

# Diseño y simulación de un procesador cuántico superconductor

Miguel Casanova  
Departamento de Electrónica y Circuitos<sup>1</sup>, Universidad Simón Bolívar

2018  
December

<sup>1</sup>I am no longer a member of this department

## **Resumen**

Your abstract goes here... ...



# Capítulo 1

## Introducción

La computación cuántica es como chévere

## Capítulo 2

# Información cuántica

### 2.1. Kets, bras y operadores

La notación bra-ket es la notación estándar en la mecánica cuántica para describir estados cuánticos. En el caso de la computación cuántica, se utilizan los kets  $|0\rangle$  y  $|1\rangle$  para describir los qubits en la base computacional. Este par de estados sería el equivalente a los bits 0 y 1 en la computación clásica. En su representación matricial, los kets  $|0\rangle$  y  $|1\rangle$  se representan de la siguiente manera:

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

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

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

$$\langle 0| = (1 \quad 0)$$

$$\langle 1| = (0 \quad 1)$$

### 2.2. Postulados de la mecánica cuántica

1. Un estado puro en mecánica cuántica se representa en términos de un vector normalizado  $|\psi\rangle$  en un espacio de Hilbert  $\mathcal{H}$ .

2. Si  $\mathcal{H}_1$  y  $\mathcal{H}_2$  son los espacios de Hilbert asociados a dos sistemas físicos, entonces el espacio del sistema compuesto  $\mathcal{H}$  estará dado por el producto tensorial de los dos espacios de Hilbert  $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ .
3. Para todo observable  $a$ , existe un operador hermítico correspondiente  $A$  que actúa sobre el espacio de Hilbert  $\mathcal{H}$ , cuyos autovalores son los posibles resultados de una medida de este observable.
4. La evolución temporal del sistema sigue la ecuación de Schrödinger  $i\hbar \frac{\partial |\psi\rangle}{\partial t} = H |\psi\rangle$ . Donde  $\hbar$  es la constante de Planck reducida y  $H$  es el Hamiltoniano del sistema, el cuál es el operador hermítico correspondiente a la energía.
5. Después de realizar una medida del observable  $a$ , el estado  $|\psi\rangle$  del sistema colapsa a al autoestado de  $A$  correspondiente a la medida.

## 2.3. Computación cuántica

This section's content...

### 2.3.1. Qubits

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

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

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

### 2.3.2. Compuertas cuánticas

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

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

#### Compuerta identidad

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

$$\text{---}\boxed{I}\text{---} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

#### Compuerta X

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

$$\text{---}\boxed{X}\text{---} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

#### Compuerta Z

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

$$\text{---}\boxed{Z}\text{---} \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

#### Compuerta Y

Esta compuerta realiza una rotación de  $\pi$  sobre el eje y de la esfera de Bloch. Su forma matricial viene dada por la matriz de Pauli  $\sigma_y$

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

### Compuerta de Hadamard

Esta compuerta transforma los estados de la base computacional  $|0\rangle$  y  $|1\rangle$  en estados de superposiciones uniformes ( $|+\rangle$  y  $|-\rangle$ ). También se puede interpretar como el mapa de la base Z a la base X.

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

### Compuerta S

Esta compuerta es la raíz cuadrada de Z.

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

### Compuerta T

Esta compuerta es la raíz cuadrada de S.

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

### Compuerta de cambio de fase

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

### Compuertas de rotación

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

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

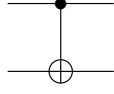
$$R_z(\theta) = \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix}$$

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

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



### Compuerta CNOT



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

### Compuerta SWAP



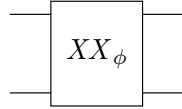
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

### Compuerta $\sqrt{\text{SWAP}}$



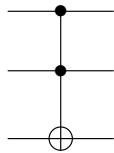
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

### Compuerta de Ising



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

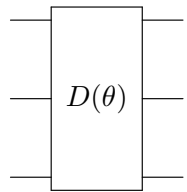
### Compuerta de Toffoli



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

### Compuerta de Fredkin

### Compuerta de Deutsch



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

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

### 2.3.3. Correspondencia entre compuertas clásicas y cuánticas

### 2.3.4. Conjuntos universales de compuertas cuánticas

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

Cualquier operador unitario puede ser escrito en función de compuertas de uno y dos qubits [Barenco et al. 1995].

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

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

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

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

### **2.3.5. Puertas no cliffordianas**

Las puertas clifford

### **2.3.6. Circuitos cuánticos**

### **2.3.7. Paralelismo cuántico**

### **2.3.8. Algoritmos cuánticos**

### **2.3.9. Criterios de DiVincenzo**

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

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

## Capítulo 3

# Superconductividad

Los qubits superconductores se basan en circuitos osciladores no lineales, hechos a partir de uniones de Josephson (Josephson Junctions - JJ). [Wendin]

El Hamiltoniano de un oscilador armónico LC está dado por

$$\hat{H} = E_C \hat{n}^2 + E_L \frac{\hat{\phi}^2}{2},$$

donde  $\hat{n}$  es la cantidad de pares de Cooper inducidos en el capacitor (En otras palabras, la carga inducida en el capacitor, medida en unidades de  $2e$ ), y  $\hat{\phi}$  es la diferencia de fase sobre el inductor. La carga  $\hat{n}$  y la fase  $\hat{\phi}$  no conmutan,  $[\hat{\phi}, \hat{n}] = i$ , lo que significa que sus valores esperados no se pueden medir simultaneamente.  $E_C = \frac{(2e)^2}{2C}$ ,  $E_L = \frac{\hbar^2}{(2e)^2 L}$  y la distancia entre niveles de energía del oscilador armónico  $\hbar\omega = \frac{\hbar}{\sqrt{LC}} = \sqrt{2E_L E_C}$ .

Para poder servir como qubit, el oscilador debe ser anarmónico, de manera que se pueda operar sobre un par específico de niveles de energía. Al agregar una JJ, el Hamiltoniano del circuito LCJ se convierte en:

$$\hat{H} = E_C (\hat{n} - n_g)^2 - E_{J0} \cos(\hat{\phi}) + E_L \frac{(\hat{\phi} - \phi_e)^2}{2},$$

donde  $n_g$  es la carga inducida por voltaje en el capacitor C (isla qubit) y  $\phi_e$  es la fase inducida por flujo sobre la JJ. La energía de Josephson  $E_{J0}$  está dada por  $E_{J0} = \frac{\hbar}{2e} I_0$  en términos de la corriente crítica  $I_0$  de la unión.

Usualmente, la JJ es del tipo Superconductor-Aislante-Superconductor con corriente crítica fija.

Con el fin de introducir la inductancia no lineal de Josephson, empezamos por

$$I_J = I_0 \sin(\phi)$$

Combinado con la ley de Lenz:

$$V = \frac{d\Phi}{dt} = \frac{\Phi_0}{2\pi} \frac{d\phi}{dt}, \quad \Phi_0 = \frac{h}{2e}$$

Se encuentra que:

$$V = \frac{\Phi_0}{2\pi} \frac{1}{I_0 \cos(\phi)} \frac{dI_J}{dt}$$

Definiendo  $L_J = V(\frac{dI_J}{dt})^{-1}$ , se obtiene finalmente la inductancia de Josephson  $L_{J0}$ :

$$L_J = \frac{\Phi_0}{2\pi} \frac{1}{I_0 \cos(\phi)} = L_{J0} \frac{1}{\cos(\phi)}$$

Esto define la inductancia de Josephson de la JJ aislada y nos permite expresar la energía de Josephson como  $E_{J0} = \frac{\hbar^2}{(2e)^2 L_{J0}}$

$$[E_C(-i\hbar \frac{\partial}{\partial \phi} - n_g)^2 + U(\phi)]\psi = E\psi$$

$$U(\phi) = -E_{J0} \cos(\phi) + E_L \frac{(\phi - \phi_e)^2}{2}$$

1.  $E_L = 0$  ( $L \sim \infty$ ) :
2.  $E_L \approx E_{J0}$  :

### 3.1. Transmonios

Tratando el transmonio como un sistema de dos niveles acoplado linealmente a un oscilador monomodo, su Hamiltoniano toma la siguiente forma:

$$\hat{H} = \hat{H}_q + \hat{H}_{qr} + \hat{H}_r = -\frac{1}{2}\epsilon\sigma_z + g\sigma_x(a + a^\dagger) + \hbar\omega(a^\dagger a + \frac{1}{2})$$

donde  $\epsilon$  es la energía de excitación del qubit,  $g$  es el acoplamiento qubit-oscilador y  $\omega$  es la frecuencia del oscilador.

Introduciendo los operadores escalera del qubit,  $\sigma_{\pm} = \frac{1}{2}(\sigma_x \pm i\sigma_y)$ , el término de interacción  $\hat{H}_{qr}$  se puede dividir en dos términos, el de Jaynes-Cummings (JC) y el anti-Jaynes-Cummings (AJC):

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

Este Hamiltoniano describe el modelo cuántico canónico de Rabi (canonical quantum Rabi model - QRM). Las ecuaciones (()) son completamente generales y aplicables a cualquier sistema qubit-oscilador. Mantener sólo el término JC corresponde a realizar la aproximación de onda rotativa (rotating wave approximation - RWA).

### 3.2. Hamiltonianos multiqubit de transmonios

Omitiendo el término del oscilador, el Hamiltoniano toma la siguiente forma general:

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

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

#### 3.2.1. Acoplamiento capacitivo

$$\begin{aligned} \hat{H}_{qq} &= \lambda_{12} \sigma_{x1} \sigma_{x2} \\ \lambda_{12} &= \frac{1}{2} \sqrt{E_{10,1} E_{10,2}} \frac{\sqrt{E_{EC1} E_{EC2}}}{E_{Cc}} = \frac{1}{2} \sqrt{E_{10,1} E_{10,2}} \frac{Cc}{\sqrt{C_1 C_2}} \approx \frac{1}{2} E_{10} \frac{C_c}{C} \\ \hat{H}_{qq} &= \lambda_{12} (\sigma_{+1} \sigma_{-2} + \sigma_{-1} \sigma_{+2}) \end{aligned}$$

### 3.2.2. Acoplamiento por el resonador

$$\begin{aligned}\hat{H}_{qq} &= \lambda_{12} \sigma_{x1} \sigma_{x2} \\ \lambda_{12} &= \frac{1}{2} g_1 g_2 \left( \frac{1}{\Delta_1} + \frac{1}{\Delta_2} \equiv g_1 g_2 \frac{1}{\Delta} \right) \\ \Delta_i &= \epsilon_i - \hbar\omega\end{aligned}$$

### 3.2.3. Acoplamiento de JJ

$$\begin{aligned}\hat{H}_{qq} &= \lambda_{12} \sigma_{y1} \sigma_{y2} \\ \lambda_{12} &\approx \frac{1}{2} E_{10} \frac{L_c}{L_J} \frac{\cos(\delta_c)}{2L_c \cos(\delta_c) + L_{Jc}}\end{aligned}$$

### 3.2.4. Acoplamiento afinable/calibrable

## 3.3. Compuertas cuánticas en transmonios

### 3.3.1. El operador de evolución temporal

La evolución temporal de un sistema complejo (many-body) puede ser descrita por la ecuación de Schrödinger para el vector de estado  $|\psi(t)\rangle$ :

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

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

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

determinado a partir del Hamiltoniano complejo (many-body) dependiente del tiempo del sistema:

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

describiendo el sistema intrínseco y las operaciones de control aplicadas. Las compuertas son el resultado de aplicar pulsos de control específicos a partes selectas de un circuito físico. Esto afecta varios términos del Hamiltoniano, haciéndolos dependientes del tiempo.

Para el transmonio, el Hamiltoniano del sistema bajo la RWA toma la forma:

$$\hat{H}_{syst} = -\frac{1}{2} \sum_{\nu i} \epsilon_i \sigma_{zi} + \sum_i g_i (\sigma_{+i} a + \sigma_{-i} a^\dagger) + \hbar \omega a^\dagger a + \frac{1}{2} \sum_{i,j;\nu} \lambda_{\nu,ij} (\sigma_{+i} \sigma_{-j} + \sigma_{-i} \sigma_{+j})$$

y el término de control se puede escribir como:

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



## Capítulo 4

# 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.

Introducción:

Dada  $f : 0, 1^n \rightarrow 0, 1$ , es decir;  $f : 0, 1, 2, \dots, N - 1 \rightarrow 0, 1$ , se tiene la promesa de que

$$f(x) = \begin{cases} 1 & \text{si } x = x_0 \\ 0 & \text{si } x \neq x_0 \end{cases}$$

Hay que determinar  $x$ .

Clásicamente hay que evaluar la función  $N = 2^n$  veces. Cuánticamente sólo se requiere evaluar  $\sqrt{2^n}$  veces.

El análisis usual del algoritmo de Grover se basa en un hecho bien conocido de la geometría plana elemental: “El producto de dos reflexiones es una rotación”

Veamos qué significa esto:

Supongamos que tenemos el oráculo

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} |x\rangle & \text{si } x \neq x_0 \\ -|x\rangle & \text{si } x = x_0 \end{cases}$$

Es decir:  $U_f = \mathbb{1} - 2|x_0\rangle\langle x_0|$

El efecto de  $U_f$  es invertir la componente de  $|\phi\rangle$  en la dirección  $|x_0\rangle$ .

Además, podemos definir otro operador unitario  $U_s = -\mathbb{1} + 2|s\rangle\langle s|$  donde  $|s\rangle = H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$

El efecto de  $U_s$  es invertir todas las componentes en direcciones perpendiculares a  $|s\rangle$ . Es decir, refleja respecto de  $|s\rangle$ .

Hagamos ahora el siguiente ejercicio:

Cosidremos el estado inicial  $|\psi\rangle$

1. Aplicamos  $U_\omega$ , que invierte la componente  $|x_0\rangle$ .
2. Aplicamos  $U_s$ , que refleja respecto de  $|s\rangle$

La combinación de estas dos inversiones es una rotación en un ángulo  $2\alpha$ .

Una vez entendido esto empecemos el algoritmo de Grover.

Algoritmo de Grover:

Asumamos que el tamaño de nuestra base de datos es  $2^n \equiv N$ , donde  $n$  es cualquier número entero distinto de cero.

Consideremos un observable  $\Omega \in H$  de dimensión  $N \geq 2$ . Este observable define un conjunto de bases ortogonales  $|x\rangle = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$  con autovalores conocidos  $\lambda_0, \lambda_1, \lambda_2, \dots, \lambda_{N-1}$ , tal que  $\hat{\Omega}|j\rangle = \lambda_j|j\rangle$ ,  $j \in 0, \dots, N-1$ .

Entonces podemos asociar un único autoestado  $|x_j\rangle$ , o autovalor  $\lambda_j$ , con cada ítem en la base de datos.

El problema de buscar en la base de datos se convierte ahora en el problema de medir un autovalor de interés al que llamaremos  $\lambda_\omega$ , asociado con el estado  $|\omega\rangle$ , el cual representa algún específico ítem  $\omega$  en nuestra base de datos y el cuál deseamos encontrar usando el algoritmo de búsqueda de Grover.

Entonces:

$$\{|x\rangle\}_{x=0,1,\dots,N-1} \text{ es ortonormal} \rightarrow |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \text{autoestado asociado a la base de datos}$$

$$\langle s|s\rangle = 1 \text{ ya que } \langle i|j\rangle = \delta_{ij}$$

Cualquier autoestado  $|\omega\rangle$  tiene la misma proyección  $\langle \omega|s\rangle = \frac{1}{\sqrt{N}}$ , y dado un ítem  $\omega$  la probabilidad de medir  $\lambda_\omega$  (que es equivalente a encontrar

$|s\rangle$  en el estado  $|\omega\rangle$  es  $|\langle\omega|s\rangle|^2 = \frac{1}{N}$ , consistentemente con lo que ocurre con una base de datos clásica.

Consideremos ahora el oráculo unitario  $U_\omega$  definido como:

$$U_\omega \equiv \mathbb{1} - 2|\omega\rangle\langle\omega|$$

Entonces  $U_\omega|x\rangle = (\mathbb{1} - 2|\omega\rangle\langle\omega|)|x\rangle = |x\rangle - 2\langle\omega|x\rangle|\omega\rangle = |x\rangle - 2\delta_{ij}|\omega\rangle$  Si  $x \neq \omega \rightarrow U_\omega|x\rangle = |x\rangle$  Si  $x = \omega \rightarrow U_\omega|x\rangle = -|\omega\rangle$

De manera tal que  $U_\omega|s\rangle = U_\omega(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle) = \frac{1}{\sqrt{N}}U_\omega(\sum_{x=0, x \neq \omega}^{N-1}|x\rangle + |\omega\rangle) = \frac{1}{\sqrt{N}}\sum_{x=0, x \neq \omega}^{N-1}|x\rangle - \frac{1}{\sqrt{N}}|\omega\rangle$ .

Esto se puede reescribir como:

$$U_\omega|s\rangle = \frac{1}{\sqrt{N}}\sum_{x=0, x \neq \omega}^{N-1}|x\rangle + (\frac{1}{\sqrt{N}}|\omega\rangle - \frac{1}{\sqrt{N}}|\omega\rangle) - \frac{1}{\sqrt{N}}|\omega\rangle$$

Por lo tanto:  $U_\omega|s\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle - \frac{2}{\sqrt{N}}|\omega\rangle \rightarrow U_\omega|s\rangle = |s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$

Llamemos  $|\psi\rangle \equiv U_\omega|s\rangle = |s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$  como  $0 \leq \langle s|\psi\rangle \leq 1$

llamemos  $\cos(\theta) \equiv \langle s|\psi\rangle \equiv \langle s|s\rangle - \frac{2}{\sqrt{N}}\langle s|\omega\rangle = 1 - \frac{2}{\sqrt{N}}\frac{1}{\sqrt{N}} \rightarrow \cos(\theta) = 1 - \frac{2}{N}$

cuando  $N$  es grande  $\cos(\theta) \approx 1$  pero nunca es uno

Cosideremos ahora un segundo operador  $U_s$  definido como:

$$U_s = 2|s\rangle\langle s| - \mathbb{1}$$

Se define el operador de Grover como  $G = U_s U_\omega$

Consideremos la iteración de Grover  $|\psi_1\rangle \equiv G|s\rangle \rightarrow |\psi_1\rangle = U_s U_\omega|s\rangle = U_s|\psi\rangle$

luego:  $|\psi_1\rangle = U_s|\psi\rangle = U_s(|s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle)$

$$|\psi_1\rangle = 2\langle s|s\rangle|s\rangle - |s\rangle - \frac{4}{\sqrt{N}}\langle s|\omega\rangle|s\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$$

$$|\psi_1\rangle = |s\rangle - \frac{4}{N}|s\rangle + \frac{2}{\sqrt{N}}ket\omega$$

$$|\psi_1\rangle = (1 - \frac{4}{N})|s\rangle + \frac{2}{\sqrt{N}}|\omega\rangle$$

La acción de  $G$  sobre  $|s\rangle$  incrementa la amplitud de probabilidad del autoestado de componente  $|\omega\rangle$ , después de la rotación.

El correspondiente ángulo de rotación  $\theta'$  viene dado por:

$$\cos(\theta') = \langle s|\psi_1\rangle = \langle s|[(1 - \frac{4}{N})|s\rangle + \frac{2}{\sqrt{N}}|\omega\rangle] = (1 - \frac{4}{N} + \frac{2}{\sqrt{N}}\frac{1}{\sqrt{N}}) = 1 - \frac{2}{N} = \cos(\theta)$$

Por lo tanto  $\cos(\theta') = \cos(\theta)$

Confirmando así que los ángulos de rotación  $\theta'$  y  $\theta$  debidos a la acción de  $G$  y  $U_\omega$  son iguales en valor absoluto. De hecho, rotando el mismo ángulo

$\theta = \theta'$  en valor absoluto, en direcciones opuestas sobre  $|s\rangle$  se forma un ángulo  $\theta'' = 2\theta$ .

$$\begin{aligned} \cos(\theta'') &= \langle \psi | \psi_1 \rangle = [\langle s | - \frac{2}{\sqrt{N}} \langle \omega |] [(1 - \frac{4}{N}) |s\rangle + \frac{2}{\sqrt{N}} |\omega\rangle] = (1 - \frac{4}{N}) \langle s | s \rangle - \\ &\frac{2}{\sqrt{N}} (1 - \frac{4}{N}) \langle \omega | s \rangle + \frac{2}{\sqrt{N}} \langle s | \omega \rangle - \frac{2}{\sqrt{N}} \frac{2}{\sqrt{N}} \langle \omega | \omega \rangle = 1 - \frac{4}{N} - \frac{2}{\sqrt{N}} (1 - \frac{4}{N}) \frac{1}{\sqrt{N}} + \\ &\frac{2}{\sqrt{N}} \frac{1}{\sqrt{N}} - \frac{4}{N} = 1 - \frac{8}{N} + \frac{8}{N^2} = 2(1 - \frac{2}{N})^2 - 1 = 2 \cos^2(\theta) - 1 = \cos(2\theta) \end{aligned}$$

Por lo tanto:  $\theta'' = 2\theta$

La relación entre los estados  $|s\rangle$ ,  $|\psi\rangle$ ,  $|\psi_1\rangle$  y  $|\omega\rangle$  y sus relaciones de proyección  $\langle \omega | s \rangle$  y  $\langle \omega | \psi_1 \rangle$  son ilustradas en la siguiente figura

Como recordamos  $\hat{\Omega} |j\rangle = \lambda_j |j\rangle \quad j \in \{0, 1, \dots, N-1\}$  y  $\omega \in 0, 1, \dots, N-1$ .

$$\hat{\Omega} |\omega\rangle = \lambda_\omega |\omega\rangle$$

Luego si realizamos una medida en el estado  $|\psi_1\rangle$  con el observable  $\hat{\Omega}$ , la probabilidad de medir  $\lambda_\omega$  es:

$$\begin{aligned} |\langle \omega | \psi_1 \rangle|^2 &= |\langle \omega | [(1 - \frac{4}{N}) |s\rangle + \frac{2}{\sqrt{N}} |\omega\rangle]|^2 = \frac{1}{N} (3 - \frac{4}{N})^2 = \frac{1}{N} (9 - \frac{24}{N} + \frac{16}{N^2}) \\ \lim_{N \rightarrow \text{grande}} |\langle \omega | \psi_1 \rangle|^2 &\approx \frac{9}{N} \end{aligned}$$

Este resultado muestra que una simple interacción de Grover y su respectiva medida aumenta casi en 9 veces el valor de la probabilidad clásica.

$$\text{Grover} \approx \frac{9}{N} \text{ Medida clásica} = \frac{1}{\sqrt{N}}$$

Siguiendo el mismo esquema, podemos aplicar el operador de Grover varias veces rotando el sistema lo más cercano posible del estado  $|\omega\rangle$  incrementando así la probabilidad de medir  $\lambda_\omega$  con la precisión requerida.

El efecto producido por los operadores unitarios  $U_\omega$  y  $G$  sobre el estado inicial se ilustra en la siguiente figura.

Para derivar una fórmula de iteración, redefinamos el autoestado original  $|s\rangle$  quitándole el estado  $|\omega\rangle$  de la serie, es decir:

$$|u\rangle \equiv \frac{1}{\sqrt{N-1}} \sum_{x=0, x \neq \omega}^{N-1} |x\rangle = \sqrt{\frac{N}{N-1}} |s\rangle - \frac{1}{\sqrt{N-1}} |\omega\rangle$$

Entonces podemos reescribir  $|s\rangle$  en términos de  $|\omega\rangle$ , tal que:

$$|s\rangle = \frac{1}{N} \sum_{x=0}^{N-1} |x\rangle \equiv \sqrt{1 - \frac{1}{N}} |u\rangle + \frac{1}{\sqrt{N}} |\omega\rangle$$

$$\text{como } 0 \leq \sqrt{1 - \frac{1}{N}} \leq 1, 0 \leq \frac{1}{\sqrt{N}} \leq 1 \text{ y } (\sqrt{1 - \frac{1}{N}})^2 + (\frac{1}{\sqrt{N}})^2 = 1$$

$$\text{podemos asociar: } \cos(\frac{\theta}{2}) = \sqrt{1 - \frac{1}{N}} \text{ y } \sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}$$

$$\text{quedándonos } |s\rangle = \cos(\theta/2) \sqrt{1 - \frac{1}{N}} + \sin(\theta/2) \frac{1}{\sqrt{N}}$$

Se puede demostrar que si aplicamos k veces el operador de Grover se obtiene:

$$G^k |s\rangle = \cos((2k+1)\frac{\theta}{2}) |u\rangle + \sin((2k+1)\frac{\theta}{2}) |\omega\rangle$$

Este resultado muestra que después de k iteraciones del operador de Grover, el estado inicial  $|s\rangle$  rota un ángulo  $k\theta$ .

La probabilidad  $p(\omega)$  de encontrar el estado  $G^k |s\rangle$  en  $|\omega\rangle$ , y por ende la medida del autovalor  $\lambda_\omega$  con el observable  $\hat{\Omega}$  está dada por

$$p(\omega) = |\langle \omega | G^k |s\rangle|^2 = \sin^2((2k+1)\frac{\theta}{2})$$

Esta probabilidad alcanza un máximo cuando  $\sin^2((2k+1)\frac{\theta}{2}) = 1$ , y eso ocurre cuando  $k_{max}\theta + \frac{\theta}{2} = \frac{\pi}{2} \rightarrow k_{max} = \frac{\pi-\theta}{2\theta}$

por otro lado, ya vimos que  $\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}$ , y si  $N$  es grande  $\theta$  se hace pequeño

$$\sin(\frac{\theta}{2}) \approx \frac{\theta}{2} - \frac{(\theta/2)^3}{3!} + \dots \approx \frac{\theta}{2} = \frac{1}{\sqrt{N}} \rightarrow \theta \approx \frac{2}{\sqrt{N}}$$

$$k_{max} = \frac{\pi}{2\theta} - \frac{\theta}{2\theta} \approx \frac{\pi}{2\frac{2}{\sqrt{N}}} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \rightarrow k_{max} \approx \frac{\pi}{4}\sqrt{N} = O(\sqrt{N})$$

El algoritmo de Grover debe detenerse cuando  $k \approx k_{max}$  ya que en dicho caso  $p(\omega) \approx 1$  y ya hemos encontrado el estado  $|\omega\rangle$  deseado.

Esto se ilustra mejor en la siguiente figura:

Esta figura es muy importante ya que en ella se muestra la probabilidad en función del número de iteraciones, desde bases de datos cuyos tamaños van desde  $N = 2^6 = 64$  hasta  $N = 2^{14} = 16384$

Debido a la dependencia de Grover del  $O(\sqrt{N})$  encontramos que en el caso clásico con  $N = 2^{14} = 16384$  iteraciones en Grover solo tenemos  $k_{max} \approx 100$  iteraciones de Grover.

En resumen:

Algoritmo Clásico  $\rightarrow$  16384 iteraciones Algoritmo de Grover  $\rightarrow \approx 100$  iteraciones

#### 4.0.1. Implementación circuital del algoritmo de Grover

Consideremos como ejemplo  $\Rightarrow N = s^3 = 8$ , luego:

1)

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

Si:  $N = 2^3 = 8$

$$|s\rangle = \frac{1}{\sqrt{2^3}} \sum_{x=0}^7 |x\rangle = H^{\otimes 3} |0\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

En resumen, necesitamos una ancilla  $|0\rangle$  y  $n$  compuertas de Hadamard para crear  $|s\rangle$ .

2)

Necesitamos crear el operador  $U_\omega$ , “el oráculo”.

$$U_\omega |x\rangle = -|\omega\rangle \text{ si } x = \omega \quad U_\omega |x\rangle = |x\rangle \text{ si } x \neq \omega$$

$$\text{Además, si } x = \{0, 1, \dots, N-1\} \Rightarrow \begin{cases} f(x) = 1 \text{ si } x = \omega \\ f(x) = 0 \text{ si } x \neq \omega \end{cases}$$

## 4.1. El operador de difusión de Grover

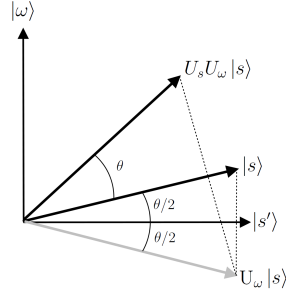
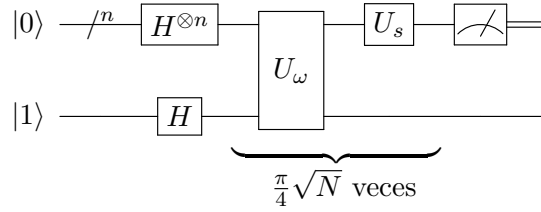


Figura 4.1: Interpretación geométrica del operador difusión

$$U_s = 2|s\rangle\langle s| - I$$

$$U_\omega = I - 2|\omega\rangle\langle\omega|$$

## 4.2. El algoritmo



1. Inicializar el estado del sistema.
2. Aplicar la transformada de Walsh-Hadamard.
3. Realizar la iteración de Grover  $\lfloor \frac{\pi}{4} \sqrt{N} \rfloor$  veces.
  - a) Aplicar  $U_\omega$ .
  - b) Aplicar  $U_s$ .
4. Realizar la medida  $\Omega$ .

## Capítulo 5

# 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.

1) Co-primos:

Dos números primos entre sí, es decir co-primos o primos relativos, son números enteros  $a$  y  $b$  que no tienen ningún factor primo en común. Es decir, sólo tienen como divisor común a 1 y -1. Esto es equivalente a decir que su máximo común divisor es 1.

Dos primos entre sí no tienen porque ser primos absolutos en forma individual.

Ejemplo:

35 — 7 6 — 3 5 — 5 2 — 2 1 — 1 1 — 1 1 — 1 —

$\text{mcd}(6, 35) = 1$  pero  $6 = 3.2.1$  -¿ no es primo  $35 = 7.5.1$  -¿ no es primo

Estimación de orden:

\* Definición de congruencia: Dado  $m \in \mathbb{Z}, m \geq 1$ , se dice que  $a, b \in \mathbb{Z}$  son congruentes módulo  $m$  si y sólo si  $m \mid (a-b)$ .

- Se denota por  $a \equiv b \pmod{m}$ , siendo  $m$  el módulo de la congruencia. - Si  $m$  divide a  $a-b$ , esto supone que ambos  $a$  y  $b$  tienen el mismo resto al ser divididos por el módulo  $m$ .

Ejemplos:

$23 \equiv 2 \pmod{7} \rightarrow 23 \equiv 37 + 2 \quad -6 \equiv 1 \pmod{7} \rightarrow -6 \equiv -71 + 1$

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

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

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

Es decir:

$$\text{Sea } x = 4, N = 13 \rightarrow 4^p = 13q + \text{remainder}((R)); 4^p \pmod{13} = \text{remainder}$$

$p$	$4^p$	$4^p = 13q + R$	$R$
0	1	$4^0 = 130 + 1$	1
1	4	$4^1 = 130 + 4$	4
2	16	$4^2 = 131 + 3$	3
3	64	$4^3 = 134 + 12$	12
4	256	$4^4 = 1319 + 9$	9
5	1024	$4^5 = 1378 + 10$	10
6	4096	$4^6 = 13315 + 1$	1
7	16384	$4^7 = 131260 + 4$	4
8	65536	$4^8 = 135041 + 3$	3
9	262144	$4^9 = 1320164 + 12$	12
10	1048576	$4^{10} = 1380659 + 9$	9
11	4194304	$4^{11} = 13322638 + 10$	10
12	16777216	$4^{12} = 131290555 + 1$	1
13	67108864	$4^{13} = 135162220 + 4$	4
14	268435456	$4^{14} = 1320648881 + 3$	3
15	1073741824	$4^{15} = 1382595524 + 12$	12
16	4294967296	$4^{16} = 13330382099 + 9$	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:

$$p_n = a_n p_{n-1} + p_{n-2} \quad q_n = a_n q_{n-1} + q_{n-2}$$

$$\text{con } n \geq 2, p_0 = a_0, q_0 = 1, p_1 = 1 + a_0 a_1 q_1 = a_1, \text{ para } n = 0, 1.$$



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  $\phi$ , 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  $\phi$ .

\* 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-primario 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  $\phi$  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" "back-end".

Analicemos la etapa front-end:

Recordemos que:

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

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

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

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

Analicemos ahora el producto tensorial a la salida de dos compuertas  $CUP$  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  $\phi$  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  $\delta$  se aleja del mínimo.

Entonces:

.) La medida tiene la maor probabilidad de dar la aproximación más cercana al estado  $\phi$ . .) 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  $\phi$ .

\* Estimación de orden:

Analicemos como la estimación de fase hace posible determinr  $r$ , el orden de  $x \bmod N$ , 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:

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

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  $0 \leq \phi_s \leq 1$

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

siendo  $r$  a determinar.

Con las siguientes propiedades:

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

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

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

El circuito para la estimación de orden es el siguiente:

Entonces:

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

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

$$CU^j(|0\rangle \otimes |1\rangle) = |0\rangle \otimes |1\rangle$$

$$\begin{aligned}
CU^j |j\rangle \otimes |1\rangle &= |j\rangle \otimes \left| x^{j_1 2^{k-1}} \bmod N \right\rangle \left| x^{j_2 2^{k-2}} \bmod N \right\rangle \dots \left| x^{j_k 2^0} \bmod N \right\rangle \\
CU^j |j\rangle \otimes |1\rangle &= |j\rangle \otimes \left| x^{j_1 2^{k-1}} x^{j_2 2^{k-2}} \dots x^{j_k 2^0} \bmod N \right\rangle \\
\therefore CU^j |j\rangle \otimes |1\rangle &= |j\rangle \otimes |x^j \bmod N\rangle
\end{aligned}$$

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

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

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

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

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

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

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  $L = \log_2 N = 4$  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:

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

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

$$\cdot) \text{Aplicamos la compuerta } \textit{Controlled}-U^j |\psi_3\rangle = \frac{1}{\sqrt{M}} |j\rangle \otimes |x^j \bmod N\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |1\rangle \otimes |8^j \bmod 15\rangle$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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  $\alpha_k$

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  $\alpha_k$  es indeterminado, luego:

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

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

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:

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

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

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

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

3 y 4 son co-primos.

La fracción  $3/4$  es un convergente de  $\phi$  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

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

- 5.1. Transformadas integrales
- 5.2. Transformada cuántica de Fourier
- 5.3. Estimación de fase
- 5.4. Estimación de orden
- 5.5. Algoritmo de Shor



## Capítulo 6

# Google PageRank

El algoritmo de PageRank fue desarrollado en 1996 en la Universidad de Stanford por Larry Page y Sergey Brin, los cuales fueron los fundadores de Google.

Este algoritmo se basa en la idea de que sitios web importantes tienen muchos vínculos que apuntan hacia ellos, lo que conduce a pensar en la web como una red ponderada orientada.

Existen muchos otros algoritmos, algunos más eficientes, pero la importancia de PageRank se sustenta en el poder económico de Google.

Ilustraremos el algoritmo de PageRank con un ejemplo sencillo:

Ejemplo:

Consideremos 5 páginas web distintas a las que denotaremos por 1, 2, 3, 4, y 5, y cuyo grafo es:

Pasos:

1. Determinar la matriz de adyacencia. Algunos autores denotan la matriz de de adyacencia por  $M$  en el protocolo de PageRank

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

2. Sumamos los elementos de cada una de las columnas.

$$3 \quad 1 \quad 2 \quad 2 \quad 3$$

Estas sumas representan el número de links que salen del nodo o vértice de la página  $p_j$ , es decir:

$I(p_j) \equiv$  Importancia de la página  $j$

$\text{outdeg}(p_j) \equiv$  número de links que salen de la página  $p_j$

$$I(p_i) \equiv \sum_{j \in B_i} \frac{I(p_j)}{\text{outdeg}(p_j)}$$

$B_i \equiv$  conjunto de páginas que son linkeadas

3. Dividimos cada elemento de  $M$  por la suma de los elementos de la columna a la cual corresponde y llamaremos a la nueva matriz obtenida  $M'$

$$M' = \begin{pmatrix} 0 & 0 & 1/2 & 1/2 & 1/3 \\ 0 & 0 & 0 & 0 & 1/3 \\ 1/3 & 0 & 0 & 1/2 & 1/3 \\ 1/3 & 0 & 1/2 & 0 & 0 \\ 1/3 & 1 & 0 & 0 & 0 \end{pmatrix}$$

4. El siguiente paso es encontrar un vector  $\vec{v}$  (algunos autores lo llaman  $\vec{I}$ ) que represente el PageRank de cada una de las páginas. Como tenemos 5 páginas web le asignamos a  $\vec{v}$  como valores  $\vec{v} = (a, b, c, d, e)^T$ , obteniendo así un vector de dimensión  $d = 5$ .
5. Obtenemos los valores de  $\{v_i\}$  a partir de los autovalores de  $M'$ , tal que:

$$M'\vec{v} = \lambda\vec{v} \text{ con } \lambda \in R$$

6. Determinamos los autovalores de  $M'$

$$\lambda_1 = 1; \quad \lambda_2 = \frac{-2}{3}; \quad \lambda_3 = \frac{-1}{2}; \quad \lambda_4 = \frac{-1}{3}; \quad \lambda_5 = \frac{1}{3}$$

Tomaremos sólo  $\lambda = 1 \rightarrow M'\vec{v} = \vec{v}$  (Ecuación autoconsistente)

7. Hallamos el autovector asociado a  $\lambda = 1$ . Obteniendo:

$$a = 6; \quad b = 1; \quad c = \frac{16}{3}; \quad d = \frac{14}{3}; \quad e = 3$$

8. Finalmente, Google ordena de mayor a menor las componentes de  $\vec{v}$ , quedándonos:

$$\begin{array}{rcl} & & - \quad a \\ & & - \quad c \\ \text{Pantalla} & \rightarrow & - \quad d \\ & & - \quad e \\ & & - \quad b \end{array}$$

La idea de PageRank de Google es que la importancia de una página viene dada por la cantidad de páginas que se enlazan con ella.

Surgen varios problemas:

1. Las matrices hyperlink (hiperenlace) pueden tener billones de entradas en filas y columnas.
2. Calcular los autovectores es un absurdo computacional.
3. Los estudios muestran que un nodo (página web) tiene un promedio de 10 enlaces, y las demás entradas de la matriz son cero.
4. No se encuentra  $\lambda = 1$  en la mayoría de los casos.

Por esta razón, un remedio (Patching) del algoritmo de PageRank fue el método de las potencias, en el cual la matriz hiperenlace

$$H_{ij} \equiv \begin{cases} \frac{1}{\text{outdeg}(P_j)} & \text{si } P_j \in B_i \\ 0 & \text{en otro caso} \end{cases}$$

debería converger a una solución autoconsistente

$$I^{k+1} = HI^k$$

donde se toma un vector  $I^0$  y se hace interactuar unas 100 veces y el orden mostrado de las páginas es el de  $I^{100}$ , ordenadas de mayor a menor. Si se normalizan las columnas de la matriz hipervínculo (hiperenlace)  $H$ , obtenemos otra matriz hiperenlace normalizada  $E$ .

**La matriz  $E$ :** se sabe de la teoría de matrices estocásticas que 1 es uno de sus autovalores. Además, también se sabe que la convergencia de  $I^k = EI^{k-1}$  a  $I = EI$  depende del segundo autovalor de  $E$  y es un hecho que  $I^k = EI^{k-1}$  converge rápidamente si  $|\lambda_2|$  es cercano a cero.

### 6.0.1. El algoritmo de remiendo (parcheo) general

Asumamos que el caminante recorre el grafo siguiendo la web con una matriz estocástica  $E$  con probabilidad  $\alpha$ , y con probabilidad  $1 - \alpha$  podrá ir a cualquier página al azar que sea de su interés. La matriz web de este proceso será:

$$G \equiv \alpha E + \frac{1 - \alpha}{N} \mathbb{I} \text{Matriz de Google}$$

$\mathbb{I}$  es una matriz en la cual todas las entradas están establecidas en 1, y  $N$  el número de nodos.

Propiedades de  $G$ :

1. Es estocástica
2. Irreducible
3. Primitiva
4. El resultado de determinar el estado auto-consistente no depende del vector Google inicial  $I^0$

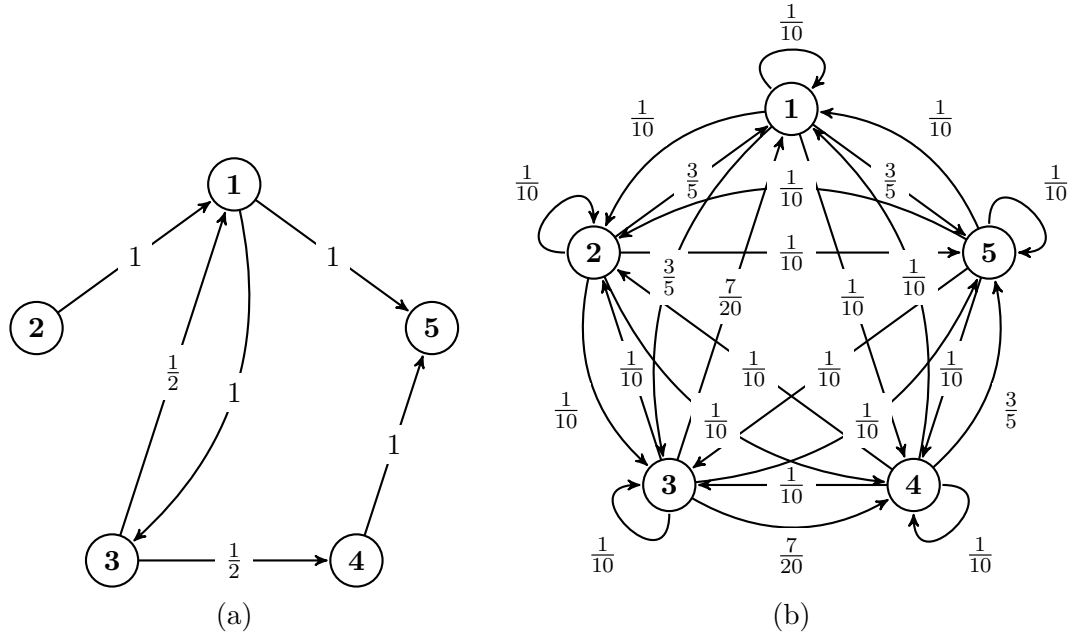


Figura 6.1: Grafo correspondiente a la matriz de adyacencia (a) de la red E (b) remendada de Google G con  $\alpha = \frac{1}{2}$

### 6.0.2. Interpretación como una caminata aleatoria

La asignación de valores de importancia se puede replantear como la probabilidad de encontrar un caminante aleatorio en cierto nodo del grafo.

Del proceso:

De la ley de probabilidad total:

$$\begin{aligned}
 &Pr(x^{(n+1)} = p_i) & Pr(x^{(n+1)} = p_i) \\
 &= \sum_j G_{ij} Pr(x^{(n)} = p_j) & = \sum_j Pr(x^{(n+1)} = p_i | x^{(n)} = p_j) Pr(x^{(n)} = p_j) \\
 &\implies G_{ij} = Pr(x^{(n+1)} = p_i | x^{(n)} = p_j)
 \end{aligned}$$

En el contexto del Internet,  $G_{ij}$  es la probabilidad de que cierto internauta, que se encuentra en la página  $p_i$ , entre en la página  $p_j$ . El factor  $\alpha E_{ij}$  es la probabilidad de que lo haga presionando un enlace presente en  $p_i$ , mientras que  $\frac{1-\alpha}{N} \mathbb{I}$  es la probabilidad de que lo haga introduciendo la URL directamente.

El factor de amortiguamiento es libre y debe ser calibrado. Se suele usar  $\alpha = 0,85$

### 6.0.3. Cuantizando las caminatas aleatorias

La forma obvia y directa de cuantizar una caminata aleatoria sería sustituir el conjunto de nodos  $\{p_i\}$  por el conjunto de kets  $\{|i\rangle\}$ . Sin embargo, esto lleva a sistemas con operadores no unitarios y no es realizable.



Esto nos obliga a buscar maneras alternativas de cuantizar las caminatas aleatorias. La cadena anterior se podría cuantizar agregando un espacio "moneda".<sup>al</sup> espacio de Hilbert generado por  $\{|i\rangle\}$ . En este caso, el operador de difusión se interpreta como "lanzar la moneda" para decidir en qué dirección ir.

$$\begin{aligned}
 U &= \sqrt{p} |i+1\rangle\langle i| \otimes |c\rangle\langle c| + \sqrt{1-p} |i-p\rangle\langle i| \otimes |s\rangle\langle s| \\
 U^\dagger &= \sqrt{p} |i\rangle\langle i+1| \otimes |c\rangle\langle c| + \sqrt{1-p} |i\rangle\langle i-p| \otimes |s\rangle\langle s| \\
 UU^\dagger &= p |i+1\rangle\langle i+1| \otimes |c\rangle\langle c| + (1-p) |i-1\rangle\langle i-1| \otimes |s\rangle\langle s|
 \end{aligned}$$

Al realizar la suma sobre  $i$  se tiene  $\mathbb{1}$ , como se deseaba. Sin embargo, esta solución todavía no es satisfactoria, pues exige que  $p_{ij} = \frac{1}{\text{outdeg}(j)}$  para que  $UU^\dagger = \mathbb{1}$ .

Casi todas las cuantizaciones cometen estos dos pecados, aumentar la dimensión del espacio de Hilbert e imponer condiciones sobre el grafo; y en general, se debe cometer al menos uno de los dos.

**Nota:** También existen caminatas cuánticas continuas, no sólo discretas.

### 6.0.4. Caminata cuántica de Szegedy

Existe un tipo particular de caminatas aleatorias conocido como caminatas bipartitas. En éstas se tiene dos conjuntos de nodos y sólo ocurren transiciones entre los dos conjuntos, no dentro del mismo.

Szegedy desarrolló una cuantización de estas caminatas. Para esto utilizó operadores de reflexión ( $W = \mathbb{1} - 2|w\rangle\langle w|$ , similares a los utilizados en el algoritmo de Grover). Aprovechándose del hecho de que un par de reflexiones equivale a una rotación (como en el algoritmo de Grover), creó el siguiente operador de evolución de la caminata:  $U = (\mathbb{1} - 2B)(\mathbb{1} - 2A)$ , donde A es el proyector sobre las transiciones de la primera partición a la segunda y B de la segunda a la primera.

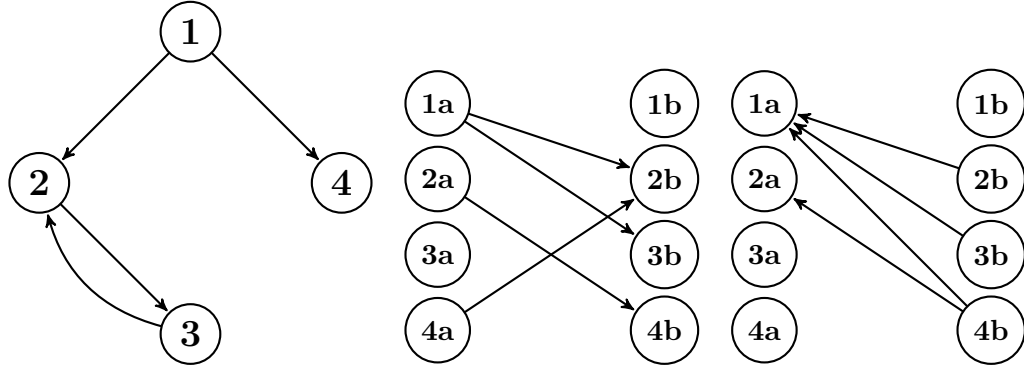
$$|\psi_i\rangle = |i\rangle_1 \otimes \sum_j \sqrt{p_{ji}} |j\rangle_2$$

$$A = \sum_i |\psi_i\rangle\langle\psi_i|$$

$$|\psi_i\rangle = \sum_i \sqrt{p_{ij}} |i\rangle_1 \otimes |i\rangle_2$$

$$B = \sum_j |\phi_j\rangle\langle\phi_j|$$

Si tomamos un grafo cualquiera y lo duplicamos en la forma de un grafo bipartito con ambas particiones iguales y transiciones iguales en ambos sentidos, podemos cuantizar cualquier tipo de caminata. Sólo hay que pagar el precio de duplicar el espacio de Hilbert generado por  $\{|i\rangle\}$ :  $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}$ .



En estos casos, podemos escribir el operador de difusión en términos de sólo A, pues como la segunda partición es un reflejo de la primera,  $B = A^T$ . Entonces:  $U = (2A^T - \mathbb{1})(2A - \mathbb{1})$

$$\Rightarrow = (2SAS - \mathbb{1})(2A - \mathbb{1}) = S(2A - \mathbb{1})S(2A - \mathbb{1}) = [S(2A - \mathbb{1})]^2$$

Donde  $S$  es el operador SWAP,  $S = \sum_{ij} |ji\rangle\langle ij|$

### 6.0.5. PageRank cuántico

Finalmente, procedemos a cuantizar el algoritmo de PageRank. Partimos del hecho de que el algoritmo de PageRank se puede formular como una caminata aleatoria, cuya matriz de probabilidades es la matriz de Google,  $G$ . Entonces seguimos el procedimiento de Szegedy, sustituyendo  $p_{ij}$  por  $G_{ij}$ .

Ahora, definimos el valor de PageRank cuántico en el paso  $m$  como:

$$I_q(P_i, m) = \left| U^{\dagger m} (\mathbb{1} \otimes |i\rangle\langle i|) \right\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_i |\psi_i\rangle$$

Esto equivale a realizar  $m$  pasos de la caminata con  $|\psi_0\rangle$  como estado inicial y realizar una medida proyeciva sobre  $|i\rangle_2$ .

Nota:  $I_q$  no converge, sino que oscila, así que se toma el centro de las oscilaciones como la medida de importancia de las páginas. Esto se hace promediando  $I_q$  sobre  $m$ :  $\langle I_q(P_i) \rangle = \frac{1}{M} \sum_{m=0}^{M-1} I_q(P_i, m)$



## Apéndice A

# Cálculos de Hamiltonianos

### A.1. Hamiltoniano de Jaynes-Cummings

El Hamiltoniano de Jaynes-Cummings es un Hamiltoniano diagonal que representa un sistema de dos niveles interactuando con un modo cuantizado de una cavidad óptica.

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

### A.2. Hamiltoniano multiquibit

El modelo de Jaynes-Cummings para varios qubits sin el término de la energía de la cavidad es el siguiente:

$$\hat{H} = \hat{H}_q + \hat{H}_{qr} = -\frac{1}{2} \sum_i \omega_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i})$$

### A.3. Pulsos de microondas

Para operar sobre los qubits se aplican pulsos de microondas.

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

RWA:

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

## A.4. Régimen rotacional del pulso

Trabajando con un sólo modo a la vez, se aplica la siguiente transformación  $U(t) = \exp[\sum_n -i\omega_d^{(n)}t(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})]$  para entrar en el régimen rotacional del pulso de control.

$$\hat{H} = U^\dagger(\hat{H}_{syst} + \hat{H}_d)U - iU^\dagger \dot{U}$$

$$e^{-\lambda X} H e^{\lambda X} = H + \lambda[H, X] + \frac{\lambda^2}{2!}[[H, X], X] + \dots$$

$$\hat{H} = U^\dagger(\omega_r a^\dagger a - \frac{1}{2} \sum_i \omega_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_k (a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t})) U - iU^\dagger \dot{U}$$

$$[\omega_r a^\dagger a, -i\omega_d t(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = 0$$

$$[-\frac{1}{2} \sum_i \omega_{qi} \sigma_{zi}, -i\omega_d t(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = 0$$

$$[\sigma_+, \sigma_z] = 2\sigma_+$$

$$[\sigma_-, \sigma_z] = -2\sigma_-$$

$$[\sigma_-, \sigma_+] = \sigma_z$$

$$[a, a^\dagger] = 1$$

$$[a, a^\dagger a] = aa^\dagger a - a^\dagger aa = (aa^\dagger - a^\dagger a)a = [a, a^\dagger]a = a$$

$$[a^\dagger, a^\dagger a] = a^\dagger a^\dagger a - a^\dagger aa^\dagger = a^\dagger(a^\dagger a - aa^\dagger) = a^\dagger[a^\dagger, a] = -a^\dagger$$

$$[\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), \sum_n -i\omega_d^{(n)} t(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = \sum_n -i\omega_d^{(n)} t[\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), (a^\dagger a)] + \sum_n -i\omega_d^{(n)} t[\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), (-\frac{1}{2} \sum_i \sigma_{zi})] = \sum_n -i\omega_d^{(n)} t \sum_i g_i (a \sigma_{+i} - a^\dagger \sigma_{-i}) - \sum_n -i\omega_d^{(n)} t \sum_i g_i (a \sigma_{+i} - a^\dagger \sigma_{-i}) = 0$$

$$\hat{H} = U^\dagger(\hat{H}_{syst})U = \hat{H}_{syst}$$

$$\begin{aligned} & [\sum_k (a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t}), \sum_n -i\omega_d^{(n)} t(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = (\sum_n -i\omega_d^{(n)} t) \sum_k (a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} - \\ & a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t}) \\ & [(\sum_n -i\omega_d^{(n)} t) \sum_k (a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} - a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t}), \sum_n -i\omega_d^{(n)} t(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = \\ & (\sum_n -i\omega_d^{(n)} t)^2 \sum_k (a \xi_k^* e^{i \sum_k \omega_d^{(k)} t} + a^\dagger \xi_k e^{-i \sum_k \omega_d^{(k)} t}) \end{aligned}$$

$$\begin{aligned}
& [(\sum_n -i\omega_d^{(n)}t)^2 \sum_k (a\xi_k^* e^{i\sum_k \omega_d^{(k)}t} + a^\dagger \xi_k e^{-i\sum_k \omega_d^{(k)}t}), (\sum_n -i\omega_d^{(n)}t)(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = \\
& (\sum_n -i\omega_d^{(n)}t)^3 \sum_k (a\xi_k^* e^{i\sum_k \omega_d^{(k)}t} - a^\dagger \xi_k e^{-i\sum_k \omega_d^{(k)}t}) \\
& [(\sum_n -i\omega_d^{(n)}t)^3 \sum_k (a\xi_k^* e^{i\sum_k \omega_d^{(k)}t} - a^\dagger \xi_k e^{-i\sum_k \omega_d^{(k)}t}), (\sum_n -i\omega_d^{(n)}t)(a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})] = \\
& (\sum_n -i\omega_d^{(n)}t)^4 \sum_k (a\xi_k^* e^{i\sum_k \omega_d^{(k)}t} + a^\dagger \xi_k e^{-i\sum_k \omega_d^{(k)}t}) \\
& e^{-X} H e^X = H + [H, X] + \frac{1}{2!} [[H, X], X] + \dots
\end{aligned}$$

$$\begin{aligned}
\hat{H} = U^\dagger (\hat{H}_d) U &= \sum_k (e^{\sum_n -i\omega_d^{(n)}t} a\xi_k^* e^{i\sum_k \omega_d^{(k)}t} + e^{-\sum_n -i\omega_d^{(n)}t} a^\dagger \xi_k e^{i\sum_k \omega_d^{(k)}t}) = \sum_k (a\xi_k^* + a^\dagger \xi_k) \\
& -iU^\dagger \dot{U} = -\sum_n \omega_d^{(n)} (a^\dagger a - \frac{1}{2} \sum_i \sigma_{zi})
\end{aligned}$$

---

En caso de un sólo drive:

$$\begin{aligned}
\hat{H} &= \Delta_c a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i}) + (a\xi^* + a^\dagger \xi) \\
\Delta_c &= \omega_c - \omega_d \quad \Delta_{qi} = \omega_{qi} - \omega_d
\end{aligned}$$

## A.5. Efecto del pulso sobre el qubit

Luego se aplica el operador de desplazamiento  $D(\alpha) = \exp[\alpha a^\dagger - \alpha^* a]$  sobre el campo  $a$  con  $\dot{\alpha} = -i\Delta_c \alpha - i\xi$  para eliminar el efecto directo del pulso sobre la cavidad.

$$\hat{H} = D^\dagger(\alpha) \hat{H}_{old} D(\alpha) - iD^\dagger(\alpha) \dot{D}(\alpha)$$

---


$$\hat{H} = \Delta_c a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^\dagger \sigma_{-i}) + (a\xi^* + a^\dagger \xi)$$

$$\begin{aligned}
\hat{H} &= \Delta_c (a^\dagger + \alpha^*)(a + \alpha) - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i ((a + \alpha)\sigma_{+i} + (a^\dagger + \alpha^*)\sigma_{-i}) \\
&+ ((a + \alpha)\xi^* + (a^\dagger + \alpha^*)\xi) - i(\dot{\alpha}(a^\dagger + \alpha^*) - \dot{\alpha}^*(a + \alpha))
\end{aligned}$$

---


$$\begin{aligned}\hat{H} = & \Delta_c a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) \\ & + \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) - \Delta_c \alpha \alpha^*\end{aligned}$$

El término  $-\Delta_c \alpha \alpha^*$  se desprecia, ya que sólo representa una fase global en la evolución del sistema.

## A.6. Régimen dispersivo

Finalmente, aplicamos la transformación  $U = \exp[\sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})]$ , donde  $\Delta_i = \omega_{qi} - \omega_c$  y realizamos la expansión de Baker-Campbell-Hausdorff de segundo grado sobre los términos  $\frac{g_i}{\Delta_i} \ll 1$ .

$$\hat{H} = U^\dagger \hat{H}_{old} U$$

---


$$\begin{aligned}[\sigma_+, \sigma_z] &= 2\sigma_+ \\ [\sigma_-, \sigma_z] &= -2\sigma_- \\ [\sigma_-, \sigma_+] &= \sigma_z \\ [a, a^\dagger] &= 1 \\ [a, a^\dagger a] &= a \\ [a^\dagger, a^\dagger a] &= -a^\dagger\end{aligned}$$

$$\begin{aligned}\hat{H} = & \Delta_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) \\ & + \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i})\end{aligned}$$

$$\begin{aligned}[\Delta_r a^\dagger a, \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})] &= \Delta_r \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} + a \sigma_{+i}) \\ [-\frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi}, \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})] &= -\sum_i \frac{g_i}{\Delta_i} \Delta_{qi} (a^\dagger \sigma_{-i} + a \sigma_{+i}) \\ [\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j} - a \sigma_{+j})] &= [\sum_i g_i (a \sigma_{+i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j})] + \\ [\sum_i g_i (a \sigma_{+i}), \sum_j \frac{g_j}{\Delta_j} (-a \sigma_{+j})] + [\sum_i g_i (a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j})] &+ [\sum_i g_i (a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (-a \sigma_{+j})] = \\ \sum_{ij} g_i (a \sigma_{+i}) \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j}) - \sum_{ij} \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j}) g_i (a \sigma_{+i}) + \sum_{ij} g_i (a^\dagger \sigma_{-i}) \frac{g_j}{\Delta_j} (-a \sigma_{+j}) &- \sum_{ij} \frac{g_j}{\Delta_j} (-a \sigma_{+j}) g_i (a^\dagger \sigma_{-i}) =\end{aligned}$$

$$\begin{aligned}
& \sum_{ij} g_i \frac{g_j}{\Delta_j} a a^\dagger \sigma_{+i} \sigma_{-j} - \sum_{ij} g_i \frac{g_j}{\Delta_j} a^\dagger a \sigma_{-j} \sigma_{+i} - \sum_{ij} g_i \frac{g_j}{\Delta_j} a^\dagger a \sigma_{-i} \sigma_{+j} + \sum_{ij} g_i \frac{g_j}{\Delta_j} a a^\dagger \sigma_{+j} \sigma_{-i} = \\
& 2 \sum_{i \neq j} g_i \frac{g_j}{\Delta_j} \sigma_{+i} \sigma_{-j} + \sum_i g_i \frac{g_i}{\Delta_i} \sigma_{+i} \sigma_{-i} + \sum_i g_i \frac{g_i}{\Delta_i} \sigma_{+i} \sigma_{-i} - 2 \sum_i g_i \frac{g_i}{\Delta_i} a^\dagger a \sigma_{zi} = \\
& - [\sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j} - a \sigma_{+j})] = [\sum_i g_i (a \sigma_{+i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j})] + \\
& [\sum_i g_i (a \sigma_{+i}), \sum_j \frac{g_j}{\Delta_j} (-a \sigma_{+j})] + [\sum_i g_i (a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (a^\dagger \sigma_{-j})] + [\sum_i g_i (a^\dagger \sigma_{-i}), \sum_j \frac{g_j}{\Delta_j} (-a \sigma_{+j})] \\
& \sum_{i \neq j} g_i \frac{g_j}{\Delta_j} \sigma_{+i} \sigma_{-j} + \sigma_{-i} \sigma_{+j} \\
& \sum_i g_i \frac{g_i}{\Delta_i} (a a^\dagger \sigma_{+i} \sigma_{-i} - a^\dagger a \sigma_{-i} \sigma_{+i}) = 2 \sum_i g_i \frac{g_i}{\Delta_i} (a a^\dagger \sigma_{+i} \sigma_{-i} - a^\dagger a \sigma_{zi} + \\
& \sigma_{+i} \sigma_{-i}) = 2 \sum_i g_i \frac{g_i}{\Delta_i} (\sigma_{+i} \sigma_{-i} - a^\dagger a \sigma_{zi}) = \\
& 2 \sum_i g_i \frac{g_i}{\Delta_i} (a a^\dagger \sigma_{+i} \sigma_{-i} - a^\dagger a \sigma_{-i} \sigma_{+i}) = 2 \sum_i g_i \frac{g_i}{\Delta_i} ((a a^\dagger + 1/2 - 1/2) \sigma_{+i} \sigma_{-i} - \\
& (a^\dagger a + 1/2 - 1/2) \sigma_{-i} \sigma_{+i}) = \sum_i g_i \frac{g_i}{\Delta_i} (\sigma_{+i} \sigma_{-i} + \sigma_{-i} \sigma_{+i}) - 2 \sum_i g_i \frac{g_i}{\Delta_i} (a^\dagger a + \\
& 1/2) \sigma_{zi} = \sum_i (g_i \frac{g_i}{\Delta_i} - 2g_i \frac{g_i}{\Delta_i} (a^\dagger a + 1/2) \sigma_{zi}) - \\
& [\sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}), \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} - a \sigma_{+i})] = [\sum_i g_i (\alpha \sigma_{+i}), \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i})] + \\
& [\sum_i g_i (\alpha^* \sigma_{-i}), \sum_i \frac{g_i}{\Delta_i} (-a \sigma_{+i})] = - \sum_i g_i \frac{g_i}{\Delta_i} (\alpha a^\dagger + \alpha^* a) \sigma_{zi} \\
& \hat{H} = \Delta_r a^\dagger a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) + \\
& \Delta_r \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} + a \sigma_{+i}) - \sum_i \frac{g_i}{\Delta_i} \Delta_{qi} (a^\dagger \sigma_{-i} + a \sigma_{+i}) + \sum_{i \neq j} g_i \frac{g_j}{\Delta_j} \sigma_{+i} \sigma_{-j} + \sigma_{-i} \sigma_{+j} + \\
& \sum_i (g_i \frac{g_i}{\Delta_i} - 2g_i \frac{g_i}{\Delta_i} (a^\dagger a + 1/2) \sigma_{zi}) - \sum_i g_i \frac{g_i}{\Delta_i} (\alpha a^\dagger + \alpha^* a) \sigma_{zi} \\
& \hat{H} = \Delta_r a^\dagger a - \sum_i \Delta_{qi} (1/2 + 2g_i \frac{g_i}{\Delta_i} (a^\dagger a + 1/2)) \sigma_{zi} + \sum_i g_i (a \sigma_{+i} + a^\dagger \sigma_{-i}) + \\
& \Delta_r \sum_i \frac{g_i}{\Delta_i} (a^\dagger \sigma_{-i} + a \sigma_{+i}) - \sum_i \frac{g_i}{\Delta_i} \Delta_{qi} (a^\dagger \sigma_{-i} + a \sigma_{+i}) + \sum_{i \neq j} g_i \frac{g_j}{\Delta_j} \sigma_{+i} \sigma_{-j} + \sigma_{-i} \sigma_{+j} + \\
& \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) - \sum_i g_i \frac{g_i}{\Delta_i} (\alpha a^\dagger + \alpha^* a) \sigma_{zi} \\
& \hat{H} = \Delta_r a^\dagger a - \sum_i \Delta_{qi} (\frac{1}{2} + 2 \frac{g_i^2}{\Delta_i} (a^\dagger a + \frac{1}{2})) \sigma_{zi} + \sum_{i \neq j} \frac{g_i g_j}{\Delta_j} (\sigma_{+i} \sigma_{-j} + \sigma_{-i} \sigma_{+j}) + \\
& \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) - \sum_i \frac{g_i^2}{\Delta_i} (\alpha a^\dagger + \alpha^* a) \sigma_{zi} \text{ —————} \\
& \hat{H} \approx \tilde{\Delta}_c a^\dagger a - \frac{1}{2} \sum_i \tilde{\Delta}_{qi} \sigma_{zi} + \sum_i (\Omega_i \sigma_{+i} + \Omega_i^* \sigma_{-i}) \\
& + \sum_{i \neq j} \frac{g_i g_j}{2 \Delta_i} (\sigma_{-i} \sigma_{+j} + \sigma_{+i} \sigma_{-j})
\end{aligned}$$

$$\tilde{\Delta}_c = (\omega_c + \sum_i \chi_i \sigma_{zi}) - \omega_d \quad \tilde{\Delta}_{qi} = (\omega_{qi} + \chi_i) - \omega_d \quad \chi_i = \frac{g_i^2}{\Delta_i}$$

## A.7. Rotaciones X-Y

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

---


$$\Omega \sigma_+ + \Omega^* \sigma_-$$

$$e^{i(x+\pi/2)} - e^{-i(x+\pi/2)} = e^{i\pi/2} e^{ix} - e^{-i\pi/2} e^{-ix} = e^{i\pi/2} e^{ix} + e^{i\pi} e^{-i\pi/2} e^{-ix} = e^{i\pi/2} e^{ix} + e^{i\pi/2} e^{-ix} = e^{i\pi/2} (e^{ix} + e^{-ix})$$

---


$$\hat{H} \approx \tilde{\Delta}_c a^\dagger a + \frac{1}{2} \tilde{\Delta}_q \sigma_z + \frac{1}{2} (\Omega^x(t) \sigma_x + \Omega^y(t) \sigma_y)$$

## A.8. Compuerta de entrelazamiento

Ejemplo con sólo dos qubits

$$\hat{H} \approx \frac{1}{2} \tilde{\Delta}_{q_1} \sigma_{z_1} + \frac{1}{2} \tilde{\Delta}_{q_2} \sigma_{z_2} + \frac{g_1 g_2 (\Delta_1 + \Delta_2)}{2 \Delta_1 \Delta_2} (\sigma_{-1} \sigma_{+2} + \sigma_{+1} \sigma_{-2})$$

Variando la frecuencia de resonancia de los qubit, se puede variar el acoplamiento entre estos.

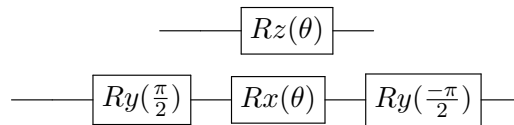
## Apéndice B

# Cálculos de matrices de adyacencia

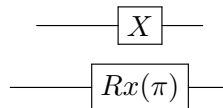
## Apéndice C

# Circuitos cuánticos

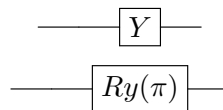
Rotaciones en Z:



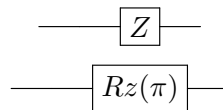
Compuerta X:



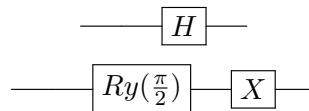
Compuerta Y:



Compuerta Z:

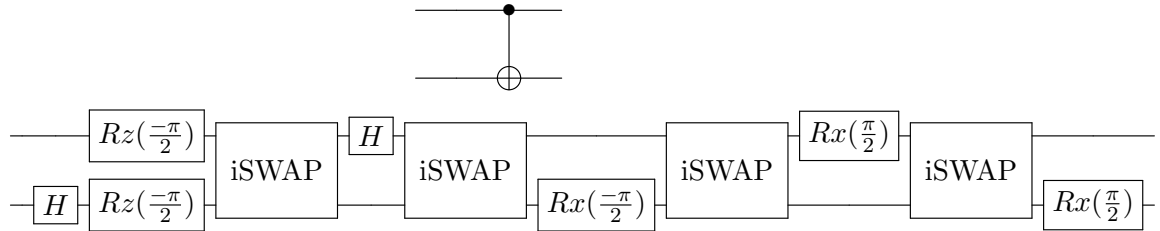


Compuerta H:



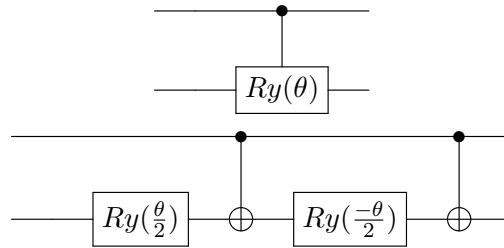


Compuerta CNOT:

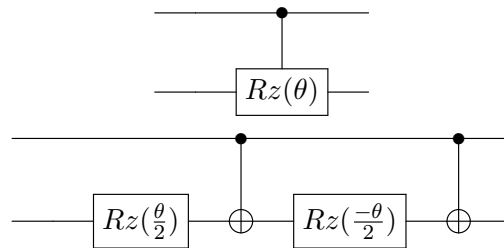


Compuerta CRy:

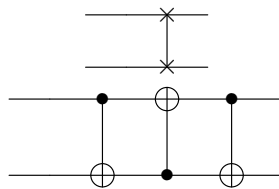
Tomado del paper de Barenco [1]



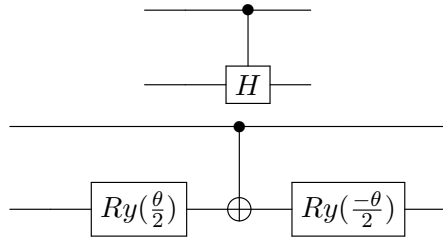
Compuerta CRz:



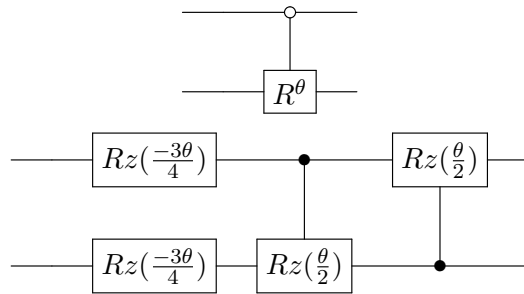
Compuerta SWAP:



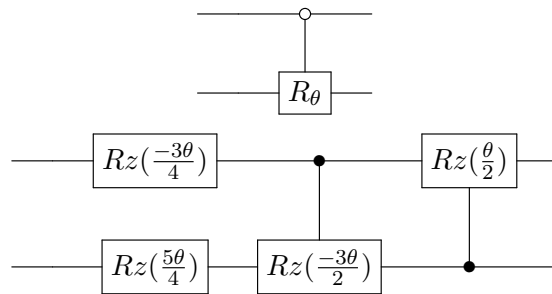
Compuerta CH:



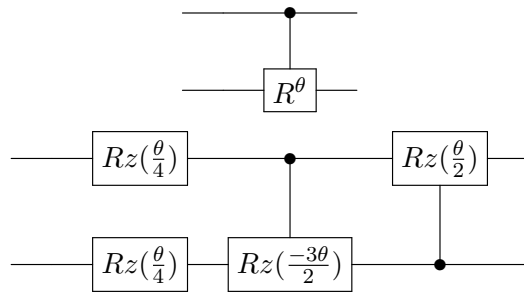
Compuerta  $CR^\theta$  blanca:



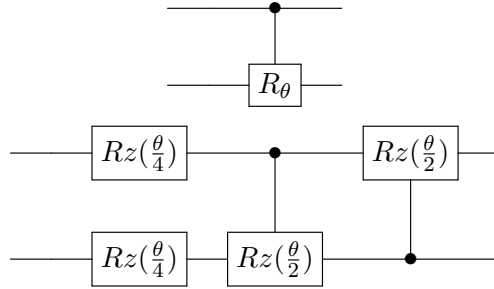
Compuerta  $CR_\theta$  blanca:



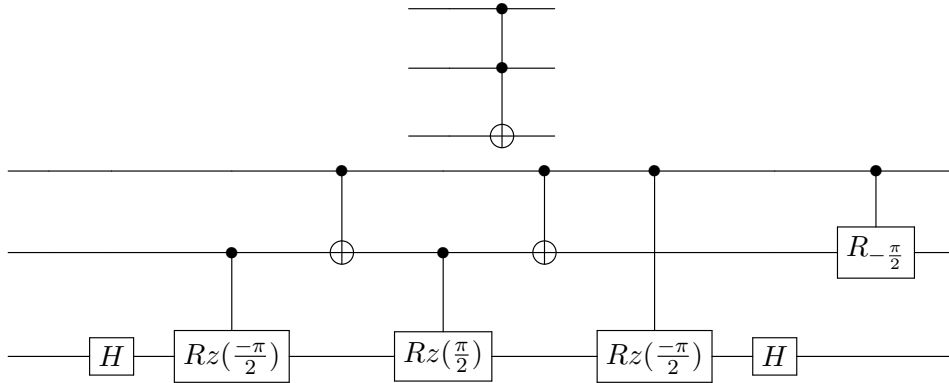
Compuerta  $CR^\theta$  negra:



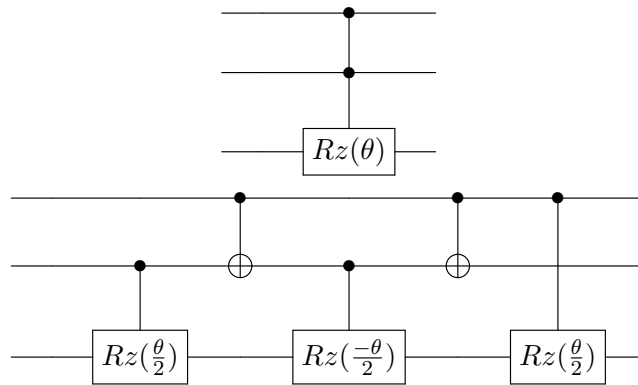
Compuerta  $CR_\theta$  negra:



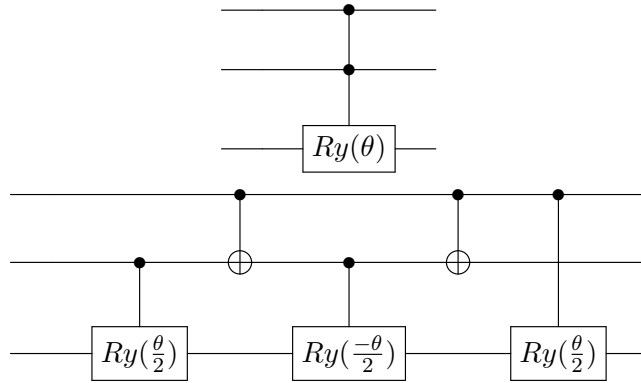
Compuerta de Toffoli (CCNOT):



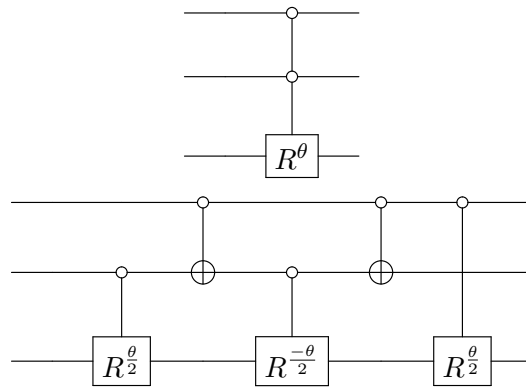
Compuerta CCRz:



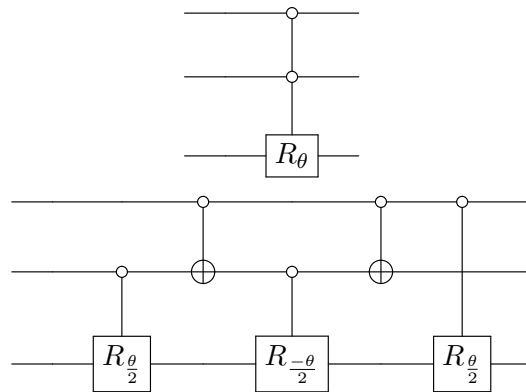
Compuerta CCRy:



Compuerta  $CCR^\theta$  blanca:

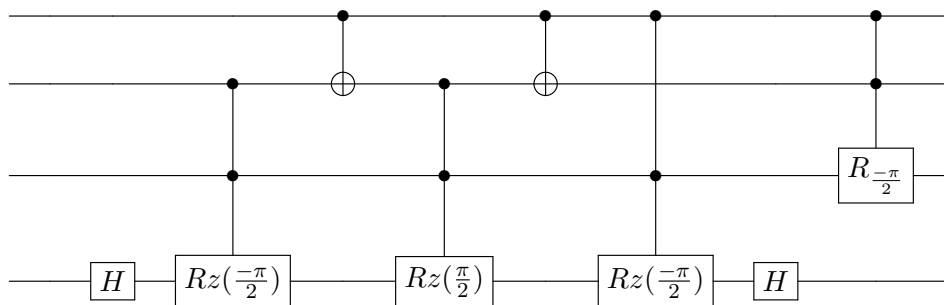


Compuerta  $CCR_\theta$  blanca:

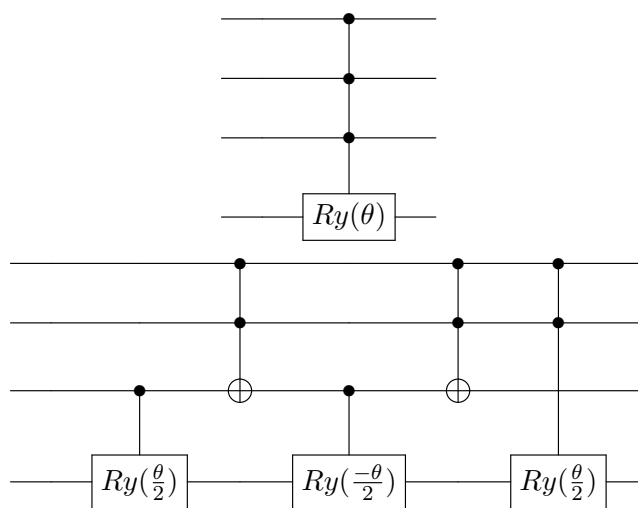


Compuerta  $CCR^\theta$  negra:

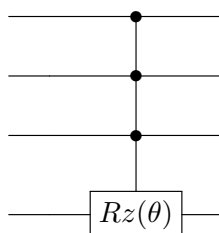


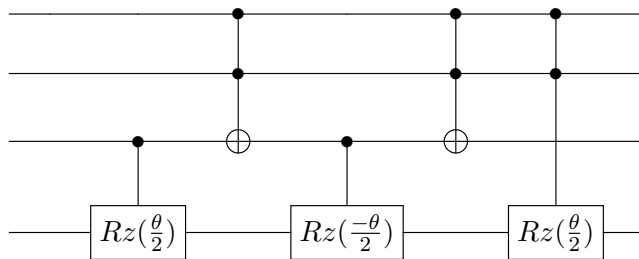


Compuerta CCCRy:

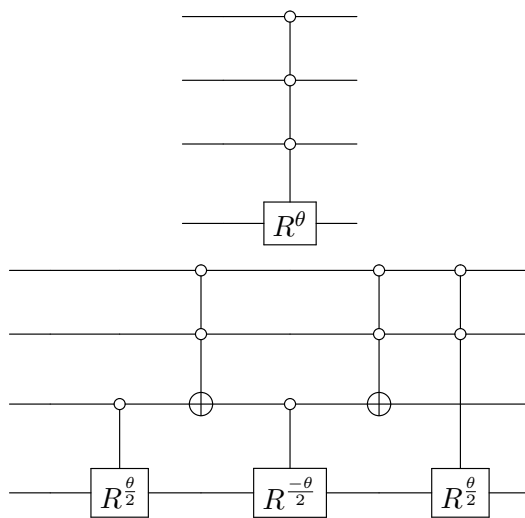


Compuerta CCCRz:

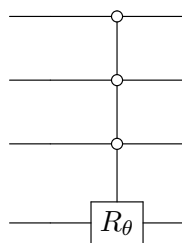


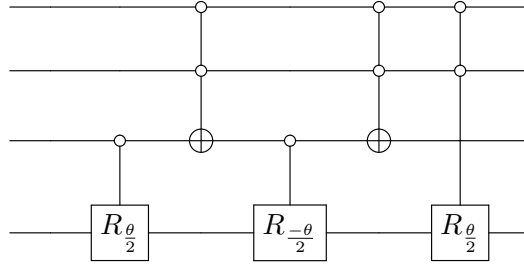


Compuerta  $CCCR^\theta$  blanca:

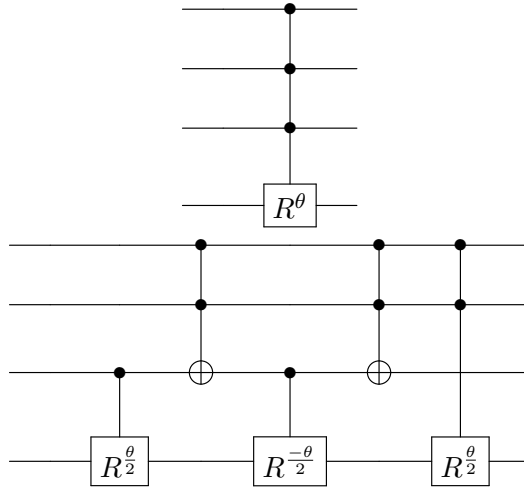


Compuerta  $CCCR_\theta$  blanca:

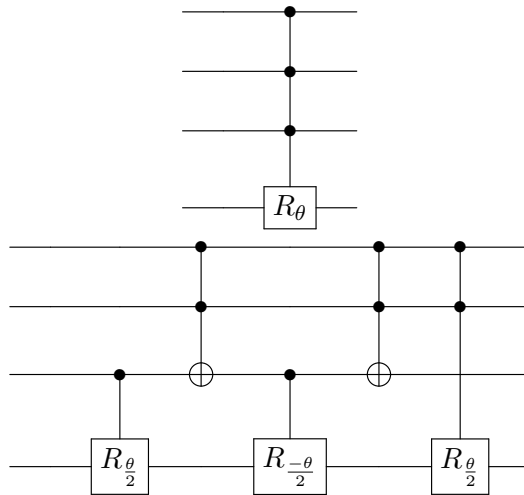




Compuerta  $CCCR^\theta$  negra:



Compuerta  $CCCR_\theta$  negra:





# 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.