

Diseño y simulación de un procesador cuántico superconductor

Miguel Casanova
Departamento de Electrónica y Circuitos¹, Universidad Simón Bolívar

2018
September

¹I am no longer a member of this department

Índice general

1. Introducción	2
2. Información cuántica	3
2.1. Función de onda	3
2.1.1. Espacio de Hilbert	5
2.2. Herramientas necesarias	6
2.2.1. Delta de Kronecker	6
2.2.2. Notación de Dirac	6
2.3. Operadores unitarios	8
2.4. Producto tensorial	8
2.4.1. Propiedades	8
2.4.2. Nota sobre la notación	8
2.5. Postulados de la mecánica cuántica	9
2.6. Matriz de densidad	9
2.6.1. Propiedades	10
2.7. Traza parcial	11
2.7.1. Comparación con el producto tensorial	12
2.8. Entrelazamiento	12
2.9. Computación cuántica	13
2.9.1. Qubits	13
2.9.2. Esfera de Bloch	13
2.9.3. Conmutador y anticonmutador	14
2.9.4. Matrices de Pauli	14
2.9.5. Compuertas cuánticas	15
2.9.6. Conjuntos universales de compuertas cuánticas	19
2.9.7. Compuertas no cliffordianas	20
2.9.8. Circuitos cuánticos	20
2.9.9. Algoritmos cuánticos	20
2.9.10. Criterios de DiVincenzo	20

2.10. Fidelidad	20
2.11. Medidas	20
3. Superconductividad	21
3.1. Cuantización macroscópica y superconductividad	21
3.2. La teoría BCS	23
3.3. Cuantización del flujo magnético y efecto Josephson	33
3.3.1. Efecto Josephson	37
3.4. Efecto Josephson	41
3.4.1. Efecto Josephson DC	42
3.4.2. Efecto Josephson AC	42
3.5. Componentes de la corriente en las uniones de Josephson	43
3.6. Qubits superconductores	43
3.7. Arquétipos de qubits superconductores	45
3.7.1. Qubit de carga	45
3.7.2. Qubit de flujo	45
3.7.3. Qubit de fase	45
3.8. Transmones	46
3.9. Hamiltonianos multiqubit de transmones	46
3.9.1. Acoplamiento capacitivo	47
3.9.2. Acoplamiento por el resonador	47
3.9.3. Acoplamiento de JJ	47
3.9.4. Acoplamiento afinable/calibrable	47
3.10. Puertas cuánticas en transmones	47
3.10.1. El operador de evolución temporal	47
3.10.2. Pulsos de microondas	48
3.10.3. Régimen rotacional del pulso	48
3.10.4. Efecto del pulso sobre el qubit	49
3.10.5. Régimen dispersivo	49
3.10.6. Rotaciones X-Y	50
3.10.7. Puerta de entrelazamiento	50
3.10.8. Puertas compuestas	50
4. El simulador	51
4.1. Parámetros de los sistemas simulados	52
5. Algoritmo de Grover	53
5.1. El algoritmo	58
5.2. Limitaciones y aplicaciones	59
5.3. Simulación	59

6. Algoritmo de Shor	61
6.1. Estimación de orden	61
6.2. Transformadas integrales	70
6.3. Transformada cuántica de Fourier	70
6.4. Estimación de fase	70
6.5. Estimación de orden	70
6.6. Algoritmo de Shor	70
7. Google PageRank	72
7.0.1. El algoritmo de remiendo (parcheo) general	75
7.0.2. Interpretación como una caminata aleatoria	76
7.0.3. Cuantizando las caminatas aleatorias	77
7.0.4. Caminata cuántica de Szegedy	78
7.0.5. PageRank cuántico	79
A. Cálculos de Hamiltonianos	80
A.1. Hamiltoniano de Jaynes-Cummings	80
A.2. Hamiltoniano multiqubit	80
A.3. Pulsos de microondas	80
A.4. Régimen rotacional del pulso	81
A.5. Efecto del pulso sobre el qubit	83
A.6. Régimen dispersivo	83
A.7. Rotaciones X-Y	85
A.8. Compuerta de entrelazamiento	86
B. Cálculos de matrices de adyacencia	87
C. Circuitos cuánticos	88

Índice de figuras

5.1.	Circuito del algoritmo de Grover, k_{max} desconocido.	56
5.2.	Interpretación geométrica del operador difusión	58
5.3.	Circuito del algoritmo de Grover.	58
5.4.	59
5.5.	59
5.6.	59
5.7.	60
7.1.	Grafo correspondiente a la matriz de adyacencia (a) de la red	
	E (b) remendada de Google G con $\alpha = \frac{1}{2}$	76

Índice de cuadros

Capítulo 6

Algoritmo de Shor

El algoritmo de Shor es un AC 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. 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 y el protocolo Diffie-Hellman de intercambio de llaves, sobre los cuáles se basa virtualmente toda la criptografía actual.

6.1. 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:

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

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

Ejemplo:

Sea $x = 4, N = 13 \rightarrow 4^p = 13q + R \quad 4^p \pmod{13} = R$

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 $r=6$

$\therefore 4^6 = 1 \pmod{13}$

* Expansión en fracciones continuas: (Emmanuel Desurvire -¿ Apéndice R)

Definamos un número real $\chi_n = a_0 \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}}$ 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 .

Propiedad 1:

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

$p_n = a_n p_{n-1} + p_{n-2}$ $q_n = a_n q_{n-1} + q_{n-2}$
con $n \geq 2, p_0 = a_0, q_0 = 1, p_1 = 1 + a_0 a_1 q_1 = a_1$, para $n = 0, 1$.

Propiedad 2:

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

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

Propiedad 3:

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

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

Entonces p/q es un convergente de x .

Asumamos como ejemplo:

$$\phi = 711/413 = 1,72154963680387$$

Entonces:

$$\phi = 711/413 = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4 + \frac{1}{5}}}}}}}$$

Supongamos que solo queremos 6 decimales de precisión, es decir sea $\tilde{\phi} = 1,721549$, tal que:

$$|\epsilon| = |\phi - \tilde{\phi}| = 3,69910^{-7}$$

Si expandimos $\tilde{\phi}$ al igual que ϕ , encontramos que con sólo 7 a_n encontramos $\tilde{\phi}$ (ver tabla R1).

Por otro lado, $\frac{p_7}{q_7} \implies \frac{711}{413}$ da la definición de ϕ .

* Algoritmo de factorización de Shor

El algoritmo de factorización de Shor permite factorizar números los cuales se pueden descomponer en un producto único de números primos.

Dicho número N es un entero no-primos de L bits.

En un ordenador cuántico el algoritmo de Shor tendrá un tiempo de corrida del orden $O((L^3))$ (polinómico) y en un ordenador clásico es del $O(e^{[L^{1/3}(\log L)^{2/3}]})$ (exponencial), mostrando así que el algoritmo de Shor es capaz de factorizar números muy grandes en tiempos polinómicos.

En dicho algoritmo se conjugan:

1. Aritmética modular ;- Clásico 2. Paralelismo cuántico ;- Cuántico 3. Transformada cuántica de Fourier ;- Cuántico

El algoritmo consiste en dos etapas:

1) Una reducción del problema de descomponer en factores al problema de encontrar el orden

2) Un algoritmo cuántico para solucionar el problema de encontrar el período.

El algoritmo de Shor fue publicado en: P.W. Shor SIAM I. Comput. 26, 1484-1509 (1997)

Siguiendo el esquema de Emmanuel Desuivre "Classical and Quantum Information Theory: An Introduction for the Telecom Scientist".

La parte cuántica del algoritmo de Shor la podemos dividir en 2 partes:

1) El algoritmo de estimación de fase 2) El algoritmo de determinación de orden

Entonces:

* 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 *controlled* - U^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:

Recordemos que:

Analicemos la compuerta $CU^p \equiv \text{controlled} - U^p \text{ gate}$:

$U|u\rangle = e^{2i\pi\phi} U^p|u\rangle = e^{2i\pi p\phi} H|0\rangle = |0\rangle + |1\rangle$ (Sin $1/\sqrt{2}$ por los momentos)

$$CU^p((|0\rangle + |1\rangle) \otimes |u\rangle) = |0\rangle \otimes |u\rangle + |1\rangle \otimes U^p|u\rangle = |0\rangle \otimes |u\rangle + |1\rangle e^{2i\pi p\phi} |u\rangle = (|0\rangle + e^{2i\pi p\phi} |1\rangle) \otimes |u\rangle$$

$$\therefore CU^p((|0\rangle + |1\rangle) \otimes |u\rangle) = (|0\rangle + e^{2i\pi p\phi} |1\rangle) \otimes |u\rangle$$

Analicemos ahora el producto tensorial a la salida de dos compuertas CU^p recordemos que $p = \{2^0, 2^1, \dots, 2^{k-1}\}$, entonces:

$$(|0\rangle + e^{2i\pi 2^1\phi} |1\rangle) \otimes (|0\rangle + e^{2i\pi 2^0\phi} |1\rangle) = |0\rangle|0\rangle + e^{2i\pi 2^0\phi} |0\rangle|1\rangle + e^{2i\pi 2^1\phi} |1\rangle|0\rangle + e^{2i\pi(2^1+2^0)\phi} |1\rangle|1\rangle = e^{2i\pi 0\phi} |0\rangle + e^{2i\pi 1\phi} |1\rangle + e^{2i\pi 2\phi} |2\rangle + e^{2i\pi 3\phi} |3\rangle$$

donde $|00\rangle \equiv |0\rangle; |01\rangle \equiv |1\rangle; |10\rangle \equiv |2\rangle; |11\rangle \equiv |3\rangle;$

es decir: $|ij\rangle \equiv |i2^0 + j2^1\rangle$ con $i, j = 0, 1$ si generalizamos: $|ijk\dots n\rangle = |i2^0 + j2^1 + k2^2 + \dots + n2^{n-1}\rangle$

$$\therefore (|0\rangle + e^{2i\pi 2^1\phi}) \otimes (|0\rangle + e^{2i\pi 2^0\phi} |1\rangle) = \sum_{k=0}^3 e^{2i\pi k\phi} |k\rangle$$

Todo número puede ser representado en forma binaria:

$$0 \leq \phi \leq 1 \implies \phi \equiv 0\phi_1\phi_2\phi_3\dots \implies \phi = \frac{\phi_1}{2} + \frac{\phi_2}{4} + \frac{\phi_3}{8} + \dots + \frac{\phi_k}{2^k} + \dots$$

para bits $\phi_i = 0, 1 \rightarrow \phi_1 = 0, \phi_2 = 1$

$$\text{luego: } 2^{k-1}\phi = 2^{k-1}(\frac{\phi_1}{2} + \frac{\phi_2}{4} + \frac{\phi_3}{8} + \dots + \frac{\phi_k}{2^k} + \dots) = \{\phi_1 2^{k-2} + \phi_2 2^{k-3} + \dots + \phi_{k-1} 2^0\} + \frac{\phi_k}{2} + \frac{\phi_{k+1}}{4} + \dots$$

$$\therefore 2^{k-2}\phi = 2^{k-2}(\frac{\phi_1}{2} + \frac{\phi_2}{4} + \frac{\phi_3}{8} + \dots + \frac{\phi_k}{2^k} + \dots) = \{\phi_1 2^{k-3} + \phi_2 2^{k-4} + \dots + \phi_{k-2} 2^0\} + \frac{\phi_{k-1}}{2} + \frac{\phi_k}{4} + \frac{\phi_{k+1}}{8} + \dots$$

Los términos dentro de los $\{ \}$ son enteros. Definamos entonces:

$$\Omega_m = \sum_{l=1}^m \frac{\phi_{k-m+l}}{2^l}$$

tal que:

$$e^{2i\pi 2^{k-1}\phi} = e^{2i\phi\Omega_1} e^{2i\pi(\frac{\phi_{k+1}}{4} + \dots)} e^{2i\pi 2^{k-2}\phi} = e^{2i\phi\Omega_2} e^{2i\pi(\frac{\phi_{k+1}}{8} + \dots)} \dots e^{2i\pi 2^0\phi} = e^{2i\phi\Omega_k} e^{2i\pi(\frac{\phi_{k+1}}{2^{k+1}} + \dots)}$$

Consideremos el caso en el cual ϕ es definido exactamente por k bits tal que $\phi_{k+1} = \phi_{k+2} = \dots = 0$

Dejando de lado el qubit $|u\rangle$ la salida del primer registro es:

$$\frac{1}{2^{k/2}} (|0\rangle + e^{2i\pi\Omega_1} |1\rangle) \otimes (|0\rangle + e^{2i\pi\Omega_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2i\pi\Omega_k} |1\rangle)$$

Como podemos recordar

$$QFT|n\rangle = \frac{1}{2^{k/2}} (|0\rangle_1 + e^{2i\pi\Omega_1} |1\rangle_1) \otimes (|0\rangle_2 + e^{2i\pi\Omega_2} |1\rangle_2) \otimes \dots \otimes (|0\rangle_k + e^{2i\pi\Omega_k} |1\rangle_k)$$

$$\text{Siendo: } 1 \leq m \leq k \rightarrow |m\rangle = \frac{1}{2^{m/2}} (|0\rangle_m + e^{2i\pi\Omega_m} |1\rangle_m)$$

$$\text{con } \Omega_m = \sum_{l=1}^m \frac{n_{k-m+l}}{2}$$

$$\text{Encontrando así que } \frac{1}{2^{k/2}} (|0\rangle + e^{2i\pi\Omega_1} |1\rangle) \otimes (|0\rangle + e^{2i\pi\Omega_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2i\pi\Omega_k} |1\rangle)$$

Es la transformada cuántica de Fourier de nuestro estado $|\phi\rangle$ obtenida con las compuertas *Controlled* - U^p .

Al ket $|\phi\rangle$ lo podemos recuperar haciendo la transformada inversa de Fourier.

Consideremos ahora el módulo del circuito cuántico "back-end"

El módulo back-end del circuito cuántico de Shor consiste en realizar la transformada cuántica inversa de Fourier y hacer medidas sobre los k qubits encontrando así los $\phi_1, \phi_2, \dots, \phi_k$.

Seguidamente consideremos ahora el caso más general en el cual $2^k\phi$ no es un entero.

$$\text{Fron-end } |0\rangle^{\otimes k} \otimes |u\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} |k\rangle \otimes |u\rangle$$

$$\text{Back-end } QFT_1^\dagger \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} |k\rangle \otimes |u\rangle \right) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} QFT^\dagger |k\rangle \otimes |u\rangle =$$

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} \left(\frac{1}{2^{k/2}} \sum_{n=0}^{N-1} e^{-\frac{2i\pi kn}{N}} |n\rangle \right) \otimes |u\rangle = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{n=0}^{N-1} e^{-2i\pi \frac{kn}{N}} e^{2i\pi k\phi} |n\rangle \otimes |u\rangle = \frac{1}{N} \sum_{n=0}^{N-1} \left(\sum_{k=0}^{N-1} (e^{2i\pi(\phi - \frac{n}{N})})^k \right) |n\rangle \otimes |u\rangle$$

$$\therefore (QFT^\dagger \otimes \mathbb{1}) \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2i\pi k\phi} |k\rangle \otimes |u\rangle \right) = \frac{1}{N} \sum_{n=0}^{N-1} \left(\frac{1 - e^{2i\pi(\phi - \frac{n}{N})N}}{1 - e^{2i\pi(\phi - \frac{n}{N})}} \right) |n\rangle \otimes |u\rangle$$

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

$$p(n) = |\langle u | \otimes \langle n | \psi_{\text{output}} \rangle|^2$$

$$p(n) = \frac{1}{N^2} \left| \frac{1 - e^{2i\pi(\phi - \frac{n}{N})N}}{1 - e^{2i\pi(\phi - \frac{n}{N})}} \right|^2$$

$$\therefore p(n) = \frac{1}{N^2} \frac{\sin^2(\pi(\phi - \frac{n}{N})N)}{\sin^2(\pi(\phi - \frac{n}{N}))}$$

La medida de n con probabilidad asociada $p(n)$, corresponde a la estimación de fase $\tilde{\phi} = n/N$. La probabilidad es máxima cuando $\delta = \phi - \tilde{\phi}$ es mínima.

$$p(n) = \frac{1}{N^2} \frac{\sin^2(\pi(\phi - \frac{n}{N})N)}{\sin^2(\pi(\phi - \frac{n}{N}))} \text{ si } N \text{ es grande} \rightarrow$$

La probabilidad $p(n)$ decae rápidamente a cero cuando el error δ se aleja del mínimo.

Entonces:

.) La medida tiene la mayor probabilidad de dar la aproximación más cercana al estado ϕ . .) El circuito de salida es de la forma $|\tilde{\phi}\rangle |u\rangle$, donde $|\tilde{\phi}\rangle$ es una superposición de estados, los cuales al medirlos dan una buena aproximación de ϕ .

* Estimación de orden:

Analicemos como la estimación de fase hace posible determinar r , el orden de x mód 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 $x \nmid N$, siendo x coprimo de N , es decir $\text{mcd}(x, N) = 1$, existe un operador $U_{x, N}$ que actúa sobre el qubit $|y\rangle \equiv \{|0\rangle, |1\rangle\}$, tal que:

$$U_{x, N} |y\rangle = |xy \text{ mód } N\rangle$$

Asumamos $\{|u_s\rangle\}_{s=0,1,\dots,r-1}$ 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 $0 \leq \phi_s \leq 1$

$$\text{Tales autoestados } |u_s\rangle \text{ se definen acorde a: } |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi ks}{r}} |x^k \text{ mód } N\rangle,$$

siendo r a determinar.

Con las siguientes propiedades:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$$

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi ks}{r}} |u_s\rangle = |x^k \text{ mód } N\rangle$$

$$p(s) = |c_s|^2 = \frac{1}{r}$$

El circuito para la estimación de orden es el siguiente:

Entonces:

$$U_{x, y} |y\rangle = |xy \text{ mód } N\rangle$$

$$j = 2^0, 2^1, 2^2, \dots, 2^{k-1}$$

$$\begin{aligned}
CU^j(|0\rangle \otimes |1\rangle) &= |0\rangle \otimes |1\rangle \\
CU^j|j\rangle \otimes |1\rangle &= |j\rangle \otimes \left| x^{j12^{k-1}} \text{ mód } N \right\rangle \left| x^{j22^{k-2}} \text{ mód } N \right\rangle \dots \left| x^{jk2^0} \text{ mód } N \right\rangle \\
CU^j|j\rangle \otimes |1\rangle &= |j\rangle \otimes \left| x^{j12^{k-1}} x^{j22^{k-2}} \dots x^{jk2^0} \text{ mód } N \right\rangle \\
\therefore CU^j|j\rangle \otimes |1\rangle &= |j\rangle \otimes \left| x^j \text{ mód } N \right\rangle
\end{aligned}$$

Con este paso entendido vamos ahora a analizar el circuito para determinar el orden:

$$\begin{aligned}
1) |\psi_1\rangle &= |0\rangle^{\otimes k} \otimes |1\rangle \\
2) |psi_2\rangle &= \frac{1}{\sqrt{M}}(|0\rangle + |1\rangle)^{\otimes k} \otimes |1\rangle; M = 2^k \\
|psi_2\rangle &= \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} CU^j(|j\rangle \otimes |1\rangle) \\
3) |\psi_3\rangle &= CU^j |\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} CU^j(|j\rangle \otimes |1\rangle) = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (|j\rangle \otimes |x^j \text{ mód } N\rangle)
\end{aligned}$$

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

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

$$|\psi_3\rangle = \sum_{s=0}^{r-1} \left(\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{2i\pi ks/r} |k\rangle \right) \otimes \frac{1}{\sqrt{r}} |u_s\rangle$$

$$\begin{aligned}
4) \text{ Aplicamos la transformada inversa de Fourier al primer registro } |\psi_4\rangle &= \\
(QFT^\dagger \otimes \mathbb{1}) |\psi_3\rangle &= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left| \tilde{\psi}_s \right\rangle \otimes |u_s\rangle
\end{aligned}$$

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

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

lo que nos da $\frac{s}{r}$ correspondiendo a la estimación de fase $\tilde{\psi} = \frac{s}{r}$

Posteriormente aplicamos el algoritmo clásico de fracciones continuas y determinamos los co-primos.

Ejemplo:

Determinemos la factorización para $N=15$.

Asumamos, el número compuesto $N=15$ (no primo). Tomemos $L = \log_2 N = 9$ para el segundo registro (tamaño del target) y pongamos un error de probabilidad grande $\epsilon = 0,25$.

$k = 2L + 1 + \log_2(2 + \frac{1}{2\epsilon}) = 11$ (ver libro: tamaño del primer registro de control)

$$M = 2^k = 2^{11} = 2048$$

tomemos un número x aleatorio entre $[2, N-1] \rightarrow x = 8$ lo cual cumple que $\text{m.c.d}(8,15) = 1$

Pasos cuánticos:

.) $|\psi_1\rangle = |0\rangle^{\otimes k} \otimes |1\rangle$

.) $|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (|j\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2M}} (|0\rangle + |1\rangle + |2\rangle + \dots + |M-1\rangle)$

.) Aplicamos la compuerta *Controlled-U*^j $|\psi_3\rangle = \frac{1}{\sqrt{M}} |j\rangle \otimes |x^j \text{ mód } N\rangle =$

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |1\rangle \otimes |8^j \text{ mód } 15\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} (|0\rangle |1\rangle + |1\rangle |8\rangle + |2\rangle |4\rangle + |3\rangle |2\rangle + |4\rangle |1\rangle + |5\rangle |8\rangle + |6\rangle |4\rangle + |7\rangle |2\rangle + |8\rangle |1\rangle + |9\rangle |8\rangle + |0\rangle |4\rangle + |1\rangle |2\rangle + \dots)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} ((|0\rangle + |4\rangle + |8\rangle + \dots) |1\rangle + (|1\rangle + |5\rangle + |9\rangle + \dots) |8\rangle + (|2\rangle + |6\rangle + |10\rangle + \dots) |4\rangle + (|3\rangle + |7\rangle + |11\rangle + \dots) |2\rangle)$$

Definamos: $|u_1\rangle = \frac{1}{\sqrt{M}} (|0\rangle + |4\rangle + |8\rangle + \dots)$

$$|u_2\rangle = \frac{1}{\sqrt{M}} (|1\rangle + |5\rangle + |9\rangle + \dots)$$

$$|u_3\rangle = \frac{1}{\sqrt{M}} (|2\rangle + |6\rangle + |10\rangle + \dots)$$

$$|u_4\rangle = \frac{1}{\sqrt{M}} (|3\rangle + |7\rangle + |11\rangle + \dots)$$

y obtenemos: $|\psi_3\rangle = |u_1\rangle \otimes |1\rangle + |u_2\rangle \otimes |8\rangle + |u_3\rangle \otimes |4\rangle + |u_4\rangle \otimes |2\rangle$

Consideremos el primer registro $|u_2\rangle \otimes |8\rangle$, es decir $|u_2\rangle$, y apliquemos la QFT^\dagger sobre él.

$$QFT^\dagger |u_2\rangle = \frac{1}{\sqrt{M}} QFT^\dagger (|1\rangle + |5\rangle + |9\rangle + |13\rangle + \dots)$$

Recordemos que $QFT^\dagger |n\rangle = \frac{1}{\sqrt{4M}} \sum_{k=0}^{M-1} e^{-2i\pi kn/M} |k\rangle$

Luego: $QFT^\dagger |u_2\rangle = \frac{1}{\sqrt{M}} QFT^\dagger (|1\rangle + |5\rangle + |9\rangle + |13\rangle + \dots)$

$$QFT^\dagger |u_2\rangle = \frac{1}{2M} \sum_{k=0}^{M-1} (e^{-\frac{k2i\pi}{M}1} |k\rangle + e^{-\frac{k2i\pi}{M}5} |k\rangle + e^{-\frac{k2i\pi}{M}9} |k\rangle + e^{-\frac{k2i\pi}{M}13} |k\rangle + \dots)$$

$$QFT^\dagger |u_2\rangle = \frac{1}{2M} \sum_{k=0}^{M-1} (e^{-\frac{k2i\pi}{M}1} + e^{-\frac{k2i\pi}{M}5} + e^{-\frac{k2i\pi}{M}9} + e^{-\frac{k2i\pi}{M}13} + \dots) |k\rangle$$

$$QFT^\dagger |u_2\rangle = \frac{1}{2M} \sum_{k=0}^{M-1} e^{-\frac{k2i\pi}{M}1} ((e^{-\frac{k8i\pi}{M}})^0 + (e^{-\frac{k8i\pi}{M}})^1 + (e^{-\frac{k8i\pi}{M}})^2 + \dots) |k\rangle$$

$$QFT^\dagger |u_2\rangle = \frac{1}{2M} \sum_{k=0}^{M-1} e^{-k\frac{2i\pi}{M}} \sum_{m=0}^{M-1} (e^{-k\frac{8i\pi}{M}})^m |m\rangle$$

$$QFT^\dagger \sum_{k=0}^{M-1} e^{-k\frac{2i\pi}{M}} \frac{(1-e^{-8i\pi k})}{(1-e^{-k\frac{8i\pi}{M}})} |k\rangle$$

$$QFT^\dagger |u_2\rangle = \frac{1}{2M} \sum_{k=0}^{M-1} e^{-k\frac{2\pi i}{M}} \frac{(1-e^{-8i\pi k})}{e^{-k\frac{4i\pi}{M}} (e^{k\frac{4i\pi}{M}} - e^{-k\frac{4i\pi}{M}})} |k\rangle$$

$$QFT^\dagger |u_2\rangle = \frac{1}{4iM} \sum_{k=0}^{M-1} e^{k\frac{2\pi i}{M}} \frac{(1-e^{-8i\pi k})}{\sin(\frac{4\pi k}{M})} |k\rangle$$

$$QFT^\dagger |u_2\rangle = \frac{1}{4iM} \sum_{k=0}^{M-1} e^{k\frac{2\pi i}{M}} \frac{e^{-4i\pi k} (e^{4i\pi k} - e^{-4i\pi k})}{\sin(\frac{4\pi k}{M})} |k\rangle$$

$$QFT^\dagger |u_2\rangle = \frac{1}{2M} \sum_{k=0}^{M-1} e^{-k \frac{2\pi i}{M} (2M-1)} \frac{\sin(4\pi k)}{\sin(\frac{4\pi k}{M})} |k\rangle$$

Este resultado se puede reescribir de la forma:

$$QFT^\dagger |u_2\rangle = \sum_{k=0}^{M-1} \alpha_k |k\rangle$$

$$\text{siendo } \alpha_k = \frac{1}{2M} e^{-k \frac{2i\pi}{M} (2M-1)} \frac{\sin(4\pi k)}{\sin(k \frac{4\pi}{M})}$$

$$\text{correspondiendo } p(k) = |\langle k | QFT^\dagger |u_2\rangle|^2 = |\alpha_k|^2 = \frac{1}{4M^2} \frac{\sin^2(4\pi k)}{\sin^2(\frac{4\pi k}{M})}$$

Como podemos observar para todo entero $k=0,1,\dots,M-1$ el número de α_k

es cero, pero para $\frac{4\pi k}{M} = n\pi \rightarrow k = n \frac{M}{4} = n 2^7 = n 512$, n entero

el denominador es cero y α_k es indeterminado, luego:

$$\lim_{\epsilon \rightarrow 0} \frac{\sin^2(4\pi k)}{\sin^2(\frac{4\pi k}{M})} = \lim_{\epsilon \rightarrow 0} \frac{\sin^2(4\pi(\frac{nM}{4} + \epsilon))}{\sin^2(\frac{4\pi}{M}(\frac{nM}{4} + \epsilon))} = \lim_{\epsilon \rightarrow 0} \frac{\sin^2(nM\pi + 4\pi\epsilon)}{\sin^2(n\pi + \frac{4\pi}{M}\epsilon)} = \lim_{\epsilon \rightarrow 0} \frac{\sin^2(4\pi\epsilon)}{\sin^2(\frac{4\pi}{M}\epsilon)} = \frac{(4\pi\epsilon)}{(\frac{4\pi}{M}\epsilon)^2} = M^2$$

$$\text{luego: } p(k)_{\text{Máximo}} = \frac{1}{4M^2} M^2 \rightarrow p_{\text{Maximo}}(k) = \frac{1}{4}$$

En el rango $k=0,1,\dots,M-1$ los máximos de $p(k)$ están localizados en:

$$k = 0 \rightarrow n = 0 \quad k = 512 \rightarrow n = 1 \quad k = 1024 \rightarrow n = 2 \quad k = 1536 \rightarrow n = 3$$

$$\text{Al medir obtenemos: } \frac{k_i}{M} = \frac{k_i}{2^k} = \frac{k_i}{2^{13}} = \frac{k_i}{2048}$$

las cuatro posibles determinaciones de $\tilde{\phi}$ son:

$$\frac{0}{2048} \Big|_{k_i=0}; \frac{512}{2048} \Big|_{k_i=512}; \frac{1024}{2048} \Big|_{k_i=1024}; \frac{1536}{2048} \Big|_{k_i=1536};$$

$$k_i = 0 \text{ no aporta nada } k_1 = \frac{512}{2048} = \frac{1}{4} \} \text{ no satisfacen } \left| \frac{s}{r} - x \right| \leq \frac{1}{r^2}$$

$$k_2 = \frac{1024}{2048} = \frac{1}{2} \} \text{ no satisfacen } \left| \frac{s}{r} - x \right| \leq \frac{1}{r^2} \quad k_3 = \frac{1536}{2048} = \frac{1}{1+\frac{1}{3}}$$

$$\text{ya que } \frac{p_0}{1_0} = \frac{0}{1}; \frac{p_1}{q_1} = \frac{1}{1}; \frac{p_2}{q_2} = \frac{3}{4}$$

3 y 4 son co-primos.

La fracción $3/4$ es un convergente de ϕ y $r = q_2 = 4$ es el orden de x

Normalmente se suele asociar con que existen 2 N' y N'' de $N=15$ tales

que

$$N' = MCD(x^{r/2} - 1, N) = MCD(63, 15) = 3 \quad N'' = MCD(x^{r/2} + 1, N) = MCD(65, 15) = 5$$

- 6.2. Transformadas integrales
- 6.3. Transformada cuántica de Fourier
- 6.4. Estimación de fase
- 6.5. Estimación de orden
- 6.6. Algoritmo de Shor

Bibliografía

- [1] Rudolf Gross and Achim Marx. Applied superconductivity: Josephson effect and superconducting electronics. *Walther-Meißner-Institut*, 2005.
- [2] 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*, 525:73–76, 2015.
- [3] G. Wendin. Quantum information processing with superconducting circuits: a review. *IOP Science*, 2017.
- [4] 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.
- [5] 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.