# Diseño y simulación de procesadores cuánticos que implementen algoritmos cuánticos de busqueda

#### Miguel Casanova

Coordinación de Tecnología e Ingeniería Electrónica Universidad Simón Bolívar

16 de enero de 2019

#### Estructura de la presentación

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

# Objetivo General

Diseñar y simular procesadores cuánticos (PC) que implementen los algoritmos cuánticos (AC) de Grover, Shor y PageRank Cuántico (Google Cuántico).

# Objetivos Específicos

- Construir la representación circuital cuántica de los AC de Grover, Shor y de Google Cuántico.
- Estudiar la dinámica de arquitecturas superconductoras controlables por microondas basadas en transmones.
- Precisar la dinámica de secuencias de pulsos necesarios para generar con transmones la compuertas cuánticas necesarias para los AC considerados.
- Simular en Mathematica, de forma algebraica, cada una de las arquitecturas de CC considerados.
- Simular en Python, de forma numérica, con y sin decoherencia cuántica, el operador evolución de cada una de los compuertas de los CC estudiados.
- © Comparar los casos con y sin decoherencia cuántica, para cada uno de los AC estudiados, en base a los resultados obtenidos de las simulaciones numéricas y algebraicas.

#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

# Espacios de Hilbert

Un espacio de Hilbert es un espacio lineal real o complejo con un producto interno que también define un espacio normado completo.

- Producto interno
- Normado
- © Completo: Todas las sucesiones de Cauchy convergen fuertemente. Las sucesiones de Cauchy son aquellas en las que el ordenamiento no afecta la convergencia.
- $\blacksquare$  Separable: Tiene bases discretas, ortonormales y contables (Tiene dimensión comparable a  $\mathbb N).$

# Operadores

- **1** Operadores hermíticos:  $U = U^{\dagger}$ 
  - 1 Autovalores reales
  - Diagonal real
  - 3 Diagonalizable
- 2 Operadores unitarios:  $UU^{\dagger} = 1$ 
  - 1 Determinante de módulo igual a la unidad
  - Preserva normas y trazas
  - $oldsymbol{3}$  Diagonalizable

La QM que fundamenta la teoría de información cuántica se describe formalmente con los siguientes postulados desarrollados por la escuela de Copenhague a lo largo de todo el siglo XX [1]

- **I** En un tiempo fijo  $t_0$ , el estado está dado por el ket  $|\psi(t_0)\rangle$ , perteneciente al espacio de Hilbert  $\mathcal{H}$ .
- $\mathbf{Z}$  Toda cantidad física  $\mathcal{A}$ , que se pueda medir, está descrita por un operador hermítico  $\hat{A}$ . Este operador es un observable.
- El único resultado posible de una medida de la cantidad física  $\mathcal{A}$  es alguno de los autovalores del observable correspondiente  $\hat{A}$ .
- I Si un sistema en el estado normalizado  $|\psi\rangle$ , la probabilidad de obtener un valor  $\lambda$  al medir un observable  $\mathcal A$  está dada por

$$p(\lambda) = \sum_{i}^{g_n} |\langle \lambda_i | \psi \rangle|^2 \tag{1}$$

Donde  $g_n$  es el grado de degeneración de  $\hat{A}$  en  $\lambda$ ,  $|\lambda_i\rangle$  son los autoestados asociados a  $\lambda$  y el proyector  $\Pi_{\lambda}$  es  $\Pi_{\lambda} = \sum_{i=1}^{g_n} |\lambda_i\rangle\langle\lambda_i|$ .

#### Postulados de la mecánica cuántica

si Si un sistema físico está en el estado  $|\psi\rangle$ , el estado resultante luego de una medida ideal del observable  $\mathcal A$  está dado por

$$|\psi\rangle \to \frac{\Pi_{\lambda} |\psi\rangle}{\sqrt{\langle\psi|\Pi_{\lambda}|\psi\rangle}}$$
 (2)

 $\mbox{\fontfamily La evolución temporal del estado} \ |\psi(t)\rangle$  está dada por la ecuación de Schrödinger

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H}(t) |\psi(t)\rangle$$
 (3)

#### Estados puros y mixtos

Las mezclas estadísticas de estados cuánticos, también son estados cuánticos.

- $\blacksquare$  Estados puros: representados en base al ket  $|\psi\rangle$  o a la matriz densidad  $\rho=|\psi\rangle\!\langle\psi|.$ 
  - I Normalizado:  $\langle \psi | \psi \rangle = \int_{-\infty}^{\infty} |\psi(r)|^2 dV = 1$
  - **2** Traza igual a la unidad:  $Tr(\rho) = Tr(\rho^2) = 1$
- **2** Estados mixtos: representados por  $\rho = \sum_i p_i \rho_i$ , siendo  $\rho_i = |\psi_i\rangle\langle\psi_i|$ .
  - Matriz hermítica
  - 2 Traza igual a la unidad
  - 3 Autovalores no negativos
  - I Traza:  $Tr(\rho^2) < 1$

Para estados mixtos se utiliza la ecuación de Liouville-von Neumann.

$$i\hbar\dot{\rho}(t) = [\hat{H}, \rho(t)]$$
 (4)

# Sistemas multipartitos

Cuando se tiene más de un espacio de Hilbert, el sistema global se forma con el producto tensorial

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \tag{5}$$

$$|\psi,\phi\rangle = |\psi\rangle \otimes |\phi\rangle = |\psi\rangle_A \otimes |\phi\rangle_B \tag{6}$$

$$\rho_{AB} = \rho_A \otimes \rho_B \quad \text{(Estado producto)} \tag{7}$$

$$\rho_{AB} \neq \rho_A \otimes \rho_B$$
 (Estado entrelazado) (8)

Siendo  $\rho_A$  y  $\rho_B$ , la traza parcial de las particiones que conforman la matriz  $\rho_{AB}$  en el espacio de Hilbert  $\mathcal H$ 

$$\rho_A = Tr_B(\rho_{AB}) \tag{9}$$

$$\rho_B = Tr_A(\rho_{AB}) \tag{10}$$

#### Sistemas cuánticos abiertos

En la mecánica cuántica de sistemas abiertos con evolución markoviana (la evolución sólo depende del estado actual y de propiedades del sistema, no de estados pasados), la ecuación de Schrödinger toma la siguiente forma más general, conocida como Lindbladiano.

$$\dot{\rho}(t) = -i[\hat{H}, \rho(t)] + \sum_{k} \gamma_{k} [V_{k}\rho(t)V_{k}^{\dagger} - \frac{1}{2} \{V_{k}^{\dagger}V_{k}, \rho(t)\}]$$
 (11)

Los operadores  $V_k$  son operadores de colapso y ellos representan el tipo de interacción que hay entre el sistema y su entorno.

# Qubits y esfera de Bloch

Los qubits son la unidad básica de información cuántica y se suelen representar en una esfera imaginaria unitaria conocida como esfera de Bloch.

$$|0\rangle = \begin{pmatrix} 1\\0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0\\1 \end{pmatrix}$$
 (12)

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \alpha, \beta \in \mathbb{C}$$
 (13)

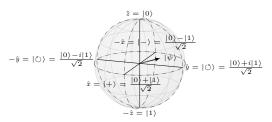


Figura: Esfera de Bloch

#### Matrices de Pauli

Estos son los operadores asociados al espín de un fermión.

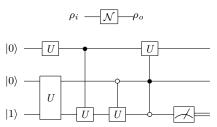
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{14}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{15}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{16}$$

Los exponenciales  $e^{i\sigma_a},\ a\in\{x,y,z\},$  forman una base en SU(2).

Una compuerta cuántica es una operación unitaria que mapea un estado de entrada en un estado de salida, definido por  $\rho_o = \mathcal{N}(\rho_i)$ .



■ Compuerta identidad

$$-I$$

Compuerta X

**3** Compuerta Z

$$Z$$
 $-$ 

Compuerta Y

$$\overline{\phantom{a}}$$

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

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

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

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ Y = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Compuerta de Hadamard

$$-H$$

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

2 Compuerta de cambio de fase

$$P_{\phi}$$

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

3 Compuertas de rotación

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

 $\blacksquare$ Rotación en X

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

Rotación en Y

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

Rotación en Z

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

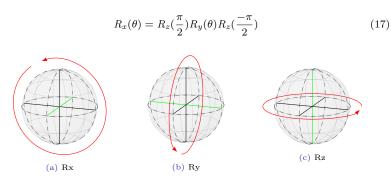
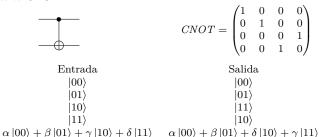


Figura: Compuertas Rx, Ry y Rz en la esfera de Bloch

#### ■ Compuerta CNOT



■ Compuerta SWAP



Compuerta SWAP



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

$$iSW\!AP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

■ Compuerta de Toffoli



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

#### Criterios de Di Vincenzo

Di Vincenzo propuso los siguientes criterios para la construcción de un computador cuántico:

- Un sistema físico escalable con qubits caracterizados.
- Za habilidad de inicializar el estado de los qubits en un estado fiducial simples. Un estado fiducial es un estado cuántico que se puede preparar consistentemente.
- 3 Tiempos de coherencia relevantemente largos.
- Un conjunto universal de compuertas cuánticas.
- 5 La capacidad de medir qubits específicos.

#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

#### Teorías BCS

- Los electrones cercanos al nivel de Fermi se acoplan en pares, debido a la interacción con la red cristalina. Esta interacción es una interacción atractiva electrón-fonón-electrón.
- Los pares de Cooper se comportan de una manera distinta a los electrones individuales.
- Existe una banda de energía, la cual inhibe las interacciones de colisión que causan la resistencia eléctrica, siempre que la energía térmica sea menor a la banda prohibida.

#### Efecto Josephson

Una unión de Josephson está formada por dos placas superconductoras A y B, separadas por un aislante. Las funciones de onda de las placas superconductoras son:  $\psi_A = \sqrt{\rho_1}e^{i\phi_1}$ ,  $\psi_B = \sqrt{\rho_2}e^{i\phi_2}$ 



Figura: Unión Josephson [2]

Por el efecto tunel, una supercorriente (corriente sin disipación) de pares de Cooper pueden pasar de una placa a la otra sin disipación.

$$V_J = \frac{\hbar}{2e} \frac{d\delta}{dt} \tag{18}$$

$$I_J = I_0 \sin(\delta) \tag{19}$$

Donde  $\delta = \phi_2 - \phi_1$  es la diferencia de fase entre las dos placas superconductoras.

# Efecto Josephson DC y AC

- Efecto Josephson DC Si las placas se encuentran sin alimentación, entonces correrá una supercorriente constante a través de ellas.
- Efecto Josephson AC Si las placas se alimentan con un voltaje DC externo, entonces la diferencia de fase entre ellas variará linealmente con el tiempo y habrá una corriente AC a través de ellas.

# Qubits superconductores

Los qubits superconductores se basan en circuitos osciladores no lineales, hechos a partir de junciones Josephson. En general, estos son circuitos LCJ, es decir, un inductor (L), un condensador (C) y una unión Josephson (J) en paralelo.

$$\begin{bmatrix} n_g & & & & \\ & & & & \\ C & & & & \\ E_c & & & E_I \end{bmatrix} \begin{bmatrix} \phi_e & & & \\ & \phi_e & & & \\ & & & & \\ E_I & & \\ E_I & & & \\ E_I & & \\ E_I & & & \\ E_I & & \\ E_$$

Figura: Circuito LCJ [3]

Dependiendo de la variable de este circuito que se utilice como qubit, los qubits superconductores se pueden clasificar en qubits de carga, de flujo y de fase. Los transmones son un tipo de qubit de carga derivado capacitivamente para hacerlo insensible a las fluctuaciones de carga.

# Qubits de carga

En estos qubits,  $L\to\infty$  y la variable de interés es la carga en la isla superconductora que se forma entre el condensador y la unión Josephson.

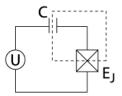


Figura: Caja de pares de Cooper [4]

Dimensiones típicas de la isla:  $1000 \mathrm{nm} \ge 50 \mathrm{nm} \ge 20 \mathrm{nm}$ . A la isla también se le conoce como caja de pares de Cooper.

# Caja de pares de Cooper

El Hamiltoniano de este sistema toma la forma

$$\hat{H} = E_C(\hat{n} - n_g)^2 - E_{J0}\cos(\hat{\phi})$$
(20)

Donde 
$$E_{J0} = \frac{\hbar}{2e} I_0 \text{ y } E_C = \frac{(2e)^2}{2C}.$$

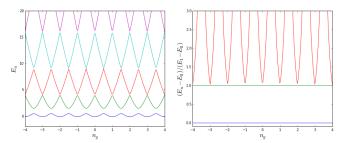


Figura: Niveles de energía de una caja de pares de Cooper

#### Transmon

Intercambiamos anarmonicidad por independencia de  $n_g$ haciendo  $\frac{E_{J0}}{E_C} \geq 50.$ 

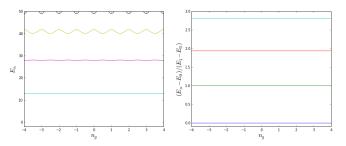


Figura: Niveles de energía de un transmon

# Modelo de Jaynes-Cummings

Para controlar los transmones y para acoplar distintos transmones, estos se conectan a un resonador. El sistema resonador-transmon tiene el mismo comportamiento que el sistema cavidad-átomo. Así que podemos utilizar el modelo de Jaynes-Cummings.

$$\hat{H} = \hat{H}_c + \hat{H}_q + \hat{H}_{qc} = \omega_c a^{\dagger} a + \frac{1}{2} \sum_i \omega_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^{\dagger} \sigma_{-i})$$
 (21)

De ahora en adelante  $\hbar=1$  y despreciaré los términos constantes, pues sólo contribuyen en fases globales a la evolución del sistema.

#### Pulsos de microondas

Para controlar los qubits se aplican pulsos de microondas al resonador.



Figura: Transmon [3]

La frecuencia de la portadora del pulso será la frecuencia de resonancia del qubit sobre el que se quiera operar.

$$\hat{H}_d = a \, \xi^* e^{i\omega_d t} + a^\dagger \, \xi e^{-i\omega_d t} \tag{22}$$

#### Hamiltoniano efectivo

Régimen rotativo del pulso: Trasladamos el sistema en frecuencia tal que la frecuencia del pulso esté en cero. Esto se realiza aplicando la siguiente transformación unitaria al Hamiltoniano

$$U(t) = \exp\left[-i\omega_d t (a^{\dagger} a + \sum_i \sigma_{zi})\right]$$
 (23)

Efecto del pulso sobre el qubit: Centramos la distribución de probabilidad del resonador en el origen del espacio de fase, para que el Hamiltoniano refleje la interacción pulso-qubit de manera directa. Esto se realiza aplicando el operador desplazamiento  $D(\alpha)$  al sistema con  $\dot{\alpha}=-i\Delta_c\alpha-i\xi\,e^{-i\omega_dt}$ , donde  $\Delta_r=\omega_r-\omega_d$ 

$$D(\alpha) = \exp\left[\alpha a^{\dagger} - \alpha^* a\right] \tag{24}$$

#### Hamiltoniano efectivo

Régimen dispersivo: Consideramos el caso en que la diferencia entre las frecuencias de resonancia de los qubits y el resonador son mucho mayores que sus constantes de acoplamiento. Esto se realiza aplicando la siguiente transformación unitaria al Hamiltoniano y aproximando con  $\frac{g_i}{\Delta_i} \ll 1$ , donde  $\Delta_i = \omega_{qi} - \omega_c$ 

$$U = \exp\left[\sum_{i} \frac{g_i}{\Delta_i} (a^{\dagger} \sigma_{-i} - a \sigma_{+i})\right]$$
 (25)

Luego de aplicar estas transformaciones, el Hamiltoniano efectivo del sistema es el siguiente  $\,$ 

$$\hat{H}_{eff} = \tilde{\Delta}_r a^{\dagger} a - \frac{1}{2} \sum_i \Delta_{qi} \sigma_{zi} + \sum_i g_i (a\sigma_{+i} + a^{\dagger} \sigma_{-i}) + \sum_i g_i (\alpha \sigma_{+i} + \alpha^* \sigma_{-i}) + \sum_{ij} \frac{g_i g_j}{2\Delta_j} \left( \sigma_{+i} \sigma_{-j} + \sigma_{+j} \sigma_{-i} \right), \quad (26)$$

# 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.

$$\hat{H}_{XY} = \frac{1}{2} (\Omega^x(t)\sigma_x + \Omega^y(t)\sigma_y)$$
 (27)

### Compuerta de entrelazamiento

Variando la frecuencia de resonancia de dos de los qubits, tal que  $\Delta_1 = \Delta_2 = \Delta$ , la interacción entre estos dos qubits es máxima. Esta interacción permite realizar las compuertas  $\sqrt{iSWAP}$  e iSWAP. Sea  $J = \frac{g_1g_2}{\Delta}$ , el término correspondiente del Hamiltoniano toma la siguiente forma

$$\hat{H}_{q_1 q_2} = \left(\frac{g_1 g_2}{2\Delta_1} + \frac{g_1 g_2}{2\Delta_2}\right) (\sigma_{-1} \sigma_{+2} + \sigma_{+1} \sigma_{-2}) = J(\sigma_{-1} \sigma_{+2} + \sigma_{+1} \sigma_{-2}). \tag{28}$$

#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

#### Parámetros de los sistemas simulados

- Frecuencias de resonancia:
  - Resonador: 10 GHz
  - ${\color{red} {\bf 2}}$  Qubit 0: 5 GHz
  - 3 Qubit 1: 6 GHz
  - 4 Qubit 2: 7 GHz
  - ${\color{red} {\bf 5}}$  Qubit 3: 8 GHz
  - 6 \*Qubit 4: 11 GHz
  - \*Qubit 5: 12 GHz
  - 8 \*Qubit 6: 13 GHz
  - \*Qubit 7: 14 GHz
- ${\bf 2}$  Constante de acoplamiento: Todas iguales a 0.1 GHz
- 3 Tasas de relajación: Todas iguales a 25 KHz
- $\blacksquare$  Tiempo de relajación: Todos iguales a  $40\mu s$
- 5 Frecuencia de resonancia para iSWAP: 9 GHz

<sup>\*</sup>Sólo aplica para el caso del sistema de 8 qubits

### Compuertas nativas

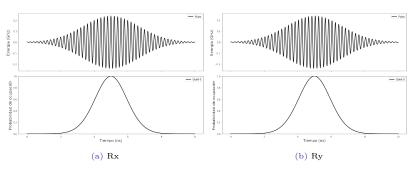


Figura: Rotaciones en X e Y de  $2\pi$ 

### Compuertas nativas

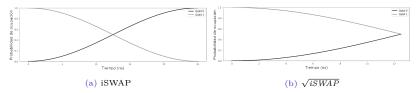
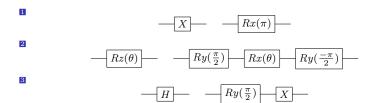
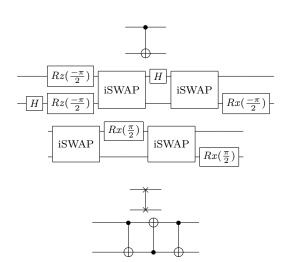


Figura: Compuertas iSWAP y  $\sqrt{iSWAP}$  aplicadas a  $|01\rangle$ 



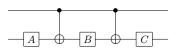


|2|





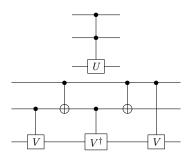
De la siguiente manera

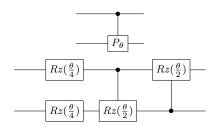


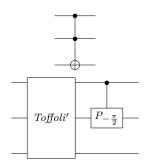
Donde A, B y C deben cumplir las siguentes dos condiciones

$$CXBXA = U (29)$$

$$CBA = 1. (30)$$







#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

# Algoritmo de Grover

El algoritmo de Grover [5], 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 [5]. 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.

## Operadores de reflexión

El fundamento del algoritmo de Grover es el hecho de la geometría plana de que dos reflexiones consecutivas generan una rotación. Le asignamos un ket a cada entrada de la base de datos en la que se realizará la búsqueda, de manera que el primer operador de reflexión será alrededor del estado de la entrada deseada

$$U_{\omega} |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} |x\rangle & \text{si } x \neq \omega \\ -|x\rangle & \text{si } x = \omega \end{cases} : U_{\omega} = \mathbb{1} - 2 |\omega\rangle\langle\omega|$$
 (31)

El segundo operador de reflexión es alrededor del estado de superposición

uniforme 
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$
  $U_s = 2 |s\rangle\langle s| - 1$  (32)

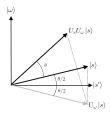


Figura: Interpretación geométrica del operador difusión

# Algoritmo de Grover

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

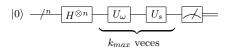


Figura: Circuito del algoritmo de Grover

- Algoritmo de amplificación de amplitud: Esta es una generalización del algoritmo de Grover, que permite utilizar un estado inicial genérico  $|\psi\rangle$  y bases de datos con más de un estado deseado  $|\omega\rangle$ .
- Algoritmo de Grover en un paso: En lugar de realizar repetidas iteraciones del algoritmo, se realiza una sóla iteración, pero se ejecuta el algoritmo en varios sistemas simultáneamente.
- Optimización del algoritmo de Grover: Se ejecuta el algoritmo en varios sistemas simultáneamente, pero se realizan varias iteraciones.

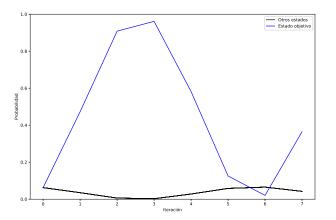


Figura: Wolfram Mathematica: Algoritmo de Grover sin relajación

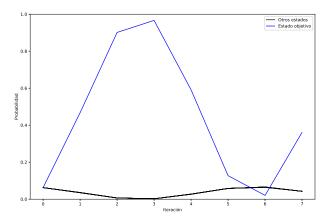


Figura: Python: Algoritmo de Grover sin relajación

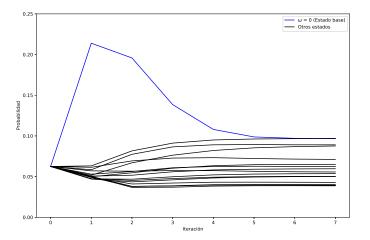
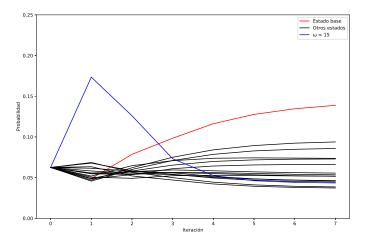


Figura: Algoritmo de Grover con relajación.  $\mathcal{W} = \{0\} = \{000\theta_2\}$ 



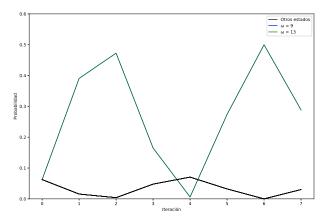


Figura: Wolfram Mathematica: Algoritmo de amplificación de amplitud sin relajación,  $\mathcal{W} = \{9,13\}$ 

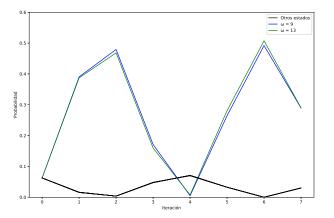


Figura: Python: Algoritmo de amplificación de amplitud sin relajación,  $W = \{9, 13\}$ 

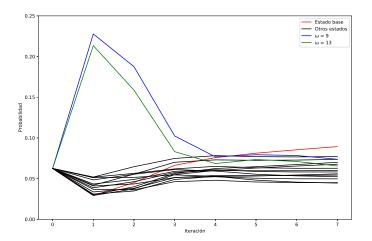


Figura: Algoritmo de amplificación de amplitud con relajación,  $\mathcal{W} \equiv \{9,13\}$ 

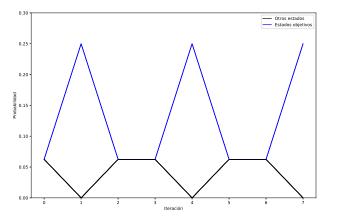


Figura: Wolfram Mathematica: Algoritmo de amplificación de amplitud sin relajación,  $\mathcal{W}=\{4,5,12,13\}=\{0100_2,0101_2,1100_2,1101_2\}$ 

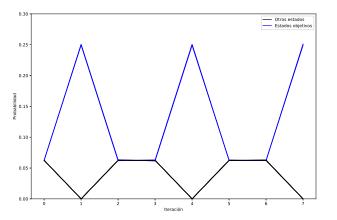


Figura: Python: Algoritmo de amplificación de amplitud sin relajación,  $\mathcal{W}=\{4,5,12,13\}=\{0100_2,0101_2,1100_2,1101_2\}$ 

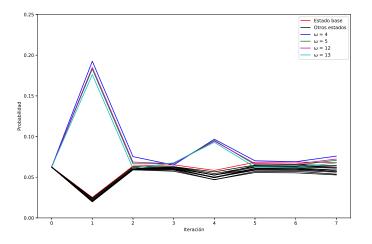


Figura: Algoritmo de amplificación de amplitud con relajación,  $W = \{4, 5, 12, 13\}$ 

#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

# Algoritmo de Shor

El algoritmo de Shor es un algoritmo cuántico de factorización de enteros. Dado un entero  $N=p\times q$ , donde p y q son primos, el algoritmo de Shor encuentra p y q en  $O((\log(N))^3)$  pasos, publicado en 1997 por Peter Shor [6]. El algoritmo clásico más eficiente para factorizar enteros es la cibra general del cuerpo de números y funciona con una complejidad heurística de  $O(e^{(\sqrt[3]{\frac{64}{9}}+o(1))(\ln(N))^{\frac{1}{3}}(\ln(\ln(N)))^{\frac{2}{3}}})$ .

y funciona con una complejidad heuristica de  $O(e^{v \cdot v})$ . Por su capacidad de factorizar números semiprimos, el algoritmo de Shor es capaz de violar el cifrado RSA [7, 8] y el protocolo Diffie-Hellman de intercambio de llaves, sobre los cuáles se basa virtualmente toda la criptografía actual.

El algoritmo de Shor está basado en el algoritmo de estimación de orden, el cuál es una aplicación del algoritmo de estimación de fase [9]. Éste último permite encontrar la fase  $\phi$  del autovalor  $e^{i\phi}$  asociado a algún autoestado  $|u\rangle$  de un operador unitario U. El algoritmo de estimación de orden utiliza esta estimación para hallar el orden r>0 tal que  $a^r\equiv 1\mod m$ , a partir del operador unitario de multiplicación modular.

#### Transformada cuántica de Fourier

Esta transformada es equivalente a la transformada discreta de Fourier, sólo que a cada frecuencia se le asigna un ket. Cuando un estado tiene una distribución periódica, esta transformada sirve para hallar el período de tal distribución. La ecuación y el circuito de la transformada inversa de Fourier son los siguientes:

$$QFT^{\dagger} = \frac{1}{\sqrt{N}} \sum_{x} \sum_{k} e^{-2\pi i k x/N} |x\rangle\langle k|$$

$$|k_{1}\rangle \qquad \qquad P_{-2\pi/2^{2}} \qquad P_{-2\pi/2^{3}} \qquad H$$

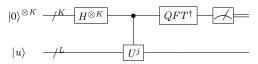
$$|k_{2}\rangle \qquad \qquad H$$

$$|k_{3}\rangle \qquad \qquad H$$

$$(33)$$

#### Estimación de fase y de orden

El algoritmo de estimación de fase sirve para hallar los autovalores de un operador unitario U. Cuando este operador es el operador de multiplicación modular  $U_{a,N}|x\rangle = |ax \mod N\rangle$  y el estado de entrada es  $|u\rangle = |1\rangle$ , el algoritmo sirve para estimar el orden de  $a^x \mod N$ .



# Algoritmo de Shor

- $\blacksquare$  Si es N es par o un cuadrado perfecto, se conoce una factorización. Fin del algoritmo.
- si Si  $GCD(a, N) \neq 1$ , entonces este número es un factor no trivial de N y se ha hallado una factorización. Fin del algoritmo.
- $\blacksquare$  Si a es par, volver al paso 3.
- **S**i no, usar el algoritmo de estimación de orden para hallar el período r de  $f(x) = a^x \mod N$ .
- 6 Si r es impar, volver al paso 3.
- **7** Si  $a^r \not\equiv 1 \mod N$ , ir al paso 3.
- Si  $a^{r/2} \equiv -1 \mod N$ , ir al paso 3.
- $\mbox{\fontfamily Finalmente},\ GCD(a^{r/2}+1,N)$ y  $GCD(a^{r/2}-1,N)$  son factores de N. Fin del algoritmo.

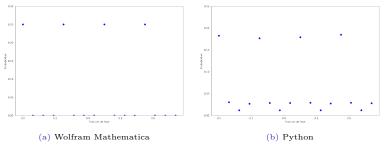


Figura: Estimación de fase del algoritmo de Shor sin pérdidas para el número 15

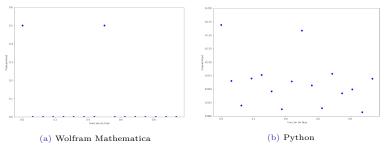


Figura: Estimación de fase del algoritmo de Shor sin pérdidas para el número 8

#### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

### PageRank

El algoritmo de PageRank fue desarrollado en 1996 en la Universidad de Stanford por Larry Page y Sergey Brin [10], 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.

El primer paso de este algoritmo es construir la matriz de adyacencia ponderada del grafo a procesar  $\,$ 

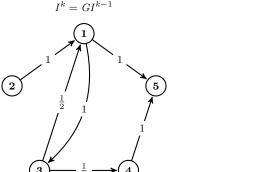
$$E_{ij} \equiv \begin{cases} \frac{1}{\text{outdeg}(P_j)} & \text{si el nodo } P_j \text{ tiene un hipervínculo a } P_i \\ 0 & \text{en otro caso} \end{cases}$$
 (34)

## PageRank

Para considerar los casos en los que se entra directamente a página por su URL, en lugar de un hipervínculo, se agrega el término  $\mathbb I$ 

$$G \equiv \alpha E + \frac{1-\alpha}{N} \mathbb{I}$$
 (Matriz de Google) (35)

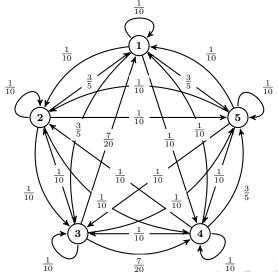
 $\mathbb I$  es una matriz en la cual todas las entradas están establecidas en 1, y N el número de nodos. El PageRank del grafo está dado por el vector al que converge la siguiente sucesión, para cualquier vector  $I^0$  inicial



(36)

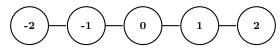
## PageRank

Transformación de un grafo al crear la matriz de Google con  $\alpha = \frac{1}{2}$ 

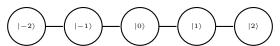


### Caminatas cuánticas

El método que parecería trivial, para cuantizar las caminatas aleatorias, de asignar un ket a cada nodo, no es realizable.

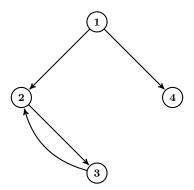


Al hacer esto, aparecen operadores no unitarios, los cuales no son realizables con compuertas cuánticas.



## Caminatas cuánticas de Szegedy

Para solucionar esto, Szegedy propuso duplicar los nodos del grafo y construir un grafo bipartito a partir de él. Un grafo bipartito es aquel donde los nodos se pueden separar en dos particiones y no hay vínculos entre nodos de la misma partición.



## Caminatas cuánticas de Szegedy

A cada nodo se le asigna un estado de la siguiente forma

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

$$A = \sum_i |\psi_i\rangle\langle\psi_i| \qquad B = \sum_j |\phi_j\rangle\langle\phi_j|.$$

$$1a \qquad 1b \qquad 1a \qquad 1b$$

$$2a \qquad 2b \qquad 2b$$

$$3a \qquad 3b \qquad 3b$$

$$4a \qquad 4b \qquad 4b$$

De esta manera, el operador que genera la caminata es U = (1 - 2B)(1 - 2A)

## PageRank cuántico

El PageRank cuántico instantaneo de cada nodo en el paso m es la probabilidad de encontrar encontrar al caminante en ese nodo, midiendo la segunda partición y comenzando la caminata con el estado inicial  $|\psi_0\rangle$ 

$$I_q(P_i, m) = Tr((\mathbb{1} \otimes |i\rangle\langle i|) U^m |\psi_0\rangle\langle\psi_0| U^{\dagger m})$$
(37)

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_i |\psi_i\rangle \tag{38}$$

Sin embargo, este valor no converge, sino que oscila. Así que tomamos, como medida de centralidad, el PageRank cuántico promedio, el cual sí converge.

$$\langle I_q(P_i)\rangle = \frac{1}{M} \sum_{m=0}^{M-1} I_q(P_i, m)$$
(39)

#### Circuitos de Loke

Loke desarrolló un método para construir los circuitos de las caminatas cuánticas de Szegedy, diagonalizando el operador U de la caminata. Primero, dividimos el grafo en subgrafos cíclicos. El operador T convierte los estados de todos los nodos de cada subgrafo en el de algún nodo de referencia del mismo subgrafo. El operador  $K_b^{\dagger}$  convierte los estados de los nodos de referencia en un estado de la base computacional para el cuál podamos construir el operador de reflexión.

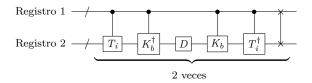


Figura: Circuito de Loke para las caminatas cuánticas de Szegedy

Cada uno de los registros corresponde a una de las particiones del grafo bipartito.

#### Circuitos de Loke

Los operadores  $T_i$ se pueden construir de manera general con operadores de permutación  ${\cal T}$ 



Figura: Operador de permutación T

Sin embargo, Loke no presenta ninguna manera de construir los operadores  $K_b$ . Sólo presenta algunos casos particulares como ejemplos. Como parte de este trabajo se ha desarrollado un método para construir estos operadores par cualquier grafo de 4 nodos, a partir de los coeficientes  $\sqrt{G_i}$  del estado inicial  $|\psi_0\rangle$  de la caminata

### Circuitos de Loke

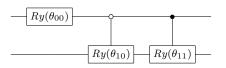


Figura: Circuito de  $K_i$ 

$$\theta_{00} = 2\cos^{-1}\left(\sqrt{G_1 + G_2}\right) \tag{40}$$

$$\theta_{10} = 2\cos^{-1}\left(\sqrt{\frac{G_1}{G_1 + G_2}}\right) \tag{41}$$

$$\theta_{11} = 2\cos^{-1}\left(\sqrt{\frac{G_3}{1 - (G_1 + G_2)}}\right).$$
 (42)

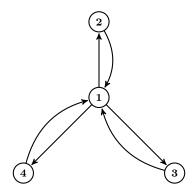


Figura: Grafo estrella

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{43}$$

$$E = \begin{pmatrix} 0 & 1 & 1 & 1\\ \frac{1}{3} & 0 & 0 & 0\\ \frac{1}{3} & 0 & 0 & 0\\ \frac{1}{3} & 0 & 0 & 0 \end{pmatrix} \tag{44}$$

$$G = \begin{pmatrix} \frac{3}{80} & \frac{71}{80} & \frac{71}{80} & \frac{71}{80} \\ \frac{740}{240} & \frac{3}{80} & \frac{30}{80} & \frac{30}{80} \\ \frac{7240}{240} & \frac{80}{80} & \frac{30}{80} & \frac{30}{80} \end{pmatrix}$$
(45)

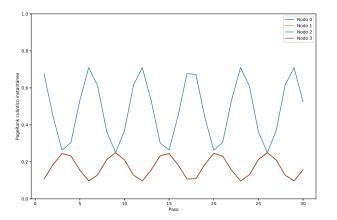


Figura: Wolfram Mathematica: PageRank cuántico instantáneo del grafo estrella sin pérdidas

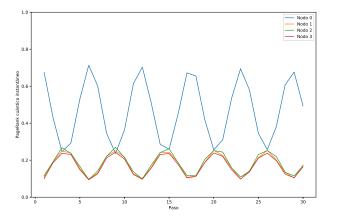


Figura: Python: PageRank cuántico instantáneo del grafo estrella sin pérdidas

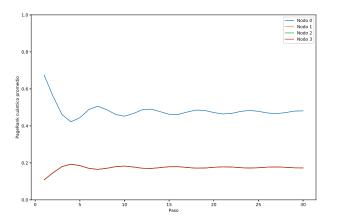


Figura: Wolfram Mathematica: PageRank cuántico promedio del grafo estrella sin pérdidas

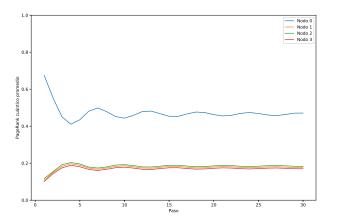


Figura: PageRank cuántico promedio del grafo estrella sin pérdidas

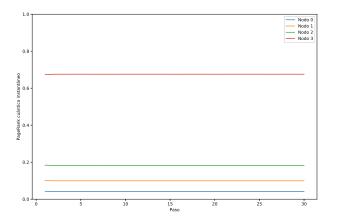


Figura: PageRank cuántico instantaneo del grafo estrella con pérdidas

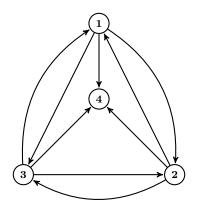


Figura: Grafo corona

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \tag{46}$$

$$E = \begin{pmatrix} 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{4} \end{pmatrix}$$
(47)

$$G = \begin{pmatrix} \frac{3}{80} & \frac{77}{240} & \frac{77}{240} & \frac{1}{4} \\ \frac{7}{240} & \frac{80}{80} & \frac{74}{240} & \frac{1}{4} \\ \frac{7}{240} & \frac{7}{240} & \frac{7}{80} & \frac{1}{4} \\ \frac{7}{240} & \frac{7}{240} & \frac{7}{240} & \frac{1}{4} \end{pmatrix}$$
(48)

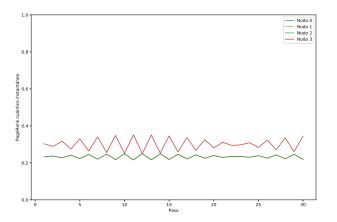


Figura: Wolfram Mathematica: PageRank cuántico instantáneo del grafo corona sin pérdidas

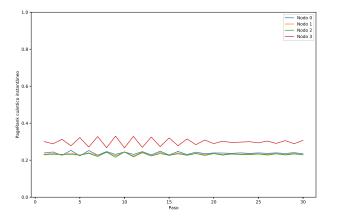


Figura: Python: PageRank cuántico instantáneo del grafo corona sin pérdidas

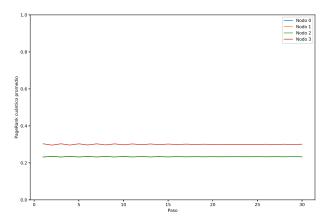


Figura: Wolfram Mathematica: PageRank cuántico promedio del grafo corona sin pérdidas

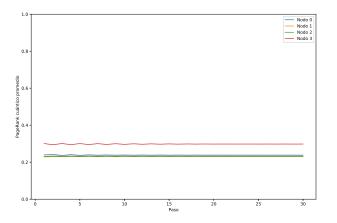


Figura: Python: PageRank cuántico promedio del grafo corona sin pérdidas

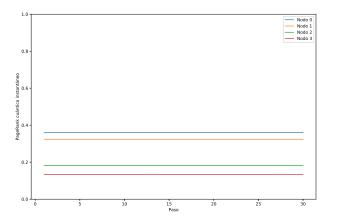


Figura: PageRank cuántico instantaneo del grafo aleatorio con pérdidas

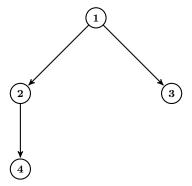


Figura: Grafo árbol

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{49}$$

$$E = \begin{pmatrix} 0 & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & 1 & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$
 (50)

$$G = \begin{pmatrix} \frac{3}{80} & \frac{3}{80} & \frac{1}{4} & \frac{1}{4} \\ \frac{37}{80} & \frac{39}{80} & \frac{1}{4} & \frac{1}{4} \\ \frac{39}{80} & \frac{39}{80} & \frac{1}{4} & \frac{1}{4} \\ \frac{39}{80} & \frac{1}{80} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$
(51)

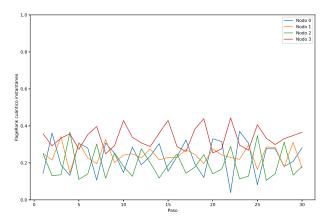


Figura: Wolfram Mathematica: PageRank cuántico instantáneo del grafo árbol sin pérdidas

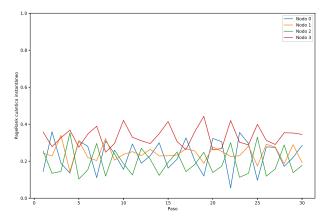


Figura: Python: PageRank cuántico instantáneo del grafo árbol sin pérdidas

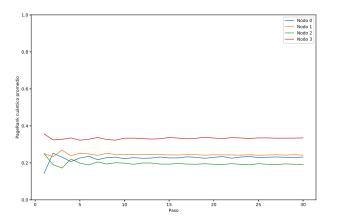


Figura: Wolfram Mathematica: PageRank cuántico promedio del grafo árbol sin pérdidas

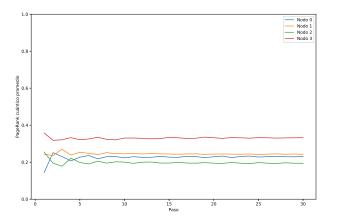


Figura: Python: PageRank cuántico promedio del grafo árbol sin pérdidas

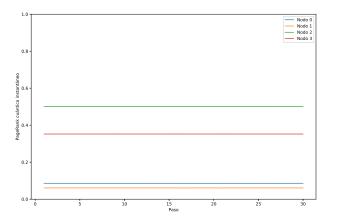


Figura: PageRank cuántico instantaneo del grafo árbol con pérdidas

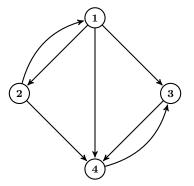


Figura: Grafo aleatorio

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \tag{52}$$

$$E = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0\\ \frac{1}{3} & 0 & 0 & 0\\ \frac{1}{3} & 0 & 0 & 1\\ \frac{1}{3} & \frac{1}{2} & 1 & 0 \end{pmatrix}$$
 (53)

$$G = \begin{pmatrix} \frac{3}{80} & \frac{37}{80} & \frac{3}{80} & \frac{3}{80} \\ \frac{7}{240} & \frac{80}{80} & \frac{3}{80} & \frac{3}{80} \\ \frac{7}{240} & \frac{80}{80} & \frac{80}{80} & \frac{30}{80} \\ \frac{7}{240} & \frac{37}{80} & \frac{80}{80} & \frac{30}{80} \end{pmatrix}$$
 (54)

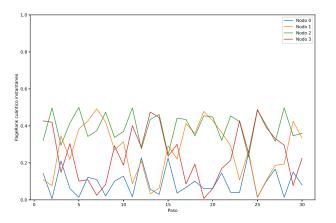


Figura: Wolfram Mathematica: PageRank cuántico instantáneo del grafo aleatorio sin pérdidas

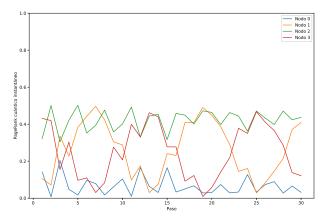


Figura: Python: PageRank cuántico instantáneo del grafo aleatorio sin pérdidas

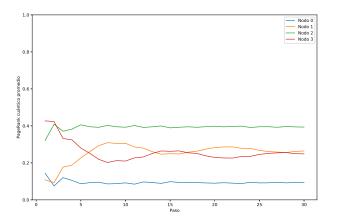


Figura: Wolfram Mathematica: PageRank cuántico promedio del grafo aleatorio sin pérdidas

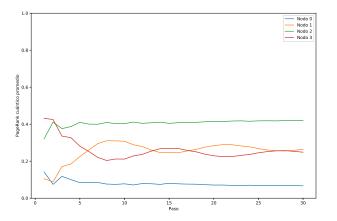


Figura: Python: PageRank cuántico promedio del grafo aleatorio sin pérdidas

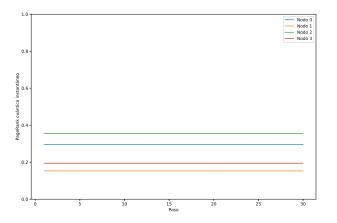


Figura: PageRank cuántico instantaneo del grafo aleatorio con pérdidas

### Tabla de contenidos

- 1 Objetivos
- 2 Información cuántica
- 3 Superconductividad
- 4 Simulador
- 5 Algoritmo de Grover
- 6 Algoritmo de Shor
- 7 PageRank
- 8 Conclusiones

### Conclusiones

En el presente trabajo se ha:

- Estudiado las bases de teoría de información cuántica y de superconductividad necesarias para entender la dinámica de los transmones.
- Construido la representación circuital cuántica de los AC de Grover, Shor y de Google Cuántico.
- Hallado las secuencias de pulsos que generan las compuertas necesarias para los algoritmos estudiados.
- Simulado en Mathematica, de forma algebraica, cada uno de los AC seleccionados y se ha simulado en Python la implementación de estos en transmones.

Los resultados de las simulaciones del algoritmo de Grover y PageRank nos indican que para sistemas con tiempos de relajación del orden de  $O(10^4 ns)$ , los protocolos de corrección de errores cuánticos son una necesidad. Este es un resultado importante, pues el record actual de tiempo de vida de un qubit superconductor es inferior a 0.1 ms, está en el mismo orden de magnitud que el del sistema simulado.

### Conclusiones

Hasta donde tenemos conocimiento, ninguno de los siguientes aportes se encuentran en la literatura científica:

- Una compuerta controlada de fase CP que permita eliminar las fases en las compuertas de negación con dos o más qubits de control, como la de Toffoli.
- Un conjunto de instrucciones cuánticas basadas en las compuertas nativas de los transmones y un simulador del sistema físico.
- Un operador de multiplicación por 3 módulo 8 sin qubits de ancilla.
- 1 La forma explícita del operador de difusión de las caminatas cuánticas de Szegedy para grafos de cuatro nodos, en función de rotaciones en Y controladas
- 5 El efecto de la relajación en los algoritmos de Grover, Shor y PageRank.

### Referencias I



C. Tannoudji, Quantum mechanics. New York: Wiley, 1977.



Miraceti.



G. Wendin, "Quantum information processing with superconducting circuits: a review," *IOP Science*, 2017. [Online]. Available: http://iopscience.iop.org/article/10.1088/1361-6633/aa7ela/pdf



Bjohnson 00.



L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC 96, 1996. [Online]. Available: http://dx.doi.org/10.1145/237814.237866



P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Review, vol. 41, no. 2, p. 303332, Jan 1999. [Online]. Available: http://dx.doi.org/10.1137/S0036144598347011



D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, "Post-quantum rsa," Cryptology ePrint Archive, Report 2017/351, 2017, https://eprint.iacr.org/2017/351.

### Referencias II



F. Grosshans, T. Lawson, F. Morain, and B. Smith, "Factoring safe semiprimes with a single quantum query," 2015.



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



S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," *Computer Networks and ISDN Systems*, vol. 30, no. 1, pp. 107 – 117, 1998, proceedings of the Seventh International World Wide Web Conference. [Online]. Available:

http://www.sciencedirect.com/science/article/pii/S016975529800110X