Búsqueda del período y transformada de Fourier

Clase nº 11 de Computación Cuántica

J. P. Paz, C. Cormick

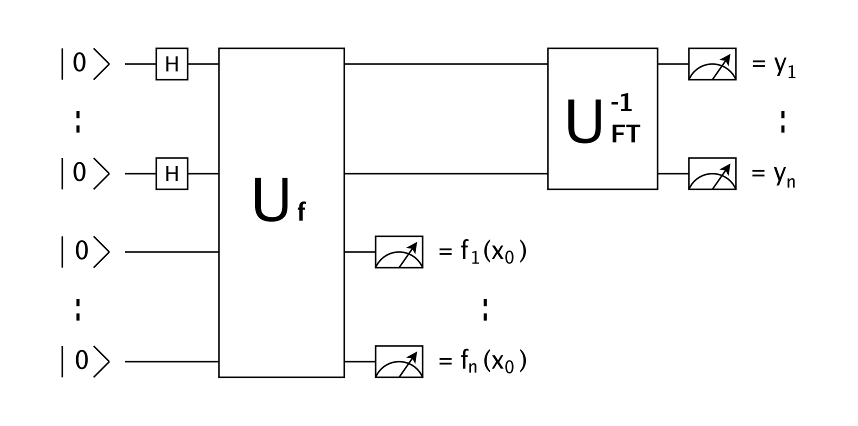
Depto. de Física, FCEyN, UBA

1$^{\mathrm{er}}$ cuatrimestre 2006

Búsqueda del período

- Se tiene $f : \mathbb{Z}_N \to \mathbb{Z}_N$, donde $N = 2^n$, tal que $f(x) = f(x+a) \;\; \forall x \;/\; x, x+a \in \mathbb{Z}_N$ y para algún $a \in \mathbb{Z}_N$ (la suma es la usual de enteros).
- El objetivo es hallar a (el período).
- El algoritmo para esto es una especie de generalización del de Simon.

El algoritmo de búsqueda del período



Las compuertas que se usan

- La compuerta U_f, que "evalúa" la función f:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

(x e y tienen n bits, $\oplus$ es la suma mod 2 bit a bit).

- La transformada de Hadamard:

$$H^{\otimes n}|x\rangle = \tfrac{1}{\sqrt{N}} \textstyle\sum_y (-1)^{x \cdot y}|y\rangle$$

donde $x \cdot y$ es el producto escalar bit a bit.

- Y U_{FT}^{-1}, la inversa de la "transformada de Fourier":

$$U_{FT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi ixy/N}|y\rangle, \quad U_{FT}^{-1}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi ixy/N}|y\rangle$$

Cómo funciona el algoritmo

- $|\psi(t_1)\rangle = (H^{\otimes n}|0\rangle)\ |0\rangle = \sum_x (1/\sqrt{N})\ |x\rangle\ |0\rangle$
- $|\psi(t_2)\rangle = U_f\ |\psi(t_1)\rangle = \sum_x (1/\sqrt{N})\ |x\rangle\ |f(x)\rangle$
- Si en la medición se obtiene $f(x_0)$, el estado luego es:

  $|\psi(t_3)\rangle = \left\{ \sum_{j=0}^{M-1} (1/\sqrt{M})\ |x_0 + ja\rangle \right\}\ |f(x_0)\rangle$

  donde $\{x_0, x_0 + a, \ldots x_0 + (M-1)a\}$ son los valores de $x \in \mathbb{Z}_N$ tales que $f(x) = f(x_0)$.
- $|\psi(t_4)\rangle = (U_{FT}^{-1} \otimes \hat{I})\ |\psi(t_3)\rangle =$

  $$= \sum_{y=0}^{N-1} \sum_{j=0}^{M-1} (1/\sqrt{MN})\ e^{-2\pi i (x_0 + ja) y / N}\ |y\rangle\ |f(x_0)\rangle$$

Cómo funciona el algoritmo

- Al medir, se tiene que:

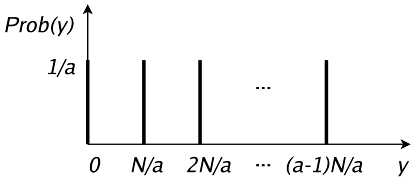
$$Prob(y) = \left| \sum_{j=0}^{M-1} \frac{e^{-2\pi i(x_0+ja)y/N}}{\sqrt{MN}} \right|^2 = \frac{1}{MN} \left| \sum_{j=0}^{M-1} e^{-2\pi ijay/N} \right|^2$$

- Supongamos N/a entero, entonces $N = Ma$, y resulta:

$$Prob(y) = \frac{1}{MN} \left| \sum_{j=0}^{M-1} e^{-2\pi ijy/M} \right|^2 = \begin{cases} \frac{1}{a} & \text{si } y = zM \ (z \in \mathbb{Z}) \\ 0 & \text{si no} \end{cases}$$

Cómo funciona el algoritmo

- Si $N = Ma$, la probabilidad de medir un dado valor de y es de la forma:



- Al repetir el algoritmo, se obtiene una secuencia de números $z_1 N/a, \ldots, z_k N/a$ $(z_j \in \mathbb{Z})$, a partir de la cual se puede estimar eficientemente a.
- Si N no es múltiplo de a, la probabilidad es más complicada pero es máxima en los enteros más cercanos a zN/a (con $z \in \mathbb{Z}$).

La transformada de Fourier

- Actúa en la forma: $U_{FT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i xy/N}|y\rangle$
- Es un operador unitario
  (mapea una base ortonormal en otra).
- $U_{FT}|0\rangle = H^{\otimes n}|0\rangle$
- Puede implementarse eficientemente a partir de compuertas "elementales".

Implementación de la transformada de Fourier

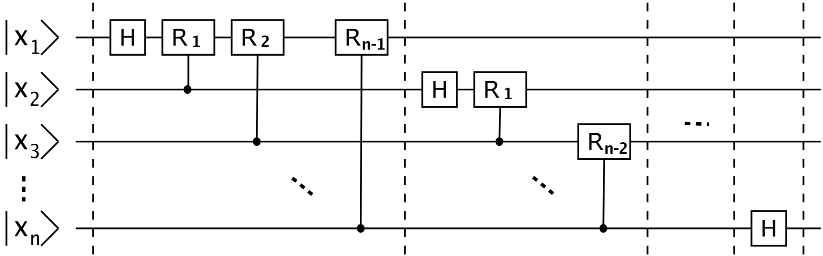
$$
\begin{aligned}
U_{FT}|x\rangle &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle, \qquad y = y_1 2^{n-1} + \ldots + y_n 2^0 \\
U_{FT}|x\rangle &= \frac{1}{\sqrt{N}} \sum_{y_1,\ldots y_n=0}^{1} e^{2\pi i (y_1/2^1)x} \ldots e^{2\pi i (y_n/2^n)x} |y_1\rangle \ldots |y_n\rangle = \\
&= \left(\sum_{y_1=0}^{1} \frac{e^{2\pi i (y_1/2^1)x}}{\sqrt{2}} |y_1\rangle \right) \ldots \left(\sum_{y_n=0}^{1} \frac{e^{2\pi i (y_n/2^n)x}}{\sqrt{2}} |y_n\rangle \right) = \\
&= \bigotimes_{j=1}^{n} \frac{|0\rangle + e^{2\pi i x/2^j} |1\rangle}{\sqrt{2}}
\end{aligned}
$$

Implementación de la transformada de Fourier

- Además $x = x_1 2^{n-1} + \ldots + x_n 2^0$, con lo cual:

$$
\begin{aligned}
U_{FT}|x\rangle &= \bigotimes_{j=1}^{n} \frac{|0\rangle + e^{2\pi i (x_1 2^{n-1} + \ldots + x_n 2^0)/2^j}|1\rangle}{\sqrt{2}} = \\
&= \left(\frac{|0\rangle + e^{2\pi i x_n/2}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{2\pi i (x_{n-1}/2 + x_n/4)}|1\rangle}{\sqrt{2}}\right)\ldots \\
&\quad \ldots\left(\frac{|0\rangle + e^{2\pi i (x_1/2 + x_2/4 + \ldots + x_n/2^n)}|1\rangle}{\sqrt{2}}\right)
\end{aligned}
$$

Implementación de la transformada de Fourier



con $R_j = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^{j+1}} \end{pmatrix}$
(y los qubits quedan ordenados al revés).