Estimación de fase y algoritmo de Shor

Clase nº 12 de Computación Cuántica

J. P. Paz, C. Cormick

Depto. de Física, FCEyN, UBA

1er cuatrimestre 2006

La clase nº 12 se trató de:

- Cómo construir distintas evoluciones unitarias.
- El algoritmo de estimación de fase.
- El algoritmo de Shor.

Construcción de la compuerta CZ

- CZ es un operador unitario que actúa sobre 2 qubits:

$$CZ = (|0\rangle\langle 0|)_1 \; I_2 + (|1\rangle\langle 1|)_1 \; Z_2$$

(los roles del control y el *target* son intercambiables).

- Para implementar CZ, usamos que:

$$CZ = e^{-i\pi(|1\rangle\langle 1|)_1 \; (|1\rangle\langle 1|)_2} = e^{-i\frac{\pi}{4}(I-Z)_1 \; (I-Z)_2}$$

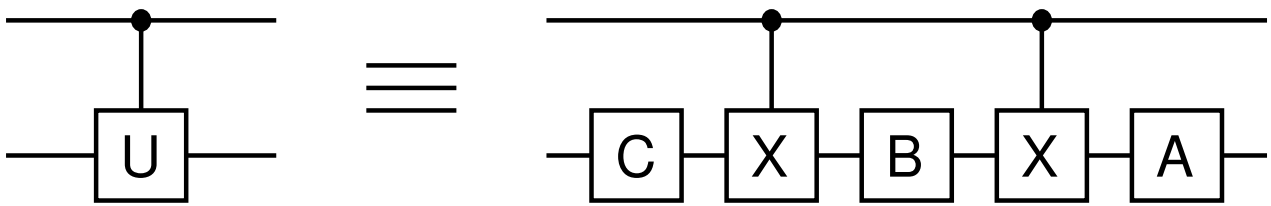
- Y como los operadores en el exponente conmutan,

$$CZ = e^{-i\frac{\pi}{4} I_1 I_2} \; e^{i\frac{\pi}{4} I_1 Z_2} \; e^{i\frac{\pi}{4} Z_1 I_2} \; e^{-i\frac{\pi}{4} Z_1 Z_2}$$

- Esto puede hacerse usando campos magnéticos en la dirección $\vec{z}$, y una interacción de la forma $H = \hbar\Omega Z_1 Z_2$.

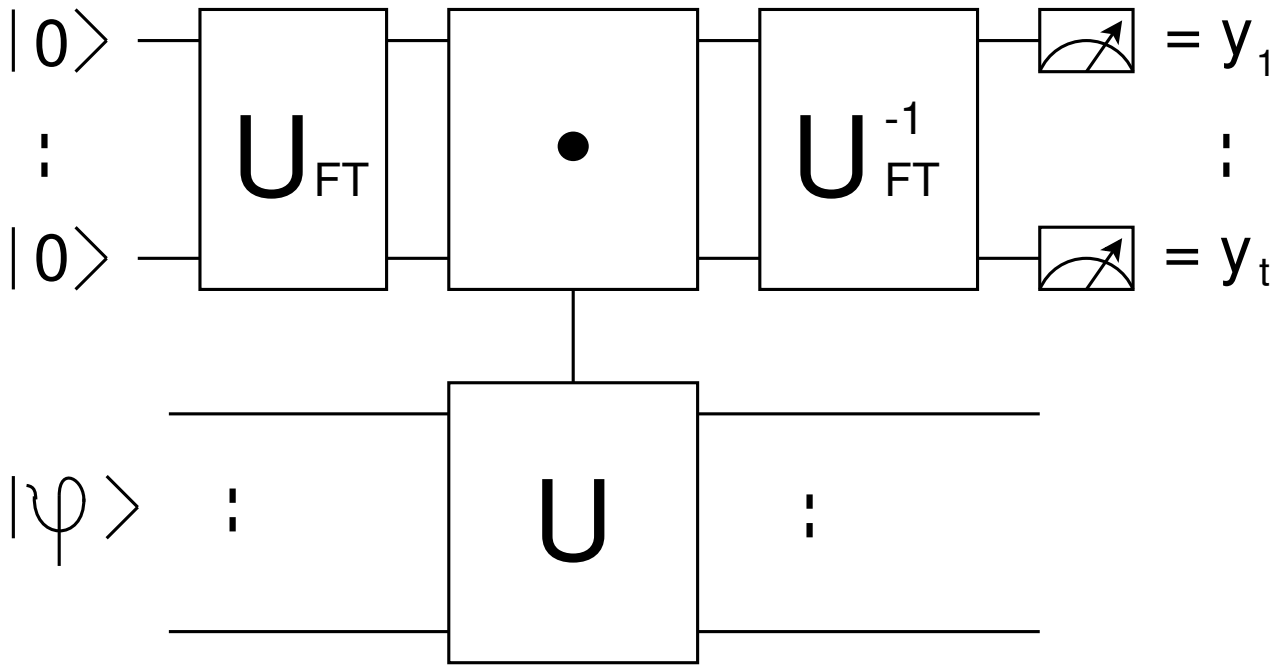
Implementación de cualquier evolución unitaria

- Cualquier evolución unitaria se puede realizar con rotaciones de 1 qubit y compuertas de 2 qubits tipo CZ o $CNOT$. A estas compuertas las llamamos "elementales".
- A su vez toda operación unitaria U de un qubit puede descomponerse: $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.
- ¿Cómo implementar C-U? Usando que todo U de 1 qubit puede escribirse como $U = AXBXC$ con $ABC = I$:



Algoritmo de estimación de fase

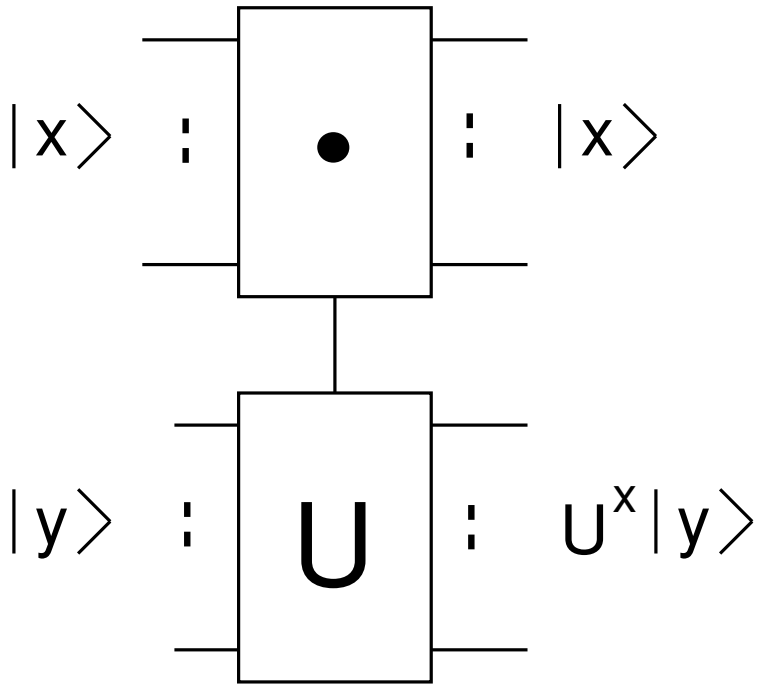
- Tenemos un operador unitario U que actúa sobre n qubits, y queremos hallar alguno de sus autovalores. El circuito para resolver este problema es el siguiente:



Algoritmo de estimación de fase

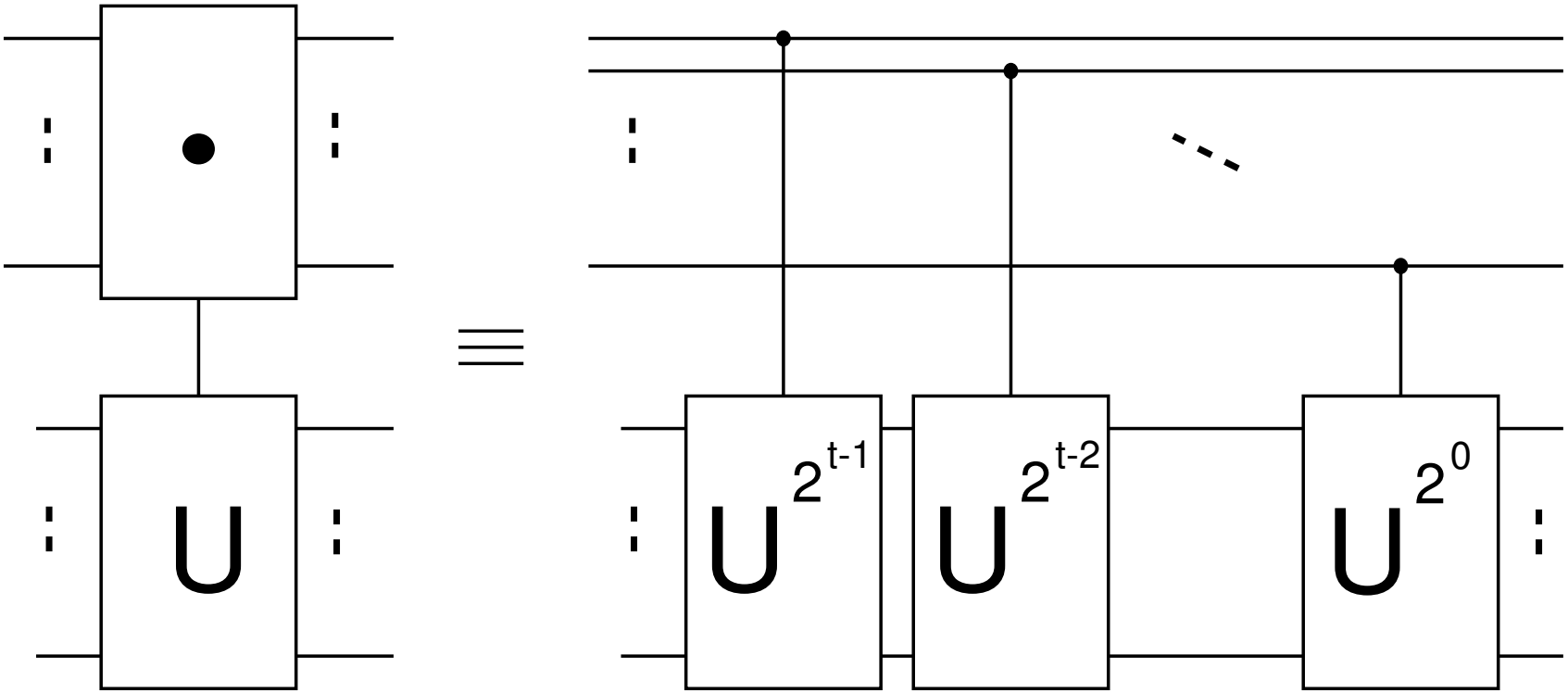
- Si el estado de entrada $|\varphi\rangle$ es autoestado de U con autovalor $e^{2\pi i\varphi}$, $\varphi \in [0, 1)$, al medir el primer registro obtenemos la mejor aproximación de φ con t bits.

- En el algoritmo de estimación de fase se usan la transformada de Fourier y su inversa, y el operador C-U generalizado, que se define como:



C-U generalizado

- El operador C-U generalizado se puede construir a partir de C-U^{2^k} $(k = 0, \ldots t-1)$en la forma:



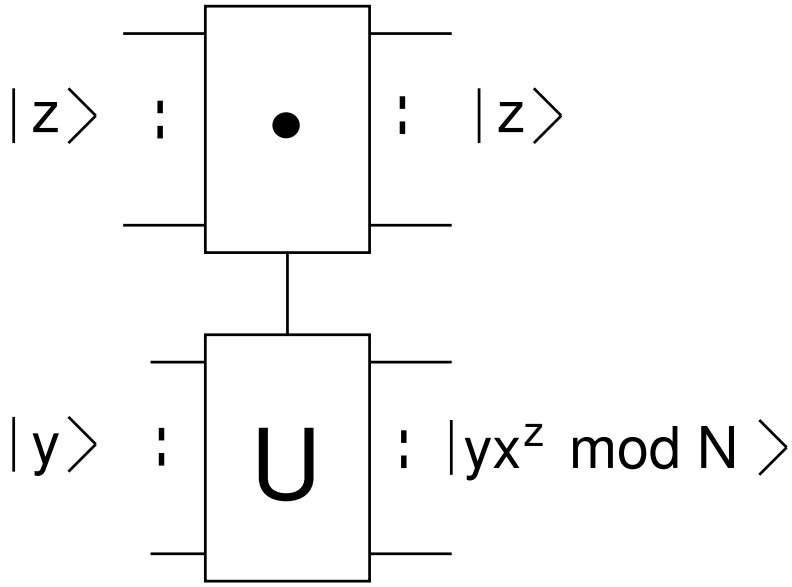
El algoritmo de Shor

- Problema: factorizar el número entero N.
- Dado un número $x < N$ coprimo con N tomado al azar, se define el orden de x mod N como el menor entero no nulo r tal que $x^r = 1 \pmod{N}$.
- Resulta entonces $x^r - 1 = 0 \pmod{N}$.
- Si r es par, entonces, $(x^{r/2} + 1)(x^{r/2} - 1) = 0 \pmod{N}$, o sea $(x^{r/2} + 1)$ y/o $(x^{r/2} - 1)$ deben contener factores comunes a N, y hallando éstos se puede factorizar N.
- La probabilidad de que r sea par es $1/2$. No hay algoritmos clásicos eficientes para hallar el orden.

El algoritmo de Shor

- El algoritmo de Shor encuentra el orden de x mod N utilizando un operador C-U generalizado, donde U es tal que $U|y\rangle = |xy \pmod N\rangle$ (la dimensión del espacio ahora es $L = 2^\ell$, con $L > N$).

- Con esta definición, C-U generalizado actúa así:



- El orden es el período de: $f(z) = x^z \pmod N$ (la "exponenciación modular").