Computación cuántica - 1er cuatrimestre 2006

Guía 5: Algoritmos cuánticos: Transformada de Fourier, estimación de fase, algoritmo de Shor

En esta guía, los estados de la base computacional se notan $|y\rangle$, con y un número entre 0 y $N-1$ (N es la dimensión del espacio de estados). Para sistemas de qubits, $N = 2^n$ y la descomposición binaria de y está dada por la n-upla $\vec{y} = (y_1, \ldots, y_n)$ según: $y = \sum_{j=1}^{n} y_j \, 2^{n-j}$, de modo que $|y\rangle \equiv |y_1\rangle \ldots |y_n\rangle$. En cualquier expresión de la forma $|x\rangle$ en que x sea un número arbitrario, se sobreentiende que se trata del estado $|x \pmod N\rangle$.

1. Mostrar que, para $\omega \in \mathbb{R}$, resulta:

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle = \frac{|0\rangle + e^{2\pi i (2^{n-1}\omega)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i (2^{n-2}\omega)}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i \omega}|1\rangle}{\sqrt{2}}$$

2. La transformada de Fourier discreta (QFT, por *quantum Fourier transform*) y su inversa actúan sobre los estados de la base computacional $\{|0\rangle, \ldots, |N-1\rangle\}$ de un espacio de dimensión N en la forma:

$$QFT_N |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle, \qquad QFT_N^{-1} |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i x y / N} |y\rangle$$

   a) Calcular $(QFT_N)^2 |x\rangle$ y $(QFT_N)^4 |x\rangle$.

   b) Indicar los posibles autovalores de QFT_N.

3. Se quiere factorizar el número impar N, que tiene al menos dos factores primos distintos. Los pasos para ello son:

   a) Se toma al azar un número x coprimo con N.

   b) Se calcula $r =$ orden de x mod N. Si r es impar, hay que volver a *a*).

   c) Si r es par, se calcula $y = x^{r/2} \pmod N$. Resulta entonces $x^r = 1 \pmod N$, o sea $y^2 = 1 \pmod N$, y por lo tanto N divide a $y^2 - 1 = (y-1)(y+1)$. Si $y = 1$ o $y = N-1$, esto se cumple trivialmente y es necesario recomenzar el algoritmo. En caso contrario, $y-1$ e $y+1$ deben contener factores comunes a N, y hallando éstos se puede factorizar N.

   Realizar estos pasos para $N = 33$ y $x = 2, 5, 7, 13$.

4. Sea a coprimo con N, se define el operador U_a que actúa en la forma $U_a |x\rangle = |xa\rangle$. Sea r el orden de a mod N.

   a) ¿Cuáles son los posibles autovalores de U_a?

   b) Se definen los estados $|\psi_{k,1}\rangle = (1/\sqrt{r}) \sum_{j=0}^{r-1} e^{-2\pi i k j / r} |a^j\rangle$. Calcular $U_a |\psi_{k,1}\rangle$.

   c) Calcular $(1/\sqrt{r}) \sum_{k=0}^{r-1} |\psi_{k,1}\rangle$.

   d) Dado b coprimo con N, hallar un conjunto $|\psi_{k,b}\rangle$ de autoestados de U_a tales que $|b\rangle = (1/\sqrt{r}) \sum_{k=0}^{r-1} |\psi_{k,b}\rangle$ (¿dónde se usa que b es coprimo con N?).