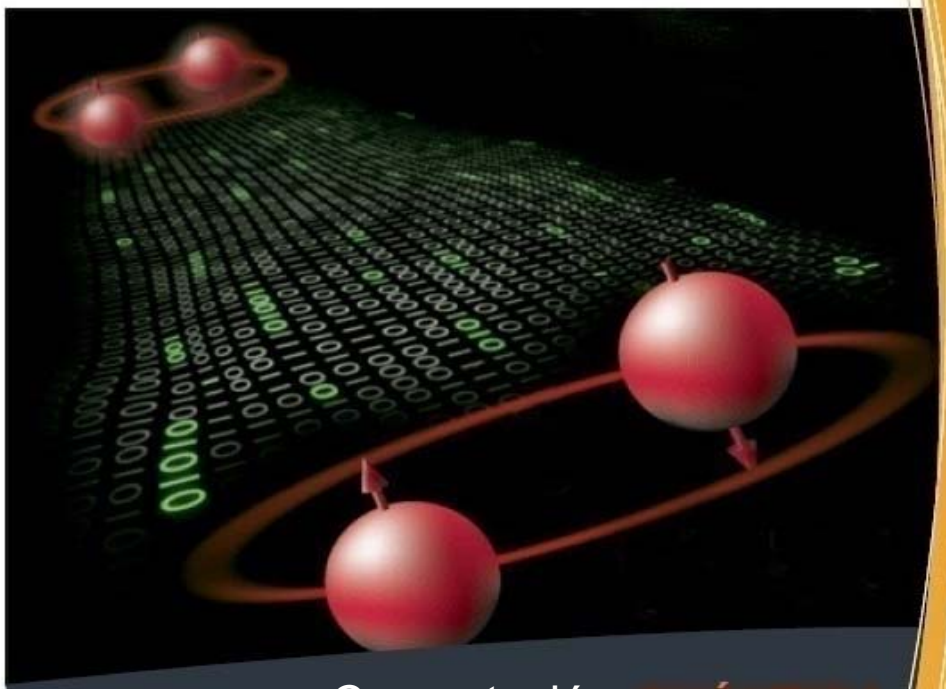
tecnologías emergentes

MÁSTER EN CIENCIAS Y TECNOLOGÍAS DE LA COMPUTACIÓN



Computación CUÁNTICA

Jesús García López de Lacalle

Computación Cuántica

- Algoritmos cuánticos
- Algoritmo de Grover:
  - ✓ Descripción del algoritmo
  - ✓ Visión geométrica del algoritmo
  - ✓ Número óptimo de iteraciones
- Algoritmo de Shor:
  - ✓ Reducción del problema de factorización
  - ✓ Transformada cuántica de Fourier
  - ✓ Detalles del algoritmo de Shor

Algoritmos cuánticos

- **Cambio de fase general R_k**

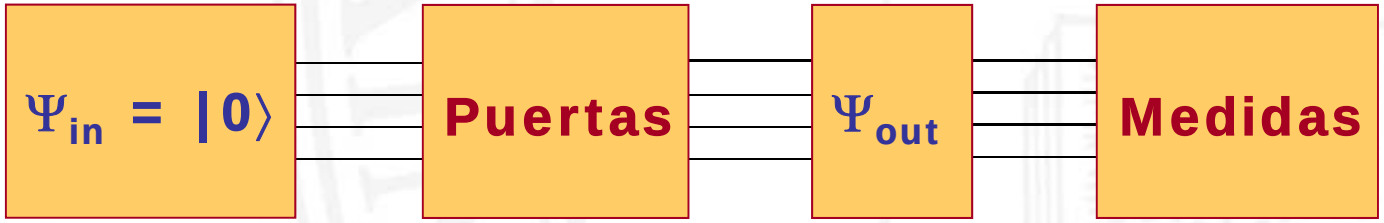
  $R_k |0\rangle = |0\rangle$

  $R_k |1\rangle = \exp(2\pi i / 2^k)|1\rangle$

- **Conjunto universal de puertas**

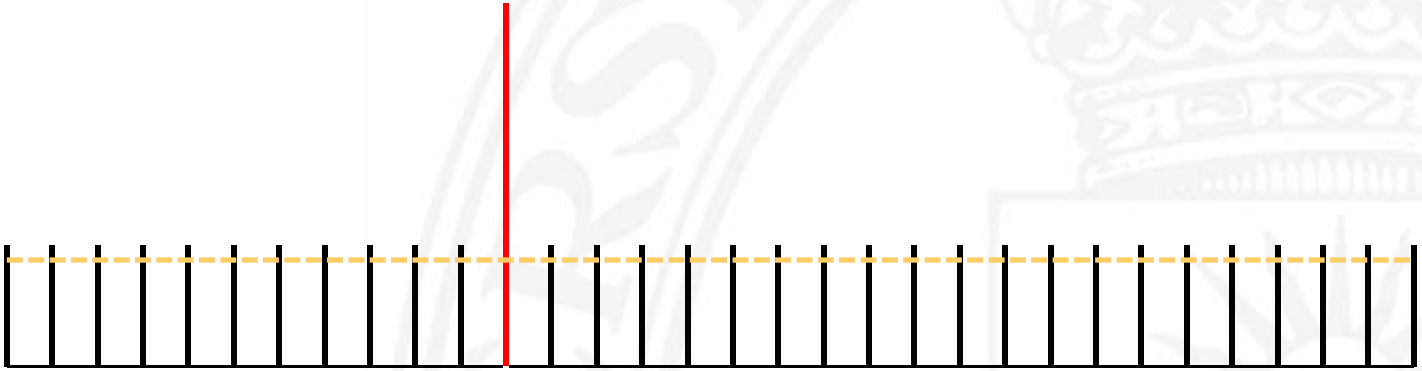
  C + puertas de un qubit

- **Algoritmos cuánticos**



Algoritmo de Grover

Descripción del algoritmo



- Oráculo
- Promedio
- Inversión sobre el promedio

Algoritmo de Grover

Descripción del algoritmo

- **Estado inicial** $\psi = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$
- **Estado general** $\sum_{x=0}^{N-1} a_x |x\rangle$
- **Items** $X_0 = \{x : f(x) = 0\}$ y $X_1 = \{x : f(x) = 1\}$
- **Aplicación del oráculo** $\sum_{x \in X_0} a_x |x\rangle - \sum_{x \in X_1} a_x |x\rangle$

Algoritmo de Grover

Descripción del algoritmo

- **Inversión** $\sum_{x=0}^{N-1} a_x|x\rangle \Longrightarrow \sum_{x=0}^{N-1}(2A - a_x)|x\rangle$
- **La inversión es *"unitaria"*** $G = 2|\psi\rangle\langle\psi| - I$
- **Y verifica** $W_n R W_n = 2|\psi\rangle\langle\psi| - I = G$

donde R es una matriz diagonal con 1 en la primera posición y -1 en el resto y $W_n = H \otimes \ldots \ldots \otimes H$

Algoritmo de Grover

Descripción del algoritmo

- Aplicar reiteradamente la transformación

$$GU$$

- ¿Cuántas veces?
- Medir

Algoritmo de Grover

Visión geométrica del algoritmo

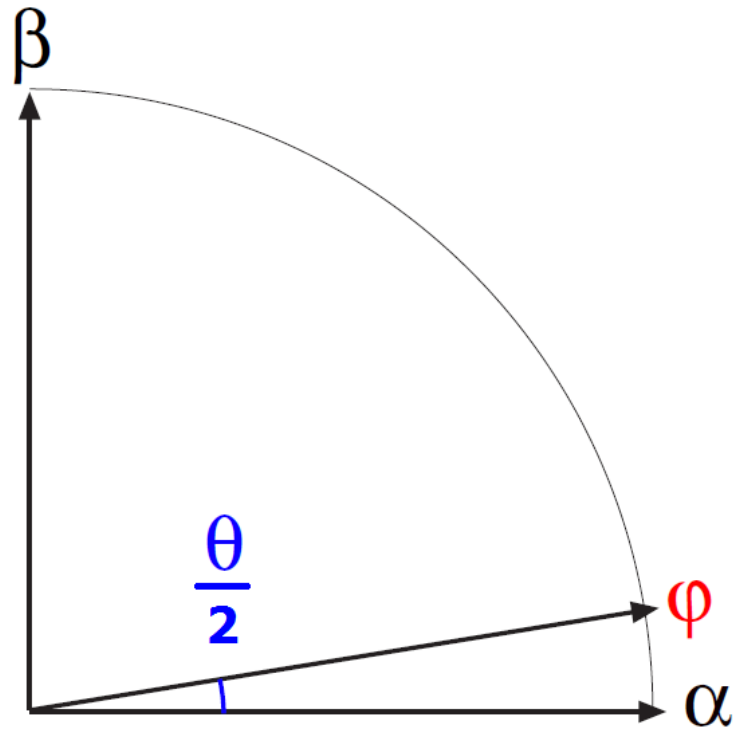
- **Todo transcurre en un plano generado por**

$$|\alpha\rangle = \frac{1}{\sqrt{N-s}} \sum_{x \in X_0} |x\rangle \quad \text{y} \quad |\beta\rangle = \frac{1}{\sqrt{s}} \sum_{x \in X_1} |x\rangle$$

- **Son vectores ortogonales**
- **$s = |X_1|$**
- **$N\text{-}s = |X_0|$**

Algoritmo de Grover

Visión geométrica del algoritmo



- G = simetría respecto de φ
- U = simetría respecto de α
- GU = rotación de ángulo θ

Algoritmo de Grover

Número óptimo de iteraciones

$$\cos\left(\frac{\theta}{2}\right) = \langle\alpha|\psi\rangle = \sqrt{\frac{N-s}{N}} \qquad \text{sen}\left(\frac{\theta}{2}\right) = \sqrt{\frac{s}{N}}$$

$$k \sim \frac{\pi}{4}\sqrt{\frac{N}{s}}$$

Algoritmo de Shor

Reducción del problema de factorización

Sea *N* un número entero compuesto e impar

Problema 1: Encontrar un factor propio de *N*

Problema 2: Elegida aleatoriamente una unidad *a* de Z_N encontrar su orden *T*

Sol. Problema 2 ⟶ Sol. Problema 1

Reducción del problema de factorización

Sea *N* un número entero compuesto e impar

Problema 1: Encontrar un factor propio de *N*.

Problema 2: Elegida aleatoriamente una unidad *a* de Z_N encontrar su orden *T*.

1. Elegir aleatoriamente $a \in \{0,1, \ldots N-1\}$
2. Si $mcd(a,N) \neq 1$ FIN
3. Calcular el orden *T* de *a* en Z_N
4. Si *T* es impar volver a 1
5. Si $mcd(a^{T/2}+1,N) \neq N$ FIN, en otro caso volver a 1

Reducción del problema de factorización

Teorema 1:

La probabilidad de que $a^{T/2}+1 \neq 0 \bmod N$ es mayor o igual que $1-(1/2)^{r-1}$ siendo r el número de factores distintos de N

Problema 3: Sea a tal que $mcd(a,N) = 1$ y $f : Z \rightarrow Z_N$ tal que $f(x)=a^x \bmod N$.
Calcular el periodo T de f

T en problema 2 = T en problema 3

$\Rightarrow$ **Transformada de Fourier**

Transformada cuántica de Fourier

La QFT es el siguiente operador lineal

$$F\,|j\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \omega^{jk}\,|k\rangle$$

$$\omega = e^{2\pi i / Q} \quad \text{y} \quad Q = 2^n$$

Relación entre la QFT y la DFT

$$y_k = \frac{1}{\sqrt{Q}} \sum_{j=0}^{Q-1} \omega^{jk}\, x_j \quad \Rightarrow \quad F\left(\sum_{j=0}^{Q-1} x_j\,|j\rangle\right) = \sum_{k=0}^{Q-1} y_k\,|k\rangle$$

Transformada cuántica de Fourier

Es una transformación unitaria

$$F\,|0\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |k\rangle$$

Si $x_{j+T} = x_j$ para todo j (índices módulo N)

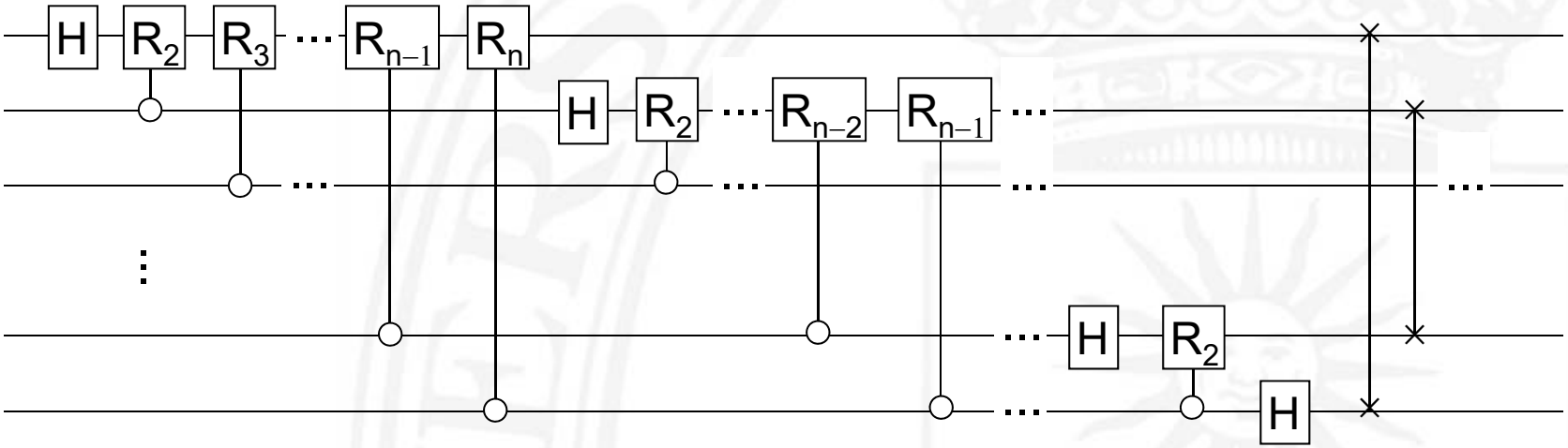
$$F\left(\sum_{j=0}^{Q-1} x_j\,|j\rangle\right) = \sum_{k=0}^{T-1} y_{kS}\,|kS\rangle$$

TS = Q

T = periodo
S = frecuencia

Transformada cuántica de Fourier

Teorema 2: El siguiente algoritmo calcula la QFT



Número de puertas cuánticas:

Algoritmo cuántico	Algoritmo clásico
$O(n^2)$	$O(n2^n)$

Detalles del algoritmo de Shor

1. Elegir a aleatoriamente entre 0 y $N-1$.
   Si $mcd(a,N) \neq 1$ fin.
2. Determinar el periodo T de la función
   $f(x) = a^x \bmod N$.
3. Si T es impar ir al paso 1.
4. Si $mcd(a^{T/2}+1,N) \neq N$ fin, en otro caso ir al paso 1.

Detalles del algoritmo de Shor

1. Iniciar $\Psi_0 = |0\rangle|0\rangle$

   1er reg: n qubits t.q. $N^2 \leq Q < 2N^2$ con $Q = 2^n$

   2º reg: m qubits tal que $N \leq 2^m < 2N$

2. Aplicar la QFT al 1er reg:

$$F|0\rangle|0\rangle = \frac{1}{\sqrt{Q}} \sum_{j=0}^{Q-1} |j\rangle|0\rangle = \Phi_1$$

3. Calcular f en el 2º reg:

$$U_f \Phi_1 = \frac{1}{\sqrt{Q}} \sum_{j=0}^{Q-1} |j\rangle|f(j)\rangle = \Phi_2$$

Detalles del algoritmo de Shor

4. Aplicar la QFT al 1er reg:

$$F\,\Phi_2 = \frac{1}{Q}\sum_{j=0}^{Q-1}\sum_{k=0}^{Q-1}\omega^{jk}\,|k\rangle\,|f(j)\rangle = \Phi_3 \qquad \omega = \exp(2\pi i/2^n)$$

$$\Phi_3 = \frac{1}{Q}\sum_{k=0}^{Q-1}|k\rangle\,|A(k)\rangle \quad \text{con} \quad |A(k)\rangle = \sum_{j=0}^{Q-1}\omega^{jk}\,|f(j)\rangle$$

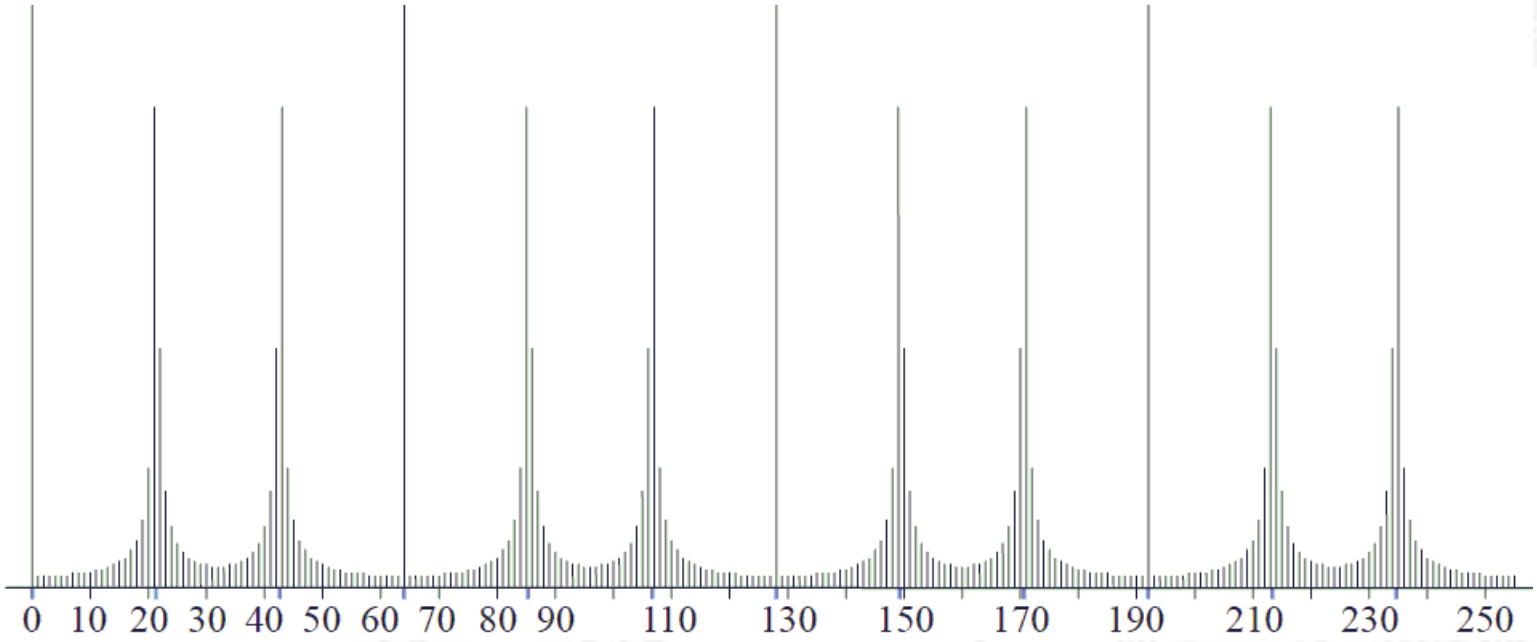
5. Medir el 1er reg:

$$k \in \{0,1,\ldots Q-1\} \quad \text{con} \quad \text{Prob}(k) = \|A(k)\|^2$$

6. Calcular el periodo *T* a partir de *k*.

Detalles del algoritmo de Shor

Ejemplo de QFT



Detalles del algoritmo de Shor

Obtención del periodo T a partir de k

$$\left|\frac{k}{Q} - \frac{j}{T}\right| \leq \frac{1}{2Q} < \frac{1}{2T^2}$$

j/T es una convergente de la fracción continua de k/Q

Detalles del algoritmo de Shor

Obtención del periodo T a partir de k

Teorema 3: La probabilidad de que $|Tk - jQ| \leq \frac{T}{2}$

es mayor o igual que $\frac{4}{\pi^2}\left[1 - \frac{1}{N}\right]^3$

Teorema 4: La probabilidad de que $mcd(d,T) = 1$

es mayor o igual que $\frac{e^{-\gamma}}{4\,C\,loglog(T)}$

Detalles del algoritmo de Shor

Prob $\geq \left(1-\frac{1}{2^{r-1}}\right) \frac{4}{\pi^2} \left[1-\frac{1}{N}\right]^3 \frac{e^{-\gamma}}{4\, C\, loglog(T)} \geq$

$$\geq \frac{e^{-\gamma}}{3\,\pi^2\, C\, loglog(N)}$$

Teorema: La probabilidad de obtener un factor Propio de N es mayor o igual que

$$\frac{e^{-\gamma}}{3\,\pi^2\, C\, loglog(N)}$$

Detalles del algoritmo

Probabilidad de éxito: $P \geq Cte \ / \ loglog(N)$

Probabilidad de éxito para $N \leq 255$