio no lineal, elaborada por Gerry y Knight [12].

de la interacción Kerr [12]. El MZI y sus elementos ya han sido presentados en la sección 2.5.1. El elemento adicional, la interacción Kerr cruzada, está dado por el hamiltoniano [12]

$$\hat{H}_{CK} = \hbar K \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b} = \hbar K \hat{n}_a \hat{n}_b. \tag{2.75}$$

Comparando este hamiltoniano con el de (2.72), se hace notar el cambio de operador número cuadrado para la auto-interacción, hacia un operador número para cada modo que se acopla. La evolución unitaria en el tiempo generada por este hamiltoniano queda [12]

$$\hat{U}_{CK} = e^{-iKt\hat{n}_a\hat{n}_b}. \tag{2.76}$$

En esta, como en todas las interacciones Kerr, el tiempo de interacción se modula de acuerdo a la velocidad de la luz v en el medio y la longitud l que la luz recorre en el medio, de manera que $t = l/v$ [12]. De la sección 2.5.1, se tiene que la evolución unitaria del desplazador de fase es

$$\hat{U}_{PS} = e^{i\theta\hat{n}_c}, \tag{2.77}$$

y los divisores de haz y detectores son del mismo tipo que en la sección mencionada [12]. Partiendo estas condiciones y poniendo un estado coherente a la entrada del modo a, el estado después del primer divisor es [12]

$$|\psi\rangle = \frac{1}{\sqrt{2}} |\alpha\rangle_a \left(|10\rangle_{bc} + i\, |01\rangle_{bc} \right).$$

Después del paso por el medio Kerr y por el desplazador de fase, contando con que cada operador actúa sólo sobre su respectivo modo, el estado es

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(\left| e^{-iKt}\alpha \right\rangle_a |10\rangle_{bc} + ie^{i\theta} |\alpha\rangle_a |01\rangle_{bc} \right),$$

donde la presencia de un fotón en el modo b es lo que permite al operador $\hat{U}_{CK}$ actuar también sobre el modo a [12]. Eligiendo para la interacción Kerr que $Kt = \pi$, este estado queda [12]

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|-\alpha\rangle_a |10\rangle_{bc} + ie^{i\theta} |\alpha\rangle_a |01\rangle_{bc} \right).$$

Tras pasar el segundo divisor de haz, el estado total final es

$$|\psi\rangle = \frac{1}{2} \left[\left(|-\alpha\rangle_a - e^{i\theta} |\alpha\rangle_a \right) |10\rangle_{bc} + i \left(|-\alpha\rangle_a + e^{i\theta} |\alpha\rangle_a \right) |01\rangle_{bc} \right],$$

de manera que, al realizar una medida en los detectores del MZI, un estado entrelazado inevitablemente se proyectará en el modo a, y las características específicas de dicho estado se pueden modular con el desplazador de fase [12].

2.5.3. Computación cuántica

Los fotones son fáciles de producir y manipular, tienen un espín a la vez que pueden ser tratados como sistemas de variable continua [11]. Por estas razones, son buenos candidatos para ser portadores de información cuántica [11]. Tanto el espín de los fotones como sus estados número se pueden usar para almacenar y manipular información cuántica, pero ambas opciones tienen desventajas importantes [11]. En el caso de la codificación por polarización (espín), la naturaleza bosónica de los fotones impide que tengan comportamientos no-lineales naturalmente; por tal razón se utilizan no-linealidades inducidas por medición, donde la combinación de transformaciones unitarias, modos fotónicos auxiliares y fotodetección producen no-linealidades efectivas, pero este método está sujeto a cierta probabilidad de éxito y fracaso [11].

En el caso de la codificación de información cuántica en estados número (o de Fock), se requieren compuertas lógicas cuánticas que actúen dentro de la misma capa de Fock, es decir, que conserven el número total de fotones durante las operaciones [11]. Las compuertas que no cumplen con esta condición, requieren una gran

cantidad de recursos adicionales para implementarse a menos que se implemente otro método de codificación complementario [11]. Otro problema que surge en este enfoque proviene del uso de efecto Kerr para implementar algunas compuertas, y las dificultades experimentales para provocar dicho fenómeno en la magnitud necesaria [12].

En general, la óptica como implementación de computación cuántica ofrece la ventaja tiempos de operación de compuerta muy cortos, limitados únicamente por el tiempo de operación de los fotodetectores [11]. Las principales desventajas son: el ensamblado de los sistemas de interferometría requeridos, y el emparejamiento de modos en grandes redes [11]. En el siguiente capítulo se describirá una de las posibles implementaciones de compuertas lógicas cuánticas utilizando óptica cuántica.

3. IMPLEMENTACIÓN DE COMPUERTAS CUÁNTICAS EN ÓPTICA CUÁNTICA

3.1. Introducción

El procesamiento de información cuántica en un sistema físico específico requiere de un conjunto de condiciones mínimas que permitan implementar la computación cuántica con errores tolerables [9]. En primer lugar, se necesita que el sistema provea una representación física robusta de qubit, de manera que este mantenga sus propiedades cuánticas durante un proceso de computación. La segunda condición es que sea posible implementar un Conjunto Universal de Compuertas cuánticas en la representación elegida, de manera que los qubits sean manipulables. También debe ser posible preparar el sistema en estados iniciales específicos. Y finalmente, se requiere la capacidad de medir una salida tras un proceso computacional.

Estas condiciones deben balancearse para ser efectivas, dado que algunas pueden ser contradictorias entre sí: por ejemplo, el sistema debe estar lo suficientemente aislado para que el qubit pueda mantenerse en una superposición de estados cuánticos, pero no puede estar tan aislado que no haya capacidad de medición [9].

En el Capítulo 2 se estableció la cuantización escalar del campo electromagnético y los efectos que dicha cuantización tiene en el tratamiento de la luz [9]. Además, con el interferómetro de Mach-Zehnder, se pudo observar que se pueden establecer estados cuánticos superpuestos respecto a la información sobre la trayectoria que tome un fotón [9]. A partir de estas ideas, se plantea la *representación de doble riel* (traducción de *dual-rail representation*) de la computación cuántica: un qubit consiste en la información sobre la trayectoria tomada por un fotón de entre dos posibles caminos (de ahí el nombre doble riel), donde la superposición de estados corresponde a una superposición de las dos posibles trayectorias del fotón y una medición consiste en ubicar al fotón en una de estas posiciones [9]. El esquema

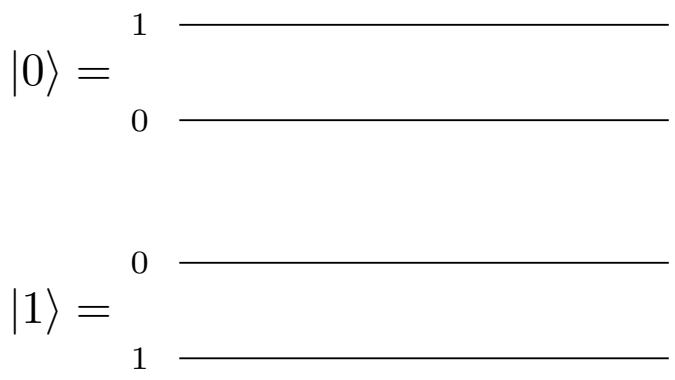

Figura 3.1. Base computacional de un qubit en representación de doble riel, elaboración propia con el diseño de Nielsen y Chuang [9].

gráfico de la representación de doble riel, con una trayectoria superior y una inferior, y su correspondencia a la base computacional de qubits se encuentra en la figura 3.1.

Experimentalmente, es posible obtener un solo fotón a partir de un estado coherente $|\alpha\rangle$ [9]. Estos estados son radiados por osciladores forzados, como el láser, cuando son bombeados muy por encima de su umbral de emisión; atenuando esta luz se pueden conseguir bajas cantidades de fotones con altas probabilidades: por ejemplo, para un estado con $\alpha = \sqrt{0.1}$, se obtiene el estado atenuado

$$\sqrt{0.90}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + \ldots,$$

de manera que, si se detecta luz que traspasa el atenuador, es altamente probable que sea un solo fotón [9]. Para mejorar la sincronicidad entre fotones, se puede utilizar conversión paramétrica espontánea, con materiales ópticos no lineales como el KH_2PO_4, los cuales reciben un fotón de frecuencia ω_0 y emiten dos fotones cuánticamente entrelazados de frecuencias ω_1 y ω_2 tal que $\omega_1 + \omega_2 = \omega_0$ [9]. Esto, junto a la conservación de momentum, permite usar la detección de un fotón para determinar la existencia de otro fotón sin absorberlo [9]. Utilizando esta detección como condición para que otro fotón sea dejado pasar, se pueden sincronizar múltiples fuentes fotónicas [9].

Los instrumentos ópticos lineales (espejos, desplazadores de fase óptica y divisores de haz) junto a medios no lineales, permiten *en principio* implementar un Conjunto Universal de Compuertas cuánticas como el descrito en el Capítulo 1 en

el modelo de doble riel [9].

La medición de fotones individuales se puede realizar con alta eficiencia cuántica con diversas tecnologías [9]. La eficiencia cuántica es la probabilidad $0 < \eta < 1$ de que un fotón incidente provoque una señal eléctrica medible [9].

De esta manera, el modelo de doble riel cumple en principio con los 4 requerimientos de un sistema físico para poder realizar computación cuántica: [9]

1. Se tiene una representación robusta de qubits dado que los fotones pueden viajar largas distancias y sólo interactúan entre sí en condiciones específicas, conservando sus propiedades cuánticas con facilidad.

2. Existe la posibilidad de implementar un Conjunto Universal de Compuertas cuánticas con medios ópticos existentes.

3. Se pueden generar fotones individuales con sincronicidad modulable, para preparar estados iniciales (que pueden ser modificados con compuertas lógicas cuánticas según la necesidad).

4. Finalmente, se pueden realizar las mediciones proyectivas requeridas para determinar el estado del sistema en la base computacional.

Sin embargo, hay que tomar en cuenta que existen dificultades en el uso de medios ópticos no lineales para la implementación de compuertas; es decir, un impedimento respecto a la segunda condición [9]. Además, otra dificultad con este modelo de computación está en la complejidad experimental del ensamblaje de los sistemas de interferometría, especialmente por la exacta alineación necesaria para que funcionen [9].

3.2. Implementaciones

3.2.1. Compuertas de un qubit

3.2.1.1. Compuerta NOT

Una compuerta **NOT** o σ_x realiza el cambio $\alpha |0\rangle + \beta |1\rangle \rightarrow \beta |0\rangle + \alpha |1\rangle$, como se explicó en la sección 1.2.1 del Capítulo 1; en la representación de doble riel, la negación de un estado es el cambio de trayectoria del fotón, lo que se consigue con

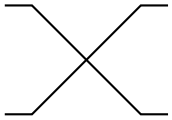

Figura 3.2. Compuerta **NOT** en representación de doble riel, elaboración propia.

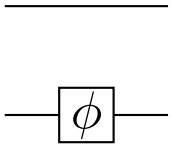

Figura 3.3. Compuerta **PHASE** o R_z en representación de doble riel, elaboración propia con el diseño de Benenti, Casati y Strini [7].

espejos que afecten las posibles trayectorias de la manera que se observa en la figura 3.2. En esta imagen, los espejos se posicionan en los vértices que indican cambios de trayectoria (no contando el punto donde se cruzan trayectorias). Los espejos inducen desplazamientos de fase en estados fotónicos [12], pero como ambas trayectorias está sometidas a la misma cantidad de reflexiones, el desfase sobre un estado $\alpha|0\rangle + \beta|1\rangle$ es global y, por tanto, irrelevante.

3.2.1.2. Desplazador de fase

Como se discutió en la sección 1.2.1 del Capítulo 1, un desplazamiento de fase es una rotación $R_z(\phi)$ en la esfera de Bloch, y sólo afecta al estado $|1\rangle$. Ópticamente, este efecto se logra poniendo en la trayectoria inferior del qubit un material de índice de refracción lineal diferente al del entorno, de manera que el camino óptico será diferente para los estados $|0\rangle$ y $|1\rangle$ [7]. La longitud necesaria depende de la diferencia entre índices de refracción y la frecuencia ω del fotón [9]. La figura 3.3 representa esta implementación. Según se vio de la explicación en la sección 2.4.3 del Capítulo 2, un fotón (o superposición de estados fotónicos) siempre sufre un desplazamiento de fase dependiente del tiempo [1], pero en el modelo de doble riel este desfase es global. El espacio donde el índice de refracción difiere entre trayectorias es lo que imparte un cambio de fase condicional sobre los estados computacionales [9]. El caso especial de desfase $\phi = \pi$ corresponde a la compuerta σ_z [15].

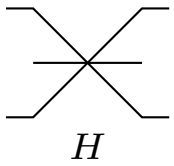

Figura 3.4. Compuerta de Hadamard en representación de doble riel, elaboración propia con el diseño de Benenti, Casati y Strini [7].

Dado que la fase corresponde es la función periódica $e^{i\phi}$, desplazadores de fase de diferente tamaño pueden impartir el mismo desfase. Si se requiere aplicar un desfase pequeño, se puede obtener el mismo efecto con un trozo de material refractante de mayor tamaño.

3.2.1.3. Compuerta de Hadamard

En la sección 2.5.1 del Capítulo 2 se explicaron los divisores de haz; el divisor descrito en particular produce estados fotónicos que en la base computacional se parecen a los producidos por una compuerta de Hadamard, excepto por un desfase $\pm i$ [12]. Sin embargo, este desfase es producido por la construcción del divisor, de manera que es posible construir un divisor de haz cuyos desfases entre estados base correspondan a la compuerta de Hadamard, agregando capas de material que alteren la longitud del camino óptico (lo cual es equivalente a compuertas de fase $R_z(\phi)$ descritas en el apartado 3.2.1.2) [12]. En la representación de doble riel, dicho divisor de haz se puede ilustrar como se ve en la figura 3.4, donde se están usando espejos para desviar los fotones hacia el divisor.

El hamiltoniano de esta interacción es

$$\hat{H}_H = i\frac{\pi}{4}\left(\hat{a}\hat{b}^\dagger - \hat{a}^\dagger\hat{b}\right),$$

de manera que la evolución está dada por

$$\hat{U}_H = e^{\frac{\pi}{4}\left(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger\right)},$$

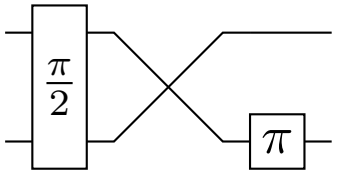

Figura 3.5. Compuerta σ_y en representación de doble riel, elaboración propia.

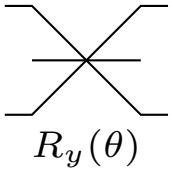

Figura 3.6. Compuerta $R_y(\theta)$ en representación de doble riel, elaboración propia con el diseño de Nielsen y Chuang [9].

que realiza [9]

$$\hat{U}_H \left(\alpha \left|0\right\rangle + \beta \left|1\right\rangle\right) = \alpha \left|+\right\rangle + \beta \left|-\right\rangle .$$

3.2.1.4. Compuerta σ_y

El efecto del operador de Pauli σ_y es equivalente a aplicar una compuerta σ_x seguida de una σ_z, junto a una fase global i [15]. Entonces, en la representación de doble riel, la compuerta corresponde a la imagen en la figura 3.5.

3.2.1.5. Compuerta $R_y(\theta)$

Una rotación al rededor del eje y de la esfera de Bloch sobre un estado genérico del qubit efectúa la transformación

$$R_y(\theta) \left(\alpha \left|0\right\rangle + \beta \left|1\right\rangle\right) = \alpha \left(\cos\frac{\theta}{2} \left|0\right\rangle + \sin\frac{\theta}{2} \left|1\right\rangle\right) + \beta \left(\cos\frac{\theta}{2} \left|1\right\rangle - \sin\frac{\theta}{2} \left|0\right\rangle\right),$$

que corresponde a un divisor de haz $\cos^2\left(\frac{\theta}{2}\right) : \sin^2\left(\frac{\theta}{2}\right)$ [9]. Entonces, una rotación $R_y(\theta)$ requiere de un divisor de haz construido específicamente para el valor del parámetro θ [9], como aparece en la representación de la figura 3.6 para doble riel. Alternativamente, se puede realizar una aproximación con compuertas σ_y y $R_z(\phi)$, utilizando el hecho de que $R_y(\theta) = e^{i\theta\sigma_y/2}$ con la expansión de Taylor de e^x [7].

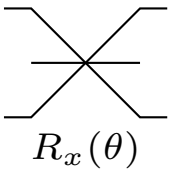

Figura 3.7. Compuerta $R_x(\theta)$ en representación de doble riel, elaboración propia.

El operador de evolución de esta compuerta es

$$\hat{U}_y = e^{\frac{\theta}{2}\left(\hat{a}^\dagger \hat{b} - \hat{a}\hat{b}^\dagger\right)}.$$

3.2.1.6. Compuerta $R_x(\theta)$

Similarmente a la rotación en el eje y, la rotación en el eje x produce un efecto [7]

$$R_x(\theta)\left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) = \alpha\left(\cos\frac{\theta}{2}\left|0\right\rangle - i\sin\frac{\theta}{2}\left|1\right\rangle\right) + \beta\left(\cos\frac{\theta}{2}\left|1\right\rangle - i\sin\frac{\theta}{2}\left|0\right\rangle\right),$$

que corresponde a un divisor de haz ajustado a θ [9], cuya representación de doble riel está en la figura 3.7.

Dada el álgebra $su(2)$ que rige el grupo $SU(2)$ de rotaciones en $\mathbb{C}^2$, una compuerta de rotación en x se puede construir como el producto de una compuerta $R_y(\theta)$ y $R_z(\phi)$, un divisor de haz y un desplazador de fase [9]. Por otro lado, una rotación $R_x(\theta)$ se puede aproximar con compuertas **NOT** y desplazadores de fase de la misma manera que $R_y(\theta)$, dado que σ_x es el generador de la rotación al rededor del eje x [12]. Esta compuerta está asociada a la evolución unitaria [9]

$$\hat{U}_x = e^{-i\frac{\theta}{2}\left(\hat{a}^\dagger \hat{b} + \hat{a}\hat{b}^\dagger\right)}.$$

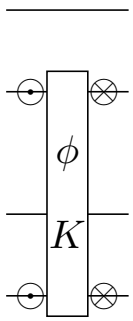

Figura 3.8. Compuerta **CPHASE** en representación de doble riel, elaboración propia con el diseño de Benenti, Casati y Strini [7].

3.2.2. Compuertas de dos qubits

3.2.2.1. Compuerta CPHASE

En la sección 2.5.2 del Capítulo 2 se explicó la interacción Kerr cruzada, cuyo operador de evolución temporal es

$$\hat{U}_{CK} = e^{-iKt\hat{n}_a\hat{n}_b},$$

donde K es proporcional a la susceptibilidad eléctrica no-lineal, y a, b son modos lumínicos diferentes que se acoplan a la interacción [12]. Este acoplo permite utilizar un trozo de material con susceptibilidad Kerr como un desplazamiento de fase condicionado entre qubits fotónicos de doble riel [12]. Dicha implementación se visualiza en la figura 3.8. En ella se observa la notación $\odot$ y $\otimes$, que significa que las trayectorias marcadas son desviadas con espejos a una posición *fuera de la página* paralela a su ruta original, para que el bloque de material que funciona como compuerta solo afecte al par de trayectorias requeridas sin afectar otras, y ser devueltas a su lugar. La longitud de este desvío debe calcularse para que no provoque un desfase adicional.

En el operador de evolución se puede ver que el desfase es negativo, pero el tiempo de interacción se puede ajustar (usando la longitud del material y tomando en cuenta la frecuencia asociada a la energía del fotón) para lograr el desfase equivalente deseado, de manera similar que los desplazadores de fase lineales. En la sección 2.5.2 del Capítulo 2 se explicó que un solo modo de luz también puede sufrir un desfase

por efecto Kerr; sin embargo, esta interacción está modelada por la evolución

$$\hat{U}_K = e^{-iKt\left(\hat{n}^2-\hat{n}\right)},$$

por lo que un solo fotón ($n = 1$) no presentaría efectos de la interacción [12].

En la sección 1.2.2 del Capítulo 1 se presentó la compuerta **CPHASE** como una combinación de compuertas **CNOT** y de fase de un solo qubit; dado que, como se verá más adelante, la compuerta **CNOT** implementada para fotones en doble riel utiliza interacción Kerr cruzada, es más eficiente la implementación de la compuerta **CPHASE** que se muestra en la figura 3.8.

3.2.2.2. Compuerta CNOT

La compuerta **CNOT** en el doble riel fotónico consiste en el qubit objetivo primero sometido a un divisor de haz con operador de evolución

$$\hat{U}_{BS} = e^{i\pi\left(\hat{c}^\dagger\hat{d}+\hat{c}\hat{d}^\dagger\right)},$$

que es el descrito en la sección 2.5.1 del Capítulo 2. Luego de eso, el modo superior (donde está el fotón en el estado computacional $|0\rangle$) del qubit objetivo se acopla en interacción Kerr cruzada de fase $\phi = \pi$ con el modo inferior (donde está el fotón en el estado computacional $|1\rangle$) del qubit control [12]. Tras esto, se aplica sobre el qubit objetivo un divisor de haz de operador $\hat{U}_{BS}^\dagger$, y finalmente se ajustan las fases de ambos modos de este mismo qubit [12].

En la figura 3.9 se puede observar la compuerta. Según la demostración en la sección 1.3 del Capítulo 1, el conjunto de las compuertas de un solo qubit junto a la compuerta **CNOT** forman un Conjunto Universal de Compuertas cuántico, de manera que solamente se requiere la implementación exitosa estas compuertas para mostrar la universalidad del modelo de doble riel para computación cuántica [9].

3.2.2.3. Compuertas CNOT generalizadas

Una compuerta **CNOT** cuya condición de activación es $|0\rangle$ en vez de $|1\rangle$ se construye con una compuerta **CNOT** estándar y compuertas **NOT**, según lo mostrado en la sección 1.2.2 del Capítulo 1. En la representación de doble riel, la figura 3.10 muestra esta compuerta.

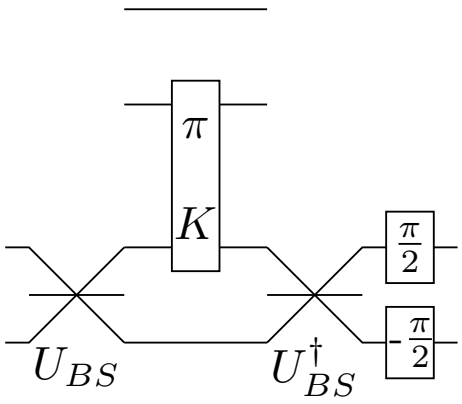

Figura 3.9. Compuerta **CNOT** en representación de doble riel, elaboración propia con el diseño de Benenti, Casati y Strini [7].

Por otro lado, de acuerdo a ese mismo capítulo, la compuerta **CNOT** donde los papeles de qubit control y qubit objetivo están invertidos se construye con la versión estándar de la compuerta y cuatro compuertas de Hadamard [7]. La figura 3.11 muestra la representación de doble riel óptico de la compuerta.

3.2.2.4. Compuerta SWAP

Esta compuerta intercambia los estados de dos qubits, y se arma con una compuerta **CNOT** estándar, luego una compuerta invertida, y finalmente otra compuerta estándar [7]. La figura 3.12 corresponde a esta compuerta en representación de doble riel.

3.2.2.5. Compuerta C-U

En la sección 1.2.2 del Capítulo 1 se construyo la compuerta **C-U**, una compuerta controlada generalizada de dos qubits, utilizando solamente compuertas **CNOT** y compuertas de un solo qubit. La representación de doble riel óptico correspondiente se encuentra en las figuras 3.13 y 3.14 (la figura completa divida debido a su longitud).

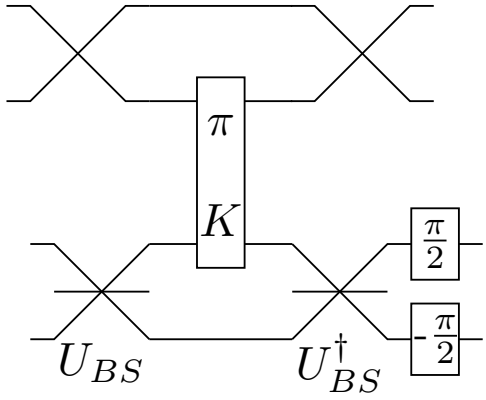

Figura 3.10. Compuerta **CNOT** de condición de control invertida en representación de doble riel, elaboración propia.

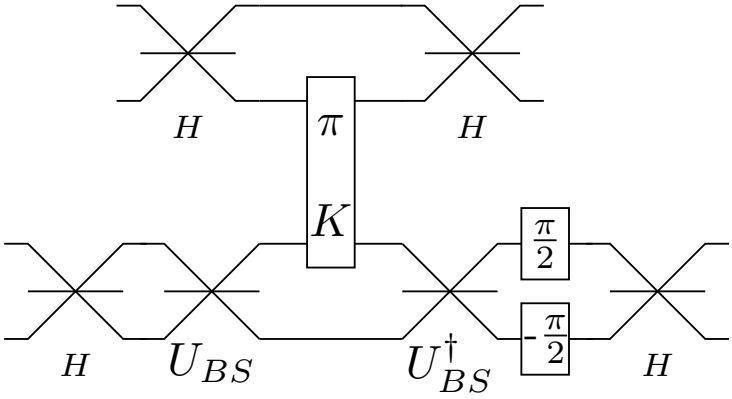

Figura 3.11. Compuerta **CNOT** invertida en representación de doble riel, elaboración propia.

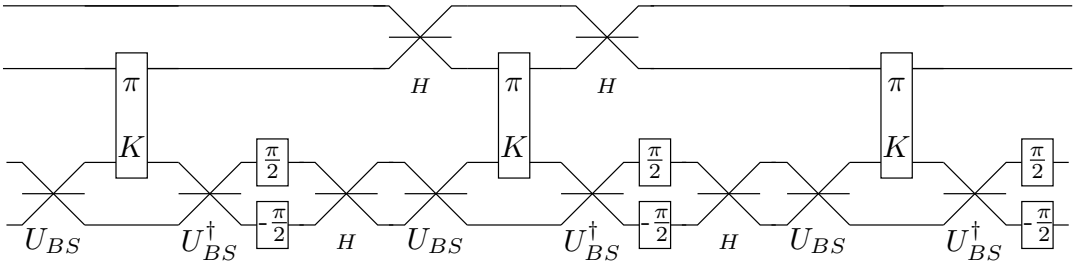

Figura 3.12. Compuerta **SWAP** en representación de doble riel, elaboración propia.

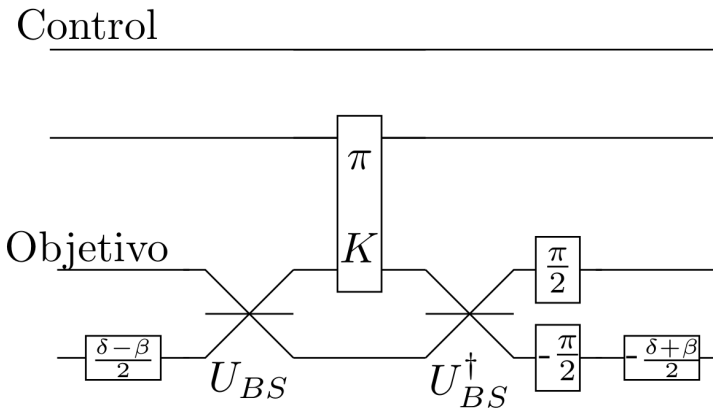

Figura 3.13. Compuerta **C-U** en representación de doble riel, elaboración propia. Parte 1.

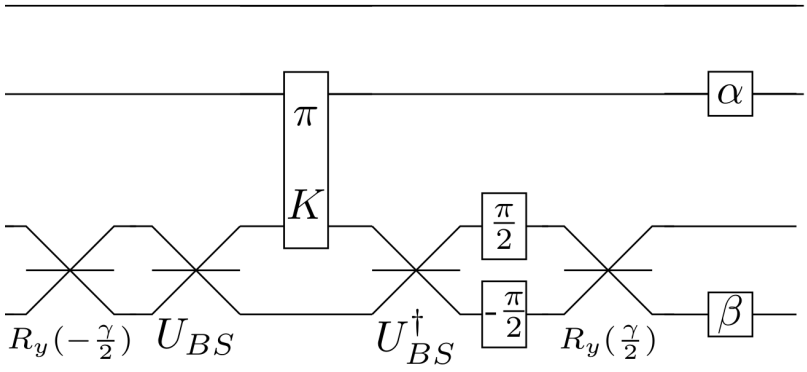

Figura 3.14. Compuerta **C-U** en representación de doble riel, elaboración propia. Parte 2.

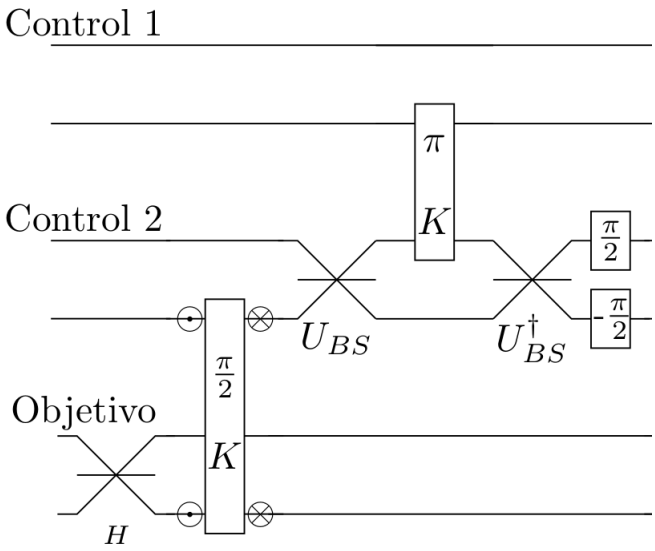

Figura 3.15. Compuerta de Tiffoli en representación de doble riel, elaboración propia. Parte 1.

3.2.3. Compuertas de múltiples qubits

3.2.3.1. Compuerta de Tiffoli

La compuerta C^2-**NOT** o de Tiffoli se construye con compuertas **CNOT** estándar, compuertas de Hadamard y compuertas **CPHASE**, como se vio en la sección 1.3 del Capítulo 1. En las figuras 3.15 y 3.16 (la figura completa divida debido a su longitud) aparece la construcción de doble riel óptico de esta compuerta, la cual permite armar compuertas C^k-**U**.

3.2.3.2. Compuerta C^3-U

Como ejemplo de las compuertas genéricas C^k-**U** cuya construcción se demostró en el Capítulo 1, en las figuras 3.17, 3.18, 3.19 y 3.20 (la figura completa divida debido a su longitud) se presenta la construcción en doble riel de una compuerta C^3-**U**, utilizando compuertas de Tiffoli (figuras 3.15 y 3.16) y una compuerta **C-U** (figuras 3.13 y 3.14). En estas imágenes, tanto las compuertas de Tiffoli como la compuerta **C-U** pasan sobre qubits que no están involucrados en la compuerta particular.

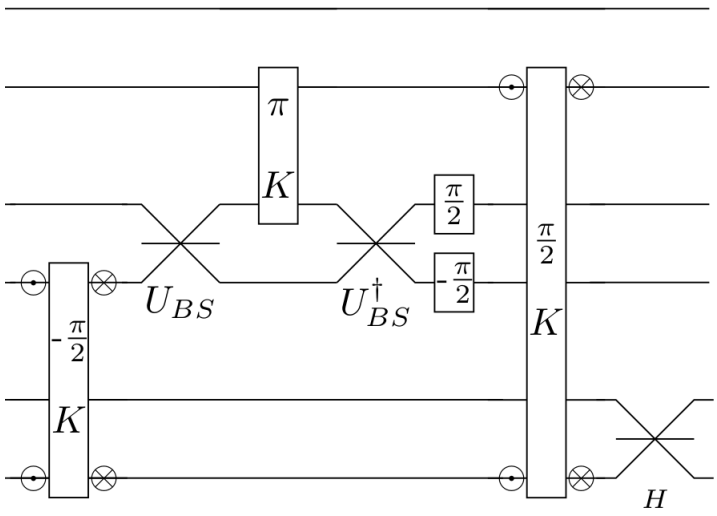

Figura 3.16. Compuerta de Tiffoli en representación de doble riel, elaboración propia. Parte 2.

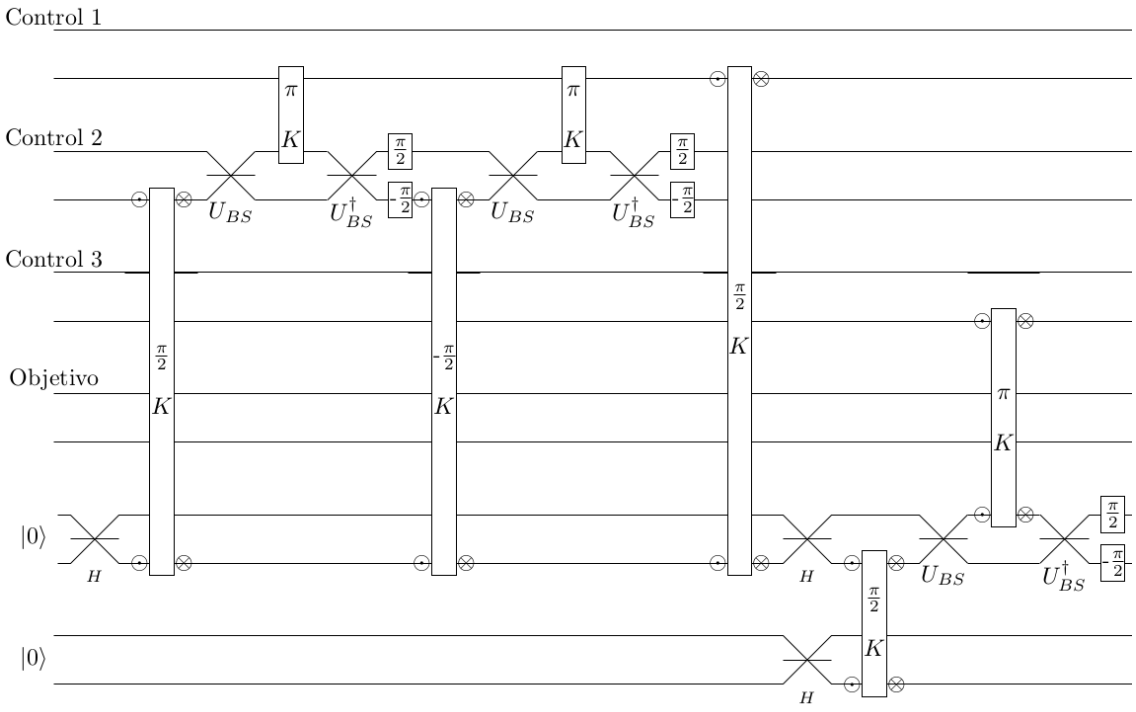

Figura 3.17. Compuerta C^3-**U** en representación de doble riel, elaboración propia. Parte 1.

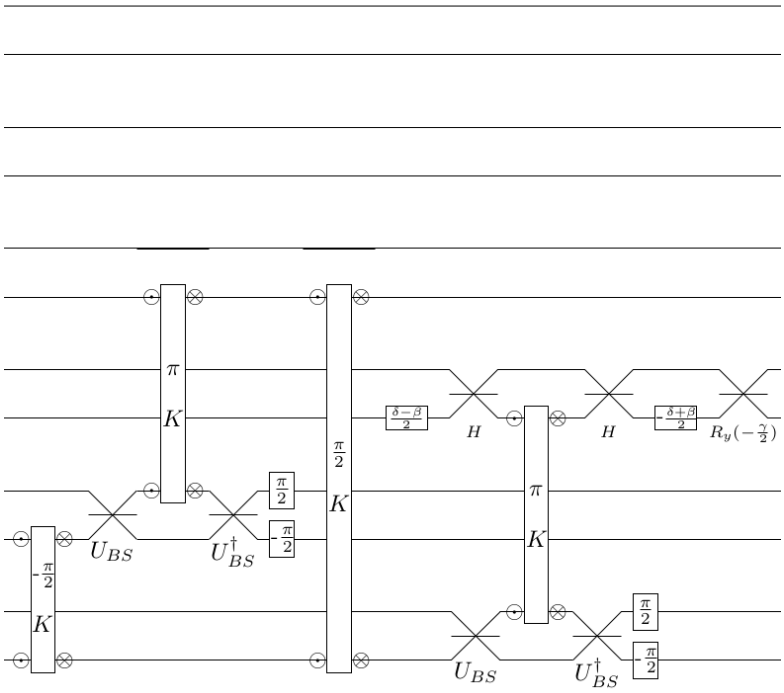

Figura 3.18. Compuerta C^3**-U** en representación de doble riel, elaboración propia. Parte 2.

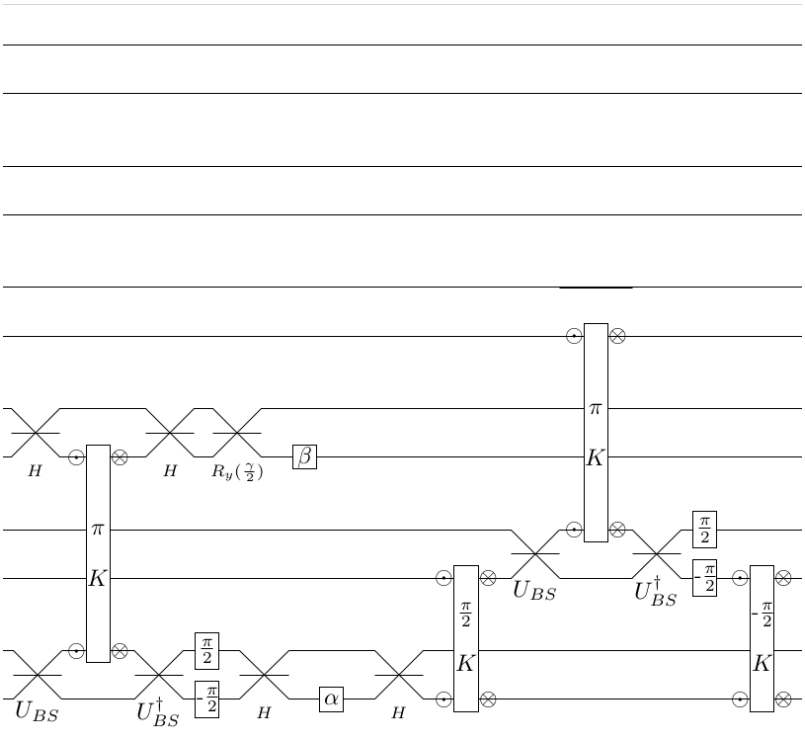

Figura 3.19. Compuerta C^3**-U** en representación de doble riel, elaboración propia. Parte 3.

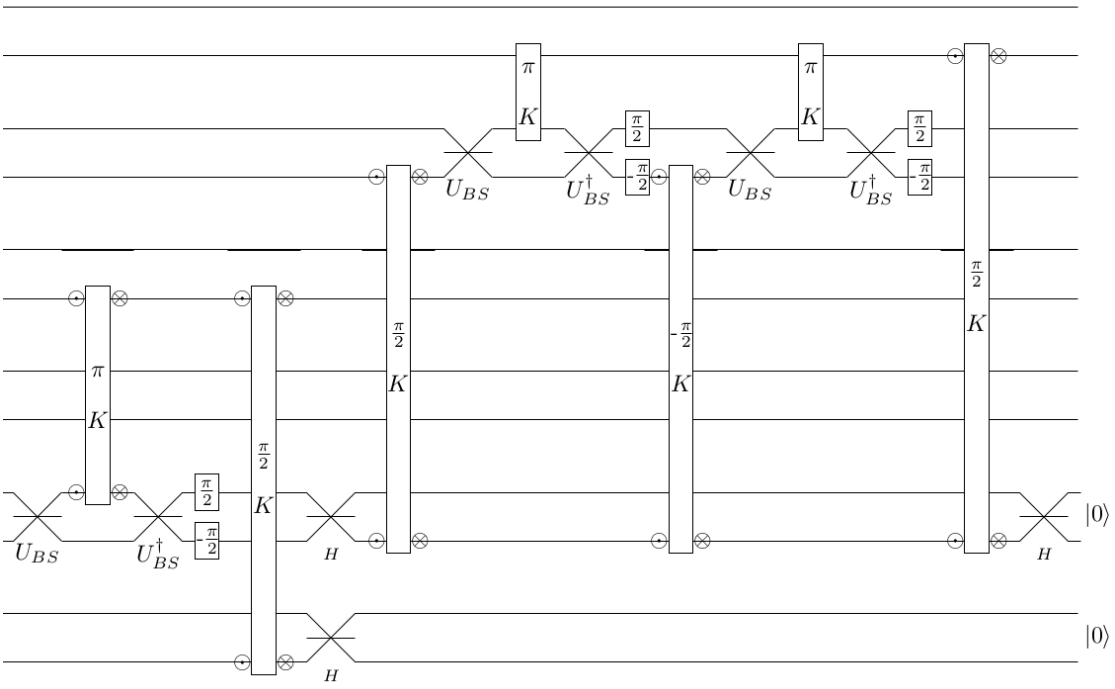

Figura 3.20. Compuerta C^3-**U** en representación de doble riel, elaboración propia. Parte 4.

3.2.4. Algoritmos

Dado que es posible construir un Conjunto Universal de Compuertas cuánticas en la representación de doble riel óptico, entonces se pueden construir algoritmos cuánticos usando este modelo [9]. En esta sección se presentan los siguientes algoritmos de acuerdo a sus descripciones en las secciones 1.4 y 1.5 del Capítulo 1: el sumador cuántico, el algoritmo de Deutsch, la transformada de Fourier cuántica, un ejemplo simple del algoritmo de Grover, y un ejemplo simple del algoritmo de Shor.

3.2.4.1. Sumador cuántico

Este algoritmo consiste en una aplicación sucesiva de solamente dos de tipos sub-algoritmos, la operación de suma **S** y la operación de acarreo **C**, formados únicamente con compuertas **CNOT** y de Tiffoli [7]. En la figura 3.21 está el sub-algoritmo **S** en el doble riel. Correspondientemente, el sub-algoritmo **C** se encuentra en las figuras 3.22 y 3.23 (la figura completa divida debido a su longitud).

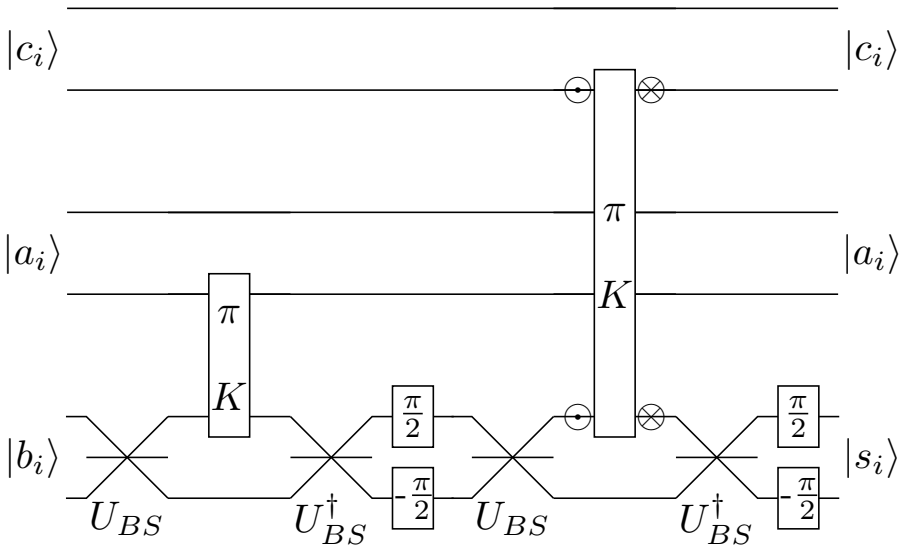

Figura 3.21. Sumador cuántico: sub-algoritmo **S** en representación de doble riel, elaboración propia.

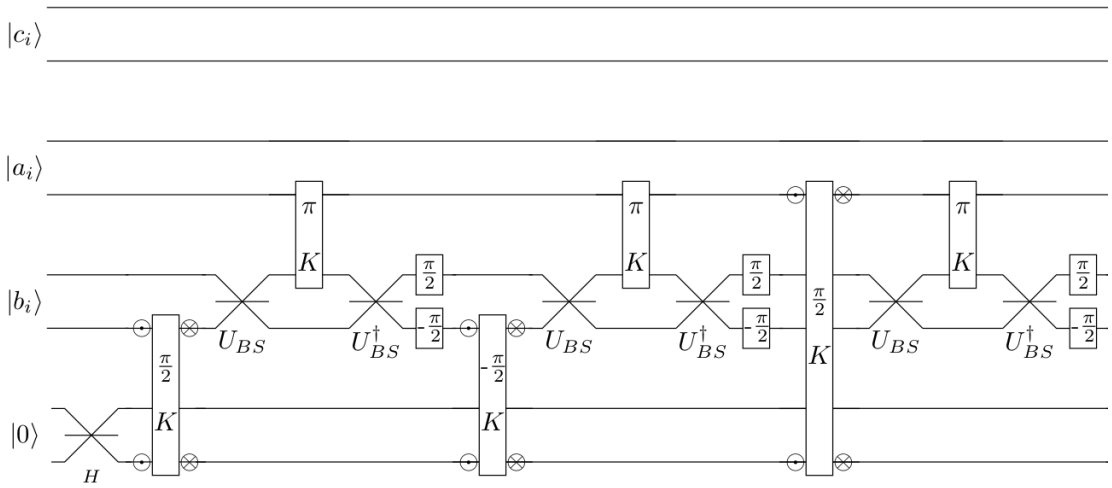

Figura 3.22. Sumador cuántico: sub-algoritmo **C** en representación de doble riel, elaboración propia. Parte 1.

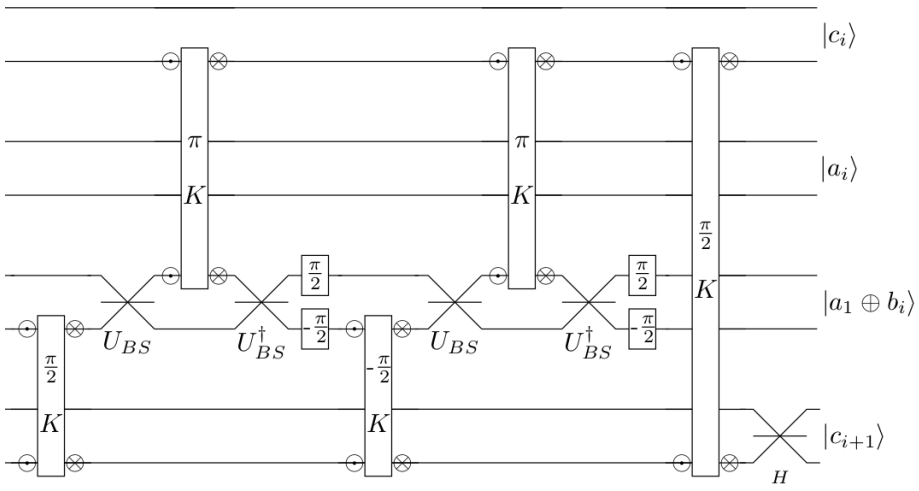

Figura 3.23. Sumador cuántico: sub-algoritmo **C** en representación de doble riel, elaboración propia. Parte 2.

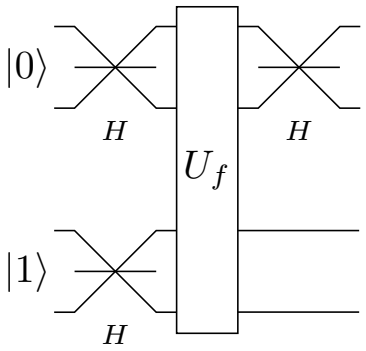

Figura 3.24. Algoritmo de Deutsch en representación de doble riel, elaboración propia.

3.2.4.2. Algoritmo de Deutsch

El algoritmo de Deutsch, como explicó la sección 1.4.3, determina si una función f de un solo qubit es constante o balanceada. Emplea la evolución unitaria U_f que corresponde a la función desconocida, y compuertas de Hadamard, según se mostró en la sección mencionada; la representación correspondiente está en la figura 3.24. La generalización, conocida como algoritmo de Deutsch-Jozsa, es idéntica a el caso particular, con el mismo qubit auxiliar inicializado en $|1\rangle$, pero con n qubits principales con sus correspondientes compuertas de Hadamard [9].

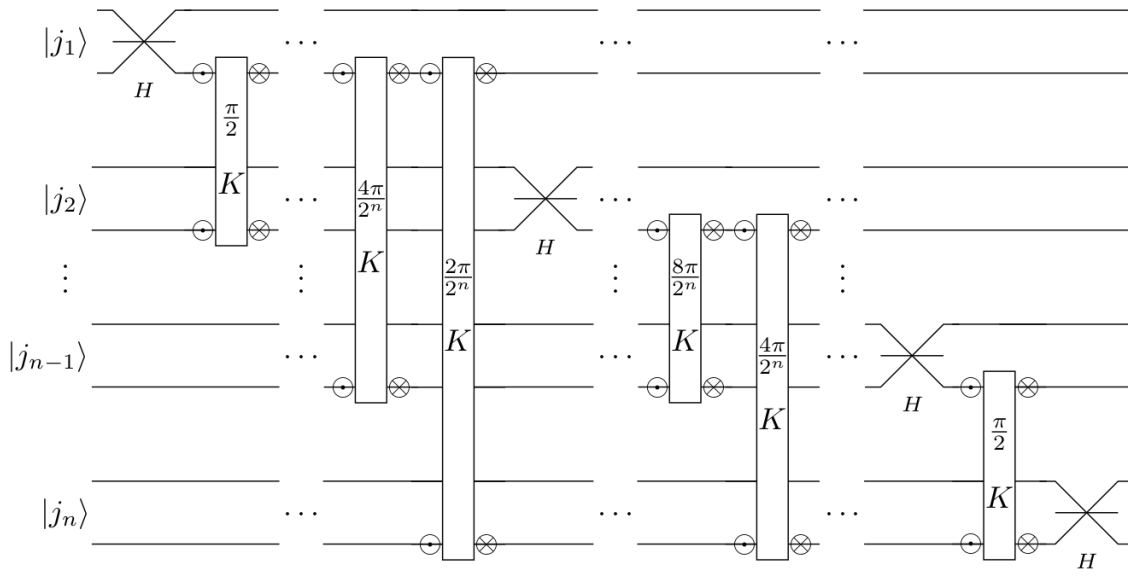

Figura 3.25. Transformada de Fourier cuántica en representación de doble riel, elaboración propia. Parte 1.

3.2.4.3. Transformada de Fourier cuántica

Este algoritmo consiste únicamente en compuertas de Hadamard y **CPHASE**, además de compuertas **SWAP** que ordenan adecuadamente los estados cuánticos finales [9]. Su representación de doble riel óptico está en las figuras 3.25, 3.26 y 3.27 (la figura completa divida debido a su longitud).

3.2.4.4. Algoritmo de Grover: ejemplo

En la sección 1.5.1 del Capítulo 1 se explicó el algoritmo de Grover para una base de datos con N elementos, y se mostró el caso específico de una búsqueda entre $N = 4$ elementos, el cual se presenta en la figura 3.28 como un doble riel óptico.

3.2.4.5. Algoritmo de Shor: ejemplo

Para ilustrar de manera simple el funcionamiento del algoritmo de Shor en la representación de doble riel óptico, se utiliza el ejemplo trivial del número 15 para factorizar [15]. Este problema es equivalente a hallar el período de la función

$$f(x) = a^x \mod 15,$$

donde $\gcd(a, 15) = 1$ [12]. El valor $a = 2$ cumple esta condición, y se evalúa $f(x)$ sobre tres qubits, es decir, con $x = [0, 5]$ entero. Para evaluar $f(x)$ se utiliza la

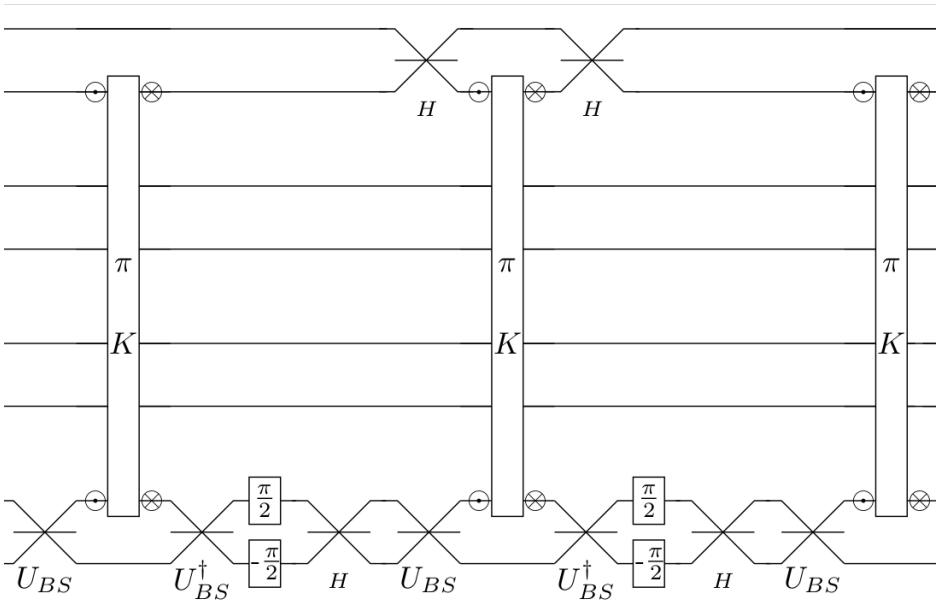

Figura 3.26. Transformada de Fourier cuántica en representación de doble riel, elaboración propia. Parte 2.

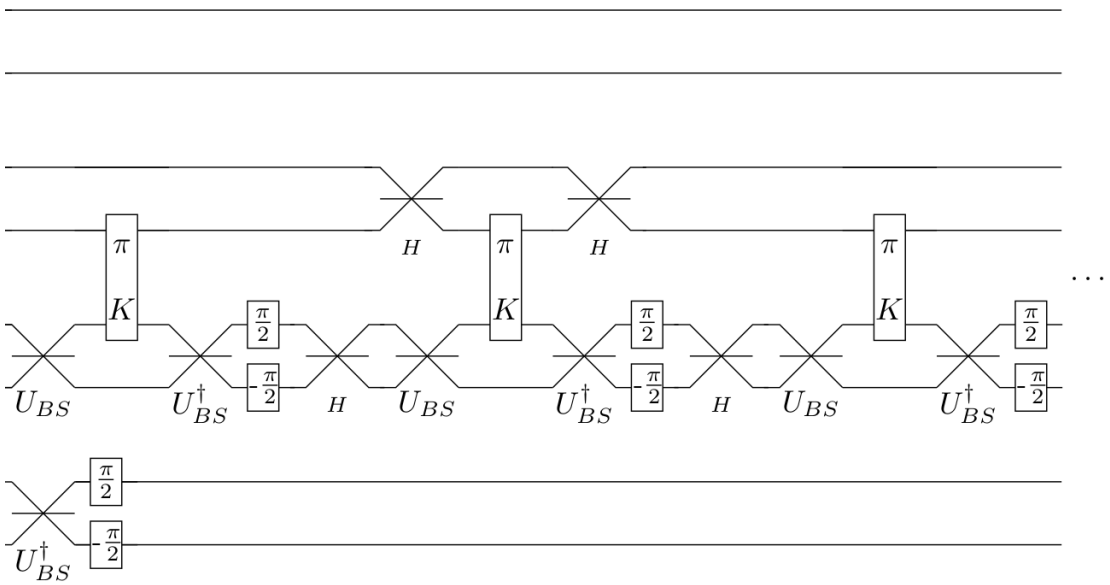

Figura 3.27. Transformada de Fourier cuántica en representación de doble riel, elaboración propia. Parte 3.

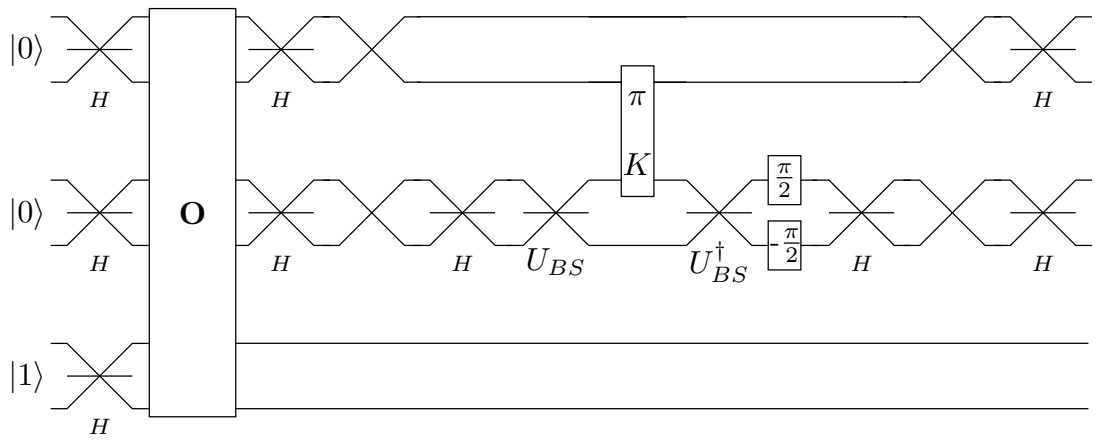

Figura 3.28. Algoritmo de Grover para $N = 4$ en representación de doble riel, elaboración propia.

evaluación de funciones por mintérminos; este método no es eficiente, pero permite ilustrar este tipo de algoritmo que fue descrito en la sección 1.4.1 del Capítulo 1. En este caso, la evaluación de $f(x)$ por mintérminos sobre 3 qubits principales requiere de 4 qubits auxiliares para almacenar el resultado, y se utilizan 4 compuertas de Tiffoli generalizadas.

En las figuras 3.29, 3.30 y 3.31 (la figura completa divida debido a su longitud) aparece la representación de doble riel del proceso del algoritmo de Shor según fue descrito en la sección 1.5.2 del Capítulo 1: compuertas de Hadamard sobre el registro principal para obtener todo el rango requerido de x, evaluación de $f(x)$ almacenando el resultado en el registro auxiliar, medición sobre el registro auxiliar, aplicación de transformada de Fourier sobre el registro principal, y medición del registro principal.

3.2.5. Materiales

Los espejos, desplazadores de fase, y divisores de haz son los dispositivos ópticos más accesibles que existen [9]. Los espejos altamente reflectantes son comunes, incluso espejos con pérdidas en el orden de 0.01 % no son inusuales [9]. Como ya se ha mencionado antes, un desplazador de fase es un segmento de material cuyo índice de refracción es diferente al medio principal del sistema de la computadora cuántica; líquidos, gases, geles, líquidos teñidos y sólidos cristalinos proveen posibles implementaciones de desplazadores de fase óptica [9].

Un divisor de haz es una pieza de vidrio parcialmente reflectante, que suele

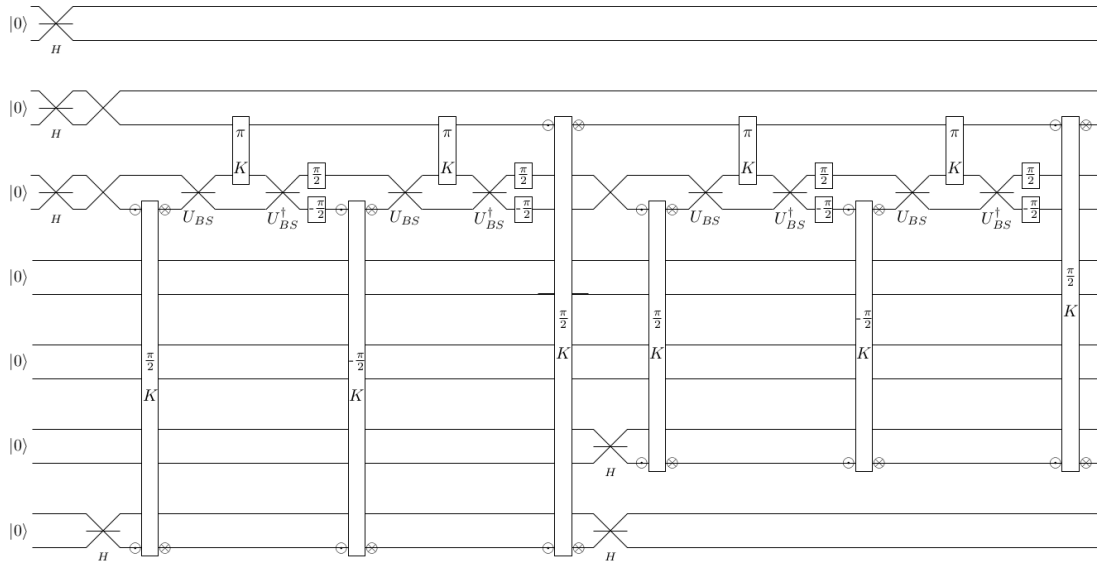

Figura 3.29. Algoritmo de Shor para factorizar 15 en representación de doble riel, elaboración propia. Parte 1, evaluación de $f(x)$.

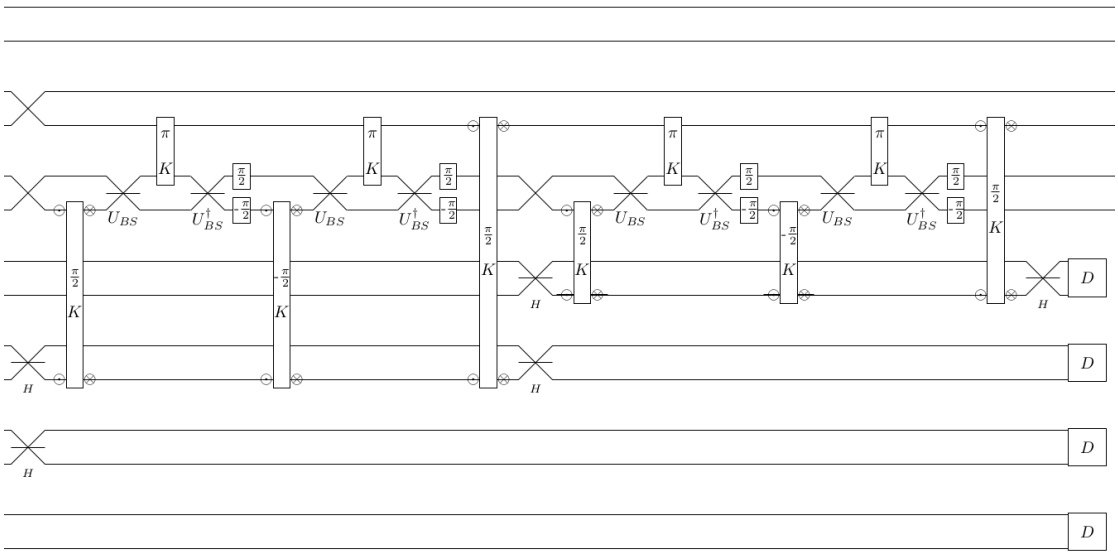

Figura 3.30. Algoritmo de Shor para factorizar 15 en representación de doble riel, elaboración propia. Parte 2, evaluación de $f(x)$ y medición de registro auxiliar.

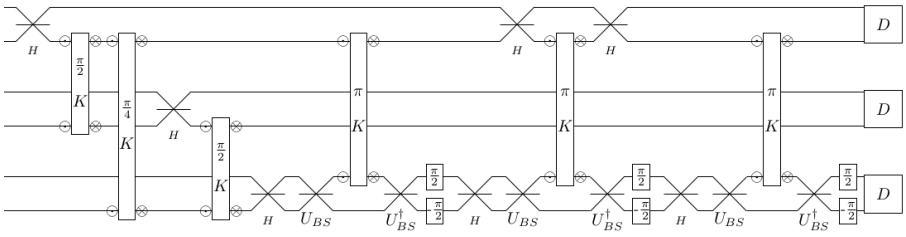

Figura 3.31. Algoritmo de Shor para factorizar 15 en representación de doble riel, elaboración propia. Parte 3, transformada de Fourier sobre registro principal y medición final.

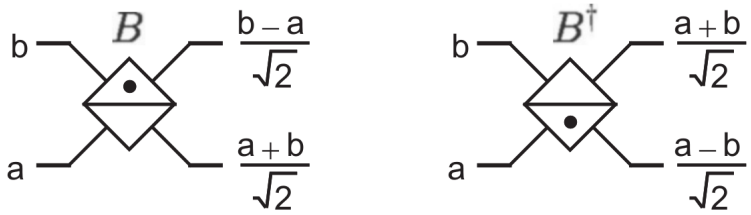

Figura 3.32. Esquema de divisor de haz construido con prismas y placa delgada de metal, elaborado por Nielsen y Chuang [9].

construirse con una delgada lámina metálica entre dos prismas, los cuales proveen también de desplazamientos de fase asociados a la longitud de la trayectoria de los fotones [9]. Las características de grosor, forma y reflexión de un prisma determinan qué clase de compuerta son: Hadamard, R_x, o R_y [9]. En la figura 3.32 se encuentra un esquema de esta construcción de divisor de haz, donde los triángulos corresponden a los prismas, e invertir físicamente el aparato provoca el cambio del operador de evolución $U_{BS} \rightarrow U_{BS}^{\dagger}$ [9].

Comparado con los fenómenos ópticos lineales de los materiales, el efector Kerr es débil al ser producido por una susceptibilidad eléctrica de tercer orden [9]. Una interacción Kerr muy débil no permite aplicar un desfase tan grande como π, lo cual implica que utilizarlo como compuerta cuántica en el modelo de doble riel no es realista [9]. Además la no-linealidad siempre tiene asociada una absorción lumínica, por lo que se perderían alrededor de 50 fotones por cada uno que logre obtener un desfase de magnitud π, según cálculos teóricos para el mejor arreglo posible [9]. Estos impedimentos respecto a la débil no-linealidad de materiales disponibles fue uno de los principales problemas en los intentos de desarrollo de computadoras ópticas clásicas [9].

Sin embargo, la investigación sobre materiales con alta susceptibilidad Kerr y

las condiciones que la provocan es un área de investigación y desarrollo abierta [12]. Por ejemplo, se ha encontrado que materiales modernos, tales como nanotubos de carbono y grafeno presentan fuertes respuestas no-lineales ópticas de tercer orden, es decir, el orden del efecto Kerr (en comparación con otros materiales Kerr conocidos) [14]. En el caso del grafeno, una sola capa de este material exhibe una alta respuesta de susceptibilidad $\chi^{(3)}$, con una absorción de 2.3 % por capa de grafeno, para fotones en el espectro visible e infrarrojo [14]. Desarrollos en el área de la ciencia de los materiales pueden llevar a una respuesta Kerr de baja absorción lo suficientemente intensa para implementarse en computación cuántica [12].

3.3. Manejo de error

3.3.1. Incertezas de procesos computacionales

Los errores unitarios descritos en la sección 1.5.4 del Capítulo 1 afectan a la representación de doble riel óptico de computación cuántica, como a cualquier otra, alterando los coeficientes de las superposiciones de estados [7]. Como se puede observar a lo largo de la sección 3.2, las compuertas ópticas que aplican operadores unitarios sobre los qubits consisten combinaciones de espejos, espejos parciales y dos tipos de desplazadores de fase [9], y los efectos de estas compuertas se pueden visualizar como rotaciones en la esfera de Bloch de cada qubit [7].

Considerando la normalización adecuada, un operador unitario actúa sobre un estado de un qubit como

$$\alpha\,|0\rangle + \beta\,|1\rangle \rightarrow \eta\,|0\rangle + \xi\,|1\rangle\,,$$

de manera que el error en el operador unitario aparece como incertezas en los valores de los coeficientes

$$\eta = \bar{\eta} \pm \Delta\eta,$$

$$\xi = \bar{\xi} \pm \Delta\xi,$$

aunque se sigue cumpliendo $|\eta|^2 + |\xi|^2 = 1$ [7]. Estas incertezas tienen dos fuentes: incerteza en las tasas de transmisión y reflexión de los espejos parciales, e incertezas en el desfase impartido por los desplazadores. La incerteza por desfase puede darse tanto en desplazadores lineales individuales, así como en los desplazadores incluidos en los divisores de haz, además de los desplazadores de interacción Kerr. Las incer-

tezas de ambos tipos, espejos parciales y desfase, provienen a su vez de incertezas en las características ópticas y geométricas medidas del material [19].

En la sección sobre errores unitarios del Capítulo 1 se establecieron las cotas superiores de error en las compuertas cuánticas [7]. Si el máximo error impartido por un elemento del circuito computacional es ϵ, entonces la diferencia entre el estado cuántico final real y el ideal estará limitada según

$$\left\| \left| \tilde{\psi}_n \right\rangle - |\psi_n\rangle \right\| < n\epsilon,$$

para errores alineados sumándose linealmente (errores sistemáticos en la caracterización de los elementos de circuito) [7]. Para errores aleatorios este límite superior es [7]

$$\left\| \left| \tilde{\psi}_n \right\rangle - |\psi_n\rangle \right\| < \sqrt{n}\,\epsilon.$$

Por tanto, la precisión de la medición y fabricación de los materiales usados, y la cantidad usada de dichos materiales determinan el peor error posible en el estado final tras un proceso de computación [19].

Todo algoritmo cuántico se completa con una medición final del registro de qubits; las incertezas en los coeficientes η y ξ tras un proceso computacional alteran las probabilidades p_i de medir un resultado u otro [7]. Según se explicó en el Capítulo 1, el error en estas probabilidades de medición tiene un límite superior

$$\sum_i |p_i - \tilde{p}_i| \leq 2 \left\| \left| \tilde{\psi}_n \right\rangle - |\psi_n\rangle \right\|,$$

de manera que también está limitado por el error máximo ϵ y la cantidad n de aparatos ópticos utilizados [7]. Entonces, una computadora cuántica con tolerancia al error será una donde las diferencias $p_i - \tilde{p}_i$, y por tanto $n\epsilon$ o $\sqrt{n}\,\epsilon$, sean lo suficientemente pequeñas para que el resultado correcto siga siendo el más probable, aunque no sea el único posible [9].

En la sección de Materiales 3.2.5 se explicó que los aparatos ópticos que se utilizan en la representación de doble riel de la computación cuántica tienen tasas de absorción lumínica, es decir, eliminan fotones [9]; un fotón eliminado dentro de un circuito óptico cuántico arruinaría completamente un proceso computacional. En un extremo se encuentran los espejos, donde absorciones de un fotón entre 10^4 son

comunes; por otro lado, los materiales con un fuerte efecto Kerr transmitirán un fotón por cada 50 que eliminen, en el mejor de los casos [9]. Sin embargo, como también se mencionó en la sección 3.2.5, experimentos con grafeno mostraron un fuerte efecto Kerr con una tasa de absorción de 2.3 % por cada lámina de grafeno [14].

Tanto los errores unitarios como los errores por absorción de fotones pueden manejarse usando la idea detrás de los códigos de corrección de errores descritos en la sección 1.5.4 del Capítulo 1: la redundancia. Ambos tipos de errores son probabilísticos, por lo que una computadora cuántica tolerante al error tendrá una alta probabilidad de producir el resultado correcto, aun si no lo produce siempre [9].

En el caso de la absorción de fotones, los errores serían sumamente evidentes, ya que si el fotón de un qubit es eliminado, el qubit deja de existir. Múltiples ejecuciones de un proceso computacional permitirían diferenciar fácilmente entre resultados legítimos y resultados espurios, y almacenar los resultados legítimos para su uso correspondiente; si se logran bajas tasas de absorción en todos los elementos del sistema, la proporción de resultados espurios sería baja. Por otro lado, los errores unitarios tolerables producirían solamente una pequeña cantidad de resultados espurios frente a una mayoría de resultados legítimos, de manera que se usaría votación por mayoría para elegir resultados legítimos y caracterizar la tasa de error del proceso particular. En combinación, las redundancias para los errores unitarios estarían englobadas dentro de los resultados legítimos en relación a los errores por absorción de fotones.

La computación óptica tiene la ventaja de una alta velocidad de ejecución de procesos (literalmente a la velocidad de la luz), solamente limitada por los procesos electrónicos asociados a la producción y detección de los fotones [11]. Por tanto, la repetición de procesos como manejo de error en la representación de doble riel de la computación cuántica no sería un obstáculo importante en la eficiencia del modelo.

Otra forma de emplear la redundancia para el manejo de errores asociados a las incertezas de las compuertas cuánticas, es codificar la información reemplazando los qubits individuales por bloques de qubits [9]. En este caso las compuertas cuánticas individuales son reemplazadas por copias de la compuerta actuando cada una sobre cada uno de los qubits del bloque, efectuando una compuerta equivalente en los

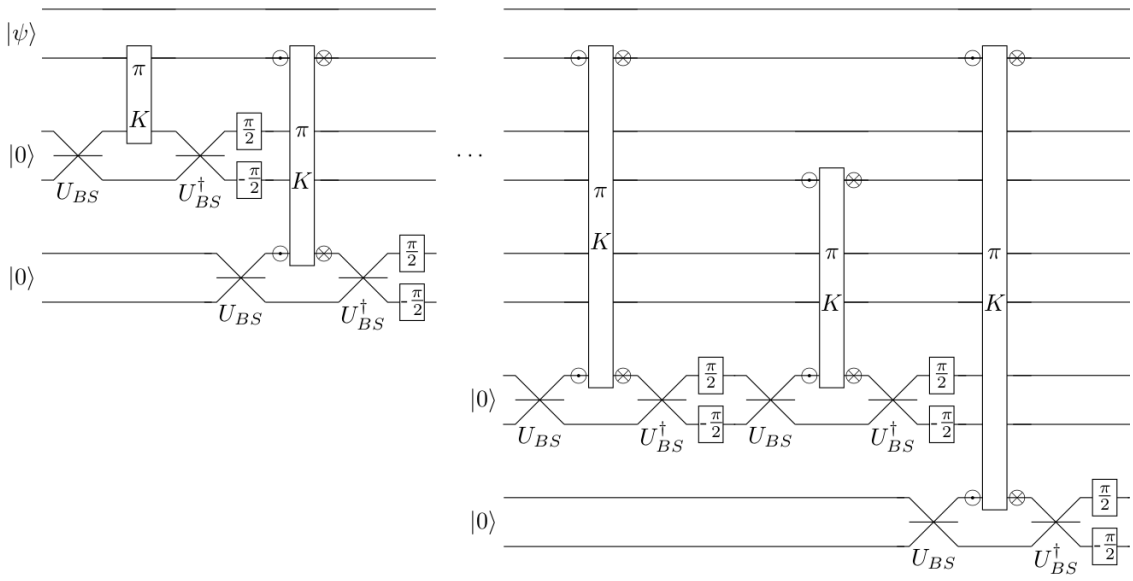

Figura 3.33. Código de tres qubits para inversión del bit en representación de doble riel, elaboración propia. Parte 1.

bloques de qubits [9]. Utilizando a lo largo del proceso mediciones de síndrome de error y códigos de corrección similares a los descritos en la siguiente sección, se reducen los errores en los procesos computacionales [9].

3.3.2. Transmisión por canales ruidosos

La transmisión de información cuántica a través de canales que tienen una probabilidad ϵ de corromperla, fue explicada en la última parte del Capítulo 1. Cuando el ruido de un canal de transmisión tiene la probabilidad de provocar un error por inversión de bit, se utiliza el método protección y corrección conocido código de tres qubits (que a su vez utiliza dos qubits auxiliares) [8]. En la representación de doble riel óptico, este código se implementa como se observa en las figuras 3.33, 3.34, 3.35 y 3.36 (la figura completa divida debido a su longitud). En la primera de estas imágenes, el paso por el canal ruidoso se representa como '$\cdots$'.

Para canales ruidosos que inducen errores por inversión de fase, se utiliza también un código de tres qubits [8]. Como se vio en el Capítulo 1, este código es idéntico al de inversión del bit, con la diferencia de que sobre los tres qubits se aplican compuertas de Hadamard antes de entrar al canal ruidoso, y también al salir del canal [8], lo cual se ilustra en la figura 3.37. Las compuertas de Hadamard permiten que la inversión de fase se convierta en una inversión del bit, de manera que se le pueda

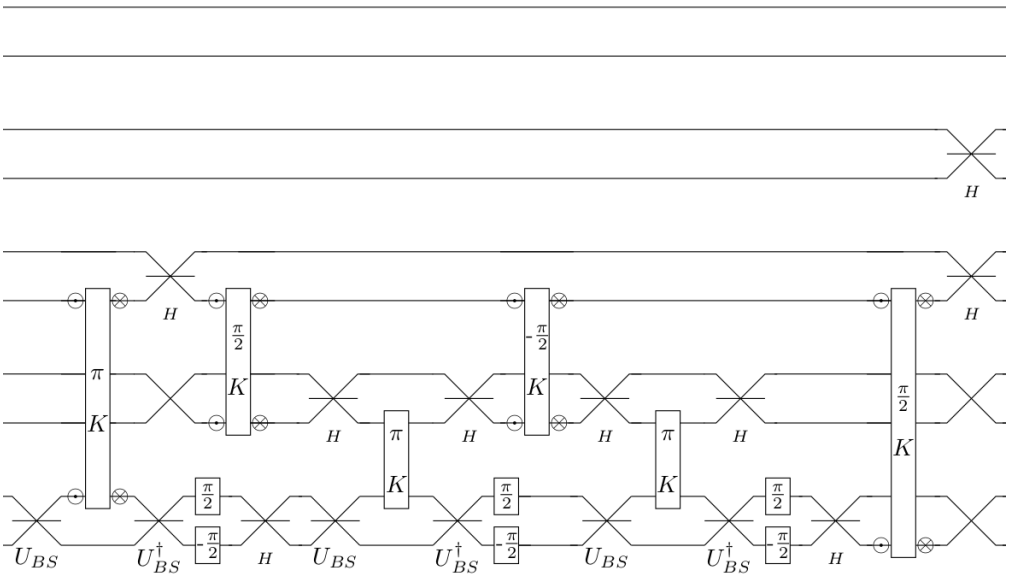

Figura 3.34. Código de tres qubits para inversión del bit en representación de doble riel, elaboración propia. Parte 2.

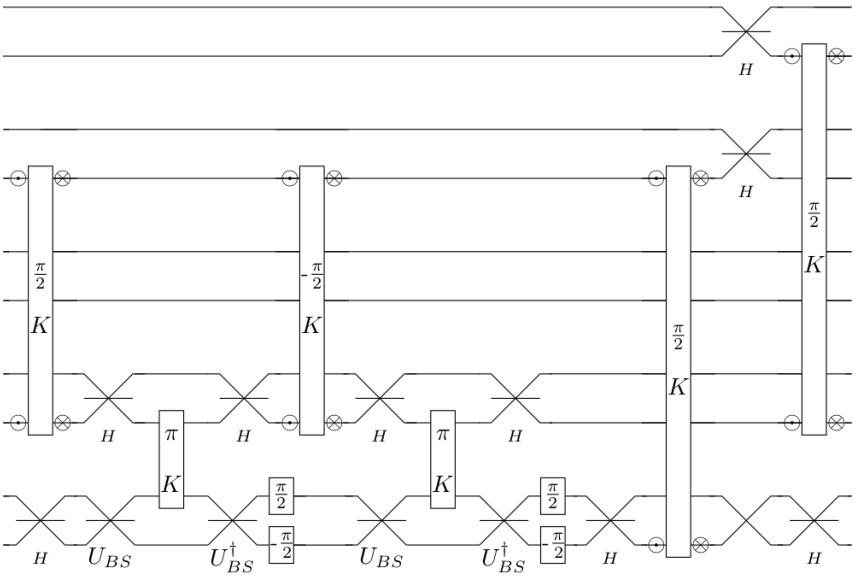

Figura 3.35. Código de tres qubits para inversión del bit en representación de doble riel, elaboración propia. Parte 3.

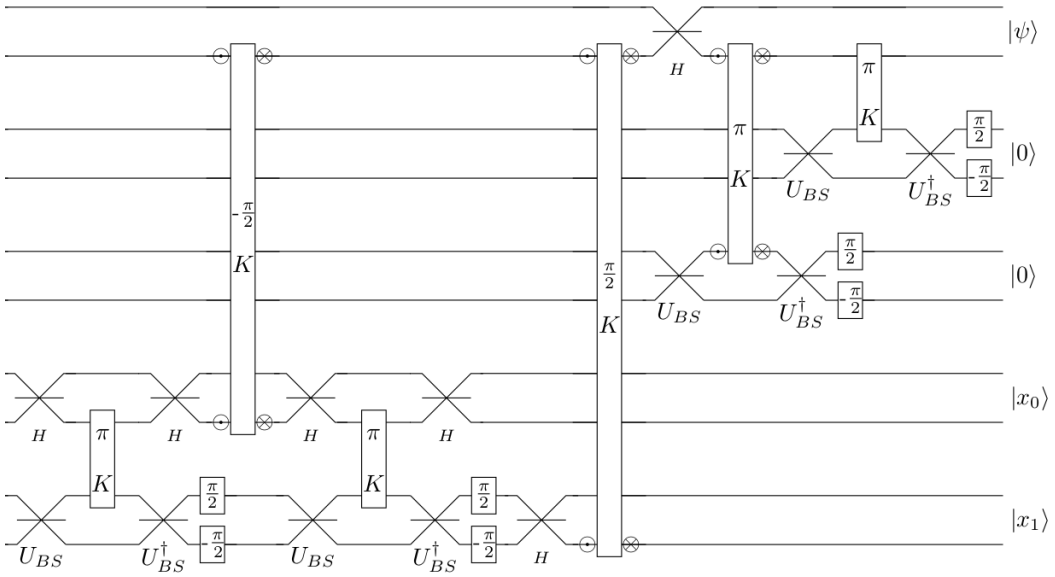

Figura 3.36. Código de tres qubits para inversión del bit en representación de doble riel, elaboración propia. Parte 4.

dar el mismo tratamiento de detección y corrección de a ambos tipos de errores [8].

Para corregir errores más generales que inversiones del bit y de fase, se utiliza el código de nueve qubits de Shor, descrito en el último apartado del Capítulo 1. Este código codifica un qubit en tres bloques de tres qubits cada uno, utilizando una combinación de las codificaciones utilizadas en los códigos para inversión del bit y para inversión de fase [8]. Tras el paso por el canal ruidoso, el código emplea 6 qubits auxiliares y compuertas **CNOT** estándar para hallar síndrome de error por inversión del qubit; luego utiliza dos qubits auxiliares más y compuertas C^6**-NOT** para hallar síndrome de error por inversión de fase [8]. Como se mostró en el capítulo en referencia, todos los posibles errores sobre un qubit individual se reducen a una de tres posibilidades: inversión del bit, inversión de fase, y la combinación de ambos. Una compuerta C^6**-NOT** se puede construir utilizando la demostración del Capítulo 1 para la compuerta C^k**-U**, donde $\mathbf{U} = \sigma_x$.

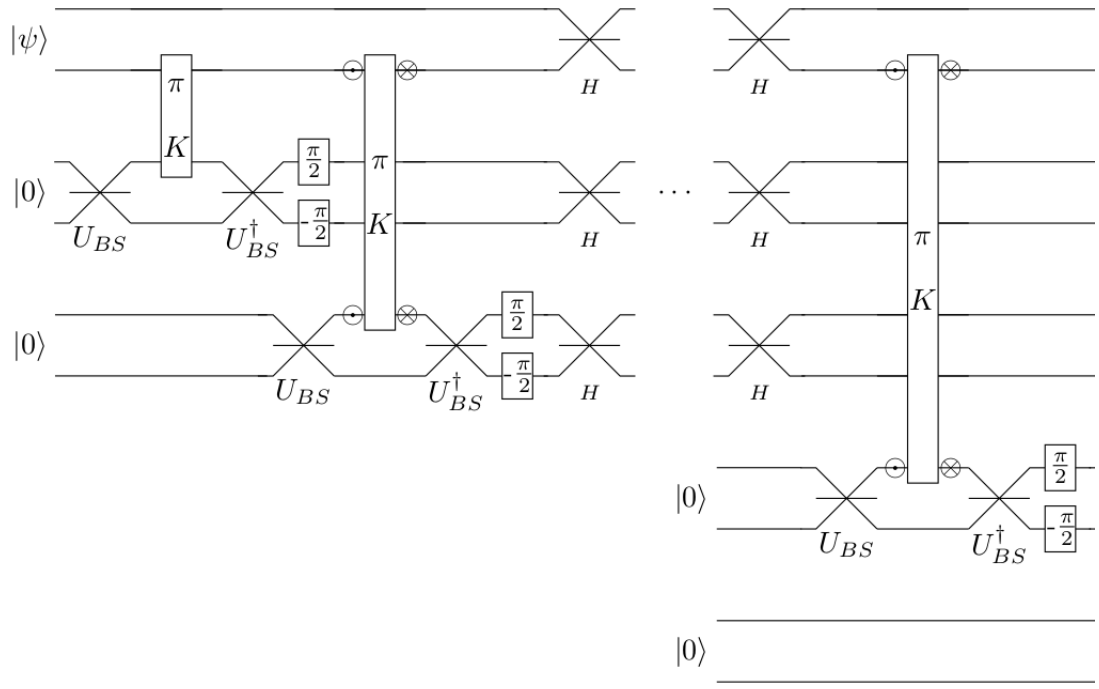

Figura 3.37. Código de tres qubits para inversión de fase en representación de doble riel, elaboración propia. Sección que difiere del código para inversión del bit.

CONCLUSIONES

1. La idea fundamental de la computación cuántica es que la superposición de estados cuánticos, y el entrelazamiento cuántico relacionado, permiten realizar operaciones computacionales sobre registros informáticos que se encuentran en múltiples estados a la vez. Esta idea significa que un solo proceso de computación cuántica realizaría el equivalente a múltiples procesos clásicos, y este paralelismo resultaría en aumentos de eficiencia significativos respecto de la computación clásica. Como mostró el desarrollo del algoritmo de Shor en el Capítulo 1, esta menor necesidad de recursos permitiría que la computación cuántica sea capaz de realizar eficientemente tareas que ninguna computadora clásica podría realizar en un tiempo razonable.

2. La manipulación del estado de un registro de qubits se realiza a través de compuertas lógicas cuánticas, análogamente a la manipulación de bits clásicos con compuertas lógicas clásicas. Una compuerta cuántica es un operador unitario que evoluciona el estado de un qubit o qubits de una manera preestablecida, y la construcción de sucesiones de compuertas cuánticas para lograr un estado final específico del registro es la base de la programación cuántica. Existen conjuntos finitos de compuertas cuánticas con cuyos elementos se puede construir una operación computacional arbitraria, conocidos como Conjuntos universales de compuertas; uno de estos conjuntos está compuesto por las compuertas cuánticas de un solo qubit y la compuerta **CNOT** estándar.

3. La óptica cuántica es el estudio de los fenómenos que surgen a partir de la cuantización escalar del campo electromagnético, donde los fotones surgen como la eigenbase $\{|n\rangle\}_0^\infty$ del hamiltoniano de oscilador armónico simple asociado a esta cuantización. Los medios ópticos provocan evoluciones de los estados fotónicos que en el límite clásico corresponden a efectos conocidos en la óptica clásica: los espejos cambian la trayectoria de los fotones, los espejos parciales imponen una probabilidad de transmisión y una de reflexión, y los cambios de índice de refracción se manifiestan en desplazamientos de fase de los estados

cuánticos. Los medios Kerr provocan desplazamientos de fase acoplados entre dos modos fotónicos.

4. En la representación de doble riel óptico de los qubits, las compuertas lógicas cuánticas se construyen con medios ópticos lineales y con medios Kerr (no-lineal de tercer orden): los espejos cambian las trayectorias de los fotones, los cambios de índice de refracción imponen desfases sobre los estados fotónicos, los divisores de haz (espejos parciales con prismas) provocan que un fotón quede en una superposición de dos posibles trayectorias, y los medios Kerr permiten acoplar dos fotones de diferentes qubits en un desfase, lo que permite el funcionamiento de compuertas de dos qubits. Con estas operaciones se puede armar el Conjunto universal de compuertas descrito previamente y, por tanto, todos los algoritmos cuánticos deseados; sin embargo, las limitaciones asociadas al efecto Kerr necesario son el principal obstáculo para que este modelo de computación cuántica sea realista.

TRABAJO A FUTURO Y RECOMENDACIONES

1. Las limitaciones de los materiales Kerr disponibles impiden utilizar la representación de doble riel óptico de la computación cuántica; por otro lado, el trabajo sobre las propiedades cuánticas del grafeno presentado por Hendry en [14] muestra avances hacia conseguir altas susceptibilidades Kerr en longitudes de onda visibles con bajas tasas de absorción lumínica. De esta manera, se recomienda la investigación sobre propiedades ópticas no lineales porque es importante para el desarrollo de la computación cuántica, y presenta oportunidades para avanzar el conocimiento de esta área.

2. Como menciona Drake en [11], es posible utilizar simultáneamente más de un tipo de implementación óptica de computación cuántica, buscando que las ventajas de cada tipo de implementación compense los defectos del otro u otros. Esto presenta la posibilidad de investigar comparativamente diversas implementaciones de computación cuántica y sus compuertas lógicas en busca de formas de acoplar diferentes tipos de implementaciones para llegar a lograr una computadora cuántica verdaderamente tolerante al error, oportunidad que debe estudiarse a profundidad.

3. En este trabajo se presentaron métodos de estimación de incerteza para errores unitarios, y códigos para proteger información cuántica contra el ruido en canales de transmisión cuántica, pero sólo para errores que afectan qubits individualmente y en canales sin memoria. Como muestran Benenti, Casati y Strini [8] y Nielsen y Chuang [9], los errores cuánticos son un área que requiere un estudio profundo de los avances logrados hasta ahora. Además, como explica Hidary [15], la investigación sobre errores en la computación cuántica y métodos de protección contra estos es una de las áreas en las que se debe invertir recursos significativos debido a su importancia para lograr una computadora cuántica que verdaderamente supere a las mejores computadoras clásicas disponibles actualmente.

4. El estudio a mayor profundidad de la computación cuántica general, la información cuántica y materia condensada son el punto de partida para proponer posibles implementaciones de computación cuántica y superar los problemas que cada método conlleva.

BIBLIOGRAFÍA

[1] A. Aspect, C. Fabre y G. Grynberg. *Introduction to Quantum Optics: From the Semi-classical Approach to Quantized Light.* Cambrige University Press, Cambridge, UK, 2010.

[2] A. Aspect, J. Dalibard, y G. Roger. *Experimental Test of Bell's Inequalities Using Time- Varying Analyzers.* Physical Review Letters 49, 1804, EEUU, 1982.

[3] A. Aspect, P. Grangier, y G. Roger. *Experimental Tests of Realistic Local Theories via Bell's Theorem.* Physical Review Letters 47, 460, EEUU, 1981.

[4] A. Aspect, P. Grangier, y G. Roger. *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment : A New Violation of Bell's Inequalities.* Physical Review Letters 49, 91, EEUU, 1982.

[5] J. S. Bell. *On the Einstein Podolsky Rosen paradox.* Physics 1 (3), 195, EEUU, 1964.

[6] J. S. Bell. *On the Problem of Hidden Variables in Quantum Mechanics.* Reviews of Modern Physics 38, 447, EEUU, 1966.

[7] G. Benenti, G. Casati y G. Strini. *Principles of Quantum Computation and Information, Volume I: Basic Concepts.* World Scientific Publishing Co. Pte. Ltd., Singapore, 2004.

[8] G. Benenti, G. Casati y G. Strini. *Principles of Quantum Computation and Information, Volume II: Basic Tools and Special Topics.* World Scientific Publishing Co. Pte. Ltd., Singapore, 2007.

[9] I. Chuang y M. Nielsen. *Quantum Computation and Quantum Information. 10th Anniversary Edition.* Cambrige University Press, Cambridge, UK, 2010.

[10] S. Cook y L .Levin. *Millennium Problems: P vs NP Problem* Clay Mathematics Institute, Massachusetts, EEUU, 2000.

[11] G. Drake. *Springer Handbooks of Atomic, Molecular, and Optical Physics.* Springer Science+Business Media, Inc., New York, 2006.

[12] C. Gerry y P. Knight. *Introductory Quantum Optics.* Cambrige University Press, Cambridge, UK, 2005.

[13] E. Hecht. *Optics. Global Edition. 5th ed.* Pearson Education Limited, Harlow, Inglaterra, UK, 2019.

[14] E. Hendry, et al. *Strong nonlinear optical response of graphene flakes measured by four-wave mixing.* arXiv:0912.5321 [cond-mat.mtrl-sci], 2009.

[15] J. Hidary. *Quantum Computing: An Applied Approach.* Springer Nature Switzerland AG, Cham, Suiza, 2019.

[16] E. Schrödinger. *Die gegenwärtige Situation in der Quantenmechanik.* Naturwissenschaften 23 (48), 807, y (49), 823, y (50), 844, Alemania, 1935.

[17] E. Schrödinger. *Discussion of Probability Relations between Separated Systems.* Mathematical Proceedings of the Cambridge Philosophical Society 31, 555, Cambridge, UK, 1935.

[18] E. Schrödinger. *Probability relations between separated systems.* Mathematical Proceedings of the Cambridge Philosophical Society 32, 446, Cambridge, UK, 1936.

[19] J. R. Taylor. *An Introduction to Error Analysis.* University Science Books, Sausalito, California, EEUU, 1997.

[20] J. Yin, et al. *Satellite-based entanglement distribution over 1200 kilometers.* China, 2017.