Tarea-1CC

Curso: Introducción a Teoría de la Computación
Profesores: Laura Elena Morales Guerrero y Sergio Rajsbaum. Ayudante: Fabiola Zárate

Fecha: Mayo 12, 2005; entregar martes mayo 17
– Se puede entregar en equipos de a lo más dos personas, pero cada una debe entregarla por separado, indicando el nombre de la otra persona
– Explica en detalle todas tus respuestas

"I've got some grad student. He's thinking about the meaning of quantum mechanics. He's doomed!"
-John McCarthy

1. Lea el artículo de Deutsch y resuma su contenido en no ms de cuartilla y media: Deutsch, D. "Quantum Theory, The Church-Turing Principle and the Universal Quantum Computer" Proceedings Royal Society London, Vol A400 (1985), pp.07-117.

2. En computación probabilística clásica nos encontramos con un árbol de probabilidades. Cada nodo en el árbol se etiqueta con una configuración (la descripción instantánea del contenido de la cinta, la(s) localización (es) de las cabezas) del estado interno de la MT. Las aristas del árbol se etiquetan con números reales en el intervalo [0,1] y corresponden a las probabilidades de transición de una configuración "padre" a una configuración "hijo". Cada nivel del árbol representa un paso (en sentido temporal) de manera que la profundidad del árbol representa el tiempo de acción de la máquina. Se pueden asignar probabilidades a cada nodo multiplicando las probabilidades a lo largo de la trayectoria desde la raíz hasta ese nodo. Clásicamente, la probabilidad de que la computación esté en la configuración c al tiempo t es la suma de las probabilidades asignadas a cada nodo al nivel t al cual se ha asignado la configuración c. Este árbol representa una computación probabilística si satisface la dos restricciones de:
   a) Localidad: la probabilidad asignada a cada arista de un nodo a otro, debe corresponder a la acción de un paso de la MTP.
   b) Probabilidad Clásica: La suma de las probabilidades en cualquier nivel debe ser 1.

   Demuestre que si la suma de las probabilidades en las aristas que salen de cada nodo es igual a uno, entonces, la restricción de probabilidad clásica se satisface.

3. En una computación cuántica, en vez de asignar probabilidades en valores reales, se asignan "amplitudes de probabilidad" en valores complejos (cuya norma es, a lo más, uno). La amplitud de cada nodo en el árbol de la computación es meramente el producto de las amplitudes a lo largo de la trayectoria de cada nodo y la amplitud asociada al estar en la configuración c al tiempo t, es la suma de las amplitudes de todos los nodos en el nivel t etiquetado con c. Las amplitudes de probabilidad corresponden a probabilidades de la siguiente forma: la probabilidad es el valor absoluto del cuadrado de la amplitud. Esta etiquetación del árbol debe a su vez, satisfacer las dos restricciones:
   a) Localidad: la misma que la clásica; la etiquetación del árbol debe corresponder a la acción de la MT.
   b) Probabilidad Cuántica: Si se representa a la computación cuántica por una matriz M, entonces, M debe ser unitaria (lo que quiere decir que la transpuesta conjugada de M es igual a su inversa). Esta condición de probabilidad cuántica implica que la suma de las *probabilidades* en cada nivel sea uno ($\Sigma|\omega_i|^2 = 1$). Ahora, sin embargo, no es suficiente requerir tan sólo que la suma de los cuadrados de las amplitudes que salen de cada nodo sea uno. Esto es debido a los efectos de *interferencia* (cancelación) entre las configuraciones.

   Dé un ejemplo de un árbol etiquetado donde la suma de las probabilidades que sale de cada nodo sea uno pero en el que la suma de las amplitudes en algún nivel no lo sea. (Sugerencia: con dos niveles es suficiente.) Encuentre

4. a) Muestre que si todas las entradas en una matriz M son números reales en el intervalo $[-1, 1]$ entonces M es unitaria $\iff$ es ortonormal, es decir, que el producto punto de cualquier par de filas o de columnas distintas es siempre cero y el producto de una fila o una columna consigo misma es uno.
   b) Demuestre que M tiene inversa. Para tener inversa una matriz debe ser cuadrada pero no todas las matrices cuadradas tienen inversa.

   Nótese que una matriz unitaria tiene inversa, lo que significa, a diferencia de la computación clásica, que la computación cuántica es, necesariamente, *reversible*.

5. Demuestre que el conjunto de puertas lógicas: $\{I, X, Y, Z\}$ que actúan sobre un qubit sencillo y está definido por:
   $I \equiv |0><0| + |1><1| = identidad$
   $X \equiv |0><1| + |1><0| = NOT$
   $Z \equiv P(\pi)$
   $Y \equiv iXZ$
   $H \equiv 1/\sqrt{2}[(|0> + |1>)<0| + (|0> - |1>)<1|]$
   (donde H representa una rotación de Hadamard), es un grupo bajo la multiplicación. Es decir, se satisfacen los axiomas:
   Asociatividad $(a * b) * c = a * (b * c)$
   Elemento identidad $e * a = a * e = a$
   Elemento inverso $a * b = b * a = e$
   ¿Es necesario agregar el axioma de cerradura?
   Cerradura $\forall a, b \in G, a * b \in G$

   El operador P está representado por la matriz $P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & \exp i\theta \end{pmatrix}$ y también se escribe como: $|0><0| + \exp(i\theta)|1><1|$.

6. Considere el par de qubits $|0>$ y $|1>$ que bajo cierta transformación unitaria cambian a:
   $|0> \rightarrow a|0> + b|1>$
   $|1> \rightarrow c|0> + d|1>$
   ¿Cuál es la transformación unitaria que la describe?
   (Sugerencia: encuentre la matriz $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ que satisfaga $|a|^2 = |b|^2 = 1/2$ y $|c|^2 = |d|^2 = 1/2$

7. Considere un registro de memoria con tres qubits originalmente en el estado $|0>$ cada uno. Es decir, $|0>, |0>, |0>$. Coloque cada estado en una superposición de $|0>$ y $|1>$ rotando cada $|0>$ por $\pi/4$ usando el operador unitario $U(\pi/4)$ (donde $U(\pi/4) = \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$). Muestre que el estado de cada qubit es:
   $\frac{1}{\sqrt{2}}(|0> + |1>)$, $\frac{1}{\sqrt{2}}(|0> + |1>)$, $\frac{1}{\sqrt{2}}(|0> + |1>)$. Cree un registro de memoria como el producto directo de los tres qubits anteriores y muestre que el estado en conjunto es:
   $\frac{1}{2(\sqrt{2})}(|000> + |001> + |010> + |011> + |100> + |101> + |110> + |111>)$

   "Lea" el registro (al observar el sistema, la superposición colapsará a cualquiera de los ocho eigenestados con igual probabilidad) y obtenga, por ejemplo, el valor $|011>$. Convierta la cuerda qubit (011) a base 10 y demuestre que equivale al número 3. Este número es un número creado estrictamente al azar. Es uno de los ocho posibles valores en el intervalo $[0, 7]$.