Computación cuántica - 1$^{\text{er}}$ cuatrimestre 2006
Guía 3: Modelo de circuitos - Compuertas básicas

1. Dada una función $f(x)$ desarrollable en serie de potencias, $f(x) = \sum_{j=0}^{\infty} f_j x^j$, y una matriz cuadrada A, se define $f(A) = \sum_{j=0}^{\infty} f_j A^j$. Mostrar que:

   a) si A es diagonalizable, $A = \sum_k a_k |\phi_k\rangle\langle\phi_k|$, resulta $f(A) = \sum_k f(a_k)|\phi_k\rangle\langle\phi_k|$.

   b) si A es tal que $A^2 = I$, entonces $e^{iAx} = cos(x)I + isen(x)A$.

2. Dado el estado de un qubit $|\psi\rangle = a|0\rangle + b|1\rangle$, se llama "vector de Bloch" al formado por los valores de expectación de las matrices de Pauli en el estado $|\psi\rangle$: $\vec{v} = (v_x, v_y, v_z) = = (\langle X\rangle, \langle Y\rangle, \langle Z\rangle)$.

   a) Calcular $\vec{v}$ en función de a, b.

   b) Mostrar que $\vec{v}^2 = 1$, y por lo tanto los posibles $\vec{v}$ están en el borde de una esfera de radio 1 (la "esfera de Bloch").

   c) Mostrar que la aplicación del operador $R_x(\phi) = e^{-i\phi\sigma_x/2}$ rota $\vec{v}$ en un ángulo ϕ en torno del eje x (usar el resultado del ejercicio 1.*b*, y pensar cómo se transforman las componentes de un vector al rotarlo respecto del eje x).

3. Cualquier operador unitario de un qubit U puede escribirse como $U = e^{i\alpha} R_{\hat{n}}(\phi)$, con $R_{\hat{n}}(\phi) = e^{-i\phi\hat{n}\cdot\vec{\sigma}/2}$. Hallar valores de $\alpha, \hat{n}, \phi$ que correspondan a las compuertas:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

4. Probar que $HXH = Z$, $HYH = -Y$, $HZH = X$.

5. *a)* Probar que $XR_y(\phi)X = R_y(-\phi)$, $XR_z(\phi)X = R_z(-\phi)$.

   b) Cualquier operador unitario sobre un qubit U puede descomponerse en la forma $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$; probar que puede entonces escribirse $U = e^{i\alpha} AXBXC$, con $ABC = I$.
   Ayuda: tomar $A = R_z(\beta)R_y(\gamma/2)$, $B = R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$.

6. Probar que la compuerta C-U (U controlado):

   a) es equivalente a $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$ (donde el primer qubit es el control).

   b) no es equivalente a C-$e^{i\phi}U$ (excepto cuando $\phi = 2k\pi, k \in \mathbb{Z}$).

7. El error al aproximar la compuerta U por el operador V (U y V unitarios) se define como $E(U,V) = max_{|\psi\rangle} ||(U-V)|\psi\rangle||$; mostrar que $E(U_2U_1, V_2V_1) \leq E(U_2, V_2) + E(U_1, V_1)$.

8. *a)* Si $R_n(\alpha)$ y $R_n(\beta)$ son dos rotaciones en torno del mismo eje, mostrar que $E(R_n(\alpha), R_n(\beta)) = |e^{i\alpha/2} - e^{i\beta/2}| \leq |(\alpha-\beta)/2|$.

   b) Sea $\alpha \in [0, 2\pi)$ tal que $\beta/\pi \notin \mathbb{Q}$. Mostrar que dados $\epsilon > 0$, $\theta \in [0, 2\pi)$, existe $k \in \mathbb{N}$ tal que $E(R_n(\alpha)^k, R_n(\theta)) < \epsilon$ (pista: tomar un número $N \in \mathbb{N}$ / $N > 2\pi/\epsilon$, y considerar los ángulos $\alpha_j = j\alpha$ con $j = 0, 1, \ldots, N$; ver que debe haber dos de ellos cuya distancia –sobre el círculo de radio 1– sea menor que ϵ).