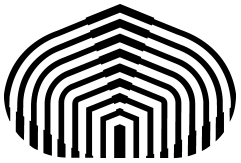


Universidad Simón Bolívar
Decanato de Estudios Profesionales
Coordinación de Tecnología e Ingeniería de Electrónica

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

Índice general

Índice de Figuras **6**

1. Introducción **10**

2. Información cuántica **18**
2.1. Operadores lineales . . . 18
2.2. Delta de Kronecker . . . 19
2.3. Operadores hermíticos . . . 19
2.4. Operadores unitarios . . . 20
2.5. Conmutador y anticonmutador . . . 21
2.6. Espacios de Hilbert . . . 22
2.7. Estados cuánticos . . . 24
2.8. Sistemas multipartitos . . . 30
2.9. Postulados de la mecánica cuántica . . . 33
2.10. Entrelazamiento . . . 34
2.11. Qubits . . . 35

3. Superconductividad **60**
3.1. Cuantización macroscópica y superconductividad . . . 60
3.2. La teoría BCS . . . 62
3.3. Cuantización del flujo magnético y efecto tunel Giaver . . . 70
3.4. Efecto Josephson . . . 76
3.5. Componentes de la corriente en las junciones de Josephson . . . 81
3.6. Qubits superconductores . . . 82
3.7. Arquetipos de qubits superconductores . . . 84
3.8. Transmones . . . 84
3.9. Hamiltonianos multiqubit de transmones . . . 87
3.10. Compuertas cuánticas en transmones . . . 88
3.10.1. Rotaciones X-Y . . . 90
3.10.2. Compuerta de entrelazamiento . . . 90
3.10.3. Compuertas compuestas . . . 91

4. El simulador de compuertas cuánticas en transmones **92**
4.1. Parámetros de los sistemas simulados . . . 93
4.2. Compuertas nativas . . . 94

4.2.1. Rx y Ry . . . 94
4.2.2. iSWAP . . . 96
4.3. Compuertas compuestas . . . 97
4.3.1. X . . . 97
4.3.2. Y . . . 97
4.3.3. Rz . . . 98
4.3.4. Z . . . 98
4.3.5. H . . . 99
4.3.6. CNOT . . . 99
4.3.7. SWAP . . . 99
4.3.8. Compuertas condicionales generales . . . 100
4.3.9. CP . . . 104

5. Algoritmo de Grover 112
5.1. El algoritmo . . . 117
5.2. Variaciones y generalizaciones del algoritmo de Grover . . . 117
5.2.1. Algoritmo de amplificación de amplitud . . . 117
5.2.2. Algoritmo de Grover en un paso . . . 120
5.2.3. Optimización del algoritmo de Grover . . . 121
5.3. Simulaciones . . . 122

6. Algoritmo de Shor 128
6.1. Transformada cuántica de Fourier . . . 128
6.2. Estimación de fase . . . 130
6.3. Estimación de orden . . . 132
6.4. Expansión en fracciones contínuas . . . 136
6.5. Algoritmo de factorización de Shor . . . 137
6.6. Simulaciones . . . 138
6.6.1. Factorización del número 15 . . . 138
6.6.2. Factorización del número 8 . . . 141

7. Google PageRank 143
7.1. El algoritmo de remiendo (parcheo) general . . . 146
7.2. Interpretación como una caminata aleatoria . . . 147
7.3. Cuantizando las caminatas aleatorias . . . 148
7.4. Caminata cuántica de Szegedy . . . 149
7.5. PageRank Cuántico . . . 150
7.6. Circuitos de las caminatas cuánticas de Szegedy . . . 150
7.7. Simulaciones . . . 155
7.7.1. Grafo estrella . . . 155
7.7.2. Grafo corona . . . 159
7.7.3. Grafo árbol . . . 163
7.7.4. Grafo aleatorio . . . 167

8. Conclusiones 172

A. Cálculos de Hamiltonianos **176**
A.1. Régimen rotacional del pulso . . . 176
A.2. Efecto del pulso sobre el qubit . . . 181
A.3. Régimen dispersivo . . . 182

B. Códigos del simulador **187**
B.1. Wolfram Mathematica . . . 187
B.2. Python . . . 194

C. Códigos de la simulación del algoritmo de Grover **207**
C.1. Wolfram Mathematica . . . 207
C.2. Python . . . 208

D. Códigos de la simulación del algoritmo de Shor **211**
D.1. Wolfram Mathematica . . . 211
D.2. Python . . . 214

E. Códigos de la simulación del algoritmo de PageRank **217**
E.1. Wolfram Mathematica . . . 217
E.2. Python . . . 220
E.2.1. Grafo estrella . . . 224
E.2.2. Grafo corona . . . 228
E.2.3. Grafo árbol . . . 230
E.2.4. Grafo aleatorio . . . 233

Índice de figuras

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. 67
3.3. Cuantización del flujo magnético 72
3.4. Diagrama de energía de una junción metal-aislante-metal en la que no puede haber efecto túnel 74
3.5. Diagrama de energía de una junción metal-aislante-metal en la que puede haber efecto túnel 75
3.6. Diagrama de energía de una junción superconductor-aislante-metal en la que puede haber efecto Giaver 76
3.7. Curva característica I-V de una unión Josephson 80

4.1. Rotaciones en X e Y de 2π 95
4.2. Rotaciones en X e Y de π 95
4.3. Rotaciones en X e Y de $\frac{\pi}{2}$ 95
4.4. Compuertas iSWAP y $\sqrt{iSWAP}$ aplicadas a $|00\rangle$ 96
4.5. Compuertas iSWAP y $\sqrt{iSWAP}$ aplicadas a $|01\rangle$ 96
4.6. Compuertas iSWAP y $\sqrt{iSWAP}$ aplicadas a $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ 96
4.7. Compuertas iSWAP y $\sqrt{iSWAP}$ aplicadas a $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ 97

5.1. Circuito del algoritmo de Grover, k_{max} desconocido. 114
5.2. Interpretación geométrica del operador difusión 116
5.3. Circuito del algoritmo de Grover. 117
5.4. Evolución de las probabilidades en el algoritmo de Grover sin relajación 124
5.5. Evolución de las probabilidades en el algoritmo de Grover con relajación, $\mathcal{W} = \{0\}$ 125
5.6. Evolución de las probabilidades en el algoritmo de amplificación de amplitud sin relajación, $\mathcal{W} = \{9, 13\}$ 126
5.7. Evolución de las probabilidades en el algoritmo de amplificación de amplitud sin relajación, $\mathcal{W} = \{4, 5, 12, 13\}$ 126
5.8. Evolución de las probabilidades en el algoritmo de amplificación de amplitud con relajación 127

6.1. Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas 139

6.2. Distribución de probabilidad en la estimación de fase del algoritmo de Shor sin pérdidas 141

7.1. Grafo de ejemplo para el PageRank clásico 143
7.2. Transformación de un grafo al crear la matriz de Google con $\alpha = \frac{1}{2}$ 147
7.3. Operador de permutación 152
7.4. Circuito de Loke [ref 152
7.5. Circuito de K_i 153
7.6. Grafo estrella 156
7.7. Circuito de K_1 para el grafo estrella 156
7.8. Circuito de K_2 para el grafo estrella 157
7.9. K_b del grafo estrella 157
7.10. T del grafo estrella 157
7.11. Preparación del estado inicial para la caminata en el grafo estrella . 157
7.12. Circuito del PageRank cuántico del grafo estrella 158
7.13. PageRank cuántico instantáneo del grafo estrella sin pérdidas 158
7.14. PageRank cuántico promedio del grafo estrella sin pérdidas 158
7.15. PageRank cuántico instantaneo del grafo estrella con y sin pérdidas 159
7.16. PageRank cuántico promedio del grafo estrella con y sin pérdidas . 159
7.17. Grafo corona 160
7.18. Circuito de K_1 para el grafo corona 160
7.19. Circuito de K_2 para el grafo corona 161
7.20. K_b del grafo corona 161
7.21. T del grafo corona 161
7.22. Preparación del estado inicial para la caminata en el grafo corona . 161
7.23. Circuito del PageRank cuántico del grafo corona 162
7.24. PageRank cuántico instantáneo del grafo corona sin pérdidas 162
7.25. PageRank cuántico promedio del grafo corona sin pérdidas 162
7.26. PageRank cuántico instantaneo del grafo aleatorio con y sin pérdidas 163
7.27. PageRank cuántico promedio del grafo aleatorio con y sin pérdidas 163
7.28. Grafo árbol 163
7.29. Circuito de K_1 para el grafo árbol 164
7.30. Circuito de K_2 para el grafo árbol 164
7.31. Circuito de K_3 para el grafo árbol 165
7.32. K_b del grafo árbol 165
7.33. T del grafo árbol 165
7.34. Preparación del estado inicial para la caminata en el grafo árbol . . 165
7.35. Circuito del PageRank cuántico del grafo árbol 166
7.36. PageRank cuántico instantáneo del grafo árbol sin pérdidas 166
7.37. PageRank cuántico promedio del grafo árbol sin pérdidas 166
7.38. PageRank cuántico instantaneo del grafo árbol con y sin pérdidas . 167
7.39. PageRank cuántico promedio del grafo árbol con y sin pérdidas . . 167
7.40. Grafo aleatorio 167
7.41. Circuito de K_1 para el grafo aleatorio 168

7.42. Circuito de K_2 para el grafo aleatorio 168
7.43. Circuito de K_3 para el grafo aleatorio 169
7.44. K_b del grafo aleatorio 169
7.45. T del grafo aleatorio 169
7.46. Preparación del estado inicial para la caminata en el grafo aleatorio 169
7.47. Circuito del PageRank cuántico del grafo aleatorio 170
7.48. PageRank cuántico instantáneo del grafo aleatorio sin pérdidas . . . 170
7.49. PageRank cuántico promedio del grafo aleatorio sin pérdidas 170
7.50. PageRank cuántico instantaneo del grafo aleatorio con y sin pérdidas 171
7.51. PageRank cuántico promedio del grafo aleatorio con y sin pérdidas 171

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 [ref]. 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 [ref] 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 [ref]. 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 $a^r \equiv 1 \mod m$, a partir del operador unitario de multiplicación modular.

6.1. Transformada cuántica de Fourier

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

$$U = \sum_x \sum_y K(x, y) \, |y\rangle\langle x| \tag{6.1}$$

Aplica la transformada

$$|x\rangle \to K(x,y)\,|y\rangle \tag{6.2}$$

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

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

$$\omega_n = e^{2\pi i/N} \tag{6.3}$$

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

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

La transformada integral discreta con el Kernel K,

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

se llama la transformada discreta de Fourier (DFT).

El Kernel K es unitario ya que:

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

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

El Kernel para $n = 1$ es:

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

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

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

La QFT inversa está dada por:

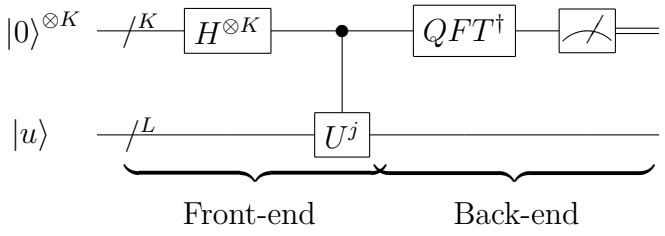
$$QFT^{-1} = QFT^{\dagger} = \frac{1}{\sqrt{N}} \sum_x \sum_k e^{-2\pi i k x/N} \, |x\rangle\langle k| \tag{6.9}$$

6.2. Estimación de fase

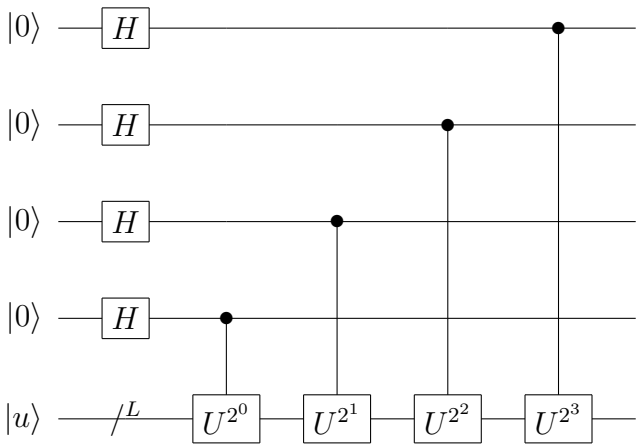
Asumamos que tenemos un operador U, con autoestados $|u\rangle$ de dimensión L, y con autovalores complejos desconocidos $\lambda_\phi = e^{2i\pi\phi}$, donde ϕ es un número real tal que $0 \leq \phi \leq 1$, a ser determinado.

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

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 $\mathbb{1}$ y el estado de salida es igual al de entrada.

$$CU^j |0000\rangle \otimes |u\rangle = e^{i0\times 2\pi\phi} |0\rangle \otimes |u\rangle \tag{6.10}$$

$|1\rangle = |0001\rangle$:

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 $e^{i2\pi\phi}$.

$$CU^j |0001\rangle \otimes |u\rangle = e^{i1\times 2\pi\phi} |1\rangle \otimes |u\rangle \tag{6.11}$$

$|6\rangle = |0110\rangle$:

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 vez la fase del autovalor $e^{i2\pi\phi}$.

$$CU^j \left|0110\right\rangle \otimes \left|u\right\rangle = e^{i6\times 2\pi\phi} \left|6\right\rangle \otimes \left|u\right\rangle \tag{6.12}$$

Como se puede ver, $CU^j \left|n\right\rangle \otimes \left|u\right\rangle = e^{in2\pi\phi} \left|n\right\rangle \otimes \left|u\right\rangle$. Por lo tanto, como las compuertas cuánticas son operadores lineales, sabemos que

$$CU^j \left|s\right\rangle \otimes \left|u\right\rangle = CU^j \frac{1}{\sqrt{2^K}} \sum_k \left|k\right\rangle \otimes \left|u\right\rangle = \frac{1}{\sqrt{2^K}} \sum_k e^{ik2\pi\phi} \left|k\right\rangle \otimes \left|u\right\rangle \tag{6.13}$$

Ahora, se aplica la QFT inversa al primer registro.

$$QFT^\dagger = \frac{1}{\sqrt{2^K}} \sum_x \sum_k e^{-i2\pi kx/2^K} \left|x\right\rangle\!\left\langle k\right| \tag{6.14}$$

$$\begin{aligned} QFT^\dagger \tfrac{1}{\sqrt{2^K}} \sum_k e^{ik2\pi\phi} \left|k\right\rangle \otimes \left|u\right\rangle &= \tfrac{1}{2^K} \sum_x \sum_k e^{ik2\pi\phi} e^{-i2\pi kx/2^K} \left|x\right\rangle \otimes \left|u\right\rangle \\ &= \tfrac{1}{2^K} \sum_x \sum_k \left(e^{i2\pi(\phi - \frac{x}{2^K})}\right)^k \left|x\right\rangle \otimes \left|\phi\right\rangle \\ &= \tfrac{1}{2^K} \sum_x \tfrac{1-e^{i2\pi(\phi-\frac{x}{2^K})2^K}}{1-e^{i2\pi(\phi-\frac{x}{2^K})}} \left|x\right\rangle \otimes \left|\phi\right\rangle \end{aligned} \tag{6.15}$$

La probabilidad de medir x a la salida del registro será:

$$p(x) = \left|(\left\langle x\right| \otimes \left\langle u\right|) \left|\psi_{output}\right\rangle\right|^2 = \frac{1}{4^K} \left| \frac{1 - e^{i2\pi(\phi - \frac{x}{2^K})2^K}}{1 - e^{i2\pi(\phi - \frac{x}{2^K})}} \right|^2 = \frac{1}{4^K} \frac{\sin^2(\pi(\phi - \frac{x}{2^K})2^K)}{\sin^2(\pi(\phi - \frac{x}{2^K}))} \tag{6.16}$$

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 $a \equiv b \mod m$, 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:

$$23 \equiv 2 \mod 7 \rightarrow 23 = 3 \times 7 + 2$$
$$-6 \equiv 1 \mod 7 \rightarrow -6 = -1 \times 7 + 1$$

Además si $m \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$ tales que:

$$a + c \equiv b + d \mod m$$
$$ac \equiv bd \mod m$$

Por definición el orden de $x \mod N$ es el menor entero r distinto de cero que satisface $x^r = 1 \mod N$

Ejemplo:

Sea $x = 4$ y $N = 13$ entonces $4^p = 13q + R$ obteniendo $4^p \mod 13 = R$

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 $4^r = 1 \mod 13$ con r=6

$$\therefore 4^6 = 1 \mod 13$$

Analicemos como la estimación de fase hace posible determinar r, el orden de $x \mod N$, 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 M, es decir mcd(x,M)=1, existe un operador $U_{x,N}$ tal que:

$$U_{x,N} |y\rangle = |xy \mod N\rangle \tag{6.17}$$

Sea $\{|u_s\rangle\}_{s=0,1,\ldots,r-1}$ el conjunto de r autoestados de U, asociados con los autovalores $e^{i2\pi s/r}$ tal que $U |u_s\rangle = e^{2i\pi s/r} |u_s\rangle$ 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: $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi ks}{r}} \left|x^k \mod N\right\rangle$, siendo r a determinar.

Con las siguientes propiedades:

1. $\frac{1}{\sqrt{r}} \sum_{s=0} r - 1 \, |u_s\rangle = |1\rangle$
2. $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} \, |u_s\rangle = \left|x^k \mod N\right\rangle$
3. $p(s) = |c_s|^2 = \frac{1}{r}$

Entonces:

$$CU^j \, |j\rangle \otimes |1\rangle = |j\rangle \otimes \left|x^j \mod N\right\rangle \tag{6.18}$$

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. $|\psi_2\rangle = \frac{1}{\sqrt{M}}(|0\rangle + |1\rangle)^{\otimes k} \otimes |1\rangle \, ; M = 2^k$

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} CU^j(|j\rangle \otimes |1\rangle) \tag{6.19}$$

3. $|\psi_3\rangle = CU^j \, |\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} CU^j(|j\rangle \otimes |1\rangle) = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (|j\rangle \otimes |x^j \mod N\rangle)$

   Pero ya vimos que: $|x^j \mod N\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} \, |u_s\rangle$, por lo tanto:

$$|\psi_3\rangle = \sum_{s=0}^{r-1} \sum_{k=0}^{M-1} \frac{1}{\sqrt{M}} e^{2i\pi ks/r} \, |k\rangle \otimes \frac{1}{\sqrt{r}} \, |u_s\rangle \tag{6.20}$$

4. Aplicamos la QFT inversa al primer registro, y nos queda:

$$|\psi_4\rangle = (QFT^\dagger \otimes \mathbb{1}) \, |\psi_3\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\tilde{\psi_s}\right\rangle \otimes |u_s\rangle \tag{6.21}$$

Finalmente, al medir el primer registro, proyectamos la superposición que conforma $|\psi_4\rangle$ en uno de los r estados de $|\psi_s\rangle$

$$p(s) = |(\left\langle \tilde{\psi}_s \right| \otimes \langle u_s|)\,|\psi_4\rangle\,|^2 = \frac{1}{r} \tag{6.22}$$

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 contínuas

Definamos un número real

$$\chi_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{2 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots a_n}}}}} \tag{6.23}$$

Con $n \leq N$. Cada número real en el conjunto $\{x_0, x_1, ..., x_{N-1}, x_N\}$ se denomina un convergente de x_n, mientras que x_n se denomina el n-ésimo convergente de x_N.

El conjunto finito $\{a_0, a_1, a_2, ..., a_n\}$ de números reales positivos corresponde a la cociente $x_n = \frac{p_n}{q_n}$, donde los p_n y q_n son:

$$p_n = a_n p_{n-1} + p_{n-2} \tag{6.24}$$

$$q_n = a_n q_{n-1} + q_{n-2} \tag{6.25}$$

Con $n \geq 2$ y

$$p_0 = a_0, q_0 = 1, p_1 = 1 + a_0 a_1 y q_1 = a_1 \tag{6.26}$$

Para n = 0, 1.

Los números reales p_n, q_n son coprimos y satisfacen la relación:

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n \tag{6.27}$$

Dado un número racional x, si dos enteros p, q son tales que:

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2} \tag{6.28}$$

Entonces p/q es un convergente de x.

Asumamos como ejemplo:

$$\phi = \frac{711}{413} = 1{,}72154963680387 \tag{6.29}$$

Entonces:

$$\phi = \frac{711}{413} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \frac{1}{5}}}}}}} \tag{6.30}$$

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 es N es par, el número 2 es un 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 $f(x) = a^x mod N$.
7. Si r es impar, volver al paso 3.
8. Si $a^r \not\equiv 1 \mod N$, ir al paso 3.
9. Si $a^{r/2} \equiv -1 \mod N$, 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.

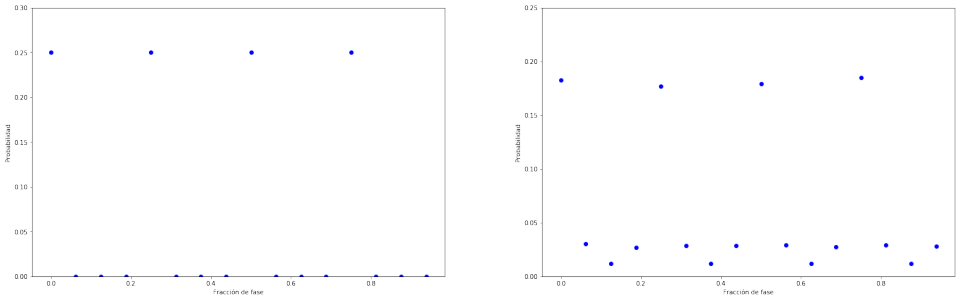
6.6. Simulaciones

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.



(A) Wolfram Mathematica (B) Python

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:

$$\tilde{\varphi} = 0 + \frac{1}{4} \tag{6.31}$$

   De donde recuperamos el número racional $1/4$, de donde el orden estimado es $r = 4$. Como r es par, $7^4 \mod 15 \equiv 1$ y $7^{4/2} \mod 15 \equiv 4 \mod 15 \not\equiv -1 \mod 15$, podemos continuar y hallar la siguiente factorización:

$$15 = GCD(7^{4/2}+1, 15) \times GCD(7^{4/2}-1, 15) = GCD(50, 15) \times GCD(48, 15) = 5 \times 3 \tag{6.32}$$

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:

$$\tilde{\varphi} = 0 + \frac{1}{2} \tag{6.33}$$

   De donde recuperamos el número racional $1/2$, de donde el orden estimado es $r = 2$. El orden r es par y $7^{2/2} \mod 15 \equiv 7 \mod 15 \not\equiv -1 \mod 15$, pero $7^2 \mod 15 \equiv 4 \mod 15 \not\equiv 1 \mod 15$, 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:

$$\tilde{\varphi} = 0 + \cfrac{1}{1 + \cfrac{1}{3}} \tag{6.34}$$

   De donde recuperamos el número racional $3/4$, de donde el orden estimado es $r = 4$. Entonces, este caso es similiar 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, $x^r \mod N \equiv 1$ y $x^{r/2} \mod N \not\equiv -1$, pero sólo se obtienen los factores triviales 1 y 15.

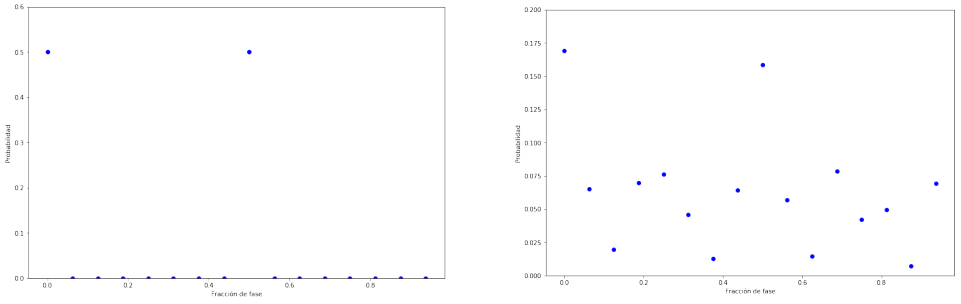
   En la simulación matemática estos casos no ocurren, pero en la simulación circuital ocurren con 0.276276 de probabilidad.

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.



(A) Wolfram Mathematica (B) Python

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:

   $$\tilde{\varphi} = 0 + \frac{1}{2} \tag{6.35}$$

   De donde recuperamos el número racional $1/2$, de donde el orden estimado es $r = 2$. Como r es par, $3^2 \mod 8 \equiv 1$ y $3^{3/2} \mod 8 \equiv 3 \mod 8 \not\equiv -1 \mod 8$, 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, $x^r \mod N \equiv 1$ y $x^{r/2} \mod N \not\equiv -1$, 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.

Apéndices

Bibliografía

[1] 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

[2] J. A. Jones and D. Jaksch, "Quantum information, computation and communication," 2009. [Online]. Available: http://dx.doi.org/10.1017/CBO9781139028509

[3] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," 2009. [Online]. Available: http://dx.doi.org/10.1017/CBO9780511976667

[4] M. Nakahara, *Quantum computing : from linear algebra to physical realizations*. Boca Raton: CRC Press, 2008.

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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

[25] N. Johansson and J. Åke Larsson, "Realization of shor's algorithm at room temperature," 2017.

[26] 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

[27] 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

[28] 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

[29] 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

[30] 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

[31] 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

[32] 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

[33] 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

[34] "Quantum manifesto." [Online]. Available: https://msu.euramet.org/current_calls/fundamental_2017/documents/Quantum_Manifesto.pdf

[35] 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

[36] 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

[37] F. Yan, A. M. Iliyasu, 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

[38] 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

[39] 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

[40] 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

[41] 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

[42] A. Galindo and P. Pascual, "Quantum mechanics i," 1990. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-83854-5

[43] R. Gross and A. Marx, "Applied superconductivity: Josephson effect and superconducting electronics," *Walther-MeiSSner-Institut*, 2005.

[44] 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

[45] A. P. Drozdov, M. I. Eremets, 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.

[46] M. Tinkham, *Introduction to superconductivity.* New York: McGraw Hill, 1996.

[47] 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

[48] H. Fröhlich, "Theory of the superconducting state," *Unknown*, 1950. [Online]. Available: None

[49] 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

[50] 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

[51] 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.

[52] 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

[53] 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

[54] 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

[55] 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

[56] 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

[57] 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

[58] 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/pra/abstract/10.1103/PhysRevA.75.032329

[59] 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/pra/abstract/10.1103/PhysRevA.67.032301

[60] 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/pra/abstract/10.1103/PhysRevA.52.3457

[61] 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

[62] 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

[63] ——, "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

[64] V. G. A. P, C. H. Bennett, and I. Thomas, "Optimization of grovers search algorithm."

[65] 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