Diseño, desarrollo, implementación y prueba de un simulador cuántico para el algoritmo de Simon

Autor: Rodrigo Arias Mallo
Director: Vicente Moret Bonillo

18 de febrero de 2016

Introducción

Resumen: Resolución de un problema mediante un algoritmo cuántico. Simulación y comprobación de los resultados.

- Presentación del problema
- Solución clásica
- Solución cuántica
- Complejidad teórica
- Simulador
- Resultados experimentales
- Conclusiones y trabajo futuro

Problema de Simon

Sea f una función binaria

$$f : \{0,1\}^n \to \{0,1\}^n$$

que cumple la propiedad

$$f(\boldsymbol{x}) = f(\boldsymbol{y}) \iff \boldsymbol{y} = \boldsymbol{x} \oplus \boldsymbol{s}$$

con $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{s} \in \{0,1\}^n$ y el período $\boldsymbol{s} \neq \boldsymbol{0}$.

Objetivo: Encontrar $\boldsymbol{s}$ tratando la función f como una caja negra.

Función f de ejemplo

Ejemplo de 2 bits, y un período $\boldsymbol{s} = 01$

$\boldsymbol{x}$	$f(\boldsymbol{x})$
00	00
01	00
10	01
11	01

$$f(\boldsymbol{x}) = f(\boldsymbol{y}) \iff \boldsymbol{y} = \boldsymbol{x} \oplus \boldsymbol{s}$$
$$f(00) = f(01) \iff 01 = 00 \oplus 01$$
$$f(10) = f(11) \iff 11 = 10 \oplus 01$$

Solución clásica

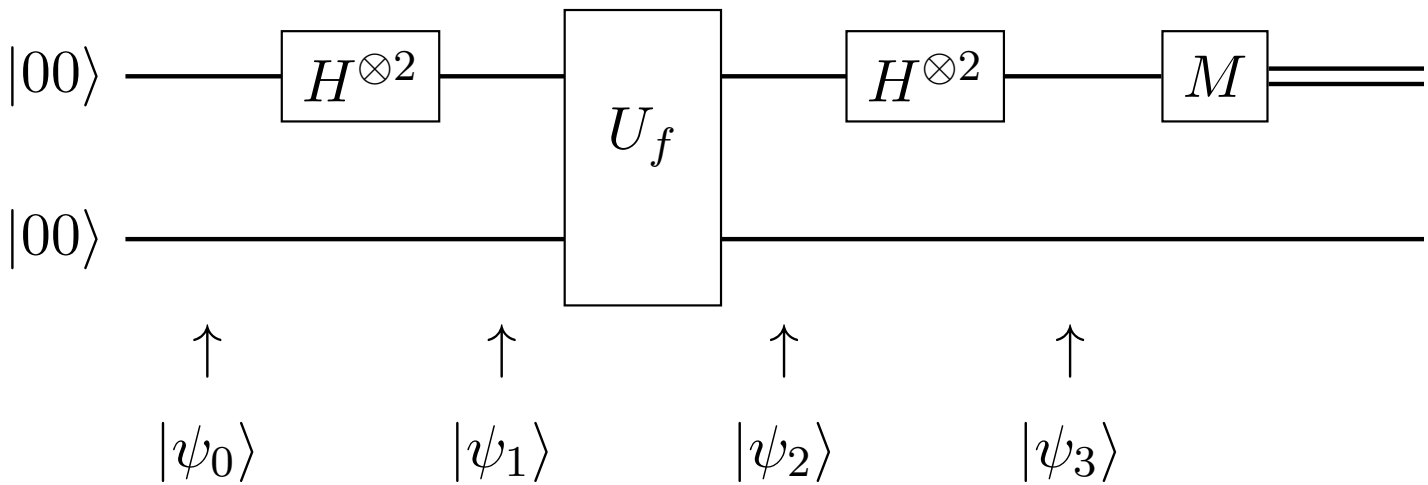
- Una solución sencilla consiste en probar entradas hasta obtener una salida repetida.

$$f(00) = f(01) \implies 01 = 00 \oplus \boldsymbol{s} \implies \boldsymbol{s} = 00 \oplus 01 = 01$$

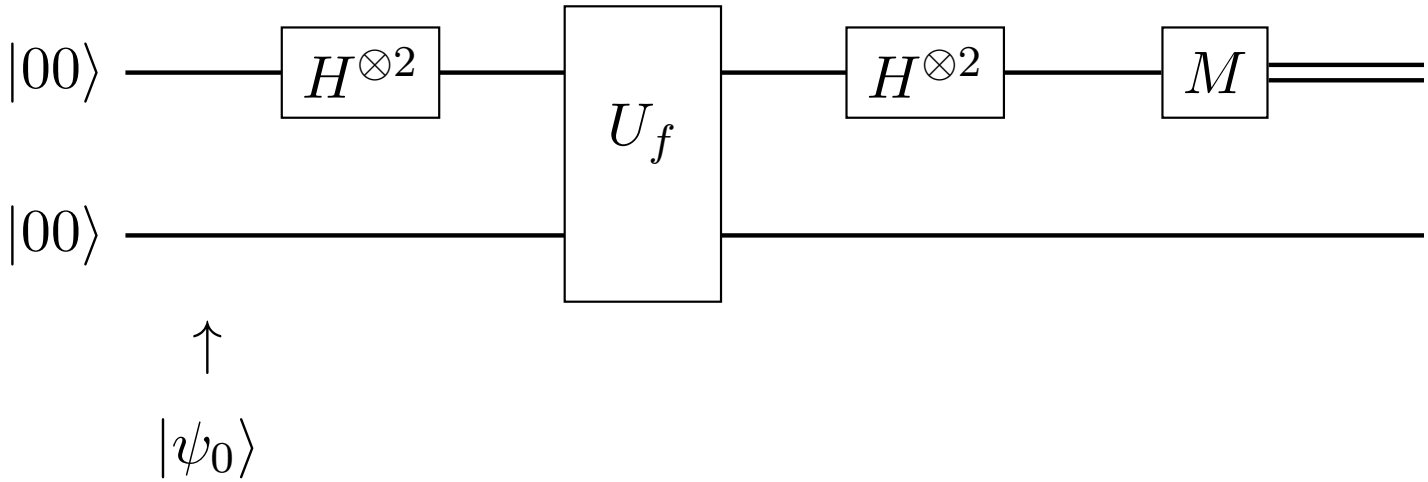
- Hay $2^n/2$ salidas diferentes.
- Es necesario probar en el peor caso $2^n/2 + 1$ entradas: $O(2^n)$.

Solución cuántica: $O(2^n) \rightarrow O(n)$

- Para solucionar este problema, Daniel R. Simon propuso una solución empleando la **computación cuántica**.
- Soluciona el problema en $O(n)$.



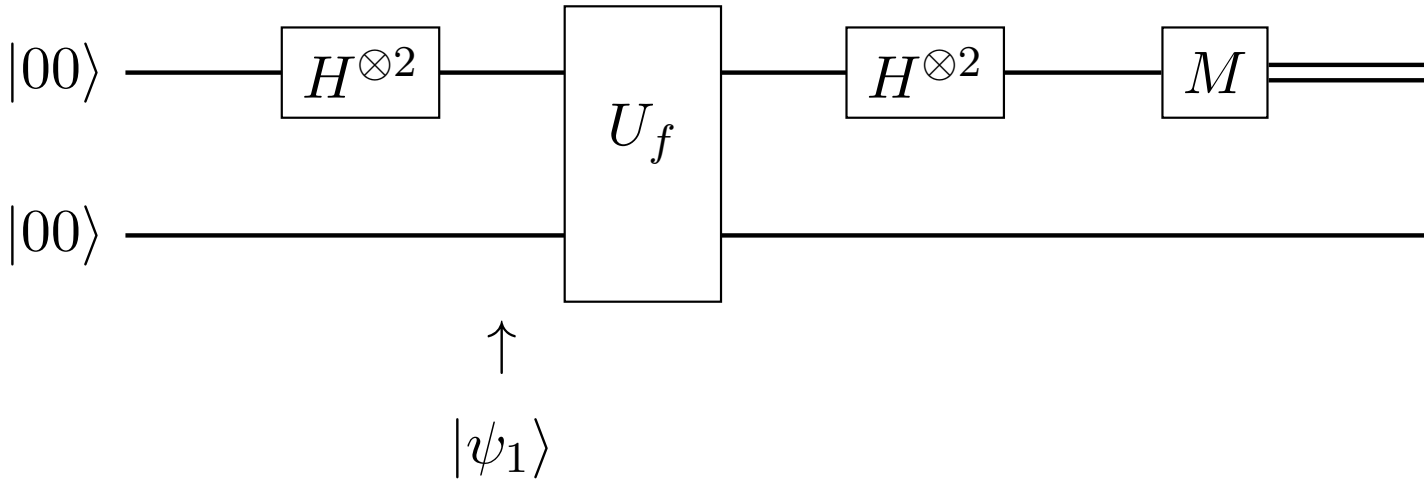
Funcionamiento



Primero se inicializa el circuito con ceros.

$$|\psi_0\rangle = |00, 00\rangle$$

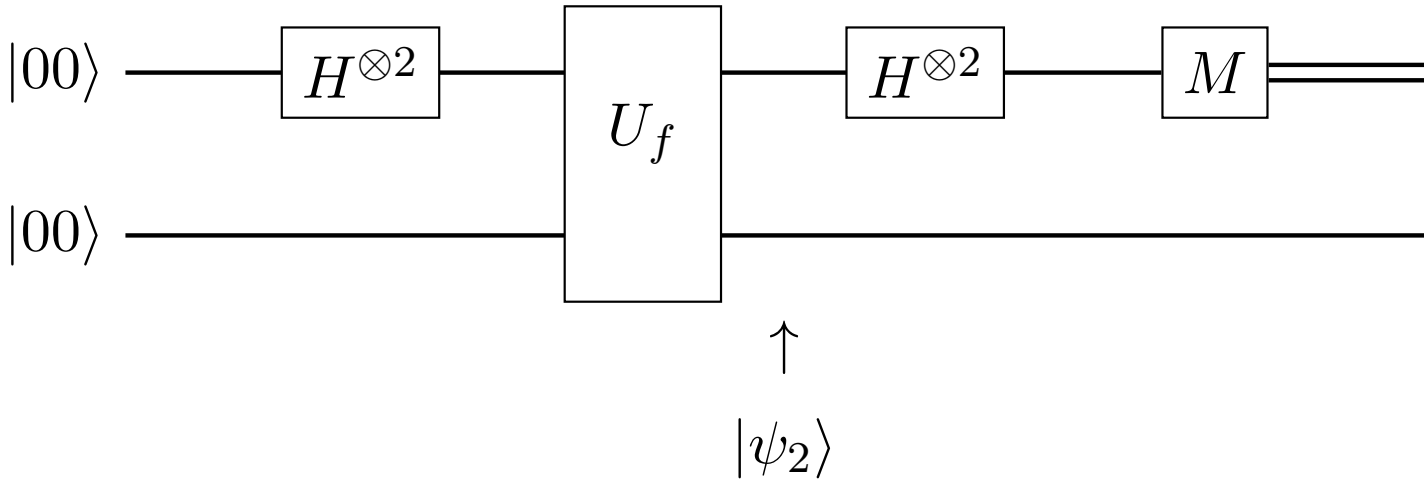
Funcionamiento



Se aplica el operador de Hadamard sobre la línea superior, obteniendo un estado **entrelazado**.

$$|\psi_1\rangle = \frac{1}{2}\Big(|00,00\rangle + |01,00\rangle + |10,00\rangle + |11,00\rangle \Big)$$

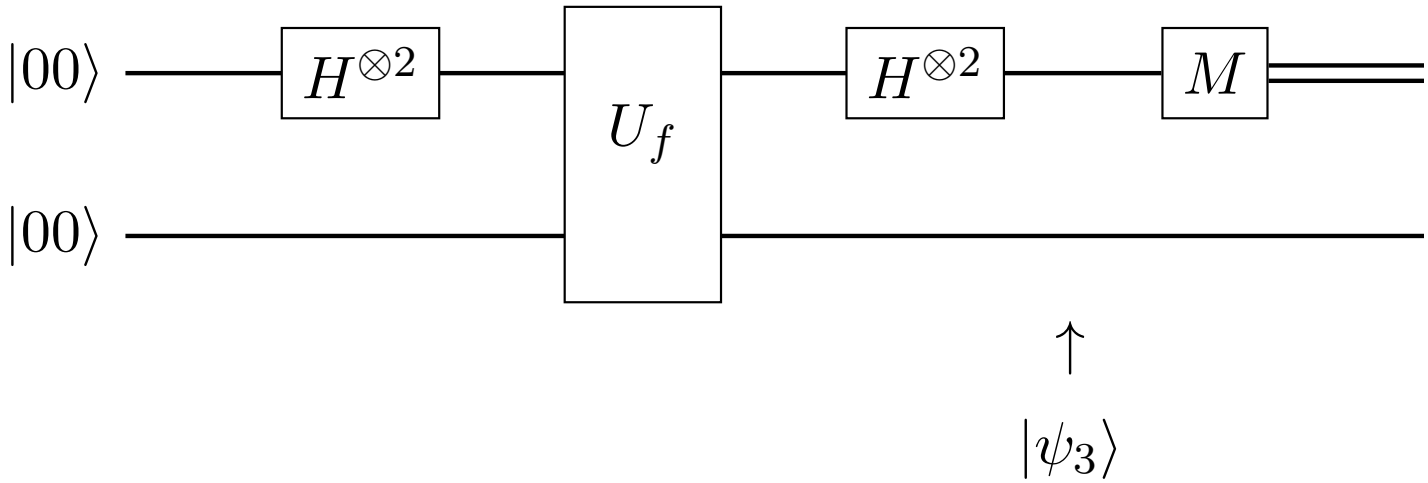
Funcionamiento



El operador U_f definido como $U_f\,|\boldsymbol{x}\rangle\,|\boldsymbol{y}\rangle = |\boldsymbol{x}\rangle\,|\boldsymbol{y} \oplus f(\boldsymbol{x})\rangle$, realiza el cómputo de f en **paralelo**.

$$|\psi_2\rangle = \frac{1}{2}\Big(|00, f(00)\rangle + |01, f(01)\rangle + |10, f(10)\rangle + |11, f(11)\rangle \Big)$$

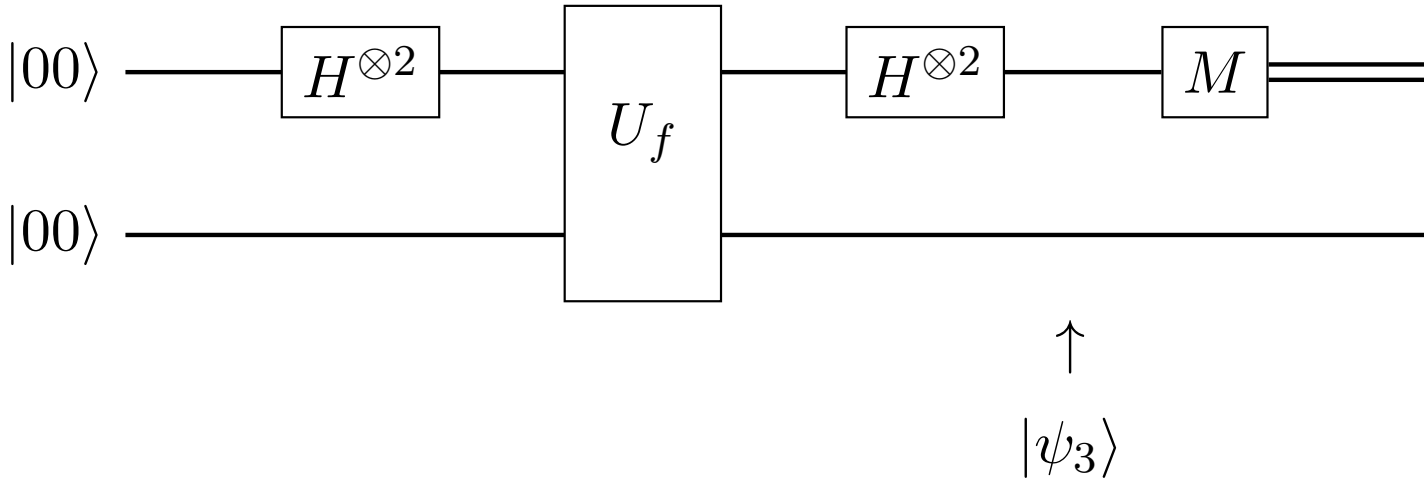
Funcionamiento



Finalmente el operador de Hadamard se aplica de nuevo, produciendo el efecto de **interferencia**.

$$\begin{aligned}|\psi_3\rangle = 1/4\big(&+ |00,00\rangle + |01,00\rangle + |10,00\rangle + |11,00\rangle \\ &+ |00,00\rangle - |01,00\rangle + |10,00\rangle - |11,00\rangle \\ &+ |00,01\rangle + |01,01\rangle - |10,01\rangle - |11,01\rangle \\ &+ |00,01\rangle - |01,01\rangle - |10,01\rangle + |11,01\rangle\big)\end{aligned}$$

Funcionamiento



Obteniéndose

$$|\psi_3\rangle = 1/2\left(|\mathbf{00}, 00\rangle + |\mathbf{00}, 01\rangle + |\mathbf{10}, 00\rangle - |\mathbf{10}, 01\rangle\right)$$

Al medir la línea superior se obtienen vectores $\boldsymbol{x}$ tal que $\boldsymbol{x} \cdot \boldsymbol{s} = 0$, con igual probabilidad.

$$\boldsymbol{x} \in \{00, 10\}$$

Complejidad teórica

Una vez obtenidos $n-1$ vectores $\boldsymbol{x}$ linealmente independientes, se puede resolver el sistema de ecuaciones y calcular $\boldsymbol{s}$.

$$\begin{cases} \boldsymbol{x}^{(1)} \cdot \boldsymbol{s} = 0 \\ \boldsymbol{x}^{(2)} \cdot \boldsymbol{s} = 0 \\ \vdots \\ \boldsymbol{x}^{(n-1)} \cdot \boldsymbol{s} = 0 \end{cases}$$

El número de ejecuciones promedio $E[R]$ será:

$$E[R] = \sum_{j=1}^{\infty} j \cdot p(R = j)$$

Siendo $p(R = j)$ la probabilidad de terminar en j iteraciones.

Complejidad teórica

Construyendo una recurrencia, se calcula $E[R]$

$$E[R] = \prod_{j=0}^{n-2}(1-2^{j-n+1}) \cdot \sum_{p=1}^{\infty} p \cdot 2^{(p-n+1)(-n+1)} \cdot \binom{p-1}{n-2}_{q=2}$$

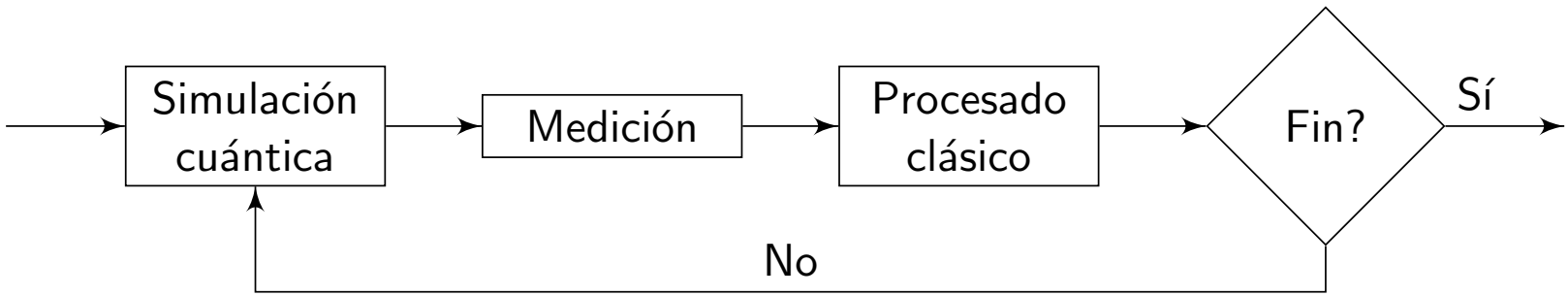
Obteniéndose computacionalmente los valores:

n	2	3	4	5	6	7	8	9	10
$E[R]$	2.00	3.33	4.47	5.54	6.57	7.59	8.59	9.60	10.60
$\frac{E[R]}{n}$	1.00	1.11	1.12	1.11	1.10	1.08	1.08	1.07	1.06

Se observa una complejidad lineal: $O(n)$

Simulador cuántico

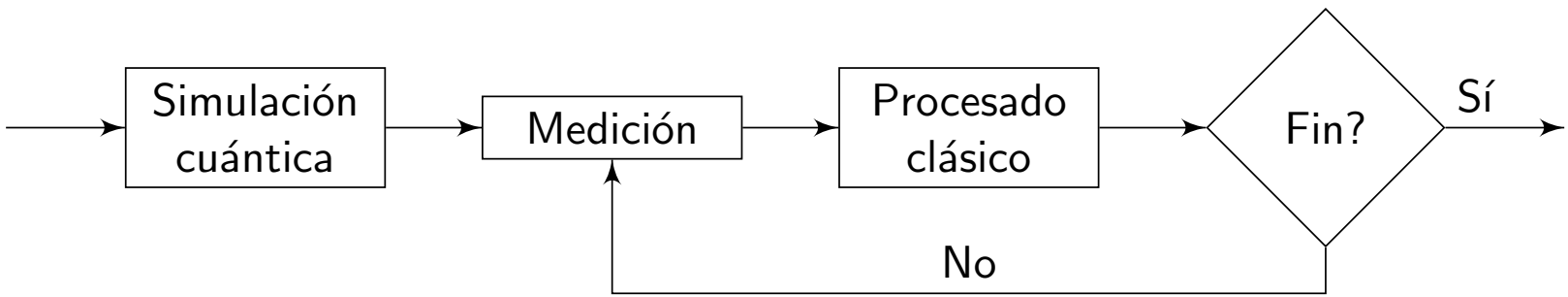
Realiza la simulación del circuito, la medición y el procesado clásico final, imitando el comportamiento de un ordenador cuántico.



Problema: La simulación cuántica es muy costosa.

Diseño del simulador

Permite reutilizar el estado final $|\psi_3\rangle$ tras la simulación cuántica para realizar las mediciones.



Estructuras de datos

- Para almacenar los estados y operadores se emplean **matrices huecas**.
- Permiten ahorrar espacio y reducir el número de operaciones.
- Implementados en paquetes de cálculo como `scipy`
- Varios formatos (COO y CSR).

El simulador está implementado en `python` empleando los paquetes `qutip`, `scipy` y `numpy`.

Análisis de la simulación

- Análisis de **tiempo** y **espacio** de la simulación
- Análisis de **complejidad** del circuito cuántico.
- La simulación del circuito cuántico se divide en dos etapas QC_0 y QC_f para permitir un análisis más detallado.

Tiempo de la simulación

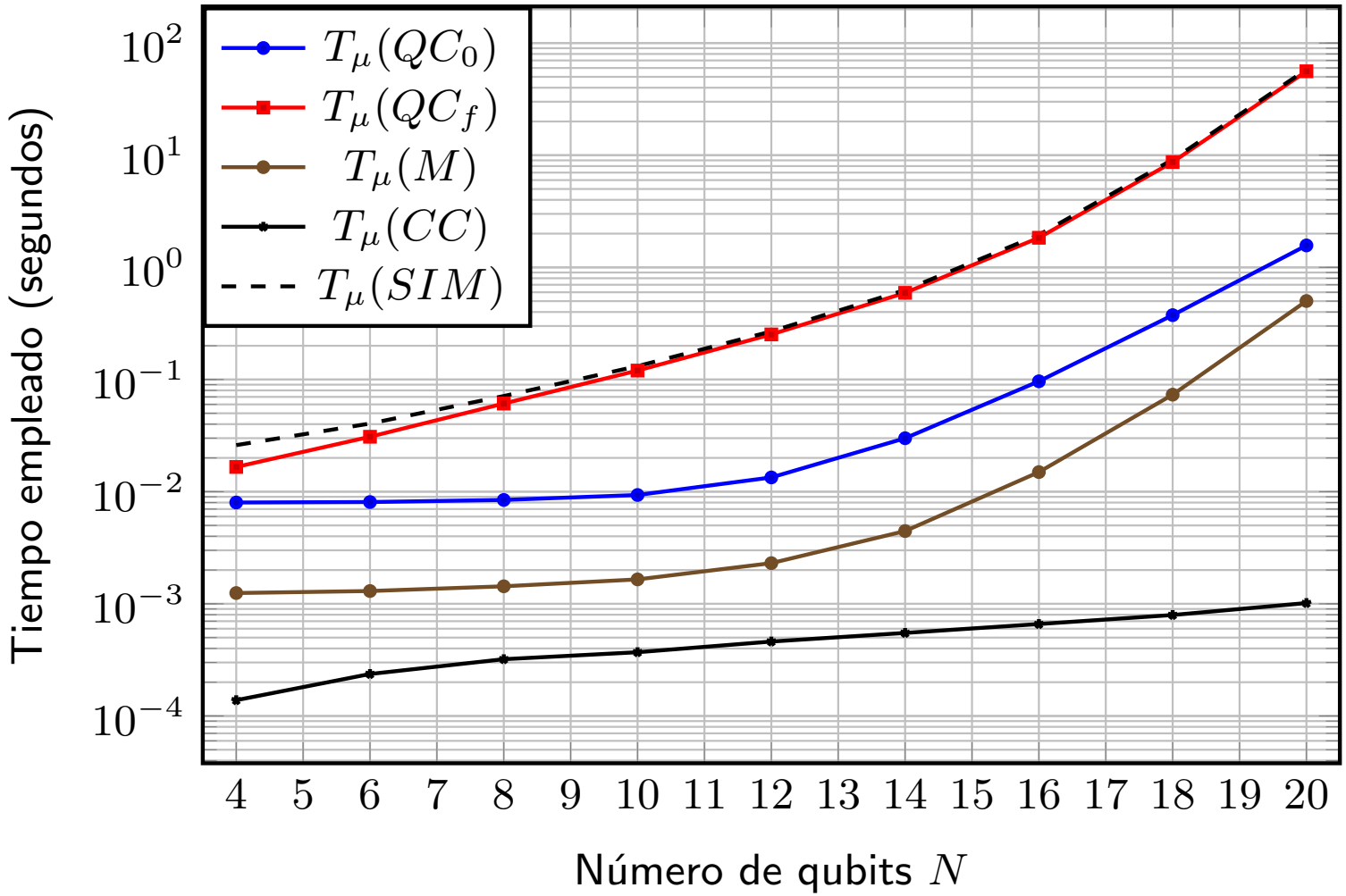


Figura: Tiempo de simulación en escala logarítmica.

Espacio de la simulación

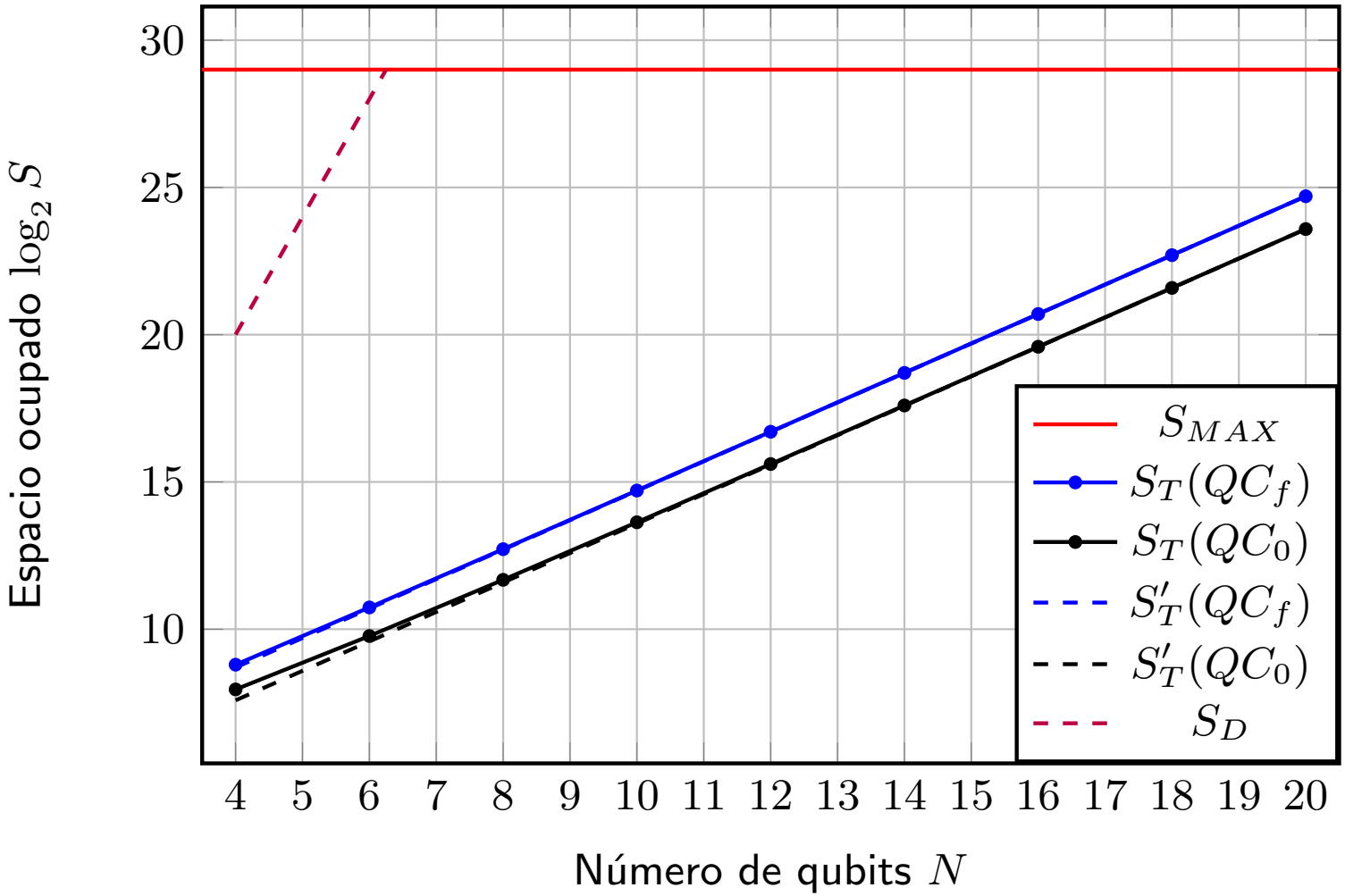


Figura: Espacio necesario para la simulación en bytes (escala logarítmica). El espacio requerido sin emplear matrices huecas, usando matrices densas se muestra como S_D. La memoria disponible para la simulación es $S_{MAX} = 2^{29}$.

Complejidad experimental del algoritmo de Simon

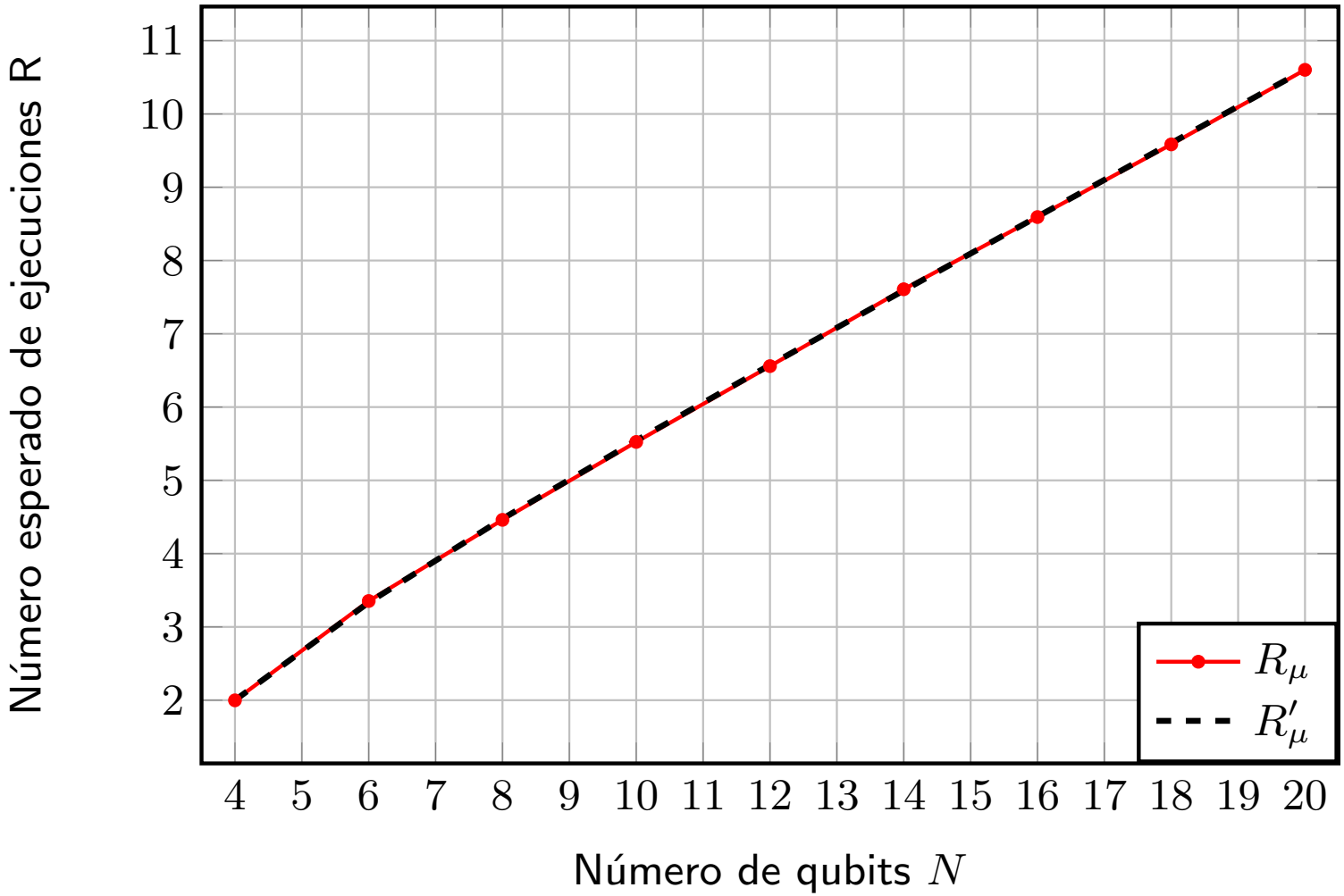


Figura: Número esperado de iteraciones a medida que aumentan los qubits. Se observa el valor experimental R_μ comparado con el teórico R'_μ.

Conclusiones

- La computación cuántica puede resolver algunos problemas **mucho** más rápido que la computación clásica.
- Realizar la simulación de un circuito cuántico es muy costoso.
- La simulación de circuitos permite comprobar los resultados teóricos.

Trabajo futuro

- Probar otros algoritmos cuánticos.
- Realizar el análisis de un algoritmo cuántico de forma automática, para determinar su complejidad.

Gracias por su atención.