Computación cuántica - 1er cuatrimestre 2006
Guía 4: Algoritmos de Deutsch-Jozsa, Bersntein-Vazirani, Simon, Grover

En esta guía, los estados de la base computacional se notan $|\vec{x}\rangle = |x_1\rangle \dots |x_n\rangle$, con $x_j \in \{0,1\}$.

1. Dada una función $f : \{0,1\}^n \to \{0,1\}$, se define el operador U_f que actúa en la forma: $U_f|\vec{x}\rangle|k\rangle = |\vec{x}\rangle|k \oplus f(\vec{x})\rangle$ (la notación $a \oplus b$ se usa para $a+b$ módulo 2).
   a) ¿Cuál es la función f para la que U_f corresponde a la compuerta $CNOT$?
   b) Ver que U_f transforma $|\vec{x}\rangle|-\rangle$ en $(-1)^{f(\vec{x})}|\vec{x}\rangle|-\rangle$.
   c) El item *b*) muestra que con un qubit auxiliar en el estado $|-\rangle$ y una aplicación de U_f se puede implementar el operador $\widetilde{U}_f$ que transforma $|\vec{x}\rangle$ en $(-1)^{f(\vec{x})}|\vec{x}\rangle$; mostrar cómo una sola aplicación de C-$\widetilde{U}_f$ permite implementar U_f.

2. La compuerta de Hadamard H actúa sobre el estado de la base computacional de un qubit $|k\rangle$ en la forma $H|k\rangle = (|0\rangle + (-1)^k|1\rangle)/\sqrt{2}$. La transformada de Hadamard $H^{\otimes n}$ es el operador que aplica compuertas de Hadamard sobre n qubits a la vez. Mostrar que:
$$H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z}} (-1)^{\vec{x}\cdot\vec{z}} |\vec{z}\rangle$$

3. Mostrar que:
$$H^{\otimes n}\left(\frac{|\vec{x}\rangle + |\vec{x} \oplus \vec{s}\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2^{n-1}}} \sum_{\vec{z} \in s^\perp} (-1)^{\vec{x}\cdot\vec{z}} |\vec{z}\rangle$$
   donde $\vec{x} \oplus \vec{s}$ es la n-upla que se obtiene al sumar $\vec{x}$ y $\vec{s}$ componente a componente módulo 2, y $s^\perp$ es el espacio de las n-uplas binarias ortogonales a s, o sea $s^\perp = \{\vec{z} \;/\; \vec{z}\cdot\vec{s} = 0 \pmod 2\}$.

4. Se nota $\mathbb{Z}_2^n$ al espacio de las n-uplas binarias; sea W un subespacio de $\mathbb{Z}_2^n$ con dimensión m (o sea, una base de W son m elementos cuyas combinaciones lineales, con coeficientes binarios, generan todos los elementos de W). Sea $\vec{w}_1, \dots, \vec{w}_k$ una sucesión al azar de elementos de W. Llamamos V_i al subespacio de $\mathbb{Z}_2^n$ generado por $\vec{w}_1, \dots, \vec{w}_i$, y $N(j)$ al menor índice i tal que la dimensión de V_i es j; o sea, $N(j)$ es la cantidad de elementos de la sucesión (en orden) que hay que tomar para obtener j de ellos que sean linealmente independientes. $N(m)$ es entonces el menor índice i tal que $V_i = W$. Mostrar que el valor de expectación de $N(m)$ es menor o igual que $m + 1/3$ (ver que esto permite acotar el número promedio de iteraciones en el algoritmo de Simon).
   Ayuda: definir $M(1) = \langle N(1)\rangle$, $M(j) = \langle N(j) - N(j-1)\rangle (j > 1)$, de modo que $\langle N(m)\rangle = = M(1) + \dots + M(m)$. Ver que $M(j)$ es la cantidad promedio de elementos al azar que hay que agregar a un subespacio de dimensión $j-1$ para llevarlo a uno de dimensión j.

5. *a*) Sea U_0 tal que $U_0|\vec{0}\rangle = |\vec{0}\rangle,\ U_0|\vec{x}\rangle = -|\vec{x}\rangle\ \forall\ \vec{x} \neq \vec{0}$. Mostrar que $U_0 = -I + 2|\vec{0}\rangle\langle\vec{0}|$.
   b) Sea $|\psi\rangle = H^{\otimes n}|\vec{0}\rangle$, y $U_\psi = H^{\otimes n} U_0 H^{\otimes n}$. Mostrar que $U_\psi = -I + 2|\psi\rangle\langle\psi|$.
   c) Probar que un estado $|\phi\rangle = \sum_{\vec{x}} c_{\vec{x}}|\vec{x}\rangle$ es ortogonal a $|\psi\rangle$ si y sólo si $\sum_{\vec{x}} c_{\vec{x}} = 0$.
   d) Probar que U_ψ invierte los coeficientes respecto del promedio, o sea, si para el estado $|\phi\rangle = \sum_{\vec{x}} c_{\vec{x}}|\vec{x}\rangle$ se define la amplitud promedio $\mu = (1/N)\sum_{\vec{x}} c_{\vec{x}}$, entonces resulta $U_\psi|\phi\rangle = \sum_{\vec{x}}(2\mu - c_{\vec{x}})|\vec{x}\rangle$ (y como $|\psi\rangle$ tiene todos sus coeficientes iguales, $U_\psi|\psi\rangle = |\psi\rangle$).

6. Sea $f(\vec{x})$ una función con t soluciones (valores de $\vec{x}$ para los que $f(\vec{x}) = 1$). Hallar el número óptimo de iteraciones en el algoritmo de Grover para hallar alguna de las soluciones.