Universidad Complutense de Madrid

Curso de Master 2007-08

Información y Computación Cuánticas

De la siguiente lista de problemas correspondiente a la parte II del curso, los matriculados en el presente curso deben entregar como mínimo dos problemas. Cada problema lleva una letra que indica el grado de dificultad relativo entre ellos: B=Bajo, M=Medio, A=Alto, y se tendrá en cuenta a la hora de calificar.

Los problemas pueden entregarse resueltos mediante envío por correo ordinario o por email si estan pasados a latex o similar, a la dirección indicada más abajo.

La fecha límite de entrega aparecerá en la página web del master:

http://www.ucm.es/info/giccucm/index.html

PARTE II: Puertas Lógicas Cuánticas, Teleportación, Codificación Densa, Criptografía, Algoritmos Cuánticos, Estados Bell, etc...

Enviar a: Miguel A. Martín-Delgado
Departamento de Física Teórica I,
Facultad de Ciencias Físicas,
Universidad Complutense
28040 MADRID.
mardel@miranda.fis.ucm.es

Problema 1. (B) Las puertas lógicas cuánticas CNOT y Fase-controlada se definen como

$$\begin{aligned} U_{\rm CNOT} = U_{\rm XOR} &= |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes U_{\rm NOT} \\ &= \frac{1}{2}(1+\sigma_3)\otimes 1 + \frac{1}{2}(1-\sigma_3)\otimes\sigma_1 \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \end{aligned}$$

$$U_{{\rm CPh}(\phi)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & {\rm e}^{{\rm i}\phi} \end{pmatrix}$$

Demostrar que la puerta CNOT se puede construir con 2 puertas Hadamard y una Fase-controlada con $\phi = \pi$. Construir el circuito cuántico asociado a esta descomposición de CNOT.

$$U_{\rm H} = \frac{1}{\sqrt{2}}(\sigma_1 + \sigma_3) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Problema 2. (B)

La puerta lógica de Toffoli actúa sobre 3 bits y se define como CCNOT (una NOT doblemente controlada):

$$U_{\mathrm{T}} := U_{\mathrm{CCNOT}}$$

i) Con ayuda de una Toffoli, construir una puerta NOT (monaria).
ii) Con ayuda de una Toffoli, construir una puerta AND (binaria). Esto es una versión reversible de la AND usual que es irreversible.
(NOTA: estos resultados junto con las relaciones de de Morgan se usan para demostrar la universalidad de la puerta Toffoli en computación clásica.)

Problema 3. (M) Argumentar que las siguientes operaciones con puertas lógicas cuánticas no contradicen el teorema de No-Clonación Cuántica:
i/ La evaluación de funciones Booleanas $f : \{0,1\}^m \to \{0,1\}$ definida por el siguiente operador unitario

$$U_f|x_1 \dots x_m\rangle_s|x_{m+1}\rangle_t := |x_1 \dots x_m\rangle_s|f(x_1 \dots x_m) \oplus x_{m+1}\rangle_t.$$

ii/ La evaluación de la puerta Toffoli con input bits $(1, x, 0), x = 0, 1$ produce una clonación aparente de la variable x dada por:

$$U_{\mathrm{CCNOT}}(1, x, 0) = (1, x, x).$$

Problema 4. (M) Hacer el protocolo de teleportación cuántica paso a paso, para cuando el estado que se comparte desde Alicia a Benito es el siguiente estado de Bell:

$$|\Phi^+\rangle_{\mathrm{AB}} := \frac{1}{\sqrt{2}}[|00\rangle_{\mathrm{AB}} + |11\rangle_{\mathrm{AB}}]$$

Problema 5. (A) Realizar un protocolo de teleportación cuántica que teleporte un estado de n qudits dado por:

$$|\varphi\rangle_{\mathrm{A}} := \sum_{\mathbf{p}\in\mathbf{Z}_D^n} \alpha_{\mathbf{p}}|\mathbf{p}\rangle, \quad \sum_{\mathbf{p}\in\mathbf{Z}_D^n} |\alpha_{\mathbf{p}}|^2 = 1,$$

desde Alicia hasta Benito. Se supone que para ello Alicia y Benito comparten n pares de Bell de qudits del tipo genérico $|\mathbf{i}\,\mathbf{j}\rangle_{\mathcal{B}}$ siguiente

$$|\mathbf{i}\,\mathbf{j}\rangle_{\mathcal{B}} := \bigotimes_{k=1}^{n} |i_k\; j_k\rangle_{\mathcal{B}} = \underset{\mathbf{k}}{\mathcal{S}} \varphi(\mathbf{i}\cdot\mathbf{k})|\mathbf{k}\;\mathbf{k}-\mathbf{j}\rangle,$$
$$|\mathbf{i}\,\mathbf{j}\rangle := \bigotimes_{k=1}^{n} |i_k\; j_k\rangle,$$

con $\mathbf{i},\mathbf{j} \in \mathbf{Z}_D^n$, y los simbolos definidos a la manera usada en clase:

$$\underset{k}{\mathcal{S}} := \frac{1}{\sqrt{D}} \sum_{k\in\mathbf{Z}_D}, \quad \delta(k) := \sqrt{D}\delta_{k,0}, \quad \varphi(k) := \mathrm{e}^{\frac{2\pi \mathrm{i}}{D}k},$$

elegidos de modo que se cumpla $\mathcal{S}_k\, \varphi(ik) = \delta(i)$ y $\mathcal{S}_k\, \delta(i-k)f(k) = f(i)$ $(i \in \mathbf{Z}_D)$.

Problema 6. (M) Hacer un escenario de Entanglement Swapping (Teleportación de Entanglement) entre Alicia, Carlos y Benito (sistemas A-C-B) suponiendo que el par de Bell compartido por Alicia-Carlos y Carlos-Benito está dado por:

$$|\Psi^+\rangle_{\mathrm{AB}} := \frac{1}{\sqrt{2}}[|01\rangle_{\mathrm{AB}} + |10\rangle_{\mathrm{AB}}]$$

Problema 7. (B) Consideremos un estado puro de un qubit dado por

$$|\Psi\rangle := \alpha_0|0\rangle + \alpha_1|1\rangle, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

La probabilidad de que al medir obtengamos el estado $|i\rangle$ es $|\alpha_i|^2$, con $i = 0, 1$. Consideremos además un estado mezcla de un qubit dado por

$$\rho := |\alpha_0|^2|0\rangle\langle 0| + |\alpha_1|^2|1\rangle\langle 1|.$$

También la probabilidad de que al medir obtengamos el estado $|i\rangle$ es $|\alpha_i|^2$, con $i = 0, 1$. ¿Son equivalentes las descripciones cuánticas de los estados $|\Psi\rangle$ y ρ?

Problema 8:Algoritmo de Grover (M)

Se nos da una lista de solo 4 elementos desordenados y equiprobables $\mathcal{L} = \{0, 1, 2, 3\}$, con el objeto de aplicar el algoritmo de Grover para encontrar cualquiera de esos 4 elementos. Como paso previo, necesitamos construir un oráculo cuántico para cada uno de elementos de la lista. Usando las relaciones siguientes

$$f_{x_0}(x) = \begin{cases} 0 & \text{si } x \neq x_0 \\ 1 & \text{si } x = x_0 \end{cases}$$

$$U_{f_{x_0}}|x\rangle|y\rangle = |x\rangle|y \oplus f_{x_0}(x)\rangle$$

y el estado inicial $|\Psi\rangle_{\text{in}}$ dado por

$$|\Psi\rangle_{\text{in}} = \frac{1}{2^{3/2}}[|00\rangle + |01\rangle + |10\rangle + |11\rangle] \otimes (|0\rangle - |1\rangle)$$

se pide construir los 4 oráculos $U_0 := U_{00}, U_1 := U_{01}, U_2 := U_{10}, U_3 := U_{11}$. Para ello, calcular $U_{f_{x_0}}|\Psi\rangle_{\text{in}}$.

Problema 9:Algoritmo de Grover (A)

Se nos da de nuevo una lista de solo 4 elementos desordenados y equiprobables $\mathcal{L} = \{0, 1, 2, 3\}$, con el objeto de aplicar el algoritmo de Grover para encontrar el elmento $x_0 = 3$. Para ello, tomemos un registro cuántico de 2 qubits.

Se pide:

i) Calcular los operadores de Grover G_1, G_2

ii) Calcular el kernel de Grover $K = G_2 G_1$.

iii) Aplicar K a una superposción equiprobable de estados de la lista $\mathcal{L}$.

iv) ¿Cuántas iteraciones m del kernel K son necesarias para obtener el elmento 3 buscado?. ¿Con qué certeza?

Problema 10:Algoritmo de Grover (A)

Consideremos dos operadores de Grover G_1, G_2 dados por

$$G_1 = \alpha P_1 + \beta Q_1, \;\; P_1^2 = P_1, \; Q_1^2 = Q_1, \;\; P_1 + Q_1 = 1$$
$$G_2 = \gamma P_2 + \delta Q_2, \;\; P_2^2 = P_2, \; Q_2^2 = Q_2, \;\; P_2 + Q_2 = 1$$

donde $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ son números complejos de norma unidad. Tomemos ahora la siguiente elección:

$$P_1 = P_{x_0} = |x_0\rangle\langle x_0|$$
$$P_2 = \bar{P} = |k_0\rangle\langle k_0|, \quad |k_0\rangle = \frac{1}{\sqrt{N}}(1, \ldots, 1)^{\mathrm{t}}$$

Calcular la forma matricial de los operadores Grover G_1, G_2 en la base 2-dimensional expandida por los vectores

$$\{|x_0\rangle, |x_\perp\rangle := \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle\}$$

donde N es el número de elementos que forman la lista desordenada. Calcular el kernel de Grover $K = G_2 G_1$ en esta base cuando $\alpha = \gamma = -1$.

Problema 11:Algoritmo de Grover (A)

El kernel de Grover en la base expandida por los vectores $\{|x_0\rangle, |x_\perp\rangle := \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle\}$ (donde $|x_0\rangle$ es el item que andamos buscando entre N elementos) toma la siguiente expresión

$$K = \frac{1}{N} \begin{pmatrix} 1 + \delta(1-N) & -\beta(1+\delta)\sqrt{N-1} \\ (1+\delta)\sqrt{N-1} & \beta(1+\delta-N) \end{pmatrix}$$

con β, δ dos números complejos de módulo unidad. En esta base, el estado inicial es

$$|x_{\mathrm{in}}\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}|x_\perp\rangle$$

Sean $\{|\kappa_1\rangle, |\kappa_2\rangle\}$, los autovectores del Grover kernel K con autovalores $\mathrm{e}^{\mathrm{i}\omega_1}, \mathrm{e}^{\mathrm{i}\omega_2}$.

i) Demostrar que la amplitud de probabilidad de encontrar el item x_0 despues de $m \in \mathbb{N}$ intentos es

$$\langle x_0|K^m|x_{\mathrm{in}}\rangle = \mathrm{e}^{\mathrm{i}m\omega_1}\left(\frac{1}{\sqrt{N}} + (\mathrm{e}^{\mathrm{i}m\Delta\omega} - 1)\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{\mathrm{in}}\rangle\right)$$

con $\Delta\omega = \omega_2 - \omega_1$.

ii) Comprobar que los autovalores de K sin normalizar son

$$|\kappa_{1,2}\rangle \propto \begin{pmatrix} \frac{A \mp \sqrt{-4(\mathrm{Det}K)N^2 + A^2}}{2(1+\delta)\sqrt{N-1}} \\ 1 \end{pmatrix}$$

con $A := (\beta - \delta)N + (1 - \beta)(1 + \delta)$.

iii) Calcular el comportamiento asintótico del vector $|\kappa_2\rangle$ cuando $N \gg 1$ comprobando que

$$|\kappa_2\rangle \propto \begin{pmatrix} \frac{\beta-\delta}{1+\delta}\sqrt{N} + O(\frac{1}{\sqrt{N}}) \\ 1 \end{pmatrix}$$

Ver que si $\beta \neq \delta$, entonces $|\kappa_2\rangle \sim |x_0\rangle$, luego $\langle x_0|\kappa_2\rangle\langle\kappa_2|x_{\text{in}}\rangle = O(\frac{1}{\sqrt{N}})$.