



Universidad Simón Bolívar
Decanato de Estudios Profesionales
Coordinación de 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

Índice general

Índice de Figuras	7
Lista de Tablas	10
1. Introducción	11
1.1. JUSTIFICACION	16
1.2. OBJETIVOS	18
1.2.1. Objetivo General:	18
1.2.2. Objetivos Específicos:	18
1.2.3. Fases del Proyecto	18
1.2.4. REFERENCIAS	19
2. Información cuántica	22
2.1. Función de onda	22
2.2. Espacio de Hilbert	23
2.3. Delta de Kronecker	24
2.4. Operadores hermíticos	25
2.5. Operadores unitarios	25
2.6. Notación de Dirac	25
2.7. Producto tensorial	27
2.8. Postulados de la mecánica cuántica	29
2.9. Matriz densidad	30
2.10. Traza parcial	32
2.10.1. Comparación con el producto tensorial	33
2.11. Entrelazamiento	33
2.12. Computación cuántica	34
2.12.1. Qubits	34
2.12.2. Esfera de Bloch	35
2.12.3. Conmutador y anticonmutador	35
2.12.3.1. Conmutador	36
2.12.3.2. Anticonmutador	36
2.12.4. Matrices de Pauli	36
2.12.5. Circuitos cuánticos	37
2.12.6. Compuertas cuánticas de un qubit	39
2.12.6.1. Compuerta identidad	39

2.12.6.2. Compuerta X	40
2.12.6.3. Compuerta Z	40
2.12.6.4. Compuerta Y	41
2.12.6.5. Compuerta de Hadamard	42
2.12.6.6. Compuerta S	42
2.12.6.7. Compuerta T	43
2.12.6.8. Compuerta de cambio de fase	43
2.12.6.9. Compuertas de rotación	44
2.12.7. Compuertas multiqubit	45
2.12.7.1. Compuerta CNOT	45
2.12.7.2. Compuerta SWAP	46
2.12.7.3. Compuerta $\sqrt{\text{SWAP}}$	47
2.12.7.4. Compuerta de Ising	47
2.12.7.5. Compuerta de Toffoli	48
2.12.7.6. Compuerta de Deutsch	48
2.12.8. Conjuntos universales de compuertas cuánticas	49
2.12.9. Criterios de DiVincenzo	49
2.13. Fidelidad	50
2.14. Medidas proyectivas	51
2.15. Sistemas cuánticos abiertos	52
3. Superconductividad	59
3.1. Cuantización macroscópica y superconductividad	59
3.2. La teoría BCS	61
3.3. Cuantización del flujo magnético y efecto tunel Giaver	69
3.4. Efecto Josephson	75
3.5. Componentes de la corriente en las uniones de Josephson	80
3.6. Qubits superconductores	81
3.7. Arquetipos de qubits superconductores	82
3.7.1. Qubit de carga	82
3.7.2. Qubit de flujo	83
3.7.3. Qubit de fase	83
3.8. Transmones	83
3.9. Hamiltonianos multiqubit de transmones	84
3.9.1. Acoplamiento capacitivo	84
3.9.2. Acoplamiento por el resonador	84
3.9.3. Acoplamiento de JJ	85
3.9.4. Acoplamiento afinable/calibrable	85
3.10. Compuertas cuánticas en transmones	85
3.10.1. El operador de evolución temporal	85
3.10.2. Pulsos de microondas	86
3.10.3. Régimen rotacional del pulso	86
3.10.4. Efecto del pulso sobre el qubit	86
3.10.5. Régimen dispersivo	87

3.10.6. Rotaciones X-Y	87
3.10.7. Compuerta de entrelazamiento	88
3.10.8. Compuertas compuestas	88
4. El simulador	89
4.1. Parámetros de los sistemas simulados	90
4.2. Compuertas nativas	91
4.2.1. Rx y Ry	91
4.2.2. iSWAP	93
4.3. Compuertas compuestas	94
4.3.1. X	94
4.3.2. Y	94
4.3.3. Rz	94
4.3.4. Z	95
4.3.5. H	95
4.3.6. CNOT	96
4.3.7. SWAP	96
4.3.8. Compuertas condicionales generales	96
4.3.9. CP	100
5. Algoritmo de Grover	108
5.1. El algoritmo	112
5.2. Variaciones y generalizaciones del algoritmo de Grover	113
5.2.1. Algoritmo de amplificación de amplitud	113
5.2.2. Algoritmo de Grover en un paso	116
5.2.3. Optimización del algoritmo de Grover	117
5.3. Simulaciones	118
5.3.1. Algoritmo de Grover en un paso y optimización	122
6. Algoritmo de Shor	122
6.1. Transformada cuántica de Fourier	122
6.2. Estimación de fase	124
6.3. Estimación de orden	127
6.4. Expansión en fracciones continuas	130
6.5. Algoritmo de factorización de Shor	131
6.6. Simulaciones	132
6.6.1. Factorización del número 15	132
6.6.2. Factorización del número 8	135
7. Google PageRank	137
7.1. El algoritmo de remiendo (parcheo) general	140
7.2. Interpretación como una caminata aleatoria	141
7.3. Cuantizando las caminatas aleatorias	142
7.4. Caminata cuántica de Szegedy	142
7.5. PageRank cuántico	144

7.6. Circuitos de las caminatas cuánticas de Szegedy	144
7.7. Simulaciones	149
7.7.1. Grafo estrella	149
7.7.2. Grafo corona	153
7.7.3. Grafo árbol	157
7.7.4. Grafo aleatorio	161
A. Cálculos de Hamiltonianos	165
A.1. Hamiltoniano de Jaynes-Cummings	165
A.2. Hamiltoniano multiqubit	165
A.3. Pulsos de microondas	165
A.4. Régimen rotacional del pulso	166
A.5. Efecto del pulso sobre el qubit	170
A.6. Régimen dispersivo	171
A.7. Rotaciones X-Y	174
A.8. Compuerta de entrelazamiento	175
B. Códigos del simulador	176
B.1. Wolfram Mathematica	176
B.2. Python	183
C. Códigos de la simulación del algoritmo de Grover	196
C.1. Wolfram Mathematica	196
C.2. Python	198
D. Códigos de la simulación del algoritmo de Shor	200
D.1. Wolfram Mathematica	200
D.2. Python	204
E. Códigos de la simulación del algoritmo de PageRank	208
E.1. Wolfram Mathematica	208
E.2. Python	208
E.2.1. Grafo estrella	212
E.2.2. Grafo corona	215
E.2.3. Grafo árbol	218
E.2.4. Grafo aleatorio	221

Índice de figuras

2.1. Esfera de Bloch	35
2.2. Compuerta I en la esfera de Bloch	40
2.3. Compuerta X en la esfera de Bloch	40
2.4. Compuerta Z en la esfera de Bloch	41
2.5. Compuerta Y en la esfera de Bloch	41
2.6. Compuerta H en la esfera de Bloch	42
2.7. Compuerta S en la esfera de Bloch	43
2.8. Compuerta T en la esfera de Bloch	43
2.9. Compuerta P en la esfera de Bloch	44
2.10. Compuertas Rx, Ry y Rz en la esfera de Bloch	45
3.1. Diagrama de Feynman de la interacción electrón-fonón-electrón	65
3.2. Construcción geométrica de los posibles electrones candidatos para formar pares de Cooper, siendo $\hbar K$ el momentum del centro de masas.	66
3.3. Cuantización del flujo magnético	71
3.4. Imposibilidad de efecto túnel a través de la barrera	73
3.5. Posibilidad de efecto túnel a través de la barrera	74
3.6. Efecto Giaver: Efecto túnel entre un metal y un superconductor	75
3.7. Curva característica de una unión Josephson	79
4.1. Rotaciones en X e Y de 2π	92
4.2. Rotaciones en X e Y de π	92
4.3. Rotaciones en X e Y de $\frac{\pi}{2}$	92
4.4. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $ 00\rangle$	93
4.5. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $ 01\rangle$	93
4.6. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $\frac{ 00\rangle+ 11\rangle}{\sqrt{2}}$	93
4.7. Compuertas iSWAP y \sqrt{iSWAP} aplicadas a $\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}}$	93
5.1. Circuito del algoritmo de Grover, k_{max} desconocido.	110
5.2. Interpretación geométrica del operador difusión	112
5.3. Circuito del algoritmo de Grover.	112
5.4. Evolución de las probabilidades en el algoritmo de Grover sin relación	119
5.5. Evolución de las probabilidades en el algoritmo de Grover con relación, $\mathcal{W} = \{15\}$	120

5.6. Evolución de las probabilidades en el algoritmo de Grover con relación, $\mathcal{W} = \{6\}$	120
5.7. Evolución de las probabilidades en el algoritmo de Grover con relación, $\mathcal{W} = \{0\}$	121
5.8. Evolución de las probabilidades en el algoritmo de Grover sin relación $\mathcal{W} = \{9, 13\}$	121
5.9. Evolución de las probabilidades en el algoritmo de Grover sin relación, $\mathcal{W} = \{9, 13\}$	122
5.10. Evolución de las probabilidades en el algoritmo de Grover sin relación $\mathcal{W} = \{4, 5, 12, 13\}$	122
5.11. Evolución de las probabilidades en el algoritmo de Grover con relación $\mathcal{W} = \{4, 5, 12, 13\}$	122
6.1. Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas	133
6.2. Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas	135
7.1. Transformación de un grafo al crear la matriz de Google con $\alpha = \frac{1}{2}$	141
7.2. Operador de permutación	146
7.3. Circuito de Loke para las caminatas cuánticas de Szegedy	146
7.4. Circuito de K_i	147
7.5. Grafo estrella	150
7.6. Circuito de K_1 para el grafo estrella	150
7.7. Circuito de K_2 para el grafo estrella	151
7.8. K_b del grafo estrella	151
7.9. T del grafo estrella	151
7.10. Preparación del estado inicial para la caminata en el grafo estrella	151
7.11. Circuito del PageRank cuántico del grafo estrella	152
7.12. PageRank cuántico instantáneo del grafo estrella sin pérdidas	152
7.13. PageRank cuántico promedio del grafo estrella sin pérdidas	152
7.14. PageRank cuántico instantaneo del grafo estrella con y sin pérdidas	153
7.15. PageRank cuántico promedio del grafo estrella con y sin pérdidas	153
7.16. Grafo corona	154
7.17. Circuito de K_1 para el grafo corona	154
7.18. Circuito de K_2 para el grafo corona	155
7.19. K_b del grafo corona	155
7.20. T del grafo corona	155
7.21. Preparación del estado inicial para la caminata en el grafo corona	155
7.22. Circuito del PageRank cuántico del grafo corona	156
7.23. PageRank cuántico instantáneo del grafo corona sin pérdidas	156
7.24. PageRank cuántico promedio del grafo corona sin pérdidas	156
7.25. Grafo árbol	157
7.26. Circuito de K_1 para el grafo árbol	158
7.27. Circuito de K_2 para el grafo árbol	158

7.28. Circuito de K_3 para el grafo árbol	158
7.29. K_b del grafo árbol	158
7.30. T del grafo árbol	158
7.31. Preparación del estado inicial para la caminata en el grafo árbol . . .	159
7.32. Circuito del PageRank cuántico del grafo árbol	159
7.33. PageRank cuántico instantáneo del grafo árbol sin pérdidas	159
7.34. PageRank cuántico promedio del grafo árbol sin pérdidas	160
7.35. PageRank cuántico instantaneo del grafo árbol con y sin pérdidas . .	160
7.36. PageRank cuántico promedio del grafo árbol con y sin pérdidas . .	160
7.37. Grafo aleatorio	161
7.38. Circuito de K_1 para el grafo aleatorio	162
7.39. Circuito de K_2 para el grafo aleatorio	162
7.40. Circuito de K_3 para el grafo aleatorio	162
7.41. K_b del grafo aleatorio	162
7.42. T del grafo aleatorio	162
7.43. Preparación del estado inicial para la caminata en el grafo aleatorio	163
7.44. Circuito del PageRank cuántico del grafo aleatorio	163
7.45. PageRank cuántico instantáneo del grafo aleatorio sin pérdidas . . .	163
7.46. PageRank cuántico promedio del grafo aleatorio sin pérdidas	164
7.47. PageRank cuántico instantaneo del grafo aleatorio con y sin pérdidas	164
7.48. PageRank cuántico promedio del grafo aleatorio con y sin pérdidas .	164

Índice de cuadros

Capítulo 5

Algoritmo de Grover

El algoritmo de Grover es un 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. 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.

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

Veamos lo que sucede al aplicar esta secuencia de rotaciones sobre el estado $|s\rangle$:

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

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

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 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 $9(1 - \frac{4}{3N})\frac{1}{N}$.

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

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

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 $|\omega\rangle$.

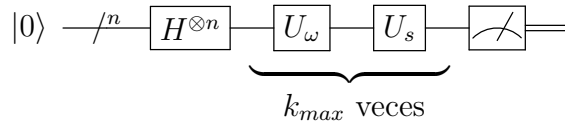


FIGURA 5.1: Circuito del algoritmo de Grover, k_{max} desconocido.

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 $U_s U_\omega$.

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

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

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 escribimos 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:

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

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

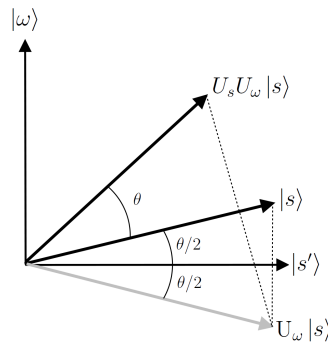


FIGURA 5.2: Interpretación geométrica del operador difusión

5.1. El algoritmo

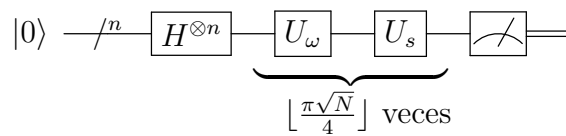


FIGURA 5.3: Circuito del algoritmo de Grover.

1. Preparar el estado fiducial.
2. Aplicar la transformada de Walsh-Hadamard.
3. Realizar la iteración de Grover $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ 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 [ref] y por Grover en 1998 [ref]. 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 $\sin(\theta) = \langle\psi|\Pi_{\mathcal{W}}|\psi\rangle$. De aquí podemos hallar 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 $U_{\mathcal{W}} = \mathbb{1} - 2\Pi_{\mathcal{W}}$, 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:

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

Como se puede ver, el operador $U_\psi U_{\mathcal{W}}$ rota un ángulo de 2θ . Por lo que si se aplica k veces a $|\psi\rangle$, 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:

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

Mientras menor sea θ , más tenderá $(U_\psi U_W)^{k_{max}} |\psi\rangle$ 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_A el operador asociado a un algoritmo cuántico \mathcal{A} , entonces, tal que, partiendo del estado fiducial, retorne el estado $|\psi\rangle$. Es decir, $U_A |0\rangle = |\psi\rangle$, entonces, podemos reescribir U_ψ de la siguiente manera:

$$U_\psi = (2|\psi\rangle\langle\psi| - \mathbb{1}) = (2U_A |0\rangle\langle 0| U_A^\dagger - \mathbb{1}) = U_A(2|0\rangle\langle 0| - \mathbb{1})U_A^\dagger = U_A U_0 U_A^\dagger \quad (5.29)$$

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

Ahora consideremos el caso en el que $U_A = H^{\otimes n}$, 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.

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

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

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

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

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

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

En [ref] Grover propone una manera alternativa para ejecutar su algoritmo. En lugar de realizar $O(\sqrt{N})$ iteraciones, propone realizar una sola iteración en $\Omega(\sqrt{N \log(N)})$ sistemas identicos simultáneamente. 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 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

En [ref] Garg y Pande 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 han encontrado 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 realizan 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 relajación $\gamma = 25KHz$.

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 espacio 2D 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 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.

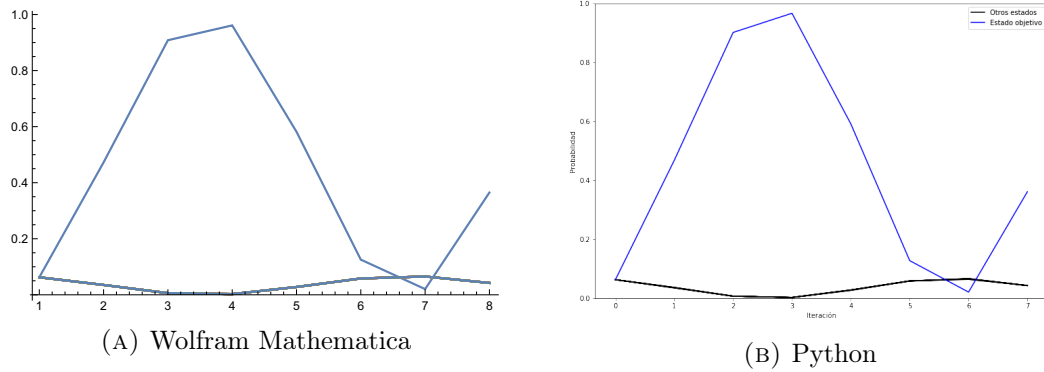


FIGURA 5.4: Evolución de las probabilidades en el algoritmo de Grover sin relajación

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 estado excitados, es decir, a estados de energías superiores y esto es energía que el entorno absorbe por efecto Purcell. 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 5.5, 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 5.7 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 5.6 presenta el caso en el que $|\omega\rangle = |0110\rangle$. Este es un caso intermedio y el sistema tiene un efecto distinto sobre cada partición.

Los tiempos de vida no son suficientes

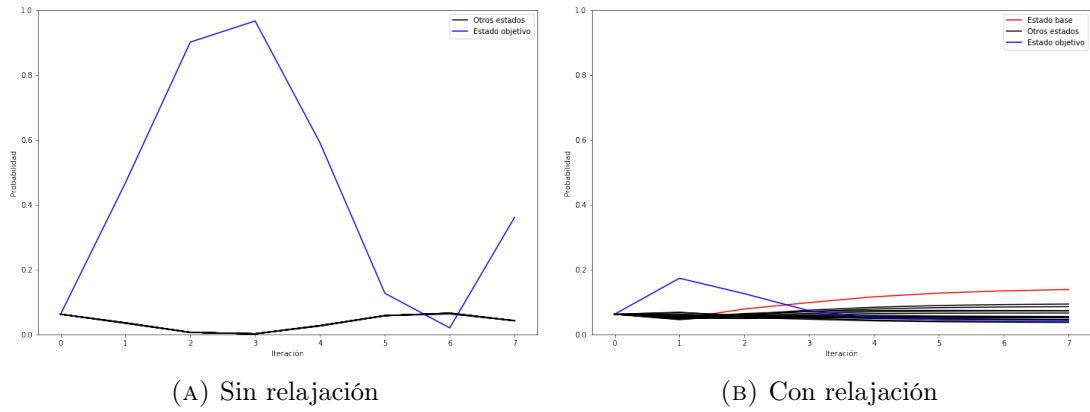


FIGURA 5.5: Evolución de las probabilidades en el algoritmo de Grover con relajación, $\mathcal{W} = \{15\}\{1111_2\}$

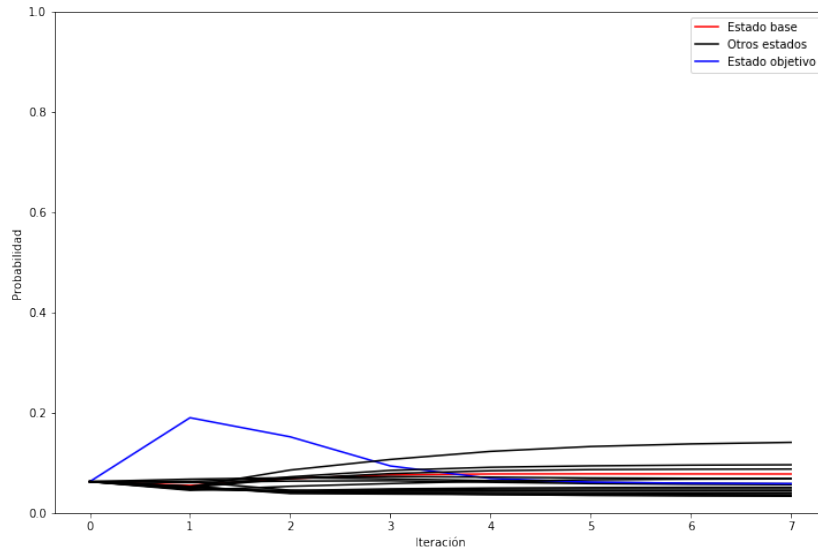
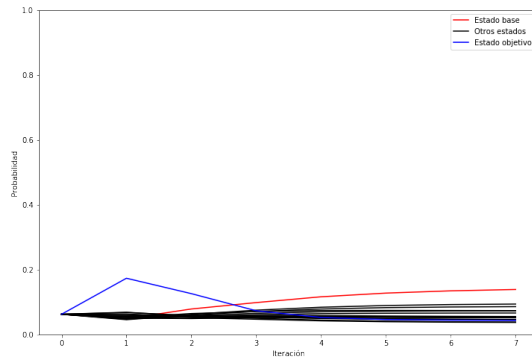


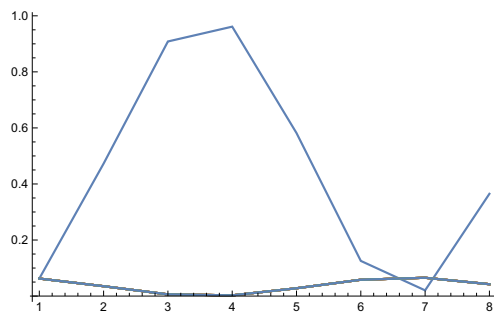
FIGURA 5.6: Evolución de las probabilidades en el algoritmo de Grover con relajación, $\mathcal{W} = \{6\} = \{0110_2\}$

(A) $\omega = 15$

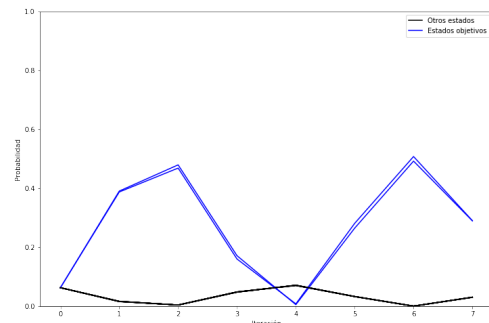
img/grover0000loss.png

(B) $\omega = 0$ FIGURA 5.7: Evolución de las probabilidades en el algoritmo de Grover con relajación, $\mathcal{W} = \{0\} = \{0000_2\}$

Ahora veamos los casos en los que se tiene más de un estado deseado



(A) Wolfram Mathematica



(B) Python

FIGURA 5.8: Evolución de las probabilidades en el algoritmo de Grover sin relajación $\mathcal{W} = \{9, 13\} = \{1001_2, 1101_2\}$

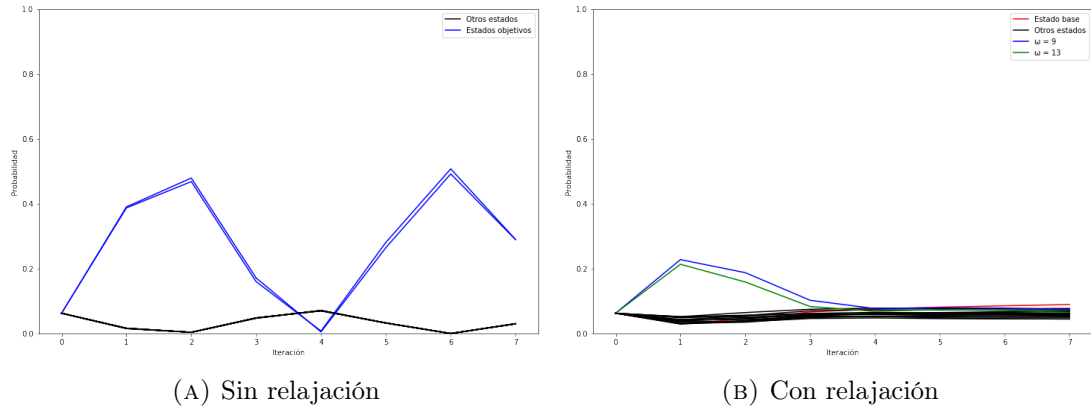


FIGURA 5.9: Evolución de las probabilidades en el algoritmo de Grover sin relajación $\mathcal{W} = \{9, 13\} = \{1001_2, 1101_2\}$

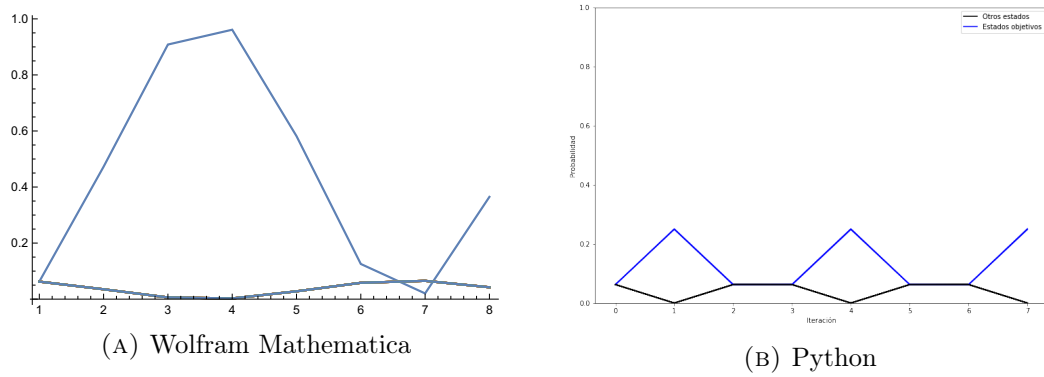


FIGURA 5.10: Evolución de las probabilidades en el algoritmo de Grover sin relajación $\mathcal{W} = \{4, 5, 12, 13\} = \{0100_2, 0101_2, 1100_2, 1101_2\}$

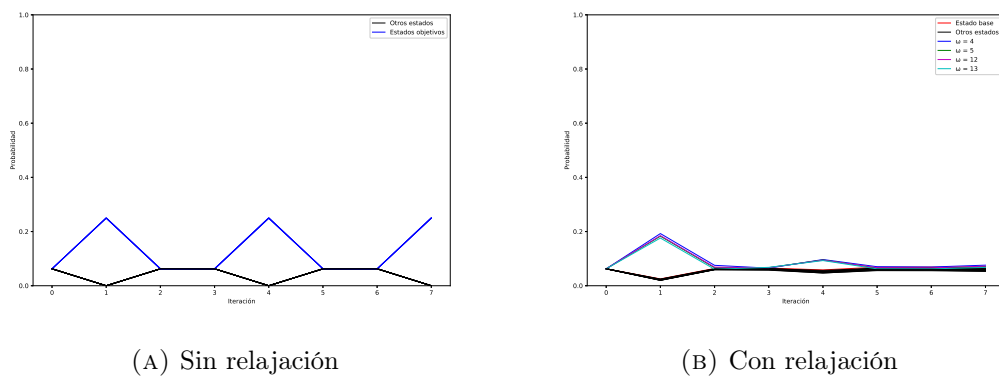


FIGURA 5.11: Evolución de las probabilidades en el algoritmo de Grover con relajación $\mathcal{W} = \{4, 5, 12, 13\} = \{0100_2, 0101_2, 1100_2, 1101_2\}$

5.3.1. Algoritmo de Grover en un paso y optimización

Bibliografía

- [1] Adriano Barenco, Charles H. Bennet, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, Jhon A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 1995.
- [2] Sttiwuer Díaz-Solórzano. Esquemas de medidas. *QIC*, 2014.
- [3] Rudolf Gross and Achim Marx. Applied superconductivity: Josephson effect and superconducting electronics. *Walther-Meißner-Institut*, 2005.
- [4] Onnes 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.
- [5] 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*, 525:73–76, 2015.
- [6] J. Bardeen, L. N. Cooper, and J. R. Schrieffer. Theory of superconductivity. *Physical Review Journals Archive*, 1957.
- [7] Herbert Fröhlich. Theory of the superconducting state. *Unknown*, 1950.
- [8] M Cyrot. Ginzburg-landau theory for superconductors. *Reports on Progress in Physics*, 36(2):103, 1973.
- [9] Jr. Bascom S. Deaver and William M. Fairbank. Experimental evidence for quantized flux in superconducting cylinders. *Physical Review Letters*, 1961.
- [10] B.D. Josephson. Possible new effects in superconductive tunnelling. *Physics Letters*, 1(7):251 – 253, 1962.
- [11] P. W. Anderson and J. M. Rowell. Probable observation of the josephson superconducting tunneling effect. *Phys. Rev. Lett.*, 10:230–232, Mar 1963.

-
- [12] Sidney Shapiro. Josephson currents in superconducting tunneling: The effect of microwaves and other observations. *Phys. Rev. Lett.*, 11:80–82, Jul 1963.
 - [13] G. Wendin. Quantum information processing with superconducting circuits: a review. *IOP Science*, 2017.
 - [14] Alexandre Blais, Jay 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.
 - [15] Norbert Schuch and Jens Siewert. Natural two-qubit gate for quantum computation using the xy interaction. *Physical Review A*, 2003.
 - [16] T. Loke and J.B. Wang. Efficient quantum circuits for szegedy quantum walks. *Annals of Physics*, 382:64 – 84, 2017.