



Universidad Simón Bolívar
Decanato de Estudios Profesionales
Coordinación de Tecnología e Ingeniería de Electrónica

Diseño y simulación de procesadores cuánticos que implementen algoritmos cuánticos de búsqueda

Por:
Miguel Casanova
Realizado con la asesoría de:
Enrique Castro y Sttiwuer Diaz

PROYECTO DE GRADO
Presentado ante la Ilustre Universidad Simón Bolívar
como requisito parcial para optar al título de
Ingeniero Electrónico

Sartenejas, noviembre de 2018

Resumen

El computador cuántico es la promesa tecnológica más relevante del presente siglo, siendo los circuitos cuánticos superconductores los candidatos idóneos para la construcción escalable de procesadores cuánticos eficientes. Un procesador cuántico ejecuta algoritmos cuánticos aplicando secuencias programables de compuertas cuánticas a un registro de entrada conformado por qubits, los cuales evolucionan a un estado cuántico final, el cual es la solución de un algoritmo. Dicho estado cuántico final se caracteriza por tener una familia de correlaciones cuánticas tales como entrelazamiento, discordia cuántica y medida geométrica de la discordia. Experimentalmente, se han logrado implementar en la última década procesadores cuánticos superconductores en base a arquitecturas de transmones, con qubits y qutrits, para los algoritmos cuánticos de Deutsch, Deutsch-Jozsa y Grover. En el presente trabajo se diseñaron y simularon, en base a arquitecturas superconductoras de transmones, procesadores cuánticos que implementen eficientemente los algoritmos cuánticos de Grover y Shor. Además, el internet cuántico permite la comunicación cuántica entre procesadores cuánticos remotos, utilizando procesadores cuánticos locales, que están interconectados por canales de comunicación cuántica que permiten la transmisión de qubits entre los diferentes procesadores, para resolver problemas que son inviables clásicamente, razón por la cual se estudia la posibilidad de construir circuitos cuánticos del algoritmo de Google Cuántico, así como su representación en una arquitectura superconductora de transmones. En cada uno de los casos estudiados se diseñaron los circuitos cuánticos asociados, su simulación en Python y Mathematica, y se estudió de la información cuántica generada respectivamente.

Agradecimientos

Muchas gracias a Aileen Salas, Alejandro Linares, Alessandra Marrero, Alfredo Ríos, Alfredo Villegas, Álvaro Rodrigues, Amira Ibrahim, Andrea Molina, Andrea Ramírez, Andrea Sánchez, Andrés Torres, Antonio Sanjurjo, Augusto Hidalgo, Carlos Castañeda, Carlos Sánchez, Carlos Sanoja, Carlota Casanova, Carmen Affigne, Carmen Aguilar, Chris Carias, Cristhian Da Silva, Cristina Sánchez, Daniela Díaz, Daniela González, David Altuve, David Atias, Diosa Medina, Domingo Luis, Domingo Vargas, Eddie Chang, Eder Buitrago, Edgard Bonilla, Elinor Appel, Elkin Montoya, Enrique Castro, Enzo D'Argento, Enzo D'Argento, Éric Leroux, Eduardo Hernández, Edward Klindt, Elba Guerra, Elba Guerra, Elías Tsoukatos, Elinor Appel, Esteban Puky, Eugenio Martínez, Frederick Klindt, Gabriel Marzinotto, Gabriel Mercado, Gabriel Napoli, Gabriel Olivieri, Gabriel Rodríguez, Gabriela D'Argento, Gerardo Fernández, Génesis Jiménez, Gilberto Marín, Gloria Jesurún, Giancarlo Cuticchia, Gianpaolo Cuticchia, Gonzalo Silva, Gustavo Kufatty, Grace Lafontant, Guillermo Olmos, Guillermo Villegas, Haydn Barros, Héctor Liberatore, Javier Ramos, Jeinny Pérez, Jessica Rondón, Jesús Angarita, Johel Arteaga, Jonathan Klindt, Jorge Osorio, Jorge Sánchez, José Arcila, José Carrero, Josle Marquina, José Cappelletto, José Domínguez, Josué Rico, Juan Febles, Juan Pérez, Julio Fuenmayor, Juver Rosillo, Karelía Díaz, Kevin Ng, Kira Casanova, Laura Ocanto, Lénore Casanova, Leonardo Ward, Lin Song, Lionel Rodríguez, Loinas Barrera, Luis Flores, Luis Anselmi, Luis Vásquez, Magali Godoy, Manuel Morgado, María Palma, María Jiménez, Mario Quintero, Mathias San Miguel, Maurizio Dall'Est, Michelle Márquez, Michelle Woo, Miguel Casanova, Miguel Casanova, Novel Certad, Oriana Esparragoza, Pablo Betancourt, Pablo Giuliani, Pedro Maldonado, Pedro Ovalles, Pedro Pérez, Pelusa Medina, Rafael Silva, Rafael Tellez, Raul Barroso, Rintaro Kanaki, Roberto Gudiño, Rosty Bruce, Rubén Rojas, Rubmary Rojas, Said Alvarado, Samira Sánchez, Samuel Zambrano, Sara Berman, Silvio Rivero, Simón Rincón, Stefanni Flores, Steven Leung, Steven Scalzo, Sttiwuer Díaz, Shunichi Watanabe, Terfa El Ryfaie, Valentina Cegarra, Zeigneth Angarita y demás personas que seguro no recuerdo en este momento por su compañía, asistencia, atención, apoyo, tutoría y amistad a lo largo de todos estos años.

Índice general

Índice de Figuras	7
1. Introducción	10
2. Información cuántica	19
2.1. Espacios de Hilbert	19
2.2. Operadores lineales	22
2.3. Delta de Kronecker	22
2.4. Operadores hermíticos	23
2.5. Operadores unitarios	23
2.6. Conmutador y anticonmutador	24
2.7. Estados cuánticos	25
2.8. Sistemas multipartitos	30
2.9. Postulados de la mecánica cuántica	33
2.10. Entrelazamiento	35
2.11. Qubits	36
2.12. Esfera de Bloch	37
2.13. Matrices de Pauli	38
2.14. Circuitos cuánticos	38
2.15. Compuertas cuánticas de un qubit	41
2.15.1. Compuerta identidad	41
2.15.2. Compuerta X	41
2.15.3. Compuerta Z	42
2.15.4. Compuerta Y	43
2.15.5. Compuerta de Hadamard	43
2.15.6. Compuerta S	44
2.15.7. Compuerta T	44
2.15.8. Compuerta de cambio de fase	45
2.15.9. Compuertas de rotación	45
2.16. Compuertas multiqubit	47
2.16.1. Compuerta CNOT	47
2.16.2. Compuerta SWAP	47
2.16.3. Compuerta $\sqrt{\text{SWAP}}$	48
2.16.4. Compuerta de Ising	49
2.16.5. Compuerta de Toffoli	49

2.16.6. Compuerta de Deutsch	50
2.17. Conjuntos universales de compuertas cuánticas	51
2.18. Criterios de DiVincenzo	51
2.19. Fidelidad	52
2.20. Medidas proyectivas	53
2.21. Sistemas cuánticos abiertos	54
3. Superconductividad	61
3.1. Cuantización macroscópica y superconductividad	61
3.2. La teoría BCS	63
3.3. Cuantización del flujo magnético y efecto tunel Giaver	71
3.4. Efecto Josephson	77
3.5. Componentes de la corriente en las uniones de Josephson	82
3.6. Cuantización del oscilador armónico LC	83
3.7. Qubits superconductores	85
3.8. Arquetipos de qubits superconductores	86
3.9. Transmones	87
3.10. Hamiltonianos multiqubit de transmones	89
3.11. Compuertas cuánticas en transmones	90
3.11.1. Rotaciones X-Y	92
3.11.2. Compuerta de entrelazamiento	93
3.11.3. Compuertas compuestas	94
4. El simulador de compuertas cuánticas en transmones	95
4.1. Parámetros de los sistemas simulados	96
4.2. Compuertas nativas	97
4.2.1. Rx y Ry	97
4.2.2. iSWAP	99
4.3. Compuertas compuestas	100
4.3.1. X	100
4.3.2. Y	100
4.3.3. Rz	101
4.3.4. Z	101
4.3.5. H	102
4.3.6. CNOT	102
4.3.7. SWAP	102
4.3.8. Compuertas condicionales generales	103
4.3.9. CP	107
5. Algoritmo de Grover	115
5.1. El algoritmo	119
5.2. Variaciones y generalizaciones del algoritmo de Grover	120
5.2.1. Algoritmo de amplificación de amplitud	120
5.2.2. Algoritmo de Grover en un paso	123
5.2.3. Optimización del algoritmo de Grover	124

5.3. Simulaciones	125
6. Algoritmo de Shor	131
6.1. Transformada cuántica de Fourier	131
6.2. Estimación de fase	133
6.3. Estimación de orden	135
6.4. Expansión en fracciones continuas	139
6.5. Algoritmo de factorización de Shor	140
6.6. Simulaciones	141
6.6.1. Factorización del número 15	141
6.6.2. Factorización del número 8	144
7. Google PageRank	146
7.1. El algoritmo de remiendo (parcheo) general	149
7.2. Interpretación como una caminata aleatoria	150
7.3. Cuantizando las caminatas aleatorias	151
7.4. Caminata cuántica de Szegedy	152
7.5. PageRank Cuántico	153
7.6. Circuitos de las caminatas cuánticas de Szegedy	154
7.7. Simulaciones	158
7.7.1. Grafo estrella	159
7.7.2. Grafo corona	163
7.7.3. Grafo árbol	167
7.7.4. Grafo aleatorio	171
8. Conclusiones	176
A. Cálculos de Hamiltonianos	180
A.1. Régimen rotacional del pulso	180
A.2. Efecto del pulso sobre el qubit	184
A.3. Régimen dispersivo	186
B. Códigos del simulador	192
B.1. Wolfram Mathematica	192
B.2. Python	199
C. Códigos de la simulación del algoritmo de Grover	212
C.1. Wolfram Mathematica	212
C.2. Python	213
D. Códigos de la simulación del algoritmo de Shor	216
D.1. Wolfram Mathematica	216
D.2. Python	219
E. Códigos de la simulación del algoritmo de PageRank	222
E.1. Wolfram Mathematica	222

E.2. Python	225
E.2.1. Grafo estrella	229
E.2.2. Grafo corona	233
E.2.3. Grafo árbol	235
E.2.4. Grafo aleatorio	238

Índice de figuras

2.1. Esfera de Bloch	37
2.2. Compuerta I en la esfera de Bloch	41
2.3. Compuerta X en la esfera de Bloch	42
2.4. Compuerta Z en la esfera de Bloch	42
2.5. Compuerta Y en la esfera de Bloch	43
2.6. Compuerta H en la esfera de Bloch	44
2.7. Compuerta S en la esfera de Bloch	44
2.8. Compuerta T en la esfera de Bloch	45
2.9. Compuerta P en la esfera de Bloch	45
2.10. Compuertas Rx, Ry y Rz en la esfera de Bloch	46
3.1. Diagrama de Feynman de la interacción electrón-fonón-electrón . . .	66
3.2. Construcción geométrica de los posibles electrones candidatos para formar pares de Cooper, siendo $\hbar K$ el momentum del centro de masas.	68
3.3. Cuantización del flujo magnético	73
3.4. Diagrama de energía de una unión metal-aislante-metal en la que no puede haber efecto túnel	75
3.5. Diagrama de energía de una unión metal-aislante-metal en la que puede haber efecto túnel	76
3.6. Diagrama de energía de una unión superconductor-aislante-metal en la que puede haber efecto Giaver	77
3.7. Curva característica I-V de una unión Josephson	81
4.1. Rotaciones en X e Y de 2π	98
4.2. Rotaciones en X e Y de π	98
4.3. Rotaciones en X e Y de $\frac{\pi}{2}$	98
4.4. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $ 00\rangle$	99
4.5. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $ 01\rangle$	99
4.6. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $\frac{ 00\rangle+ 11\rangle}{\sqrt{2}}$	99
4.7. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}}$	100
5.1. Circuito del algoritmo de Grover, k_{max} desconocido.	117
5.2. Interpretación geométrica del operador difusión	119
5.3. Circuito del algoritmo de Grover.	120
5.4. Evolución de las probabilidades en el algoritmo de Grover sin relajación	126

5.5. Evolución de las probabilidades en el algoritmo de Grover con relajación, $\mathcal{W} = \{0\}$	128
5.6. Evolución de las probabilidades en el algoritmo de amplificación de amplitud sin relajación, $\mathcal{W} = \{9, 13\}$	129
5.7. Evolución de las probabilidades en el algoritmo de amplificación de amplitud sin relajación, $\mathcal{W} = \{4, 5, 12, 13\}$	129
5.8. Evolución de las probabilidades en el algoritmo de amplificación de amplitud con relajación	130
6.1. Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas	142
6.2. Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas	144
7.1. Grafo de ejemplo para el PageRank clásico	146
7.2. Transformación de un grafo al crear la matriz de Google con $\alpha = \frac{1}{2}$	150
7.3. Operador de permutación	155
7.4. Circuito de Loke [1] para las caminatas cuánticas de Szegedy	156
7.5. Circuito de K_i	157
7.6. Grafo estrella	159
7.7. Circuito de K_1 para el grafo estrella	160
7.8. Circuito de K_2 para el grafo estrella	160
7.9. K_b del grafo estrella	160
7.10. T del grafo estrella	160
7.11. Preparación del estado inicial para la caminata en el grafo estrella	161
7.12. Circuito del PageRank cuántico del grafo estrella	161
7.13. PageRank cuántico instantáneo del grafo estrella sin pérdidas	161
7.14. PageRank cuántico promedio del grafo estrella sin pérdidas	162
7.15. PageRank cuántico instantaneo del grafo estrella con y sin pérdidas	162
7.16. PageRank cuántico promedio del grafo estrella con y sin pérdidas	163
7.17. Grafo corona	164
7.18. Circuito de K_1 para el grafo corona	164
7.19. Circuito de K_2 para el grafo corona	165
7.20. K_b del grafo corona	165
7.21. T del grafo corona	165
7.22. Preparación del estado inicial para la caminata en el grafo corona	165
7.23. Circuito del PageRank cuántico del grafo corona	166
7.24. PageRank cuántico instantáneo del grafo corona sin pérdidas	166
7.25. PageRank cuántico promedio del grafo corona sin pérdidas	166
7.26. PageRank cuántico instantaneo del grafo aleatorio con y sin pérdidas	167
7.27. PageRank cuántico promedio del grafo aleatorio con y sin pérdidas	167
7.28. Grafo árbol	167
7.29. Circuito de K_1 para el grafo árbol	168
7.30. Circuito de K_2 para el grafo árbol	168
7.31. Circuito de K_3 para el grafo árbol	169

7.32. K_b del grafo árbol	169
7.33. T del grafo árbol	169
7.34. Preparación del estado inicial para la caminata en el grafo árbol . . .	169
7.35. Circuito del PageRank cuántico del grafo árbol	170
7.36. PageRank cuántico instantáneo del grafo árbol sin pérdidas	170
7.37. PageRank cuántico promedio del grafo árbol sin pérdidas	170
7.38. PageRank cuántico instantaneo del grafo árbol con y sin pérdidas . .	171
7.39. PageRank cuántico promedio del grafo árbol con y sin pérdidas . .	171
7.40. Grafo aleatorio	171
7.41. Circuito de K_1 para el grafo aleatorio	172
7.42. Circuito de K_2 para el grafo aleatorio	172
7.43. Circuito de K_3 para el grafo aleatorio	173
7.44. K_b del grafo aleatorio	173
7.45. T del grafo aleatorio	173
7.46. Preparación del estado inicial para la caminata en el grafo aleatorio	173
7.47. Circuito del PageRank cuántico del grafo aleatorio	174
7.48. PageRank cuántico instantáneo del grafo aleatorio sin pérdidas . . .	174
7.49. PageRank cuántico promedio del grafo aleatorio sin pérdidas	174
7.50. PageRank cuántico instantaneo del grafo aleatorio con y sin pérdidas	175
7.51. PageRank cuántico promedio del grafo aleatorio con y sin pérdidas	175

Capítulo 1

Introducción

La computación cuántica [2, 3, 4, 5] está entre las tecnologías más avanzadas, prometedoras y desafiantes del presente siglo. La computación cuántica es un paradigma de computación distinto al de la computación clásica y su objetivo principal es el de controlar la evolución temporal estados cuánticos entrelazados en sistemas multipartitos de alta complejidad. Para ellos se usan qubits, los cuáles son estados cuánticos que pueden estar superpuestos con fases locales relativas complejas, y que además presentan correlaciones cuánticas, que no tienen ningún análogo con aquellas existentes en las arquitecturas existentes para los computadores clásicos, tales como el entrelazamiento, la discordia cuántica, la medida geométrica y la medida geométrica de la discordia. Un algoritmo cuántico es un proceso lógico encaminado a realizar una tarea específica. Con frecuencia, las etapas de un algoritmo cuántico se pueden concretar en la evaluación de una función sobre distintos parámetros de entrada. El paralelismo cuántico permite a los algoritmos cuánticos evaluar una función simultáneamente sobre todas las posibles cadenas de n bits. El problema es que la información queda almacenada en las amplitudes de probabilidad del estado cuántico resultante, y para acceder a ella se requiere una medición cuántica, la cual, en el contexto de las medidas fuertes tipo von-Neumann, destruye parte de la información. Un algoritmo cuántico se representa por un circuito que evoluciona de izquierda a derecha. El estado de entrada suele ser un n -qubit en el estado $|0\rangle$, y las medidas cuánticas proyectivas fuertes se realizan a la salida del circuito.

Los algoritmos cuánticos se pueden clasificar en tres clases:

1. Algoritmos cuánticos basados en la transformada cuántica de Fourier (QFT): estos se basan en que podemos formar la serie de Fourier en una superposición de estados cuánticos, y poder operar con ella para obtener los resultados que deseamos. Este tipo de algoritmo cuántico es muy importante ya que existen muchos problemas actuales se resuelven a través de la QFT, y una versión cuántica de dicho algoritmo, la cual que provee de un cálculo aún más rápido genera nuevas expectativas tecnológicas.
2. Algoritmos cuánticos de búsqueda: Se considera que este tipo de algoritmos es uno de los más importantes ya que muchos problemas tecnológicos pueden reducirse a una búsqueda en bases de datos no estructuradas. Además promete una eficiencia cuadrática en las búsquedas. Uno de los beneficios de utilizar este tipo de algoritmos es que no destruye el conjunto de datos de búsqueda, sino que simplemente marca los valores que satisfacen la condición de búsqueda. Este hecho es muy significativo, ya que al no poderse clonar qubits se garantiza que los resultados encontrados son únicos.
3. Algoritmos cuánticos de simulación: La computación cuántica es la mejor oportunidad tecnológica actual para realizar simulaciones en sistemas cuánticos, y por consiguiente clásicos. En una computadora clásica se necesitan una cantidad exponencial de recursos para poder simular un sistema, sin embargo en una computadora cuántica la cantidad de recursos es lineal. Sin embargo, la eficiencia que se obtiene al simular el sistema no garantiza que se obtenga la información que se desea de la simulación ya que al medir obtenemos una cantidad lineal de datos y no toda la información del sistema. Entonces el reto está en encontrar la manera de encontrar como extraer la información necesaria del sistema sin destruirla parcial o totalmente. Actualmente esta área del conocimiento está avanzando a ritmos muy acelerados, y la mayoría de los laboratorios de computación cuántica a nivel mundial están logrando grandes avances en este tópico. Los algoritmos cuánticos están formulados y descritos usando un lenguaje de programación cuántica de alto nivel. Dependiendo de la elección del código de corrección de error cuántico a usar como código de superficie, el compilador toma esa descripción como entrada, realiza la optimización y genera una implementación tolerante a fallas del algoritmo cuántico original. Se necesita una microarquitectura de control para decodificar las instrucciones cuánticas en las señales de control requeridas en tiempos precisos, así como la detección de errores cuánticos en tiempo real y su corrección. Finalmente, basado en la tecnología cuántica específica usada, por ejemplo qubits superconductores, iones atrapados, spin

qubits, centros de vacantes de nitrógeno, etc [5], el control las señales se traducen en los impulsos requeridos, y estos se envían al chip a través de una interfaz cuántica-clásica. En este contexto en el presente trabajo nos vamos a centrar en el estudio de los algoritmos de búsqueda de Grover, de Shor y de Google cuántico.

El algoritmo cuántico de búsqueda de Grover resuelve el problema de búsqueda no estructurada en una lista de N datos, con una solución única, usando solamente $O(\sqrt{N})$ evaluaciones. En este algoritmo se aprovecha el paralelismo cuántico para evaluar simultáneamente f sobre todos los posibles x de $[0, N - 1]$, construyendo una superposición con la transformación de Walsh-Hadamard, y se simula con su circuito cuántico asociado.

La dificultad computacional de resolver el problema de la factorización de enteros es la base del criptosistema RSA. El algoritmo de Shor es un algoritmo cuántico que permite factorizar un número N en tiempos de $O(poly(\log(N)))$. Dado N impar y con al menos dos factores primos, el problema de encontrar un factor primo de N se puede reducir al de encontrar el orden de un entero positivo a tal que $mcd(a, N) = 1$. Es decir, se debe encontrar el mínimo $t > 0$ tal que $a^t \bmod N = 1$. El algoritmo de Shor es polinomial respecto al número de dígitos de N . El problema de la factorización se puede reducir al cálculo del período de una función entera, y para ello se puede usar la QFT. Es decir, si f es una función entera y periódica de periodo T , su QFT se anula en todos los elementos del dominio salvo en los múltiplos de la frecuencia ω tal que $\omega T = Q$.

$$F_n\left(\sum_{j=0}^{Q-1} f_j |j\rangle\right) = \sum_{k=0}^{T-1} \hat{f}_{\omega_k} |\omega_k\rangle \quad (1.1)$$

Se aplica la QFT a f y se miden todos los qubits de forma tal que se obtiene ω_k , tal que $0 \leq k \leq T$. Esta propiedad permite obtener la frecuencia, y por tanto el período, de la función f .

En las últimas dos décadas se han desarrollado numerosas plataformas para construir computadores cuánticos. Las más avanzadas hasta ahora se basan en uniones superconductoras de Josephson y en trampas de iones. Particularmente, en el caso de los qubits superconductores [6, 7, 8], los más trabajados al día de hoy son los transmones, los cuales son qubits de carga basados en una caja de Cooper derivada capacitivamente de una unión de Josephson, diseñada para tener una

sensibilidad reducida a ruidos de carga. Debido a su tamaño microscópico, del orden de micrómetros, los circuitos superconductores se acoplan fuertemente a su entorno en comparación con sistemas microscópicos bien aislados. Aunque esto pudiera parecer un obstáculo aparentemente insuperable, ya se han descubierto y eliminado muchas fuentes de ruido con diseños notablemente inteligentes, y los tiempos de coherencia del qubit se han alargado varios órdenes de magnitud [7] en la última década, haciendo que los sistemas superconductores sean cada vez más la elección más prometedora para el diseño de procesadores cuánticos de múltiples qubits. Actualmente, los procesadores cuánticos se controlan con señales eléctricas bien definidas, por ejemplo, frecuencia de microondas y pulsos, que requieren parámetros y tiempos precisos.

Otras plataformas, bastante prometedoras, que se han comenzado a desarrollar recientemente son los qubits “flip-flop” [9, 10, 11, 12], basados en spines electrónicos y nucleares acoplados en sistemas de estado sólido, que permiten acoplamiento de qubits a distancias lo suficientemente largas como para introducir circuitos clásicos de control entre los qubits; y los qubits de modos cero de Majorana, basados en estructuras topológicas de puntos cuánticos y pistas superconductoras sobre sistemas de estado sólido, que son inmunes a errores locales. IBM e Intel, han construido chips de hasta 16 y 17 qubits, respectivamente, utilizando circuitos superconductores. Google e IBM tienen, cada uno, proyectos para construir chips superconductor de 49 qubits para aplicaciones comerciales, entre finales del 2017 y principios del 2018. En el presente trabajo utilizaremos arquitecturas superconductoras basadas en transmones para el desarrollo y simulación de los algoritmos cuánticos propuestos. El transmon [12] es una implementación de Uniones Josephson (JJ) basando en cajas de pares de Cooper, que permiten construir compuertas cuánticas que poseen poca decoherencia cuántica. Su nombre es una abreviatura del término qubit de oscilación de plasma derivado de línea de transmisión (transmission line shunted plasma oscillation qubit). En estos los potenciales involucrados permiten construir sistemas de qubit de múltiples niveles, y los niveles más altos son los que a menudo se usan para la implementación de compuertas de 2 qubits. Estos niveles son excitados por microondas. Estos han sido muy eficientes en la implementación de algoritmos cuánticos como el de Grover [13, 14, 15, 16], el de DeutschJozsa [16, 17, 18] y el de Shor [19, 20, 21]. Recientemente el algoritmo de Grover ha sido estudiado más detenidamente, y se han encontrado nuevas optimizaciones [22], y se también han analizado sus correlaciones cuánticas [23, 24]. Similarmente el algoritmo de Shor se ha optimizado recientemente [25, 26], y se han creado circuitos

cuánticos mucho más eficientes que los originales, que perfeccionan significativamente la QFT sobre la que se basa dicho algoritmo, hasta el punto que se puede simular en tarjetas FPGA avanzadas [27].

Todo algoritmo cuántico tiene siempre un circuito cuántico asociado. Los primeros algoritmos cuánticos de búsqueda se diseñaron considerando compuertas cuánticas unitarias llamadas oráculos, las cuales eran, matemáticamente hablando, cajas negras que realizaban funciones cuánticas, aunque no se conociera que compuertas cuánticas las conformaban. Sin embargo, es a partir de 2013, con el trabajo de Johnson y colaboradores [28] que la simulación de circuitos cuánticos en computadores clásicos, para obtener los resultados de una búsqueda cuántica, han adquirido capital importancia. La idea de no simular dichos circuitos cuánticos, sino de implementarlos físicamente ya es un hecho para empresas como IBM, NCIT, GOOGLE e INTEL. Recién en el 2016, La empresa IBM publicó en Internet una página web de acceso libre, en la cual si se deseaba simular un circuito cuántico sólo debía escribirlo sobre una plataforma específica, y ella lo simulaba y daba los resultados solicitados, en tiempos muy breves, los cuales mostraban de manera diáfana la ventaja del computador cuántico sobre el clásico.. Aún más, ellos ofrecían la posibilidad de lograr la realización experimental de dicho circuito, para un número finito de qubits con solo solicitárselo a dicha empresa. IBM implementaba el circuito en arquitecturas de transmones, y daba los resultados. Esta oportunidad única para los investigadores del área tenía solo dos limitantes: (1) nadie sabía cuál era la tecnología que ellos usaban, y (2) era una versión beta que se ofrecía públicamente para que las masas de investigadores en el mundo al usarlas ayudaran a la IBM a que por ensayo y error pudieran detectar sus errores de diseño. Ya a mediados de este año se puso como norma de la empresa que quien deseara usar esos beneficios tecnológicos debería pagar, comercializando así el uso de dicha herramienta.

Siguiendo en el contexto de desarrollar computadores cuánticos acordes a las realidades comerciales y de investigación, ya se han desarrollado circuitos cuánticos completamente tolerantes a errores cuánticos [29], permitiendo así crear circuitos cuánticos de alto nivel de precisión. Sin embargo, los métodos de control existentes introducen un alto consumo de recursos, largos tiempos de configuración y de complejidad de control. Por esta razón, el diseño de procesadores cuánticos capaces de implementar algoritmos cuánticos con funciones específicas, de forma eficiente y que minimicen los recursos de control es uno de los retos más grandes para los Ingenieros Electrónicos y de los Físicos, en el área de Estado Sólido. Por otro lado,

el desarrollo de las tecnologías superconductoras ha logrado que algunos algoritmos que existían solo en el mundo teórico de la computación cuántica tales como el algoritmo para resolver sistemas de ecuaciones lineales [30], se hayan logrado implementar experimentalmente en el 2017 [31], obteniendo resultados precisos que tienen muy alta fidelidad.

Una de las aplicaciones más importantes para la navegación en las Redes de Comunicación Cuántica que actualmente se están desarrollando en Europa, Asia y Estados Unidos, es el algoritmo de Google Cuántico [32, 33]. Su implementación experimental [34] ha ilustrado la importancia del mismo para cuantificar las cadenas de Markov dentro de la matriz del algoritmo de busque de Google. En este trabajo, se desea Diseñar y simular procesadores cuánticos que implementen los algoritmos cuánticos de Grover, Shor y Google Cuántico, en base a arquitecturas superconductoras de transmones y con énfasis en incorporar las innovaciones más modernas que hay para los algoritmos de Grover y Shor.

Por otro lado, la Computación Cuántica y la Comunicación Cuántica son dos áreas tecnológicas que apenas teniendo dos décadas de desarrollo, ofrecen resultados muy prometedores. En particular los últimos dos años marcan una diferencia histórica en el área, diferencia que ya promete que en menos de 5 años se comercializaran muchísimas aplicaciones novedosas que afectaran las culturas tecnológicas de las sociedades mundiales futuras. En mayo de 2016, la Comunidad Europea llego a un acuerdo conocido como el Quantum Manifesto [35], en el cual todos los países miembros se comprometían a aportar entre todos el monto de 1 billón de euros, el cual se usará para lograr que toda Europa en el 2035 tenga la totalidad de sus tecnologías basadas en plataformas cuánticas, desde el ordenador cuántico más simple usado por el ciudadano común, hasta la totalidad de las redes de comunicación. Se prevé el desarrollo aplicaciones en todas las áreas del conocimiento humano con un desarrollo imperativo en las tecnologías militares, medicina, energía alternativas, etc.

Actualmente, el Quantum Manifesto, ha servido como motivación para que los países del primer mundo traten de crear una red cuántica de comunicación global en el planeta [36]. Es importante entender que cuando estas tecnologías se desarrollen se podrán construir computadores cuánticos universales capaces de resolver problemas que a un supercomputador actual le tomaría más tiempo que la edad actual del universo, lo que significa para la raza humana un cambio total en su evolución tecnológica creando nuevos paradigmas en la interpretación del Universo.

En el año 2017, el número de avances logrados en investigación básica y con grandes oportunidades de aplicación comercial ha sido muy amplio, entre las cuales podemos citar:

1. La creación del primer cheque cuántico con un procesador cuántico de 5 qubits [37].
2. El diseño de circuitos clásicos que simulan el algoritmo de Shor [26].
3. El desarrollo de tecnologías cuánticas para el procesamiento de cuánticos imágenes y de películas, las cuales permitirían realizar el procesado de estas con fidelidades muy superiores a las de HD actuales, usando para ello algoritmos cuánticos asistidos por computadores cuánticos [38].
4. El desarrollo de sistemas de distribución de llaves cuánticas (QKD) en criptografía cuántica, basados en procesos de aprendizaje cuántico (quantum machine learning) [39]. Actualmente en los países del primer mundo se desean construir computadores cuánticos que tengan QKD con aprendizaje cuántico.
5. La posibilidad de construir computadores cuánticos nanométricos muy eficientes, y resistentes, con diamantes artificiales excitados con nanofotónica [40].
6. La creación de redes cuánticas de comunicación satelital que permiten distribuir entrelazamiento a 1200 Km de distancia, por nanosatélites [41]. Estas ampliaciones están en este momento en desarrollo experimental-militar, y el gobierno chino ha informado que van a comercializarse a partir del 2018.
7. El desarrollo de algoritmos y circuitos cuánticos capaces de simular eficientemente las redes neurales, logrando por primera vez reproducir los comportamientos reales de dichas redes basándose en la distribución del entrenamiento cuántico [42]. Este resultado es muy importante ya que al desarrollar computadores cuánticos capaces de reproducir estas redes podríamos realizar inimaginables avances en el entendimiento del cerebro humano, y del estudio de la inteligencia artificial cuántica.

Como podemos observar el cambio tecnológico que se avecina, puede colocar a muchos países en profundas desventajas con otros. Solo aquellos que tengan acceso y entiendan estas nuevas tecnologías podrán ir al ritmo del desarrollo de las mismas,

y aquellos que no lo hagan tendrán solo dos opciones: o las compran (creando así una profunda dependencia), o se quedan en un total atraso tecnológico.

Es por esta razón que se propone el presente trabajo de grado. En Venezuela no existe actualmente ningún desarrollo de tecnologías cuánticas, ni en Ingeniería Electrónica, ni en la Física aplicada. Por otro lado, debido a la realidad país actual, es imposible crear ningún computador cuántico, ni superconductor ni en base a tecnologías de silicón, diamante, puntos cuánticos, trampa de iones, átomos neutros, etc [5]. Sin embargo, si poseemos el nivel teórico para diseñar y simular arquitecturas superconductoras basadas en transmones, de computadores cuánticos que puedan realizar funciones específicas de aplicación directa tanto comerciales como de investigación básica. Este trabajo sería pionero en Venezuela, y los logros obtenidos motivarán a la Universidad Simón Bolívar para continuar realizando otros trabajos de grado (Pregrado, Maestría y Doctorado), capaces de generar temas de investigación, e implementar aplicaciones industriales que permitan en un futuro no lejano alcanzar una masa crítica de Ingenieros y Físicos capaces de permitir la actualización e inclusión del país en estas nuevas tecnologías de frontera.

En resumen, en el presente trabajo de grado se diseñaron y simularon procesadores cuánticos capaces de implementar los algoritmos cuánticos de Grover, Shor y Google Cuántico.

La estructura de este trabajo es la siguiente:

1. Introducción
2. Información cuántica: Este capítulo es una revisión bibliográfica de las bases de la teoría de información cuántica necesarias para entender los algoritmos cuánticos y las simulaciones realizadas.
3. Superconductividad: Este capítulo es una revisión bibliográfica, siguiendo el hilo desde los primeros hechos experimentales de la superconductividad y la teoría BCS, hasta las compuertas cuánticas en transmones.
4. El simulador de compuertas cuánticas en transmones: Este capítulo explica el funcionamiento del simulador desarrollado y cómo se ha construido el conjunto de compuertas cuánticas disponibles para el procesador cuántico simulado, a partir de las compuertas nativas de los transmones.
5. Algoritmo de Grover: La primera parte de este capítulo es una revisión bibliográfica del algoritmo de búsqueda de Grover y sus variaciones. La segunda

parte es el análisis de los resultados de las simulaciones realizadas de este algoritmo, tanto para un sistema cerrado, como para un sistema abierto.

6. Algoritmo de Shor: La primera parte de este capítulo es una revisión bibliográfica del algoritmo de factorización de Shor. La segunda parte es el análisis de los resultados de las simulaciones realizadas de este algoritmo.
7. Google PageRank: La primera parte de este capítulo es una revisión bibliográfica del algoritmo de medida de centralidad en grafos, PageRank, su cuantización y la construcción de los circuitos de este algoritmo. Sin embargo, con respecto a los circuitos, en la literatura sólo se encuentra un método para simplificar la implementación de los operadores necesarios, más no la forma explícita de estos circuitos para grafos arbitrarios. Para poder realizar las simulaciones, se ha hallado la forma explícita de estos circuitos para todo grafo arbitrario de cuatro nodos, que son el tipo de grafos que soporta el procesador simulado. Finalmente, la última parte es el análisis de los resultados de las simulaciones realizadas de este algoritmo, tanto para un sistema cerrado, como para un sistema abierto.
8. Conclusiones
9. Apéndices:
 - a) Cálculos de Hamiltonianos: En este apéndice se realiza el cálculo del Hamiltoniano efectivo de los transmones, a partir del cual se generan las compuertas cuánticas del procesador.
 - b) Código del simulador: En este apéndice se presenta el código comentado y explicado del simulador y de la implementación de las compuertas cuánticas desarrolladas.
 - c) Códigos de la simulación del algoritmo de Grover: En este apéndice se presenta el código comentado y explicado del algoritmo de Grover, para cada uno de los casos simulados.
 - d) Códigos de la simulación del algoritmo de Shor: En este apéndice se presenta el código comentado y explicado del algoritmo de Shor, para cada uno de los casos simulados.
 - e) Códigos de la simulación del algoritmo de PageRank: En este apéndice se presenta el código comentado y explicado del algoritmo de PageRank, para cada uno de los casos simulados.

Capítulo 2

Información cuántica

En esta sección introduciremos las bases matemáticas fundamentales para empezar a trabajar con la Teoría de Información Cuántica. Se dará una breve introducción a la notación de Dirac y su aplicación en la Mecánica Cuántica (QM, por sus siglas en inglés). Una vez establecidas las bases matemáticas se describirán los postulados de la QM: Descripción del estado de un sistema, descripción de cantidades físicas, medición de cantidades físicas, colapso del estado cuántico, evolución temporal, postulado de simetrización y variables de espín. Se definirá el entrelazamiento cuántico, su importancia en el cómputo cuántico de los sistemas de dos niveles. Finalmente, explicaremos las bases de la computación cuántica y daremos una introducción a los sistemas cuánticos abiertos y el Lindbladiano.

2.1. Espacios de Hilbert

Sea \mathcal{V} un espacio vectorial, real o complejo, y consideremos una función $\|\cdot\| : \mathcal{V} \rightarrow \mathbb{R}$ que denominaremos norma si satisface los siguientes axiomas:

1. **Positividad:** La norma es una función definida positiva, es decir, para cualquier vector $\mathbf{v} \in \mathcal{V}$ se cumple que

$$\|\mathbf{v}\| \geq 0. \quad (2.1)$$

2. **Escalamiento:** Sea λ un escalar arbitrario de \mathcal{V} , es decir, un número real o complejo, según aplique. Consideremos un vector $\mathbf{v} \in \mathcal{V}$, entonces se cumple que

$$\|\lambda \mathbf{v}\| = |\lambda| \|\mathbf{v}\|. \quad (2.2)$$

3. **Desigualdad triangular:** La suma de la norma de dos vectores cualesquiera $\mathbf{v}, \mathbf{w} \in \mathcal{V}$ siempre es mayor o igual que la suma de la norma de estos, siendo igual en el caso en el caso en que estos vectores son paralelos.

$$\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|. \quad (2.3)$$

La estructura algebraica $\mathcal{N} = \{\mathcal{V}, \|\cdot\|\}$ compuesta por un espacio vectorial \mathcal{V} y una norma $\|\cdot\|$ recibe el nombre de espacio normado.

Sea \mathcal{V} un espacio vectorial complejo y la función $\langle \cdot | \cdot \rangle : \mathcal{V} \times \mathcal{V} \rightarrow \mathbb{C}$ una función sesquilineal, positiva, no degenerada y simétrica respecto a la compleja conjugada, entonces diremos que esta función define un producto escalar. La propiedad de sesquilinealidad se refiere a que el funcional $\langle \cdot | \cdot \rangle$ es antilineal en el primer argumento y lineal en el segundo. En concreto, la sesquilinealidad satisface la siguiente igualdad

$$\left\langle \sum_i \alpha_i \mathbf{v}_i \middle| \sum_j \beta_j \mathbf{w}_j \right\rangle = \sum_i \sum_j \alpha_i^* \beta_j \langle \mathbf{v}_i | \mathbf{w}_j \rangle. \quad (2.4)$$

La propiedad de positividad se refiere a que $\langle \mathbf{v} | \mathbf{v} \rangle > 0$ para cualquier $\mathbf{v} \in \mathcal{V}$ no nulo. La propiedad de no degenerado se refiere a que un único vector cumple la relación $\langle \mathbf{w} | \mathbf{w} \rangle$, el cual es el vector nulo. La propiedad de simetría ante la conjugación compleja se refiere a que el producto escalar satisface la siguiente propiedad

$$\langle \mathbf{v} | \mathbf{w} \rangle = \langle \mathbf{w} | \mathbf{v} \rangle^*. \quad (2.5)$$

La estructura algebraica $\mathcal{P} = \{\mathcal{V}, \langle \cdot | \cdot \rangle\}$ compuesta por un espacio vectorial \mathcal{V} y un producto escalar $\langle \cdot | \cdot \rangle$ recibe el nombre de espacio de pre-Hilbert. Estos espacios son considerados como casos particulares de espacios normados, ya que la norma es inducida por el producto escalar de la siguiente manera

$$\|\mathbf{v}\| = \sqrt{\langle \mathbf{v} | \mathbf{v} \rangle} \quad \forall \mathbf{v} \in \mathcal{V}. \quad (2.6)$$

Ahora introduciremos otros conceptos necesarios para definir un espacio de Hilbert:

1. **Convergencia fuerte:** Sea $\{\mathbf{v}_n\}^{n \in \mathcal{N}}$ una sucesión cualquiera en un espacio normado \mathcal{N} , diremos que dicha sucesión converge fuertemente a un vector $\mathbf{v} \in \mathcal{V}$ siempre que

$$\lim_{n \rightarrow \infty} \|\mathbf{v}_n - \mathbf{v}\| = 0. \quad (2.7)$$

2. **Convergencia débil:** Sea $\{\mathbf{v}_n\}^{n \in \mathcal{N}}$ una sucesión cualquiera en un espacio de pre-Hilbert \mathcal{P} , diremos que dicha sucesión converge débilmente a un vector $\mathbf{v} \in \mathcal{V}$ siempre que

$$\lim_{n \rightarrow \infty} \langle \mathbf{v}_n | \mathbf{w} \rangle = \langle \mathbf{v} | \mathbf{w} \rangle. \quad (2.8)$$

Resulta claro que la convergencia débil no implica la convergencia fuerte, pero la convergencia fuerte sí implica la convergencia débil.

El ordenamiento de una sucesión puede ser un factor determinante para su convergencia. Las sucesiones de Cauchy son aquellas en las que el ordenamiento no afecta la convergencia. Es decir, son aquellas sucesiones que cumplen que

$$\lim_{n, m \rightarrow \infty} \|\mathbf{v}_n - \mathbf{v}_m\| = 0. \quad (2.9)$$

Todas las sucesiones fuertemente convergentes son de Cauchy, sin embargo, en general, lo recíproco no es cierto. La razón es que en algunas sucesiones en \mathcal{N} convergen a un vector que no pertenece a \mathcal{N} . Un espacio normado es completo si toda sucesión de Cauchy converge fuertemente en él. Todo espacio normado \mathcal{N} y completo recibe el nombre de espacio de Banach \mathcal{B} , y todo espacio de pre-Hilbert \mathcal{P} y completo recibe el nombre de espacio de Hilbert \mathcal{H} .

Finalmente, un espacio de Hilbert separable es aquel cuya base puede ser generado por una base contable. Una base contable es una base con la cardinalidad de algún subconjunto de los números naturales. En otras palabras, es una base cuyos elementos se pueden contar o enumerar. Esto implica que una base contable debe ser finita o infinita discreta.

2.2. Operadores lineales

Sea \mathcal{H} un espacio de Hilbert. Un operador $A : \mathcal{H} \rightarrow \mathcal{H}$ es lineal si para todo par de vectores $\mathbf{v}, \mathbf{w} \in \mathcal{H}$ y para un escalar α , se cumple que

$$A(\mathbf{v} + \mathbf{w}) = A\mathbf{v} + A\mathbf{w} \quad (2.10)$$

$$A(\alpha\mathbf{v}) = \alpha A\mathbf{v}. \quad (2.11)$$

En QM se utiliza extensamente el operador adjunto A^\dagger de operadores lineales A . En la representación matricial $[A_{ij}]$, el operador adjunto A^\dagger corresponde a la transpuesta conjugada, es decir:

$$A^\dagger = ([A_{ij}]^T)^* = [A_{ji}^*], \quad (2.12)$$

Donde A_{ji}^* representa el complejo conjugado de cada una de las entradas de la matriz y $[A_{ij}]^T$ representa la transpuesta de la matriz.

2.3. Delta de Kronecker

La delta de Kronecker δ_{ij} es un símbolo que representa dos posibles valores, dependiendo de sus subíndices,

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases} \quad (2.13)$$

Dado que el símbolo sólo es diferente de cero cuando sus índices son iguales, las sumas que incluyen la delta de Kronecker pueden ser simplificadas fácilmente.

$$\sum_j \delta_{ij} B_j = 0B_1 + 0B_2 + \dots + 1B_i + \dots = B_i. \quad (2.14)$$

La delta de Kronecker también es importante porque el operador identidad, en su representación matricial, tiene como elementos la delta de Kronecker. Esto es $\mathbb{1} = [\delta_{ij}]$.

2.4. Operadores hermíticos

En espacios de dimensión finita, a un operador se le llama hermítico o autoadjunto cuando su adjunto coincide con el operador. Es decir, los operadores hermíticos H son operadores tales que

$$H = H^\dagger. \quad (2.15)$$

Estos operadores cumplen con la propiedad de que todos sus autovalores son reales, y sus autovectores son ortogonales. En la representación matricial, los operadores hermíticos corresponden a matrices cuadradas cuyos elementos de la diagonal son reales, y los términos por debajo de la diagonal son el conjugado complejo de los términos por encima de la diagonal. Todo operador hermítico puede ser diagonalizado mediante un operador unitario, por medio de la siguiente operación:

$$H_d = U^\dagger H U. \quad (2.16)$$

2.5. Operadores unitarios

Las transformaciones lineales que mantienen invariante al producto escalar en \mathcal{H} son llamadas operadores unitarios. En consecuencia de esto, un operador unitario U es un operador tal que

$$U U^\dagger = U^\dagger U = \mathbb{1}. \quad (2.17)$$

Es decir, un operador unitario U es aquel cuya inversa es igual a su operador adjunto. Los operadores unitarios tienen determinantes de módulo igual a la unidad. El conjunto de todos los operadores unitarios junto con la operación de multiplicación de matrices forman un grupo, llamado grupo unitario; denotado $U(n)$, donde n es la dimensión del espacio donde operan. Aquellas transformaciones unitarias, cuyo determinante sea real y positivo, forman un subgrupo llamado grupo de transformaciones unitarias especiales; denotado como $SU(n)$, donde n es la dimensión del espacio donde operan. Los operadores unitarios pueden ser escritos en función de operadores hermíticos, de la siguiente manera:

$$U = e^{iH}, \quad (2.18)$$

Donde U es un operador unitario y H es un operador hermítico. Los operadores unitarios, además, preservan la traza y la norma. Es decir:

$$\|U\mathbf{v}\| = \|\mathbf{v}\| \quad (2.19)$$

$$Tr(UA) = Tr(A). \quad (2.20)$$

Todo operador unitario puede ser diagonalizado con otro operador unitario.

$$U_d = V^\dagger U V. \quad (2.21)$$

2.6. Conmutador y anticonmutador

Estas son operaciones comunes en la QM y revelan propiedades importantes del álgebra de los operadores involucrados. Sean dos operadores A y B , entonces el producto de estos operadores puede ser escrito como

$$AB = \frac{1}{2}(AB + BA) + \frac{1}{2}(AB - BA) = \frac{1}{2}\{A, B\} + \frac{1}{2}[A, B], \quad (2.22)$$

$$BA = \frac{1}{2}(AB + BA) - \frac{1}{2}(AB - BA) = \frac{1}{2}\{A, B\} - \frac{1}{2}[A, B], \quad (2.23)$$

Donde hemos definido el conmutador $[A, B] = AB - BA$ y el anticonmutador $\{A, B\} = AB + BA$.

Si $[A, B] = 0$, se dice que A y B conmutan entre sí, pues $AB = BA$. Si dos operadores conmutan, ellos realizarán la misma transformación compuesta sin importar el orden en que se apliquen. De igual manera, si $\{A, B\} = 0$, se dice que anticonmutan, ya que $AB = -BA$. Si dos operadores anticonmutan, invertir el orden en el que se aplican introduce una fase de π .

$$[A, B] = 0 \implies AB = BA, \quad (2.24)$$

$$\{A, B\} = 0 \implies AB = -BA = e^{i\pi} BA. \quad (2.25)$$

Como ejemplo, en primer lugar, de la importancia del conmutador, consideremos la transformación $\mathcal{E}_U(H) = UHU^\dagger$, donde U es un operador unitario y H es un operador lineal tal que $[H, U] = 0$, resulta que

$$\mathcal{E}_U(H) = UHU^\dagger = HUU^\dagger = H\mathbf{1} = H. \quad (2.26)$$

Es decir, H es simétrico o invariante con respecto a $\mathcal{E}_U(H)$.

En segundo lugar, como ejemplo de la importancia del anticonmutador, consideremos la misma transformación, pero un operador H tal que $\{H, U\} = 0$, entonces

$$\mathcal{E}_U(H) = UHU^\dagger = -HUU^\dagger = -H\mathbf{1} = -H. \quad (2.27)$$

Es decir, H es antisimétrico con respecto a $\mathcal{E}_U(H)$. En otras palabras, $\mathcal{E}_U(H)$ invierte la fase de H .

2.7. Estados cuánticos

Un sistema físico es aquel que consta de fuentes y campos que interactúan entre sí, y a partir del cual será posible extraer o transmitir algún tipo de información. Aquellas propiedades de un sistema físico que sean susceptibles a la medida reciben el nombre de observables o magnitudes físicas. No todas las propiedades de un sistema físico son independientes, unas se pueden describir en función de las otras y el conjunto minimal de observables necesarios para describir todas las propiedades del sistema se conoce como conjunto irreducible de observables (CIO) u observables fundamentales (OF). El conjunto de medidas realizadas sobre el CIO puede ser representado como coordenadas de un espacio vectorial, al cual llamaremos espacio de estado; de manera que los estados del sistema serán caracterizados a partir de puntos en dicho espacio.

En la QM, a todo sistema físico se le hace corresponder un espacio de Hilbert \mathcal{H} , complejo y separable. A cada observable \mathcal{A} del sistema le corresponde un operador hermítico \hat{A} , cuyos autovalores son los valores que pueden resultar de una medida de \mathcal{A} . No todos los operadores hermíticos corresponden a un observable, pero el recíproco sí es cierto. En particular, es de interés el Hamiltoniano \hat{H} , el cual es el operador asociado a la energía del sistema.

La notación bra-ket es la notación estándar en la QM para describir estados cuánticos. Un ket $|\psi\rangle$ representa un vector único asociado al estado ψ . En la representación matricial, un ket es un vector columna unitario. Un uso de los kets $|i\rangle$ es representar vectores con una única entrada no nula e igual a 1, en la posición $i + 1$. En el caso de la computación cuántica, se utilizan los kets $|0\rangle$ y $|1\rangle$ para describir los qubits en la base computacional. Este par de estados sería el equivalente a los bits 0 y 1 en la computación clásica. En su representación matricial, los kets $|0\rangle$ y $|1\rangle$ se representan de la siguiente manera:

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

Un bra es transpuesto conjugado, es decir, el adjunto, de un ket. Los bras de la base computacional son $\langle 0|$ y $\langle 1|$. En la representación matricial estos son la transpuesta conjugada de los kets y se representan de la siguiente manera:

$$\langle 0| = |0\rangle^\dagger = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = |1\rangle^\dagger = \begin{pmatrix} 0 & 1 \end{pmatrix}.$$

El producto interno de dos kets es el producto de un bra seguido de un ket, denotado como $\langle\phi|\psi\rangle$. El resultado de este producto es un número complejo y cumple las siguientes propiedades:

$$\langle\phi|\psi\rangle = z \tag{2.28}$$

$$(\langle\phi|\psi\rangle)^\dagger = \langle\psi|\phi\rangle = z^*. \tag{2.29}$$

El producto externo, o producto diádico, es el producto de un ket seguido de un bra $|\phi\rangle\langle\psi|$. El resultado es un proyector que toma la componente en $|\psi\rangle$ de un estado cuántico y la convierte en $|\phi\rangle$. Ejemplos:

$$\begin{aligned}
|0\rangle\langle 0| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \\
|0\rangle\langle 1| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \\
|1\rangle\langle 0| &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \\
|1\rangle\langle 1| &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Para un estado genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, se tiene que

$$\begin{aligned}
\Pi = |\psi\rangle\langle\psi| &= (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \\
&= |\alpha|^2|0\rangle\langle 0| + \alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|.
\end{aligned}$$

Este producto exterior se conoce como proyector y cumple con las siguientes propiedades:

$$\Pi^2 = |\psi\rangle\langle\psi| |\psi\rangle\langle\psi| = 1 |\psi\rangle\langle\psi| = \Pi \quad (2.30)$$

$$\Pi^\dagger = (|\psi\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\psi| = \Pi. \quad (2.31)$$

La notación de Dirac se relaciona con el formalismo de funciones de onda de la siguiente manera:

$$\psi(x, t) = \langle x | \psi(t) \rangle, \quad (2.32)$$

Donde $\langle x|$ es el bra del ket asociado a la variable posición.

Los ensambles estadísticas de estados cuánticos también son estados cuánticos. Esto nos lleva a distinguir entre estados puros y estados mixtos o mezcla. Los estados puros son los que podemos representar en la notación de bra-kets de Dirac, mientras que los estados mezcla se suelen representar en la notación de matrices

u operadores densidad. Un estado puro, descrito por un ket $|\psi\rangle$, tiene la siguiente matriz densidad:

$$\rho = |\psi\rangle\langle\psi|. \quad (2.33)$$

Por otro lado, si tenemos un ensamble $\{|\psi_i\rangle\}$, el estado mixto tiene la siguiente matriz densidad:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad (2.34)$$

Donde p_i es la probabilidad asociada a cada estado puro de la mezcla y $\sum_i p_i = 1$.

Las matrices densidad tienen las siguientes propiedades:

1. Traza igual a uno: $Tr(\rho) = 1$
2. Hermíticas: $\rho^\dagger = \rho$
3. Autovalores no negativos: $\rho|\lambda_i\rangle = \lambda_i|\lambda_i\rangle, \quad \lambda_i \geq 0$

Las matrices densidad asociadas a un estado puro, o mixto, se pueden identificar con la traza del cuadrado de la matriz densidad:

1. Estado puro: $Tr(\rho^2) = 1$
2. Estado mixto $Tr(\rho^2) < 1$

En una matriz densidad, los elementos de la diagonal son las poblaciones y los elementos fuera de ésta son las transiciones. Las poblaciones representan la probabilidades de que el sistema se encuentre en cada estado de la base tras una medida, mientras que las transiciones hacen referencia a la coherencia cuántica entre los elementos de la base que conforman el estado. Por ejemplo, el estado con superposición cuántica: $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ tiene la siguiente matriz densidad:

$$\rho_1 = |\psi\rangle\langle\psi| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}. \quad (2.35)$$

Mientras que el estado de mezcla clásica $\rho = (\rho_0 + \rho_1)/2$ tiene la siguiente matriz de probabilidad:

$$\rho_2 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \quad (2.36)$$

Como se puede ver, ambos estados tienen probabilidad $1/2$ de encontrarse en $|0\rangle$ o en $|1\rangle$ que son los estados de la base. Sin embargo, en el primer estado, esto se debe a que es un único estado cuántico con superposición coherente. Mientras que en el segundo estado esto se debe a que es un estado mezcla de dos estados cuánticos, es decoherente. Este es un buen momento para notar la diferencia entre un estado mixto y estado coherente, pues un estado mezcla también puede ser coherente.

Tomemos los mismos estados ρ_1 y ρ_2 anteriores y construyamos el estado

$$\rho = \frac{1}{2}(\rho_1 + \rho_2) = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix}. \quad (2.37)$$

Este es un estado mezcla, pero aún así tiene elementos fuera de la diagonal, los cuales indican coherencia. Es decir, este estado tiene componente de superposición cuántica, además de la mezcla clásica.

La evolución de los estados puros está dada por la ecuación de Schrödinger

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle, \quad (2.38)$$

Donde i es la unidad imaginaria $\sqrt{-1}$, \hbar es la constante de Planck reducida $h/2\pi$ y \hat{H} es el Hamiltoniano del sistema. La generalización de la ecuación de Schrödinger para estados puros y mixtos es la ecuación de Liouville-von Neumann.

$$i\hbar \dot{\rho}(t) = [\hat{H}, \rho(t)]. \quad (2.39)$$

La QM es una teoría probabilística. Los vectores de estado se construyen con amplitudes complejas de probabilidad asociadas a cada elemento de la base del espacio de Hilbert \mathcal{H} , y las matrices densidad a partir de probabilidades asociadas a cada estado que compone la mezcla. En la QM, una partícula puede encontrarse en cualquier parte del universo, en cualquier momento con, con cualquier energía, de

acuerdo a cierta distribución de probabilidad. Sea $|u\rangle$ un autoestado del operador hermítico, asociado a un observable \mathcal{A} . Entonces, la función de distribución de probabilidad de \mathcal{A} asociada al estado $|\psi\rangle$ es la siguiente:

$$f_{\mathcal{A}}(u) = |\langle u|\psi\rangle|^2. \quad (2.40)$$

Esto es, el módulo al cuadrado de la proyección de $|\psi\rangle$ en $|u\rangle$. De hecho, debido a esto es que los estados cuánticos deben estar normalizados.

$$|\langle\psi|\psi\rangle|^2 = 1 \quad (2.41)$$

$$\sum |\langle\psi_i|\psi\rangle|^2 = 1, \quad (2.42)$$

Donde la suma es sobre los estados de alguna base de \mathcal{H} . En los formalismos de matriz de densidad y de función de onda, la normalización se escribe de las siguientes maneras:

$$Tr(\rho) = 1 \quad (2.43)$$

$$\int_S |\psi(r, t)|^2 d^3r = 1. \quad (2.44)$$

El valor esperado $\langle\mathcal{A}\rangle$ del mismo observable \mathcal{A} , en función del ket, la base de \mathcal{H} , la matriz densidad y la función de onda, es el siguiente:

$$\langle\mathcal{A}\rangle = \langle\psi|\hat{A}|\psi\rangle \quad (2.45)$$

$$\langle\mathcal{A}\rangle = \sum_i \langle\psi_i|\hat{A}|\psi_i\rangle \quad (2.46)$$

$$\langle\mathcal{A}\rangle = Tr(\hat{A}\rho). \quad (2.47)$$

2.8. Sistemas multipartitos

Cuando un sistema compuesto por dos (o más) espacios de Hilbert, \mathcal{H}_A y \mathcal{H}_B , el espacio del sistema completo se escribe en función del producto tensorial $\mathcal{H} =$

$\mathcal{H}_A \otimes \mathcal{H}_B$. Aquí, \mathcal{H}_A y \mathcal{H}_B se conocen como las particiones de \mathcal{H} . De igual manera, para representar un estado de \mathcal{H} en un ket, en lugar de dos, se realiza el producto tensorial $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. También se pueden agregar subíndices a los kets para hacer énfasis en las particiones:

$$\begin{aligned} |\psi\rangle & \in \mathcal{H} \\ |\psi\rangle_A \otimes |\phi\rangle_B & \in \mathcal{H}_A \otimes \mathcal{H}_B \\ |\psi_1\rangle_1 \otimes |\psi_2\rangle_2 \otimes \dots \otimes |\psi_n\rangle_n & \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n \end{aligned} \quad (2.48)$$

En la representación matricial el producto tensorial se realiza de la siguiente manera:

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

El producto tensorial tiene las siguientes propiedades:

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1 |\psi_1\rangle) \otimes (U_2 |\psi_2\rangle) \quad (2.49)$$

$$|\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi_2\rangle \otimes |\psi_1\rangle \quad (2.50)$$

$$\alpha(|\psi_1\rangle \otimes |\psi_2\rangle) = (\alpha |\psi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes (\alpha |\psi_2\rangle) \quad (2.51)$$

$$(|\psi_1\rangle \otimes |\psi_2\rangle)^\dagger = \langle \psi_1 | \otimes \langle \psi_2 |. \quad (2.52)$$

En el caso de los bras y los kets, el producto tensorial también se puede escribir de la forma $|\psi\phi\rangle$, en lugar de $|\psi\rangle \otimes |\phi\rangle$.

$$|\psi\rangle_A \otimes |\phi\rangle_B = |\psi\rangle \otimes |\phi\rangle = |\psi_A \phi_B\rangle = |\psi\phi\rangle. \quad (2.53)$$

Ejemplos:

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

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

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

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

$$\mathbb{1} \otimes \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La operación inversa del producto tensorial, para obtener \mathcal{H}_A o \mathcal{H}_B a partir de \mathcal{H} , es la traza parcial.

La traza parcial se define de la siguiente manera:

$$Tr_A(\rho_{AB}) = \sum_i ({}_A\langle i| \otimes \mathbb{1}_B) \rho(|i\rangle_A \otimes \mathbb{1}_B). \quad (2.54)$$

Esta traza elimina la porción de ρ_{AB} perteneciente a \mathcal{H}_A . Si pudiesemos escribir $\rho_{AB} = \rho_A \otimes \rho_B$, entonces $Tr_A(\rho_{AB}) = \rho_B$

En caso que se quiera tener ρ_A en lugar de ρ_B , entonces tenemos que tomar la traza parcial de la partición B, en lugar de la partición A, de la siguiente manera:

$$Tr_B(\rho_{AB}) = \sum_i (\mathbb{1}_A \otimes {}_B\langle i|) \rho(\mathbb{1}_A \otimes |i\rangle_B). \quad (2.55)$$

Para entender mejor la traza parcial, recordemos la definición de la traza normal:

$$\text{Tr}(\rho) = \sum_i \langle i | \rho | i \rangle. \quad (2.56)$$

El par $\langle i | i \rangle$ lo que hace es seleccionar el i -ésimo elemento de la diagonal de la matriz ρ , entonces es la suma de todas las poblaciones en cada estado $|i\rangle$ de la base de \mathcal{H} y mapea este espacio de Hilbert a uno escalar (en el caso de las matrices densidad, las mapea al número 1, por la normalización de las probabilidades). La traza parcial hace algo similar, solo que se aplica sobre la información de las particiones de \mathcal{H}_A o de \mathcal{H}_B , dejando a la otra partición intacta. Es decir, el efecto de la traza y de las trazas parciales sobre una matriz densidad es, en resumen, el siguiente:

1. $\text{Tr}(\rho_{AB}) = 1$, donde $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$
2. $\text{Tr}_A(\rho_{AB}) = \rho_B$, donde $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ y $\rho_B \in \mathcal{H}_B$
3. $\text{Tr}_B(\rho_{AB}) = \rho_A$, donde $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ y $\rho_A \in \mathcal{H}_A$

Finalmente, comparemos algunos de los aspectos del producto tensorial y de la traza parcial.

1. El producto tensorial se puede realizar con kets o con matrices densidad. Pero la traza parcial sólo se puede aplicar a matrices densidad.
2. El producto tensorial de dos estados puros es otro estado puro. Sin embargo, las trazas parciales de un estado puro no necesariamente son estados puros. En la próxima sección se explicará más al respecto.

2.9. Postulados de la mecánica cuántica

La QM que fundamenta la teoría de información cuántica se describe formalmente con los siguientes postulados desarrollados por la escuela de Copenhague a lo largo de todo el siglo XX [43].

1. La descripción de un sistema físico en QM está dada en términos de los elementos de un espacio de Hilbert complejo separable asociado al sistema físico. En cada instante de tiempo t , un estado puro del sistema se representa por el vector unitario $|\psi(t)\rangle$ en el espacio de Hilbert correspondiente. Tal vector se llama vector de estado o ket.

2. Todo observable de un sistema físico está representado en el formalismo de QM por un operador lineal hermítico el cual actúa en el espacio de Hilbert asociado con el sistema físico en consideración.
3. Si un sistema físico está en un estado descrito por un vector normalizado $|\psi\rangle$ o una matriz densidad ρ , la probabilidad de obtener un valor λ al medir un observable \mathcal{A} está dada por

$$p(\lambda) = \sum_i^{g_n} |\langle \lambda_i | \psi \rangle|^2 \quad (2.57)$$

$$p(\lambda) = \text{Tr}(\Pi_\lambda \rho), \quad (2.58)$$

Donde g_n es el grado de degeneración de \hat{A} en λ , es decir, la cantidad de autoestados asociados a este mismo autovalor, $|\lambda_i\rangle$ son los autoestados asociados a λ y el proyector Π_λ es $\Pi_\lambda = \sum_i^{g_n} |\lambda_i\rangle\langle\lambda_i|$.

4. Si un sistema físico está en el estado $|\psi\rangle$ o ρ , el estado resultante luego de una medida ideal del observable \mathcal{A} está dado por

$$|\psi\rangle \rightarrow \frac{\Pi_\lambda |\psi\rangle}{\sqrt{\langle\psi| \Pi_\lambda |\psi\rangle}} \quad (2.59)$$

$$p(\lambda) \rightarrow \frac{\mathcal{E}_\lambda(\rho)}{\text{Tr}(\Pi_\lambda \rho)}, \quad (2.60)$$

Donde el mapa $\mathcal{E}_\lambda(\rho) = \sum_i^{g_n} |\lambda_i\rangle\langle\lambda_i| \rho |\lambda_i\rangle\langle\lambda_i|$.

5. En un intervalo de tiempo entre dos medidas consecutivas, los estados puros de un sistema continúan siendo puros, y existen kets $|\psi(t)\rangle$ tales que la evolución del estado del sistema está dada por la ecuación de Schrödinger

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H}(t) |\psi(t)\rangle, \quad (2.61)$$

Donde $\hat{H}(t)$ es un observable llamado Hamiltoniano, el cual representa la energía del sistema. Los observables del sistema se representan por operadores que son constantes en el tiempo, a menos que los dispositivos de medida cambien en el tiempo, en tal caso, los operadores deberán contener dichos cambios.

6. Para un sistema físico en el cual las coordenadas cartesianas son q_1, q_2, \dots, q_N , con los correspondientes momenta conjugados p_1, p_2, \dots, p_N , los operadores X y P , los cuales representan estos observables en QM, deben satisfacer las relaciones de conmutación

$$[X_r, X_a] = 0, [P_r, P_a] = 0, [X_r, P_a] = i\hbar\delta_{ra}. \quad (2.62)$$

Si el sistema tiene un observable cuya expresión clásica es $A(q_1, \dots, q_N, p_1, \dots, p_N; t)$, la aplicación usual en QM del operador correspondiente se obtiene sustituyendo las variables q_r y p_a por los operadores X_r y P_a , respectivamente.

2.10. Entrelazamiento

Consideremos el estado $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ e intentemos escribirlo en función de $|\psi_1\rangle$ y $|\psi_2\rangle$, tal que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

$$\begin{aligned} |\psi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle. \end{aligned}$$

De aquí se debe cumplir que:

$$\alpha\gamma = \frac{1}{\sqrt{2}} \quad \alpha\delta = 0 \quad \beta\gamma = 0 \quad \beta\delta = \frac{1}{\sqrt{2}}$$

Pero esto implicaría, al mismo tiempo que:

1. Al menos una variable de cada uno de los siguientes pares de variables es cero: $\{\alpha, \delta\}$ y $\{\beta, \gamma\}$
2. Ninguna de las siguientes variables es cero: $\alpha, \beta, \gamma, \delta$

Lo cual resulta contradictorio y se concluye que existen estados no separables. Veamos qué significa esto en términos de la distribución de probabilidades:

	$ \psi\rangle_A = 0\rangle$	$ \psi\rangle_A = 1\rangle$	$P(A)$
$ \psi\rangle_B = 0\rangle$	1/2	0	1/2
$ \psi\rangle_B = 1\rangle$	0	1/2	1/2
$P(B)$	1/2	1/2	

De esta tabla se puede ver que las particiones A y B no son independientes, pues las probabilidades condicionadas no son el producto de las probabilidades sin condicionar $P(A|B) \neq P(A)P(B)$. Es decir, existe una correlación.

A la correlación que causa la inseparabilidad de los sistemas se le conoce como entrelazamiento y es la correlación cuántica que va más allá de la interacción espacial.

Si se toma la traza parcial de un estado entrelazado puro, el resultado es un estado mixto, como consecuencia de la inseparabilidad de los estados entrelazados.

De aquí surge la siguiente clasificación de los estados cuánticos:

1. Estado producto: $\rho = \rho_A \otimes \rho_B$
2. Estado separable: $\rho = \sum_{ij} p_{ij}(\rho_{A_i} \otimes \rho_{B_j})$
3. Estado entrelazado: $\rho \neq \sum_{ij} p_{ij}(\rho_{A_i} \otimes \rho_{B_j})$

Además, también tenemos la siguiente clasificación de estados en función de la coherencia cuántica:

1. Estado cuántico-cuántico: $\rho = \rho_{AB}$
2. Estado clásico-cuántico: $\rho = \sum_i p_i |i\rangle\langle i| \otimes \rho_B$
3. Estado clásico-clásico: $\rho = \sum_{ij} p_{ij}(|i\rangle\langle i| \otimes |j\rangle\langle j|)$

2.11. Qubits

Un qubit es un sistema físico de dos niveles, es decir, es un objeto cuyo estado es un elemento del espacio de Hilbert de dimensión $\dim(\mathcal{H}) = 2$ y puede ser escrito de la siguiente manera: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde $\{|0\rangle, |1\rangle\}$ forma una base de \mathcal{H}

y donde α y β son números complejos, tales que $|\alpha|^2 + |\beta|^2 = 1$, conocidos como amplitudes de probabilidad.

El qubit se puede pensar como el equivalente en IC del bit, el cual, por sus propiedad cuánticas, puede estar no sólo puede estar en el estado $|0\rangle$ y en el estado $|1\rangle$, sino también en superposiciones de estos dos.

2.12. Esfera de Bloch

El estado de un qubit también se puede escribir de la siguiente manera: $|\psi\rangle = e^{i\phi_0} \cos(\theta) |0\rangle + e^{i\phi_1} \sin(\theta) |1\rangle = e^{i\phi_0} (\cos(\theta) |0\rangle + e^{i(\phi_1 - \phi_0)} \sin(\theta) |1\rangle)$, donde θ , ϕ_0 y ϕ_1 son números reales. La fase global ϕ_0 es ignorable, pues no tiene ningún efecto sobre las probabilidades. Entonces, sin pérdida de generalidad, $|\psi\rangle = \cos(\theta) |0\rangle + \sin(\theta) e^{i\phi} |1\rangle$, donde $\theta \in [0, \pi]$ y $\phi \in [0, 2\pi]$. De esta manera, podemos representar los qubits en una esfera unitaria, conocida como esfera de Bloch. En esta esfera el ket $|0\rangle$ corresponde al vector $(0,0,1)$, mientras que el ket $|1\rangle$ corresponde al vector $(0,0,-1)$.

Todas las operaciones de un qubit se pueden ver como rotaciones en la esfera de Bloch. Por ejemplo, un *bit-flip* sería una rotación de π sobre el eje X, tal que $(0, 0, 1) \rightarrow (0, 0, -1)$, es decir $|0\rangle \rightarrow |1\rangle$.

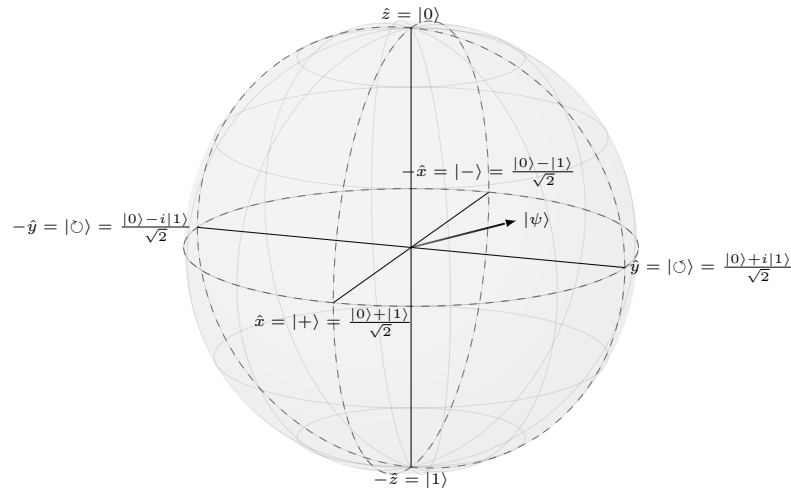


FIGURA 2.1: Esfera de Bloch

2.13. Matrices de Pauli

Estas matrices son de especial importancia en la QM y representan el spin de una partícula. Ellas son:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2.63)$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (2.64)$$

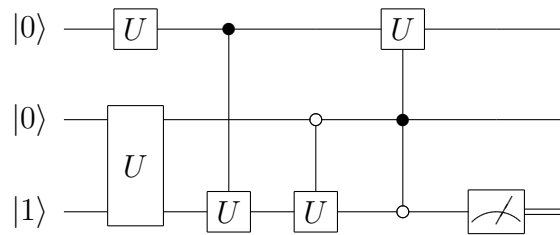
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.65)$$

Las matrices de Pauli cumplen las siguientes propiedades:

1. Autovalores ± 1
2. Hermiticas
3. $[\sigma_i, \sigma_j] = i\sigma_k$, donde $(i, j) \in \{(x, y), (y, z), (z, x)\}$
4. $[\sigma_j, \sigma_i] = -i\sigma_k$, donde $(i, j) \in \{(x, y), (y, z), (z, x)\}$

2.14. Circuitos cuánticos

El equivalente a los circuitos digitales en la computación cuántica es los circuitos cuánticos. Ellos describen la secuencia de operaciones que se deben aplicar a los qubits para ejecutar cierto algoritmo. Esas operaciones pueden ser transformaciones unitarias, conocidas como compuertas cuánticas, o medidas proyectivas. Es importante resaltar que estos circuitos no representan componentes tangibles, sino componentes de información. De esta manera, las compuertas cuánticas no son componentes electrónicos de ninguna manera, sólo representan las transformaciones que se aplican a los qubits. En este sentido, los circuitos cuánticos son más el análogo del lenguaje de máquina que de los circuitos digitales. En general, las compuertas cuánticas se implementan con distintos tipo de ondas y pulsos electromagnéticos.



En esta figura se observan los siguientes elementos:

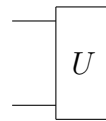
1. Estado inicial: Este es el estado con el que se inicia el algoritmo.

$$|\psi\rangle$$

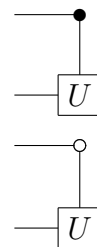
2. Compuerta de un qubit: Representa una operación unitaria sobre el qubit en cuya línea se encuentra.



3. Compuerta multiqubit: Representa una operación unitaria sobre los qubits en cuyas líneas se encuentra.

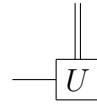


4. Compuerta condicionada cuánticamente: El punto blanco o negro indica que el qubit de esa línea es el qubit de control. Si el punto es blanco, se aplica la compuerta U si el qubit de control es $|0\rangle$. Si el punto es negro, se aplica la compuerta U si el qubit de control es $|1\rangle$. Es caso de que el qubit de control se encuentre en estado de superposición, la compuerta se aplica y no se aplica, simultáneamente.



5. Compuerta condicionada clásicamente: Equivalente a un if de cualquier lenguaje de programación clásica. Sólo se aplica la compuerta U si el bit de

control es 1.



6. Medida proyectiva: Representa una medida proyectiva del qubit en cuya línea se encuentra.



7. Cable cuántico: No es un cable físico, sólo lleva ese nombre en analogía a los circuitos clásicos, donde las compuertas sí son componentes electrónicos en conexión. En el caso de los circuitos cuánticos, este elemento sólo representa que se mantiene la coherencia del qubit y que no se aplica ninguna compuerta sobre él en ese paso del algoritmo.



8. Cable clásico: Representa el bit clásico que se obtiene tras la medida de un qubit.



Las compuertas cuánticas difieren de las compuertas clásicas en que las primeras son reversibles. Esto implica que una compuerta cuántica siempre tiene la misma cantidad de entradas que de salidas y que conociendo la compuerta y la salida, se puede conocer inequívocamente la entrada. Este no es el caso con las compuertas clásicas. Por ejemplo, una compuerta AND tiene dos entradas, pero una sólo salida y no hay manera de conocer la entrada si la salida es 0. De hecho, incluso si se extiende la compuerta AND para incluir una de las entradas como una segunda salida, de manera de tener la misma cantidad de salidas que de entradas, como es el caso con las compuertas cuánticas, sigue siendo imposible conocer la otra entrada si ambas salidas son 0.

Otra diferencia está en la variedad de compuertas que pueden existir. Como ejemplo, consideremos las compuertas de una entrada y una salida. En el caso clásico, sólo existen dos compuertas: el buffer y el NOT. Mientras que en el caso cuántico, existen infinitas compuertas de un qubit, pues cualquier elemento de $SU(2)$ puede ser una compuerta.

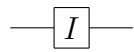
2.15. Puertas cuánticas de un qubit

Las operaciones unitarias con las que se opera sobre los qubits reciben el nombre de puertas cuánticas.

Las puertas de un sólo qubit pueden ser vistas como rotaciones en la esfera de Bloch.

2.15.1. Puerta identidad

Esta operación es equivalente a *no-operation* en una computadora clásica.



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

Entrada	Salida
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$ 1\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$\alpha 0\rangle + \beta 1\rangle$

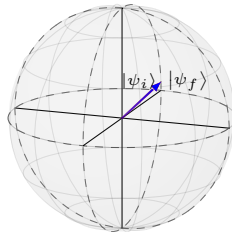
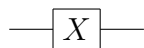


FIGURA 2.2: Puerta I en la esfera de Bloch

2.15.2. Puerta X

Este es el equivalente al NOT clásico, pues transforma los $|0\rangle$ en $|1\rangle$ y viceversa, ya que realiza una rotación de π sobre el eje X en la esfera de Bloch. Su forma matricial viene dada por la matriz de Pauli σ_x



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

Entrada	Salida
$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$\beta 0\rangle + \alpha 1\rangle$

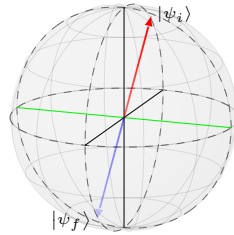
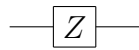


FIGURA 2.3: Compuerta X en la esfera de Bloch

2.15.3. Compuerta Z

Esta compuerta no tiene análogo clásico, pues lo que realiza es un cambio de fase de π . Esto equivale a una rotación de π sobre el eje Z en la esfera de Bloch. Su forma matricial viene dada por la matriz de Pauli σ_z



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

Entrada	Salida
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$- 1\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$\alpha 0\rangle - \beta 1\rangle$

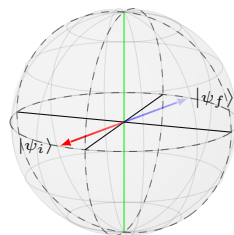


FIGURA 2.4: Compuerta Z en la esfera de Bloch

2.15.4. Compuerta Y

Esta compuerta realiza una rotación de π sobre el eje y de la esfera de Bloch. Distintos autores definen la forma matricial de esta compuerta de dos maneras distintas, una forma viene dada por la matriz de Pauli σ_y y otra es esta matriz por una fase global de i .

$$\text{---} \boxed{Y} \text{---} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ ó } Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Entrada	Salida
$ 0\rangle$	$i 1\rangle$ ó $- 1\rangle$
$ 1\rangle$	$-i 0\rangle$ ó $ 0\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$-i\beta 0\rangle + i\alpha 1\rangle$ ó $\beta 0\rangle - \alpha 1\rangle$

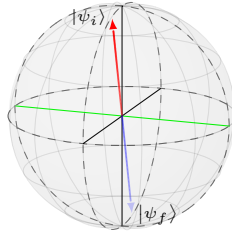


FIGURA 2.5: Compuerta Y en la esfera de Bloch

2.15.5. Compuerta de Hadamard

Esta compuerta transforma los estados de la base computacional $|0\rangle$ y $|1\rangle$ en estados de superposiciones uniformes $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ y $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. También se puede interpretar como el mapa de la base Z a la base X. Ella consiste de una rotación de π sobre el eje $(x+z)$ y se puede realizar con una rotación de $\pi/2$ sobre el eje Y seguida de la compuerta X.

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

Entrada	Salida
$ 0\rangle$	$\frac{ 0\rangle + 1\rangle}{\sqrt{2}}$
$ 1\rangle$	$\frac{ 0\rangle - 1\rangle}{\sqrt{2}}$
$\alpha 0\rangle + \beta 1\rangle$	$\frac{\alpha + \beta}{\sqrt{2}} 0\rangle + \frac{\alpha - \beta}{\sqrt{2}} 1\rangle$

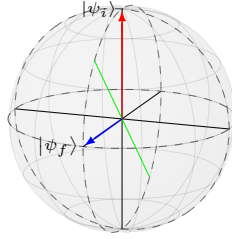


FIGURA 2.6: Compuerta H en la esfera de Bloch

2.15.6. Compuerta S

Esta compuerta es la raíz cuadrada de Z e introduce una fase de $\pi/2$ al qubit.

$$\text{---} \boxed{S} \text{---} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Entrada	Salida
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$i 1\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$\alpha 0\rangle + i\beta 1\rangle$

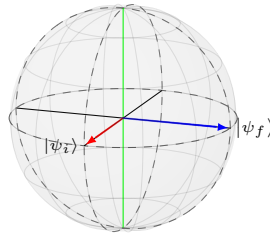


FIGURA 2.7: Compuerta S en la esfera de Bloch

2.15.7. Compuerta T

Esta compuerta es la raíz cuadrada de S e introduce una fase de $\pi/4$ al qubit.

$$\text{---} \boxed{T} \text{---} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$$

Entrada	Salida
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$e^{\frac{i\pi}{4}} 1\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$\alpha 0\rangle + e^{\frac{i\pi}{4}} \beta 1\rangle$

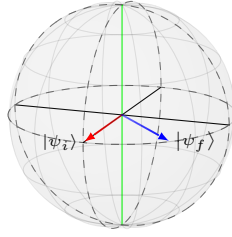


FIGURA 2.8: Compuerta T en la esfera de Bloch

2.15.8. Compuerta de cambio de fase

Esta compuerta es similar a Z, S y T, sólo que introduce una fase ϕ cualquiera al qubit.

$$\text{---} \boxed{P_\phi} \text{---} \quad P_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Entrada	Salida
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$e^{i\phi} 1\rangle$
$\alpha 0\rangle + \beta 1\rangle$	$\alpha 0\rangle + e^{i\phi} \beta 1\rangle$

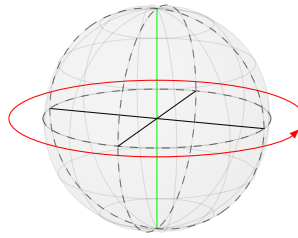


FIGURA 2.9: Compuerta P en la esfera de Bloch

2.15.9. Compuertas de rotación

Una rotación general en la esfera de Bloch se escribe de la siguiente manera:

$$R(\theta, \hat{r}) = e^{i\frac{\theta}{2}\vec{\sigma}\cdot\hat{r}} = \begin{pmatrix} \cos(\frac{\theta}{2}) + iz \sin(\frac{\theta}{2}) & \sin(\frac{\theta}{2})(ix + y) \\ \sin(\frac{\theta}{2})(ix - y) & \cos(\frac{\theta}{2}) - iz \sin(\frac{\theta}{2}) \end{pmatrix}$$

Donde \hat{r} es el vector unitario asociado al eje de la rotación, θ es el ángulo que se rota y $\vec{\sigma}$ es el vector de las matrices de Pauli $(\sigma_x, \sigma_y, \sigma_z)$.

Si $\hat{r} = (1, 0, 0)$, se tiene la rotación general sobre X.

$$R_x(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & i \sin(\frac{\theta}{2}) \\ i \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$$

Si $\hat{r} = (0, 1, 0)$, se tiene la rotación general sobre Y.

$$R_y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & \sin(\frac{\theta}{2}) \\ -\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$$

Si $\hat{r} = (0, 0, 1)$, se tiene la rotación general sobre Z.

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

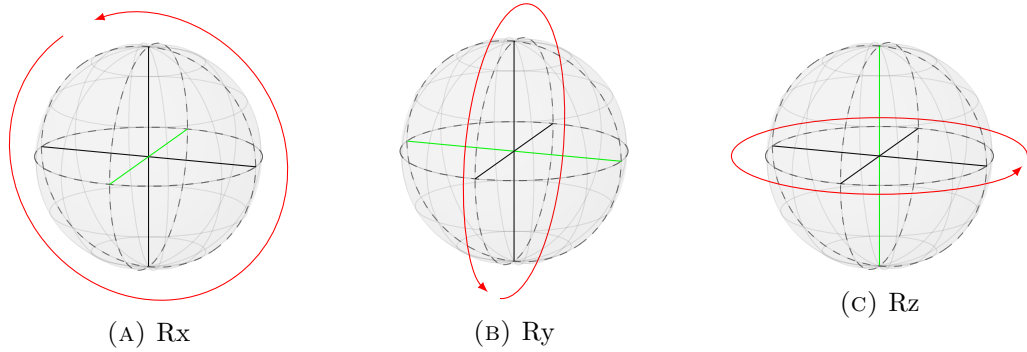


FIGURA 2.10: Compuertas Rx, Ry y Rz en la esfera de Bloch

Para realizar cualquier rotación en la esfera de Bloch, basta con poder realizar rotaciones generales sobre dos ejes ortogonales de ella. A partir de secuencias tres rotaciones alrededor de estos dos ejes se puede realizar cualquier rotación alrededor de cualquier otro eje. Por ejemplo, las rotaciones alrededor de X, en función de rotaciones alrededor de Y y Z se realizan de la siguiente manera:

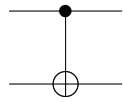
$$R_x(\theta) = R_z(\frac{\pi}{2})R_y(\theta)R_z(\frac{-\pi}{2})$$

2.16. Compuertas multiqubit

Las compuertas multiqubit involucran interacción entre los qubits.

2.16.1. Compuerta CNOT

La compuerta CNOT, o *controlled-NOT*, es un ejemplo de una compuerta condicionada. De hecho, es la compuerta X condicionada. Ella recibe dos qubits de entrada, un *control* y un *target*. Si el qubit de control es $|0\rangle$ se aplica $\mathbb{1}$ sobre el qubit objetivo y si el qubit de control es $|1\rangle$, se aplica X sobre el qubit objetivo. Esta compuerta se puede escribir en función de proyectores en la partición del qubit de control de la siguiente manera: $CNOT = \Pi_0 \otimes \mathbb{1} + \Pi_1 \otimes X$.



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

Entrada	Salida
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$
$\alpha 00\rangle + \beta 01\rangle + \gamma 10\rangle + \delta 11\rangle$	$\alpha 00\rangle + \beta 01\rangle + \delta 10\rangle + \gamma 11\rangle$

2.16.2. Compuerta SWAP

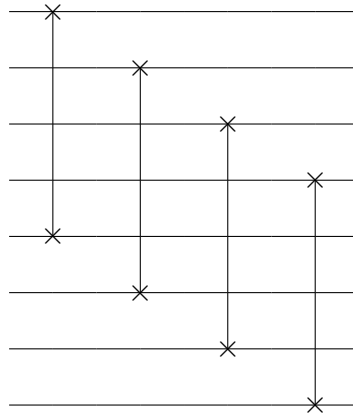
La compuerta SWAP, como su nombre lo indica, intercambia el contenido de dos particiones de qubits. Es decir, transforma $|\psi\rangle \otimes |\phi\rangle$ en $|\phi\rangle \otimes |\psi\rangle$.



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

Entrada	Salida
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 10\rangle$
$ 10\rangle$	$ 01\rangle$
$ 11\rangle$	$ 11\rangle$
$\alpha 00\rangle + \beta 01\rangle + \gamma 10\rangle + \delta 11\rangle \rightarrow \alpha 00\rangle + \gamma 01\rangle + \beta 10\rangle + \delta 11\rangle$	

Si se tiene un sistema de qubits dividido en dos partes o registros del mismo tamaño, también se llama SWAP a la compuerta que intercambia estos dos registros. Es decir, a la operación que transforma $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle \otimes |\phi_1\rangle \otimes \dots \otimes |\phi_n\rangle$ en $|\phi_1\rangle \otimes \dots \otimes |\phi_n\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$. Ella se construye de la siguiente manera:



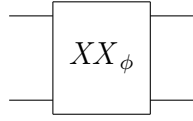
2.16.3. Compuerta $\sqrt{\text{SWAP}}$

$$\begin{array}{c}
 \text{---} \times \text{---} \\
 \text{---} \times \text{---}
 \end{array}
 \begin{pmatrix}
 1 & 0 & 0 & 0 \\
 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\
 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\
 0 & 0 & 0 & 1
 \end{pmatrix}$$

Entrada	Salida
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$\frac{1+i}{2} 01\rangle + \frac{1-i}{2} 10\rangle$
$ 10\rangle$	$\frac{1-i}{2} 01\rangle + \frac{1+i}{2} 10\rangle$
$ 11\rangle$	$ 11\rangle$
$\alpha 00\rangle + \beta 01\rangle + \gamma 10\rangle + \delta 11\rangle \rightarrow \alpha 00\rangle + (\frac{1+i}{2}\beta + \frac{1-i}{2}\gamma) 01\rangle + (\frac{1-i}{2}\beta + \frac{1+i}{2}\gamma) 10\rangle + \delta 11\rangle$	

2.16.4. Compuerta de Ising

Esta compuerta es fundamental para las computadoras cuánticas a base de trampas de iones, pues se puede realizar de manera nativa en estos sistemas [44, 45].



$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & -ie^{i\phi} \\ 0 & 1 & -i & 0 \\ 0 & -i & 1 & 0 \\ -ie^{-i\phi} & 0 & 0 & 1 \end{pmatrix}$$

Entrada

$$|00\rangle$$

$$|01\rangle$$

$$|10\rangle$$

$$|11\rangle$$

$$\alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle \quad \frac{\alpha - ie^{i\phi}\delta}{\sqrt{2}} |00\rangle + \frac{\beta - i\gamma}{\sqrt{2}} |01\rangle + \frac{\gamma - i\beta}{\sqrt{2}} |10\rangle + \frac{\delta - ie^{-i\phi}\alpha}{\sqrt{2}} |11\rangle$$

Salida

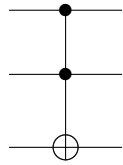
$$\frac{1}{\sqrt{2}}(|00\rangle - ie^{-i\phi}|11\rangle)$$

$$\frac{1}{\sqrt{2}}(|01\rangle - i|10\rangle)$$

$$\frac{1}{\sqrt{2}}(-i|01\rangle + |10\rangle)$$

$$\frac{1}{\sqrt{2}}(-ie^{i\phi}|00\rangle + |11\rangle)$$

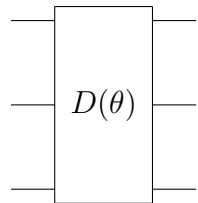
2.16.5. Compuerta de Toffoli



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

Entrada	Salida
$ 000\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 100\rangle$
$ 101\rangle$	$ 101\rangle$
$ 110\rangle$	$ 111\rangle$
$ 111\rangle$	$ 110\rangle$
$\alpha 000\rangle + \beta 001\rangle + \gamma 010\rangle + \delta 011\rangle$	$\alpha 000\rangle + \beta 001\rangle + \gamma 010\rangle + \delta 011\rangle$
$+ \epsilon 100\rangle + \zeta 101\rangle + \eta 110\rangle + \theta 111\rangle$	$+ \epsilon 100\rangle + \zeta 101\rangle + \theta 110\rangle + \eta 111\rangle$

2.16.6. Compuerta de Deutsch



$$\begin{pmatrix}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & i \cos(\theta) & \sin(\theta) \\
 0 & 0 & 0 & 0 & 0 & 0 & \sin(\theta) & i \cos(\theta)
 \end{pmatrix}$$

$$|a, b, c\rangle \rightarrow \begin{cases} i \cos(\theta) |a, b, c\rangle + \sin(\theta) |a, b, c \oplus 1\rangle & \text{si } a = b = 1 \\ |a, b, c\rangle & \text{en otro caso} \end{cases}$$

Entrada	Salida
$ 000\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 100\rangle$
$ 101\rangle$	$ 101\rangle$
$ 110\rangle$	$i \cos(\theta) 110\rangle + \sin(\theta) 111\rangle$
$ 111\rangle$	$\sin(\theta) 110\rangle + i \cos(\theta) 111\rangle$
$\alpha 000\rangle + \beta 001\rangle + \gamma 010\rangle + \delta 011\rangle$	$\alpha 000\rangle + \beta 001\rangle + \gamma 010\rangle + \delta 011\rangle$
$+ \epsilon 100\rangle + \zeta 101\rangle + \eta 110\rangle + \iota 111\rangle$	$+ \epsilon 100\rangle + \zeta 101\rangle + (i \cos(\theta)\eta + \sin(\theta)\iota) 110\rangle$ $+ (\sin(\theta)\eta + i \cos(\theta)\iota) 111\rangle$

2.17. Conjuntos universales de compuertas cuánticas

Un conjunto universal de compuertas cuánticas (CUCC) es un conjunto finito de compuertas cuánticas con el cuál se puede aproximar cualquier operación unitaria arbitrariamente bien.

Cualquier operador unitario puede ser escrito en función de compuertas de uno y dos qubits [46].

Un CUCC simple es $\{H, T, CNOT\}$.

Existe un CUCC de una sólo compuerta, la compuerta de Deutsch, $D(\theta)$.

La compuerta de Toffoli es un caso especial de la compuerta de Deutsch, $D(\frac{\pi}{2})$.

Otro CUCC consiste en la compuerta de Ising y la compuerta de cambio de fase, $\{XX_\phi, R_z(\theta)\}$. Este conjunto es nativo en algunas computadoras cuánticas de trampas de iones.

2.18. Criterios de DiVincenzo

Para construir un computador cuántico, se deben cumplir las siguientes condiciones experimentales:

1. Un sistema físico escalable con qubits bien caracterizados.
2. La habilidad de inicializar el estado de los qubits en un estado fiducial simple.
3. Tiempos de coherencia relevantes largos.
4. Un conjunto universal de compuertas cuánticas.
5. La capacidad de medir qubits en específico.

2.19. Fidelidad

La fidelidad de dos distribuciones clásicas de probabilidad $\{p_x\}$ y $\{q_x\}$ es una medida de distancia entre ellas, y se define como:

$$F(p_x, q_x) = \sum_x \sqrt{p_x q_x}. \quad (2.66)$$

Cuando las distribuciones $\{p_x\}$ y $\{q_x\}$ son idénticas, la fidelidad entre ellas es igual a 1. La interpretación geométrica de la fidelidad es que esta es el producto interno de dos vectores de componentes $\sqrt{p_x}$ y $\sqrt{q_x}$, que yacen en la esfera unitaria.

En el caso de los estados cuánticos, la fidelidad toma la siguiente forma [4]

$$F(\rho, \sigma) = \text{Tr}(\sqrt{\rho^{1/2} \sigma \rho^{1/2}}). \quad (2.67)$$

Como ρ es hermítico, sabemos que es diagonalizable con un operador unitario. Sea U el operador que diagonaliza ρ de manera que

$$D = U^\dagger \rho U, \quad (2.68)$$

Donde D es un operador diagonal tal que su representación matricial es $[d_i]$. A partir de D , la raíz cuadrada de ρ se calcula de la siguiente ecuación

$$\rho^{1/2} = U D^{1/2} U^\dagger, \quad (2.69)$$

Donde $D^{1/2}$ es un operador diagonal cuya representación matricial está dada por $[\sqrt{d_i}]$. En otras palabras, $\rho^{1/2}$ es una matriz con los mismos autovectores que ρ , pero cuyos autovalores correspondientes son la raíz cuadrada de los de ρ .

En ciertos casos especiales, la fidelidad se puede simplificar de las siguientes maneras:

1. Si ρ y σ conmutan, es decir, que existe una base en la que ambos son diagonales, entonces la fidelidad cuántica toma la forma de la fidelidad clásica

$$F(\rho, \sigma) = \text{Tr}(\sum_i \sqrt{r_i s_i} |i\rangle\langle i|) = \sum_i \sqrt{r_i s_i} = F(r_i, s_i), \quad (2.70)$$

Donde r_i y s_i son los autovalores de ρ y σ , respectivamente.

2. Si σ es un estado puro $|\psi\rangle$, entonces la fidelidad toma la forma

$$F(|\psi\rangle, \rho) = \text{Tr}(\sqrt{\langle\psi|\rho|\psi\rangle\langle\psi|\psi\rangle}) = \sqrt{\langle\psi|\rho|\psi\rangle}. \quad (2.71)$$

3. Si ambos estados son puros, entonces la fidelidad es:

$$F(|\psi\rangle, |\varphi\rangle) = \sqrt{\langle\psi|\varphi\rangle\langle\varphi|\psi\rangle} = |\langle\psi|\varphi\rangle|. \quad (2.72)$$

2.20. Medidas proyectivas

El esquema de medidas proyectivas, también llamadas medidas de von Neumann, se encuentra formado por proyectores ortogonales asociados a la medida espectral de un observable [47]. Este esquema es uno de los tipos de medidas de uso más común, ya que está directamente asociada a la medición de una propiedad del sistema o un conjunto compatible de ellas, y tales propiedades son caracterizadas a través de operadores autoadjuntos. Esta medida fue empleada por von Neumann para descomponer a los observables de un sistema cuántico en una combinación lineal de proyectores, donde cada proyector está asociado a los subespacios \mathcal{M}_λ que son dejados invariantes por el operador en cuestión y, los coeficientes de la combinación lineal corresponden a los posibles valores que arroja el observable tras una medición. En este esquema, la probabilidad $P_\lambda(p)$ de obtener un valor $\lambda \in \Delta$ después de medir el observable en cuestión en el estado $\hat{\rho}$ viene dada por el valor medio del proyector $\hat{\Pi}_{\mathcal{M}_\lambda}$ asociado al autovalor λ , mientras que el estado después

de la medida viene dado por el autovector correspondiente a dicho autovalor. En este caso, las medidas proyectivas vienen dadas por

$$MP_s = \{\hat{\Pi}_m : \mathcal{H} \rightarrow \mathcal{M}_{\lambda_m} \subseteq \mathcal{H} \text{ tal que } \hat{\Pi}_m \hat{\Pi}_n = \delta_{m,n} \hat{\Pi}_m, \\ \sum_m \hat{\Pi}_m = \mathbb{1}, P_{\lambda_m}(\rho) = (\hat{\Pi}_m)_\rho \text{ y } \rho_{\lambda_m} \xrightarrow{\text{colapso}} \hat{\Pi}_m\}. \quad (2.73)$$

Cabe destacar que al realizar nuevamente la medida el estado resultante no se modifica, siempre que la dimensión de \mathcal{M}_λ sea igual a uno, es decir, el proyector $\hat{\Pi}_{\mathcal{M}_\lambda}$ sea de rango uno. Este hecho se conoce con el nombre de repetibilidad, propiedad que no está presente en los otros esquemas de medidas.

2.21. Sistemas cuánticos abiertos

Consideremos el espacio de Hilbert bipartito $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Como ya vimos antes, si tenemos una matriz de densidad $\rho \in \mathcal{H}$, la manera de escribir la matriz de densidad del subsistema A está dada por la traza parcial $\rho_A = \text{Tr}_B(\rho)$.

En \mathcal{H}_A las medidas están dadas por un conjunto de operadores hermíticos $\{M_k\}$, cada uno de ellos asociado a un posible resultado k . Supongamos que no podemos ver el subsistema B y que sólo vemos A con ρ_A . Entonces, la probabilidad de obtener un resultado k cuando realicemos la medida $\{M_k\}$ será

$$p_A(k) = \text{Tr}(M_k \rho_A). \quad (2.74)$$

En el sistema total esta medida corresponde a un operador $\tilde{M}_k = M_k \otimes \mathbb{1}$ y la probabilidad de obtener el resultado k sería

$$p_A(k) = \text{Tr}(\tilde{M}_k \rho). \quad (2.75)$$

Si $\{|\psi_i^A\rangle, |\varphi_j^B\rangle\}$ es una base de \mathcal{H} , entonces

$$\begin{aligned}
p_A(k) &= \text{Tr}[(M_k \otimes \mathbb{1})\rho] \\
&= \sum_{ij} \langle \psi_i^A | \langle \varphi_j^B | (M_k \otimes \mathbb{1}) \rho | \psi_i^A \rangle | \varphi_j^B \rangle \\
&= \sum_i (\langle \psi_i^A | M_k \otimes \mathbb{1}) \left[\sum_j (\mathbb{1} \otimes \langle \varphi_j^B |) \rho (\mathbb{1} \otimes | \varphi_j^B \rangle) \right] (| \psi_i^A \rangle \otimes \mathbb{1}) \quad (2.76) \\
&= \sum_i \langle \psi_i^A | M_k \text{Tr}_B(\rho) | \psi_i^A \rangle \\
&= \sum_i \langle \psi_i^A | M_k \rho_A | \psi_i^A \rangle = \text{Tr}(M_k \rho_A).
\end{aligned}$$

Así que ρ_A está inequívocamente dado por la traza parcial $\text{Tr}_B(\rho)$.

Una propiedad importante de la traza parcial es que incluso si ρ es un estado puro, ρ_A y ρ_B pueden ser mixtos, esto ocurre si $|\phi\rangle$ es un estado entrelazado.

Dada la matriz de densidad $\rho(t_0)$, tomando la traza parcial en B en el tiempo t_1 , tendríamos el estado $\rho_A(t_1)$, dado por:

$$\rho_A(t_1) = \text{Tr}_B[U(t_1, t_0)\rho(t_0)U^\dagger(t_1, t_0)]. \quad (2.77)$$

Si el operador de evolución no puede ser factorizado de la manera $U(t_1, t_0) = U_A(t_1, t_0) \otimes U_B(t_1, t_0)$, entonces los sistemas A y B están interactuando e intercambian energía e información entre ellos, es decir, son sistemas cuánticos abiertos.

Ahora, ¿qué pasa si queremos estudiar sólo la dinámica de ρ_A ?, a pesar de saber que no podemos factorizar $U(t_1, t_0)$ en dos particiones. Este problema se soluciona desarrollando un mapa dinámico que actúe en \mathcal{H}_A que transforme los estados del subsistema A del tiempo t_0 al tiempo t_1 .

$$\mathcal{E}_{(t_1, t_0)} : \rho_A(t_0) \rightarrow \rho_A(t_1). \quad (2.78)$$

El problema es que en general este mapa no depende sólo de $U(t_1, t_0)$ y de las propiedades de B , sino también de A en sí mismo. Para aclarar este punto, escribamos el estado total ρ como la suma de dos contribuciones:

$$\rho(t) = \rho_A(t_0) \otimes \rho_B(t_1) + \rho_{corr}(t_0), \quad (2.79)$$

Donde el término $\rho_{corr}(t_0)$ no es un estado cuántico y satisface

$$Tr_A[\rho_{corr}(t_0)] = Tr_B[\rho_{corr}(t_0)] = 0. \quad (2.80)$$

Este término contiene las correlaciones, tanto clásicas como cuánticas, entre los dos subsistemas. Sustituyendo 2.79 en 2.77 tenemos

$$\begin{aligned} \rho_A(t_1) &= Tr_B[U(t_1, t_0)(\rho_A(t_0) \otimes \rho_B(t_0) + \rho_{corr}(t_0))U^\dagger(t_1, t_0)] \\ &= \sum_i \lambda_i Tr_B[U(t_1, t_0)(\rho_A(t_0) \otimes |\psi_i\rangle\langle\psi_i|)U^\dagger(t_1, t_0)] \\ &+ Tr_B[U(t_1, t_0)\rho_{corr}(t_0)U^\dagger(t_1, t_0)] \\ &= \sum_{ij} K_{ij}(t_1, t_0)\rho_A(t_0)K_{ij}^\dagger(t_1, t_0) + \zeta(t_1, t_0) \\ &= \mathcal{E}_{(t_1, t_0)}[\rho_A(t_0)], \end{aligned} \quad (2.81)$$

Donde $K_{ij}(t_1, t_0) = \sqrt{\lambda_i} \langle\psi_j| U(t_1, t_0) |\psi_i\rangle$ y hemos usado la descomposición espectral de $\rho_B(t_0) = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$. Los operadores $K_{ij}(t_1, t_0)$ dependen sólo del operador de evolución global y del estado inicial del subsistema B , pero la parte no homogénea $\zeta(t_1, t_0) = Tr_B[U(t_1, t_0)\rho_{corr}(t_0)U^\dagger(t_1, t_0)]$ puede no ser independiente de ρ_A debido al término de correlación ρ_{corr} .

Vista esta dependencia, reescribamos $\mathcal{E}_{(t_1, t_0)}$ de la siguiente manera:

$$\mathcal{E}_{(t_1, t_0)}[\rho_A] = \rho_A(t_1) = \sum_{ij} K_{ij}(t_1, t_0, \rho_A)\rho_A(t_0)K_{ij}^\dagger(t_1, t_0, \rho_A). \quad (2.82)$$

Hemos escrito el mapa dinámico de manera homogénea y ahora K_{ij} depende de ρ_A en el tiempo t_0 . Un mapa con esta forma siempre existe. Para demostrar esto, basta con considerar el siguiente caso particular:

$$\mathcal{E}_{(t_1, t_0)}[\rho_A] = Tr_2[U_{SWAP}\rho_A(t_0) \otimes \rho_A(t_1)U_{SWAP}^\dagger] = \rho_A(t_1). \quad (2.83)$$

Aquí U_{SWAP} representa el operador SWAP entre las particiones 1 y 2, tal que $U_{SWAP}(\rho \otimes \sigma)U_{SWAP}^\dagger$. Así, $\rho_A(t_1)$ pasa a la partición 1 y es el resultado de la traza parcial. Entonces, si utilizamos la descomposición espectral de $\rho_A(t_1)$ tendremos

$$\begin{aligned} \mathcal{E}_{(t_1, t_0)}[\rho_A] &= Tr_2[U_{SWAP}\rho_A(t_0) \otimes \rho_A(t_1)U_{SWAP}^\dagger] \\ &= \sum_i \lambda_i Tr_2[U_{SWAP}\rho_A(t_0) \otimes |\lambda_i\rangle U_{SWAP}^\dagger] \\ &= \sum_{ij} K_{ij}(t_1, t_0, \rho_A)\rho_A(t_0)K_{ij}^\dagger(t_1, t_0, \rho_A), \end{aligned} \quad (2.84)$$

Donde $K_{ij}(t_1, t_0, \rho_A) = \sqrt{\lambda_i} \langle \lambda_j | U_{SWAP} | \lambda_i \rangle$. Cabe mencionar que esta descomposición no es única.

Un mapa dinámico universal es aquel que es independiente del estado al que se aplica. Los operadores $K_{ij}(t_1, t_0)$ que lo conforman se conocen como operadores de Krauss. Los mapas dinámicos universales son completamente positivos y los operadores de Krauss cumplen la siguiente propiedad

$$\sum_{ij} K_{ij}^\dagger(t_1, t_0) K_{ij}(t_1, t_0) = \mathbb{1}. \quad (2.85)$$

Decimos que un sistema tiene evolución markoviana cuando su evolución puede ser descrita por mapas dinámicos universales tales componibles de la siguiente manera:

$$\mathcal{E}_{(t_2, t_0)} = \mathcal{E}_{(t_2, t_1)} \mathcal{E}_{(t_1, t_0)}. \quad (2.86)$$

Esta propiedad de composición se conoce como condición de divisibilidad. Típicamente, la evolución de los sistemas abiertos no es markoviana, porque se desarrollan correlaciones que hacen que el mapa dinámico que la describe no sea universal. Sin embargo, si el término ρ_{corr} no afecta mucho la dinámica del sistema, un modelo markoviano puede dar una buena aproximación de la evolución temporal.

Consideremos entonces una evolución markoviana. Esto nos permite construir la siguiente ecuación de diferencias:

$$\rho(t + \epsilon) - \rho(t) = [\mathcal{E}_{(t+\epsilon, 0)} - \mathcal{E}_{(t, 0)}] \rho(0) = [\mathcal{E}_{(t+\epsilon, t)} - \mathbb{1}] \mathcal{E}_{(t, 0)} [\rho(0)] = [\mathcal{E}_{(t+\epsilon, t)} - \mathbb{1}] \rho(t). \quad (2.87)$$

Si el límite cuando ϵ tiende a cero está bien definido, entonces podemos construir la ecuación diferencial de $\rho(t)$, llamada ecuación maestra:

$$\frac{d\rho(t)}{dt} = \lim_{\epsilon \rightarrow 0} \frac{\rho(t + \epsilon) - \rho(t)}{\epsilon} = \lim_{\epsilon \rightarrow 0} \frac{[\mathcal{E} - \mathbb{1}]}{\epsilon} \rho(t) = \mathcal{L}_t \rho(t), \quad (2.88)$$

Donde hemos definido el generador de la evolución como:

$$\mathcal{L}_t = \lim_{\epsilon \rightarrow 0} \frac{[\mathcal{E} - \mathbb{1}]}{\epsilon}. \quad (2.89)$$

Sea $\{F_j, j = 1, \dots, N^2\}$ una base ortonormal completa con respecto al producto interno de Hilbert-Schmidt $(F_n, F_m) = \text{Tr}(F_n^\dagger F_m) = \delta_{nm}$, tal que $F_{N^2} = \mathbb{1}/\sqrt{N}$, para que el resto de los operadores tengan traza cero. Ahora la expansión de Krauss en esta base nos da

$$\mathcal{E}_{(t_2, t_1)}[\rho] = \sum_{nm} c_{nm}(t_2, t_1) F_n \rho F_m^\dagger, \quad (2.90)$$

Donde los elementos c_{nm} son la multiplicación de los productos internos de K_{ij} con los elementos de la base elegida.

$$c_{nm}(t_2, t_1) = \sum_{ij} (F_n, K_{ij}(t_2, t_1))(F_m, K_{ij}(t_2, t_1))^*. \quad (2.91)$$

En esta base el generador \mathcal{L}_t toma la siguiente forma:

$$\begin{aligned} \mathcal{L}_t(\rho) &= \lim_{\epsilon \rightarrow 0} \sum_{nm} \frac{c_{nm}(t+\epsilon, t) F_n \rho F_m^\dagger - \rho}{\epsilon} \\ &= \lim_{\epsilon \rightarrow 0} \left[\frac{c_{N^2 N^2}(t+\epsilon, t) - N}{N\epsilon} \rho \right. \\ &\quad + \sum_{n=1}^{N^2-1} \frac{1}{\sqrt{N}} \left(\frac{c_{n N^2}(t+\epsilon, t)}{\epsilon} F_n \rho + \frac{c_{N^2 n}(t+\epsilon, t)}{\epsilon} \rho F_n^\dagger \right) \\ &\quad \left. + \sum_{n,m=1}^{N^2-1} \frac{c_{nm}(t+\epsilon, t)}{\epsilon} F_n \rho F_m^\dagger \right]. \end{aligned} \quad (2.92)$$

Ahora, definamos los coeficientes $\alpha_{nm}(t)$ como:

$$\alpha_{N^2 N^2}(t) = \lim_{\epsilon \rightarrow 0} \frac{c_{N^2 N^2}(t+\epsilon, t) - N}{\epsilon} \quad (2.93)$$

$$\alpha_{n N^2}(t) = \lim_{\epsilon \rightarrow 0} \frac{c_{n N^2} \epsilon}{\epsilon}, \quad n = 1, \dots, N^2 - 1 \quad (2.94)$$

$$\alpha_{nm}(t) = \lim_{\epsilon \rightarrow 0} \frac{c_{nm} \epsilon}{\epsilon}, \quad n = 1, \dots, N^2 - 1. \quad (2.95)$$

También definimos los siguientes operadores:

$$F(t) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N^2-1} \alpha_{jN^2}(t) F_j \quad (2.96)$$

$$G(t) = \frac{\alpha_{N^2N^2}}{2N} \mathbb{1} + \frac{1}{2} [F^\dagger(t) + F(t)] \quad (2.97)$$

$$H(t) = \frac{1}{2i} [F^\dagger(t) - F(t)]. \quad (2.98)$$

Este último operador, $H(t)$, es hermítico. En términos de estos operadores, sustituyendo, el generador de la ecuación maestra toma la siguiente forma:

$$\mathcal{L}_t(\rho) = -i[H(t), \rho] + \{G(t), \rho\} + \sum_{n,m=1}^{N^2-1} \alpha_{nm}(t) F_n \rho F_m^\dagger. \quad (2.99)$$

Ya que los mapas dinámicos universales preservan la traza de cualquier matriz de densidad ρ ,

$$0 = \text{Tr}[\mathcal{L}(\rho)] = \text{Tr} \left[\left(2G(t) + \sum_{n,m=1}^{N^2-1} \alpha_{nm}(t) F_m^\dagger F_n \right) \rho \right]. \quad (2.100)$$

Las siguientes propiedades de la traza de los conmutadores y los anticonmutadores

$$\text{Tr}([A, B]) = \text{Tr}(AB - BA) = \text{Tr}(AB) - \text{Tr}(BA) = 0 \quad (2.101)$$

$$\text{Tr}(\{A, B\}) = \text{Tr}(AB + BA) = \text{Tr}(AB) + \text{Tr}(BA) = 2\text{Tr}(AB). \quad (2.102)$$

Dado este hecho, podemos concluir que

$$G(t) = -\frac{1}{2} \sum_{n,m=1}^{N^2-1} \alpha_{nm}(t) F_m^\dagger F_n. \quad (2.103)$$

Sustituyendo, el generador nos queda de con la siguiente forma

$$\mathcal{L}_t(\rho) = -i[H(t), \rho] + \sum_{n,m=1}^{N^2-1} \alpha_{nm}(t) [F_n \rho F_m^\dagger - \frac{1}{2} \{F_m^\dagger F_n, \rho\}]. \quad (2.104)$$

La matriz de coeficientes $\{\alpha_{nm}(t)\}$ es una matriz semidefinida positiva, así que podemos diagonalizarla con una matriz unitaria $u(t)$, tal que

$$\sum_{nm} u_{jn}(t) \alpha_{nm}(t) u_{km}^*(t) = \gamma_j(t) \delta_{jk}. \quad (2.105)$$

Cada autovalor $\gamma_j(t)$ es mayor o igual a cero. Ahora tenemos los nuevos operadores $V_m(t)$

$$V_m(t) = \sum_{n=1}^{N^2-1} u_{mn}^*(t) F_n F_j = \sum_{m=1}^{N^2-1} u_{mn}(t) V_m(t). \quad (2.106)$$

Con estos últimos operadores, el generador de la ecuación maestra se convierte en

$$\mathcal{L}_t(\rho) = -i[H(t), \rho] + \sum_m \gamma_m(t) \left[V_m(t) \rho V_m^\dagger(t) - \frac{1}{2} \{V_m^\dagger(t) V_m(t), \rho\} \right]. \quad (2.107)$$

Con $\gamma_m(t) \geq 0$ para todo m y t . Finalmente, Kossakowski [48] y Lindblad [49] analizaron este problema para el caso de ecuaciones temporalmente homogéneas, es decir, el caso en el que el mapa dinámico universal depende sólo de la diferencia entre los tiempos t_2 y t_1 , $\tau = t_2 - t_1$, en lugar de los tiempos en sí mismos, $\mathcal{E}_{(t_2, t_1)} = \mathcal{E}_{(\tau)}$. La ecuación diferencial generada en este caso se conoce como Lindbladiano.

$$\dot{\rho}(t) = -i[\hat{H}, \rho(t)] + \sum_k \gamma_k [V_k \rho(t) V_k^\dagger - \frac{1}{2} \{V_k^\dagger V_k, \rho(t)\}]. \quad (2.108)$$

En esta ecuación \hat{H} es el Hamiltoniano del sistema, V_k son operadores de salto o colapso, y γ_k son tasas de decaimiento. El término $-i[\hat{H}, \rho(t)]$ representa la evolución unitaria y es el mismo de la ecuación de Liouville-von Neumann. Los términos $\gamma_k V_k \rho(t) V_k^\dagger$ representan el efecto del entorno en el sistema y los términos $-\frac{1}{2} \{V_k^\dagger V_k, \rho(t)\}$ son términos de normalización para el caso en el que el entorno no afecta al sistema.

Capítulo 3

Superconductividad

3.1. Cuantización macroscópica y superconductividad

Uno de los mayores principios de la mecánica cuántica es el hecho de que cantidades físicas como la energía o el momentum están, bajo ciertas condiciones, cuantizados. Es decir, que sólo tienen valores discretos. Sin embargo, por un largo tiempo se creyó que la cuantización sólo era relevante para sistemas microscópicos, como los núcleos, los átomos o las moléculas. De hecho, considerando el comportamiento de objetos macroscópicos, que consistan de una gran cantidad de átomos, los efectos de la cuantización no pueden ser observados, aunque cada átomo individual obedezca las leyes de la mecánica cuántica. Esto se debe al hecho de que los movimientos térmicos enmascaran las regularidades cuánticas. Sin embargo, para ciertos fenómenos ha sido demostrado que es posible observar cuantización macroscópica. Así que podemos observar la cuantización de parámetros que caracterizan a sistemas macroscópicos muchos órdenes de magnitud más grandes que sistemas como los átomos. Esto se debe a altos niveles de correlaciones por efectos de coherencia [50].

En 1911 Kamerlingh Onnes [51] descubrió que el Hg conduce sin resistencia cuando se enfría a temperatura del He líquido (4.2K). Kamerlingh Onnes fue el primer físico que licuó el He, poco tiempo después de esto, midiendo resistividades de distintos metales a estas bajas temperaturas, se encontró, en su laboratorio, que el Hg a 4.2K conduce sin resistencia. No con una resistencia despreciablemente pequeña, sino con resistencia cero.

Podría pensarse que el caso del Hg es la excepción y la cuantización macroscópica es un fenómeno particular de este elemento, sin embargo resulta que el número de elementos y materiales superconductores es muy grande. La tabla periódica está llena de elementos que, bajo cierta temperatura crítica, se convierten en superconductores. En realidad la pregunta no sería por que un elemento es superconductor, sino por qué no lo es. Ahora bien, las temperaturas a las cuales ocurre el efecto son extraordinariamente bajas. La mayoría de los superconductores tienen temperaturas críticas por debajo de los 30K y requieren ser enfriados con He líquido. Cabe mencionar que existen superconductores de “alta temperatura” con temperaturas críticas en el orden de los 100K y que pueden ser enfriados con N líquido, hechos a partir de cerámicas con estructuras cristalinas. El record de la mayor temperatura crítica reportada de un superconductor es 203K [52]. Sin embargo, en este capítulo no haremos ninguna referencia a ellos, ya que requieren el desarrollo de teorías más avanzadas.

En 1913 [53] se comprobó que si se aplica un campo magnético exterior al material en estado superconductor, se perdía el estado de conducción perfecta. Este campo, cuyo valor depende de la temperatura, se llama campo crítico. Tenemos así el primer indicio de que la interacción superconductividad-magnetismo juega un papel primordial en los fenómenos superconductores.

Ahora bien, un superconductor es mucho más que un conductor perfecto. La siguiente característica fundamental de un superconductor consiste en que cuando el campo magnético aplicado no es mayor que el campo crítico un superconductor actúa como un material diamagnético perfecto ($\chi = -1$). Por lo tanto, no existen líneas de campo magnético en el interior de un material superconductor, salvo en una pequeña zona próxima a la superficie de aproximadamente 500Å. Este efecto se conoce con el nombre de efecto Meissner-Ochsenfeld. Es importante mencionar que este no es el caso en un conductor ideal, pues en ellos el campo magnético quedaría atrapado en el material sin que haya razón para que sea expulsado.

Otra característica típica de la superconductividad es que el flujo del campo magnético que atraviesa un anillo superconductor está cuantizado. Es decir, el flujo que atraviesa un superconductor vale un número entero de veces una unidad de flujo elemental llamada el fluxoide Φ_0 y cuyo valor es $\Phi_0 = h/2e$, donde h es la constante de Planck y e la carga del electrón.

Existe otro efecto cuántico macroscópico asociado a la superconductividad, conocido como el efecto Josephson, el cual será el fundamento de los qubits superconductores. Este efecto es un caso del efecto túnel. Si se separan dos superconductores

distintos, o bien el mismo superconductor por una barrera, por ejemplo un aislante o un estrechamiento en el superconductor (lo que se conoce como una unión débil), se tiene paso de corriente por la barrera sin que aparezca caída de potencial a ambos lados de la barrera.

3.2. La teoría BCS

En 1957 John Bardeen, Leon Cooper y J. Robert Schieffer [54] encontraron la llave para poder explicar, desde un punto de vista microscópico, la superconductividad. Realmente existen bastantes materiales que se desvían de la teoría estricta BCS, como pueden ser aleaciones, compuestos y algunos elementos (el mismo Hg, donde se descubrió la superconductividad, es un ejemplo de superconductor que no cumple los estrictos requisitos de la teoría BCS). Esto no significa que la teoría sea incorrecta, sino incompleta y para tratar ciertas situaciones y ciertos compuestos o elementos hay que evitar algunas de las aproximaciones que se realizan en el desarrollo de esta teoría.

Experimentalmente se observó que la temperatura crítica T_c de los superconductores, como el Hg, depende de la masa de los iones en el metal. Dado que existen varios isótopos del Hg se pudieron preparar varias muestras y se comprobó experimentalmente que si M es la masa del ion se tiene que $T_c \propto M^{-\alpha}$ donde el exponente α es dependiente del tipo del metal. Esto indica que los iones de la red juegan un papel fundamental en la superconductividad. Este fenómeno se llama efecto isotópico.

Adicionalmente, existen las siguientes diferencias entre los metales normales y los superconductores:

1. Metal normal:

- a) El calor específico electrónico de un metal no superconductor a muy baja temperatura varía linealmente con la temperatura. En un metal existen dos contribuciones al calor específico, una de ellas es la normal de la red. Esta contribución varía como T^3 y prácticamente desaparece a bajas temperaturas. Existe otra contribución al calor específico propia de los metales. A esta contribución, que es la predominante a bajas temperaturas, es a la que nos referimos y varía como T .

- b) Un metal en estado normal no es transparente, es decir, que el material permita el paso de onda electromagnética sin decaer, a la radiación visible e infrarroja.

2. Superconductor:

- a) La variación del calor específico en función de la temperatura sigue una ley exponencial.
- b) En un metal en estado superconductor existe, en el rango del infrarrojo lejano, una frecuencia de corte para la cual el metal es transparente a esa radiación.

Estos dos efectos en superconductores son una señal de que en un superconductor existe una banda prohibida de energía. Esta banda no es del mismo tipo que la que existe en semiconductores. La banda de energía prohibida en semiconductores se origina por la periodicidad del potencial asociado a la red cristalina, mientras la banda de energía en los superconductores se origina por el acoplamiento entre electrones. Otra comprobación experimental de este hecho son las anomalías en el efecto túnel, conocido como túnel Giaever.

Los electrones de conducción, por su movimiento al azar en una red cristalina, donde los iones vibran, cambian constantemente de momentum. La propagación de las vibraciones de los iones de la red se llama fonones. La interacción electrón-fonón es la que produce la resistividad. Que un metal conduzca sin resistencia eléctrica implica que los electrones de conducción en su movimiento en el cristal no cambian de momentum. Se debe, entonces, encontrar una interacción entre los electrones de conducción y los fonones que produzca este efecto. En un cristal la interacción fundamental entre electrones y fonones es la interacción coulombiana. Pues bien, esto es todo lo necesario para construir la teoría BCS: electrones, fonones e interacción coulombiana.

La interacción coulombiana electrón de conducción-red cristalina (iones) se puede ver esquemáticamente de la siguiente forma: Supongamos un electrón de conducción que se mueve por el cristal y fijémonos en un punto concreto de la red, formada por iones positivos. Al pasar el electrón por ese punto de la red, por interacción coulombiana, el ión se sentirá atraído por ese electrón y la red se deformará localmente. Ya que las frecuencias de vibración de la red (de los fonones) son del orden de 10^{13} Hz y las velocidades de los electrones de conducción son del orden de 10^{16} Å/s , ocurrirá que cuando la red vuelva a su posición de equilibrio, el electrón

que la ha deformado se encontrará muy lejos, del orden de 10^3\AA , esto es del orden de varios cientos de parámetros de la red del ion que ha sido sacado de su posición de equilibrio. Esto es así porque las velocidades de los electrones de conducción en su movimiento aleatorio, velocidades de Fermi, que son del orden de $10^{16} \text{\AA}/s$, son muy grandes, entonces el tiempo que le toma a los electrones alejarse, es mucho menor a los tiempos de relajación de la red, ligados a las frecuencias de los fonones. Mientras que la red está deformada por sus cercanías pasan muchos otros electrones de conducción, que sienten una fuerza de atracción por la red, mayor que la que sentirían si ésta no estuviera deformada. En resumen, se puede establecer una cierta conexión, una cierta interacción atractiva entre los electrones de conducción vía los fonones. Esto es, un electrón de conducción deforma la red y un segundo electrón de conducción se siente atraído por esta deformación y en cierta manera “ligado” al primer electrón, el cual puede estar físicamente muy alejado del primero. Esta idea de como una interacción de corto alcance electrón-fonón, puede dar lugar a una interacción de largo alcance electrón-electrón, se debe a Fröhlich (1950) [55] y es la base de la teoría de la superconductividad.

Ahora veamos el papel que juega la interacción coulombiana repulsiva directa entre los electrones de conducción. Esta interacción decrece con $1/r^2$, siendo r la distancia entre los electrones, es decir que disminuye rápidamente con la distancia. Luego se tendrá que la interacción neta entre los electrones de conducción será la suma de estas dos interacciones una repulsiva, que es la que podríamos decir normal y otra, vía fonón, que es atractiva. La interacción neta será atractiva solamente cuando estemos haciendo el balance entre electrones cuya interacción coulombiana repulsiva es muy pequeña, debido a la gran separación que hay entre los electrones.

Luego, Cooper demostró que si se tienen dos electrones con una interacción atractiva neta, por muy pequeña que sea, el mar de Fermi de los electrones de conducción es inestable y se produce un estado ligado con momenta k y espines opuestos, llamado par de Cooper. Bardeen, Cooper y Schieffer escribieron un hamiltoniano cuántico para el sistema en cuestión y el estado fundamental formado por estos pares, de tal manera fueron capaces de desarrollar expresiones para la temperatura crítica superconductora; dedujeron la existencia de una banda prohibida de energía en los superconductores, tal que para romper un par de Cooper via la interacción con los fonones de la red, hay que suministrar una energía superior o igual a la de esa banda prohibida, y asimismo deducen el efecto isotópico.

Queda, por último, ver de dónde se obtiene la conducción eléctrica sin resistencia, es decir sin que los electrones de conducción cambien de momentum. Hay que señalar que el estado fundamental propuesto por la teoría BCS no está formado por un conjunto de pares de Cooper cualesquiera. Los pares no actúan independientemente unos de otros y para romper un par hay que suministrar energía (la correspondiente a la banda prohibida) de tipo térmico, subiendo la temperatura, o de tipo magnético, aplicando un campo magnético. Mientras que no se suministre una energía superior a la de la banda prohibida los electrones superconductores forman pares de Cooper de momentum constante. Esto es, conducen sin resistencia a no ser que se rompan los pares. Ahora bien, estos electrones se están moviendo en una red cristalina, que estará a una cierta temperatura, por debajo de la temperatura crítica, que no es suficiente para romper los pares. Por lo tanto, verán fonones e interaccionarán con ellos. Los pares están interrelacionados y el resto se acomoda para hacer posible que en su conjunto de k no varíe. Aquí se puede utilizar una imagen debida a Schieffer. Supongamos que tenemos un conjunto de esquiadores, la mitad hombres y la mitad mujeres, que bajan una pendiente cogidos de la mano, hombre con mujer (aquí tenemos los pares de Cooper), pero estas parejas no bajan cada uno por su lado, sino que lo hacen al mismo tiempo y de alguna manera enlazados, de tal manera que si algún miembro de la pareja se encuentra en el camino un obstáculo (un fonón), siempre que no sea muy importante (de energía menor que la de la banda prohibida) el conjunto de pares aguantarán el golpe y harán posible que se siga bajando sin perder velocidad, sin cambiar k , sin resistencia. Esta interacción se puede representar con el diagrama de Feynman de la Figura 3.1.

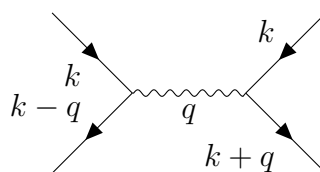


FIGURA 3.1: Diagrama de Feynman de la interacción electrón-fonón-electrón: Cuando el primer electrón llega a un punto de la red y la atrae, emite un fonón. El segundo electrón absorbe este fonón y queda acoplado al primer electrón.

Los electrones que participan en esta interacción son los de la banda de conducción, con energías del orden de unos pocos electrón voltio. Los fonones disponibles tienen unas energías que son como máximo del orden de la energía de Debye. Dado que la temperatura de Debye suele ser del orden de algo más de 100K, se tiene que las energías de los fonones disponibles son de unos pocos milielectrón voltio, esto es muy pequeña comparada con la de los electrones. Se tiene que la capa de los

electrones de conducción en la esfera de Fermi que intercambian fonones, según este esquema es una franja muy estrecha.

Si llamamos $\hbar k, \hbar k'$ y $\hbar k_1, \hbar k'_1$, los momenta de los electrones antes y después de la interacción la ley de conservación del momentum nos dice que

$$\hbar k_1 + \hbar k'_1 = \hbar k + \hbar k' = \hbar K, \quad (3.1)$$

Donde hemos llamado K al momentum del centro de masas de los electrones. Conviene aprovechar este punto para indicar el convenio habitual en cuanto al signo de la energía de los electrones. Se toman como energías positivas los valores de la energía superiores a la energía de Fermi y como energías negativas los valores inferiores a la energía, E_F , de Fermi. Es decir que ϵ_k será negativa si k está dentro de la superficie de Fermi y positiva en caso contrario. Está claro que los únicos electrones que pueden intervenir en todo este proceso son los que tienen energías próximas a la de Fermi dado que solamente estos electrones pueden tener estados libres accesibles sin violar el principio de exclusión de Pauli. Por lo tanto, estamos solamente considerando como candidatos a electrones superconductores unos pocos de todos los de la esfera de electrones de conducción de Fermi, aquellos que están en una estrecha franja de espesor $\hbar\omega_D$ donde ω_D es la frecuencia de Debye, por lo tanto del orden de unos pocos meV de la energía de Fermi. En esta situación se conserva el momentum $\hbar K$ del centro de masas de los dos electrones. En la Figura 3.2 se representa gráficamente todo lo que acabamos de decir, además se observa en esta figura que son, dentro de la estrecha franja, muy pocos los electrones que cumplen todas las condiciones y que por lo tanto pueden ser candidatos a formar pares de Cooper. Solamente los electrones cuyos momenta caen en la intersección de las dos capas esféricas son los posibles electrones superconductores. Es fácil ver que si disminuimos el valor del momentum del centro de masas del sistema la intersección aumentará y se hará máxima si hacemos $K = 0$, donde toda la franja está formada por posibles pares de Cooper. Es decir, los pares de Cooper se forman con electrones de momenta opuestos, como ya habíamos anticipado unas líneas más arriba, esto es $k, -k$. Además, este argumento que acabamos de desarrollar está apoyado en que la energía del sistema disminuye al ir formándose pares, lo que se puede demostrar, pero no de una manera fácil.

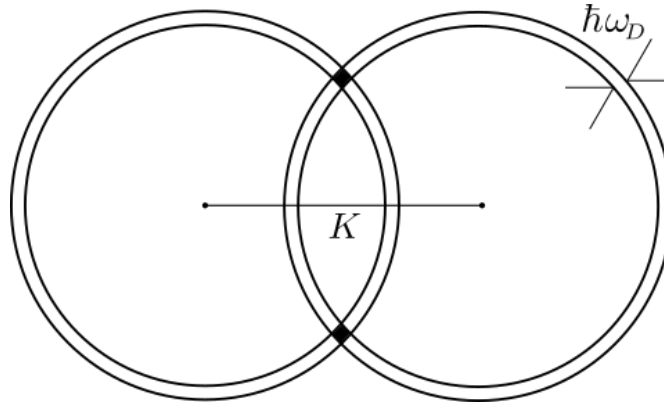


FIGURA 3.2: Construcción geométrica de los posibles electrones candidatos para formar pares de Cooper, siendo $\hbar K$ el momentum del centro de masas.

Otro aspecto de los señalados anteriormente, que podemos abordar ahora, es que los pares estaban formados por electrones no sólo con momenta opuestos, sino también con espines opuestos, esta última característica es ahora muy fácil de tratar, dado que los electrones son fermiones, es decir cumplen el principio de exclusión de Pauli y tienen funciones de onda antisimétricas. Se puede demostrar que la parte orbital (es decir, olvidándose de la parte de espín) de la función de onda de los pares de Cooper, depende tan sólo del módulo del momentum. Por lo tanto, frente al intercambio de la posición de los dos electrones del par se tienen una función simétrica. Luego la parte de espín debe ser antisimétrica, es decir los espines de la pareja son opuestos. Se tiene que un par de Cooper está formado por dos electrones tal que $k \uparrow, -k \downarrow$.

En este punto surge uno de los peligros típicos de la teoría BCS, que pone de manifiesto la gran cantidad de sutilezas que encierra. Dado que un par de Cooper es una entidad cuyo espín es cero, como los bosones, es fácil caer en la tentación de tratar a los pares de Cooper como bosones. Además hemos indicado que un número creciente de pares de Cooper es energéticamente favorable. Ahora bien, el principio de Pauli sigue vigente: Así, el estado formado, por ejemplo, por $k \uparrow, -k \downarrow$ no puede estar ocupado por más de un par de electrones al mismo tiempo. Además, los operadores con los que se construye el hamiltoniano de la teoría BCS, no siguen las reglas de conmutación de los operadores de bosones. Resulta de todas formas llamativo y conviene resaltarlo que la electrodinámica bosónica reproduce muy bien el comportamiento superconductor, por ejemplo la teoría clásica de la superconductividad de London se puede deducir de un gas cargado de bosones y de allí se puede extraer de una manera natural el efecto Meissner [56].

Pasaremos a continuación a describir de la manera más sencilla posible la función de onda del estado fundamental superconductor y algunas de las expresiones de la teoría BCS.

La función de onda del estado fundamental de N electrones, según la propone la teoría BCS, es el producto de funciones de onda de pares convenientemente antisimetrizadas, que se puede representar por:

$$\phi(1, 2, \dots, N) \propto \phi(1, 2)\phi(3, 4)\dots\phi(N-1, N). \quad (3.2)$$

Si no escribimos explícitamente la parte de espín y sólo lo hacemos con la parte orbital tendríamos

$$\phi(1, 2, \dots, N) \propto \sum_{k_1} \sum_{k_2} \dots \sum_{k_3} g_{k_1} \dots g_{k_{N/2}} e^{i(k_1 r_1 - r_2 k_2 + \dots + k_{N/2} r_{N-1} - k_{N/2} r_N)}, \quad (3.3)$$

Donde cada término de esta función de onda describe una configuración donde los N electrones se agrupan en $N/2$ pares que son

$$(k_1, -k_1) \dots (k_{N/2}, -k_{N/2}). \quad (3.4)$$

La parte de espín es inmediata cada electrón de cada par tiene espines opuestos. Como vemos la función de onda es una función complicada que abarca todos los pares relacionados entre ellos. También se puede escribir de una manera más compacta como:

$$\phi = \prod_k \phi_k. \quad (3.5)$$

Antes de continuar merece la pena señalar algún otro aspecto de los pares de Cooper, estos pares están fuertemente relacionados entre sí, de tal manera que se puede decir que del orden de un millón de pares tienen sus centros de masa dentro del espacio en el que se extiende un par dado, esto es los pares de electrones que forman un par de Cooper están muy alejados uno del otro, estando fuertemente correlacionados unos pares con otros. Se puede demostrar, que la disminución de la energía en la fase superconductora respecto al estado normal, debida a la

interacción entre pares, depende de cómo se elijan esos pares. El conjunto de pares de Cooper no son independientes unos de otros, están muy correlacionados.

Otro punto que hay que aclarar en lo anterior es que estamos considerando el caso en que no tenemos corriente eléctrica neta, ya que los electrones apareados tienen momentum total cero. Los estados portadores de corriente superconductora son aquellos en que los pares tienen momenta que serán $(k + \frac{q}{2} \uparrow, -k + \frac{q}{2} \downarrow)$ y los electrones tendrán una velocidad de arrastre neta que será

$$v_a = \frac{\hbar q}{2m}. \quad (3.6)$$

Otro aspecto importante de la teoría BSC es que predice la existencia de una banda prohibida de energía Δ , la cual se puede medir experimentalmente y que está relacionada con la temperatura crítica por la ecuación BCS. Este parámetro Δ es el parámetro crucial de la teoría BCS que acompaña la aparición del estado superconductor.

Hay que resaltar que esta banda reúne unas características muy particulares, por lo pronto se diferencia claramente de las bandas prohibidas que juegan un papel importante en sólidos, especialmente en los semiconductores. En superconductores tenemos una banda prohibida que está situada en la banda de conducción y que tiene una marcada dependencia con la temperatura. Asimismo, mientras que en un semiconductor se necesita excitar por encima de la banda prohibida a los electrones para tener conducción eléctrica, en un superconductor se tiene la supercorriente sin necesidad de tener estados excitados, se tiene conducción eléctrica por debajo del nivel de Fermi, esto es por debajo de la banda prohibida que existe en la banda de conducción.

Este parámetro Δ aparece en la sencilla e importante relación que se obtiene en la teoría BCS

$$2\Delta(0) = 3.52k_B T_c, \quad (3.7)$$

Donde T_c es la temperatura crítica superconductora.

3.3. Cuantización del flujo magnético y efecto tunel Giaver

En la teoría de Ginzburg-Landau [57] de las transiciones de fase se introduce el concepto de parámetro de orden, que es una magnitud que aparece acompañando a la transición. Un ejemplo típico de parámetro de orden es la imanación de saturación, que es la magnitud que aparece cuando se tiene la transición de fase del estado paramagnético al ferromagnético. El modelo macroscópico de la superconductividad está basado en la hipótesis de que existe una función de onda macroscópica $\psi(r, t)$ que describe el comportamiento del ensemble completo de electrones superconductores y que es el parámetro de orden de la transición superconductora, tal que su módulo al cuadrado nos da la densidad de electrones superconductores que aparecen al pasar el metal del estado normal al superconductor. En el estado normal, el parámetro de orden (densidad de electrones superconductores) se desvanece. Por supuesto, esta hipótesis puede ser justificada por la teoría microscópica de la superconductividad (Teoría BCS). Esta teoría se basa en la idea de que en metales superconductores existe una fuerza atractiva entre los electrones cercanos al nivel de Fermi. A temperaturas bajo la temperatura crítica T_c , esta fuerza atractiva crea un nuevo estado cuántico diferente del mar de Fermi de un metal normal. Una pequeña porción de los electrones cercanos al nivel de Fermi están ligados a pares de Cooper. En el caso más simple, el movimiento interno de los pares no tiene momentum angular orbital (estados simétricos) y consecuentemente el principio de Pauli requiere que los dos espines sean opuestos. Contrario a ligar dos átomos a una molécula, el estado orbital del par de Cooper tiene un radio mucho mayor, típicamente entre 10nm y $1\mu\text{m}$, de manera que pares individuales se solapan fuertemente en espacio y por lo tanto, la ligadura resulta cooperativa. En particular, la energía de ligadura de cualquier par depende de cuantos otros pares se hayan condensado y, más aún, el movimiento del centro de masas de los pares está fuertemente correlacionado tal que cada par reside en el mismo estado con el mismo movimiento de centro de masas. Es este estado el que describimos con una función de onda macroscópica y que le da al sistema sus propiedades superfluídicas. Por ejemplo, el movimiento del centro de masas puede ser descrito por la función de onda

$$\psi(r, t) = \psi_0 e^{i\theta(r, t)} = \psi_0 e^{ik_s \dot{r} - i\omega t}, \quad (3.8)$$

Donde cada par tiene el mismo momentum $\hbar k_s$ o velocidad de par $v_s = \hbar k/m$. Además, se cumple que

$$n_s = |\psi|^2, \quad (3.9)$$

Donde n_s es la densidad de electrones superconductores.

Por otro lado, sabemos que la cantidad de movimiento de una partícula de masa m^* y carga e^* en presencia de un campo magnético representado por su potencial vectorial A , se escribe como

$$\mathbf{p} = -i\hbar\nabla\psi(r, t) = \hbar\nabla\phi = m^*\mathbf{v} + \frac{e^*}{c}\mathbf{A}. \quad (3.10)$$

Si tenemos una densidad de partículas, todas ellas teniendo el mismo momentum \mathbf{p} podemos escribir $n_s\mathbf{p} = n_s(m^*\mathbf{v} + \frac{e^*}{c}\mathbf{A})$.

Recordando la expresión general de la densidad de corriente eléctrica en función de la densidad de portadores, de la carga y de la velocidad promedio se pueden escribir

$$\mathbf{J} = n_s e^* \mathbf{v}. \quad (3.11)$$

Que en nuestro caso será

$$\hbar\nabla\phi = \frac{m^*}{n_s e^*} J + \frac{e^*}{c} A. \quad (3.12)$$

Con esta expresión estamos preparados para demostrar la cuantización del flujo magnético en superconductores, para ellos basta con recordar algo trivial, como es que el parámetro de orden superconductor sólo puede tener un único valor en cada punto, es decir, la densidad de electrones superconductores debe ser única en cada punto, esta simple consideración se materializa en que podemos escribir

$$\phi(2\pi) - \phi(0) = n2\pi. \quad (3.13)$$

Recordando la definición de circulación y de gradiente, y siendo C un camino cerrado, la expresión anterior la podemos escribir como

$$\oint_C \nabla \phi dl = n2\pi. \quad (3.14)$$

Si ahora suponemos que este camino C está en el interior de un superconductor, alejado de los bordes y rodeando a un hueco, como se representa en la Figura 3.3 y suponemos que tenemos aplicado un campo magnético a este superconductor, se tiene

$$\oint_C \left(\frac{m^*}{\hbar n_s e^*} J + \frac{e^*}{\hbar e} A \right) dl = n2\pi. \quad (3.15)$$

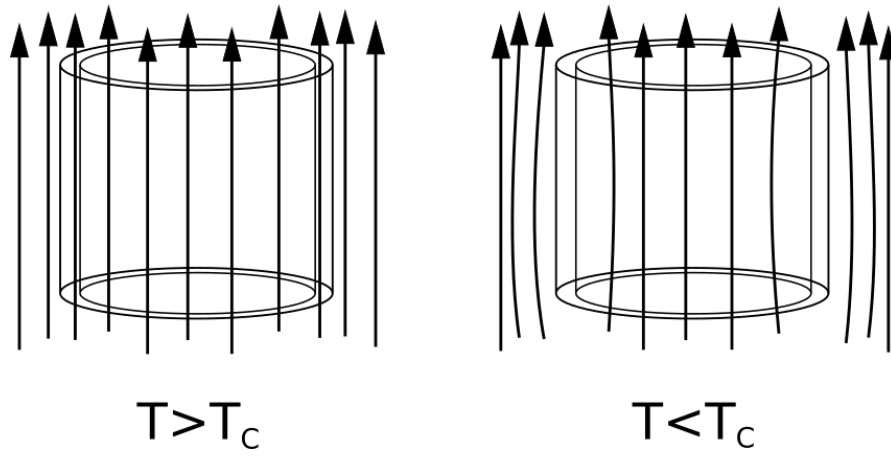


FIGURA 3.3: Cuantización del flujo magnético

Dado que estamos en un camino interior al superconductor y allí no existe corriente (las únicas corrientes que existen en una situación como la que estamos describiendo, están apantallando el campo magnético y están situadas cerca de los bordes tanto de la cavidad como de la superficie del material superconductor), tendremos

$$\oint_C A dl = \frac{n\hbar c}{e^*}. \quad (3.16)$$

Recordando el teorema de Stokes se tiene

$$\oint_C A dl = \iint_S B ds = \Phi. \quad (3.17)$$

Que en nuestro caso será $\Phi = n\Phi_0$ expresión que nos indica que el flujo magnético que encierra la cavidad es un número entero de un flujo elemental conocido con el nombre de fluxoide y cuyo valor es

$$\Phi_0 = \frac{hc}{2e} = 2,0710^{-7} gauss\ cm^2. \quad (3.18)$$

Siendo e^* la carga del portador de corriente, el par de Cooper $e^* = 2e$.

Este efecto fue encontrado experimentalmente de forma simultánea en 1961 por Deaver-Fairbanks [58] y por Doll-Näbauer [59].

El efecto túnel es un efecto típico del carácter cuántico de los electrones, desde el punto de vista de la física clásica es completamente imposible que se produzca el efecto que vamos a discutir.

Los electrones se pueden representar por funciones de onda, de tal manera que existe una cierta probabilidad de que un electrón pueda ir de un metal a otro atravesando una barrera aislante estrecha, que puede ser vacío o un óxido. La función de onda del electrón decae de una manera exponencial fuera de la superficie del metal, la amplitud de la onda no es totalmetne nula fuera del metal, es como si el electrón se desparramase fuera de la superficie. Si situamos un metal junto al otro, separados tan sólo por una barrera, como puede ser, por ejemplo, el óxido de la superficie, existe una probabilidad pequeña, pero no nula de que el electrón atraviese ese túnel y aparezca al otro lado, en el otro metal.

Antes de seguir hay que hacer notar que la energía necesaria para hacer pasar un electrón que está en el nivel de Fermi de un metal al vacío (función de trabajo del metal) es mayor que la energía necesaria para transferir ese electrón a un aislante.

Por razones de simplicidad vamos a hacer toda la discusión siguiente, salvo cuando se diga expresamente lo contrario, para temperatura de 0K. La Figura 3.4 nos indica la situación entre dos partes del mismo metal separadas por un aislante. Todos los estados por debajo de la energía de Fermi están ocupados, mientras que todos los estados por encima de E_F están vacíos.

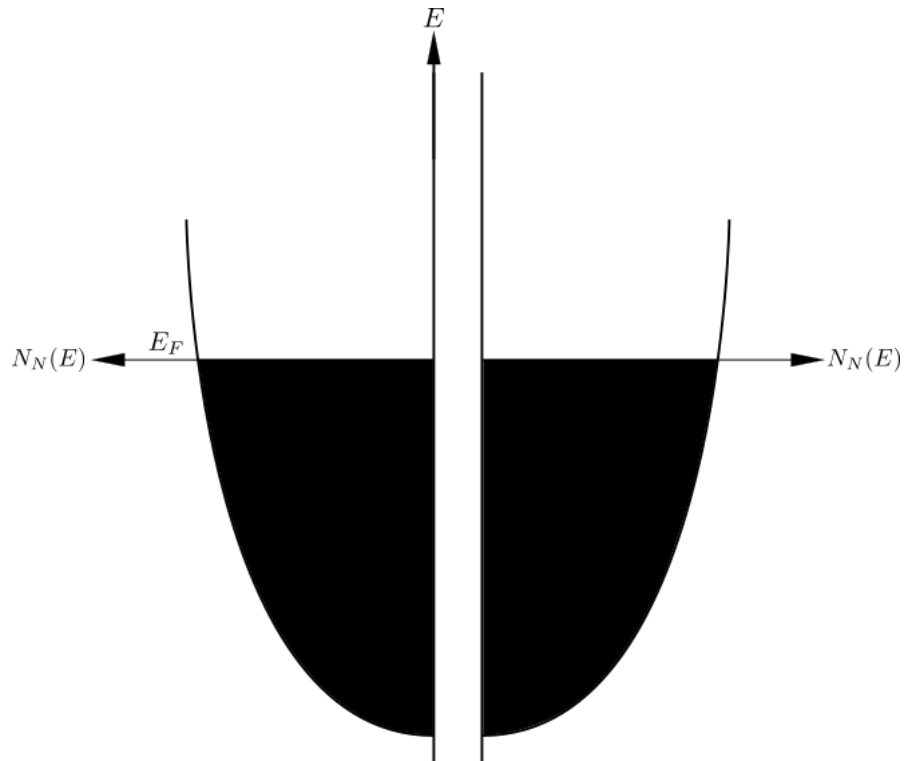


FIGURA 3.4: Diagrama de energía de una unión metal-aislante-metal en la que no puede haber efecto túnel: En este diagrama ambos lados de la barrera tienen los mismos niveles de energía ocupados. Por lo tanto, no puede haber efecto túnel, porque las transiciones deben ser horizontales y no puede haber dos electrones ocupando el mismo estado.

Para que se pueda tener efecto túnel hacen falta dos condiciones. La primera es que, como es lógico, los electrones solamente pueden ir de un estado ocupado a un estado desocupado y la segunda es que se tiene que conservar la energía, es decir que las transiciones, en la gráfica, tienen que ser horizontales. Por lo tanto en la situación de la Figura 3.4 no tendremos efecto túnel. No se pueden tener transiciones horizontales al no existir estados vacíos. Todos los estados en el mismo nivel de energía, a ambos lados de la barrera, están ocupados.

Si aplicamos una diferencia de potencial constante a la barrera lo que estamos haciendo es aumentando la energía de los electrones de un lado de la barrera respecto al otro, y entonces tenemos la posibilidad de que se tenga corriente por efecto túnel, Figura 3.5.

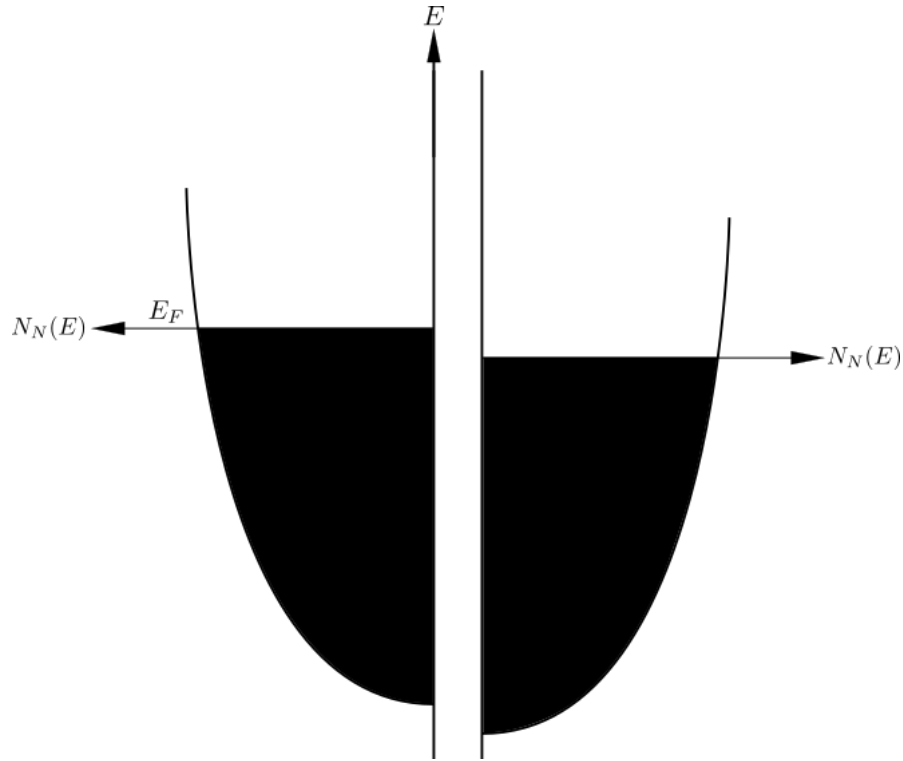


FIGURA 3.5: Diagrama de energía de una unión metal-aislante-metal en la que puede haber efecto túnel: En este diagrama los electrones de uno de los lados de la barrera ocupan niveles de energía más altos que los del otro lado. Por lo tanto, estos electrones pueden pasar al otro lado de la barrera y ocupar los estados que en ese lado se encuentran vacíos.

La intensidad de esta corriente túnel depende de varios parámetros. Por ejemplo, a mayor diferencia de potencial aplicada mayor corriente. Está claro que cuantos más estados tengamos en el nivel de Fermi mayor será la probabilidad de tener corriente túnel, lo cual puede indicar que quizás con experimentos de efecto túnel podemos obtener información sobre este importante parámetro y en general sobre la superficie de Fermi, pero como es de esperar la corriente túnel también depende de la anchura, altura y forma de la barrera y estos parámetros son muy difíciles de determinar, lo cual hace que en metales normales del efecto túnel se obtenga una información mucho menos rica de lo que se podía esperar. Ocurre todo lo contrario con el efecto túnel cuando uno de los dos metales está en estado superconductor, como pasaremos a ver a continuación.

La existencia de una banda de energía en el estado superconductor [3.6](#) hace que el efecto túnel en una estructura formada por superconductor-aislante-metal en estado normal, tenga características especiales (Giaver, 1960 [[60](#)]). Es claro que necesitamos previamente disponer de electrones normales por encima de la banda

prohibida superconductora, esto es hay que romper pares de Cooper, como primera medida, es decir diferencias de potencial aplicadas menores que la banda prohibida no producirán efecto túnel. Esto es, diferencias de potencial aplicadas a la barrera no producen corriente túnel, salvo que vengán un valor umbral, que es precisamente el ancho de la banda prohibida. De entrada ya tenemos una muy importante propiedad del efecto túnel superconductor, que nos permite medir la banda prohibida superconductora y medir la variación de esta banda con la temperatura.

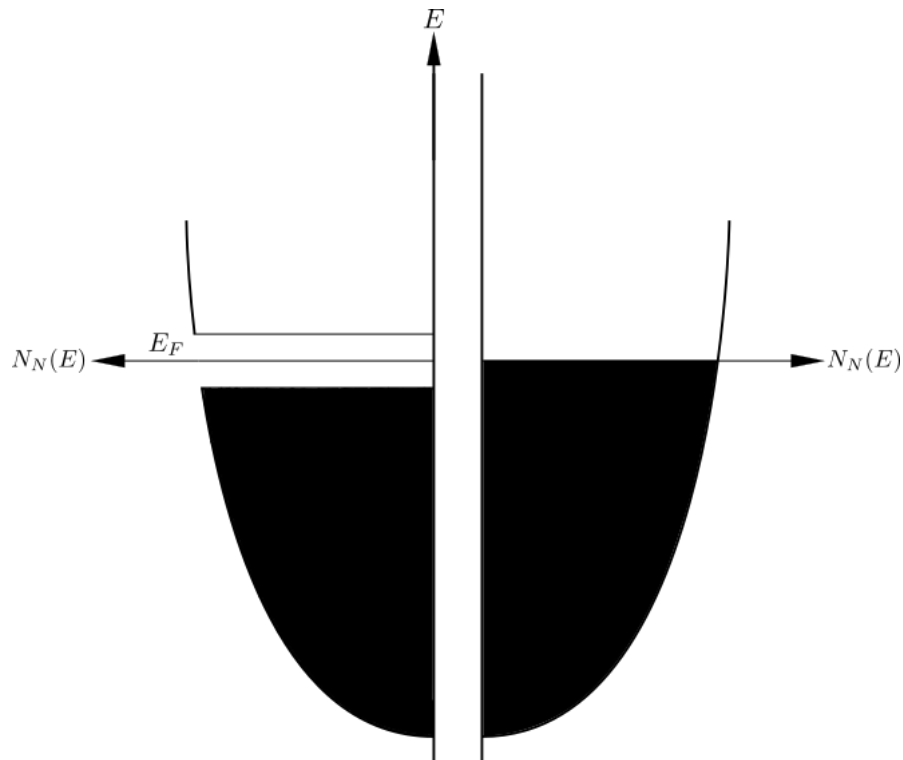


FIGURA 3.6: Diagrama de energía de una unión superconductor-aislante-metal en la que puede haber efecto Giaver: En este diagrama, al producirse excitaciones que lleven electrones por encima de la banda prohibida, rompiendo pares de Cooper, los electrones excitados podrían pasar al otro lado de la barrera por efecto túnel.

3.4. Efecto Josephson

El efecto Josephson fue postulado teóricamente por Josephson (1962) [61] y comprobado experimentalmente por P.W. Anderson y Rowell (1963) [62] y por Shapiro (1963) [63], casi simultáneamente. Este es un efecto túnel de pares de Cooper entre superconductores, mientras que el efecto túnel tratado en las líneas anteriores es túnel de electrones normales entre superconductores o entre un metal normal y

un superconductor. En concreto la sugerencia de Josephson es que puede existir efecto túnel entre dos superconductores que se encuentren separados por una barrera aislante (en principio más delgada que las tratadas en el efecto túnel Giaver), donde la corriente túnel sea exclusivamente de pares de Cooper sin que se tenga una diferencia de potencial entre ambos lados de la barrera.

Se va a seguir la deducción de Feynman [64] por su sencillez y claridad. Supongamos que tenemos un superconductor separado en dos partes por un aislante lo suficientemente estrecho como para que la función de onda superconductora a un lado de la barrera se sobrelape con la del otro lado. Sean ψ_1 y ψ_2 las funciones de onda superconductoras a los dos lados de la barrera (1) y (2).

El tunelamiento de pares del lado (2) al lado (1) aumenta la amplitud ψ_1 de la función de onda de los pares en el lado (1), es decir, aumenta la cantidad de pares de Cooper en el lado (1). Supongamos que el ritmo de crecimiento de ψ_1 es proporcional a ψ_2 , amplitud de la función de onda de los pares en el lado (2). Podemos escribir el ritmo de cambio de ψ_1 de la forma $A\psi_2$ donde A es una característica de la barrera y nos da información de la probabilidad de transferencia de pares del lado (2) al lado (1).

Podemos escribir la ecuación de Schrödinger para el lado superconductor (1) teniendo en cuenta esto último, como

$$\frac{-\hbar}{i} \frac{\partial \psi_1}{\partial t} = E_1 \psi_1 + A \psi_2, \quad (3.19)$$

Donde E_1 es la energía del estado más bajo de energía del superconductor del lado (1).

Análogamente, podemos escribir para el superconductor del lado (2)

$$\frac{-\hbar}{i} \frac{\partial \psi_2}{\partial t} = E_2 \psi_2 + A \psi_1. \quad (3.20)$$

Escribiendo explícitamente la función de onda superconductora, $\psi_i = \sqrt{n_{s_i}} e^{i\varphi_i}$, donde, como ya vimos, n_{s_i} es la densidad de electrones superconductores en el lado (i).

Por lo tanto las ecuaciones anteriores pueden ser escritas como

$$\frac{-\hbar}{i} \frac{1}{2\sqrt{n_{s_1}}} \frac{\partial n_{s_1}}{\partial t} + \hbar \frac{\partial \varphi_1}{\partial t} \sqrt{n_{s_1}} = E_1 \sqrt{n_{s_1}} + A \sqrt{n_{s_2}} e^{i(\varphi_2 - \varphi_1)} \quad (3.21)$$

$$\frac{-\hbar}{i} \frac{1}{2\sqrt{n_{s_2}}} \frac{\partial n_{s_2}}{\partial t} + \hbar \frac{\partial \varphi_2}{\partial t} \sqrt{n_{s_2}} = E_2 \sqrt{n_{s_2}} + A \sqrt{n_{s_1}} e^{i(\varphi_1 - \varphi_2)}. \quad (3.22)$$

Si ahora igualamos las partes reales y las partes imaginarias de estas ecuaciones tenemos

$$\frac{\partial \varphi_1}{\partial t} = \frac{j_0}{2n_{s_1}} \cos(\delta) + E_1/\hbar \quad (3.23)$$

$$\frac{\partial \varphi_2}{\partial t} = \frac{j_0}{2n_{s_2}} \cos(\delta) + E_2/\hbar \quad (3.24)$$

$$\frac{\partial n_{s_1}}{\partial t} = -j_0 \sin(\delta) \quad (3.25)$$

$$\frac{\partial n_{s_2}}{\partial t} = j_0 \sin(\delta), \quad (3.26)$$

Donde $\delta = \varphi_2 - \varphi_1$ y $j_0 = \frac{2A}{\hbar} (n_{s_1} n_{s_2})^{1/2}$. En lo que sigue, asumiremos que se tiene el mismo superconductor en ambos lados, así que tomaremos $n_{s_1} = n_{s_2}$. Entonces:

$$\frac{\partial \delta}{\partial t} = \frac{\partial \varphi_2}{\partial t} - \frac{\partial \varphi_1}{\partial t} = (E_2 - E_1)/\hbar \quad (3.27)$$

$$j = \frac{\partial n_{s_2}}{\partial t} = -\frac{\partial n_{s_1}}{\partial t} = j_0 \sin(\delta). \quad (3.28)$$

De aquí salen directamente las relaciones de Josephson para corriente y voltaje:

$$V_J = \frac{\hbar}{2e} \frac{\partial \delta}{\partial t} \quad (3.29)$$

$$I_J = I_0 \sin(\delta), \quad (3.30)$$

Donde el voltaje V_J es la diferencia de potencial entre los dos extremos de la unión de Josephson, e I_J es la supercorriente que fluye a través de ésta.

Existe una clara diferencia entre este efecto túnel y el considerado al principio. En este caso de efecto Josephson tenemos túnel de pares de Cooper, mientras que

en el caso anterior el túnel era de electrones individuales. En el efecto Josephson son bastante estrechas del orden o menores que la longitud coherente (tamaño de los pares de Cooper), en realidad el aislante actúa como un mal superconductor, las funciones de onda de ambos lados se pueden solapar, existiendo una diferencia de fase a ambos lados de la barrera, y como resultado de todo esto se establece una corriente continua a través de la barrera. En realidad, se puede demostrar que el mínimo de energía se alcanza cuando las fases se igualan y por lo tanto no se tiene corriente a través de la barrera, pero basta con aplicar una corriente de una fuente externa, siempre menor que I_0 , para que las fases dejen de ser iguales y si esta desigualdad no varía con el tiempo, se tiene a través de la barrera una corriente constante sin que se tenga caída de potencial. No hace falta colocar un óxido, o un aislante, para que actúe de barrera, ya que se puede utilizar un estrechamiento en el superconductor, producido mediante una técnica conocida como fotolitografía, o cualquier otra técnica que nos produzca que una parte del superconductor esté unida a otra mediante un estrangulamiento lo suficientemente estrecho como para ser una unión débil. También se pueden obtener este tipo de uniones débiles con contactos entre superconductores de tipo puntual, o bien separando dos superconductores por una capa delgada de un metal en estado normal. Como acabamos de mencionar el tamaño de los pares de Cooper es una indicación del orden de magnitud de esta unión débil.

Los órdenes de magnitud de los parámetros que intervienen en el efecto Josephson son, para una unión de 1mm^2 de área $R = 1\Omega$, $I_0 = 1\text{mA}$ y $\Delta = 1\text{meV}$. Normalmente las densidades de corriente a través de las uniones son del orden de un millón de veces menores que las densidades de corriente crítica superconductora en un superconductor. Es decir, en general, en un superconductor se tiene que pasar de la densidad de corriente crítica para hacer desaparecer la superconductividad, pero si el superconductor tiene en algún punto una unión débil de densidades de corriente un millón de veces menores hacen que se tenga caída de potencial en el paso de corriente por la unión.

Si hacemos pasar una corriente mayor que I_0 , aparece una diferencia de potencial y teniendo en cuenta que al mismo tiempo que este efecto túnel (Josephson) de pares podemos tener el efecto túnel normal (Giaver) de electrones, el resultado se puede ver en la Figura 3.7 donde se representa la curva característica I,V. Como sea la conexión en la realidad entre estos dos túneles depende de las características de la unión y del circuito exterior.

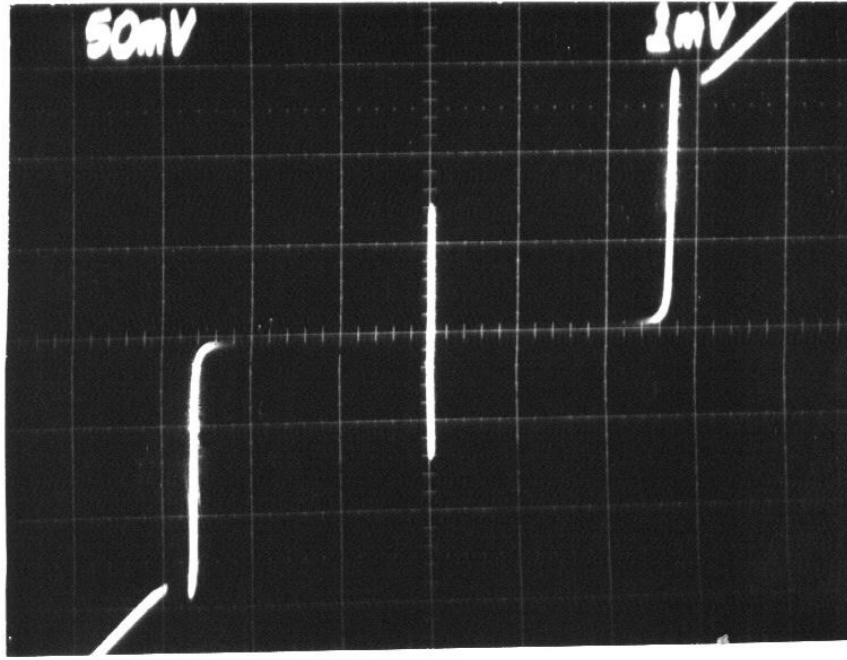


FIGURA 3.7: Curva característica I-V de una unión Josephson [65]: El eje vertical tiene una escala de $50\mu A$ y el eje horizontal $1mV$. La barra en $V = 0$ corresponde a la supercorriente producida por efecto Josephson. Para $V > 3mV$ se entra en el régimen ohmico de la unión de Josephson, el cuál se produce por el tamaño finito de la banda prohibida

Finalmente, hay que considerar lo que ocurre si aplicamos a la unión Josephson una diferencia de potencial externa constante, V , o lo que es lo mismo, tenemos una intensidad pasando por la barrera superior a I_0 . El cálculo es análogo al anterior, muy sencillo y nos conduce a que la intensidad a través de la barrera tiene la expresión

$$I = I_0 \sin((\varphi_2 - \varphi_1) + \omega t) = I_0 \sin(\delta + \omega t), \quad (3.31)$$

Donde $\omega = \frac{2eV}{\hbar}$. En realidad el punto de partida de esta deducción es la dependencia con el tiempo de la fase, una diferencia de potencial aplicada a la unión lo que hace es variar en el tiempo la fase, y el ritmo de variación de la fase viene dado por la ecuación $\frac{d\delta}{dt} = \frac{E_2 - E_1}{\hbar} = \frac{qV}{\hbar} = \frac{2eV}{\hbar}$.

Es decir, una diferencia de potencial constante aplicada a una barrera Josephson produce una corriente alterna de pares (una supercorriente), por ejemplo una diferencia de potencial del orden de $1\mu V$ da lugar a una corriente que oscila con una frecuencia de 484MHz. Además de esta corriente de pares, tenemos la corriente

debida al efecto túnel normal de los electrones individuales. Ahora podemos volver a la Figura 3.7 donde tendremos que hasta que se alcanza el valor I_0 tenemos paso de corriente por la unión sin caída de potencial. Una vez que $I > I_0$, entonces aparece un voltaje y nos situamos en un punto de la gráfica del efecto túnel de electrones normales (Giaver), tenemos una diferencia de potencial aplicada, luego existe túnel normal y además, esto no está representado en la gráfica, tenemos una supercorriente (corriente de pares de Cooper) que está oscilando.

3.5. Componentes de la corriente en las uniones de Josephson

La corriente en las uniones Josephson tiene tres componentes:

1. I_d , la corriente de desplazamiento: Como la corriente en un capacitor. La unión de Josephson forma un capacitor de placas paralelas superconductoras con un material aislante o un metal normal entre ellas, entonces podemos hablar de una corriente de desplazamiento I_d . La capacitancia C de este dispositivo está definida de la misma manera que en el estado normal: $C = \epsilon_r \frac{A}{4\pi d}$, donde ϵ_r es la constante dieléctrica relativa de la capa que separa a los dos superconductores, d la separación de los superconductores y A el área de los mismos.
2. I_n , la corriente ordinaria: Por los electrones individuales. Cuando la temperatura $T \neq 0$, siempre habrá movimiento térmico de cargas cuya energía es del orden de $k_B T$, donde k_B es la constante de Boltzmann. Cuando T es menor, pero cercano a la temperatura crítica T_c , la energía de acoplamiento de los pares de Cooper $E_g = 2\Delta$ es mucho menor a $k_B T$, lo cual resulta en la disminución de los pares de Cooper y el aumento de la concentración de electrones normales. Si el voltaje a través de la unión es mayor al asociado a la energía de la brecha $V_g = |\Delta_1 + \Delta_2|/e$, los pares de Cooper de un lado de la unión se rompen y uno de los electrones de cada uno de los pares disueltos pasa al otro lado, es decir, se produce un tunelamiento de electrones normales. Si la concentración de electrones individuales aumenta, el comportamiento de la unión tenderá a uno de tipo óhmico, es decir, la unión tenderá a comportarse como una resistencia.

3. I_s , la supercorriente: Por los pares de Cooper, se puede expresar en términos de una corriente crítica I_0 y la diferencia de fase entre las funciones de onda macroscópicas de las dos placas superconductoras, de manera que $I_s = I_0 \sin(\delta)$. La corriente crítica es un parámetro experimental importante del dispositivo que puede alterarse tanto por la temperatura como por un campo magnético aplicado.

3.6. Cuantización del oscilador armónico LC

En la mecánica Hamiltoniana clásica, la evolución dinámica de un sistema clásico está descrito por un conjunto de variables canónicas conjugadas $r = (q, p)$ de la siguiente manera:

$$\frac{dp}{dt} = -\frac{\partial H}{\partial q} \quad (3.32)$$

$$\frac{dq}{dt} = +\frac{\partial H}{\partial p}, \quad (3.33)$$

Donde el Hamiltoniano H es la suma de la energía potencial V y la energía cinética T , $H = T + V$.

El bracket de Poisson de dos funciones en coordenadas canónicas es

$$\{f, g\} = \sum_{i=1}^N \left(\frac{\partial f}{\partial q_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q_i} \right), \quad (3.34)$$

Donde p y q cumplen que:

$$\{q_i, q_j\} = 0; \quad \{p_i, p_j\} = 0; \quad \{q_i, p_j\} = \delta_{i,j}.$$

Paul Dirac introdujo el método de analogía clásica para la cuantización de sistemas físicos [66]. Este método consiste en cuantizar las teorías clásicas intentando mantener las estructuras formales de la teoría clásica en la mayor medida posible.

Dirac propuso la siguiente relación:

$$\{q, p\} \rightarrow \frac{1}{i\hbar} [\hat{q}, \hat{p}]. \quad (3.35)$$

Luego se demostró que esta relación no aplica para todo sistema físico, sino que es un caso especial de una relación más general. Sin embargo, para los casos a estudiar en este trabajo, sí se cumple.

El procedimiento a seguir para cuantizar circuito LC será:

1. Construir el Hamiltoniano clásico del sistema en términos de coordenadas canónicas.
2. Sustituir los observables por operadores cuánticos.
3. Forzar la relación de conmutación canónica

Un ejemplo de variables canónicamente conjugadas son la carga y el flujo magnético. Por esto, podemos cuantizar un oscilador armónico LC con la cuantización canónica.

La energía en un capacitor es $\frac{Q^2}{2C}$.

La energía en un inductor es $\frac{\phi^2}{2L}$.

Por lo tanto, el Hamiltoniano clásico del sistema es:

$$H = \frac{Q^2}{2C} + \frac{\phi^2}{2L}, \quad (3.36)$$

Donde tenemos que:

$$\frac{\partial H}{\partial Q} = \frac{Q}{C} = -L \frac{dI}{dt} = -\frac{d\phi}{dt} \quad (3.37)$$

$$\frac{\partial H}{\partial \phi} = \frac{\phi}{L} = I = \frac{dQ}{dt}. \quad (3.38)$$

Esto demuestra que ϕ y Q son coordenadas canónicas. Donde ϕ y Q son posición y momentum generalizados, respectivamente. Así que procedemos a sustituirlas por los operadores $\hat{\phi}$ y \hat{q} y escribimos el Hamiltoniano cuántico

$$\hat{H} = \frac{\hat{q}^2}{2C} + \frac{\hat{\phi}^2}{2L}, \quad (3.39)$$

Donde $[\hat{\phi}, \hat{q}] = i\hbar$

Esto, además, significa que la carga en el capacitor y el flujo en el inductor no pueden ser medidos simultáneamente, pues el orden de las medidas afecta el resultado. Finalmente, la frecuencia de resonancia de este oscilador es $\omega = \frac{1}{\sqrt{LC}}$ y los niveles de energía se encuentran separados por $\hbar\omega$

3.7. Qubits superconductores

Los qubits superconductores se basan en circuitos osciladores no lineales, hechos a partir de uniones Josephson [67]. Estos osciladores son anarmónicos, de manera que se pueda operar sobre un par específico de niveles de energía.

Primero, reescribimos el Hamiltoniano del circuito LC en términos de la cantidad de pares de Cooper y de la diferencia de fase en los extremos del inductor, en lugar de la carga y el flujo

$$\hat{H} = \frac{(2e)^2}{2C} \hat{n}^2 + \frac{\hbar^2}{(2e)^2 L} \frac{\hat{\delta}^2}{2}. \quad (3.40)$$

De aquí $\hat{q} = 2e\hat{n}$ y $\hat{\phi} = \frac{\hbar}{2e}\hat{\delta}$.

Ahora introducimos el término de la unión Josephson, para considerar un circuito LCJ (Inductor - Condensador - Unión Josephson). Para esto, primero hallemos la expresión de la energía almacenada en la unión:

$$\begin{aligned} E_J &= \int I_J V_J dt = \int I_0 \sin(\delta) \frac{\hbar}{2e} \frac{d\delta}{dt} dt \\ &= \frac{\hbar I_0}{2e} \int \sin(\delta) d\delta = -\frac{\hbar I_0}{2e} \cos(\delta) = -E_{J0} \cos(\delta). \end{aligned} \quad (3.41)$$

Donde $E_{J0} = \frac{\hbar I_0}{2e}$ se conoce como energía de Josephson. Con este término, el Hamiltoniano del circuito LCJ será:

$$\begin{aligned} \hat{H} &= \frac{(2e)^2}{2C} (\hat{n} - n_g)^2 + \frac{\hbar^2}{(2e)^2 L} \frac{(\hat{\delta} - \hat{\delta}_e)^2}{2} - \frac{\hbar I_0}{2e} \cos(\hat{\delta}) \\ &= E_C (\hat{n} - n_g)^2 + E_L \frac{(\hat{\delta} - \hat{\delta}_e)^2}{2} - E_{J0} \cos(\hat{\delta}) \end{aligned} \quad (3.42)$$

En este Hamiltoniano también hemos separado los términos n_g y δ_e , los cuales representan la carga inducida por voltaje en el capacitor C (isla qubit) y δ_e es la fase inducida por flujo sobre la unión Josephson.

Para describir el sistema en términos de la ecuación de Schrödinger en función de la diferencia de fase δ , se introduce $\hat{n} = -i\hbar \frac{\partial}{\partial \delta}$. Quedando la siguiente ecuación:

$$E_C(-i\hbar \frac{\partial}{\partial \delta} - n_g)^2 \psi + U(\delta)\psi = E\psi \quad (3.43)$$

$$U(\delta) = -E_{J0} \cos(\delta) + E_L \frac{(\delta - \delta_e)^2}{2} \quad (3.44)$$

Variando el término E_L , tenemos dos casos principales. El primero, cuando E_L tiende a cero, es decir, cuando la inductancia tiende a infinito y el circuito se convierte en uno CJ. En este caso, el potencial es de tipo coseno puro, y la solución toma la forma de funciones de Mathieu (las cuales se definen como la solución a esta ecuación). La dispersión de los niveles de energía, y su dependencia de n_g , dependerá del cociente E_{J0}/E_C . Por esto resulta de especial interés el caso en el que la capacitancia C es grande. El segundo caso principal es aquel en el que E_L es del mismo orden de magnitud que E_{J0} . En este caso, el potencial deja de ser periodico y describe una parábola modulada por una función sinusoidal. La forma del fondo de la parábola modulada y la estructura de los niveles de energía dependerán altamente del cociente E_L/E_{J0} y del flujo externo ϕ_e .

3.8. Arquetipos de qubits superconductores

Existen tres arquetipos principales de qubit superconductores. Ellos son los siguientes:

1. Qubit de carga

Si E_L tiende a cero, la carga almacenada en la isla superconductora entre el capacitor y la unión Josephson se puede usar como qubit. El potencial de este tipo de qubit es de forma de coseno. Los transmones son un tipo particular de qubit de carga.

2. Qubit de flujo

Si E_L es comparable con E_{J0} , el flujo a través del lazo formado por el inductor y la unión Josephson se puede usar como qubit. El potencial de este tipo de qubit es de forma cuártica.

3. Qubit de fase

Si se polariza la unión Josephson con una fuente de corriente, la fase en ambos extremos de la unión Josephson se puede usar como qubit. El potencial de este tipo de qubit es de forma cúbica.

3.9. Transmiones

Los transmiones son un tipo de qubit de carga derivado capacitivamente para hacerlo insensible a las fluctuaciones de carga. La manera de interactuar con los transmiones es acoplándolos a un resonador. Tratando el transmión como un sistema de dos niveles y el resonador como un oscilador monomodo, podemos modelar este sistema con el Hamiltoniano de Jaynes-Cummings [67, 68], el cuál describe un átomo o un átomo artificial que interactúa con un oscilador armónico cuántico:

$$\hat{H} = \hat{H}_q + \hat{H}_{qr} + \hat{H}_r = -\frac{1}{2}\hbar\omega_q\sigma_z + \hbar g\sigma_x(a + a^\dagger) + \hbar\omega_r(a^\dagger a + \frac{1}{2}), \quad (3.45)$$

Donde ω_q es la frecuencia de resonancia del qubit, g es la constante de acoplamiento qubit-oscilador, y ω_r es la frecuencia de resonancia del resonador. El operador a es el operador de aniquilación bosónico del oscilador y su efecto al ser aplicado al estado del sistema es aniquilar fotones del resonador. Similarmente, a^\dagger es el operador de creación bosónico del oscilador y su efecto al ser aplicado al estado del sistema es crear fotones en el resonador.

$$a |n\rangle = \sqrt{n} |n-1\rangle \quad (3.46)$$

$$a^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle. \quad (3.47)$$

Aquí n es la cantidad de fotones en el resonador. De estas ecuaciones podemos deducir el operador de número, el cuál es:

$$a^\dagger a |n\rangle = a^\dagger \sqrt{n} |n-1\rangle = \sqrt{(n-1)+1} \sqrt{n-1} |(n-1)+1\rangle = n |n\rangle. \quad (3.48)$$

En cuanto a los operadores del qubit, tenemos el operador de aniquilación fermiónico σ_- , el cuál disminuye el nivel de energía del qubit, y el operador de creación fermiónico $\sigma_+ = \sigma_-^\dagger$, el cuál aumenta el nivel de energía del qubit.

$$\sigma_- = |0\rangle\langle 1| \quad (3.49)$$

$$\sigma_+ = |1\rangle\langle 0|. \quad (3.50)$$

También tenemos el operador σ_z , que es el análogo del operador de número para el qubit y el operador σ_x que hace un *bit-flip*.

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \sigma_- \sigma_+ - \sigma_+ \sigma_- \quad (3.51)$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \sigma_- + \sigma_+. \quad (3.52)$$

El término de interacción del Hamiltoniano de Jaynes-Cummings lo podemos descomponer en el término de Jaynes-Cummings, y el término anti-Jaynes-Cummings.

$$\hat{H}_{qr} = \hat{H}_{qr}^{JC} + \hat{H}_{qr}^{AJC} = g(\sigma_+ a + \sigma_- a^\dagger) + g(\sigma_+ a^\dagger + \sigma_- a). \quad (3.53)$$

El término H_{qr}^{AJC} describe oscilaciones de alta frecuencia. En los sistemas típicos, estas oscilaciones están en el orden de los teraherzios (THz) y tienen amplitudes muy pequeñas. Debido al orden de las frecuencias de estas oscilaciones, no las podemos medir con la tecnología utilizada para la computación cuántica. Las mediciones en el régimen de los teraherzios son un tema de investigación activo en el que todavía nos estamos adentrando [69]. Por esto y la amplitud despreciable de estas oscilaciones, es común hacer la aproximación de onda rotante, con la cual se aplica una transformación al Hamiltoniano de manera que desaparezca el término que contiene la contribución de las altas frecuencias H_{qr}^{AJC} . Trabajaremos con el Hamiltoniano de Jaynes-Cummings bajo esta aproximación. Además, también usaremos unidades naturales, es decir, que tendremos que $\hbar = 1$ y $c = 1$, donde \hbar es la constante reducida de Planck y c es la velocidad de la luz. En estas unidades la energía se mide en Hz.

$$\hat{H}_{RWA} = \hat{H}_r + \hat{H}_q + \hat{H}_{qr} = \omega_r a^\dagger a - \frac{1}{2} \omega_q \sigma_z + g(a \sigma_+ + a^\dagger \sigma_-). \quad (3.54)$$

En este Hamiltoniano tenemos el término $\hat{H}_r = \omega_r a^\dagger a$, correspondiente a la energía del resonador. Este término da la cantidad de fotones de frecuencia ω_r en el resonador y por lo tanto, la energía de este subsistema (recordemos que elegimos $\hbar = 1$). En el primer Hamiltoniano que presentamos también había un término $+\frac{1}{2}\omega_r$, este término se puede descartar, pues sólo representa un término constante de energía y como es una constante por la identidad, sólo actúa como una fase global en la evolución del sistema, así que no afecta las probabilidades. El término $\hat{H}_q = -\frac{1}{2}\omega_q \sigma_z$ representa la energía del qubit. ω_q es la diferencia de energía entre los dos niveles del qubit y el nivel cero de energía se ha tomado tal que el espectro del qubit esté centrado alrededor del cero. Así, el qubit tiene energía $-\frac{1}{2}\omega_q$ cuando está en el estado $|0\rangle$ y energía $\frac{1}{2}\omega_q$ cuando está en el estado $|1\rangle$. Finalmente, el término de interacción $H_{qr} = g(a\sigma_+ + a^\dagger\sigma_-)$ indica que las emisiones en el resonador corresponden a absorciones del qubit y viceversa. La manera en la que interactúan el resonador y el qubit es intercambiando energía.

3.10. Hamiltonianos multiqubit de transmones

Cuando tenemos más de un qubit acoplado al mismo resonador, estos interactúan virtualmente a través de emisiones y absorciones con el resonador [67]. Omitiendo el término del oscilador, esto se refleja en el Hamiltoniano, de forma general, de la siguiente manera:

$$\hat{H} = \hat{H}_q + \hat{H}_{qr} + \hat{H}_{qq} = -\frac{1}{2} \sum_i \epsilon_i \sigma_{zi} + \sum_i g_i \sigma_{xi} (a + a^\dagger) + \frac{1}{2} \sum_{i,j;\nu} \lambda_{\nu,ij} \sigma_{\nu i} \sigma_{\nu j}. \quad (3.55)$$

Por simplicidad, se considera que el término \hat{H}_{qr} se refiere sólo a la lectura y las operaciones de bus, dejando la interacción indirecta qubit-qubit via el resonador ser incluidas en \hat{H}_{qq} via la constante de acoplamiento $\lambda_{\nu,ij}$. Existen distintos tipos de acoplamiento qubit-qubit, entre ellos se encuentran los siguientes:

1. Acoplamiento capacitivo

Este acoplamiento se logra conectando transmones con un capacitor y tiene el siguiente término de interacción:

$$\hat{H}_{qq} = \lambda_{12} \sigma_{x1} \sigma_{x2}, \quad (3.56)$$

Siendo

$$\lambda_{12} = \frac{1}{2} \sqrt{E_{10,1} E_{10,2}} \frac{\sqrt{E_{C1} E_{C2}}}{E_{Cc}} \quad (3.57)$$

$$= \frac{1}{2} \sqrt{E_{10,1} E_{10,2}} \frac{C_c}{\sqrt{C_1 C_2}} \approx \frac{1}{2} E_{10} \frac{C_c}{C} \quad (3.58)$$

$$\hat{H}_{qq} = \lambda_{12} (\sigma_{+1} \sigma_{-2} + \sigma_{-1} \sigma_{+2}). \quad (3.59)$$

2. Acoplamiento por el resonador

Este acoplamiento se logra conectando transmones a un mismo resonador a modo de bus, y tiene el siguiente término de interacción:

$$\hat{H}_{qq} = \lambda_{12} \sigma_{x1} \sigma_{x2}, \quad (3.60)$$

Siendo

$$\lambda_{12} = \frac{1}{2} g_1 g_2 \left(\frac{1}{\Delta_1} + \frac{1}{\Delta_2} \equiv g_1 g_2 \frac{1}{\Delta} \right) \quad (3.61)$$

$$\Delta_i = \epsilon_i - \hbar \omega. \quad (3.62)$$

3. Acoplamiento de unión Josephson

Este acoplamiento se logra conectando transmones con una unión Josephson y tiene el siguiente término de interacción:

$$\hat{H}_{qq} = \lambda_{12} \sigma_{y1} \sigma_{y2}, \quad (3.63)$$

Siendo

$$\lambda_{12} \approx \frac{1}{2} E_{10} \frac{L_c}{L_J} \frac{\cos(\delta_c)}{2L_c \cos(\delta_c) + L_{Jc}}. \quad (3.64)$$

3.11. Compuertas cuánticas en transmones

Las compuertas cuánticas se construyen agregando términos al Hamiltoniano del sistema de manera que el operador de evolución, de un tiempo t_0 a un tiempo

t_1 , sea igual al operador de la compuerta deseada. La evolución temporal de un sistema cuántico puede ser descrita por la ecuación de Schrödinger para el vector de estado $|\psi(t)\rangle$:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H}(t) |\psi(t)\rangle$$

en términos del operador evolución $\hat{U}(t, t_0)$

$$|\psi(t)\rangle = \hat{U}(t, t_0) |\psi(t_0)\rangle$$

El Hamiltoniano del sistema lo podemos descomponer en los siguientes términos:

$$\hat{H} = \hat{H}_{sys} + \hat{H}_{ctrl}(t)$$

Los cuales describen al sistema intrínseco, \hat{H}_{sys} y las operaciones de control aplicadas, \hat{H}_{ctrl} . Las compuertas son el resultado de aplicar pulsos de control específicos a partes selectas de un circuito físico. Esto afecta varios términos del Hamiltoniano, haciéndolos dependientes del tiempo. En general, los términos de control se pueden escribir como:

$$\hat{H}_{ctrl} = \sum_{i;\nu} f_{\nu i}(t) \sigma_{\nu i} + \frac{1}{2} \sum_{i,j;\nu} h_{\nu,ij}(t) \sigma_{\nu i} \sigma_{\nu j} + k(t) a^\dagger a$$

Pulsos de microondas aplicados al resonador tienen el siguiente Hamiltoniano

$$\hat{H}_d = \sum_k (a + a^\dagger) (\xi_k e^{-i\omega_d^{(k)} t} + \xi_k^* e^{i\omega_d^{(k)} t}). \quad (3.65)$$

Aplicando la aproximación de onda rotante (RWA) tenemos

$$\hat{H}_d = \sum_k a \xi_k^* e^{i\omega_d^{(k)} t} + a^\dagger \xi_k e^{-i\omega_d^{(k)} t}. \quad (3.66)$$

En el apéndice A, se realizan con detalle los cálculos asociados a la deducción del Hamiltoniano efectivo que dará lugar a las compuertas que construiremos. Un bus de transmones controlado con pulsos de microondas y con frecuencias de resonancia

modulables tendrá el siguiente Hamiltoniano efectivo con el que podemos realizar rotaciones en X-Y, y la compuerta de entrelazamiento \sqrt{iSWAP} .

$$\hat{H}_{eff} = \tilde{\Delta}_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_i (\Omega \sigma_{+i} + \Omega^* \sigma_{-i}) + \sum_{ij} \frac{g_i g_j}{2 \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) \quad (3.67)$$

En este Hamiltoniano $\tilde{\Delta}_r$ es la diferencia entre las frecuencias del resonador, con un pequeño desplazamiento χ dependiente del estado de cada qubit, y la del pulso de control aplicado. De igual manera, Δ_{qi} es la diferencia entre la frecuencia de resonancia de cada qubit y la frecuencia del pulso aplicado. Δ_i es la diferencia entre la frecuencia de cada qubit y la del resonador. El término $\sum_{ij} \frac{g_i g_j}{2 \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i})$ representa el acoplamiento por el resonador entre los qubits. El término $\sum_i (\Omega \sigma_{+i} + \Omega^* \sigma_{-i})$ representa el efecto del pulso de control sobre los qubits.

3.11.1. Rotaciones X-Y

Tomando $\Omega(t) = \Omega^x(t) \cos(\omega_d t) + \Omega^y(t) \sin(\omega_d t)$, donde ω_d es igual a la frecuencia de resonancia de uno de los qubits logramos rotaciones sobre los ejes X e Y. Las amplitudes de estas rotaciones vienen dadas por $\int_0^{t_0} \Omega^x(t) dt$ y $\int_0^{t_0} \Omega^y(t) dt$, respectivamente, donde t_0 es la duración del pulso.

Tomemos un pulso modulado de la siguiente manera $\Omega(t) = \Omega^x(t) \cos(\omega_d t) = \frac{\Omega^x(t)}{2} (e^{i\omega_d t} + e^{-i\omega_d t})$, donde ω_d coincide con la frecuencia de resonancia de alguno de los qubits. El término correspondiente en el Hamiltoniano será $\frac{1}{2} (\Omega^x(t) \sigma_{+i} + \Omega^x(t) \sigma_{-i}) = \frac{\Omega^x(t)}{2} \sigma_{xi}$. Generando así, rotación en X para el qubit i. Si variamos la fase del pulso, tal que $\Omega(t) = \Omega^k(t) \cos(\omega_d t + \phi_k)$, entonces podremos generar rotaciones alrededor de cualquier eje del plano X-Y dentro de la esfera de Bloch. Por ejemplo, sea $\phi_y = \pi/2$, entonces tendremos $\Omega(t) = \Omega^y(t) \sin(\omega_d t) = \frac{\Omega^y(t)}{2} \frac{-ie^{i\omega_d t} + ie^{-i\omega_d t}}{2i}$. Así, el término en el Hamiltoniano será $\frac{\Omega^y(t)}{2} (-i\sigma_{-i} + i\sigma_{+i}) = \frac{\Omega^y(t)}{2} \sigma_{yi}$. Por lo tanto, aplicando pulsos modulados en fase y cuadratura podemos generar rotaciones en X-Y tales que

$$\hat{H}_{XY} = \frac{1}{2} (\Omega^x(t) \sigma_x + \Omega^y(t) \sigma_y), \quad (3.68)$$

Lo cual nos da la siguiente contribución a la evolución del sistema:

$$\hat{H}_{XY} = \frac{1}{2}(\Omega^x(t)\sigma_x + \Omega^y(t)\sigma_y). \quad (3.69)$$

3.11.2. Compuerta de entrelazamiento

Ahora estudiemos lo que sucede si modulamos la frecuencia de resonancia de dos qubits en el mismo valor, así que $\Delta_1 = \Delta_2 = \Delta$ y sea $J = \frac{g_1 g_2}{\Delta}$. Vamos a enfocarnos en el término de acoplamiento por el resonador entre estos dos qubits.

$$\hat{H}_{q_1 q_2} = \left(\frac{g_1 g_2}{2\Delta_1} + \frac{g_1 g_2}{2\Delta_2}\right)(\sigma_{-1}\sigma_{+2} + \sigma_{+1}\sigma_{-2}) = J(\sigma_{-1}\sigma_{+2} + \sigma_{+1}\sigma_{-2}). \quad (3.70)$$

Este elemento contribuirá a la evolución del sistema de la siguiente manera:

$$U(t_1, t_0) = e^{-iJ(\sigma_{-1}\sigma_{+2} + \sigma_{+1}\sigma_{-2})(t_1 - t_0)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(J(t_1 - t_0)) & -i \sin(J(t_1 - t_0)) & 0 \\ 0 & -i \sin(J(t_1 - t_0)) & \cos(J(t_1 - t_0)) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (3.71)$$

Por lo que si tomamos t_1 y t_0 tales que $t_1 - t_0 = \frac{\pi}{4J}$ podemos generar la compuerta \sqrt{iSWAP}

$$U(t_0 + \frac{\pi}{4J}, t_0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -i \frac{1}{\sqrt{2}} & 0 \\ 0 & -i \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \sqrt{iSWAP}. \quad (3.72)$$

Intuitivamente sigue que si dejamos que esta interacción ocurra por el doble de tiempo, es decir $t_1 - t_0 = \frac{\pi}{2J}$ generaremos la compuerta $iSWAP$.

$$U(t_0 + \frac{\pi}{2J}, t_0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = iSWAP. \quad (3.73)$$

3.11.3. Compuertas compuestas

Con los transmones se pueden realizar rotaciones X - Y y la compuerta i SWAP. Sin embargo, los algoritmos no se escriben en función de sólo estas compuertas, también se necesitan H , $CNOT$, entre otras. Entonces, debemos construir estas otras compuertas en función de R_x , R_y e i SWAP. Esto es posible, ya que con secuencias de rotaciones en X e Y se puede realizar cualquier compuerta de un sólo qubit, ya que estas consisten de rotaciones en la esfera de Bloch y con rotaciones sobre dos ejes ortogonales se pueden lograr rotaciones sobre cualquier eje en la esfera. Luego, con un conjunto universal de compuertas de un sólo qubit y una compuerta de entrelazamiento, se tiene un conjunto universal de compuertas cuánticas.

Capítulo 4

El simulador de compuertas cuánticas en transmones

El simulador de compuertas cuánticas en transmones se desarrolló en Python 3.6, utilizando la librería Qutip 4.2. Esta es una librería que incluye varias herramientas para realizar simulaciones de sistemas mecánico cuánticos, entre ellas, un solucionador de ecuaciones maestras. El funcionamiento básico del simulador desarrollado es el siguiente:

1. Leer estado inicial
2. Construir Hamiltoniano del sistema
3. Introducir Hamiltoniano y estado inicial en el solucionador de ecuaciones maestras.
4. Retornar solución

De esta manera, se simulan las compuertas naturales de los transmones. Luego, a partir de estas se construyen todas las demás compuertas que se necesitaran para construir un conjunto de compuertas cuánticas con el cual poder ejecutar los algoritmos de Grover, Shor y PageRank.

Se simularon dos sistemas distintos, uno de cuatro qubits y otro de ocho qubits. El diseño original era el de cuatro qubits, con él se realizaron las simulaciones del algoritmo de Grover y del PageRank. Sin embargo, el algoritmo de Shor requiere de al menos ocho qubits para factorizar el número compuesto impar más pequeño:

el número 15. Posteriormente también se realizó una generalización del simulador para poder trabajar con sistemas de n qubits.

El tipo de acoplamiento entre los qubits elegido es el acoplamiento de tipo bus. De esta manera trabajamos con un único resonador, el cual se puede tracear. Esto reduce significativamente la dimensión del sistema a simular y nos permite tener más qubits. Además, de esta forma, la interacción es más directa y basta con la compuerta iSWAP para construir cualquier otra compuerta multiqubits, el cual no sería el caso con qubits acoplados a distintos resonadores, pues se necesitarían compuertas de interacción entre resonadores.

4.1. Parámetros de los sistemas simulados

Se han elegido parámetros típicos de los sistemas de qubits[70].

1. Frecuencias de resonancia:
 - a) Resonador: 10GHz
 - b) Qubit 0: 5GHz
 - c) Qubit 1: 6GHz
 - d) Qubit 2: 7GHz
 - e) Qubit 3: 8GHz
 - f) *Qubit 4: 11GHz
 - g) *Qubit 5: 12GHz
 - h) *Qubit 6: 13GHz
 - i) *Qubit 7: 14GHz
2. Constante de acoplamiento: Todas iguales a 0.1GHz
3. Tasas de relajación: Todas iguales a 25KHz
4. Tiempo de relajación: Todos iguales a $40\mu s$
5. Frecuencia de resonancia para iSWAP: 9GHz

*Sólo aplica para el caso del sistema de 8 qubits

4.2. Compuertas nativas

Como se vio en el capítulo anterior, en los transmones se puede ejecutar de manera natural las compuertas Rx, Ry e iSWAP. Estas compuertas se implementan en el simulador y es a partir de ellas que se contruyen todas las demás.

$$H_{R_x} = -\frac{1}{2} \sum_i \Delta_{q_i} \sigma_{z_i} + \xi(t) \sigma_{x_{target}}, \quad (4.1)$$

$$H_{R_y} = -\frac{1}{2} \sum_i \Delta_{q_i} \sigma_{z_i} + \xi(t) \sigma_{y_{target}}, \quad (4.2)$$

$$H_{iSWAP} = \frac{g_1 g_2}{\Delta_{swap}} (\sigma_{+1} \sigma_{-2} + \sigma_{-1} \sigma_{+2}). \quad (4.3)$$

4.2.1. Rx y Ry

Estas compuertas se logran, aplicando un pulso gaussiano de microondas en fase (Rx), o en cuadratura (Ry). Se han elegido pulsos de 10ns de duración, truncados en $\pm 3\sigma$.

$$\xi(t) = A \Pi\left(\frac{t - \mu}{6\sigma}\right) \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(t-\mu)^2}{2\sigma^2}}, \quad (4.4)$$

Donde $\mu = 5ns$, $\sigma = \frac{5}{3}ns$, $\Pi(t)$ es la función rectangular, $A = \frac{\theta}{N}$ y $N = 0,9973$ es una constante de normalización. De esta manera se tiene el pulso gaussiano truncado deseado de 0ns a 10ns, cuya área bajo la curva sea igual al ángulo θ de la rotación.

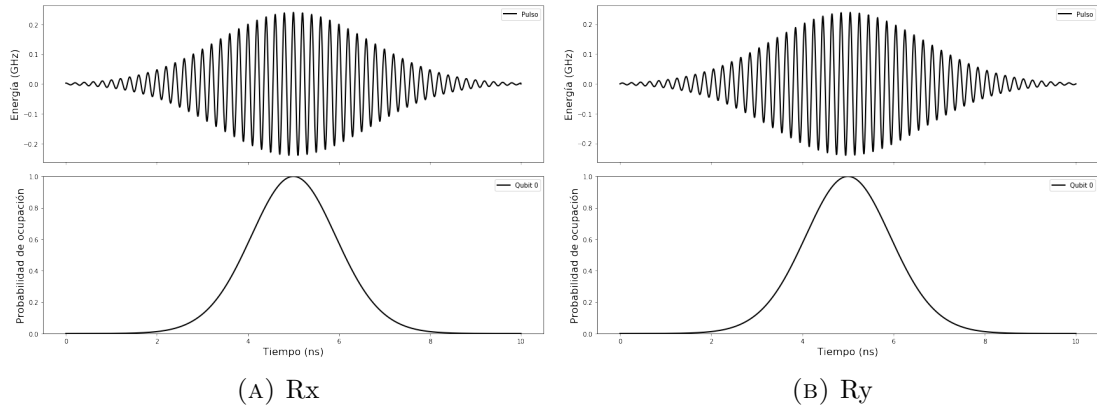


FIGURA 4.1: Rotaciones en X e Y de 2π

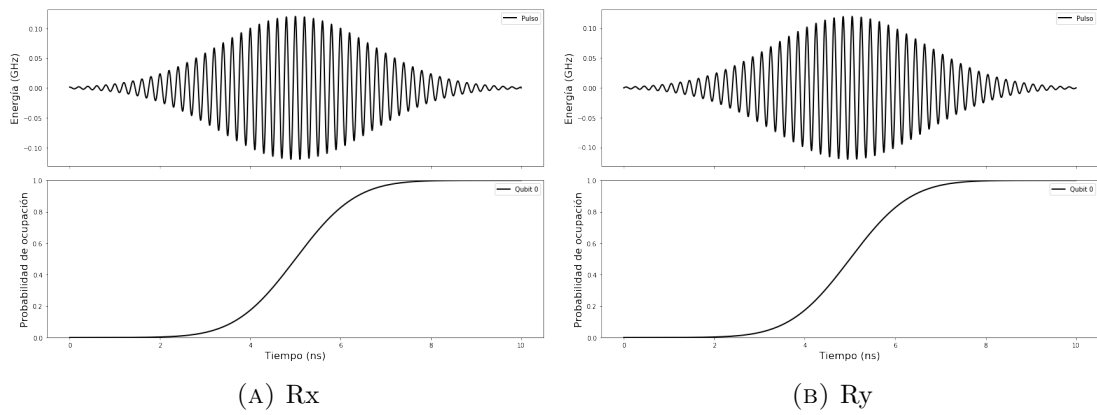


FIGURA 4.2: Rotaciones en X e Y de π

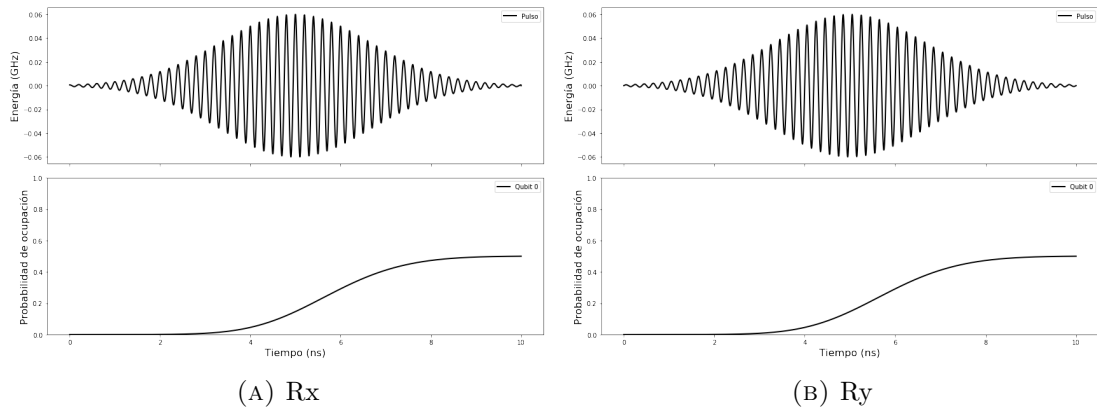


FIGURA 4.3: Rotaciones en X e Y de $\frac{\pi}{2}$

4.2.2. iSWAP

Esta compuerta se logra aplicando un campo magnético tal que la frecuencia de resonancia de los dos qubits deseados se mueva a $\omega_{swap} = 9GHz$. Esta interacción se deja durante $\frac{\pi}{2J}$, donde $J = \left| \frac{g_1 g_2}{\Delta_{swap}} \right|$ y $\Delta_{swap} = \omega_{swap} - \omega_r$. Esto es, esta interacción se deja por 25ns.

Si se desea realizar la compuerta \sqrt{iSWAP} , se debe dejar la misma interacción por sólo 12.5ns, que es la mitad del tiempo.

Es importante mencionar que la Figura 4.4 no está vacía, sino que la probabilidad de ocupación de ambos qubits es constante e igual a cero. Esta Figura refleja como las compuertas $iSWAP$ e \sqrt{iSWAP} dejan invariantes a los pares de qubits que se encuentran en el mismo estado.

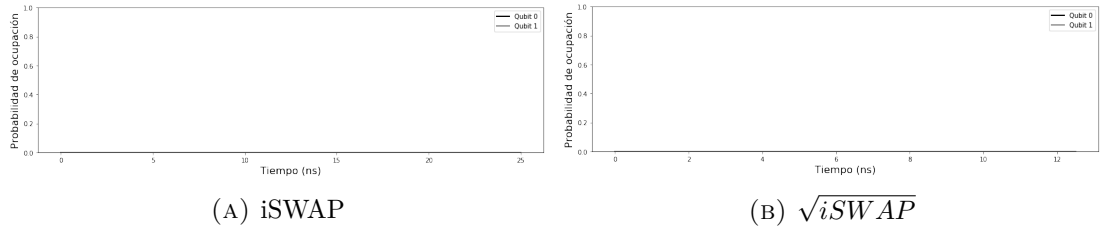


FIGURA 4.4: Compuertas $iSWAP$ y \sqrt{iSWAP} aplicadas a $|00\rangle$

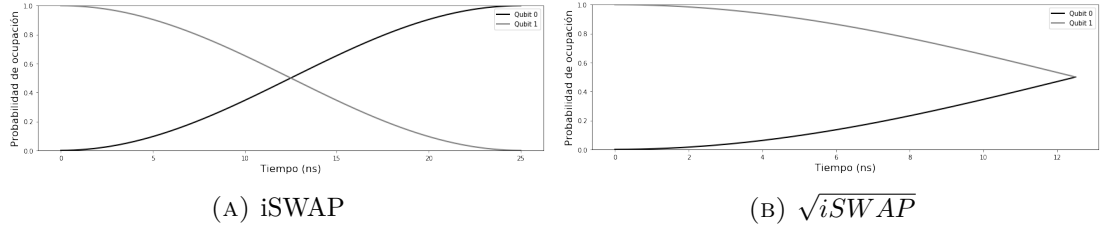


FIGURA 4.5: Compuertas $iSWAP$ y \sqrt{iSWAP} aplicadas a $|01\rangle$

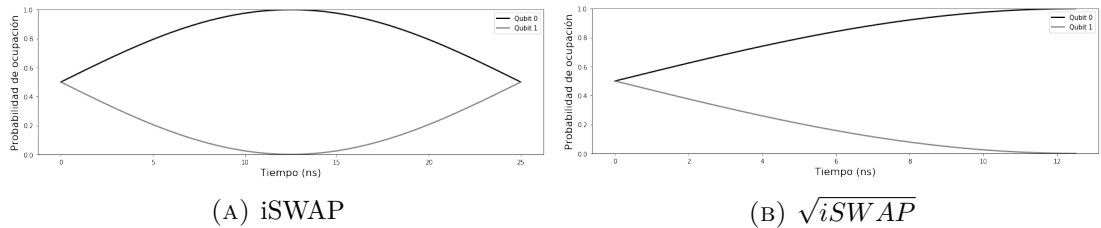


FIGURA 4.6: Compuertas $iSWAP$ y \sqrt{iSWAP} aplicadas a $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

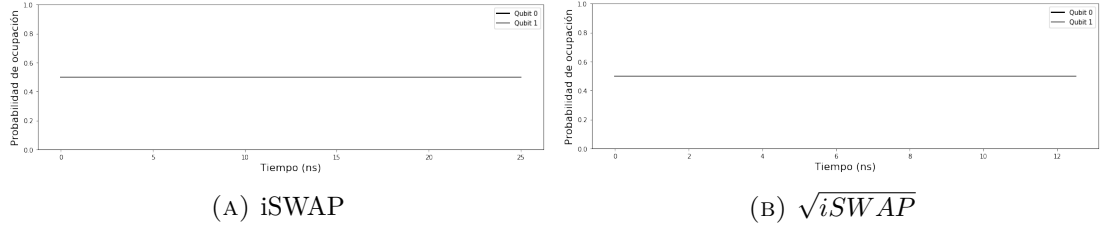


FIGURA 4.7: Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

4.3. Compuertas compuestas

Las compuertas anteriores forman un conjunto universal de compuertas cuánticas. A partir de secuencias de rotaciones en X e Y se puede formar cualquier rotación sobre cualquier eje de la esfera de Bloch, es decir, se puede realizar cualquier compuerta de un qubit. Con esto y cualquier compuerta de entrelazamiento, en nuestro caso \sqrt{iSWAP} , se tiene un conjunto universal de compuertas cuánticas y se puede realizar cualquier otra compuerta a partir de ellas.

4.3.1. X

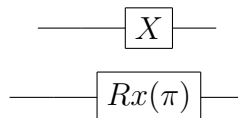
Como tenemos $R_x(\theta)$, basta con hacer $\theta = \pi$ para realizar X, módulo una fase global de $-i$.

$$X = \begin{pmatrix} \cos(\frac{\pi}{2}) & -i \sin(\frac{\pi}{2}) \\ -i \sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2}) \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (4.5)$$

4.3.2. Y

Como tenemos $R_y(\theta)$, basta con hacer $\theta = \pi$ para realizar Y, módulo una fase global de $-i$.

$$Y = \begin{pmatrix} \cos(\frac{\pi}{2}) & -\sin(\frac{\pi}{2}) \\ \sin(\frac{\pi}{2}) & \cos(\frac{\pi}{2}) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (4.6)$$

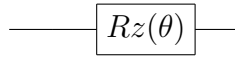


4.3.3. Rz

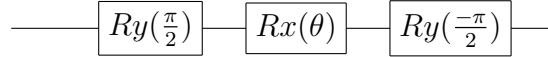
Esta compuerta se realiza aplicando una transformación a Rx tal que el eje de rotación se rote y coincida con el eje Z. Es decir, el eje X se rota $\pi/2$ alrededor de Y:

$$\begin{aligned} Rz(\theta) &= Ry\left(\frac{-\pi}{2}\right)Rx(\theta)Ry\left(\frac{\pi}{2}\right) \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \quad (4.7) \end{aligned}$$

Es decir,



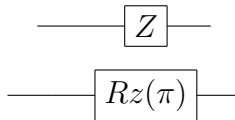
Es equivalente a



4.3.4. Z

Ahora, con Rz, se puede realizar Z haciendo $\theta = \pi$, módulo una fase global de $-i$.

$$Z = \begin{pmatrix} e^{-i\frac{\pi}{2}} & 0 \\ 0 & e^{-i\frac{\pi}{2}} \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (4.8)$$

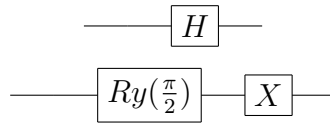


4.3.5. H

Esta compuerta transforma la base X en la base Z y se realiza con $Ry(\pi/2)$ seguido de X.

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (4.9)$$

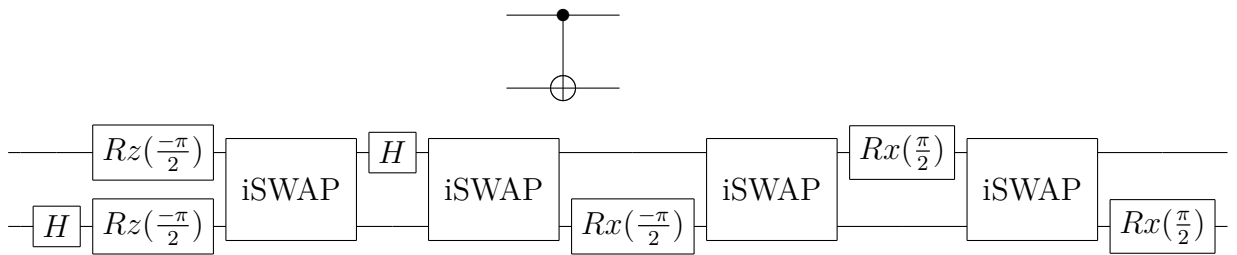
Sólo que en nuestro caso, X también agrega una fase global de $-i$.



4.3.6. CNOT

Esta compuerta se realizó siguiendo el esquema de Schuch y Siewert [71]. De esta manera se logra la compuerta CNOT, módulo una fase global de $\frac{-1-i}{\sqrt{2}}$.

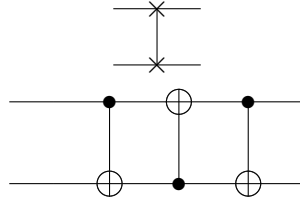
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (4.10)$$



4.3.7. SWAP

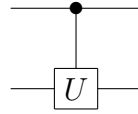
Esta compuerta se realiza con una secuencia de CNOTs.

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (4.11)$$

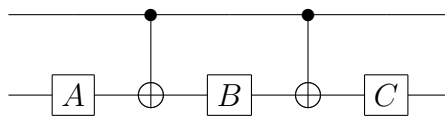


4.3.8. Compuertas condicionales generales

Barenco y colaboradores [46] demostraron que con la compuerta CNOT y compuertas de un qubit se puede realizar cualquier compuerta condicional bipartita



De la siguiente manera

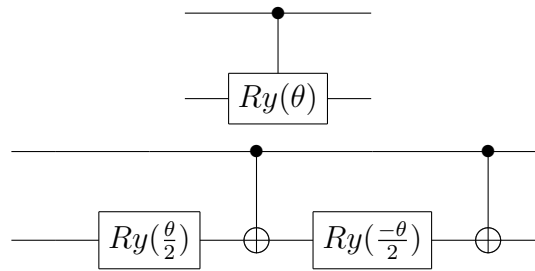


Donde A , B y C deben cumplir las siguientes dos condiciones

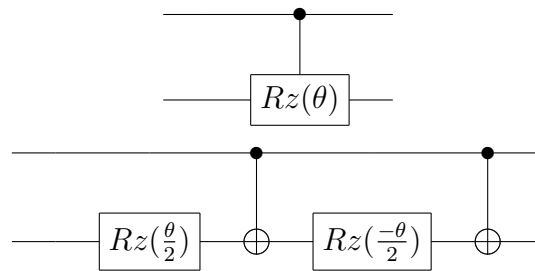
$$CXBXA = U \quad (4.12)$$

$$CBA = \mathbb{1}. \quad (4.13)$$

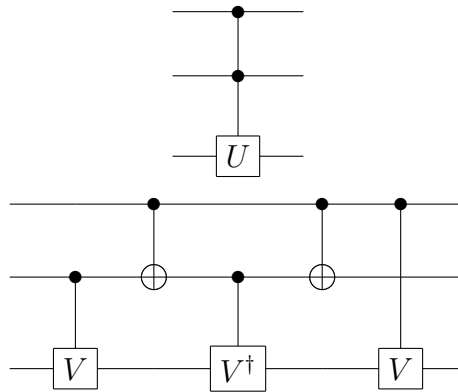
Siguiendo este esquema se construyó CRy.



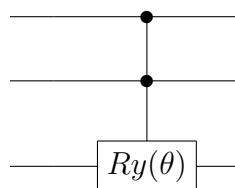
De la misma manera se obtuvo CRz.

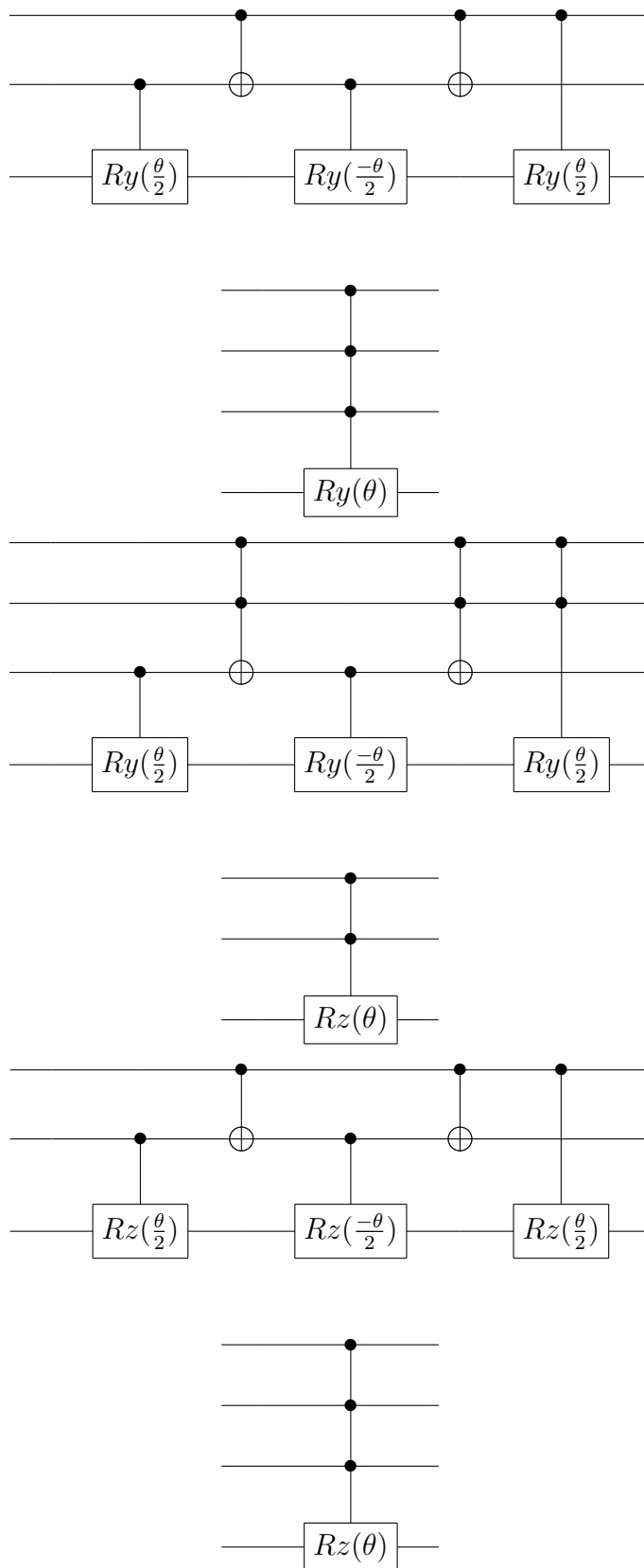


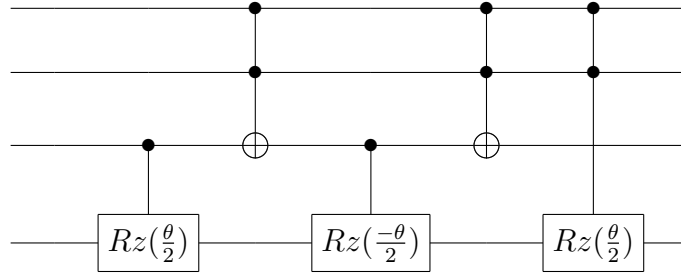
Barenco y colaboradores también propusieron un método para agregar más qubits de control a una compuerta condicional:



Es importante resaltar que cuando $U = X$ se obtiene la compuerta de Toffoli. De esta manera se construyó: CCRy, CCCRy, CCRz y CCCRz.







También se contruyó parcialmente de esta manera la compuerta de Toffoli, CC-CNOT y CCCCNOT, sin embargo, debido a la fase global que queda al realizar X, Y y Z a partir de Rx, Ry y Rz, hace falta una componente adicional para poder construir estas compuertas. Esto ocurre porque la fase global también queda condicionada y deja de ser global. Para ilustrar mejor este detalle, tomemos como ejemplo el caso de Toffoli. Siguiendo el esquema anterior se llega a:

$$Toffoli' = e^{\pi/8} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 0 \end{pmatrix}. \quad (4.14)$$

En lugar de:

$$Toffoli = e^{\phi} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \quad (4.15)$$

Barenco et al. proponen métodos alternativos para lograr aproximaciones de esta compuerta, pero todas ellas introducen fases locales (sólo que de π en lugar de $-\pi/2$), lo cual convierte a la compuerta en una completamente distinta. Es por

esto que en este trabajo se ha desarrollado la compuerta de fase condicional y un método para eliminar la fase local que introduce la compuerta *Toffoli*'.

4.3.9. CP

Rz, y la compuerta de cambio de fase P, son completamente equivalentes cuando actúan como compuertas de un qubit, pues la única diferencia entre ellas es una fase global. Sin embargo, cuando se condicionan, dejan de ser equivalentes.

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} Rz(\theta) \quad (4.16)$$

$$CRz(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{-i\theta/2} & 0 \\ 0 & 0 & 0 & e^{i\theta/2} \end{pmatrix} \quad (4.17)$$

$$CP_\theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix} \neq e^{i\theta/2} CRz(\theta). \quad (4.18)$$

Se puede construir un sistema de ecuaciones con las fases introducidas por $Rz(\theta_1) \otimes \mathbb{1}$, $\mathbb{1} \otimes Rz(\theta_2)$, $CRz_1(\theta_3)$ y $CRz_0(\theta_4)$, donde CRz_0 y CRz_1 son la compuerta CRz con el qubit de la partición 1 y el qubit de la partición 0 como target, respectivamente, tal que:

$$CRz_0(\theta_4)CRz_1(\theta_3)(\mathbb{1} \otimes Rz(\theta_2))(Rz(\theta_1) \otimes \mathbb{1}) = \begin{pmatrix} e^{i(-\theta_1-\theta_2)/2} & 0 & 0 & 0 \\ 0 & e^{i(-\theta_1+\theta_2-\theta_4)/2} & 0 & 0 \\ 0 & 0 & e^{i(\theta_1-\theta_2-\theta_3)/2} & 0 \\ 0 & 0 & 0 & e^{i(\theta_1+\theta_2+\theta_3+\theta_4)/2} \end{pmatrix}, \quad (4.19)$$

Donde se quiere que:

$$(-\theta_1 - \theta_2)/2 = \phi \quad (4.20)$$

$$(-\theta_1 + \theta_2 - \theta_4)/2 = \phi \quad (4.21)$$

$$(\theta_1 - \theta_2 - \theta_3)/2 = \phi \quad (4.22)$$

$$(\theta_1 + \theta_2 + \theta_3 + \theta_4)/2 = \phi + \theta. \quad (4.23)$$

Esto se logra tomando:

$$\theta_1 = \theta/4 \quad (4.24)$$

$$\theta_2 = \theta/4 \quad (4.25)$$

$$\theta_3 = \theta/2 \quad (4.26)$$

$$\theta_4 = \theta/2 \quad (4.27)$$

$$CRz_0(\theta_4)CRz_1(\theta_3)(\mathbb{1} \otimes Rz(\theta_2))(Rz(\theta_1) \otimes \mathbb{1}) = \begin{pmatrix} e^{i(-\theta)/4} & 0 & 0 & 0 \\ 0 & e^{i(-\theta)/4} & 0 & 0 \\ 0 & 0 & e^{i(-\theta)/4} & 0 \\ 0 & 0 & 0 & e^{i3\theta/4} \end{pmatrix} = e^{-\theta/4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}. \quad (4.28)$$

Esta compuerta agrega una fase de $e^{i\theta}$ al ket $|11\rangle$. Con este mismo método también se pueden construir versiones de esta compuerta que agreguen la misma fase a los kets $|00\rangle$, $|01\rangle$, $|10\rangle$.

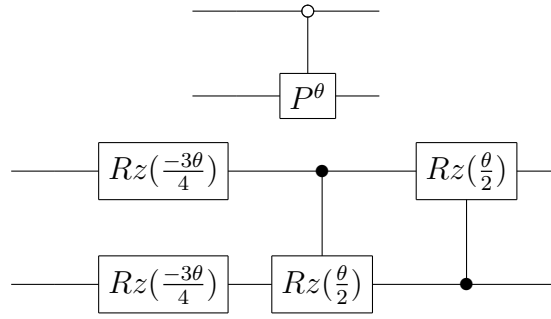
1. Para agregar una fase al estado $|00\rangle$, se utiliza la compuerta CP^θ blanca, la cual se construye con los siguientes ángulos:

$$\theta_1 = -3 * \theta/4$$

$$\theta_2 = -3 * \theta/4$$

$$\theta_3 = \theta/2$$

$$\theta_4 = \theta/2$$



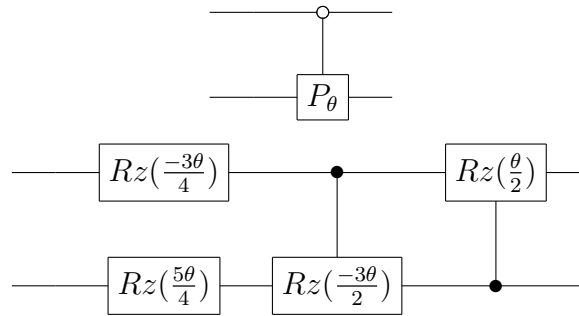
2. Para agregar una fase al estado $|01\rangle$, se utiliza la compuerta CP_θ blanca, la cual se construye con los siguientes ángulos:

$$\theta_1 = -3\theta/4$$

$$\theta_2 = 5\theta/4$$

$$\theta_3 = -3\theta/2$$

$$\theta_4 = \theta/2$$



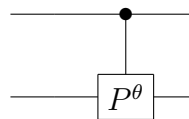
3. Para agregar una fase al estado $|10\rangle$, se utiliza la compuerta CP^θ negra, la cual se construye con los siguientes ángulos:

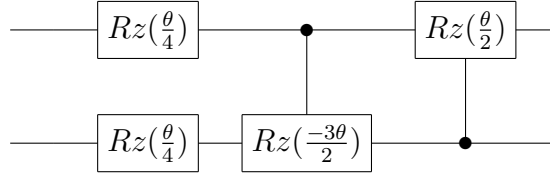
$$\theta_1 = \theta/4$$

$$\theta_2 = \theta/4$$

$$\theta_3 = -3\theta/2$$

$$\theta_4 = \theta/2$$





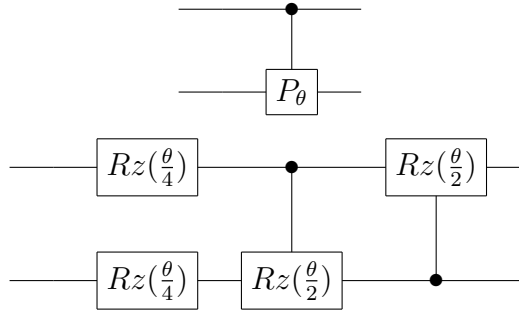
4. Para agregar una fase al estado $|11\rangle$, se utiliza la compuerta CP_θ negra, la cual se construye con los siguientes ángulos:

$$\theta_1 = \theta/4$$

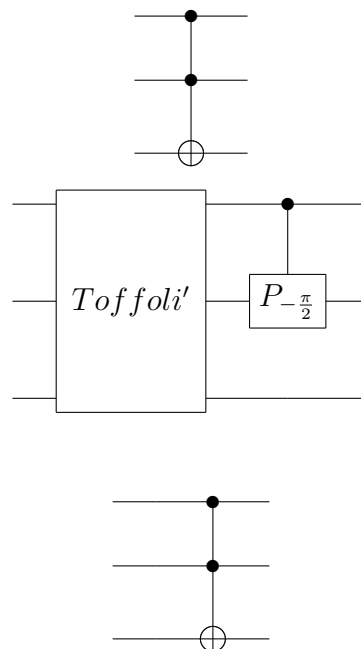
$$\theta_2 = \theta/4$$

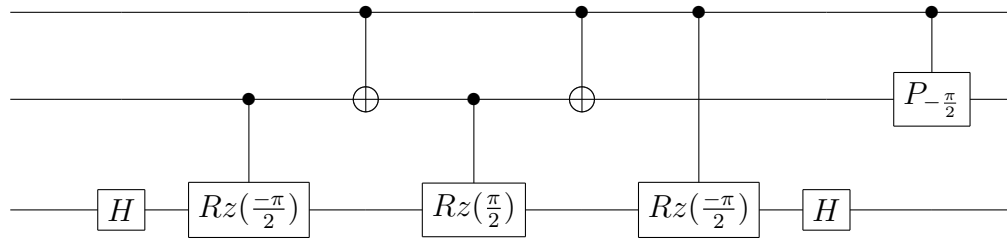
$$\theta_3 = \theta/2$$

$$\theta_4 = \theta/2$$



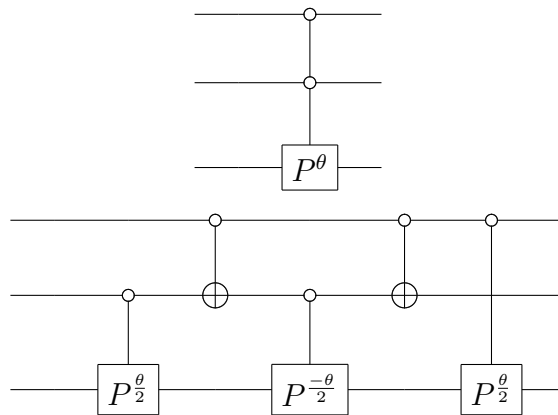
Finalmente, para realizar la compuerta de Toffoli, se debe aplicar la compuerta CP_θ después de $Tofoli'$ con $\theta = -\pi/2$ a los qubits de control de Toffoli.



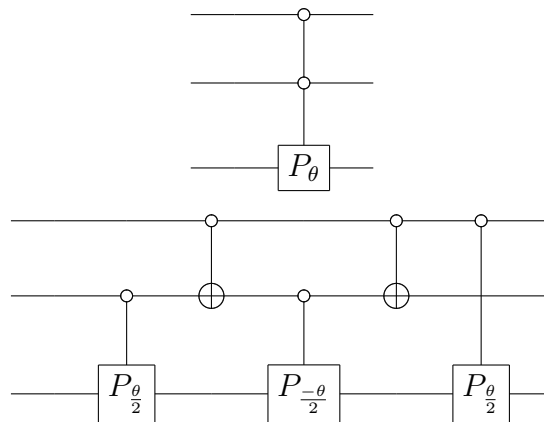


De la misma manera, con CCP se puede realizar CCCNOT. CCP y CCCP se pueden realizar con el método de Barenco.

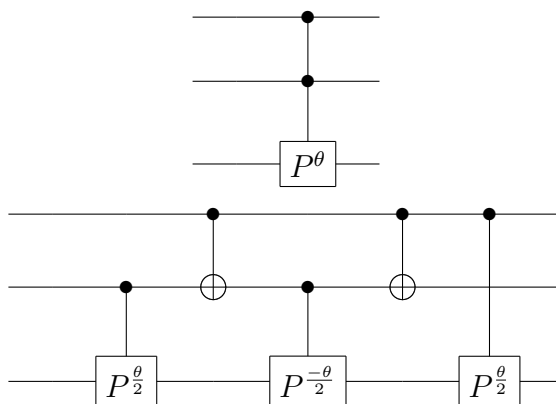
Compuerta CCP^θ blanca:



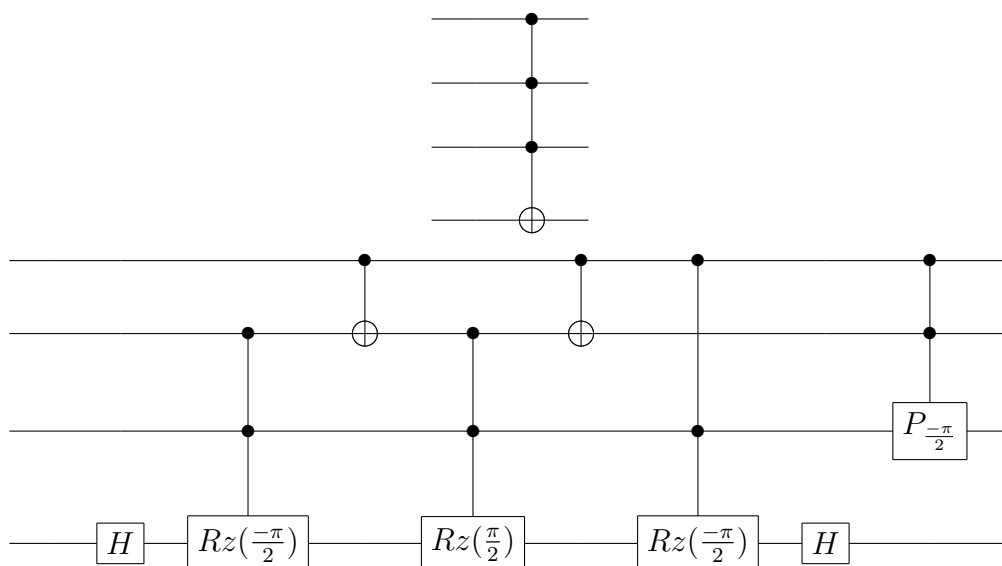
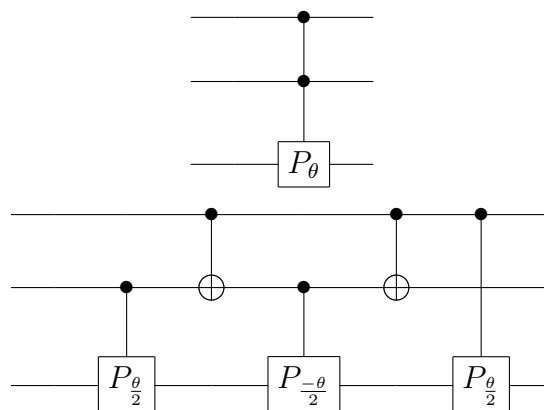
Compuerta CCP_θ blanca:



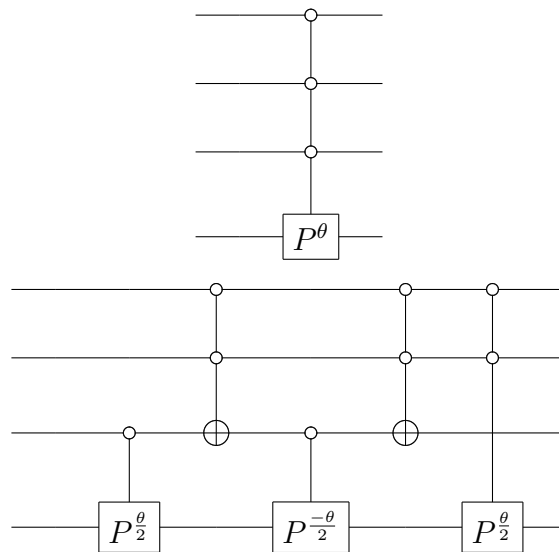
Compuerta CCP^θ negra:



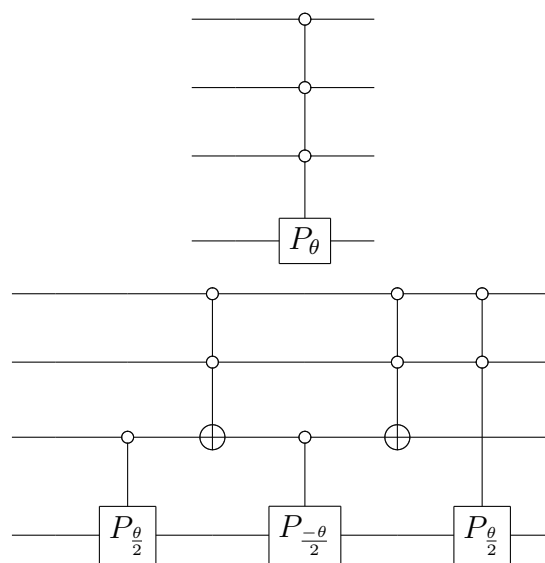
Compuerta CCP_θ negra:



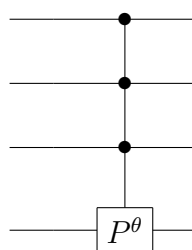
Compuerta $CCCP^\theta$ blanca:

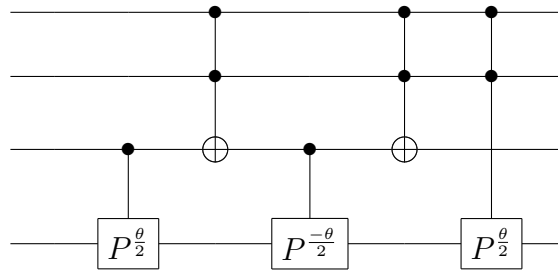


Compuerta $CCCP_\theta$ blanca:

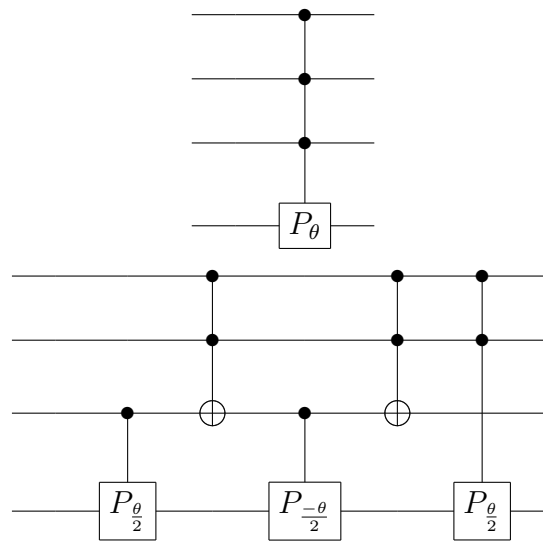


Compuerta $CCCP^\theta$ negra:





Compuerta $CCCP_\theta$ negra:



Capítulo 5

Algoritmo de Grover

El algoritmo de Grover [13], es un algoritmo cuántico (AC) que realiza una búsqueda en una secuencia no ordenada de datos con $N = 2^n$ entradas. Clásicamente esta búsqueda tendría un orden de complejidad de $O(N)$, pues, como los datos no están ordenados, la cantidad promedio de evaluaciones que se deben realizar crece linealmente con la cantidad de entradas. En el caso del algoritmo de Grover, la complejidad de la búsqueda es de $O(\sqrt{N})$, pues se requieren aproximadamente $\frac{\pi\sqrt{N}}{4}$ iteraciones para hallar la entrada deseada [13]. En cuanto a la cantidad de qubits requeridos, se necesitan $O(\log_2 N)$ qubits, pues se debe realizar un estado superpuesto donde cada componente de la superposición represente una entrada de la secuencia de datos.

Supongamos que la secuencia de datos no ordenada tiene la siguiente función asociada:

$$f(x) = \begin{cases} 1 & \text{si } x = \omega \\ 0 & \text{si } x \neq \omega \end{cases}, \quad (5.1)$$

Donde ω es el dato que se desea encontrar. Esta función devuelve 1 si se evalúa la entrada que almacena el dato deseado y 0 en cualquier otro caso.

El algoritmo de Grover se basa en la disponibilidad de un operador cuántico, llamado *oráculo*, tal que se introduzca un fase global de π si $f(x_0) = 1$ y deje el estado del sistema intacto si $f(x_0) = 0$. Es decir, el oráculo realiza una reflexión alrededor de $|\omega\rangle$.

$$U_\omega |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} |x\rangle & \text{si } x \neq \omega \\ -|x\rangle & \text{si } x = \omega \end{cases} \quad (5.2)$$

$$U_\omega = \mathbb{1} - 2|\omega\rangle\langle\omega|. \quad (5.3)$$

Además de éste, se necesita otro operador de reflexión, U_s , el cual realiza una reflexión alrededor del estado de superposición uniforme $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$. Así, por el hecho de la geometría plana elemental de que el producto de dos reflexiones es una rotación, se logra aproximar el estado del sistema al estado asociado a la entrada deseada.

$$U_s = 2|s\rangle\langle s| - \mathbb{1}. \quad (5.4)$$

Al producto de estas dos rotaciones $U_s U_\omega$ se le conoce como operador de difusión. Veamos lo que sucede al aplicar el operador de difusión sobre el estado $|s\rangle$:

$$\begin{aligned} U_\omega |s\rangle &= (\mathbb{1} - 2|\omega\rangle\langle\omega|) |s\rangle = |s\rangle - 2|\omega\rangle\langle\omega| |s\rangle \\ &= |s\rangle - \frac{2}{\sqrt{N}} |\omega\rangle\langle\omega| \sum_{x=0}^{N-1} |x\rangle = |s\rangle - \frac{2}{\sqrt{N}} |\omega\rangle. \end{aligned} \quad (5.5)$$

Similarmente podemos observar que

$$\begin{aligned} U_s(|s\rangle - \frac{2}{\sqrt{N}} |\omega\rangle) &= (2|s\rangle\langle s| - \mathbb{1})(|s\rangle - \frac{2}{\sqrt{N}} |\omega\rangle) \\ &= 2(|s\rangle - \frac{4}{N} |s\rangle) - (|s\rangle - \frac{2}{\sqrt{N}} |\omega\rangle) = |s\rangle - \frac{4}{N} |s\rangle + \frac{2}{\sqrt{N}} |\omega\rangle \\ &= \frac{N-4}{N} |s\rangle + \frac{2}{\sqrt{N}} |\omega\rangle. \end{aligned} \quad (5.6)$$

Ahora veamos lo que sucede al aplicar esta secuencia de rotaciones sobre el estado $|\omega\rangle$:

$$U_\omega |\omega\rangle = (\mathbb{1} - 2|\omega\rangle\langle\omega|) |\omega\rangle = |\omega\rangle - 2|\omega\rangle = -|\omega\rangle \quad (5.7)$$

$$U_s(-|\omega\rangle) = (2|s\rangle\langle s| - \mathbb{1})(-|\omega\rangle) = -\frac{2}{\sqrt{N}}|s\rangle + |\omega\rangle. \quad (5.8)$$

Se observa así, que al aplicar $U_s U_\omega$ sobre $|s\rangle$, se amplifica la componente de $|\omega\rangle$ en la superposición de $\frac{1}{\sqrt{N}}$ a $\frac{3N-4}{N\sqrt{N}}$. Es decir que la probabilidad de medir el valor deseado crece de $\frac{1}{N}$ a $9(1 - \frac{4}{3N})\frac{1}{N}$.

$$\langle\omega|U_s U_\omega|s\rangle = \frac{N-4}{N} \frac{1}{\sqrt{N}} + \frac{2}{\sqrt{N}} = \frac{3N-4}{N\sqrt{N}}. \quad (5.9)$$

Y la probabilidad cuántica será

$$p(\omega) = |\langle\omega|U_s U_\omega|s\rangle|^2 = \frac{(3N-4)^2}{N^3} = 9(1 - \frac{4}{3N})\frac{1}{N}. \quad (5.10)$$

Por otro lado, se observa que al aplicar $U_s U_\omega$ sobre $|\omega\rangle$, aparece una componente de $|s\rangle$, así que en ese caso, la probabilidad de medir el valor deseado disminuye. Por lo que debe existir una cantidad de iteraciones k_{max} tras las cuales se alcanza la probabilidad máxima de medir $|\omega\rangle$, partiendo de $|s\rangle$ y a partir de donde esta probabilidad empieza a disminuir.

De esta manera, el algoritmo de Grover consiste en aplicar k_{max} veces $U_s U_\omega$, partiendo del estado $|s\rangle$, es decir rotar este estado hasta que se aproxime lo más posible a $|\omega\rangle$.

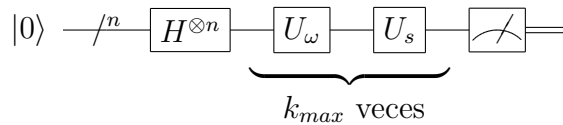


FIGURA 5.1: Circuito del algoritmo de Grover, k_{max} desconocido.

Para hallar k_{max} , veamos el ángulo que se rota con cada aplicación de $U_s U_\omega$. Primero definamos el estado $|s'\rangle$ como la superposición uniforme de todos los estados de la base computacional excepto $|\omega\rangle$, es decir:

$$|s'\rangle = \frac{1}{N-1} \sum_{x \neq \omega} |x\rangle = \frac{\sqrt{N}}{\sqrt{N-1}} |s\rangle - \frac{1}{\sqrt{N-1}} |\omega\rangle. \quad (5.11)$$

Los estados $|s'\rangle$ y $|\omega\rangle$ son ortonormales, $\langle s'|\omega\rangle = 0$, por lo que generan un espacio bidimensional de Hilbert. Este espacio contiene a $|s\rangle$, pues:

$$|s\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |s'\rangle + \frac{1}{\sqrt{N}} |\omega\rangle. \quad (5.12)$$

Además, se ha visto que $U_s U_\omega |s\rangle$ y $U_s U_\omega |\omega\rangle$ se escriben en función de sólo $|s\rangle$ y $|\omega\rangle$. Así que podemos inducir que $(U_s U_\omega)^k |s\rangle$ pertenece al espacio generado por $\{|s'\rangle, |\omega\rangle\}$, donde $k \in \{0, 1, 2, \dots\}$. Esto indica que este espacio contiene al plano en el que se realizan las rotaciones $U_s U_\omega$.

Ahora que conocemos una base del plano de rotación, podemos hallar el ángulo que se rota con cada aplicación de $U_s U_\omega$.

$$U_\omega |\psi\rangle = (\mathbb{1} - 2|\omega\rangle\langle\omega|)(\alpha |s'\rangle + \beta |\omega\rangle) = \alpha |s'\rangle - \beta |\omega\rangle. \quad (5.13)$$

De la misma forma

$$\begin{aligned} U_s(\alpha |s'\rangle - \beta |\omega\rangle) &= (2|s\rangle\langle s| - \mathbb{1})(\alpha |s'\rangle - \beta |\omega\rangle) \\ &= \alpha \left(2 \frac{\sqrt{N-1}}{\sqrt{N}} |s\rangle - |s'\rangle \right) - \beta \left(\frac{2}{\sqrt{N}} |s\rangle - |\omega\rangle \right) \\ &= \alpha \left(\left(2 \frac{N-1}{N} - 1 \right) |s'\rangle + 2 \frac{\sqrt{N-1}}{N} |\omega\rangle \right) - \beta \left(\frac{2\sqrt{N-1}}{N} |s'\rangle + \left(\frac{2}{N} - 1 \right) |\omega\rangle \right) \\ &= \left(\alpha \frac{N-2}{N} - \beta \frac{2\sqrt{N-1}}{N} \right) |s'\rangle + \left(\alpha 2 \frac{\sqrt{N-1}}{N} + \beta \frac{N-2}{N} \right) |\omega\rangle. \end{aligned} \quad (5.14)$$

De aquí se deduce que $\cos(\Delta\theta) = \frac{N-2}{N}$ y que $\sin(\Delta\theta) = 2 \frac{\sqrt{N-1}}{N}$. De hecho, se comprueba que:

$$\cos^2(\Delta\theta) + \sin^2(\Delta\theta) = \frac{(N-2)^2}{N^2} + 4 \frac{N-1}{N^2} = \frac{N^2 - 4N + 4}{N^2} + 4 \frac{N-1}{N^2} = 1. \quad (5.15)$$

Ahora podemos escribir las componentes de $|s\rangle$ en función del ángulo inicial θ_0 :

$$\cos(\theta_0) = \frac{\sqrt{N-1}}{\sqrt{N}} \quad (5.16)$$

$$\sin(\theta_0) = \frac{1}{\sqrt{N}}. \quad (5.17)$$

Finalmente, lo que se quiere es que:

$$\theta_0 + k\Delta\theta \rightarrow \frac{\pi}{2}. \quad (5.18)$$

Es decir, que:

$$\cos^{-1}\left(\frac{\sqrt{N-1}}{\sqrt{N}}\right) + k \cos^{-1}\left(\frac{N-2}{N}\right) \rightarrow \frac{\pi}{2} \quad (5.19)$$

$$\sin^{-1}\left(\frac{1}{\sqrt{N}}\right) + k \sin^{-1}\left(2\frac{\sqrt{N-1}}{N}\right) \rightarrow \frac{\pi}{2}. \quad (5.20)$$

Si tomamos $N \gg 1$ en (4.12), tenemos que:

$$2k\frac{1}{\sqrt{N}} \rightarrow \frac{\pi}{2} \quad (5.21)$$

$$k_{max} \approx \frac{\pi\sqrt{N}}{4}. \quad (5.22)$$

En la Figura 5.2 podemos entonces visualizar gráficamente la acción del operador difusión sobre $|s\rangle$.

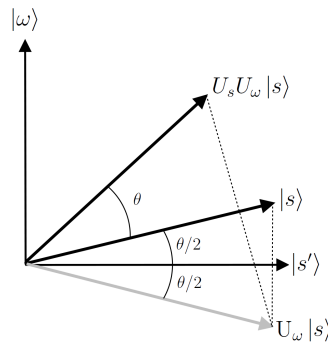


FIGURA 5.2: Interpretación geométrica del operador difusión

5.1. El algoritmo

El circuito cuántico asociado al algoritmo de Grover tiene la siguiente representación:

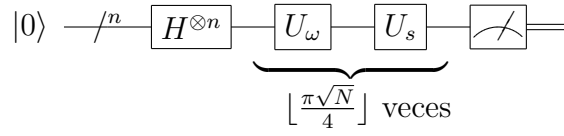


FIGURA 5.3: Circuito del algoritmo de Grover.

Dicho algoritmo se puede describir detalladamente en los siguientes pasos:

1. Preparar el estado fiducial.
2. Aplicar la transformada de Walsh-Hadamard.
3. Realizar la iteración de Grover $\lfloor \frac{\pi\sqrt{N}}{4} \rfloor$ veces.
 - a) Aplicar U_{ω} .
 - b) Aplicar U_s .
4. Realizar la medida Ω .

5.2. Variaciones y generalizaciones del algoritmo de Grover

A continuación estudiaremos el algoritmo de amplificación de amplitud, el cual es una generalización del algoritmo de Grover para bases de datos con cualquier cantidad de estados objetivos, y el algoritmo de Grover en un paso, el cual es una variación del algoritmo de Grover en la que se mide en cada iteración.

5.2.1. Algoritmo de amplificación de amplitud

Esta generalización fue desarrollada independientemente por Brassar y Høyer en 1997 [72], y por Grover en 1998 [73]. Con este algoritmo se pueden utilizar funciones oráculo que marquen 1 para más de una entrada de la base de datos en la cual se realizará la búsqueda. Entonces, sea \mathcal{W} el conjunto de entradas a encontrar, tenemos la función oráculo:

$$f(x) = \begin{cases} 1 & \text{si } x \in \mathcal{W} \\ 0 & \text{si } x \notin \mathcal{W} \end{cases}. \quad (5.23)$$

Ahora sea el proyector $\Pi_{\mathcal{W}}$ tal que proyecte los estados del espacio de Hilbert \mathcal{H} asociado a la base de datos en el espacio de Hilbert generado por los estados objetivos $\mathcal{H}_{\mathcal{W}}$:

$$\Pi_{\mathcal{W}} = \sum_k |\omega_k\rangle\langle\omega_k|. \quad (5.24)$$

Donde los estados $|\omega_k\rangle$ son los estados asociados a las entradas de la base de datos pertenecientes a \mathcal{W} .

Sea el estado inicial:

$$|\psi\rangle = \sin(\theta) |\psi_1\rangle + \cos(\theta) |\psi_0\rangle, \quad (5.25)$$

Donde $|\psi_1\rangle = \frac{\Pi_{\mathcal{W}}|\psi\rangle}{\sin(\theta)}$ y $\sin(\theta) = \langle\psi|\Pi_{\mathcal{W}}|\psi\rangle$. Lo que nos conduce a precisar que $|\psi_0\rangle = \frac{(\mathbb{1} - \Pi_{\mathcal{W}})|\psi\rangle}{\cos(\theta)}$, y que $\cos(\theta) = \langle\psi|(\mathbb{1} - \Pi_{\mathcal{W}})|\psi\rangle$.

Ahora definamos los siguientes operadores de reflexión $U_\psi = (2|\psi\rangle\langle\psi| - \mathbb{1})$ y $U_{\mathcal{W}} = \mathbb{1}(\mathbb{1} - 2\Pi_{\mathcal{W}})$, estos son las generalizaciones de U_s y U_ω , del algoritmo de Grover, respectivamente. El producto de ellos, $U_\psi U_{\mathcal{W}}$ es un operador de rotación en el plano generado por $|\psi_0\rangle$ y $|\psi_1\rangle$, de la misma manera que $U_s U_\omega$ es un operador de rotación en el plano generado por $|s'\rangle$ y $|\omega\rangle$. Ahora veamos el efecto de $U_\psi U_{\mathcal{W}}$ y el ángulo que rota este operador:

$$\begin{aligned} U_\psi U_{\mathcal{W}} |\psi\rangle &= (2|\psi\rangle\langle\psi| - \mathbb{1})(\mathbb{1} - 2\Pi_{\mathcal{W}}) |\psi\rangle \\ &= (2|\psi\rangle\langle\psi| - \mathbb{1})[(\mathbb{1} - \Pi_{\mathcal{W}}) - \Pi_{\mathcal{W}}] |\psi\rangle \\ &= (2|\psi\rangle\langle\psi| - \mathbb{1})(\cos(\theta) |\psi_0\rangle - \sin(\theta) |\psi_1\rangle) \\ &= (2|\psi\rangle\langle\psi| - \mathbb{1})(|\psi\rangle - 2\sin(\theta) |\psi_1\rangle) \\ &= |\psi\rangle + (-4\sin^2(\theta) |\psi\rangle + 2\sin(\theta) |\psi_1\rangle) \\ &= (3 - 4\sin^2(\theta)) \sin(\theta) |\psi_1\rangle + (1 - 4\sin^2(\theta)) \cos(\theta) |\psi_0\rangle \\ &= \sin(3\theta) |\psi_1\rangle + \cos(3\theta) |\psi_0\rangle. \end{aligned} \quad (5.26)$$

Como se puede ver, el operador $U_\psi U_{\mathcal{W}}$ rota un ángulo de $\Delta\theta = 3\theta - \theta = 2\theta$. Por lo que si se aplica k veces a $|\psi\rangle$, después de un cálculo inductivo tendremos:

$$(U_\psi U_{\mathcal{W}})^k |\psi\rangle = \sin((2k+1)\theta) |\psi_1\rangle + \cos((2k+1)\theta) |\psi_0\rangle. \quad (5.27)$$

De esta manera, el $k = k_{max}$ para el cual se obtiene la probabilidad máxima de medir un elemento de $\mathcal{H}_{\mathcal{W}}$, es decir, el k que maximiza la amplitud de probabilidad de la componente $|\psi_1\rangle$ de $|\psi\rangle$, es $\lfloor \frac{\pi}{4\theta} \rfloor$. Así:

$$\begin{aligned} (U_\psi U_{\mathcal{W}})^{k_{max}} |\psi\rangle &= \sin\left(\left(2\lfloor \frac{\pi}{4\theta} \rfloor + 1\right)\theta\right) |\psi_1\rangle + \cos\left(\left(2\lfloor \frac{\pi}{4\theta} \rfloor + 1\right)\theta\right) |\psi_0\rangle \\ &\approx \sin\left(\frac{\pi}{2}\right) |\psi_1\rangle + \cos\left(\frac{\pi}{2}\right) |\psi_0\rangle = |\psi_1\rangle. \end{aligned} \quad (5.28)$$

Mientras menor sea θ , más tenderá asintóticamente $(U_\psi U_{\mathcal{W}})^{k_{max}} |\psi\rangle$ a $|\psi_1\rangle$, pero mayor será k_{max} .

Como se puede ver, el algoritmo de amplificación de amplitud se puede utilizar como algoritmo de búsqueda con una cantidad arbitraria de estados objetivos y un estado inicial arbitrario, no sólo $|s\rangle$ como en el algoritmo de Grover. Sin embargo, este no es sólo un algoritmo de búsqueda, sino también un algoritmo de optimización. En este sentido, la amplificación de amplitud también se puede utilizar como subrutina para mejorar el resultado de otros algoritmos. Sea $U_{\mathcal{A}}$ el operador asociado a un algoritmo cuántico \mathcal{A} , entonces, tal que, partiendo del estado fiducial, retorne el estado $|\psi\rangle$. Es decir, $U_{\mathcal{A}}|0\rangle = |\psi\rangle$, entonces, podemos reescribir U_ψ de la siguiente manera:

$$U_\psi = (2|\psi\rangle\langle\psi| - \mathbb{1}) = (2U_{\mathcal{A}}|0\rangle\langle 0|U_{\mathcal{A}}^\dagger - \mathbb{1}) = U_{\mathcal{A}}(2|0\rangle\langle 0| - \mathbb{1})U_{\mathcal{A}}^\dagger = U_{\mathcal{A}}U_0U_{\mathcal{A}}^\dagger. \quad (5.29)$$

De esta manera, a cualquier algoritmo, que actúe sobre un espacio de Hilbert \mathcal{H} que se pueda descomponer en un espacio de estados buenos $\mathcal{H}_{\mathcal{W}}$, y un espacio de estados malos $\mathcal{H} \setminus \mathcal{H}_{\mathcal{W}}$, se le puede aplicar la amplificación de amplitud para mejorar su resultado.

Ahora consideremos el caso en el que $U_{\mathcal{A}} = H^{\otimes n}$, es decir, el caso en el que $|\psi\rangle = |s\rangle$. Este sería el caso particular del algoritmo de amplificación de amplitud en el que se utiliza el mismo estado inicial del algoritmo de Grover.

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle = \frac{1}{\sqrt{N}} \sum_{i \in \mathcal{W}} |i\rangle + \frac{1}{\sqrt{N}} \sum_{j \notin \mathcal{W}} |j\rangle \quad (5.30)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{W}} \sum_{i \in \mathcal{W}} |i\rangle \quad (5.31)$$

$$\sin \theta = \sqrt{\frac{W}{N}} \quad (5.32)$$

$$|\psi_0\rangle = \frac{1}{\sqrt{N-W}} \sum_{j \notin \mathcal{W}} |j\rangle \quad (5.33)$$

$$\cos \theta = \sqrt{\frac{N-W}{N}}. \quad (5.34)$$

Si tomamos $N \gg W$, tendríamos que $\theta \approx \sqrt{\frac{W}{N}}$, entonces $k_{max} \approx \frac{\pi}{4} \sqrt{\frac{N}{W}}$. Es interesante notar que mientras más estados buenos haya, menos iteraciones se necesitan. Pero a cambio, para hallar todos esos estados buenos, se debe ejecutar el algoritmo más veces. En caso de que \mathcal{W} sea de dimensión 1, se recuperaría exactamente el algoritmo de Grover.

5.2.2. Algoritmo de Grover en un paso

Grover [74] propone una manera alternativa para ejecutar su algoritmo. En lugar de realizar $O(\sqrt{N})$ iteraciones del algoritmo, en un sólo sistema cuántico, y medir el estado del sistema una sólo vez, propone utilizar varios sistemas cuánticos, ejecutar el algoritmo en cada uno de estos sistemas, pero realizar sólo una iteración antes de medir cada sistema. Partiendo de la ecuación 5.10, la probabilidad de medir cada uno de los estados, cuando N es grande, luego de aplicar una iteración del algoritmo de Grover es aproximadamente:

$$p(x) \approx \begin{cases} \frac{9}{N} & \text{si } x = \omega \\ \frac{1}{N} & \text{si } x \neq \omega \end{cases}. \quad (5.35)$$

Así que con η sistemas se tendrá, en promedio $9\eta/N \pm O(\sqrt{\eta/N})$ medidas del valor deseado y $\eta/N \pm O(\sqrt{\eta/N})$ medidas de cualquiera de cada uno de los otros estados. La idea es tener suficientes sistemas para poder elegir con seguridad el valor que más se repita como el valor deseado. Por el teorema del límite central, la probabilidad de que una variable particular se desvíe más de $\pm\gamma\sqrt{\eta/N}$ de su valor

esperado es menor que $e^{-\Omega(\gamma^2)}$. De esta manera, si $\eta = \Omega(N \log(N))$, entonces, con una probabilidad cercana a 1, el valor deseado ocurrirá con mayor frecuencia que cualquiera de los otros $N - 1$.

Este esquema también se puede aplicar al algoritmo de amplificación de amplitud, pero con una condición: Que la cantidad de estados marcados sea menor a $N/4$. Esto es porque no hay manera de diferenciar los W estados asociados a \mathcal{W} deseados de los otros $N - W$. Entonces, si W es cercano a $N/2$, resultará imposible identificar correctamente los estados deseados.

Es importante mencionar que aunque esta versión del algoritmo se pueda ejecutar con una sola iteración, resulta menos eficiente que el algoritmo de Grover tradicional. Esto es porque esas $\Omega(N \log(N))$ mediciones necesitarán ser procesadas para hallar los valores más frecuentes, lo cual tendrá una complejidad temporal del mismo orden $\Omega(N \log(N))$, la cual es mayor a la complejidad temporal $O(\sqrt{N})$ de la versión tradicional del algoritmo. De esta forma, la única verdadera ventaja de esta variación estaría en el caso en que se tengan sistemas con tiempos de vida tales que no permitan realizar las iteraciones necesarias para ejecutar la versión tradicional del algoritmo de Grover.

5.2.3. Optimización del algoritmo de Grover

Garg y Pande [75] proponen una optimización del algoritmo de Grover, mezclando el algoritmo de Grover tradicional y el algoritmo de Grover de un paso. La idea de ellos es ejecutar el algoritmo en múltiples sistemas idénticos, como en el algoritmo de un paso, pero realizar más de una iteración, como en el algoritmo tradicional. De esta manera, reducen la cantidad η de sistemas necesarios y la cantidad k de iteraciones necesarias. Ellos hanan que tomando $\eta = k$, entonces sólo se necesitan $O(\sqrt[3]{N})$.

Partiendo de (5.17) y (5.26), sabemos que en cada iteración de Grover, cuando N es grande, se rota un ángulo de aproximadamente $2/\sqrt{N}$ y que el ángulo inicial es aproximadamente $1/\sqrt{N}$. Así que luego de k iteraciones, se tendrá un ángulo de aproximadamente $(2k + 1)/\sqrt{N}$. Por lo tanto, la probabilidad de medir cada estado será:

$$p(x) \approx \begin{cases} \frac{(2k+1)^2}{N} & \text{si } x = \omega \\ \frac{1}{N} & \text{si } x \neq \omega \end{cases}. \quad (5.36)$$

Si realizamos esto en η sistemas idénticos, entonces, mediremos el valor deseado $\eta(2k+1)^2/N \pm O(\sqrt{\eta k^2/N})$ veces y cada otro estado $\eta/N \pm O(\sqrt{\eta k^2/N})$ veces. Si tomamos $\eta = k$, entonces, mediremos ω alrededor de $k(2k+1)^2/N \pm O(\sqrt{k^3/N})$ veces. Ahora, si tomamos k en el orden de $O(\sqrt[3]{N})$, tendremos ω alrededor de $\sqrt[3]{N}(2\sqrt[3]{N}+1)^2 \pm O(1)$ veces. Como N es grande, podemos hacer la aproximación $2\sqrt[3]{N}+1 \approx 2\sqrt[3]{N}$ y entonces, tendremos ω alrededor de $4 \pm O(1)$ veces. Mientras que todos los otros valores ocurran sólo $N^{-2/3} \pm O(1)$ veces cada uno. Así que, el estado medido con mayor frecuencia ha de ser, con seguridad, el estado deseado.

Finalmente, la parte cuántica de este algoritmo tiene una complejidad temporal de $O(\sqrt[3]{N})$ y el procesamiento posterior de las mediciones realizadas también tendrá una complejidad temporal de $O(\sqrt[3]{N})$, pues esta es la cantidad de datos a procesar. Por lo tanto, la complejidad total de este algoritmo es $O(\sqrt[3]{N})$, la cual es menor a $O(\sqrt{N})$ de la versión tradicional y a $\Omega(N \log(N))$ de la versión en un paso.

5.3. Simulaciones

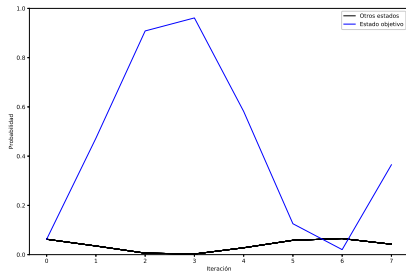
Se realizaron simulaciones del algoritmo de Grover con $|\omega\rangle = |0000\rangle$, $|\omega\rangle = |0110\rangle$ y $|\omega\rangle = |1111\rangle$. También se realizaron simulaciones del algoritmo de amplificación de amplitud con $\mathcal{W} = \{9, 13\} = \{1001_2, 1101_2\}$ y $\mathcal{W} = \{4, 5, 12, 13\} = \{0100_2, 0101_2, 1100_2, 1101_2\}$.

Un conjunto de las simulaciones se ha realizado en Wolfram Mathematica, implementando los operadores, es decir U_ω , $U_{\mathcal{W}}$, U_s y la transformada de Hadamard, directamente, de manera matricial, de acuerdo a las definiciones dadas anteriormente. Otro conjunto de las simulaciones ha realizado en Python, definiendo todos los operadores y transformaciones en base a sus construcciones circuitales, a partir de las compuertas nativas de los transmones, resolviendo la ecuación maestra del sistema al aplicar cada compuerta nativa. Al primer conjunto lo llamaremos simulaciones matemáticas, y al segundo, simulaciones circuitales. El código todas las simulaciones de este capítulo se encuentra en el apéndice C.

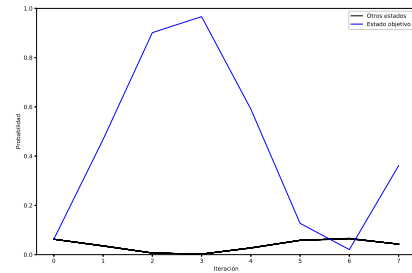
En el caso de la simulaciones matemáticas, sólo se ha simulado el caso sin relajación. Por otro lado, en el caso de la simulaciones circuitales, se ha simulado el sistema tanto sin relajación, como con relajación. En el caso del sistema con relajación, se ha utilizado la ecuación maestra de Lindblad con los operadores de colapso σ_{-i} y tasa de decaimiento $\gamma = 25KHz$.

Como el espacio de Hilbert del sistema en el que sea ejecutado el algoritmo es de 16 dimensiones, ya que es de cuatro qubits, se necesitan $\lfloor \frac{\pi\sqrt{16}}{4} \rfloor = 3$ iteraciones para tener la máxima probabilidad de medir el estado deseado. Sin embargo, la simulación se ha realizado con 7 iteraciones, para apreciar la naturaleza oscilatoria de este algoritmo. Recordemos que este algoritmo consiste en rotaciones en el plano generado por $|\omega\rangle$ y $|s'\rangle$, es decir, que si se aplican más de 3 rotaciones, la probabilidad de éxito debería disminuir, hasta que el estado del sistema se alinee con $-|s'\rangle$, volver a aumentar hasta llegar a $-|\omega\rangle$, disminuir hasta pasar por $|s'\rangle$, pasar de nuevo por el estado inicial $|s\rangle$, y repetirse otra vez el ciclo. La hipótesis es que veremos aproximadamente un período de senoide muestreada, con alrededor de seis muestras por período, en la gráfica de la evolución de la probabilidad de medir $|\omega\rangle$, ya que si luego de tres iteraciones se llega al punto de probabilidad máxima, alrededor de la sexta iteración se debe llegar al punto de probabilidad mínima y en la séptima volvería a aumentar.

En la Figura 5.4 se puede observar la gráfica de la evolución de la probabilidad de medir cada estado en cada iteración del algoritmo de Grover con $|\omega\rangle = |1111\rangle$. Como se puede observar, ambas figuras son bastante similares. La fidelidad entre los estados finales de ambas simulaciones es 0.999875. Además, se ha confirmado la hipótesis de que la evolución de la probabilidad de medir $|1111\rangle$ tiene forma sinusoidal.



(A) Wolfram Mathematica



(B) Python

FIGURA 5.4: Evolución de las probabilidades en el algoritmo de Grover sin relajación

Ahora, compararemos los resultados de la simulación circuital con y sin relajación. Como se puede ver en la Figura 5.5, en el caso con relajación, los estados que no contienen el valor deseado dejan de tener todos la misma probabilidad. Los estados que involucran el estado base ganan probabilidad debido a la relajación de los qubits. La fidelidad entre los estados resultantes de los casos con y sin relajación es de 0.250818.

Además, en el caso con relajación, la probabilidad de medir el estado deseado depende de cuál sea este estado. Mientras más particiones en $|1\rangle$ contenga este estado, peor será el efecto de la relajación en el algoritmo. Esto ocurre porque el algoritmo debe llevar estas particiones a estados excitados, es decir, a estados de energías superiores, y esto es energía que el entorno absorbe por efecto Purcell [76]. El efecto Purcell describe cómo la tasa de emisión espontánea de un sistema cuántico se ve alterada por el entorno del sistema. Las particiones en el estado $|0\rangle$ están en su estado base y no se ven afectadas por este fenómeno, pues este es su estado de mínima energía. Esto se ve reflejado en las siguientes figuras.

En la Figura 5.5c, se tiene $|\omega\rangle = |1111\rangle$, así que este es el caso en el que el entorno tiene el mayor efecto sobre el algoritmo, pues es el caso en el que el sistema tiene las mayores energías. Por otro lado, la Figura 5.5a presenta el caso en el que $|\omega\rangle = |0000\rangle$, este es el caso en el que el entorno tiene el menor efecto sobre el algoritmo, pues es el caso en el que el sistema tiene las menores energías. La Figura 5.5b presenta el caso en el $|\omega\rangle = |0110\rangle$. Este es un caso intermedio y el sistema tiene un efecto distinto sobre cada partición.

El tiempo de vida de los qubits no es suficiente para ejecutar el algoritmo de Grover en su forma tradicional. Esto requeriría tres iteraciones, pero para ese momento, el estado deseado ya no es el más probable, debido a la decoherencia. El único caso en el que el estado deseado sigue siendo el más probable luego de la tercer iteración es el caso en el que este es el estado base. Sin embargo, en todos los casos, la probabilidad máxima de medir el estado correcto ocurre en la primera iteración. Debido a esto, resulta mejor utilizar el algoritmo de Grover en un paso. En cuanto a la versión optimizada, como nuestro sistema tiene cuatro qubits, $N = 16$, el error introducido por las aproximaciones realizadas en el desarrollo de este algoritmo es demasiado grande. La cantidad de iteraciones y subsistemas necesarios estaría alrededor de $\sqrt[3]{N} = 2,519842$, lo cual está en el mismo orden que 1 y sería equivalente a aplicar el algoritmo de Grover en un paso, que, debido a la corto tiempo de vida de los qubits, es la única variante de este algoritmo que es realizable en este sistema.

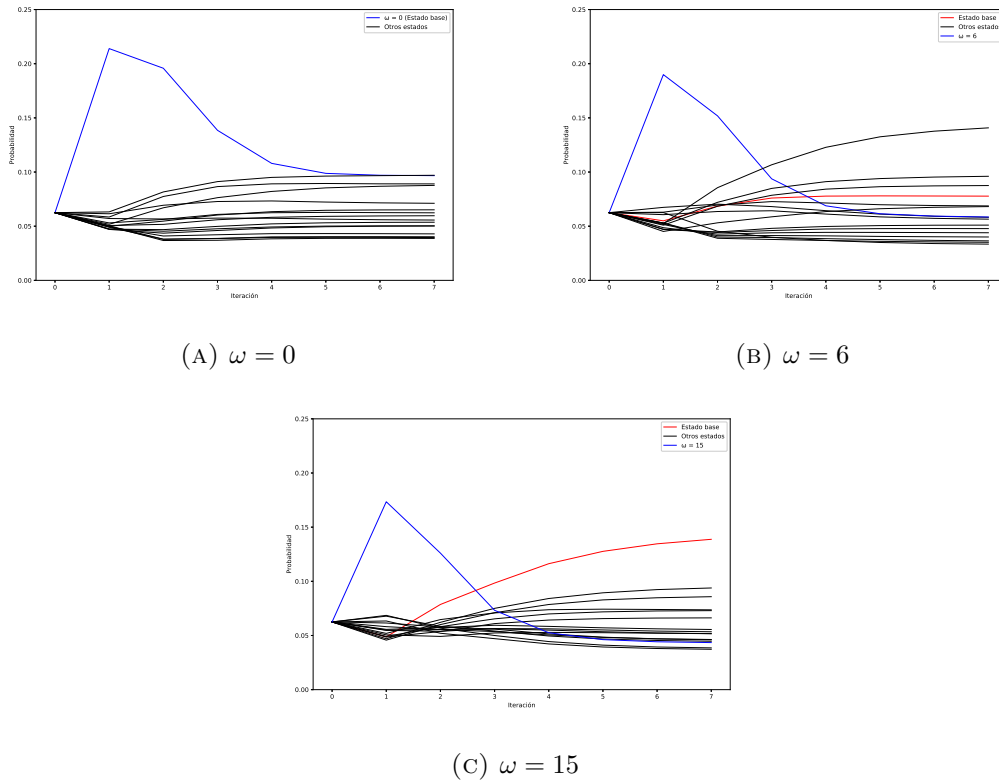
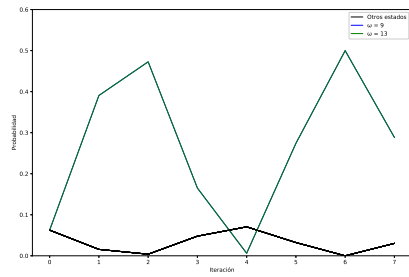


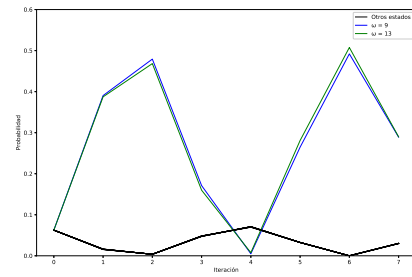
FIGURA 5.5: Evolución de las probabilidades en el algoritmo de Grover con relajación. En (a) se tiene $\mathcal{W} = \{0\} = \{0000_2\}$, este es el caso que se ve menos afectado por el decaimiento de los qubits. En (b) se tiene $\mathcal{W} = \{6\} = \{0110_2\}$. En (c) se tiene $\mathcal{W} = \{15\} = \{1111_2\}$, este es el caso que se ve más afectado por el decaimiento de los qubits.

Ahora veamos los casos en los que se tiene más de un estado deseado, es decir, el algoritmo de amplificación de amplitud. La Figura 5.6 muestra el caso en el que se tienen dos estados deseados, sin relajación. Las graficas obtenidas de la simulación matematica y la simulación circuital son idénticas. Lo mismo ocurre en la Figura 5.7 con el caso en el que se han seleccionado cuatro estados deseados.

La cantidad de iteraciones necesarias en el caso de dos estados deseados es $\lfloor \frac{\pi}{4} \sqrt{\frac{16}{2}} \rfloor = \lfloor 2,221441 \rfloor = 2$. Mientras que en el caso de cuatro estados deseados es $\lfloor \frac{\pi}{4} \sqrt{\frac{16}{4}} \rfloor = \lfloor \pi/2 \rfloor = 1$. Estos valores se confirman viendo las gráficas. En la Figura 5.6, correspondiente al caso de $W = 2$, el pico de mayor probabilidad para los dos estados deseados se encuentra en la segunda iteración. Mientras que en la Figura 5.7, correspondiente al caso de cuatro estados deseados, el pico de máxima probabilidad se encuentra luego de la primera iteración. Aumentar el tamaño del conjunto de estados deseados tiene el efecto de aumentar la frecuencia de las oscilaciones generadas por este algoritmo.

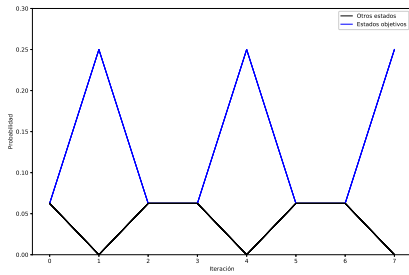


(A) Wolfram Mathematica

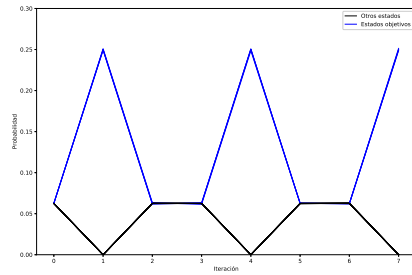


(B) Python

FIGURA 5.6: Evolución de las probabilidades en el algoritmo de amplificación de amplitud sin relajación, $\mathcal{W} = \{9, 13\} = \{1001_2, 1101_2\}$



(A) Wolfram Mathematica



(B) Python

FIGURA 5.7: Evolución de las probabilidades en el algoritmo de amplificación de amplitud con relajación, $\mathcal{W} = \{4, 5, 12, 13\} = \{0100_2, 0101_2, 1100_2, 1101_2\}$

En la Figura 5.8 se presentan los resultados de la simulaciones con relajación del algoritmo de amplificación de amplitud. Se nota que en estos casos se logran tener más iteraciones antes de que la decoherencia haga irreconocibles los estados deseados. Esto ocurre porque estos casos fueron elegidos tal que los operadores de reflexión utilizados $U_{\mathcal{W}}$ involucren menos qubits de control que los operadores U_{ω} . En consecuencia, cada iteración es más corta y se pueden realizar más iteraciones en el tiempo de vida de los qubits.

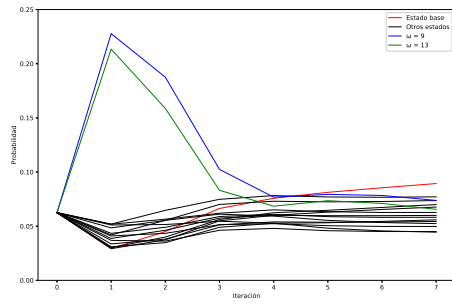
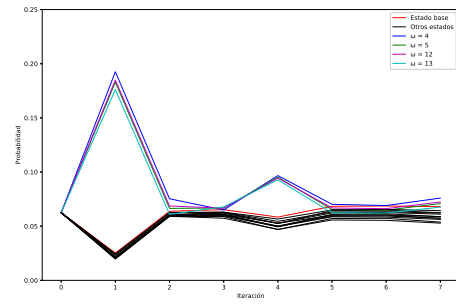

 (A) $\mathcal{W} = \{9, 13\}$

 (B) $\mathcal{W} = \{4, 5, 12, 13\}$

FIGURA 5.8: Evolución de las probabilidades en el algoritmo de amplificación de amplitud con relajación. En (a) se tiene $\mathcal{W} = \{9, 13\} = \{1001_2, 1101_2\}$, en (b) se tiene $\mathcal{W} = \{4, 5, 12, 13\} = \{0100_2, 0101_2, 1100_2, 1101_2\}$

Capítulo 6

Algoritmo de Shor

El algoritmo de Shor es un algoritmo cuántico de factorización de enteros. Dado un entero $N = p \times q$, donde p y q son primos, el algoritmo de Shor encuentra p y q en $O((\log(N))^3)$ pasos, publicado en 1997 por Peter Shor [19]. El algoritmo clásico más eficiente para factorizar enteros es la cibra general del cuerpo de números y funciona con una complejidad heurística de $O(e^{(\sqrt[3]{\frac{64}{9}} + o(1))(\ln(N))^{\frac{1}{3}}(\ln(\ln(N)))^{\frac{2}{3}}})$. Por su capacidad de factorizar números semiprimos, el algoritmo de Shor es capaz de violar el cifrado RSA [77, 78] y el protocolo Diffie-Hellman de intercambio de llaves, sobre los cuáles se basa virtualmente toda la criptografía actual.

El algoritmo de Shor está basado en el algoritmo de estimación de orden, el cuál es una aplicación del algoritmo de estimación de fase [4]. Éste último permite encontrar la fase ϕ del autovalor $e^{i\phi}$ asociado a algún autoestado $|u\rangle$ de un operador unitario U . El algoritmo de estimación de orden utiliza esta estimación para hallar el orden $r > 0$ tal que $a^r \equiv 1 \pmod{m}$, a partir del operador unitario de multiplicación modular.

6.1. Transformada cuántica de Fourier

Una transformada integral cuántica es una transformada integral discreta que actúa en un espacio de Hilbert y tiene un operador unitario asociado, tal que:

$$U = \sum_x \sum_y K(x, y) |y\rangle\langle x|. \quad (6.1)$$

Aplica la transformada

$$|x\rangle \rightarrow K(x, y) |y\rangle, \quad (6.2)$$

Donde $K(x, y)$ se conoce como el Kernel de la transformada.

Una de las transformadas integrales cuánticas más importantes es la transformada cuántica de Fourier (QFT). Sea ω_n la n -ésima raíz primitiva de la unidad:

$$\omega_n = e^{2\pi i/N}, \quad (6.3)$$

Donde $N = 2^n$. El número complejo ω_n define el Kernel K como:

$$K(x, y) = \frac{1}{\sqrt{N}} \omega_n^{xy}. \quad (6.4)$$

La transformada integral discreta con el Kernel K ,

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_x \omega^{-xy} f(x), \quad (6.5)$$

Se llama la transformada discreta de Fourier (DFT).

El Kernel K es unitario ya que:

$$\begin{aligned} (KK^\dagger)(x, y) &= \langle x | KK^\dagger | y \rangle = \langle x | K \sum_z |z\rangle \langle z| K^\dagger | y \rangle \\ &= \sum_z K(x, z) K^\dagger(z, y) = \frac{1}{N} \sum_z \omega^{-xz} \omega^{yz} = \frac{1}{N} \sum_z \omega^{-(z-y)z} = \delta_{xy} \end{aligned} \quad (6.6)$$

La transformada integral cuántica definida con este Kernel se llama QFT.

El Kernel para $n = 1$ es:

$$K_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & e^{2\pi i/2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (6.7)$$

El cual no es más que la compuerta de Hadamard. Para $n = 2$, tenemos $\omega_2 = e^{2\pi i/4} = i$ y:

$$K_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_2^{-1} & \omega_2^{-2} & \omega_2^{-3} \\ 1 & \omega_2^{-2} & \omega_2^{-4} & \omega_2^{-6} \\ 1 & \omega_2^{-3} & \omega_2^{-6} & \omega_2^{-9} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}. \quad (6.8)$$

La QFT inversa está dada por:

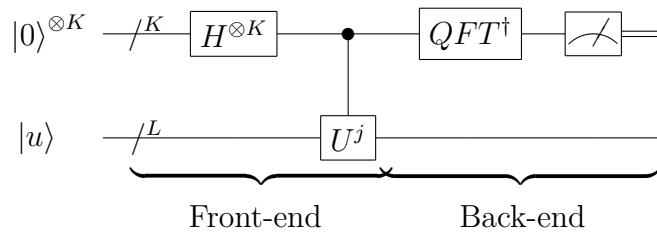
$$QFT^{-1} = QFT^\dagger = \frac{1}{\sqrt{N}} \sum_x \sum_k e^{-2\pi i k x / N} |x\rangle\langle k|. \quad (6.9)$$

6.2. Estimación de fase

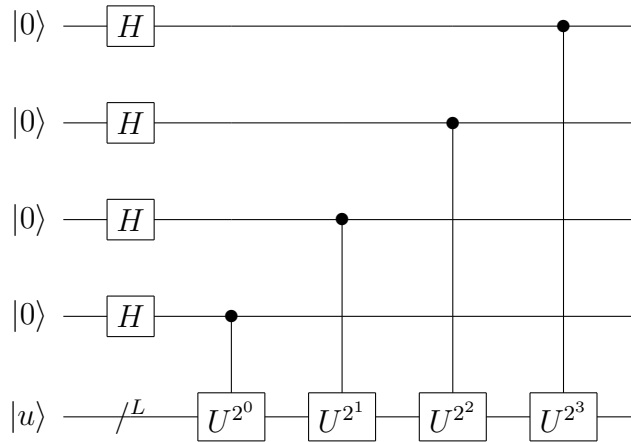
Asumamos que tenemos un operador U , con autoestados $|u\rangle$ de dimensión L , y con autovalores complejos desconocidos $\lambda_\phi = e^{2i\pi\phi}$, donde ϕ es un número real tal que $0 \leq \phi \leq 1$, a ser determinado.

Asumamos también que somos capaces de construir una familia de operadores CU^p , donde $p = 2^0, 2^1, 2^2, \dots, 2^{k-1}$

El circuito cuántico del algoritmo de estimación de fase viene expresado en dos etapas, a las que llamaremos “front-end” y “back-end”.



Analicemos la etapa front-end:



El circuito consta de dos registros. El primer registro empieza con el estado $|0\rangle$, mientras que el segundo empieza con un autoestado $|u\rangle$. Se aplica la transformada de Hadamard al primer registro para convertirlo en $|s\rangle$. Ahora se aplica U controlado por cada uno de los qubits del primer registro, como se ve en el circuito, tal que se aplique la fase del autovalor asociado a $|u\rangle$ n veces al estado $|n\rangle$. Para ilustrar mejor esto, veamos el efecto de CU^j en distintos estados.

$|0\rangle = |0000\rangle :$

Como este estado está compuesto de sólo qubits $|0\rangle$, CU^j actúa como 1 y el estado de salida es igual al de entrada.

$$CU^j |0000\rangle \otimes |u\rangle = e^{i0 \times 2\pi\phi} |0\rangle \otimes |u\rangle. \quad (6.10)$$

$|1\rangle = |0001\rangle :$

La última partición de este estado es $|1\rangle$, así que la componente $CU^{2^0} = CU$ de CU^j actúa como U , por lo tanto, aparece una vez la fase del autovalor $e^{i2\pi\phi}$.

$$CU^j |0001\rangle \otimes |u\rangle = e^{i1 \times 2\pi\phi} |1\rangle \otimes |u\rangle. \quad (6.11)$$

$|6\rangle = |0110\rangle :$

La segunda y la tercera partición de este estado son $|1\rangle$, así que las componentes $CU^{2^1} = CU^2$ y $CU^{2^2} = CU^4$ de CU^j actúan como U^2 y U^4 . En total se tiene U^6 , por lo tanto, aparece seis veces la fase del autovalor $e^{i2\pi\phi}$.

$$CU^j |0110\rangle \otimes |u\rangle = e^{i6 \times 2\pi\phi} |6\rangle \otimes |u\rangle. \quad (6.12)$$

Como se puede ver, $CU^j |n\rangle \otimes |u\rangle = e^{in2\pi\phi} |n\rangle \otimes |u\rangle$. Por lo tanto, como las compuertas cuánticas son operadores lineales, sabemos que

$$CU^j |s\rangle \otimes |u\rangle = CU^j \frac{1}{\sqrt{2^K}} \sum_k |k\rangle \otimes |u\rangle = \frac{1}{\sqrt{2^K}} \sum_k e^{ik2\pi\phi} |k\rangle \otimes |u\rangle. \quad (6.13)$$

Ahora, se aplica la QFT inversa al primer registro.

$$QFT^\dagger = \frac{1}{\sqrt{2^K}} \sum_x \sum_k e^{-i2\pi kx/2^K} |x\rangle\langle k| \quad (6.14)$$

$$\begin{aligned} QFT^\dagger \frac{1}{\sqrt{2^K}} \sum_k e^{ik2\pi\phi} |k\rangle \otimes |u\rangle &= \frac{1}{2^K} \sum_x \sum_k e^{ik2\pi\phi} e^{-i2\pi kx/2^K} |x\rangle \otimes |u\rangle \\ &= \frac{1}{2^K} \sum_x \sum_k \left(e^{i2\pi(\phi - \frac{x}{2^K})} \right)^k |x\rangle \otimes |\phi\rangle \\ &= \frac{1}{2^K} \sum_x \frac{1 - e^{i2\pi(\phi - \frac{x}{2^K})2^K}}{1 - e^{i2\pi(\phi - \frac{x}{2^K})}} |x\rangle \otimes |\phi\rangle. \end{aligned} \quad (6.15)$$

La probabilidad de medir x a la salida del registro será:

$$p(x) = |(\langle x| \otimes \langle u|) |\psi_{output}\rangle|^2 = \frac{1}{4^K} \left| \frac{1 - e^{i2\pi(\phi - \frac{x}{2^K})2^K}}{1 - e^{i2\pi(\phi - \frac{x}{2^K})}} \right|^2 = \frac{1}{4^K} \frac{\sin^2(\pi(\phi - \frac{x}{2^K})2^K)}{\sin^2(\pi(\phi - \frac{x}{2^K}))}. \quad (6.16)$$

La medida de x con probabilidad asociada $p(x)$, corresponde a la estimación de fase $\tilde{\phi} = \frac{x}{2^K}$. La probabilidad es máxima cuando $\delta = \phi - \tilde{\phi}$ es mínima. La probabilidad $p(n)$ decae rápidamente a cero cuando el error δ se aleja del mínimo.

6.3. Estimación de orden

Dado $m \in \mathbb{N}$, se dice que $a, b \in \mathbb{Z}$ son congruentes módulo m si y sólo si $(a-b)/m \in \mathbb{Z}$.

1. Se denota por $a \equiv b \pmod{m}$, siendo m el módulo de la congruencia.
2. Si m divide a $(a - b)$, ambos a y b tienen el mismo resto al ser divididos por el módulo m .

Ejemplos:

$$\begin{aligned} 23 &\equiv 2 \pmod{7} \rightarrow 23 = 3 \times 7 + 2 \\ -6 &\equiv 1 \pmod{7} \rightarrow -6 = -1 \times 7 + 1. \end{aligned}$$

Además si $m \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$ tales que:

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ ac &\equiv bd \pmod{m}. \end{aligned}$$

Por definición el orden de $x \pmod{N}$ es el menor entero r distinto de cero que satisface $x^r = 1 \pmod{N}$

Ejemplo:

Sea $x = 4$ y $N = 13$ entonces $4^p = 13q + R$ obteniendo $4^p \pmod{13} = R$

p	4^p	$4^p = 13q + R$	R
0	1	$4^0 = 13 \times 0 + 1$	1
1	4	$4^1 = 13 \times 0 + 4$	4
2	16	$4^2 = 13 \times 1 + 3$	3
3	64	$4^3 = 13 \times 4 + 12$	12
4	256	$4^4 = 13 \times 19 + 9$	9
5	1024	$4^5 = 13 \times 78 + 10$	10
6	4096	$4^6 = 13 \times 315 + 1$	1
7	16384	$4^7 = 13 \times 1260 + 4$	4
8	65536	$4^8 = 13 \times 5041 + 3$	3
9	262144	$4^9 = 13 \times 20164 + 12$	12
10	1048576	$4^{10} = 13 \times 80659 + 9$	9
11	4194304	$4^{11} = 13 \times 322638 + 10$	10
12	16777216	$4^{12} = 13 \times 1290555 + 1$	1
13	67108864	$4^{13} = 13 \times 5162220 + 4$	4
14	268435456	$4^{14} = 13 \times 20648881 + 3$	3
15	1073741824	$4^{15} = 13 \times 82595524 + 12$	12
16	4294967296	$4^{16} = 13 \times 330382099 + 9$	9

Como podemos ver el período es $r=6$, el cual corresponde al menor r entero distinto de cero para el cual se cumple $4^r = 1 \pmod{13}$ con $r=6$

$$\therefore 4^6 = 1 \pmod{13}$$

Analicemos como la estimación de fase hace posible determinar r , el orden de $x \pmod{N}$, con alta probabilidad y precisión. Primero necesitamos introducir el operador U y sus correspondientes autovectores y autovalores.

Asumamos que dados dos enteros x y N que satisfacen que $x < N$, siendo x coprimo de N , es decir $\text{mcd}(x, N)=1$, existe un operador $U_{x, N}$ tal que:

$$U_{x, N} |y\rangle = |xy \pmod{N}\rangle. \quad (6.17)$$

Sea $\{|u_s\rangle\}_{s=0,1,\dots,r-1}$ el conjunto de r autoestados de U , asociados con los autovalores $e^{i2\pi s/r}$ tal que $U |u_s\rangle = e^{i2\pi s/r} |u_s\rangle$ en el cual la fase es $\phi_s = s/r$ con $0 \leq \phi_s \leq 1$

Tales autoestados $|u_s\rangle$ se definen acorde a: $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi ks}{r}} |x^k \text{ mód } N\rangle$, siendo r a determinar.

Con las siguientes propiedades:

1. $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} r-1 |u_s\rangle = |1\rangle$
2. $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} |u_s\rangle = |x^k \text{ mód } N\rangle$
3. $p(s) = |c_s|^2 = \frac{1}{r}$

Entonces:

$$CU^j |j\rangle \otimes |1\rangle = |j\rangle \otimes |x^j \text{ mód } N\rangle. \quad (6.18)$$

Con este paso entendido vamos ahora a analizar el circuito para determinar el orden:

1. $|\psi_1\rangle = |0\rangle^{\otimes k} \otimes |1\rangle$
2. $|\psi_2\rangle = \frac{1}{\sqrt{M}}(|0\rangle + |1\rangle)^{\otimes k} \otimes |1\rangle; M = 2^k$

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} CU^j(|j\rangle \otimes |1\rangle) \quad (6.19)$$

$$3. |\psi_3\rangle = CU^j |\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} CU^j(|j\rangle \otimes |1\rangle) = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (|j\rangle \otimes |x^j \text{ mód } N\rangle)$$

Pero ya vimos que: $|x^j \text{ mód } N\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} |u_s\rangle$, por lo tanto:

$$|\psi_3\rangle = \sum_{s=0}^{r-1} \sum_{k=0}^{M-1} \frac{1}{\sqrt{M}} e^{2i\pi ks/r} |k\rangle \otimes \frac{1}{\sqrt{r}} |u_s\rangle \quad (6.20)$$

4. Aplicamos la QFT inversa al primer registro, y nos queda:

$$|\psi_4\rangle = (QFT^\dagger \otimes \mathbb{1}) |\psi_3\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{\psi}_s\rangle \otimes |u_s\rangle \quad (6.21)$$

Finalmente, al medir el primer registro, proyectamos la superposición que conforma $|\psi_4\rangle$ en uno de los r estados de $|\psi_s\rangle$

$$p(s) = |\langle \tilde{\psi}_s | \otimes \langle u_s | | \psi_4 \rangle|^2 = \frac{1}{r}. \quad (6.22)$$

lo que nos da $\frac{s}{r}$ correspondiendo a la estimación de fase $\tilde{\psi} = \frac{s}{r}$. Ahora aplicamos el algoritmo clásico de fracciones continuas y determinamos los coprimos.

6.4. Expansión en fracciones continuas

Definamos un número real

$$\chi_n = a_0 + \frac{1}{a_1 + \frac{1}{2 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\dots a_n}}}}}. \quad (6.23)$$

Con $n \leq N$. Cada número real en el conjunto $\{x_0, x_1, \dots, x_{N-1}, x_N\}$ se denomina un convergente de x_n , mientras que x_n se denomina el n -ésimo convergente de x_N .

El conjunto finito $\{a_0, a_1, a_2, \dots, a_n\}$ de números reales positivos corresponde a la cociente $x_n = \frac{p_n}{q_n}$, donde los p_n y q_n son:

$$p_n = a_n p_{n-1} + p_{n-2} \quad (6.24)$$

$$q_n = a_n q_{n-1} + q_{n-2}. \quad (6.25)$$

Con $n \geq 2$ y

$$p_0 = a_0, q_0 = 1, p_1 = 1 + a_0 a_1, q_1 = a_1, \quad (6.26)$$

Para $n = 0, 1$.

Los números reales p_n, q_n son coprimos y satisfacen la relación:

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n. \quad (6.27)$$

Dado un número racional x , si dos enteros p, q son tales que:

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}. \quad (6.28)$$

Entonces p/q es un convergente de x .

Asumamos como ejemplo:

$$\phi = \frac{711}{413} = 1,72154963680387, \quad (6.29)$$

Entonces:

$$\phi = \frac{711}{413} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4 + \frac{1}{5}}}}}}}. \quad (6.30)$$

6.5. Algoritmo de factorización de Shor

Se asume que el número de entrada N es un número compuesto. El algoritmo de Shor halla dos factores de este número. El algoritmo es el siguiente:

1. Si N es par, el número 2 es un factor no trivial de N y se ha hallado una factorización. Fin del algoritmo.
2. Evaluar \sqrt{N} . Si N es un cuadrado perfecto, ya se ha hallado la factorización. Fin del algoritmo.

3. Elegir un número aleatorio $a < N$.
4. Si $GCD(a, N) \neq 1$, entonces este número es un factor no trivial de N y se ha hallado una factorización. Fin del algoritmo.
5. Si a es par, volver al paso 3.
6. Si no, usar el algoritmo de estimación de orden para hallar el período r de $f(x) = a^x \bmod N$.
7. Si r es impar, volver al paso 3.
8. Si $a^r \not\equiv 1 \pmod N$, ir al paso 3.
9. Si $a^{r/2} \equiv -1 \pmod N$, ir al paso 3.
10. Finalmente, $GCD(a^{r/2} + 1, N)$ y $GCD(a^{r/2} - 1, N)$ son factores de N . Fin del algoritmo.

6.6. Simulaciones

Se han realizado simulaciones del algoritmo de Shor factorizando el número 15 y el número 8. En este caso, no se han realizado simulaciones con pérdidas, debido al tiempo que esto hubiese requerido. Se inició la simulación del algoritmo factorizando el número 15 y en más de 48 horas no terminó de aplicar el primer operador de multiplicación modular condicionado. Así que con este algoritmo sólo compararemos la simulación matemática con la simulación circuital sin pérdidas. El código de ambas simulaciones se encuentra en el apéndice [D](#).

6.6.1. Factorización del número 15

Se ha elegido el número 7 para crear el operador unitario de multiplicación modular $U_{7,15}$. Este número cumple las condiciones de ser menor que 15, de ser impar y de ser coprimo con 15.

En la Figura [6.1](#) se puede observar la distribución de probabilidad de la estimación de fase del operador de multiplicación por 7, módulo 15. Como se puede observar, en el caso de la simulación circuital, las estimaciones incorrectas tienen probabilidades distintas de cero. Por otro lado, la fidelidad entre los estados finales de ambas simulaciones es 0.363599.

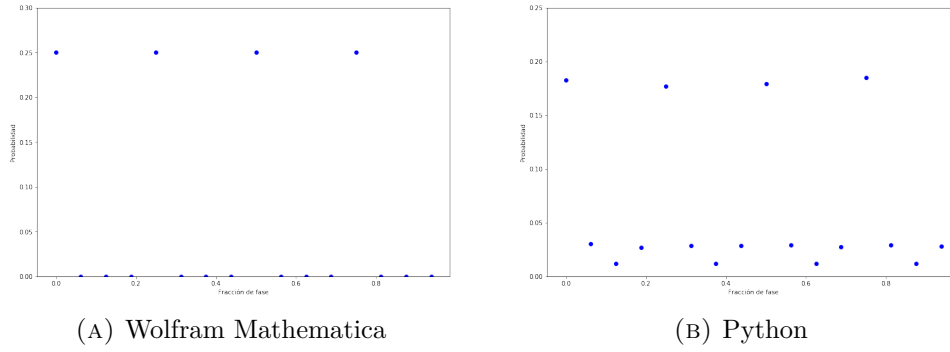


FIGURA 6.1: Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas

Aunque la fidelidad sea tan baja, la probabilidad medir alguno de los cuatro estados correctos en el resultado de la simulación circuital es de 0.723724. Es decir, que sólo se mediría un valor incorrecto alrededor de un cuarto de las veces. Además, la fidelidad clásica entre las distribuciones de la estimación de fase es de 0.850689.

Entonces, tenemos las siguientes estimaciones de fase: $0 \times 2\pi$, $0,25 \times 2\pi$, $0,5 \times 2\pi$, $0,75 \times 2\pi$. Analicemos el algoritmo tras obtener cada una de estas estimaciones.

1. Caso $0 \times 2\pi$:

En este caso no se puede hacer nada, pues no se puede hacer expansión en fracciones continuas con el número cero. Este caso ocurre con 0.25 de probabilidad en la simulación matemática y con 0.182651 de probabilidad en la simulación circuital.

2. Caso $0,25 \times 2\pi$:

En este caso, se tiene la siguiente expansión en fracciones continuas:

$$\tilde{\varphi} = 0 + \frac{1}{4}. \quad (6.31)$$

De donde recuperamos el número racional $1/4$, de donde el orden estimado es $r = 4$. Como r es par, $7^4 \bmod 15 \equiv 1$ y $7^{4/2} \bmod 15 \equiv 4 \bmod 15 \not\equiv -1 \bmod 15$, podemos continuar y hallar la siguiente factorización:

$$15 = GCD(7^{4/2}+1, 15) \times GCD(7^{4/2}-1, 15) = GCD(50, 15) \times GCD(48, 15) = 5 \times 3. \quad (6.32)$$

Este caso ocurre con 0.25 de probabilidad en la simulación matemática y con 0.177 de probabilidad en la simulación circuital.

3. Caso $0,5 \times 2\pi$:

En este caso, se tiene la siguiente expansión en fracciones continuas:

$$\tilde{\varphi} = 0 + \frac{1}{2}. \quad (6.33)$$

De donde recuperamos el número racional $1/2$, de donde el orden estimado es $r = 2$. El orden r es par y $7^{2/2} \bmod 15 \equiv 7 \bmod 15 \not\equiv -1 \bmod 15$, pero $7^2 \bmod 15 \equiv 4 \bmod 15 \not\equiv 1 \bmod 15$, así que el algoritmo nos indica que volvamos al primer paso.

Este caso ocurre con 0.25 de probabilidad en la simulación matemática y con 0.179174 de probabilidad en la simulación circuital.

4. Caso $0,75 \times 2\pi$:

En este caso, se tiene la siguiente expansión en fracciones continuas:

$$\tilde{\varphi} = 0 + \frac{1}{1 + \frac{1}{3}}. \quad (6.34)$$

De donde recuperamos el número racional $3/4$, de donde el orden estimado es $r = 4$. Entonces, este caso es similar al de $\tilde{\varphi} = 0,25$ y se tienen los factores 5 y 3. Este caso ocurre con 0.25 de probabilidad en la simulación matemática y con 0.184898 de probabilidad en la simulación circuital.

5. El resto de los casos:

En el resto de los casos, las estimaciones de orden que se obtienen son 8 y 16. Estas estimaciones sólo ocurren en caso de error en la ejecución del algoritmo debido a falta de fidelidad en las compuertas. Si el algoritmo se ejecuta en un sistema sin decoherencia, sin relajación y con compuertas perfectas, estas estimaciones no ocurrirán. Aun así, ellas pasan las pruebas r par, $x^r \bmod N \equiv 1$ y $x^{r/2} \bmod N \not\equiv -1$, pero sólo se obtienen los factores triviales 1 y 15.

En la simulación matemática estos casos no ocurren, pero en la simulación circuital ocurren con 0.276276 de probabilidad.

En total, tenemos que se logra factorizar el número 15 ejecutando el algoritmo de Shor con el operador $U_{7,15}$ con una probabilidad de 0.5 en la simulación matemática y con una probabilidad de 0.361898, esto es, la mitad de las veces en la simulación matemática y más de un tercio de las veces en la simulación circuital.

6.6.2. Factorización del número 8

Se ha elegido el número 3 para crear el operador unitario de multiplicación modular $U_{3,8}$. Este número cumple las condiciones de ser menor que 8, de ser impar y de ser coprimo con 8. El número 8 sin embargo, es par, así que, siguiendo estrictamente el algoritmo, se tendría la factorización con el número 2 y finalizaría el algoritmo. Sin embargo, como 15 es el único número compuesto, no par y no cuadrado que se puede escribir con cuatro bits, aplicaremos la etapa cuántica de todas maneras.

En la Figura 6.2 se puede observar la distribución de probabilidad de la estimación de fase del operador de multiplicación por 3, módulo 8. Como se puede observar, en el caso de la simulación circuital, las estimaciones incorrectas tienen probabilidades distintas de cero. Por otro lado, la fidelidad entre los estados finales de ambas simulaciones es 0.390136.

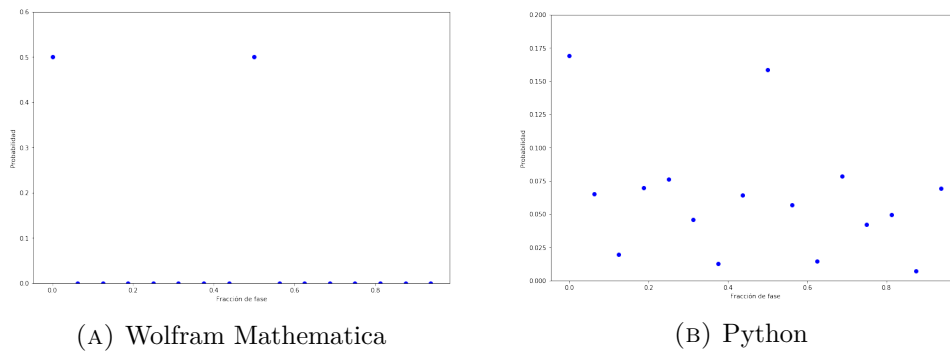


FIGURA 6.2: Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas

Aunque la fidelidad sea tan baja, la probabilidad medir alguno de los dos estados correctos en el resultado de la simulación circuital es de 0.327688. Es decir, que sólo se mediría un valor correcto alrededor de un tercio de las veces. La fidelidad clásica entre las distribuciones de la estimación de fase es de 0.572365.

Entonces, tenemos las siguientes estimaciones de fase: $0 \times 2\pi$ y $0,5 \times 2\pi$. Analicemos el algoritmo tras obtener cada una de estas estimaciones.

1. Caso $0 \times 2\pi$:

En este caso no se puede hacer nada, pues no se puede hacer expansión en fracciones continuas con el número cero. Este caso ocurre con 0.5 de probabilidad en la simulación matemática y con 0.169189 de probabilidad en la simulación circuital.

2. Caso $0,5 \times 2\pi$:

En este caso, se tiene la siguiente expansión en fracciones continuas:

$$\tilde{\varphi} = 0 + \frac{1}{2}. \quad (6.35)$$

De donde recuperamos el número racional $1/2$, de donde el orden estimado es $r = 2$. Como r es par, $3^2 \bmod 8 \equiv 1$ y $3^{3/2} \bmod 8 \equiv 3 \bmod 8 \not\equiv -1 \bmod 8$, podemos continuar y hallar los siguientes factores:

Este caso ocurre con 0.5 de probabilidad en la simulación matemática y con 0.1585 de probabilidad en la simulación circuital.

3. El resto de los casos:

En el resto de los casos, las estimaciones de orden que se obtienen son 4, 8 y 16. Estas estimaciones sólo ocurren en caso de error en la ejecución del algoritmo debido a falta de fidelidad en las compuertas. Si el algoritmo se ejecuta en un sistema sin decoherencia, sin relajación y con compuertas perfectas, estas estimaciones no ocurrirán. Aun así, ellas pasan las pruebas r par, $x^r \bmod N \equiv 1$ y $x^{r/2} \bmod N \not\equiv -1$, pero sólo se obtienen los factores triviales 1 y 8.

En la simulación matemática estos casos no ocurren, pero en la simulación circuital ocurren con 0.636401 de probabilidad.

En total, tenemos que se logra factorizar el número 8 ejecutando el algoritmo de Shor con el operador $U_{3,8}$ con una probabilidad de 0.5 en la simulación matemática y con una probabilidad de 0.1585, esto es, la mitad de las veces en la simulación matemática y alrededor de un sexto de las veces en la simulación circuital.

Capítulo 7

Google PageRank

El algoritmo de PageRank fue desarrollado en 1996 en la Universidad de Stanford por Larry Page y Sergey Brin [79], los cuales fueron los fundadores de Google.

Este algoritmo se basa en la idea de que sitios web importantes tienen muchos vínculos que apuntan hacia ellos, lo que conduce a pensar en la web como una red ponderada orientada. Existen muchos otros algoritmos, algunos más eficientes, pero la importancia de PageRank se sustenta en el poder económico de Google.

Ilustraremos el algoritmo de PageRank con un ejemplo sencillo. Consideremos 5 páginas web distintas a las que denotaremos por 1, 2, 3, 4, y 5, y cuyo grafo es:

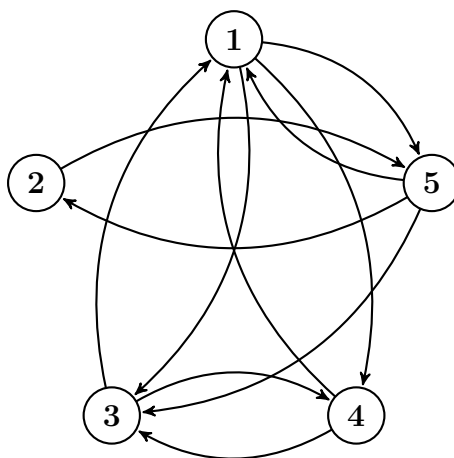


FIGURA 7.1: Grafo de ejemplo para el PageRank clásico

Entonces se deben realizar los siguientes pasos:

1. Determinar la matriz de adyacencia. Algunos autores denotan la matriz de adyacencia por M en el protocolo de PageRank

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

2. Sumamos los elementos de cada una de las columnas.

$$\begin{matrix} 3 & 1 & 2 & 2 & 3 \end{matrix}$$

Estas sumas representan el número de links que salen del nodo o vértice de la página p_j .

3. Dividimos cada elemento de M por la suma de los elementos de la columna a la cual corresponde y llamaremos a la nueva matriz obtenida M'

$$M' = \begin{pmatrix} 0 & 0 & 1/2 & 1/2 & 1/3 \\ 0 & 0 & 0 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/2 & 1/3 \\ 1/3 & 0 & 1/2 & 0 & 0 \\ 1/3 & 1 & 0 & 0 & 0 \end{pmatrix}$$

4. El siguiente paso es encontrar un vector \vec{v} (algunos autores lo llaman \vec{I}) que represente el PageRank de cada una de las páginas. Como tenemos 5 páginas web le asignamos a \vec{v} como valores $\vec{v} = (a, b, c, d, e)^T$, obteniendo así un vector de dimensión $d = 5$.
5. Obtenemos los valores de $\{v_i\}$ a partir de los autovalores de M' , tal que:

$$M'\vec{v} = \lambda\vec{v} \text{ con } \lambda \in R$$

6. Determinamos los autovalores de M'

$$\lambda_1 = 1; \quad \lambda_2 = \frac{-2}{3}; \quad \lambda_3 = \frac{-1}{2}; \quad \lambda_4 = \frac{-1}{3}; \quad \lambda_5 = \frac{1}{3}$$

Tomaremos sólo $\lambda = 1 \rightarrow M'\vec{v} = \vec{v}$ (Ecuación autoconsistente)

7. Hallamos el autovector asociado a $\lambda = 1$. Obteniendo:

$$a = 6; \quad b = 1; \quad c = \frac{16}{3}; \quad d = \frac{14}{3}; \quad e = 3$$

8. Finalmente, Google ordena de mayor a menor las componentes de \vec{v} , quedándonos:

$$\begin{array}{rcl} & & - a \\ & & - c \\ \text{Pantalla} & \rightarrow & - d \\ & & - e \\ & & - b \end{array}$$

La idea de PageRank de Google es que la importancia de una página viene dada por la cantidad de páginas que se enlazan con ella.

Surgen varios problemas:

1. Las matrices hyperlink (hiperenlace) pueden tener billones de entradas en filas y columnas.
2. Calcular los autovectores es un absurdo computacional.
3. Los estudios muestran que un nodo (página web) tiene un promedio de 10 enlaces, y las demás entradas de la matriz son cero.
4. No se encuentra $\lambda = 1$ en la mayoría de los casos.

Por esta razón, un remedio (Patching) del algoritmo de PageRank fue el método de las potencias [32], en el cual la matriz hiperenlace

$$H_{ij} \equiv \begin{cases} \frac{1}{\text{outdeg}(P_j)} & \text{si } P_j \in B_i \\ 0 & \text{en otro caso} \end{cases}$$

debería converger a una solución autoconsistente

$$I^{k+1} = HI^k$$

donde se toma un vector I^0 y se hace interactuar unas 100 veces y el orden mostrado de las páginas es el de I^{100} , ordenadas de mayor a menor. Si se normalizan las columnas de la matriz hipervínculo (hiperenlace) H , obtenemos otra matriz hiperenlace normalizada E .

La matriz E : se sabe de la teoría de matrices estocásticas que 1 es uno de sus autovalores. Además, también se sabe que la convergencia de $I^k = EI^{k-1}$ a $I = EI$ depende del segundo autovalor de E , λ_2 , y es un hecho que $I^k = EI^{k-1}$ converge rápidamente si $|\lambda_2|$ es cercano a cero.

7.1. El algoritmo de remiendo (parcheo) general

Asumamos que el caminante recorre el grafo siguiendo la web con una matriz estocástica E con probabilidad α , y con probabilidad $1 - \alpha$ podrá ir a cualquier página al azar que sea de su interés. La matriz web de este proceso será:

$$G \equiv \alpha E + \frac{1 - \alpha}{N} \mathbb{I} \text{Matriz de Google}$$

\mathbb{I} es una matriz en la cual todas las entradas están establecidas en 1, y N el número de nodos.

Propiedades de G :

1. Es estocástica
2. Irreducible
3. Primitiva
4. El resultado de determinar el estado auto-consistente no depende del vector Google inicial I^0

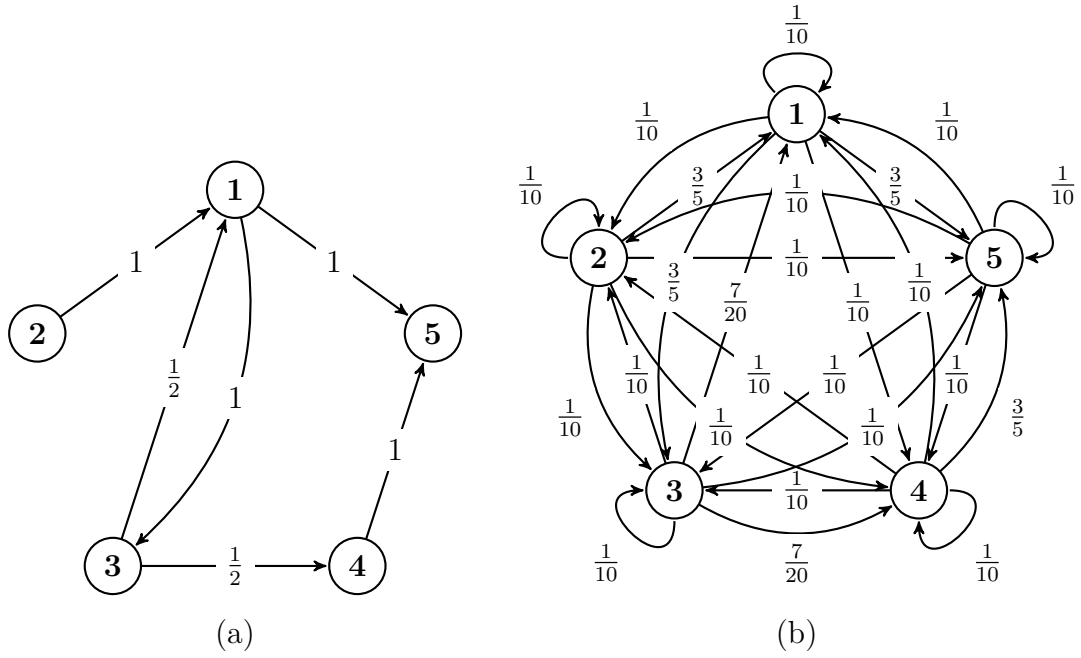


FIGURA 7.2: Transformación de un grafo al crear la matriz de Google con $\alpha = \frac{1}{2}$: Grafo correspondiente a la matriz de adyacencia (a) de la red E (b) remendada de Google G con $\alpha = \frac{1}{2}$

7.2. Interpretación como una caminata aleatoria

La asignación de valores de importancia, se puede replantear como la probabilidad de encontrar un caminante aleatorio en cierto nodo del grafo. En este contexto, tendremos que la probabilidad de encontrar el caminante en el nodo i , en el paso $n + 1$ de la caminata es

$$Pr(x^{(n+1)} = p_i) = \sum_j G_{ij} Pr(x^{(n)} = p_j). \quad (7.1)$$

Utilizando la ley de probabilidad total,

$$Pr(x^{(n+1)} = p_i) = \sum_j Pr(x^{(n+1)} = p_i | x^{(n)} = p_j) Pr(x^{(n)} = p_j), \quad (7.2)$$

Podemos demostrar que G_{ij} es la probabilidad de que el caminante, dado que está en el nodo j , en el paso n , pase al nodo i , en el paso $n + 1$:

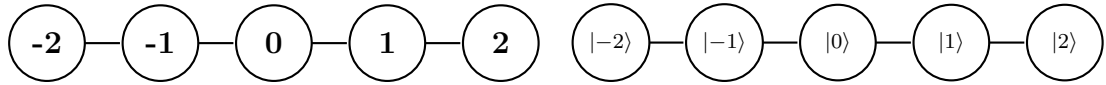
$$G_{ij} = Pr(x^{(n+1)} = p_i | x^{(n)} = p_j). \quad (7.3)$$

En el contexto del Internet, G_{ij} es la probabilidad de que cierto internauta, que se encuentra en la página p_i , entre en la página p_j . El factor αE_{ij} es la probabilidad de que lo haga presionando un enlace presente en p_i , mientras que $\frac{1-\alpha}{N} \mathbb{I}$ es la probabilidad de que lo haga introduciendo la URL directamente.

El factor de amortiguamiento es libre y debe ser calibrado. Se suele usar $\alpha = 0,85$ [32]

7.3. Cuantizando las caminatas aleatorias

La forma obvia y directa de cuantizar una caminata aleatoria sería sustituir el conjunto de nodos $\{p_i\}$ por el conjunto de kets $\{|i\rangle\}$. Sin embargo, esto lleva a sistemas con operadores no unitarios y no es realizable.



Esto nos obliga a buscar maneras alternativas de cuantizar las caminatas aleatorias. La cadena anterior se podría cuantizar agregando un espacio “moneda” al espacio de Hilbert generado por $\{|i\rangle\}$. En este caso, el operador de difusión se interpreta como “lanzar la moneda” para decidir en qué dirección ir [80].

$$\begin{aligned} U &= \sqrt{p} |i+1\rangle\langle i| \otimes |c\rangle\langle c| + \sqrt{1-p} |i-p\rangle\langle i| \otimes |s\rangle\langle s| \\ U^\dagger &= \sqrt{p} |i\rangle\langle i+1| \otimes |c\rangle\langle c| + \sqrt{1-p} |i\rangle\langle i-p| \otimes |s\rangle\langle s| \\ UU^\dagger &= p |i+1\rangle\langle i+1| \otimes |c\rangle\langle c| + (1-p) |i-1\rangle\langle i-1| \otimes |s\rangle\langle s|. \end{aligned}$$

Al realizar la suma sobre i se tiene $\mathbb{1}$, como se deseaba. Sin embargo, esta solución todavía no es satisfactoria, pues exige que $p_{ij} = \frac{1}{\text{outdeg}(j)}$ para que $UU^\dagger = \mathbb{1}$.

Casi todas las cuantizaciones cometen estos dos pecados, aumentar la dimensión del espacio de Hilbert e imponer condiciones sobre el grafo; y en general, se debe cometer al menos uno de los dos. También existen caminatas cuánticas continuas,

no sólo discretas, pero ellas siguen un esquema distinto de la computación cuántica, donde no se busca que el operador de evolución del sistema corresponda a compuertas cuánticas con las cuales construir el operador de difusión, sino directamente al operador de difusión de la caminata cuántica.

7.4. Caminata cuántica de Szegedy

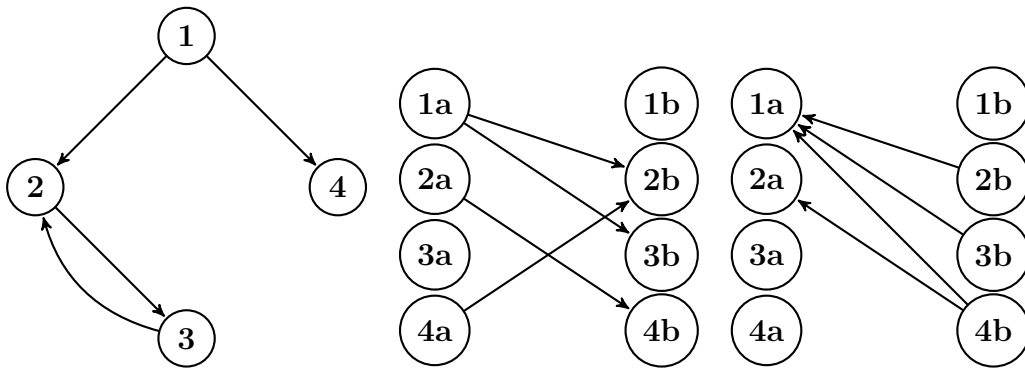
Existe un tipo particular de caminatas aleatorias conocido como caminatas bipartitas. En éstas se tiene dos conjuntos de nodos y sólo ocurren transiciones entre los dos conjuntos, no dentro del mismo.

Szegedy desarrolló una cuantización de estas caminatas. Para esto utilizó operadores de reflexión ($W = \mathbb{1} - 2|w\rangle\langle w|$, similares a los utilizados en el algoritmo de Grover [81]). Aprovechándose del hecho de que un par de reflexiones equivale a una rotación (como en el algoritmo de Grover), creó el siguiente operador de evolución de la caminata: $U = (\mathbb{1} - 2B)(\mathbb{1} - 2A)$, donde A es el proyector sobre las transiciones de la primera partición a la segunda, y B de la segunda a la primera.

$$|\psi_i\rangle = |i\rangle_1 \otimes \sum_j \sqrt{p_{ji}} |j\rangle_2 \quad |\psi_i\rangle = \sum_i \sqrt{p_{ij}} |i\rangle_1 \otimes |i\rangle_2$$

$$A = \sum_i |\psi_i\rangle\langle\psi_i| \quad B = \sum_j |\phi_j\rangle\langle\phi_j|.$$

Si tomamos un grafo cualquiera y lo duplicamos en la forma de un grafo bipartito con ambas particiones iguales y transiciones iguales en ambos sentidos, podemos cuantizar cualquier tipo de caminata. Sólo hay que pagar el precio de duplicar el espacio de Hilbert generado por $\{|i\rangle\}$: $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}$.



En estos casos, podemos escribir el operador de difusión en términos de sólo A , pues como la segunda partición es un reflejo de la primera, $B = A^T$. Entonces: $U = (2A^T - \mathbb{1})(2A - \mathbb{1})$

$$\implies = (2SAS - \mathbb{1})(2A - \mathbb{1}) = S(2A - \mathbb{1})S(2A - \mathbb{1}) = [S(2A - \mathbb{1})]^2$$

Donde S es el operador SWAP, $S = \sum_{ij} |ji\rangle\langle ij|$. Tomando $W = (2A - \mathbb{1})$, el operador de difusión es

$$U = (SW)^2. \quad (7.4)$$

7.5. PageRank Cuántico

Finalmente, procedemos a cuantizar el algoritmo de PageRank. Partimos del hecho de que el algoritmo de PageRank se puede formular como una caminata aleatoria, cuya matriz de probabilidades es la matriz de Google, G . Entonces seguimos el procedimiento de Szegedy [32, 82], sustituyendo p_{ij} por G_{ij} .

Ahora, definimos el valor de PageRank cuántico del nodo i en el paso m como el valor de la medida proyectiva sobre $|i\rangle_2$ del estado resultante de realizar m pasos de una caminata cuántica de Szegedy

$$I_q(P_i, m) = \text{Tr}((\mathbb{1} \otimes |i\rangle\langle i|)U^m |\psi_0\rangle\langle\psi_0| U^{\dagger m}). \quad (7.5)$$

Partiendo del estado inicial dado por la superposición uniforme de los estados asociados a los nodos del grafo, con fases reales, descrito por la siguiente ecuación

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_i |\psi_i\rangle. \quad (7.6)$$

I_q no converge, sino que oscila, así que se toma el centro de las oscilaciones como la medida de importancia de las páginas. Esto se hace promediando I_q sobre m :

$$\langle I_q(P_i) \rangle = \frac{1}{M} \sum_{m=0}^{M-1} I_q(P_i, m)$$

7.6. Circuitos de las caminatas cuánticas de Szegedy

Loke y Wang [1] proponen un esquema para construir eficientemente algoritmos de las caminatas cuánticas de Szegedy. Este esquema consiste en separar las reflexiones del algoritmo en distintas etapas y realizar reflexiones alrededor de estados de la base computacional.

Sea el operador de reflexión del operador de difusión

$$W = 2 \sum_i |\psi_i\rangle\langle\psi_i| - \mathbb{1} = 2 \sum_i |i\rangle\langle i| \otimes |\psi'_i\rangle\langle\psi'_i| - \mathbb{1}, \quad (7.7)$$

Donde $|\psi'_i\rangle = \sum_j \sqrt{p_{ji}} |j\rangle_2$

Si le aplicamos la transformación unitaria $K = \sum_i |i\rangle\langle i| \otimes K_i$ tal que $U_i |\psi'_i\rangle = |b\rangle$, donde $|b\rangle$ es un estado de la base computacional, tendremos:

$$\begin{aligned} KWK^\dagger &= K(2A - \mathbb{1})K^\dagger = 2KAK^\dagger - \mathbb{1} = 2 \sum_i |i\rangle\langle i| \otimes K_i |\psi'_i\rangle\langle\psi'_i| K_i^\dagger - \mathbb{1} \\ &= 2 \sum_i |i\rangle\langle i| \otimes |b\rangle\langle b| - \mathbb{1} = 2\mathbb{1}_1 \otimes |b\rangle\langle b|_2 - \mathbb{1} = D \quad (7.8) \end{aligned}$$

Lo cual se puede implementar fácilmente con compuertas de fase controladas, ya que es una reflexión alrededor de un estado de la base computacional del segundo registro. Sin embargo, esto todavía requeriría hallar N K_i distintos para un grafo de N nodos. Para disminuir la cantidad de K_i a hallar, se pueden aprovechar simetrías en la matriz de adyacencia del grafo. Si separamos el grafo en subgrafos cíclicos, bastaría con hallar un K_i por subgrafo. En los grafos cíclicos, cada fila de la matriz de adyacencia, y de la matriz de Google, es una permutación de la anterior. Lo mismo sucede con los estados asociados a cada uno de los nodos, así que, con un operador de permutación T , se podrían convertir los estados de todos los nodos de un grafo cíclico en un mismo estado de referencia. Por ejemplo, supongamos un grafo, cuyos estados $|\psi'_i\rangle$ son:

$$\begin{aligned}
|\psi'_0\rangle &= \begin{pmatrix} \sqrt{0,0375} \\ \sqrt{0,8875} \\ \sqrt{0,8875} \\ \sqrt{0,8875} \end{pmatrix} & |\psi'_1\rangle &= \begin{pmatrix} \sqrt{0,8875} \\ \sqrt{0,0375} \\ \sqrt{0,8875} \\ \sqrt{0,8875} \end{pmatrix} \\
|\psi'_2\rangle &= \begin{pmatrix} \sqrt{0,8875} \\ \sqrt{0,8875} \\ \sqrt{0,0375} \\ \sqrt{0,8875} \end{pmatrix} & |\psi'_3\rangle &= \begin{pmatrix} \sqrt{0,8875} \\ \sqrt{0,8875} \\ \sqrt{0,8875} \\ \sqrt{0,0375} \end{pmatrix} .
\end{aligned} \tag{7.9}$$

Entonces, el operador de permutación

$$T = X(1)\text{CNOT}(1, 0), \tag{7.10}$$

Permite transformar $|\psi'_1\rangle, |\psi'_2\rangle, |\psi'_3\rangle$ en $|\psi'_0\rangle$ de la siguiente manera:

$$|\psi'_0\rangle = T^\dagger |\psi'_1\rangle = T^3 |\psi'_1\rangle = T^2 |\psi'_2\rangle = T |\psi'_3\rangle . \tag{7.11}$$

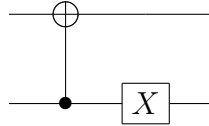


FIGURA 7.3: Operador de permutación T

Luego, siguiendo esta idea, $K_i = K_b^\dagger T_i$, donde $K_b^\dagger |\psi'_r\rangle = |b\rangle$ y $T_i |\psi'_i\rangle = |\psi'_r\rangle$. En otras palabras, $\{K_b\}$ representa el conjunto de K_i necesarios después de separar el grafo, uno por cada subgrafo cíclico; $|\psi'_r\rangle$ es un estado de referencia de cada subgrafo cíclico y podría ser el estado asociado a alguno de los nodos de ese subgrafo; T_i es un operador que transforma el estado de cada nodo en el estado de referencia del subgrafo cíclico correspondiente. En caso de haber elegido $|\psi'_r\rangle$ como el estado de alguno de los nodos del subgrafo cíclico, entonces T_i puede ser un mismo operador de permutación aplicado repetidas veces para todos los nodos del mismo subgrafo, como en el ejemplo anterior.

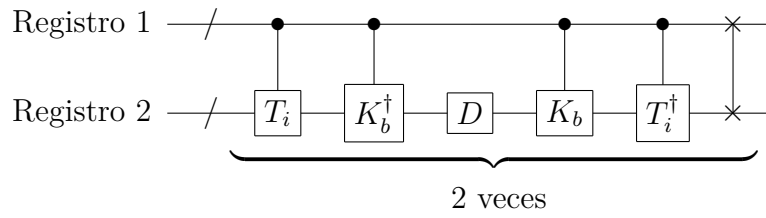


FIGURA 7.4: Circuito de Loke para las caminatas cuánticas de Szegedy

En resumen, el proceso para construir el circuito de una caminata de Szegedy es:

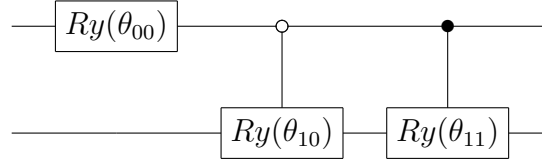
1. Hallar la matriz de Google del grafo.
2. Separar las filas de la matriz en grupos de filas tales que las filas de cada grupo sean permutaciones una de la otra.
3. Hallar los operadores de permutación T_i .
4. Hallar los operadores K_b que conviertan un estado de referencia $|\phi_{r_i}\rangle$ de cada grupo en un mismo estado de referencia $|b\rangle$ de la base computacional.
5. Hallar el operador de reflexión D .
6. Construir el operador de difusión a partir del circuito de la Figura 7.4.

Loke y Wang sólo muestran como realizar K_i para unos pocos casos particulares de caminatas cuánticas de Szegedy que utilizan como ejemplo en su paper. En este trabajo mostramos cómo realizar cualquier K_i para caminatas cuánticas de Szegedy asociadas a grafos de cuatro nodos.

Todos los coeficientes de los estados involucrados en el algoritmo de PageRank son reales positivos o cero. Es decir, que los qubits individuales que forman estos estados pertenecen todos al arco de semicircunferencia que va de $+\hat{z}$ a $-\hat{z}$, pasando por $+\hat{x}$. Esto indica que los operadores K_i deben poder construirse a partir de compuertas $Ry(\theta)$ y compuertas $Ry(\theta)$ condicionadas tomando $0 \leq \theta \leq \pi$.

En lo que sigue se considerará $|b\rangle = |0\rangle$ y que los grafos son de cuatro nodos. De esta manera, podemos asumir que

$$K_i = CRy_n(0, 1, \theta_{11})CRy_b(0, 1, \theta_{10})Ry(0, \theta_{00}). \quad (7.12)$$

FIGURA 7.5: Circuito de K_i

Entonces, para hallar K_i , debemos resolver la siguiente ecuación y hallar $\theta_{11}, \theta_{10}, \theta_{00}$

$$CRy_n(0, 1, \theta_{11})CRy_b(0, 1, \theta_{10})Ry(0, \theta_{00})|0\rangle = |\phi_{r_i}\rangle. \quad (7.13)$$

Sin embargo, esto conduce a un sistema de cuatro ecuaciones y tres variables. Para poder resolver este sistema por métodos numéricos se modifica la ecuación de la siguiente manera, sabiendo que θ_x debe ser $n2\pi$, donde n es entero, quedándonos

$$\cos\left(\frac{\theta_{00}}{2}\right)\cos\left(\frac{\theta_{10}}{2}\right) = \sqrt{G_1} \quad (7.14)$$

$$\cos\left(\frac{\theta_{00}}{2}\right)\sin\left(\frac{\theta_{10}}{2}\right) = \sqrt{G_2} \quad (7.15)$$

$$\cos\left(\frac{\theta_{11}}{2}\right)\sin\left(\frac{\theta_{00}}{2}\right) = \sqrt{G_3} \quad (7.16)$$

$$\sin\left(\frac{\theta_{00}}{2}\right)\sin\left(\frac{\theta_{11}}{2}\right) = \sqrt{G_4}. \quad (7.17)$$

Esto se puede solucionar recordando la normalización de los estados cuánticos y de las matrices estocásticas, entonces, sabemos que $G_4 = 1 - (G_1 + G_2 + G_3)$. Por lo que podemos reducir el sistema de ecuaciones a uno de tres variables

$$\cos\left(\frac{\theta_{00}}{2}\right)\cos\left(\frac{\theta_{10}}{2}\right) = \sqrt{G_1} \quad (7.18)$$

$$\cos\left(\frac{\theta_{00}}{2}\right)\sin\left(\frac{\theta_{10}}{2}\right) = \sqrt{G_2} \quad (7.19)$$

$$\cos\left(\frac{\theta_{11}}{2}\right)\sin\left(\frac{\theta_{00}}{2}\right) = \sqrt{G_3}. \quad (7.20)$$

Sumando (7.18) y (7.19), y aplicando $\cos^2(\theta) + \sin^2(\theta) = 1$, se tiene:

$$\cos^2\left(\frac{\theta_{00}}{2}\right) \cos^2\left(\frac{\theta_{10}}{2}\right) = G_1 \quad (7.21)$$

$$\cos^2\left(\frac{\theta_{00}}{2}\right) = G_1 + G_2 \quad (7.22)$$

$$\cos^2\left(\frac{\theta_{11}}{2}\right) \sin^2\left(\frac{\theta_{00}}{2}\right) = G_3. \quad (7.23)$$

Ahora, sustituyendo (7.22) en (7.21) y (7.23), y volviendo a aplicar la misma propiedad trigonométrica, se tiene:

$$\cos^2\left(\frac{\theta_{10}}{2}\right) = \frac{G_1}{G_1 + G_2} \quad (7.24)$$

$$\cos^2\left(\frac{\theta_{00}}{2}\right) = G_1 + G_2 \quad (7.25)$$

$$\cos^2\left(\frac{\theta_{11}}{2}\right) = \frac{G_3}{1 - (G_1 + G_2)}. \quad (7.26)$$

Finalmente, se tiene que los ángulos de las rotaciones deben ser:

$$\theta_{00} = 2 \cos^{-1} \left(\sqrt{G_1 + G_2} \right) \quad (7.27)$$

$$\theta_{10} = 2 \cos^{-1} \left(\sqrt{\frac{G_1}{G_1 + G_2}} \right) \quad (7.28)$$

$$\theta_{11} = 2 \cos^{-1} \left(\sqrt{\frac{G_3}{1 - (G_1 + G_2)}} \right). \quad (7.29)$$

7.7. Simulaciones

Se han realizado simulaciones del algoritmo de PageRank con un grafo estrella, un grafo corona, un grafo árbol y un grafo aleatorio, todos de cuatro nodos. Se han realizado simulaciones con y sin pérdidas. El código de las simulaciones se encuentra en el apéndice [E](#).

7.7.1. Grafo estrella

En la Figura 7.6 se observa el grafo estrella utilizado para esta simulación. Este grafo es simétrico, por lo tanto, su matriz de adyacencia es hermítica. Este no es el caso, sin embargo, una vez convertimos el grafo en uno ponderado. La matriz estocástica E no es hermítica, y por extensión la matriz de Google tampoco lo es.

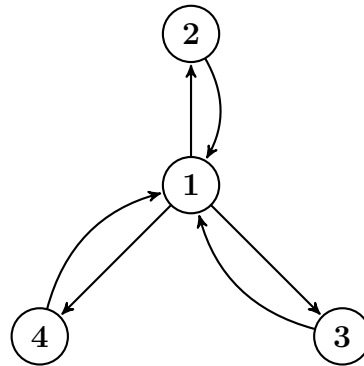


FIGURA 7.6: Grafo estrella

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad (7.30)$$

$$E = \begin{pmatrix} 0 & 1 & 1 & 1 \\ \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & 0 \end{pmatrix} \quad (7.31)$$

$$G = \begin{pmatrix} \frac{3}{80} & \frac{71}{80} & \frac{71}{80} & \frac{71}{80} \\ \frac{77}{240} & \frac{3}{80} & \frac{3}{80} & \frac{3}{80} \\ \frac{77}{240} & \frac{3}{80} & \frac{3}{80} & \frac{3}{80} \\ \frac{77}{240} & \frac{3}{80} & \frac{3}{80} & \frac{3}{80} \end{pmatrix} \quad (7.32)$$

Los tres nodos exteriores de este grafo, además, forman lo que hemos llamado un subgrafo cíclico, por lo que para este grafo necesitaremos dos operadores K_i , uno para estos tres nodos y otro para el nodo central. Las figuras 7.7 - 7.12 muestran cómo construir el circuito del operador de difusión de la caminata de Szegedy asociada a la matriz de Google de este grafo.

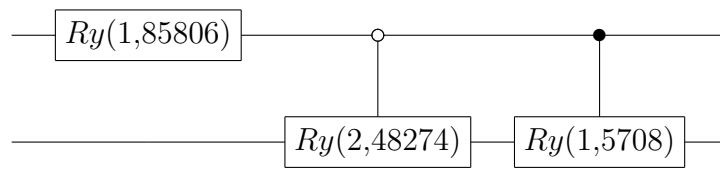


FIGURA 7.7: Circuito de K_1 para el grafo estrella

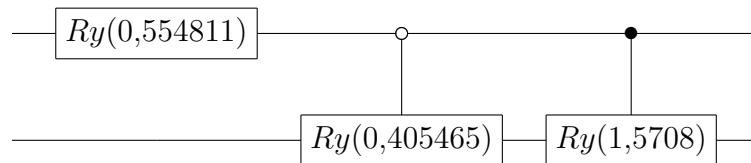


FIGURA 7.8: Circuito de K_2 para el grafo estrella

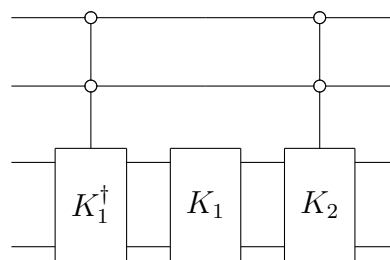


FIGURA 7.9: K_b del grafo estrella

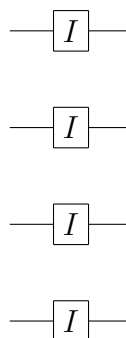


FIGURA 7.10: T del grafo estrella

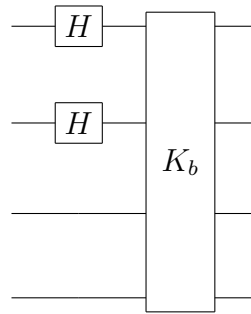


FIGURA 7.11: Preparación del estado inicial para la caminata en el grafo estrella

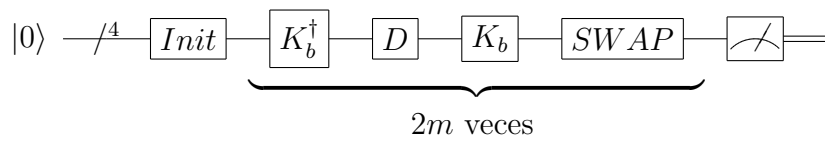
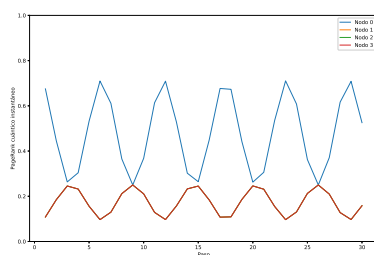
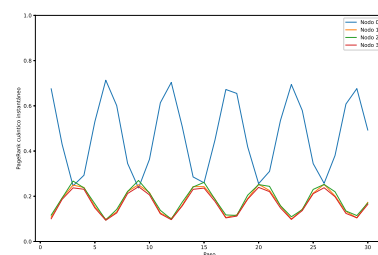


FIGURA 7.12: Circuito del PageRank cuántico del grafo estrella

En la Figura 7.13 se puede observar la gráfica del PageRank cuántico instantáneo sin relajación. En esta figura se puede observar claramente la naturaleza sinusoidal de este algoritmo, por estar basado en reflexiones. Como se puede observar, ambas figuras son bastante similares. La diferencia está en que en el caso de la simulación matemática, el PageRank cuántico de los tres nodos exteriores se solapan perfectamente, mientras que en la simulación circuital, no. Esto se debe a la limitada precisión numérica del solucionador de ecuaciones maestras.



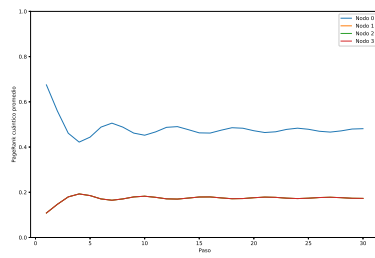
(A) Wolfram Mathematica



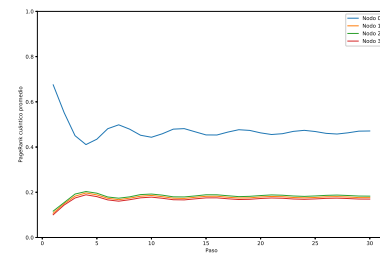
(B) Python

FIGURA 7.13: PageRank cuántico instantáneo del grafo estrella sin pérdidas

En el caso del PageRank promedio, en la Figura 7.14 podemos ver cómo este valor sí converge, a diferencia del PageRank instantáneo, el cuál oscila alrededor del valor de convergencia del PageRank promedio.



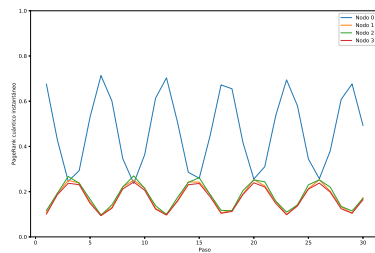
(A) Wolfram Mathematica



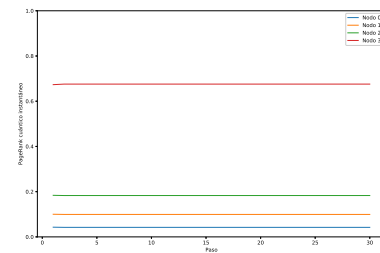
(B) Python

FIGURA 7.14: PageRank cuántico promedio del grafo estrella sin pérdidas

Ahora, compararemos los resultados de la simulación circuital con y sin pérdidas. Como se puede ver en la Figura 7.15, en el caso con pérdidas, el PageRank cuántico es constante. Esto se debe a lo larga que es cada iteración del algoritmo. En el tiempo que realiza una iteración, los qubits ya le han entregado al entorno la energía introducida por las primeras compuertas, así que el estado final de cada iteración se aproxima a la aplicación de sólo las últimas compuertas de la iteración al estado base.

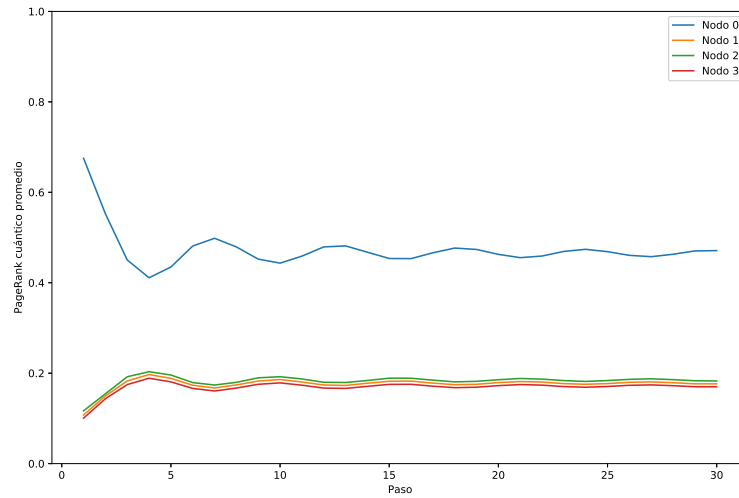


(A) Sin relajación

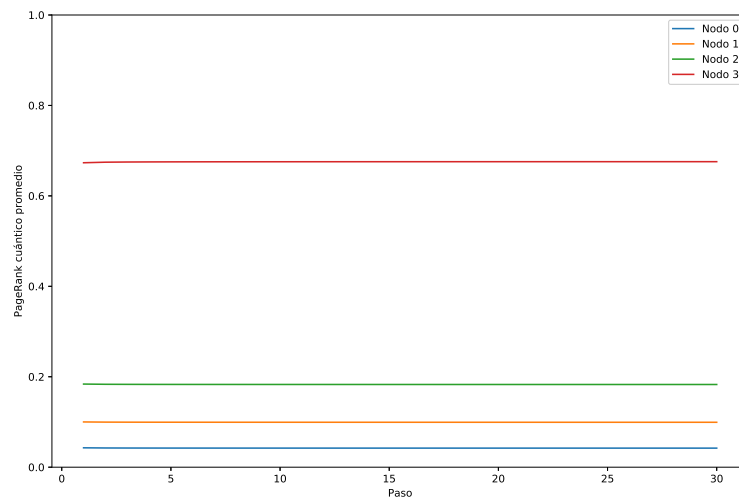


(B) Con relajación

FIGURA 7.15: PageRank cuántico instantaneo del grafo estrella con y sin pérdidas



(A) Sin relajación



(B) Con relajación

FIGURA 7.16: PageRank cuántico promedio del grafo estrella con y sin pérdidas

7.7.2. Grafo corona

En la Figura 7.17 se observa el grafo corona utilizado para esta simulación. Este grafo no es simétrico, por lo tanto, ni su matriz de adyacencia A , ni su matriz estocástica E , ni su matriz de Google G son hermíticas.

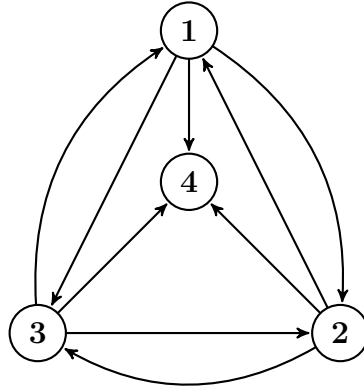


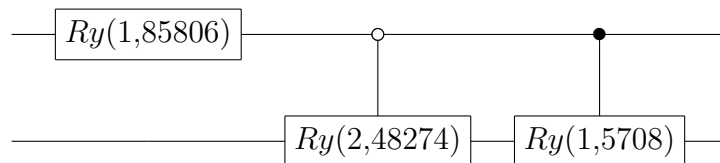
FIGURA 7.17: Grafo corona

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad (7.33)$$

$$E = \begin{pmatrix} 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{4} \end{pmatrix} \quad (7.34)$$

$$G = \begin{pmatrix} \frac{3}{80} & \frac{77}{240} & \frac{77}{240} & \frac{1}{4} \\ \frac{77}{240} & \frac{3}{80} & \frac{77}{240} & \frac{1}{4} \\ \frac{77}{240} & \frac{77}{240} & \frac{3}{80} & \frac{1}{4} \\ \frac{77}{240} & \frac{77}{240} & \frac{77}{240} & \frac{1}{4} \end{pmatrix} \quad (7.35)$$

Como en el grafo corona, en este grafo, los tres nodos exteriores un subgrafo cíclico, por lo que para este grafo también necesitaremos dos operadores K_i , uno para estos tres nodos y otro para el nodo central. Las figuras 7.18 - 7.23 muestran cómo construir el circuito del operador de difusión de la caminata de Szegedy asociada a la matriz de Google de este grafo.

FIGURA 7.18: Circuito de K_1 para el grafo corona

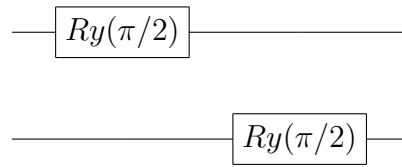


FIGURA 7.19: Circuito de K_2 para el grafo corona

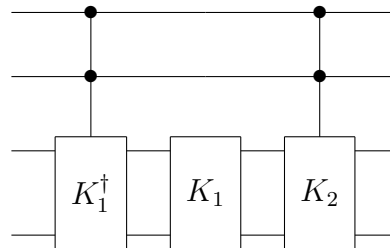


FIGURA 7.20: K_b del grafo corona

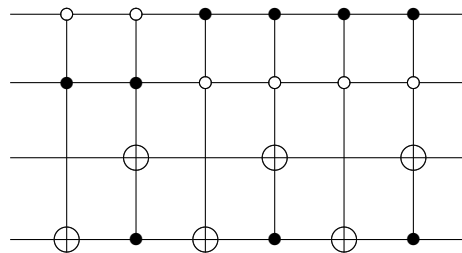


FIGURA 7.21: T del grafo corona

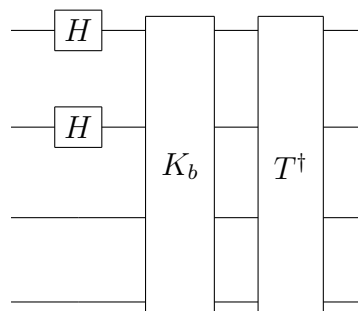


FIGURA 7.22: Preparación del estado inicial para la caminata en el grafo corona

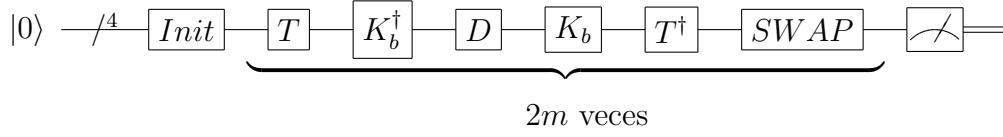
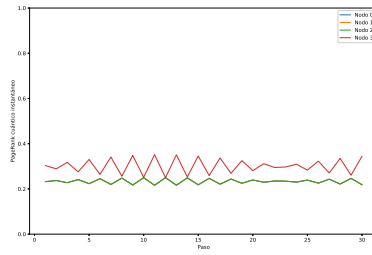
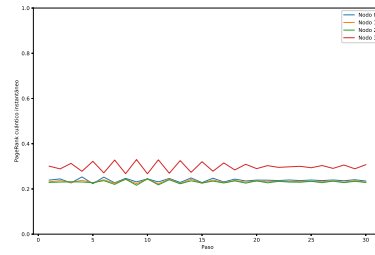


FIGURA 7.23: Circuito del PageRank cuántico del grafo corona

En la Figura 7.24 se pueden observar las gráficas del PageRank cuántico instantáneo sin relajación, resultantes de la simulación matemática, y de la simulación circuital. Como se puede observar, ambas figuras son bastante similares. En el caso de la simulación matemática, el PageRank cuántico de los tres nodos exteriores se solapan perfectamente, mientras que en la simulación circuital, no. Otra diferencia está en que las oscilaciones del PageRank cuántico en la simulación matemática son más amplias que las de la simulación circuital. Esto se debe a la limitada precisión numérica del solucionador de ecuaciones maestras.

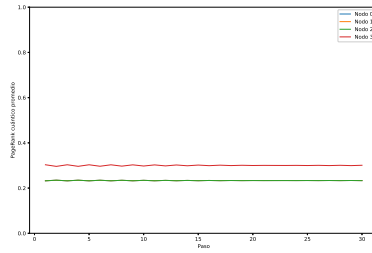


(A) Wolfram Mathematica

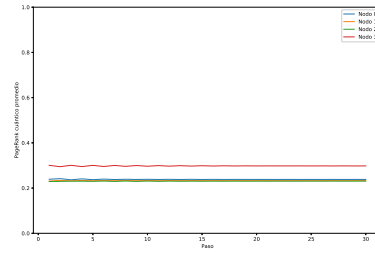


(B) Python

FIGURA 7.24: PageRank cuántico instantáneo del grafo corona sin pérdidas

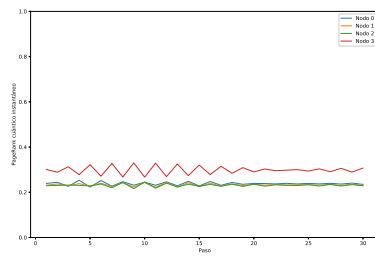


(A) Wolfram Mathematica

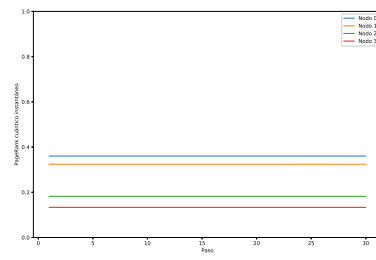


(B) Python

FIGURA 7.25: PageRank cuántico promedio del grafo corona sin pérdidas

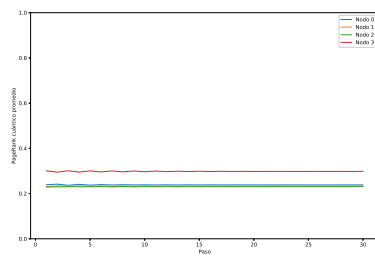


(A) Sin relajación

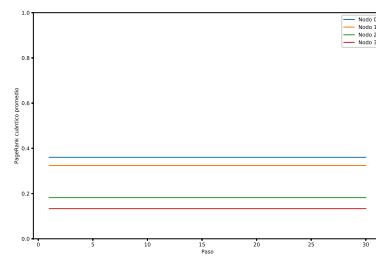


(B) Con relajación

FIGURA 7.26: PageRank cuántico instantáneo del grafo aleatorio con y sin pérdidas



(A) Sin relajación



(B) Con relajación

FIGURA 7.27: PageRank cuántico promedio del grafo aleatorio con y sin pérdidas

7.7.3. Grafo árbol

En la Figura 7.28 se observa el grafo árbol utilizado para esta simulación. Este grafo no es simétrico, por lo tanto, ni su matriz de adyacencia A , ni su matriz estocástica E , ni su matriz de Google G son hermíticas.

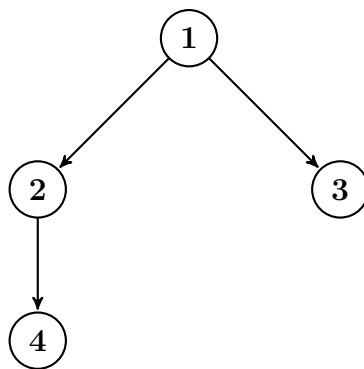


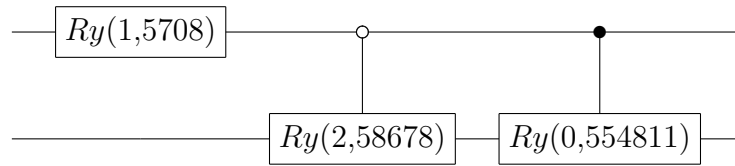
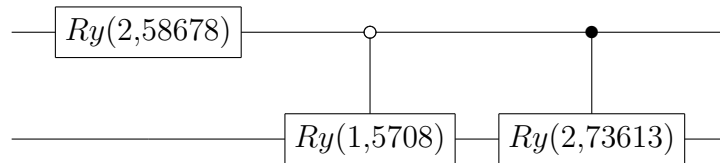
FIGURA 7.28: Grafo árbol

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (7.36)$$

$$E = \begin{pmatrix} 0 & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & 1 & \frac{1}{4} & \frac{1}{4} \end{pmatrix} \quad (7.37)$$

$$G = \begin{pmatrix} \frac{3}{80} & \frac{3}{80} & \frac{1}{4} & \frac{1}{4} \\ \frac{37}{80} & \frac{3}{80} & \frac{1}{4} & \frac{1}{4} \\ \frac{37}{80} & \frac{3}{80} & \frac{1}{4} & \frac{1}{4} \\ \frac{3}{80} & \frac{71}{80} & \frac{1}{4} & \frac{1}{4} \end{pmatrix} \quad (7.38)$$

En este grafo, los dos nodos hojas, 3 y 4, forman un subgrafo cíclico. El nodo raíz, 1, es su propio grafo cíclico, igual que el nodo 2. Por lo tanto, para este grafo necesitaremos tres operadores K_i , uno para los nodos 3 y 4, otro para el nodo 1 y otro para el nodo 2. Las figuras 7.29 - 7.35 muestran cómo construir el circuito del operador de difusión de la caminata de Szegedy asociada a la matriz de Google de este grafo.

FIGURA 7.29: Circuito de K_1 para el grafo árbolFIGURA 7.30: Circuito de K_2 para el grafo árbol

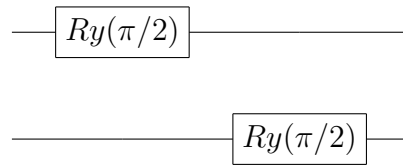


FIGURA 7.31: Circuito de K_3 para el grafo árbol

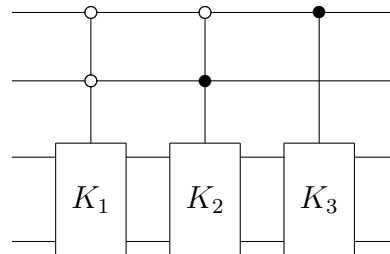


FIGURA 7.32: K_b del grafo árbol

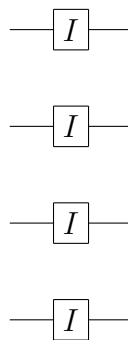


FIGURA 7.33: T del grafo árbol

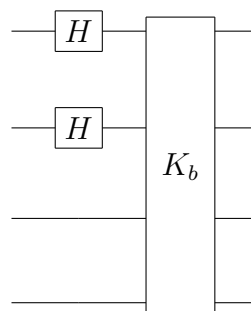


FIGURA 7.34: Preparación del estado inicial para la caminata en el grafo árbol

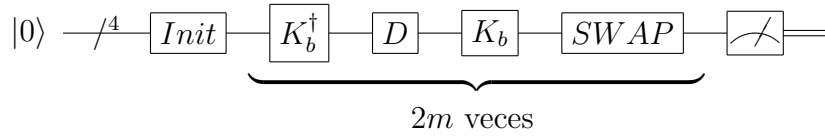
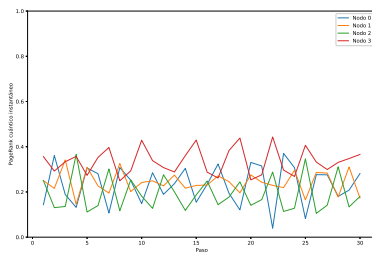
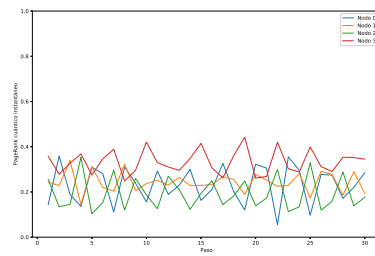


FIGURA 7.35: Circuito del PageRank cuántico del grafo árbol

En la Figura 7.36 se pueden observar las gráficas del PageRank cuántico instantáneo sin relajación, resultantes de la simulación matemática y de la simulación circuital. Como se puede observar, ambas figuras son bastante similares. De la misma manera que con el grafo corona, las oscilaciones en la simulación circuital son de menor amplitud.

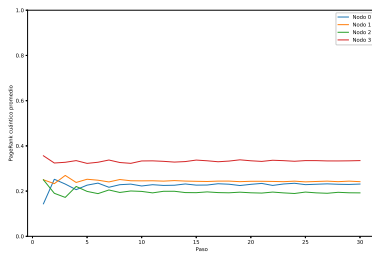


(A) Wolfram Mathematica

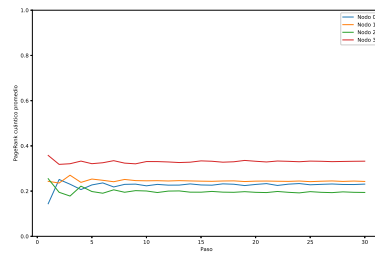


(B) Python

FIGURA 7.36: PageRank cuántico instantáneo del grafo árbol sin pérdidas



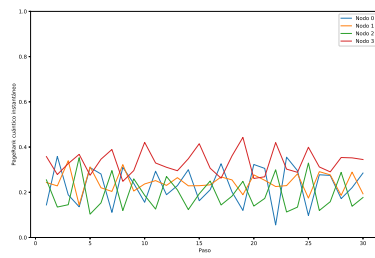
(A) Wolfram Mathematica



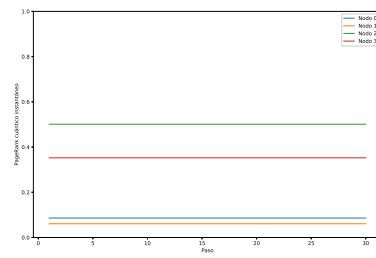
(B) Python

FIGURA 7.37: PageRank cuántico promedio del grafo árbol sin pérdidas

En el caso con pérdidas, presentado en la Figura 7.38, se observa que el PageRank cuántico es constante. Esto se debe a lo larga que es cada iteración del algoritmo. En el tiempo que realiza una iteración, los qubits ya le han entregado al entorno la energía introducida por las primeras compuertas, así que el estado final de cada iteración se aproxima a la aplicación de sólo las últimas compuertas de la iteración al estado base.

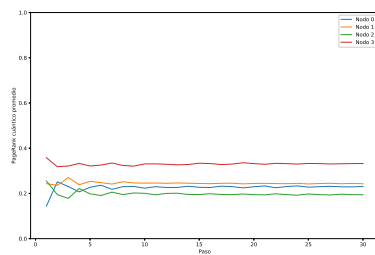


(A) Sin relajación

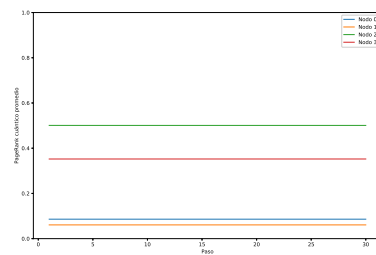


(B) Con relajación

FIGURA 7.38: PageRank cuántico instantáneo del grafo árbol con y sin pérdidas



(A) Sin relajación



(B) Con relajación

FIGURA 7.39: PageRank cuántico promedio del grafo árbol con y sin pérdidas

7.7.4. Grafo aleatorio

En la Figura 7.28 se observa último grafo utilizado para las simulaciones y fue construido de manera aleatoria. Este grafo no es simétrico, por lo tanto, ni su matriz de adyacencia A , ni su matriz estocástica E , ni su matriz de Google G son hermíticas.

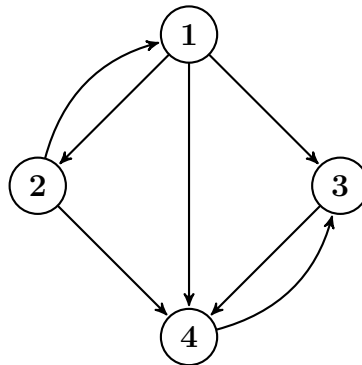


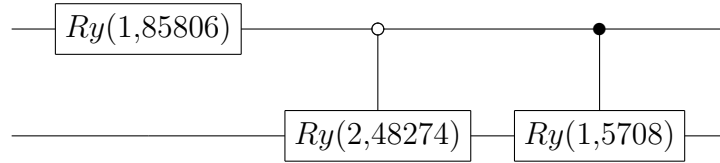
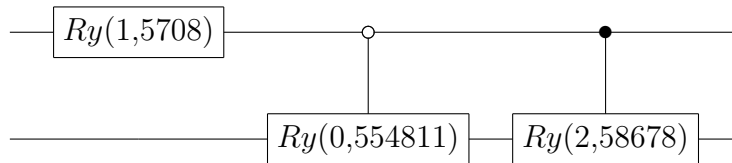
FIGURA 7.40: Grafo aleatorio

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad (7.39)$$

$$E = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & 1 \\ \frac{1}{3} & \frac{1}{2} & 1 & 0 \end{pmatrix} \quad (7.40)$$

$$G = \begin{pmatrix} \frac{3}{80} & \frac{37}{80} & \frac{3}{80} & \frac{3}{80} \\ \frac{77}{240} & \frac{3}{80} & \frac{3}{80} & \frac{3}{80} \\ \frac{77}{240} & \frac{3}{80} & \frac{3}{80} & \frac{71}{80} \\ \frac{77}{240} & \frac{37}{80} & \frac{71}{80} & \frac{3}{80} \end{pmatrix} \quad (7.41)$$

En este grafo, al igual que en el caso anterior, los nodos 3 y 4 forman un subgrafo cíclico, y los nodos 1 y 2 son sus propios subgrafos cíclicos. Por lo tanto, para este grafo también necesitaremos tres operadores K_i , uno para los nodos 3 y 4, otro para el nodo 1 y otro para el nodo 2. Las figuras 7.41 - 7.47 muestran cómo construir el circuito del operador de difusión de la caminata de Szegedy asociada a la matriz de Google de este grafo.

FIGURA 7.41: Circuito de K_1 para el grafo aleatorioFIGURA 7.42: Circuito de K_2 para el grafo aleatorio

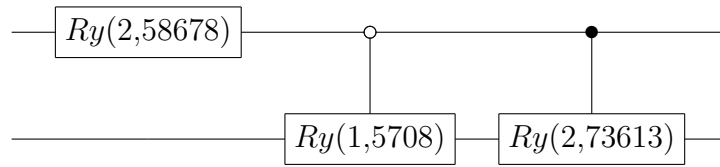


FIGURA 7.43: Circuito de K_3 para el grafo aleatorio

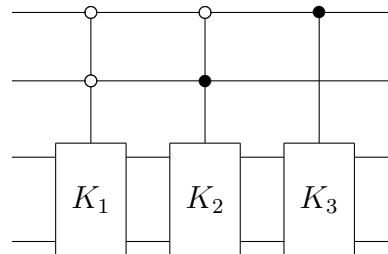


FIGURA 7.44: K_b del grafo aleatorio

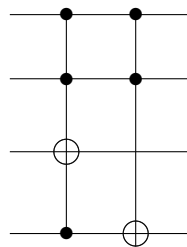


FIGURA 7.45: T del grafo aleatorio

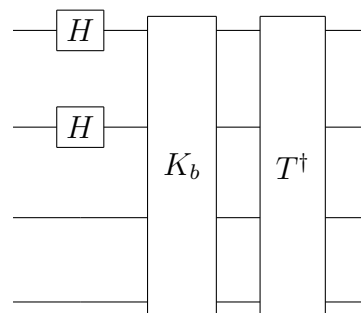


FIGURA 7.46: Preparación del estado inicial para la caminata en el grafo aleatorio

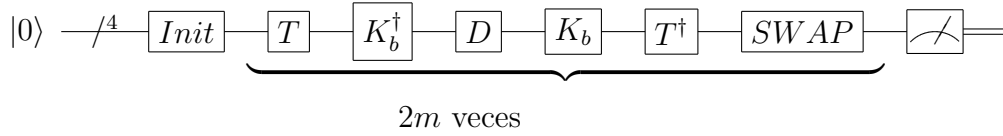
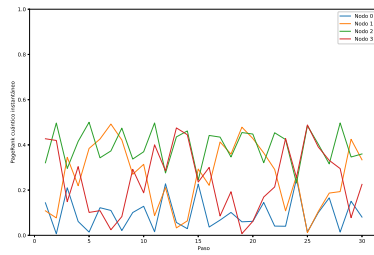
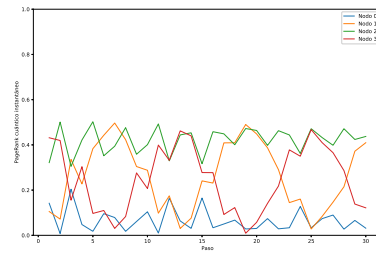


FIGURA 7.47: Circuito del PageRank cuántico del grafo aleatorio

En la Figura 7.48 se pueden observar las gráficas del PageRank cuántico instantáneo sin relajación, resultantes de la simulación matemática y de la simulación circuital. Como se puede observar, ambas figuras son bastante similares. De la misma manera que con el grafo corona, las oscilaciones en la simulación circuital son de menor amplitud. También se nota que las curvas son más suaves en el caso circuital. Por ejemplo, en la curva del nodo 3, la no monotonicidad en los tramos de subida o bajada es menor.

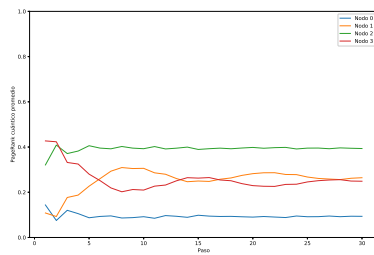


(A) Wolfram Mathematica

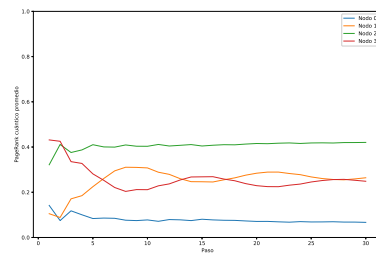


(B) Python

FIGURA 7.48: PageRank cuántico instantáneo del grafo aleatorio sin pérdidas



(A) Wolfram Mathematica

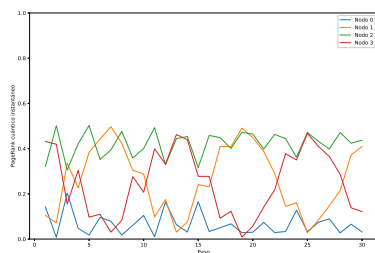


(B) Python

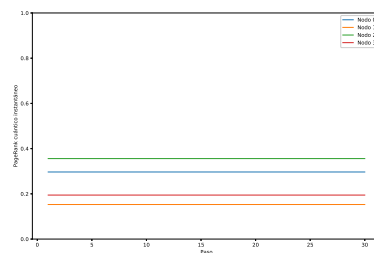
FIGURA 7.49: PageRank cuántico promedio del grafo aleatorio sin pérdidas

En el caso con pérdidas, presentado en la Figura 7.50, se observa que el PageRank cuántico es constante. Esto se debe a lo larga que es cada iteración. En el tiempo que realiza una iteración, los qubits ya le han entregado al entorno la energía introducida por las primeras compuertas, así que el estado final de cada iteración

se aproxima a la aplicación de sólo las últimas compuertas de la iteración al estado base.

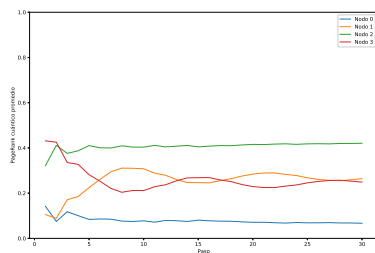


(A) Sin relajación

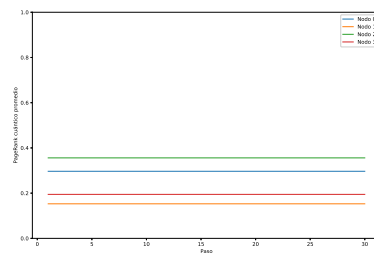


(B) Con relajación

FIGURA 7.50: PageRank cuántico instantáneo del grafo aleatorio con y sin pérdidas



(A) Sin relajación



(B) Con relajación

FIGURA 7.51: PageRank cuántico promedio del grafo aleatorio con y sin pérdidas

Capítulo 8

Conclusiones

En el presente trabajo se estudiaron las bases de Información Cuántica, los fundamentos de la QM que sustentan la superconductividad, los principios de la computación cuántica con transmones y tres algoritmos cuánticos. Se construyó un simulador de transmones acoplados a un mismo resonador, y el set de instrucciones del procesador cuántico formado por estos transmones. Con este simulador se ejecutaron los tres algoritmos estudiados, los cuales son: El algoritmo de búsqueda de Grover, el algoritmo de factorización de Shor y el algoritmo de centralidad PageRank. Además, las simulaciones se realizaron para un sistema cerrado y para un sistema abierto, de tipo markoviano.

Del algoritmo de Grover, se realizaron simulaciones del algoritmo con tres bases de datos distintas de dieciséis elementos y un estado marcado, una de dos estados marcados y una de cuatro estados marcados. Con el algoritmo de Shor se factorizaron los números quince y ocho. Luego, el algoritmo PageRank se aplicó a cuatro grafos, uno estrella, uno corona, uno árbol y uno aleatorio.

Debido a que el presente trabajo persiguió objetivos que en nuestra universidad no se dictan dentro del contenido programático de la carrera de Ingeniería Electrónica, se decidió hacer una presentación detallada de los conceptos y herramienta necesarias para la comprensión de la teoría de información cuántica, la computación cuántica superconductora y los algoritmos simulados. Hasta donde conocemos, no existe ningún otro trabajo que haya simulado estos algoritmos en un sistema abierto markoviano, y, hasta donde sabemos, es el primer trabajo de computación cuántica en un Departamento de Ingeniería Venezolano.

En el presente trabajo, se desarrollaron las siguientes herramientas y se obtuvieron los siguientes resultados novedosos:

1. Una compuerta controlada de fase CP que permita eliminar las fases en las compuertas de negación con dos o más qubits de control, como la de Toffoli.
2. Un conjunto de instrucciones cuánticas basadas en las compuertas nativas de los transmones y un simulador del sistema físico.
3. Un operador de multiplicación por 3 módulo 8 sin qubits de ancilla.
4. La forma explícita del operador de difusión de las caminatas cuánticas de Szegedy para grafos de cuatro nodos, en función de rotaciones en Y controladas.
5. El efecto de la relajación en los algoritmos de Grover, Shor y PageRank.

En el algoritmo de Grover se ha visto que con relajación, sólo se puede realizar una iteración. En la segunda ya no se puede garantizar que el estado deseado, el de probabilidad más alta, y en general tiene probabilidad mayor al final de la primera que al final de la segunda. Así que la mejor alternativa en este algoritmo es su variante de un paso. Sin embargo, debido a que se deben procesar $\Omega(N \log(N))$ medidas, se pierde la ventaja de ejecutar una búsqueda cuántica.

El algoritmo de Shor no se pudo simular con relajación, debido a los largos tiempos que esto hubiese tomado. La ejecución del operador de multiplicación modular $MUL(7, 15)$ tomó 72 horas y la del operador $MUL(3, 8)$ tomó más de 120 horas. Estos operadores se deben aplicar 15 veces en total, así que el tiempo de ejecución de estas simulaciones hubiese sido de al menos 45 y 75 días, para factorizar los números 15 y 8, respectivamente.

En cuanto al algoritmo PageRank, cada iteración del algoritmo es tan larga, que exceden el tiempo de vida de los qubits y al final de cada iteración sólo se tiene el efecto de las últimas compuertas de esta, se pierde el efecto de las primeras. Como la relajación borra toda la información del inicio de la iteración, todas las iteraciones terminan siendo iguales y se miden los mismos valores al final de cada una. Otro gran aporte del presente trabajo de grado es que las técnicas desarrolladas por Szegedy y colaboradores, por ser de muy reciente publicación, hasta donde sabemos nunca se han usado en otros trabajos para simulaciones de circuitos con transmones, lo que nos permite afirmar que nuestras simulaciones están a la punta de las simulaciones a nivel mundial.

Los resultados de las simulaciones del algoritmo de Grover y PageRank nos indican que para sistemas con tiempos de relajación del orden de $O(10^4 ns)$, los protocolos

de corrección de errores son una necesidad. Este es un resultado significativo, pues el record actual de tiempo de vida de un qubit superconductor es inferior a 0.1ms, está en el mismo orden de magnitud que el del sistema simulado.

Apéndices

Apéndice A

Cálculos de Hamiltonianos

A.1. Régimen rotacional del pulso

Partiendo del Hamiltoniano de Jaynes-Cummings para un sistema multibit con pulsos de microondas bajo la aproximación de onda rotante:

$$\begin{aligned}\hat{H}_1 &= \hat{H}_{syst} + \hat{H}_d \\ &= \omega_r a^\dagger a - \frac{1}{2} \sum_i \omega_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_k a \xi_k^* e^{i\omega_d^{(k)} t} + a^\dagger \xi_k e^{-i\omega_d^{(k)} t}.\end{aligned}\tag{A.1}$$

Aplicamos la siguiente transformación unitaria para entrar en el régimen rotacional del pulso aplicado

$$U(t) = \exp\left[\sum_n -i\omega_d^{(n)} t (a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})\right].\tag{A.2}$$

De esta manera, el Hamiltoniano en el régimen rotacional del pulso tendrá la siguiente forma:

$$\hat{H}_2 = U^\dagger (\hat{H}_{syst} + \hat{H}_d) U - iU^\dagger \dot{U},\tag{A.3}$$

Donde \dot{U} representa la derivada temporal del operador unitario U .

Utilizaremos la formula de Baker-Campbell-Hausdorff para calcular este Hamiltoniano, ya que esta nos permite realizar el producto con los exponenciales de operadores calculando sólo conmutadores [83].

$$e^{-\lambda X} H e^{\lambda X} = H + \lambda [H, X] + \frac{\lambda^2}{2!} [[H, X], X] + \dots \quad (\text{A.4})$$

Tomaremos H como el Hamiltoniano y X como el argumento completo del exponencial del operador unitario, incluyendo la parte escalar. Es decir, tendremos $X = \sum_n -i\omega_d^{(n)} t (a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})$ y $\lambda = 1$. En cuanto a los conmutadores, podemos utilizar las siguientes identidades:

$$[a, a^\dagger] = 1 \quad (\text{A.5})$$

$$[a, a^\dagger a] = aa^\dagger a - a^\dagger aa = (aa^\dagger - a^\dagger a)a = [a, a^\dagger]a = a \quad (\text{A.6})$$

$$[a^\dagger, a^\dagger a] = a^\dagger a^\dagger a - a^\dagger aa^\dagger = a^\dagger (a^\dagger a - aa^\dagger) = a^\dagger [a^\dagger, a] = -a^\dagger \quad (\text{A.7})$$

$$[\sigma_+, \sigma_z] = 2\sigma_+ \quad (\text{A.8})$$

$$[\sigma_-, \sigma_z] = -2\sigma_- \quad (\text{A.9})$$

$$[\sigma_-, \sigma_+] = \sigma_z. \quad (\text{A.10})$$

Para que el cálculo sea visualmente más manejable, aprovechamos la propiedad distributiva de los conmutadores y separaremos el Hamiltoniano \hat{H}_1 en los siguientes términos:

1. $\hat{H}_r = \omega_r a^\dagger a$
2. $\hat{H}_q = -\frac{1}{2} \sum_i \omega_{qi} \sigma_{zi}$
3. $\hat{H}_{qr} = \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i})$
4. $\hat{H}_d = \sum_k (a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t})$

Con el primer término tenemos el siguiente conmutador:

$$[\omega_r a^\dagger a, X] = 0. \quad (\text{A.11})$$

El cual es igual a cero, ya que $a^\dagger a$ conmuta con sí mismo, como todo operador, y con σ_{z_i} , ya que actúan sobre particiones distintas del sistema.

Con el segundo término tenemos el siguiente conmutador:

$$\left[-\frac{1}{2} \sum_i \omega_{qi} \sigma_{zi}, X\right] = 0. \quad (\text{A.12})$$

El cual es igual a cero, ya que σ_{z_i} conmuta consigo mismo y con $a^\dagger a$. Con el tercer término tenemos el siguiente conmutador:

$$\begin{aligned} \left[\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), X \right] &= \sum_n -i \omega_d^{(n)} t \left[\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), (a^\dagger a) \right] \\ &\quad + \sum_n -i \omega_d^{(n)} t \left[\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), \left(-\frac{1}{2} \sum_i \sigma_{zi}\right) \right] = \\ \sum_n -i \omega_d^{(n)} t \sum_i g_i (a \sigma_{+i} - a^\dagger \sigma_{-i}) - \sum_n -i \omega_d^{(n)} t \sum_i g_i (a \sigma_{+i} - a^\dagger \sigma_{-i}) &= 0. \end{aligned} \quad (\text{A.13})$$

En este caso, utilizamos el hecho de que a , a^\dagger y $a^\dagger a$ conmutan con σ_{z_i} , σ_{+i} y σ_{-i} , igual que σ_{z_i} , σ_{+i} y σ_{-i} con σ_{z_j} , σ_{+j} y σ_{-j} , donde $i \neq j$, ya que actúan sobre particiones distintas. También utilizamos las identidades (A.5 - A.10), y el hecho de que todo operador conmuta con sí mismo. De esta manera llegamos a una resta de dos términos iguales, así que este conmutador también es cero.

Con el cuarto término tenemos el siguiente conmutador:

$$\begin{aligned} \left[\sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right), X \right] &= \\ \left(\sum_n -i \omega_d^{(n)} t \right) \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} - a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right). \end{aligned} \quad (\text{A.14})$$

Aquí hemos utilizado el hecho que a y a^\dagger conmutan con σ_{z_i} y las identidades (A.6) y (A.7). Este conmutador no es igual a cero como los anteriores, así que tenemos

que utilizar este resultado para calcular $[[H, X], X]$.

$$\left[\left(\sum_n -i\omega_d^{(n)} t \right) \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} - a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right), X \right] = \left(\sum_n -i\omega_d^{(n)} t \right)^2 \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right). \quad (\text{A.15})$$

De igual manera que en el conmutador anterior, hemos utilizado el hecho de que a y a^\dagger conmutan con σ_{z_i} y las identidades (A.6) y (A.7). Este conmutador no es igual a cero como los anteriores, así que tenemos que utilizar este resultado para calcular $[[[H, X], X], X]$.

$$\left[\left(\sum_n -i\omega_d^{(n)} t \right)^2 \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right), X \right] = \left(\sum_n -i\omega_d^{(n)} t \right)^3 \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} - a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right). \quad (\text{A.16})$$

De igual manera que en el conmutador anterior, hemos utilizado el hecho de que a y a^\dagger conmutan con σ_{z_i} y las identidades (A.6) y (A.7). Este conmutador no es igual a cero como los anteriores, así que tenemos que utilizar este resultado para calcular $[[[[H, X], X], X], X]$.

$$\left[\left(\sum_n -i\omega_d^{(n)} t \right)^3 \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} - a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right), X \right] = \left(\sum_n -i\omega_d^{(n)} t \right)^4 \sum_k \left(a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t} \right). \quad (\text{A.17})$$

En este punto podemos notar cierto patrón que nos permite asegurar que el resto de los términos se puede obtener de forma inductiva. Esta serie de conmutadores nos recuerda a la serie de Taylor de la función exponencial con argumento $\sum_n -i\omega_d^{(n)} t$. Al sustituirlos en la fórmula de Baker-Campbell-Hausdorff [84], vemos que efectivamente se trata de este exponencial. Entonces, el primer término del Hamiltoniano \hat{H}_2 es:

$$\begin{aligned}
 U^\dagger(\hat{H}_1)U &= \hat{H}_{sys} + \sum_k \left(e^{\sum_n -i\omega_d^{(n)}t} a\xi_k^* e^{\sum_k i\omega_d^{(k)}t} + e^{-\sum_n -i\omega_d^{(n)}t} a^\dagger \xi_k e^{-\sum_k i\omega_d^{(k)}t} \right) \\
 &= \hat{H}_{sys} + \sum_k (a\xi_k^* + a^\dagger \xi_k).
 \end{aligned} \tag{A.18}$$

Por otro lado, el segundo término es:

$$-iU^\dagger \dot{U} = -iU^\dagger \left(-i \sum_n \omega_d^{(n)} (a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi}) \right) U = - \sum_n \omega_d^{(n)} (a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi}). \tag{A.19}$$

Es decir, $-i$ por la derivada temporal del argumento del exponencial en el que consiste U . Esto es porque todo exponencial conmuta con su argumento y en este caso, la derivada interna de U es igual al argumento del exponencial entre el escalar t , por lo que también conmuta con U . Además de que como U es unitario, se cumple que $U^\dagger U = 1$.

Finalmente, sumando y agrupando términos, nos queda que el Hamiltoniano en el régimen rotativo del pulso es:

$$\begin{aligned}
 \hat{H}_2 &= (\omega_r - \sum_n \omega_d^{(n)}) a^\dagger a - \frac{1}{2} \sum_i (\omega_{qi} - \sum_n \omega_d^{(n)}) \sigma_{zi} \\
 &\quad + \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_k (a\xi_k^* + a^\dagger \xi_k).
 \end{aligned} \tag{A.20}$$

En el caso de un pulso de un sólo modo, este Hamiltoniano toma la forma:

$$\hat{H} = \Delta_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i}) + (a\xi^* + a^\dagger \xi), \tag{A.21}$$

Donde $\Delta_r = \omega_r - \omega_d$ es la diferencia entre la frecuencia de resonancia del resonador y la frecuencia central del pulso, y $\Delta_{qi} = \omega_{qi} - \omega_d$ es la diferencia entre la frecuencia de resonancia de cada qubit y la frecuencia central del pulso.

A.2. Efecto del pulso sobre el qubit

Ahora desplazaremos el campo a , aplicando el operador de desplazamiento

$$D(\alpha) = \exp[\alpha a^\dagger - \alpha^* a], \quad (\text{A.22})$$

Al Hamiltoniano \hat{H}_2 monomodo, con $\dot{\alpha} = -i\Delta_r\alpha - i\xi$, para eliminar el efecto directo del pulso sobre el resonador y ver cómo afecta a los qubits. En el espacio de fase, lo que estamos haciendo con este desplazamiento es fijar el centro de la cuasidistribución de Wigner del sistema con respecto del origen. Los estados coherentes en el espacio de fase evolucionan describiendo oscilaciones en ambas componentes, la real y la imaginaria. Si el estado no está comprimido, la trayectoria descrita es una circunferencia. Que el estado esté comprimido, significa que la oscilación de algunas de las componentes es de menor amplitud que la otra. Así que los estados comprimidos describen trayectorias elípticas en el espacio de fase. De esta manera, el término $-i\Delta_r\alpha$ de $\dot{\alpha}$ eliminará las oscilaciones de un estado coherente no comprimido. Por otro lado, al aplicar el pulso, se desplaza el estado en el espacio de fase, el término $-i\xi$ elimina ese desplazamiento.

De esta manera, el nuevo Hamiltoniano será:

$$\hat{H}_3 = D^\dagger(\alpha)\hat{H}_2D(\alpha) - iD^\dagger(\alpha)\dot{D}(\alpha). \quad (\text{A.23})$$

Los operadores de desplazamiento cumplen con las siguientes propiedades:

$$D(-\alpha) = D^\dagger(\alpha) = D^{-1}(\alpha) \quad (\text{A.24})$$

$$D^\dagger(\alpha)aD(\alpha) = a + \alpha \quad (\text{A.25})$$

$$D^\dagger(\alpha)a^\dagger D(\alpha) = a^\dagger + \alpha^*. \quad (\text{A.26})$$

Utilizando estas dos propiedades, podemos calcular $D^\dagger(\alpha)\hat{H}_2D(\alpha)$ directamente sin utilizar la expansión de Baker-Campbell-Hausdorff, pues basta con sustituir a por $a + \alpha$ y a^\dagger por $a^\dagger + \alpha^*$.

$$\begin{aligned} D^\dagger(\alpha)\hat{H}_2D(\alpha) = \Delta_r(a^\dagger + \alpha^*)(a + \alpha) - \frac{1}{2} \sum_i \Delta_{qi}\sigma_{zi} + \sum_i g_i [(a + \alpha)\sigma_{+i} + (a^\dagger + \alpha^*)\sigma_{-i}] \\ + [(a + \alpha)\xi^* + (a^\dagger + \alpha^*)\xi]. \end{aligned} \quad (\text{A.27})$$

Estas mismas propiedades también se utilizan para calcular el otro término de \hat{H}_3 , de la siguiente manera:

$$-iD^\dagger(\alpha)\dot{D}(\alpha) = -iD^\dagger(\alpha)(\dot{\alpha}a^\dagger - \dot{\alpha}^*a)D(\alpha) = -i[\dot{\alpha}(a^\dagger + \alpha^*) - \dot{\alpha}^*(a + \alpha)]. \quad (\text{A.28})$$

Finalmente, sumando, sustituyendo $\dot{\alpha}$ y agrupando, nos queda:

$$\hat{H}_3 = \Delta_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_i g_i (\alpha\sigma_{+i} + \alpha^* \sigma_{-i}) - \Delta_c \alpha \alpha^*. \quad (\text{A.29})$$

El término $-\Delta_c \alpha \alpha^*$ se desprecia, ya que sólo representa una fase global en la evolución del sistema.

A.3. Régimen dispersivo

Finalmente, aplicamos la transformación

$$U = \exp\left[\sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})\right], \quad (\text{A.30})$$

Donde $\Delta_i = \omega_{qi} - \omega_r$ y realizamos la expansión de Baker-Campbell-Hausdorff de segundo grado sobre los términos $\frac{g_i}{\Delta_i} \ll 1$. El Hamiltoniano efectivo \hat{H}_{eff} será la aproximación del Hamiltoniano \hat{H}_4 resultante de esta expansión.

$$\hat{H}_{eff} \approx \hat{H}_4 = U^\dagger \hat{H}_3 U. \quad (\text{A.31})$$

Para resolver los conmutadores seguiremos el esquema utilizado anteriormente y separaremos el Hamiltoniano \hat{H}_3 en los siguientes términos:

1. $\hat{H}_r = \Delta_r a^\dagger a$
2. $\hat{H}_q = -\frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi}$
3. $\hat{H}_{qr} = \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i})$

$$4. \hat{H}_d = \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i})$$

Con el primer término tenemos el siguiente conmutador:

$$[\Delta_r a^\dagger a, \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})] = \Delta_r \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} + a \sigma_{+i}). \quad (\text{A.32})$$

Con el segundo término tenemos el siguiente conmutador:

$$[-\frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi}, \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})] = - \sum_i \frac{g_i}{\Delta_i} \Delta_{qi} (a^\dagger \sigma_{-i} + a \sigma_{+i}). \quad (\text{A.33})$$

Con el tercer término tenemos el siguiente conmutador:

$$\begin{aligned} & [\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j} - a \sigma_{+j})] = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} ([a \sigma_{+i}, a^\dagger \sigma_{-j}] + [a \sigma_{+i}, -a \sigma_{+j}] + [a^\dagger \sigma_{-i}, a^\dagger \sigma_{-j}] + [a^\dagger \sigma_{-i}, -a \sigma_{+j}]) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} ([a \sigma_{+i}, a^\dagger \sigma_{-j}] + [a^\dagger \sigma_{-i}, -a \sigma_{+j}]) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} (a \sigma_{+i} a^\dagger \sigma_{-j} - a^\dagger \sigma_{-j} a \sigma_{+i} - a^\dagger \sigma_{-i} a \sigma_{+j} + a \sigma_{+j} a^\dagger \sigma_{-i}) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} (a a^\dagger \sigma_{+i} \sigma_{-j} - a^\dagger a \sigma_{-j} \sigma_{+i} - a^\dagger a \sigma_{-i} \sigma_{+j} + a a^\dagger \sigma_{+j} \sigma_{-i}) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} ((1 + a^\dagger a) \sigma_{+i} \sigma_{-j} - a^\dagger a \sigma_{-j} \sigma_{+i} - a^\dagger a \sigma_{-i} \sigma_{+j} + (1 + a^\dagger a) \sigma_{+j} \sigma_{-i}) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + a^\dagger a \sigma_{+i} \sigma_{-j} - a^\dagger a \sigma_{-j} \sigma_{+i} - a^\dagger a \sigma_{-i} \sigma_{+j} + \sigma_{+j} \sigma_{-i} + a^\dagger a \sigma_{+j} \sigma_{-i}) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) + \sum_{ij} g_i \frac{g_j}{\Delta_j} a^\dagger a (\sigma_{+i} \sigma_{-j} - \sigma_{-j} \sigma_{+i} - \sigma_{-i} \sigma_{+j} + \sigma_{+j} \sigma_{-i}) = \\ & \sum_{ij} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi}. \quad (\text{A.34}) \end{aligned}$$

Con el cuarto término tenemos el siguiente conmutador:

$$\begin{aligned}
 & [\sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}), \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})] = \\
 & \sum_{ij} g_i \frac{g_j}{\Delta_j} ([\alpha \sigma_{+i}, a^\dagger \sigma_{-j}] - [\alpha^* \sigma_{-i}, a \sigma_{+j}]) = - \sum_i \frac{g_i^2}{\Delta_i} (\alpha a^\dagger + \alpha^* a) \sigma_{zi}. \quad (\text{A.35})
 \end{aligned}$$

Ahora, los términos de segundo orden, es decir $[[H, X], X]$, se obtienen de la siguiente manera.

Con el primer término tenemos el siguiente conmutador:

$$\begin{aligned}
 & [\Delta_r \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} + a \sigma_{+i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j} - a \sigma_{+j})] = \\
 & \Delta_r \sum_{ij} \frac{g_i g_j}{\Delta_i \Delta_j} ([(a^\dagger \sigma_{-i}), (-a \sigma_{+j})] + [(a \sigma_{+i}), (a^\dagger \sigma_{-j})]) = \\
 & \Delta_r \left(\sum_{ij} \frac{g_i g_j}{\Delta_i \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i^2} a^\dagger a \sigma_{zi} \right). \quad (\text{A.36})
 \end{aligned}$$

Con el segundo término tenemos el siguiente conmutador:

$$\begin{aligned}
 & [- \sum_i \frac{g_i}{\Delta_i} \Delta_{qi} (a^\dagger \sigma_{-i} + a \sigma_{+i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j} - a \sigma_{+j})] = \\
 & - \sum_{ij} \Delta_{qi} \frac{g_i g_j}{\Delta_i \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) + 2 \sum_i \Delta_{qi} \frac{g_i^2}{\Delta_i^2} a^\dagger a \sigma_{zi}. \quad (\text{A.37})
 \end{aligned}$$

Con el tercer término tenemos el siguiente conmutador, aplicando la propiedad distributiva del conmutador, tenemos dos partes. La primera:

$$\begin{aligned}
 & \left[\sum_{ij} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}), \sum_k \frac{g_k}{\Delta_k} (a^\dagger \sigma_{-k} - a \sigma_{+k}) \right] = \\
 & \left[\sum_{i \neq j} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}), \sum_k \frac{g_k}{\Delta_k} (a^\dagger \sigma_{-k} - a \sigma_{+k}) \right] = \\
 & \sum_{i \neq j, k} g_i \frac{g_j}{\Delta_j} \frac{g_k}{\Delta_k} ([\sigma_{+i} \sigma_{-j}, a^\dagger \sigma_{-k}] + [\sigma_{+i} \sigma_{-j}, -a \sigma_{+k}] + \\
 & [\sigma_{+j} \sigma_{-i}, a^\dagger \sigma_{-k}] + [\sigma_{+j} \sigma_{-i}, -a \sigma_{+k}]) = \\
 & \sum_{i \neq j} g_i \frac{g_j}{\Delta_j} ([\sigma_{+i} \sigma_{-j}, \frac{g_i}{\Delta_i} a^\dagger \sigma_{-i}] - [\sigma_{+i} \sigma_{-j}, \frac{g_j}{\Delta_j} a \sigma_{+j}] + \\
 & [\sigma_{+j} \sigma_{-i}, \frac{g_j}{\Delta_j} a^\dagger \sigma_{-j}] - [\sigma_{+j} \sigma_{-i}, \frac{g_i}{\Delta_i} a \sigma_{+i}]) = \\
 & \sum_{i \neq j} g_i \frac{g_j}{\Delta_j} \left(-\frac{g_i}{\Delta_i} a^\dagger \sigma_{zi} \sigma_{-j} - \frac{g_j}{\Delta_j} a \sigma_{+i} \sigma_{zj} - \frac{g_j}{\Delta_j} a^\dagger \sigma_{zj} \sigma_{-i} - \frac{g_i}{\Delta_i} a \sigma_{+j} \sigma_{zi} \right). \quad (\text{A.38})
 \end{aligned}$$

La segunda:

$$\begin{aligned}
 & [-2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi}, \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j} - a \sigma_{+j})] = \\
 & \quad - 2 \sum_{ij} \frac{g_i^2}{\Delta_i} \frac{g_j}{\Delta_j} ([a^\dagger a \sigma_{zi}, a^\dagger \sigma_{-j}] - [a^\dagger a \sigma_{zi}, a \sigma_{+j}]) = \\
 & \quad - 2 \sum_i \frac{g_i^3}{\Delta_i^2} ((a^\dagger a \sigma_{zi} a^\dagger \sigma_{-i} - a^\dagger \sigma_{-i} a^\dagger a \sigma_{zi}) - (a^\dagger a \sigma_{zi} a \sigma_{+i} - a \sigma_{+i} a^\dagger a \sigma_{zi})) \\
 & \quad - 2 \sum_{i \neq j} \frac{g_i^2}{\Delta_i} \frac{g_j}{\Delta_j} (\sigma_{zi} [a^\dagger a, a^\dagger] \sigma_{-j} - \sigma_{zi} [a^\dagger a, a] \sigma_{+j}) = \\
 & \quad - 2 \sum_i \frac{g_i^3}{\Delta_i^2} ((a^\dagger a \sigma_{zi} a^\dagger \sigma_{-i} - a^\dagger \sigma_{-i} a^\dagger a \sigma_{zi}) - (a^\dagger a \sigma_{zi} a \sigma_{+i} - a \sigma_{+i} a^\dagger a \sigma_{zi})) \\
 & \quad - 2 \sum_{i \neq j} \frac{g_i^2}{\Delta_i} \frac{g_j}{\Delta_j} (\sigma_{zi} a^\dagger \sigma_{-j} + \sigma_{zi} a \sigma_{+j}) = \\
 & \quad - 2 \sum_i \frac{g_i^3}{\Delta_i^2} ((a^\dagger \sigma_{zi} \sigma_{-i} (1 + a^\dagger a) - a^\dagger \sigma_{-i} \sigma_{zi} a^\dagger a) - (a^\dagger a \sigma_{zi} \sigma_{+i} a - (1 + a^\dagger a) \sigma_{+i} \sigma_{zi} a)) \\
 & \quad - 2 \sum_{i \neq j} \frac{g_i^2}{\Delta_i} \frac{g_j}{\Delta_j} (\sigma_{zi} a^\dagger \sigma_{-j} + \sigma_{zi} a \sigma_{+j}) = \\
 & \quad - 2 \sum_i \frac{g_i^3}{\Delta_i^2} ((a^\dagger \sigma_{zi} \sigma_{-i} + a^\dagger (2 \sigma_{-i}) a^\dagger a) - (a^\dagger a (-2) \sigma_{+i} a - \sigma_{+i} \sigma_{zi} a)) \\
 & \quad - 2 \sum_{i \neq j} \frac{g_i^2}{\Delta_i} \frac{g_j}{\Delta_j} (\sigma_{zi} a^\dagger \sigma_{-j} + \sigma_{zi} a \sigma_{+j}). \quad (\text{A.39})
 \end{aligned}$$

Descartaremos los términos $\sigma_z \sigma_-$, $a^\dagger a \sigma_-$, $\sigma_z (a + a^\dagger)$, sus conjugados hermíticos y los términos de orden superior, porque estamos considerando el caso en el que $\frac{g_i}{\Delta_i} \ll 1$ y en el que todas las constantes de acoplamiento g_i están en el mismo orden de magnitud. Sumando, agrupando nos queda:

$$\begin{aligned}
 [[H, X], X] & \approx \Delta_r \left(\sum_{ij} \frac{g_i g_j}{\Delta_i \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i^2} a^\dagger a \sigma_{zi} \right) + \\
 & \quad - \sum_{ij} \Delta_{qi} \frac{g_i g_j}{\Delta_i \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) + 2 \sum_i \Delta_{qi} \frac{g_i^2}{\Delta_i^2} a^\dagger a \sigma_{zi} = \\
 & \quad - \left(\sum_{ij} \frac{g_i g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi} \right). \quad (\text{A.40})
 \end{aligned}$$

$$\begin{aligned}
 [H, X] &= \Delta_r \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} + a \sigma_{+i}) - \sum_i \frac{g_i}{\Delta_i} \Delta_{qi} (a^\dagger \sigma_{-i} + a \sigma_{+i}) \\
 &\quad + \sum_{ij} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi} - \sum_i \frac{g_i^2}{\Delta_i} = \\
 &\quad - \sum_i g_i (a^\dagger \sigma_{-i} + a \sigma_{+i}) + \sum_{ij} g_i \frac{g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi} - \sum_i \frac{g_i^2}{\Delta_i}.
 \end{aligned} \tag{A.41}$$

Entonces, sumando y agrupando todos los términos restantes, nos queda:

$$\begin{aligned}
 \hat{H}_4 &\approx \Delta_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) + \\
 &\quad - \sum_i g_i (a^\dagger \sigma_{-i} + a \sigma_{+i}) + \sum_{ij} \frac{g_i g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi} \\
 &\quad - \frac{1}{2} \left(\sum_{ij} \frac{g_i g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}) - 2 \sum_i \frac{g_i^2}{\Delta_i} a^\dagger a \sigma_{zi} \right). \tag{A.42}
 \end{aligned}$$

Finalmente, agrupando términos y simplificando \hat{H}_4 , tenemos el Hamiltoniano efectivo \hat{H}_{eff} de donde saldrán todas las compuertas utilizadas en este trabajo.

$$\begin{aligned}
 \hat{H}_{eff} &= \tilde{\Delta}_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) + \\
 &\quad \sum_{ij} \frac{g_i g_j}{2 \Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i}), \tag{A.43}
 \end{aligned}$$

Donde $\tilde{\Delta}_r = (\omega_r - \frac{1}{2} \sum_i \chi_i \sigma_{zi}) - \omega_d$ y $\chi_i = \frac{g_i^2}{\Delta_i}$. En el caso de dos qubits tenemos el siguiente Hamiltoniano que se encuentra en la literatura [70]

$$\hat{H}_{eff} = \tilde{\Delta}_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i (\Omega_i \sigma_{+i} + \Omega_i^* \sigma_{-i}) + \frac{g_1 g_2 (\Delta_1 + \Delta_2)}{2 \Delta_1 \Delta_2} (\sigma_{-1} \sigma_{+2} + \sigma_{+1} \sigma_{-2}). \tag{A.44}$$

Apéndice B

Códigos del simulador

B.1. Wolfram Mathematica

Este código se realizó en el software Wolfram Mathematica 11.0 con la intención de poder crear las matrices asociadas a las compuertas programadas en Python, y corregir los posibles errores que pudiera haber en dichas compuertas durante su desarrollo.

Primero, se definen los parámetros del sistema, como la frecuencia de resonancia de los qubits y las constantes de acoplamiento.

```
 $\omega_r = 2\pi 10,0;$   
 $\omega_{q_i} := 2\pi \{5,0, 6,0, 7,0, 8,0\}[[i + 1]];$   
 $\omega_{q\text{swap}} = 2\pi 9,0;$   
 $g_i := 2\pi \{0,1, 0,1, 0,1, 0,1\}[[i + 1]];$   
 $\Delta_i := \omega_{q_i} - \omega_r;$ 
```

Ahora se definen las matrices básicas con las cuales se construirán los Hamiltonianos necesarios para realizar las compuertas y asociaciones para asignar los operadores a cada partición de una manera más legible.

```
 $\text{ket0} = \{\{1\}, \{0\}\};$   
 $\text{ket1} = \{\{0\}, \{1\}\};$   
 $\text{Id} = \text{PauliMatrix}[0];$ 
```

```

σx = PauliMatrix[1];
σy = PauliMatrix[2];
σz = PauliMatrix[3];
σp = ket1.ket0†;
σm = ket0.ket1†;

```

Las siguientes son asociaciones que se definen para automatizar la construcción de los productos tensoriales necesarios, ubicando el operador indicado en la partición adecuada.

```

QopAsc[i_, j_, qop_] := < |Mod[i + 0, 4] → qop, Mod[i + 1, 4] → Id,
Mod[i + 2, 4] → Id, Mod[i + 3, 4] → Id| > [j];
Id_i_ := KroneckerProduct[QopAsc[i, 0, Id], QopAsc[i, 1, Id],
QopAsc[i, 2, Id], QopAsc[i, 3, Id]];
σxi_ := KroneckerProduct[QopAsc[i, 0, σx], QopAsc[i, 1, σx],
QopAsc[i, 2, σx], QopAsc[i, 3, σx]];
σyi_ := KroneckerProduct[QopAsc[i, 0, σy], QopAsc[i, 1, σy],
QopAsc[i, 2, σy], QopAsc[i, 3, σy]];
σzi_ := KroneckerProduct[QopAsc[i, 0, σz], QopAsc[i, 1, σz],
QopAsc[i, 2, σz], QopAsc[i, 3, σz]];
σpi_ := KroneckerProduct[QopAsc[i, 0, σp], QopAsc[i, 1, σp],
QopAsc[i, 2, σp], QopAsc[i, 3, σp]];
σmi_ := KroneckerProduct[QopAsc[i, 0, σm], QopAsc[i, 1, σm],
QopAsc[i, 2, σm], QopAsc[i, 3, σm]];

```

Ahora se define la función del pulso gaussiano que se utilizará para las rotaciones en X-Y. También se incluye una función de un pulso rectangular.

```

GaussianPulse[x_, ts_, tf_] :=
(UnitStep[x - μ + 3σ] - UnitStep[x - μ - 3σ])
PDF[NormalDistribution[μ, σ], x]/0.997300204/.

```

```

 $\{\mu \rightarrow \frac{tf+ts}{2}, \sigma \rightarrow \frac{tf-ts}{6}\};$ 
SquarePulse[x_, ts_, tf_] :=
(UnitStep[x -  $\mu$  + 3 $\sigma$ ] - UnitStep[x -  $\mu$  - 3 $\sigma$ ]) / (6 $\sigma$ ) / .
 $\{\mu \rightarrow \frac{tf+ts}{2}, \sigma \rightarrow \frac{tf-ts}{6}\};$ 

```

Se utilizan módulos para definir el operador de evolución con el Hamiltoniano necesario para realizar las rotaciones en X-Y.

```

Rx[target_,  $\theta$ ] := Module[{H :=  $\frac{-1}{2}$  Sum[( $\omega_{q_i} - \omega_{q_{target}}$ )  $\sigma_{z_i}$ , {i, 0, 3}]},
H = H +  $\frac{1}{2} \theta$  GaussianPulse[t, 0, 10]  $\sigma_{x_{target}}$ ;
MatrixExp[-i NIntegrate[H, {t, 0, 10}]]
];
Ry[target_,  $\theta$ ] := Module[{H :=  $\frac{-1}{2}$  Sum[( $\omega_{q_i} - \omega_{q_{target}}$ )  $\sigma_{z_i}$ , {i, 0, 3}]},
H = H +  $\frac{1}{2} \theta$  GaussianPulse[t, 0, 10]  $\sigma_{y_{target}}$ ;
MatrixExp[-i NIntegrate[H, {t, 0, 10}]]
];

```

Se utilizan módulos para definir el operador de evolución con el Hamiltoniano necesario para realizar las compuertas iSWAP y \sqrt{iSWAP} .

```

sqrtiSWAP[target1_, target2_] :=
Module[
{H =  $\frac{-1}{2}$  Sum[ $\omega_{q_i} \sigma_{z_i}$ , {i, 0, 3}] +
Sum[( $g_i g_j / \Delta_i$ ) ( $\sigma_{p_i} \cdot \sigma_{m_j} + \sigma_{m_i} \cdot \sigma_{p_j}$ ) / 2, {i, 0, 3}, {j, 0, 3}],
J = 0,  $\Delta_{swap} = \omega_{q_{swap}} - \omega_r$ },
H = H +  $\frac{1}{2} (\omega_{q_{target1}} \sigma_{z_{target1}} + \omega_{q_{target2}} \sigma_{z_{target2}}) -$ 
 $g_{target1} g_{target2} (\Delta_{target1} + \Delta_{target2}) / (\Delta_{target1} \Delta_{target2})$ 
 $(\sigma_{p_{target1}} \cdot \sigma_{m_{target2}} + \sigma_{m_{target1}} \cdot \sigma_{p_{target2}}) / 2;$ 
H = H -  $\frac{1}{2} \omega_{q_{swap}} (\sigma_{z_{target1}} + \sigma_{z_{target2}}) +$ 
 $g_{target1} g_{target2} (\sigma_{p_{target1}} \cdot \sigma_{m_{target2}} + \sigma_{m_{target1}} \cdot \sigma_{p_{target2}}) / \Delta_{swap};$ 
H =  $g_{target1} g_{target2} (\sigma_{p_{target1}} \cdot \sigma_{m_{target2}} + \sigma_{m_{target1}} \cdot \sigma_{p_{target2}}) / \Delta_{swap};$ 

```

```

J = Abs [gtarget1 gtarget2 / Δswap] ;
MatrixExp [−iH  $\frac{\pi}{4J}$ ]
];
iSWAP[target1_, target2_] :=
Module[
{H =  $\frac{-1}{2}$ Sum [ωqiσzi, {i, 0, 3}] +
Sum [(gigj/Δi) (σpi·σmj + σmi·σpj)/2, {i, 0, 3}, {j, 0, 3}] ,
J = 0, Δswap = ωqswap − ωr},
H = H +  $\frac{1}{2}$  (ωqtarget1σztarget1 + ωqtarget2σztarget2) −
gtarget1gtarget2 (Δtarget1 + Δtarget2) / (Δtarget1Δtarget2)
(σptarget1·σmtarget2 + σmtarget1·σptarget2) / 2;
H = H −  $\frac{1}{2}$ ωqswap (σztarget1 + σztarget2) +
gtarget1gtarget2 (σptarget1·σmtarget2 + σmtarget1·σptarget2) / Δswap;
H = gtarget1gtarget2 (σptarget1·σmtarget2 + σmtarget1·σptarget2) / Δswap;
J = Abs [gtarget1 gtarget2 / Δswap] ;
MatrixExp [−iH  $\frac{\pi}{2J}$ ]
];

```

Finalmente, se definen todas las compuertas del simulador. Ellas no son más que el producto de matrices correspondiente a los circuitos dados en el capítulo 4

```

X[target_] := Rx[target, π] // FullSimplify;
Y[target_] := Ry[target, π] // FullSimplify;
Rz[target_, θ_] := Ry[target, −π/2].Rx[target, θ].Ry[target, π/2] //
FullSimplify;
Z[target_] := Rz[target, π] // FullSimplify;
H[target_] := X[target].Ry[target, π/2] // FullSimplify;
CNOT[control_, target_] :=
Rx[target, π/2].iSWAP[control, target].Rx[control, π/2].
iSWAP[control, target].Rx[target, π/2].iSWAP[control, target].

```

```

H[control].iSWAP[control, target].Rz[control,  $-\pi/2$ ].
Rz[target,  $-\pi/2$ ].H[target]//FullSimplify;
CRy[control_, target_,  $\theta$ ] :=
CNOT[control, target].Ry[target,  $-\theta/2$ ].CNOT[control, target].
Ry[target,  $\theta/2$ ]//FullSimplify;
CRz[control_, target_,  $\theta$ ] :=
CNOT[control, target].Rz[target,  $-\theta/2$ ].CNOT[control, target].
Rz[target,  $\theta/2$ ]//FullSimplify;
SWAP[target1_, target2_] :=
CNOT[target1, target2].CNOT[target2, target1].CNOT[target1, target2]//
FullSimplify;
CH[control_, target_] :=
Ry[target,  $-\pi/4$ ].CNOT[control, target].Ry[target,  $\pi/4$ ]//FullSimplify;
CP00[control_, target_,  $\theta$ ] :=
CRz[target, control,  $\theta/2$ ].CRz[control, target,  $\theta/2$ ].
Rz[target,  $-3\theta/4$ ].Rz[control,  $-3\theta/4$ ]//FullSimplify;
CP01[control_, target_,  $\theta$ ] :=
CRz[target, control,  $\theta/2$ ].CRz[control, target,  $-3\theta/2$ ].
Rz[target,  $5\theta/4$ ].Rz[control,  $-3\theta/4$ ]//FullSimplify;
CP10[control_, target_,  $\theta$ ] :=
CRz[target, control,  $\theta/2$ ].CRz[control, target,  $-3\theta/2$ ].
Rz[target,  $\theta/4$ ].Rz[control,  $\theta/4$ ]//FullSimplify;
CP11[control_, target_,  $\theta$ ] :=
CRz[target, control,  $\theta/2$ ].CRz[control, target,  $\theta/2$ ].
Rz[target,  $\theta/4$ ].Rz[control,  $\theta/4$ ]//FullSimplify;
Toffoli[control1_, control2_, target_] :=
CP11[control1, control2,  $-\pi/2$ ].H[target].CRz[control1, target,  $-\pi/2$ ].
CNOT[control1, control2].CRz[control2, target,  $\pi/2$ ].
CNOT[control1, control2].CRz[control2, target,  $-\pi/2$ ].H[target]//

```

```

FullSimplify;
CCRz[control1_, control2_, target_,  $\theta$ _]:=
CRz[control1, target,  $\theta/2$ ].CNOT[control1, control2].
CRz[control2, target,  $-\theta/2$ ].CNOT[control1, control2].
CRz[control2, target,  $\theta/2$ ]/FullSimplify;
CCRy[control1_, control2_, target_,  $\theta$ _]:=
CRy[control1, target,  $\theta/2$ ].CNOT[control1, control2].
CRy[control2, target,  $-\theta/2$ ].CNOT[control1, control2].
CRy[control2, target,  $\theta/2$ ]/FullSimplify;
CCNOT[control1_, control2_, target_]:=
Toffoli[control1, control2, target]/FullSimplify;
CCP00[control1_, control2_, target_,  $\theta$ _]:=
CP00[control1, target,  $\theta/2$ ].X[control1].CNOT[control1, control2].
X[control1].CP00[control2, target,  $-\theta/2$ ].X[control1].
CNOT[control1, control2].X[control1].CP00[control2, target,  $\theta/2$ ]/FullSimplify;
CCP01[control1_, control2_, target_,  $\theta$ _]:=
CP01[control1, target,  $\theta/2$ ].X[control1].CNOT[control1, control2].
X[control1].CP01[control2, target,  $-\theta/2$ ].X[control1].
CNOT[control1, control2].X[control1].CP01[control2, target,  $\theta/2$ ]/FullSimplify;
CCP10[control1_, control2_, target_,  $\theta$ _]:=
CP10[control1, target,  $\theta/2$ ].CNOT[control1, control2].
CP10[control2, target,  $-\theta/2$ ].CNOT[control1, control2].
CP10[control2, target,  $\theta/2$ ]/FullSimplify;
CCP11[control1_, control2_, target_,  $\theta$ _]:=
CP11[control1, target,  $\theta/2$ ].CNOT[control1, control2].
CP11[control2, target,  $-\theta/2$ ].CNOT[control1, control2].
CP11[control2, target,  $\theta/2$ ]/FullSimplify;

```

```

mZ[target_] := X[target].Y[target]//FullSimplify;
CCCNOT[control1__, control2__, control3__, target_] :=
CP11[control1, control3,  $-\pi/4$ ].CNOT[control1, control2].
CP11[control2, control3,  $\pi/4$ ].CNOT[control1, control2].
CP11[control2, control3,  $-\pi/4$ ].H[target].
CCRz[control1, control3, target,  $-\pi/2$ ].CNOT[control1, control2].
CCRz[control2, control3, target,  $\pi/2$ ].CNOT[control1, control2].
CCRz[control2, control3, target,  $-\pi/2$ ].H[target]//FullSimplify;
CCCRy[control1__, control2__, control3__, target__,  $\theta$ ] :=
CCRy[control1, control2, target,  $\theta/2$ ].
CCNOT[control1, control2, control3].CRy[control3, target,  $-\theta/2$ ].
CCNOT[control1, control2, control3].CRy[control3, target,  $\theta/2$ ]//
FullSimplify;
CCCRz[control1__, control2__, control3__, target__,  $\theta$ ] :=
CCRz[control1, control2, target,  $\theta/2$ ].
CCNOT[control1, control2, control3].CRz[control3, target,  $-\theta/2$ ].
CCNOT[control1, control2, control3].CRz[control3, target,  $\theta/2$ ]//
FullSimplify;
CCCP00[control1__, control2__, control3__, target__,  $\theta$ ] :=
CCP00[control1, control2, target,  $\theta/2$ ].X[control1].X[control2].
CCNOT[control1, control2, control3].X[control1].X[control2].
CP00[control3, target,  $-\theta/2$ ].X[control1].X[control2].
CCNOT[control1, control2, control3].X[control1].X[control2].
CP00[control3, target,  $\theta/2$ ]//FullSimplify;
CCCP01[control1__, control2__, control3__, target__,  $\theta$ ] :=
CCP01[control1, control2, target,  $\theta/2$ ].X[control1].X[control2].
CCNOT[control1, control2, control3].X[control1].X[control2].
CP01[control3, target,  $-\theta/2$ ].X[control1].X[control2].
CCNOT[control1, control2, control3].X[control1].X[control2].

```

```

CP01[control3, target,  $\theta/2$ ]/FullSimplify;
CCCP10[control1_, control2_, control3_, target_,  $\theta$ ] :=
CCP10[control1, control2, target,  $\theta/2$ ].
CCNOT[control1, control2, control3].CP10[control3, target,  $-\theta/2$ ].
CCNOT[control1, control2, control3].CP10[control3, target,  $\theta/2$ ]/
FullSimplify;
CCCP11[control1_, control2_, control3_, target_,  $\theta$ ] :=
CCP11[control1, control2, target,  $\theta/2$ ].
CCNOT[control1, control2, control3].CP11[control3, target,  $-\theta/2$ ].
CCNOT[control1, control2, control3].CP11[control3, target,  $\theta/2$ ]/
FullSimplify;

```

B.2. Python

Primero, se importan todos los módulos necesarios. Entre ellos, Numpy para variables y funciones numéricas, tgates para las compuertas de transmones.

```

import matplotlib.pyplot as plt
import matplotlib as mpl
import numpy as np
from scipy.stats import norm
from qutip import *

```

Ahora definimos la función del pulso gaussiano que se utilizará para las rotaciones X-Y. Esta función recibe como entradas el eje de tiempo, el tiempo de inicio del pulso y el tiempo de fin del pulso, y retorna el valor del pulso gaussiano normalizado en cada instante del eje de tiempo. También se ha definido la función de un pulso rectangular con las mismas características. Esta función no se usa en la versión actual del simulador, pero se ha dejado en el código para que pueda ser utilizada en el futuro sin necesidad de reimplementarla.

```

def gaussianpulse(x,ts,tf):

```



```

s = (tf-ts)/6
m = (ts+tf)/2
return (np.heaviside(x-m+3*s,1)-np.heaviside(x-m-3*s,1)) \
        *norm.pdf(x, loc = m, scale = s)/0.997300204

def squarepulse(x,ts,tf):
    s = (tf-ts)/6
    m = (ts+tf)/2
    return (np.heaviside(x-m+3*s,1)-np.heaviside(x-m-3*s,1))/(6*s)

```

La siguiente función es una función que se utiliza para graficar la probabilidad de ocupación de las salidas del solucionador de ecuaciones maestras y los pulsos utilizados en las compuertas.

```

def plot_drive_expect(res,args):
    tlist = res.times

    if args == 0:
        fig, axes = plt.subplots(1, 1, sharex=True, figsize=(12,4))

        axes.plot(tlist, np.real(expect(qop('n',0), res.states)), \
                    'b', linewidth=2, label="qubit 0")
        axes.plot(tlist, np.real(expect(qop('n',1), res.states)), \
                    'g', linewidth=2, label="qubit 1")
        axes.plot(tlist, np.real(expect(qop('n',2), res.states)), \
                    'c', linewidth=2, label="qubit 2")
        axes.plot(tlist, np.real(expect(qop('n',3), res.states)), \
                    'm', linewidth=2, label="qubit 3")
        axes.set_ylim(0, 1)

        axes.set_xlabel("Time (ns)", fontsize=16)
        axes.set_ylabel("Occupation probability", fontsize=16)
        axes.legend()

    else:
        fig, axes = plt.subplots(2, 1, sharex=True, figsize=(12,8))

        axes[0].plot(tlist, np.array(list(ksi_t(tlist,args))) / (2*np.pi), \

```

```

        'b', linewidth=2, label="drive envelope")
axes[0].set_ylabel("Energy (GHz)", fontsize=16)
axes[0].legend()

axes[1].plot(tlist, np.real(expect(qop('n',0), res.states)), 'b', \
            linewidth=2, label="qubit 0")
axes[1].plot(tlist, np.real(expect(qop('n',1), res.states)), 'g', \
            linewidth=2, label="qubit 1")
axes[1].plot(tlist, np.real(expect(qop('n',2), res.states)), 'c', \
            linewidth=2, label="qubit 2")
axes[1].plot(tlist, np.real(expect(qop('n',3), res.states)), 'm', \
            linewidth=2, label="qubit 3")
axes[1].set_ylim(0, 1)

axes[1].set_xlabel("Time (ns)", fontsize=16)
axes[1].set_ylabel("Occupation probability", fontsize=16)
axes[1].legend()

fig.tight_layout()

```

Ahora se definen los parámetros del sistema, como las tasas de relajación y las frecuencias de resonancia.

1. N es el tamaño del resonador. Es decir, la cantidad de fonones a la que se trunca su Hamiltoniano.
2. w_r es la frecuencia de resonancia del resonador.
3. w_q es un arreglo con las frecuencias de resonancia de los qubits.
4. w_{q_swap} es la frecuencia a la que se desplazan los qubits para realizar i SWAP y $\sqrt{i$ SWAP.
5. g es un arreglo con las constantes de acoplamiento entre los qubits y el resonador.
6. D es un arreglo con las diferencias de las frecuencias de resonancia entre los qubits y el resonador.
7. D_{swap} es la diferencia entre la frecuencia de resonancia para i SWAP y el resonador.

8. κ es la tasa de relajación del resonador.
9. γ es un arreglo con las tasas de relajación de los qubits.
10. a es el operador de destrucción del resonador.
11. n es el operador de número del resonador.

$N = 50$

```

wr = 10.0 * 2 * np.pi
wq = np.array([5.0 * 2 * np.pi, 6.0 * 2 * np.pi, 7.0 * 2 * np.pi, \
               8.0 * 2 * np.pi])
wq_swap = 9 * 2 * np.pi

g = np.array([0.1 * 2*np.pi, 0.1 * 2*np.pi, 0.1 * 2*np.pi, 0.1 * 2*np.pi])

D = wq - wr
D_swap = wq_swap - wr

chi = g**2 / abs(wr-wq)

kappa = 0.001
gamma = np.array([5e-6, 5e-6, 5e-6, 5e-6])

a = destroy(N)
# a = tensor(destroy(N), qeye(2), qeye(2), qeye(2), qeye(2))
n = a.dag() * a
Id_r = qeye(N)

```

La función `qop_part` devuelve la matriz asociada al operador solicitado, y se utiliza como parte de la función `qop` para realizar el producto tensorial de este operador, con los operadores de identidad necesarios para retornar el operador que actúe en el qubit solicitado.

La lista `c_ops` es la lista de los operadores de colapso de los qubits. En el caso sin pérdidas, esta lista es vacía. En el caso con pérdidas contiene los operadores σ_- de cada qubit.

```

def qop_part(operator, target):
    if target == 0:
        qop_dict = {'sm' : destroy(2), 'sp' : (destroy(2)).dag(),
                    'sx' : sigmax(), 'sy' : sigmay(), 'sz' : sigmaz(),
                    'n' : (destroy(2)).dag() * destroy(2)}
        return qop_dict[operator]
    else:
        return qeye(2)

def qop(operator, target):
    return tensor(qop_part(operator, target-0), qop_part(operator, \
        target-1), qop_part(operator, target-2), \
        qop_part(operator, target-3))

#c_ops = [np.sqrt(gamma[0]) * qop('sm', 0), np.sqrt(gamma[1]) * \
    qop('sm', 1), np.sqrt(gamma[2]) * qop('sm', 2), \
    np.sqrt(gamma[3]) * qop('sm', 3)]
c_ops = []

```

Las siguientes funciones son funciones para utilizar como coeficientes dependientes del tiempo en los Hamiltonianos:

```

def ksi_t(t, args):
    return args['A'] * gaussianpulse(t,args['ts'],args['tf'])

def ksi_tm(t, args):
    return args['A'] * gaussianpulse(t,args['ts'],args['tf']) * \
        np.exp(-1j*args['w']*(t-args['ts']))

def ksi_tp(t, args):
    return args['A'] * gaussianpulse(t,args['ts'],args['tf']) * \
        np.exp(1j*args['w']*(t-args['ts']))

def ksiS_t(t, args):
    return args['A'] * squarepulse(t,args['ts'],args['tf'])

def ksiS_tm(t, args):
    return args['A'] * np.exp(-1j*args['w']*(t-args['ts']))

```

```
def ksiS_tp(t, args):
    return args['A'] * np.exp(1j*args['w']*(t-args['ts']))
```

Finalmente, se definen las compuertas cuánticas. En los casos de las compuertas Rx y Ry, primero se define el vector de tiempo. Luego se asigna la frecuencia del pulso para que actúe sobre el qubit deseado. Se define la parte independiente del tiempo del Hamiltoniano y la parte dependiente del tiempo con ksi_t como coeficiente. Se asignan los argumentos del pulso y se ejecuta el solucionador de ecuaciones maestras. Se retorna el resultado del solucionador.

```
def Rx(psi0, target, theta):
    tlist = np.linspace(0, 10, 200)

    wd = wq[target]

    Dr = wr-wd
    Dq = wq-wd

    Hsyst = 0
    for i in range(4):
        Hsyst = Hsyst - Dq[i]*qop('sz',i)/2

    H_t = [[qop('sx',target)/2, ksi_t], Hsyst]

    args = {'A' : theta, 'ts' : 0, 'tf' : 10, 'w' : wq[target]}
    res = mesolve(H_t, psi0, tlist, c_ops, [], args = args)

    # plot_drive_expect(res,args)

    return res

def Ry(psi0, target, theta):
    tlist = np.linspace(0, 10, 200)

    wd = wq[target]

    Dr = wr-wd
```

```

Dq = wq-wd

Hsyst = 0
for i in range(4):
    Hsyst = Hsyst - Dq[i]*qop('sz',i)/2

H_t = [[qop('sy',target)/2, ksi_t], Hsyst]

args = {'A' : theta, 'ts' : 0, 'tf' : 10, 'w' : wq[target]}
res = mesolve(H_t, psi0, tlist, c_ops, [], args = args)

# plot_drive_expect(res,args)

return res

def Rz(psi0, target, theta):
    res = Ry(psi0, target, np.pi/2)
    res = Rx(res.states[-1], target, theta)
    return Ry(res.states[-1], target, -np.pi/2)

def X(psi0, target):
    return Rx(psi0, target, np.pi)

def Y(psi0, target):
    return Ry(psi0, target, np.pi)

def Z(psi0, target, theta):
    return Rz(psi0, target, np.pi)

def H(psi0, target):
    res = Ry(psi0, target, np.pi/2)
    return X(res.states[-1], target)

def sqrtiSWAP(psi0, target1, target2):
    wqt1 = wq[target1]
    wq[target1] = wq_swap

    wqt2 = wq[target2]

```

```

wq[target2] = wq_swap

D = wq - wr

J = np.abs(g[target1] * g[target2] * (D[target1] + D[target2]) / \
          (D[target1] * D[target2]))/2

tf = np.pi/(4*J)
tlist = np.linspace(0, tf, 250)

Hsyst = g[target1]*g[target2] * (qop('sp',target1)*qop('sm',target2) \
    + qop('sm',target1)*qop('sp',target2)) / (D_swap)

res = mesolve(Hsyst, psi0, tlist, c_ops, [])

wq[target1] = wqt1
wq[target2] = wqt2
D = wq - wr

args = {'A' : 0, 'ts' : 0, 'tf' : tf, 'w' : wq[target1]}
# plot_drive_expect(res,args)

return res

def iSWAP(psi0, target1, target2):
    wqt1 = wq[target1]
    wq[target1] = wq_swap

    wqt2 = wq[target2]
    wq[target2] = wq_swap

    D = wq - wr

    J = np.abs(g[target1] * g[target2] * (D[target1] + D[target2]) / \
          (D[target1] * D[target2]))/2

    tf = np.pi/(2*J)
    tlist = np.linspace(0, tf, 500)

```

```

Hsyst = g[target1]*g[target2] * (qop('sp',target1)*qop('sm',target2) \
    + qop('sm',target1)*qop('sp',target2)) / (D_swap)

res = mesolve(Hsyst, psi0, tlist, c_ops, [])

wq[target1] = wqt1
wq[target2] = wqt2
D = wq - wr

args = {'A' : 0, 'ts' : 0, 'tf' : tf, 'w' : wq[target1]}
# plot_drive_expect(res,args)

return res

def CNOT(psi0, control, target):
    res = H(psi0, target)
    res = Rz(res.states[-1], target, -np.pi/2)
    res = Rz(res.states[-1], control, -np.pi/2)
    res = iSWAP(res.states[-1], control, target)
    res = H(res.states[-1], control)
    res = iSWAP(res.states[-1], control, target)
    res = Rx(res.states[-1], target, np.pi/2)
    res = iSWAP(res.states[-1], control, target)
    res = Rx(res.states[-1], control, np.pi/2)
    res = iSWAP(res.states[-1], control, target)
    return Rx(res.states[-1], target, np.pi/2)

def CRy(psi0, control, target, theta):
    res = Ry(psi0,target,theta/2)
    res = CNOT(res.states[-1],control,target)
    res = Ry(res.states[-1],target,-theta/2)
    return CNOT(res.states[-1],control,target)

def CRz(psi0, control, target, theta):
    res = Rz(psi0,target,theta/2)
    res = CNOT(res.states[-1],control,target)
    res = Rz(res.states[-1],target,-theta/2)

```



```

    return CNOT(res.states[-1], control, target)

def SWAP(psi0, target1, target2):
    res = CNOT(psi0, target1, target2)
    res = CNOT(res.states[-1], target2, target1)
    return CNOT(res.states[-1], target1, target2)

def CH(psi0, control, target):
    res = Ry(psi0, target, np.pi/4)
    res = CNOT(res.states[-1], control, target)
    return Ry(psi0, target, -np.pi/4)

def CP(psi0, control, target, theta, b = 0b11):
    if b == 0b00:
        res = Rz(psi0, control, -3*theta/4)
        res = Rz(res.states[-1], target, -3*theta/4)
        res = CRz(res.states[-1], control, target, theta/2)
        res = CRz(res.states[-1], target, control, theta/2)

    elif b == 0b01:
        res = Rz(psi0, control, -3*theta/4)
        res = Rz(res.states[-1], target, 5*theta/4)
        res = CRz(res.states[-1], control, target, -3*theta/2)
        res = CRz(res.states[-1], target, control, theta/2)

    elif b == 0b10:
        res = Rz(psi0, control, theta/4)
        res = Rz(res.states[-1], target, theta/4)
        res = CRz(res.states[-1], control, target, -3*theta/2)
        res = CRz(res.states[-1], target, control, theta/2)

    elif b == 0b11:
        res = Rz(psi0, control, theta/4)
        res = Rz(res.states[-1], target, theta/4)
        res = CRz(res.states[-1], control, target, theta/2)
        res = CRz(res.states[-1], target, control, theta/2)

    return res

```

```

def Toffoli(psi0, control1, control2, target):
    res = H(psi0, target)
    res = CRz(res.states[-1], control2, target, -np.pi/2)
    res = CNOT(res.states[-1], control1, control2)
    res = CRz(res.states[-1], control2, target, np.pi/2)
    res = CNOT(res.states[-1], control1, control2)
    res = CRz(res.states[-1], control1, target, -np.pi/2)
    res = H(res.states[-1], target)
    return CP(res.states[-1], control1, control2, -np.pi/2, b = 0b11)

def CCRz(psi0, control1, control2, target, theta):
    res = CRz(psi0, control2, target, theta/2)
    res = CNOT(res.states[-1], control1, control2)
    res = CRz(res.states[-1], control2, target, -theta/2)
    res = CNOT(res.states[-1], control1, control2)
    return CRz(res.states[-1], control1, target, theta/2)

def CCRy(psi0, control1, control2, target, theta):
    res = CRy(psi0, control2, target, theta/2)
    res = CNOT(res.states[-1], control1, control2)
    res = CRy(res.states[-1], control2, target, -theta/2)
    res = CNOT(res.states[-1], control1, control2)
    return CRy(res.states[-1], control1, target, theta/2)

def CCP(psi0, control1, control2, target, theta, b = 0b11):
    res = CP(psi0, control2, target, theta/2, b = b)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
    res = CNOT(res.states[-1], control1, control2)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
    res = CP(res.states[-1], control2, target, -theta/2, b = b)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
    res = CNOT(res.states[-1], control1, control2)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)

```

```

    return CP(res.states[-1], control1, target, theta/2, b = b)

def CCNOT(psi0, control1, control2, target):
    return Toffoli(psi0, control1, control2, target)

def Z(psi0, target):
    res = Ry(psi0, target, np.pi)
    return Rx(res.states[-1], target, -np.pi)

def mZ(psi0, target):
    res = Ry(psi0, target, np.pi)
    return Rx(res.states[-1], target, np.pi)

def CCCNOT(psi0, control1, control2, control3, target):
    res = H(psi0, target)
    res = CCRz(res.states[-1], control2, control3, target, -np.pi/2)
    res = CNOT(res.states[-1], control1, control2)
    res = CCRz(res.states[-1], control2, control3, target, np.pi/2)
    res = CNOT(res.states[-1], control1, control2)
    res = CCRz(res.states[-1], control1, control3, target, -np.pi/2)
    res = H(res.states[-1], target)
    res = CP(res.states[-1], control2, control3, -np.pi/4)
    res = CNOT(res.states[-1], control1, control2)
    res = CP(res.states[-1], control2, control3, np.pi/4)
    res = CNOT(res.states[-1], control1, control2)
    return CP(res.states[-1], control1, control3, -np.pi/4)

def CCCRy(psi0, control1, control2, control3, target, theta):
    res = CRy(psi0, control3, target, theta/2)
    res = CCNOT(res.states[-1], control1, control2, control3)
    res = CRy(res.states[-1], control3, target, -theta/2)
    res = CCNOT(res.states[-1], control1, control2, control3)
    return CCRy(res.states[-1], control1, control2, target, theta/2)

def CCCRz(psi0, control1, control2, control3, target, theta):
    res = CRz(psi0, control3, target, theta/2)
    res = CCNOT(res.states[-1], control1, control2, control3)
    res = CRz(res.states[-1], control3, target, -theta/2)

```

```

    res = CCNOT(res.states[-1], control1, control2, control3)
    return CCRz(res.states[-1], control1, control2, target, theta/2)

def CCCP(psi0, control1, control2, control3, target, theta, b = 0b11):
    res = CP(psi0, control3, target, theta/2, b = b)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
        res = X(res.states[-1], control2)
    res = CCNOT(res.states[-1], control1, control2, control3)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
        res = X(res.states[-1], control2)
    res = CP(res.states[-1], control3, target, -theta/2, b = b)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
        res = X(res.states[-1], control2)
    res = CCNOT(res.states[-1], control1, control2, control3)
    if b == 0b00 or b == 0b01:
        res = X(res.states[-1], control1)
        res = X(res.states[-1], control2)
    return CCP(res.states[-1], control1, control2, target, theta/2, b = b)

```

Apéndice C

Códigos de la simulación del algoritmo de Grover

C.1. Wolfram Mathematica

El siguiente fragmento de código genera una lista de números entre 1 y 16, en orden aleatorio, donde ningún número se repite.

```
data = {};  
While[Dimensions[data][[1]] < 24,  
    AppendTo[data, RandomInteger[{1, 24}]];  
    data = DeleteDuplicates[data];]
```

Ahora declaramos el número que se buscará en la lista.

```
buscar = 16;
```

Se procede a definir las matrices necesarias para ejecutar el algoritmo. Es decir: Los kets de la base computacional, la compuerta y la transformada de Hadamard y los operadores de reflexión.

```
ket0 = {{1}, {0}};  
ket1 = {{0}, {1}};  
Id = IdentityMatrix[2];
```

```

 $H$  = HadamardMatrix[2];
 $\omega$  = Position[data, buscar][[1, 1]];
 $\text{ket}\omega$  = Table[{0}, {24}] ;
 $\text{ket}\omega$ [[ $\omega$ , 1]] = 1;
kets = KroneckerProduct[ $H$ ,  $H$ ,  $H$ ,  $H$ ].KroneckerProduct[ket0, ket0, ket0, ket0];
 $U\omega$  = KroneckerProduct[Id, Id, Id, Id] - 2 $\text{ket}\omega$ .ConjugateTranspose[ket $\omega$ ];
 $Us$  = 2kets.ConjugateTranspose[kets] - KroneckerProduct[Id, Id, Id, Id];
 $G$  =  $Us$ . $U\omega$ ;

```

Finalmente, se prepara el estado inicial y se realizan las reflexiones para ejecutar el algoritmo. Se realizan $\pi N/2$ iteraciones, el doble de las necesarias, para poder estudiar lo que ocurre si sigue rotando el estado, pasado el máxima probabilidad de medir el estado deseado.

```

 $\text{ket}\psi$  = KroneckerProduct[ket0, ket0, ket0, ket0];
 $\text{ket}\psi$  = KroneckerProduct[ $H$ ,  $H$ ,  $H$ ,  $H$ ]. $\text{ket}\psi$ ;
 $\text{ket}\psi_0$  =  $\text{ket}\psi$ ;
For [ $i = 1, i < 2\frac{\pi}{4}\sqrt{\text{Dimensions}[\text{ket}\psi][[1]]} + 1, i++$ ,  $\text{ket}\psi_i = G.\text{ket}\psi_{i-1}$ ;]

 $n$  = Floor [ $\frac{\pi}{4}\sqrt{\text{Dimensions}[\text{ket}\psi][[1]]}$ ];
toplot $j$  := Table[Abs[ket $\psi_i$ [[ $j$ , 1]]2, { $i$ , 0, 2 $n$  + 1}];
ListLinePlot[Table[toplot $i$ , { $i$ , 1, 16}], PlotRange → All]

```

C.2. Python

Primero, se importan todos los módulos necesarios. Entre ellos, Numpy para variables y funciones numéricas, tgate para las compuertas de transmones.

```

import matplotlib.pyplot as plt
import matplotlib as mpl
import numpy as np

```

```

from scipy.stats import norm
from qutip import *
import tgates
import time

```

Ahora se definen las operaciones que son explícitas para este algoritmo. Ellas son la transformada de Hadamard y los operadores de reflexión.

```

def Htrans(psi0):
    res = tgates.H(psi0, 0)
    res = tgates.H(res.states[-1], 1)
    res = tgates.H(res.states[-1], 2)
    return tgates.H(res.states[-1], 3)

def Us(psi0):
    res = Htrans(psi0)
    res = tgates.CCCP(res.states[-1], 1, 2, 3, 0, np.pi, b = 0b00)
    return Htrans(res.states[-1])

def Uomega(psi0):
    return tgates.CCCP(psi0, 0, 1, 2, 3, np.pi, b = 0b11)

qN = 2**4

```

Finalmente, se define el estado inicial y se ejecuta el algoritmo. Se realizan el doble de interacciones de las necesarias, igual que en el código de Wolfram Mathematica, para analizar lo que ocurre si se realizan más rotaciones de las necesarias.

```

psi0 = tensor(basis(2,0), basis(2,0), basis(2,0), basis(2,0))

res = Htrans(psi0)

Nit = 2*int(np.pi*np.sqrt(qN)/4)+1

for i in range(Nit):

    res = Uomega(res.states[-1])

```

```
res = Us(res.states[-1])  
  
qsave(res, 'it_{}'.format(i+1))
```


Apéndice D

Códigos de la simulación del algoritmo de Shor

D.1. Wolfram Mathematica

Primero definimos el número a factorizar y número que se utilizará para el operador de multiplicación modular. También verificamos que estos dos números sean coprimos.

```
M = 15; (*13;*)  
x = RandomInteger[{2, M - 2}]  
GCD[x, M] == 1
```

Ahora se definen las matrices necesarias para el algoritmo, como los kets de la base computacional, el operador de multiplicación, la compuerta de fase, entre otras.

```
ket0 = {{1}, {0}};  
ket1 = {{0}, {1}};  
Id = IdentityMatrix[2];  
X = PauliMatrix[1];  
Y = PauliMatrix[2];  
Z = PauliMatrix[3];  
H = HadamardMatrix[2];
```

```

P0 = ket0.ConjugateTranspose[ket0];
P1 = ket1.ConjugateTranspose[ket1];
R[φ-]:=P0 + eiφP1;
CNOT = KroneckerProduct[P0, Id] + KroneckerProduct[P1, X];
CR[φ-]:=KroneckerProduct[P0, Id] + KroneckerProduct[P1, R[φ]];
CR13[φ-]:=KroneckerProduct[P0, Id, Id] + KroneckerProduct[P1, Id, R[φ]];
ket[n-]:=Table[{n == i - 1}, {i, 1, 16}]/.{True → 1, False → 0};
Urp[x-, N-]:=Sum[ket[Mod[xi, N]].ConjugateTranspose[ket[i]], {i, 0, N - 1}]
    +Sum[ket[i].ConjugateTranspose[ket[i]], {i, N, 15}];
ρ[ψ-]:=ψ.ConjugateTranspose[ψ];
U = Urp[x, M];

```

Ahora se prepara el estado inicial y se ejecuta el algoritmo.

```

ψ0 = KroneckerProduct[ket0, ket0, ket0, ket0];
ψ0 = KroneckerProduct[H, H, H, H].ψ0;
ψ = KroneckerProduct[ket0, ket0, ket0, ket1];
ψt = KroneckerProduct[ψ0, ψ];
ψt = (KroneckerProduct[Id, Id, Id, P0, Id, Id, Id, Id]
    +KroneckerProduct[Id, Id, Id, P1, U]).ψt;
ψt = (KroneckerProduct[Id, Id, P0, Id, Id, Id, Id, Id]
    +KroneckerProduct[Id, Id, P1, Id, MatrixPower[U, 2]]).ψt;
ψt = (KroneckerProduct[Id, P0, Id, Id, Id, Id, Id, Id]
    +KroneckerProduct[Id, P1, Id, Id, MatrixPower[U, 22]]).ψt;
ψt = (KroneckerProduct[P0, Id, Id, Id, Id, Id, Id, Id]
    +KroneckerProduct[P1, Id, Id, Id, MatrixPower[U, 23]]).ψt;
ψt = KroneckerProduct[ConjugateTranspose[FourierMatrix[24]], Id, Id, Id, Id].ψt;
For[i = 0, i < 32, i++, sub0 = Mod[i, 2];
sub1 = Which[i == 0, 0, Mod[i, 2] == 0

```

```

&&sub1 == 0, 1, Mod[i, 2] == 0
&&sub1 == 1, 0, True, sub1];
sub2 = Which[i == 0, 0, Mod[i, 2] == 0
&&sub2 == 0, 1, Mod[i, 2] == 0
&&sub2 == 1, 0, True, sub2];
sub3 = Which[i == 0, 0, Mod[i, 2] == 0
&&sub3 == 0, 1, Mod[i, 2] == 0
&&sub3 == 1, 0, True, sub3];
ψti = KroneckerProduct [Psub3, Psub2, Psub1, Psub0, Id, Id, Id, Id] . ψt;
ψti = ConjugateTranspose [ψti] . ψti;

(*Organizar resultados de las medidas y graficar*)
L = Table [{i,  $\frac{i}{2^4}$ , ψti[[1, 1]]}, {i, 0, 31}];
ListPlot [Table [{ $\frac{i}{2^4}$ }, ψti[[1, 1]]}, {i, 0, 16}], PlotRange → All

(*Procesar medidas para tener la factorización*)
(*Fracciones continuas*)
L1 = Table[{Denominator[FromContinuedFraction[
ContinuedFraction[Transpose[L][[2, i]]]], L[[i, 3]]}, {i, 1, 16}];
For[i = 1, i ≤ Dimensions[L1][[1]], i++,
For[j = 1, j ≤ Dimensions[L1][[1]], j++,
If[L1[[i, 1]] == L1[[j, 1]] && i ≠ j, L1[[i, 2]] += L1[[j, 2]];
L1 = Drop[L1, {j}]; ]]]
For[i = 1, i ≤ Dimensions[L1][[1]], i++, If[OddQ[L1[[i, 1]]], L1 = Drop[L1, {i}]; ]
For [i = 1, i ≤ Dimensions[L1][[1]], i++, If [Mod [xL1[[i, 1]], M] ≠ 1, L1 = Drop[L1, {i}]; ]
For[i = 1, i ≤ Dimensions[L1][[1]], i++,
If[Mod[x $\frac{L1[[1, 1]]}{2}$ , M] == M - 1, L1 = Drop[L1, {i}]; ]
For [i = 1, i ≤ Dimensions[L1][[1]], i++, L1[[i, 2]] =  $\frac{L1[[i, 2]]}{\text{Sum}[L1[[j, 2]], \{j, 1, \text{Dimensions}[L1][[1]]\}]}$ ; ]

```

$$L2 = \text{Table} \left[\left\{ \text{GCD} \left[x^{\frac{L1[[i,1]]}{2}} + 1, M \right], L1[[i, 2]] \right\}, \{i, 1, \text{Dimensions}[L1][[1]]\} \right];$$

$$L3 = \text{Table} \left[\left\{ \text{GCD} \left[x^{\frac{L1[[i,1]]}{2}} - 1, M \right], L1[[i, 2]] \right\}, \{i, 1, \text{Dimensions}[L1][[1]]\} \right];$$

D.2. Python

Primero, se importan todos los módulos necesarios. Entre ellos, Numpy para variables y funciones numéricas, tgates8 para las compuertas de transmones.

```
import matplotlib.pyplot as plt
import matplotlib as mpl
import numpy as np
from scipy.stats import norm
from qutip import *
import tgates8
import time
```

Ahora se definen las operaciones que son explícitas para este algoritmo. Ellas son la transformada de Hadamard y los operadores de reflexión.

```
def QFT4d(psi0, target1, target2, target3, target4):
    res = tgates8.SWAP(psi0, target2, target3)
    res = tgates8.SWAP(res.states[-1], target1, target4)
    res = tgates8.H(res.states[-1], target4)
    res = tgates8.CP(res.states[-1], target4, target3, -2*np.pi/2**2)
    res = tgates8.H(res.states[-1], target3)
    res = tgates8.CP(res.states[-1], target4, target2, -2*np.pi/2**3)
    res = tgates8.CP(res.states[-1], target3, target2, -2*np.pi/2**2)
    res = tgates8.H(res.states[-1], target2)
    res = tgates8.CP(res.states[-1], target4, target1, -2*np.pi/2**4)
    res = tgates8.CP(res.states[-1], target3, target1, -2*np.pi/2**3)
    res = tgates8.CP(res.states[-1], target2, target1, -2*np.pi/2**2)
    return tgates8.H(res.states[-1], target1)
```

```
def CSWAP(psi0, control, target1, target2):
```

```

    res = tgates8.CCNOT(psi0, control, target1, target2)
    res = tgates8.CCNOT(psi0, control, target2, target1)
    return tgates8.CCNOT(psi0, control, target1, target2)

def CMUL7(psi0, control, target1, target2, target3, target4):
    res = tgates8.CNOT(psi0, control, target1)
    res = tgates8.CNOT(res.states[-1], control, target2)
    res = tgates8.CNOT(res.states[-1], control, target3)
    res = tgates8.CNOT(res.states[-1], control, target4)
    res = CSWAP(res.states[-1], control, target2, target3)
    res = CSWAP(res.states[-1], control, target1, target2)
    return CSWAP(res.states[-1], control, target1, target4)

qN = 2**8

Finalmente, se define el estado inicial y se ejecuta el algoritmo. Se realizan el doble
de interacciones de las necesarias, igual que en el código de Wolfram Mathematica,
para analizar lo que ocurre si se realizan más rotaciones de las necesarias.

psi0 = tensor(basis(2,0), basis(2,0), basis(2,0), basis(2,0),
              basis(2,0), basis(2,0), basis(2,0), basis(2,0))

res = tgates8.X(psi0, 7)

qsave(res, 'rp_0')

res = tgates8.H(res.states[-1], 0)
res = tgates8.H(res.states[-1], 1)
res = tgates8.H(res.states[-1], 2)
res = tgates8.H(res.states[-1], 3)

qsave(res, 'rp_1')

res = CMUL7(res.states[-1], 3, 4, 5, 6, 7)

qsave(res, 'rp_2')

res = CMUL7(res.states[-1], 2, 4, 5, 6, 7)

```

```
res = CMUL7(res.states[-1], 2, 4, 5, 6, 7)
```

```
qsave(res, 'rp_3')
```

```
res = CMUL7(res.states[-1], 1, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 1, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 1, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 1, 4, 5, 6, 7)
```

```
qsave(res, 'rp_4')
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
res = CMUL7(res.states[-1], 0, 4, 5, 6, 7)
```

```
qsave(res, 'rp_5')
```

```
res = QFT4d(res.states[-1], 0, 1, 2, 3)
```

```
qsave(res, 'rp_6')
```

Apéndice E

Códigos de la simulación del algoritmo de PageRank

E.1. Wolfram Mathematica

Los grafos que utilizaremos se definen de la siguiente manera:

1. Grafo estrella

$$g = \text{Graph}[\{1 \rightarrow 2, 1 \rightarrow 3, 1 \rightarrow 4, 2 \rightarrow 1, 3 \rightarrow 1, 4 \rightarrow 1\}];$$

2. Grafo corona

$$g = \text{Graph}[\{1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1, 1 \rightarrow 3, 3 \rightarrow 2, 2 \rightarrow 1, 1 \rightarrow 4, 2 \rightarrow 4, 3 \rightarrow 4\}];$$

3. Grafo árbol

$$g = \text{Graph}[\{1 \rightarrow 2, 1 \rightarrow 3, 2 \rightarrow 4\}];$$

4. Grafo aleatorio

$$g = \text{Graph}[\{1 \rightarrow 2, 1 \rightarrow 3, 1 \rightarrow 4, 2 \rightarrow 1, 2 \rightarrow 4, 3 \rightarrow 4, 4 \rightarrow 3\}];$$

Ahora, con el grafo definido, la matriz de estocástica del grafo se calcula de la siguiente manera a partir de la matriz de adyacencia:

```
Em = AdjacencyMatrix[g];
For[j = 1, j <= 4, j++,
  OutDeg = Sum[Em[[j, i]], {i, 1, 4}];
  If[OutDeg != 0, Em[[j]] = Em[[j]]/OutDeg, Em[[j]] = {1/4, 1/4, 1/4, 1/4};]
Em = Transpose[Em];
```

La matriz de Google con un α arbitrario es la siguiente:

$$G = \alpha \text{Em} + \frac{(1-\alpha)}{\text{Dimensions[Em][[1]]}} \text{Table}[1, \{\text{Dimensions[Em][[1]]}\}, \{\text{Dimensions[Em][[1]]}\}];$$

El PageRank clásico del grafo g se puede calcular de las siguientes dos maneras:

1. Cálculo manual multiplicando la matriz de Google N veces a un vector de PageRank inicial. Este método permite conocer el PageRank en cada paso de la iteración, así que se podría utilizar para graficar la evolución de los valores.

```
Ivl1 = {1}; (*PageRank inicial de cada nodo*)
Ivl2 = {0};
Ivl3 = {0};
Ivl4 = {0};
Iv = {{1}, {0}, {0}, {0}}; (*Vector de PageRank inicial*)
For[i = 1, i <= 30, i++,
  Iv = (G/.{α → 0,85}).Iv; (*Iterar con la matriz de Google*)
  (*Iv = Iv/Norm[Iv]; *)
  AppendTo[Ivl1, Iv[[1, 1]]];
  AppendTo[Ivl2, Iv[[2, 1]]];
  AppendTo[Ivl3, Iv[[3, 1]]];
  AppendTo[Ivl4, Iv[[4, 1]]];]
```


2. Cálculo con la función de PageRank incluida en Wolfram Mathematica. Esta función recibe como primer argumento el grafo y como segundo argumento el valor de α .

PageRankCentrality[$g, 0,85$]

Ahora que se han definido los parámetros del grafo, procedemos a definir la parte cuántica del algoritmo. Primero, creamos una función que retorne los kets de los estados número.

ket[$k_ , n_$]:=Table[{ $i == k$ }, { $i, 0, n - 1$ }] /. {True \rightarrow 1, False \rightarrow 0};

Utilizaremos la definición del operador de difusión dada por Paparo, así que basta con definir las proyecciones entre las particiones del grafo bipartito en un sólo sentido.

$\phi_{x_j} := \text{KroneckerProduct} \left[\text{ket}[j - 1, 4], \text{Sum} \left[\sqrt{G[[k, j]]} \text{ket}[k - 1, 4], \{k, 1, 4\} \right] \right];$

$\phi_{x0} = \text{Sum} [\phi_{x_j}, \{j, 1, 4\}] / 2;$

$\Pi x = \text{Sum} [\phi_{x_j} . \phi_{x_j}^\dagger, \{j, 1, 4\}]; (*\text{Proyector } A \rightarrow B^*)$

$S = \text{Sum}[\text{KroneckerProduct}[\text{ket}[j, 4],$

$\text{ket}[k, 4]].\text{KroneckerProduct}[\text{ket}[k, 4], \text{ket}[j, 4]]^\dagger, \{j, 0, 3\}, \{k, 0, 3\}];$

$Ux = S.(2\Pi x - \text{IdentityMatrix}[16]); (*\text{Operador de difusión } 1/2^*)$

$W = \text{MatrixPower}[Ux, 2]; (*\text{Operador de difusión } 1^*)$

Finalmente, el PageRank cuántico se calcula de la siguiente manera. Hemos tomado el valor estándar de $\alpha = 0,85$.

$a = 0,85;$

qIvl1 =

Table[{ $((\phi_{x0}^\dagger /. \{\alpha \rightarrow a\}).\text{MatrixPower}[(W^\dagger /. \{\alpha \rightarrow a\}), m].$

$\text{KroneckerProduct}[\text{IdentityMatrix}[4], \text{ket}[0, 4].\text{ket}[0, 4]^\dagger].$

$\text{MatrixPower}[(W /. \{\alpha \rightarrow a\}), m].(\phi_{x0} /. \{\alpha \rightarrow a\}))[[1, 1]], \{m, 1, 30\}];$

qIvl2 =

```

Table[ $((\phi x0 \dagger / \{ \alpha \rightarrow a \}) . \text{MatrixPower}[(W \dagger / \{ \alpha \rightarrow a \}), m] .$ 
      KroneckerProduct[IdentityMatrix[4], ket[1, 4].ket[1, 4]†].
      MatrixPower[(W/.{ $\alpha \rightarrow a$ }), m].( $\phi x0 / \{ \alpha \rightarrow a \}$ ))[[1, 1]], {m, 1, 30}];
qIvl3 =
Table[ $((\phi x0 \dagger / \{ \alpha \rightarrow a \}) . \text{MatrixPower}[(W \dagger / \{ \alpha \rightarrow a \}), m] .$ 
      KroneckerProduct[IdentityMatrix[4], ket[2, 4].ket[2, 4]†].
      MatrixPower[(W/.{ $\alpha \rightarrow a$ }), m].( $\phi x0 / \{ \alpha \rightarrow a \}$ ))[[1, 1]], {m, 1, 30}];
qIvl4 =
Table[ $((\phi x0 \dagger / \{ \alpha \rightarrow a \}) . \text{MatrixPower}[(W \dagger / \{ \alpha \rightarrow a \}), m] .$ 
      KroneckerProduct[IdentityMatrix[4], ket[3, 4].ket[3, 4]†].
      MatrixPower[(W/.{ $\alpha \rightarrow a$ }), m].( $\phi x0 / \{ \alpha \rightarrow a \}$ ))[[1, 1]], {m, 1, 30}];

```

E.2. Python

Primero, se importan todos los módulos necesarios. Entre ellos, Numpy para variables y funciones numéricas, tgates para las compuertas de transmones.

```

import matplotlib.pyplot as plt
import matplotlib as mpl
import numpy as np
from scipy.stats import norm
from qutip import *
import tgates
import time

```

Las siguientes dos funciones son los operadores de permutación hacia la derecha y hacia la izquierda, controlados. Los argumentos c1 y c2 corresponden a los valores de los qubits del primer y segundo qubit del primer registro, respectivamente, con los que se controla el operador. Si son 0, el operador se activa con el ket $|0\rangle$, si son 1, se activa con el ket $|1\rangle$ y si son -1 se tiene el caso no controlado.

```

def R2(psi0, c1, c2):

```

```
if c1 == -1 and c2 == -1:
    res = tgates.CNOT(psi0, 3, 2)
    res = tgates.X(res.states[-1], 3)

elif c1 == -1:
    psi1 = psi0

    if c2 == 0:
        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

    res = tgates.CCNOT(psi1, 1, 3, 2)
    res = tgates.CNOT(res.states[-1], 1, 3)
    psi1 = res.states[-1]

    if c2 == 0:
        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

elif c2 == -1:
    psi1 = psi0

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

    res = tgates.CCNOT(psi1, 0, 3, 2)
    res = tgates.CNOT(res.states[-1], 0, 3)
    psi1 = res.states[-1]

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

else:
    psi1 = psi0

    if c1 == 0:
```

```

        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

    if c2 == 0:
        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

    res = tgates.CCCNOT(psi1, 0, 1, 3, 2)
    res = tgates.CCNOT(res.states[-1], 0, 1, 3)
    psi1 = res.states[-1]

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

    if c2 == 0:
        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

    return res

def L2(psi0, c1, c2):
    if c1 == -1 and c2 == -1:
        res = tgates.X(psi0, 3)
        res = tgates.CNOT(res.states[-1], 3, 2)

    elif c1 == -1:
        psi1 = psi0

        if c2 == 0:
            res = tgates.X(psi1, 1)
            psi1 = res.states[-1]

        res = tgates.CNOT(psi1, 1, 3)
        res = tgates.CCNOT(res.states[-1], 1, 3, 2)
        psi1 = res.states[-1]

    if c2 == 0:

```

```
        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

elif c2 == -1:
    psi1 = psi0

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

    res = tgates.CNOT(psi1, 0, 3)
    res = tgates.CCNOT(res.states[-1], 0, 3, 2)
    psi1 = res.states[-1]

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

else:
    psi1 = psi0

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

    if c2 == 0:
        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

    res = tgates.CCNOT(psi1, 0, 1, 3)
    res = tgates.CCCNOT(res.states[-1], 0, 1, 3, 2)
    psi1 = res.states[-1]

    if c1 == 0:
        res = tgates.X(psi1, 0)
        psi1 = res.states[-1]

    if c2 == 0:
```

```

        res = tgates.X(psi1, 1)
        psi1 = res.states[-1]

    return res

```

Ahora definimos el operador de reflexión alrededor del estado de referencia de la base computacional. El estado elegido ha sido $|0\rangle$.

```

def Dd(psi0):
    return tgates.CP(psi0, 2, 3, np.pi, b=0b00)

```

El operador de SWAP entre los registros se define de la siguiente manera. Esto es, la compuerta SWAP aplicada entre el i -ésimo qubit de cada uno de los registros.

```

def reg_SWAP(psi0):
    res = tgates.SWAP(psi0, 1, 3)
    return tgates.SWAP(res.states[-1], 0, 2)

```

La parte siguiente es dependiente del grafo. Esto es, los operadores K_i y T_i y la sucesión de estos que generará el operador de difusión de la caminata cuántica de Szegedy en cada uno de los grafos.

E.2.1. Grafo estrella

Los operadores K_i y T_i del grafo estrella se definen de la siguiente manera:

```

def Kb1(psi0):
    thetay00 = 1.85806
    thetay10 = 2.48274
    thetay11 = 1.5708

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCry(res.states[-1], 0, 1, 3, 2, thetay00)

```

```

    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay11)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb1d(psi0):
    thetay00 = 1.85806
    thetay10 = 2.48274
    thetay11 = 1.5708

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, -thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb2(psi0):
    thetay00 = 0.554811
    thetay10 = 0.405465
    thetay11 = 1.5708

    res = tgates.X(psi0, 3)

```

```

    res = tgates.CRy(res.states[-1], 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CRy(res.states[-1], 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CRy(res.states[-1], 2, 3, thetay11)

    res = tgates.X(res.states[-1], 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, -thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb2d(psi0):
    thetay00 = 0.554811
    thetay10 = 0.405465
    thetay11 = 1.5708

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

```



```

res = tgates.X(res.states[-1], 2)
res = tgates.CCCry(res.states[-1], 0, 1, 2, 3, thetay10)
res = tgates.X(res.states[-1], 2)

res = tgates.CCCry(res.states[-1], 0, 1, 2, 3, thetay11)

res = tgates.X(res.states[-1], 1)
res = tgates.X(res.states[-1], 0)

res = tgates.Cry(res.states[-1], 2, 3, -thetay11)

res = tgates.X(res.states[-1], 2)
res = tgates.Cry(res.states[-1], 2, 3, -thetay10)
res = tgates.X(res.states[-1], 2)

res = tgates.X(res.states[-1], 3)
res = tgates.Cry(res.states[-1], 3, 2, -thetay00)
return tgates.X(res.states[-1], 3)

```

Ahora, creamos el estado inicial, a partir del estado fiducial.

```

psi0 = tensor(basis(2,0), basis(2,0), basis(2,0), basis(2,0))

res = tgates.H(psi0,0)
res = tgates.H(res.states[-1],1)
res = Kb1(res.states[-1])
res = Kb2(res.states[-1])

```

Finalmente, se realizan la caminata de Szegedy y se guarda el estado resultante en cada paso.

```

for i in range(60):

    res = Kb2d(res.states[-1])
    res = Kb1d(res.states[-1])
    res = Dd(res.states[-1])

```

```

res = Kb1(res.states[-1])
res = Kb2(res.states[-1])
res = reg_SWAP(res.states[-1])

qsave(res, 'itj_{}'.format(i+1))

```

E.2.2. Grafo corona

Los operadores K_i y T_i del grafo corona se definen de la siguiente manera:

```

def T1(psi0):
    res = L2(psi0, 0, 1)
    res = L2(res.states[-1], 1, 0)
    return L2(res.states[-1], 1, 0)

def T1d(psi0):
    res = R2(psi0, 1, 0)
    res = R2(res.states[-1], 1, 0)
    return R2(res.states[-1], 0, 1)

def Kb1(psi0):
    thetay00 = 1.85806
    thetay10 = 2.48274
    thetay11 = 1.5708

    res = tgates.X(psi0, 3)
    res = tgates.CRy(res.states[-1], 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)
    res = tgates.X(res.states[-1], 2)
    res = tgates.CRy(res.states[-1], 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)
    res = tgates.CRy(res.states[-1], 2, 3, thetay11)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)
    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

```

```

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, -thetay00)
    return tgates.X(res.states[-1], 3)

def Kb1d(psi0):
    thetay00 = 1.85806
    thetay10 = 2.48274
    thetay11 = 1.5708

    res = tgates.X(psi0, 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)
    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay11)

    res = tgates.CRy(res.states[-1], 2, 3, -thetay11)
    res = tgates.X(res.states[-1], 2)
    res = tgates.CRy(res.states[-1], 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)
    res = tgates.X(res.states[-1], 3)
    res = tgates.CRy(res.states[-1], 3, 2, -thetay00)
    return tgates.X(res.states[-1], 3)

def Kb2(psi0):
    res = tgates.CCRy(psi0, 0, 1, 2, np.pi/2)
    return tgates.CCRy(res.states[-1], 0, 1, 3, np.pi/2)

def Kb2d(psi0):
    res = tgates.CCRy(psi0, 0, 1, 3, -np.pi/2)
    return tgates.CCRy(res.states[-1], 0, 1, 2, -np.pi/2)

```

Ahora, creamos el estado inicial, a partir del estado fiducial.

```

psi0 = tensor(basis(2,0), basis(2,0), basis(2,0), basis(2,0))

res = tgates.H(psi0,0)

```

```

res = tgates.H(res.states[-1],1)
res = Kb1(res.states[-1])
res = Kb2(res.states[-1])
res = T1d(res.states[-1])

```

Finalmente, se realizan la caminata de Szegedy y se guarda el estado resultante en cada paso.

```

for i in range(60):

    res = T1(res.states[-1])
    res = Kb2d(res.states[-1])
    res = Kb1d(res.states[-1])
    res = Dd(res.states[-1])
    res = Kb1(res.states[-1])
    res = Kb2(res.states[-1])
    res = T1d(res.states[-1])
    res = reg_SWAP(res.states[-1])

    qsave(res, 'itj_{}'.format(i+1))

```

E.2.3. Grafo árbol

Los operadores K_i y T_i del grafo árbol se definen de la siguiente manera:

```

def Kb1(psi0):
    thetay00 = 1.5708
    thetay10 = 2.58678
    thetay11 = 0.554811

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

```

```

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay11)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb1d(psi0):
    thetay00 = 1.5708
    thetay10 = 2.58678
    thetay11 = 0.554811

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, -thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb2(psi0):
    thetay00 = 2.58678
    thetay10 = 1.5708
    thetay11 = 2.73613

    res = tgates.X(psi0, 0)

```

```

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay11)

    return tgates.X(res.states[-1], 0)

def Kb2d(psi0):
    thetay00 = 2.58678
    thetay10 = 1.5708
    thetay11 = 2.73613

    res = tgates.X(psi0, 0)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, -thetay00)
    res = tgates.X(res.states[-1], 3)

    return tgates.X(res.states[-1], 0)

def Kb3(psi0):
    res = tgates.CRy(psi0, 0, 2, np.pi/2)
    res = tgates.CRy(res.states[-1], 0, 3, np.pi/2)
    return res

def Kb3d(psi0):
    res = tgates.CRy(psi0, 0, 3, -np.pi/2)

```

```

    res = tgates.CRy(res.states[-1], 0, 2, -np.pi/2)
    return res

```

Ahora, creamos el estado inicial, a partir del estado fiducial.

```

psi0 = tensor(basis(2,0), basis(2,0), basis(2,0), basis(2,0))

res = tgates.H(psi0,0)
res = tgates.H(res.states[-1],1)
res = Kb1(res.states[-1])
res = Kb2(res.states[-1])
res = Kb3(res.states[-1])

```

Finalmente, se realizan la caminata de Szegedy y se guarda el estado resultante en cada paso.

```

for i in range(60):

    res = Kb3d(res.states[-1])
    res = Kb2d(res.states[-1])
    res = Kb1d(res.states[-1])
    res = Dd(res.states[-1])
    res = Kb1(res.states[-1])
    res = Kb2(res.states[-1])
    res = Kb3(res.states[-1])
    res = reg_SWAP(res.states[-1])

    qsave(res, 'itj_{}'.format(i+1))

```

E.2.4. Grafo aleatorio

Los operadores K_i y T_i del grafo aleatorio se definen de la siguiente manera:

```

def T3(psi0):
    return R2(psi0, 1, 1)

```

```

def T3d(psi0):
    return L2(psi0, 1, 1)

def Kb1(psi0):
    thetay00 = 1.85806
    thetay10 = 2.48274
    thetay11 = 1.5708

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay11)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb1d(psi0):
    thetay00 = 1.85806
    thetay10 = 2.48274
    thetay11 = 1.5708

    res = tgates.X(psi0, 0)
    res = tgates.X(res.states[-1], 1)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

```



```

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, -thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 1)
    return tgates.X(res.states[-1], 0)

def Kb2(psi0):
    thetay00 = 1.5708
    thetay10 = 0.554811
    thetay11 = 2.58678

    res = tgates.X(psi0, 0)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCRy(res.states[-1], 0, 1, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, thetay11)

    return tgates.X(res.states[-1], 0)

def Kb2d(psi0):
    thetay00 = 1.5708
    thetay10 = 0.554811
    thetay11 = 2.58678

    res = tgates.X(psi0, 0)

    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCCRy(res.states[-1], 0, 1, 2, 3, -thetay10)

```

```

    res = tgates.X(res.states[-1], 2)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCCry(res.states[-1], 0, 1, 3, 2, -thetay00)
    res = tgates.X(res.states[-1], 3)

    return tgates.X(res.states[-1], 0)

def Kb3(psi0):
    thetay00 = 2.58678
    thetay10 = 1.5708
    thetay11 = 2.73613

    res = tgates.X(psi0, 3)
    res = tgates.CCRy(res.states[-1], 0, 3, 2, thetay00)
    res = tgates.X(res.states[-1], 3)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCRy(res.states[-1], 0, 2, 3, thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.CCRy(res.states[-1], 0, 2, 3, thetay11)

    return res

def Kb3d(psi0):
    thetay00 = 2.58678
    thetay10 = 1.5708
    thetay11 = 2.73613

    res = tgates.CCRy(psi0, 0, 2, 3, -thetay11)

    res = tgates.X(res.states[-1], 2)
    res = tgates.CCRy(res.states[-1], 0, 2, 3, -thetay10)
    res = tgates.X(res.states[-1], 2)

    res = tgates.X(res.states[-1], 3)
    res = tgates.CCRy(res.states[-1], 0, 3, 2, -thetay00)

```

```
res = tgates.X(res.states[-1], 3)
```

```
return res
```

Ahora, creamos el estado inicial, a partir del estado fiducial.

```
psi0 = tensor(basis(2,0), basis(2,0), basis(2,0), basis(2,0))
```

```
res = tgates.H(psi0,0)
```

```
res = tgates.H(res.states[-1],1)
```

```
res = Kb1(res.states[-1])
```

```
res = Kb2(res.states[-1])
```

```
res = Kb3(res.states[-1])
```

```
res = T3d(res.states[-1])
```

Finalmente, se realizan la caminata de Szegedy y se guarda el estado resultante en cada paso.

```
for i in range(60):
```

```
    res = T3(res.states[-1])
```

```
    res = Kb3d(res.states[-1])
```

```
    res = Kb2d(res.states[-1])
```

```
    res = Kb1d(res.states[-1])
```

```
    res = Dd(res.states[-1])
```

```
    res = Kb1(res.states[-1])
```

```
    res = Kb2(res.states[-1])
```

```
    res = Kb3(res.states[-1])
```

```
    res = T3d(res.states[-1])
```

```
    res = reg_SWAP(res.states[-1])
```

```
    qsave(res, 'itj_{}'.format(i+1))
```

Referencias

- [1] T. Loke and J. Wang, “Efficient quantum circuits for szegedy quantum walks,” *Annals of Physics*, vol. 382, pp. 64 – 84, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0003491617301124>
- [2] M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa, “Introduction to quantum information science,” *Graduate Texts in Physics*, 2015. [Online]. Available: <http://dx.doi.org/10.1007/978-3-662-43502-1>
- [3] J. A. Jones and D. Jaksch, “Quantum information, computation and communication,” 2009. [Online]. Available: <http://dx.doi.org/10.1017/CBO9781139028509>
- [4] M. A. Nielsen and I. L. Chuang, “Quantum computation and quantum information,” 2009. [Online]. Available: <http://dx.doi.org/10.1017/CBO9780511976667>
- [5] M. Nakahara, *Quantum computing : from linear algebra to physical realizations*. Boca Raton: CRC Press, 2008.
- [6] G. Wendin, “Quantum information processing with superconducting circuits: a review,” *Reports on Progress in Physics*, vol. 80, no. 10, p. 106001, 2017. [Online]. Available: <http://stacks.iop.org/0034-4885/80/i=10/a=106001>
- [7] M. H. Devoret and R. J. Schoelkopf, “Superconducting circuits for quantum information: An outlook,” *Science*, vol. 339, no. 6124, p. 11691174, Mar 2013. [Online]. Available: <http://dx.doi.org/10.1126/science.1231930>
- [8] Y. Hu, Y. X. Zhao, Z.-Y. Xue, and Z. D. Wang, “Realizing universal quantum gates with topological bases in quantum-simulated superconducting chains,” *npj Quantum Information*, vol. 3, no. 1, Mar 2017. [Online]. Available: <http://dx.doi.org/10.1038/s41534-017-0009-3>

- [9] D. Rotta, F. Sebastiano, E. Charbon, and E. Prati, “Quantum information density scaling and qubit operation time constraints of cmos silicon-based quantum computer architectures,” *npj Quantum Information*, vol. 3, no. 1, Jun 2017. [Online]. Available: <http://dx.doi.org/10.1038/s41534-017-0023-5>
- [10] G. Tosi, F. A. Mohiyaddin, V. Schmitt, S. Tenberg, R. Rahman, G. Klimeck, and A. Morello, “Silicon quantum processor with robust long-distance qubit couplings,” *Nature Communications*, vol. 8, no. 1, Sep 2017. [Online]. Available: <http://dx.doi.org/10.1038/s41467-017-00378-x>
- [11] N. C. Harris, D. Bunandar, M. Pant, G. R. Steinbrecher, J. Mower, M. Prabhu, T. Baehr-Jones, M. Hochberg, and D. Englund, “Large-scale quantum photonic circuits in silicon,” *Nanophotonics*, vol. 5, no. 3, Jan 2016. [Online]. Available: <http://dx.doi.org/10.1515/nanoph-2015-0146>
- [12] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, “Charge-insensitive qubit design derived from the cooper pair box,” *Physical Review A*, vol. 76, no. 4, Oct 2007. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.76.042319>
- [13] L. K. Grover, “A fast quantum mechanical algorithm for database search,” *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC 96*, 1996. [Online]. Available: <http://dx.doi.org/10.1145/237814.237866>
- [14] A. Dewes, R. Lauro, F. R. Ong, V. Schmitt, P. Milman, P. Bertet, D. Vion, and D. Esteve, “Quantum speeding-up of computation demonstrated in a superconducting two-qubit processor,” *Physical Review B*, vol. 85, no. 14, Apr 2012. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevB.85.140503>
- [15] T. Said, A. Chouikh, K. Essammouni, and M. Bennai, “Implementation of grover quantum search algorithm with two transmon qubits via circuit qed,” *Quantum Physics Letters*, vol. 6, no. 1, p. 2935, Apr 2017. [Online]. Available: <http://dx.doi.org/10.18576/qpl/060105>
- [16] L. DiCarlo, J. M. Chow, J. M. Gambetta, L. S. Bishop, B. R. Johnson, D. I. Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and et al., “Demonstration of two-qubit algorithms with a superconducting quantum processor,” *Nature*, vol. 460, no. 7252, p. 240244, Jun 2009. [Online]. Available: <http://dx.doi.org/10.1038/nature08121>

- [17] D. Deutsch and R. Jozsa, “Rapid solution of problems by quantum computation,” *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 439, no. 1907, p. 553558, Dec 1992. [Online]. Available: <http://dx.doi.org/10.1098/rspa.1992.0167>
- [18] J. Zhao, X. Tan, D. Lan, H. Wu, G. Xue, H. Yu, and Y. Yu, “Implementation of refined deutsch-jozsa algorithm in a superconducting qutrit system,” *physica status solidi (b)*, vol. 254, no. 5, p. 1600640, Nov 2016. [Online]. Available: <http://dx.doi.org/10.1002/pssb.201600640>
- [19] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Review*, vol. 41, no. 2, p. 303332, Jan 1999. [Online]. Available: <http://dx.doi.org/10.1137/S0036144598347011>
- [20] J. M. Gambetta, J. M. Chow, and M. Steffen, “Building logical qubits in a superconducting quantum computing system,” *npj Quantum Information*, vol. 3, no. 1, Jan 2017. [Online]. Available: <http://dx.doi.org/10.1038/s41534-016-0004-0>
- [21] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, “Realization of a scalable shor algorithm,” *Science*, vol. 351, no. 6277, p. 10681070, Mar 2016. [Online]. Available: <http://dx.doi.org/10.1126/science.aad9480>
- [22] I. Chakrabarty, S. Khan, and V. Singh, “Dynamic grover search: applications in recommendation systems and optimization problems,” *Quantum Information Processing*, vol. 16, no. 6, Apr 2017. [Online]. Available: <http://dx.doi.org/10.1007/s11128-017-1600-4>
- [23] K. V. Gubaidullina and S. A. Chivilikhin, “Theoretical research of the distortion of quantum circuit in grover’s algorithm,” *Journal of Physics: Conference Series*, vol. 735, no. 1, p. 012074, 2016. [Online]. Available: <http://stacks.iop.org/1742-6596/735/i=1/a=012074>
- [24] B. Ye, T. Zhang, L. Qiu, and X. Wang, “Quantum discord and entanglement in grover search algorithm,” *Open Physics*, vol. 14, no. 1, Jan 2016. [Online]. Available: <http://dx.doi.org/10.1515/phys-2016-0020>
- [25] R. Dridi and H. Alghassi, “Prime factorization using quantum annealing and computational algebraic geometry,” *Scientific Reports*, vol. 7, no. 1, Feb 2017. [Online]. Available: <http://dx.doi.org/10.1038/srep43048>

- [26] N. Johansson and J. Åke Larsson, “Realization of shor’s algorithm at room temperature,” 2017.
- [27] Y. H. Lee, M. Khalil-Hani, and M. N. Marsono, “An fpga-based quantum computing emulation framework based on serial-parallel architecture,” *International Journal of Reconfigurable Computing*, vol. 2016, p. 118, 2016. [Online]. Available: <http://dx.doi.org/10.1155/2016/5718124>
- [28] T. H. Johnson, J. D. Biamonte, S. R. Clark, and D. Jaksch, “Solving search problems by strongly simulating quantum circuits,” *Scientific Reports*, vol. 3, no. 1, Feb 2013. [Online]. Available: <http://dx.doi.org/10.1038/srep01235>
- [29] A. Paler, I. Polian, K. Nemoto, and S. J. Devitt, “Fault-tolerant, high-level quantum circuits: form, compilation and description,” *Quantum Science and Technology*, vol. 2, no. 2, p. 025003, 2017. [Online]. Available: <http://stacks.iop.org/2058-9565/2/i=2/a=025003>
- [30] Y. Cao, A. Daskin, S. Frankel, and S. Kais, “Quantum circuit design for solving linear systems of equations,” *Molecular Physics*, vol. 110, no. 15-16, p. 16751680, Aug 2012. [Online]. Available: <http://dx.doi.org/10.1080/00268976.2012.668289>
- [31] Y. Zheng, C. Song, M.-C. Chen, B. Xia, W. Liu, Q. Guo, L. Zhang, D. Xu, H. Deng, K. Huang, and et al., “Solving systems of linear equations with a superconducting quantum processor,” *Physical Review Letters*, vol. 118, no. 21, May 2017. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevLett.118.210504>
- [32] G. D. Paparo and M. A. Martin-Delgado, “Google in a quantum network,” *Scientific Reports*, vol. 2, no. 1, Jun 2012. [Online]. Available: <http://dx.doi.org/10.1038/srep00444>
- [33] G. D. Paparo, M. Müller, F. Comellas, and M. A. Martin-Delgado, “Quantum google algorithm,” *The European Physical Journal Plus*, vol. 129, no. 7, Jul 2014. [Online]. Available: <http://dx.doi.org/10.1140/epjp/i2014-14150-y>
- [34] J. A. Izaac, X. Zhan, Z. Bian, K. Wang, J. Li, J. B. Wang, and P. Xue, “Centrality measure based on continuous-time quantum walks and experimental realization,” *Physical Review A*, vol. 95, no. 3, Mar 2017. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.95.032318>
- [35] “Quantum manifesto.” [Online]. Available: https://msu.euramet.org/current_calls/fundamental_2017/documents/Quantum_Manifesto.pdf

- [36] C. Simon, "Towards a global quantum network," *Nature Photonics*, vol. 11, no. 11, p. 678680, Oct 2017. [Online]. Available: <http://dx.doi.org/10.1038/s41566-017-0032-0>
- [37] B. K. Behera, A. Banerjee, and P. K. Panigrahi, "Experimental realization of quantum cheque using a five-qubit quantum computer," *Quantum Information Processing*, vol. 16, no. 12, Nov 2017. [Online]. Available: <http://dx.doi.org/10.1007/s11128-017-1762-0>
- [38] F. Yan, A. M. Ilyasu, and P. Q. Le, "Quantum image processing: A review of advances in its security technologies," *International Journal of Quantum Information*, vol. 15, no. 03, p. 1730001, Apr 2017. [Online]. Available: <http://dx.doi.org/10.1142/S0219749917300017>
- [39] Y.-B. Sheng and L. Zhou, "Distributed secure quantum machine learning," *Science Bulletin*, vol. 62, no. 14, p. 10251029, Jul 2017. [Online]. Available: <http://dx.doi.org/10.1016/j.scib.2017.06.007>
- [40] J. L. Zhang, K. G. Lagoudakis, Y.-K. Tzeng, C. Dory, M. Radulaski, Y. Kelaita, K. A. Fischer, S. Sun, Z.-X. Shen, N. A. Melosh, and et al., "Complete coherent control of silicon vacancies in diamond nanopillars containing single defect centers," *Optica*, vol. 4, no. 11, p. 1317, Oct 2017. [Online]. Available: <http://dx.doi.org/10.1364/OPTICA.4.001317>
- [41] D.-L. Deng, X. Li, and S. Das Sarma, "Quantum entanglement in neural network states," *Physical Review X*, vol. 7, no. 2, May 2017. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevX.7.021021>
- [42] J. Chen, L. Wang, and E. Charbon, "A quantum-implementable neural network model," *Quantum Information Processing*, vol. 16, no. 10, Aug 2017. [Online]. Available: <http://dx.doi.org/10.1007/s11128-017-1692-x>
- [43] A. Galindo and P. Pascual, "Quantum mechanics i," 1990. [Online]. Available: <http://dx.doi.org/10.1007/978-3-642-83854-5>
- [44] Y. Wang, Y. Di, and H. Wei, "Controllability of spin 1 systems and realization of ternary swap gate in two spin 1 systems coupled with ising interaction," *Science China Physics, Mechanics and Astronomy*, vol. 53, no. 10, p. 18731877, Aug 2010. [Online]. Available: <http://dx.doi.org/10.1007/s11433-010-4110-2>

- [45] G. Mkrtchian, “Universal quantum logic gates in a scalable ising spin quantum computer,” *Physics Letters A*, vol. 372, no. 32, p. 52705273, Aug 2008. [Online]. Available: <http://dx.doi.org/10.1016/j.physleta.2008.06.030>
- [46] A. Barenco, C. H. Bennet, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, “Elementary gates for quantum computation,” *Physical Review A*, 1995. [Online]. Available: <https://journals.aps.org/pr/abstract/10.1103/PhysRevA.52.3457>
- [47] S. Díaz-Solórzano, “Esquemas de medidas,” *QIC*, 2014.
- [48] A. Kossakowski, “On quantum statistical mechanics of non-hamiltonian systems,” *Reports on Mathematical Physics*, vol. 3, no. 4, p. 247274, Dec 1972. [Online]. Available: [http://dx.doi.org/10.1016/0034-4877\(72\)90010-9](http://dx.doi.org/10.1016/0034-4877(72)90010-9)
- [49] G. Lindblad, “On the generators of quantum dynamical semigroups,” *Communications in Mathematical Physics*, vol. 48, no. 2, p. 119130, Jun 1976. [Online]. Available: <http://dx.doi.org/10.1007/BF01608499>
- [50] R. Gross and A. Marx, “Applied superconductivity: Josephson effect and superconducting electronics,” *Walther-Meißner-Institut*, 2005.
- [51] O. H.K., “Further experiments with liquid helium. g. on the electrical resistance of pure metals, etc. vi. on the sudden change in the rate at which the resistance of mercury disappears,” *Springer, Dordrecht*, 1911. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-94-009-2079-8_17
- [52] A. P. Drozdov, M. I. Erements, I. A. Troyan, V. Ksenofontov, and S. I. Shylin, “Conventional superconductivity at 203 kelvin at high pressures in the sulfur hydride system,” *Nature*, vol. 525, pp. 73–76, 2015.
- [53] M. Tinkham, *Introduction to superconductivity*. New York: McGraw Hill, 1996.
- [54] J. Bardeen, L. N. Cooper, and J. R. Schrieffer, “Theory of superconductivity,” *Physical Review Journals Archive*, 1957. [Online]. Available: <https://journals.aps.org/pr/abstract/10.1103/PhysRev.108.1175>
- [55] H. Fröhlich, “Theory of the superconducting state,” *Unknown*, 1950. [Online]. Available: [None](#)
- [56] J. Bardeen, “Theory of the meissner effect in superconductors,” *Physical Review*, vol. 97, no. 6, p. 17241725, Mar 1955. [Online]. Available: <http://dx.doi.org/10.1103/PhysRev.97.1724>

- [57] M. Cyrot, “Ginzburg-landau theory for superconductors,” *Reports on Progress in Physics*, vol. 36, no. 2, p. 103, 1973. [Online]. Available: <http://stacks.iop.org/0034-4885/36/i=2/a=001>
- [58] J. Bascom S. Deaver and W. M. Fairbank, “Experimental evidence for quantized flux in superconducting cylinders,” *Physical Review Letters*, 1961. [Online]. Available: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.7.43>
- [59] R. Doll and M. Naebauer, “Experimental proof of magnetic flux quantization in a superconducting ring,” *Physical Review Letters - PHYS REV LETT*, vol. 7, pp. 51–52, 07 1961.
- [60] I. Giaever, “Electron tunneling between two superconductors,” *Phys. Rev. Lett.*, vol. 5, pp. 464–466, Nov 1960. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.5.464>
- [61] B. Josephson, “Possible new effects in superconductive tunnelling,” *Physics Letters*, vol. 1, no. 7, pp. 251 – 253, 1962. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0031916362913690>
- [62] P. W. Anderson and J. M. Rowell, “Probable observation of the josephson superconducting tunneling effect,” *Phys. Rev. Lett.*, vol. 10, pp. 230–232, Mar 1963. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.10.230>
- [63] S. Shapiro, “Josephson currents in superconducting tunneling: The effect of microwaves and other observations,” *Phys. Rev. Lett.*, vol. 11, pp. 80–82, Jul 1963. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.11.80>
- [64] R. Feynman, *The Feynman lectures on physics*. Reading, Mass: Addison-Wesley Pub. Co, 1963.
- [65] P. Carelli, 2006. [Online]. Available: https://commons.wikimedia.org/wiki/File:I-V_characteristics_of_Josephson_Junction.JPG
- [66] P. A. M. Dirac, “The fundamental equations of quantum mechanics,” *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 109, no. 752, p. 642653, Dec 1925. [Online]. Available: <http://dx.doi.org/10.1098/rspa.1925.0150>

- [67] G. Wendin, “Quantum information processing with superconducting circuits: a review,” *IOP Science*, 2017. [Online]. Available: <http://iopscience.iop.org/article/10.1088/1361-6633/aa7e1a/pdf>
- [68] A. Blais, R.-S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf, “Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation,” *Physical Review A*, vol. 69, no. 6, Jun 2004. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.69.062320>
- [69] C. A. Schmuttenmaer, “Exploring dynamics in the far-infrared with terahertz spectroscopy,” *Chemical Reviews*, vol. 104, no. 4, pp. 1759–1780, 2004, PMID: 15080711. [Online]. Available: <https://doi.org/10.1021/cr020685g>
- [70] A. Blais, J. Gambetta, A. Wallraff, D. I. Schuster, S. M. Girvin, M. H. Devoret, , and R. J. Schoelkopf, “Quantum-information processing with circuit quantum electrodynamics,” *Physical Review A*, 2007. [Online]. Available: <https://journals.aps.org/prabstract/10.1103/PhysRevA.75.032329>
- [71] N. Schuch and J. Siewert, “Natural two-qubit gate for quantum computation using the xy interaction,” *Physical Review A*, 2003. [Online]. Available: <https://journals.aps.org/prabstract/10.1103/PhysRevA.67.032301>
- [72] G. Brassard and P. Hoyer, “An exact quantum polynomial-time algorithm for simons problem,” *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*. [Online]. Available: <http://dx.doi.org/10.1109/ISTCS.1997.595153>
- [73] L. K. Grover, “Quantum computers can search rapidly by using almost any transformation,” *Physical Review Letters*, vol. 80, no. 19, p. 43294332, May 1998. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevLett.80.4329>
- [74] —, “Quantum computers can search arbitrarily large databases by a single query,” *Physical Review Letters*, vol. 79, no. 23, p. 47094712, Dec 1997. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevLett.79.4709>
- [75] V. G. A. P, C. H. Bennett, and I. Thomas, “Optimization of grovers search algorithm.”
- [76] S. Haroche and D. Kleppner, “Cavity quantum electrodynamics,” *Physics Today*, vol. 42, no. 1, p. 2430, Jan 1989. [Online]. Available: <http://dx.doi.org/10.1063/1.881201>

- [77] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, “Post-quantum rsa,” Cryptology ePrint Archive, Report 2017/351, 2017, <https://eprint.iacr.org/2017/351>.
- [78] F. Grosshans, T. Lawson, F. Morain, and B. Smith, “Factoring safe semiprimes with a single quantum query,” 2015.
- [79] S. Brin and L. Page, “The anatomy of a large-scale hypertextual web search engine,” *Computer Networks and ISDN Systems*, vol. 30, no. 1, pp. 107 – 117, 1998, proceedings of the Seventh International World Wide Web Conference. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S016975529800110X>
- [80] T. G. Wong, “Equivalence of szegedys and coined quantum walks,” *Quantum Information Processing*, vol. 16, no. 9, Jul 2017. [Online]. Available: <http://dx.doi.org/10.1007/s11128-017-1667-y>
- [81] F. Magniez, A. Nayak, J. Roland, and M. Santha, “Search via quantum walk,” *SIAM Journal on Computing*, vol. 40, no. 1, p. 142164, Jan 2011. [Online]. Available: <http://dx.doi.org/10.1137/090745854>
- [82] R. A. M. Santos, “Szegedys quantum walk with queries,” *Quantum Information Processing*, vol. 15, no. 11, p. 44614475, Aug 2016. [Online]. Available: <http://dx.doi.org/10.1007/s11128-016-1427-4>
- [83] M. Suzuki, “Decomposition formulas of exponential operators and lie exponentials with some applications to quantum mechanics and statistical physics,” *Journal of Mathematical Physics*, vol. 26, no. 4, p. 601612, Apr 1985. [Online]. Available: <http://dx.doi.org/10.1063/1.526596>
- [84] W. Louisell, *Quantum statistical properties of radiation*. New York: Wiley, 1973.