Algoritmo de Grover

Clase nº 10 de Computación Cuántica

J. P. Paz, C. Cormick

Depto. de Física, FCEyN, UBA

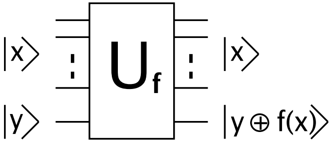
1$^{\text{er}}$ cuatrimestre 2006

El algoritmo de Grover

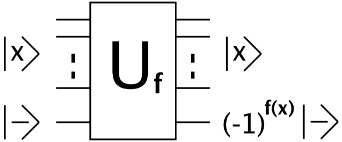
- Es el primero que muestra una superioridad de las computadoras cuánticas sobre las clásicas, en un problema que puede tener alguna utilidad (búsqueda).
- Se tiene $f : \{0,1\}^n \to \{0,1\}$, con la promesa de que
  $$f(x) = \begin{cases} 1 & x = x_0 \\ 0 & x \neq x_0 \end{cases} \qquad \text{(para algún } x_0\text{).}$$
  El objetivo es hallar x_0.
- Clásicamente hay que evaluar la función un número de veces de orden 2^n.
- Cuánticamente el número puede reducirse a orden $\sqrt{2^n}$ (la complejidad del problema sigue siendo exponencial).

Las compuertas que se usan

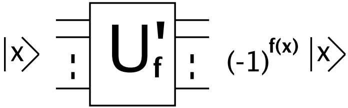
- Hasta ahora "evaluamos" f usando la compuerta:



- Si el segundo registro se prepara en el estado $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, la acción de U_f es:



- Podemos ignorar el registro auxiliar, y definir una compuerta U_f':



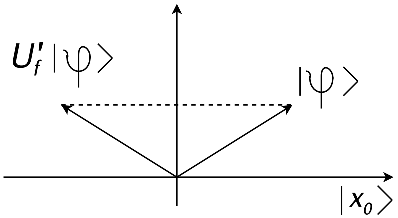
Las compuertas que se usan

- Para la función f que nos interesa, el efecto de U'_f es:

$$U'_f|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & x \neq x_0 \\ -|x\rangle & x = x_0 \end{cases}$$

- O sea, $U'_f = I - 2|x_0\rangle\langle x_0|$

- El efecto de U'_f es invertir la componente en la dirección de $|x_0\rangle$:



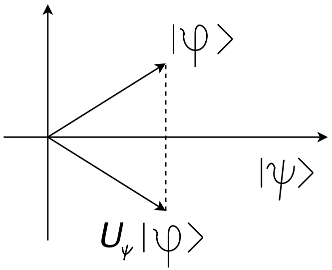
Las compuertas que se usan

- Además definimos otro operador unitario parecido,

$$U_\psi = -I + 2|\psi\rangle\langle\psi|$$

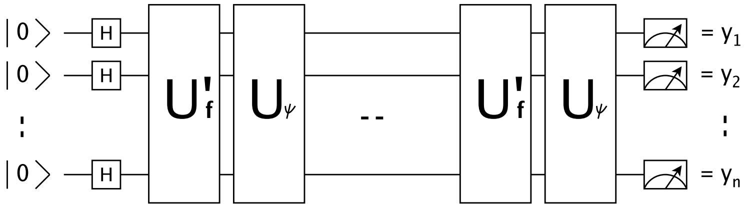
donde $|\psi\rangle = H^{\otimes n}|0\rangle = (1/\sqrt{2^n})\sum_x |x\rangle$.

- El efecto de U_ψ es invertir todas las componentes en direcciones perpendiculares a $|\psi\rangle$ (o sea, refleja respecto de $|\psi\rangle$):



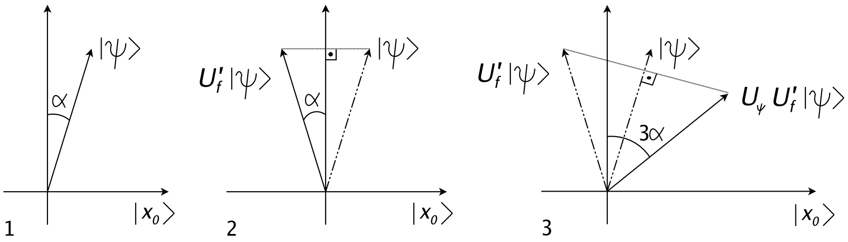
El algoritmo de Grover

- El algoritmo de Grover consiste en preparar el estado $|\psi\rangle$, luego aplicar reiteradamente el operador de Grover $G = U_\psi U_f'$, y finalmente medir.



El efecto del algoritmo de Grover

- El estado inicial es $|\psi\rangle$ (1); luego se aplica U'_f, que invierte la componente $|x_0\rangle$ (2), y después U_ψ, que refleja respecto de $|\psi\rangle$ (3); la combinación de estas dos inversiones es una rotación en ángulo 2α (que se repite).



El efecto del algoritmo de Grover

- El estado inicial forma con la "dirección" ortogonal a $|x_0\rangle$ un ángulo $\alpha \sim sen(\alpha) = (1/\sqrt{2^n})$.
- En cada aplicación de G, el estado se rota un ángulo 2α hacia $|x_0\rangle$. Al cabo de t iteraciones, el ángulo es $(2t+1)\alpha$.
- Hay que dejar de iterar cuando el ángulo es cercano a $\pi/2$, o sea luego de $t \sim \sqrt{2^n}\ \pi/4$ repeticiones.
- Finalmente se mide, y con alta probabilidad se obtiene x_0.