Tarea-Examen de CC

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

Fecha: Mayo 31, 2005; entregar jueves Junio 7

– 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

1. El operador $\sqrt{NOT}$ no tiene símil clásico. Demuestre que si la acción de la puerta $\sqrt{NOT}$ sobre un qubit sencillo se define como: $\sqrt{NOT} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$ la matriz que lo representa es unitaria (y, por lo tanto, reversible). Aplique consecutivamente el operador $\sqrt{NOT}$ para comprobar que $\sqrt{NOT}.\sqrt{NOT} = NOT$. Para que este operador actúe sobre 4 qubits, forme el producto directo de este operador con los operadores identidad colocados en las posiciones "muertas". El operador deberá actuar sobre el cuarto de los 4 qubits. Es decir: $\sqrt{NOT}[4,4] = \hat{I} \otimes \hat{I} \otimes \hat{I} \otimes \sqrt{NOT}$ ¿De qué tamaño es la matriz resultante? Esbózela. Dé un ejemplo de los eigenvectores del sistema de 4-qubits. Haga actuar el operador $\sqrt{NOT}[4,4].\sqrt{NOT}[4,4]$ sobre cada uno de los 16 eigenvectores del sistema para construir la tabla de verdad del operador. Para simular el cuadrado de la raíz cuadrada de la operación NOT, son necesarios 4 qubits.

2. Sean c y a los operadores de creación y aniquilación (no confundir con fenómenos de interferencia) definidos respectivamente por: $c = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ y, $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. El operador de creación convierte el estado cero al estado uno y el estado uno al estado nulo (i.e., un vector columna de ceros). El de aniquilación convierte el estado uno al cero y convierte el cero al nulo. Compruebe lo anterior. Existen versiones de estos operadores que actúan en el $i-$ésimo de cuatro bits usando el producto directo de uno de ellos en combinación con la identidad, como sigue:

$$c_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

   Obtenga la forma explícita de c_2. En general, c_i y a_i representan los operadores de creación y aniquilación que actúan sobre el $i-$ésimo de los k q-bits. Los operadores de creación y aniquilación son necesarios para mover los cursores de un circuito. Para moverse del sitio $i-$ésimo al $(i+1)$, se aniquila el cursor en el sitio i y se re-crea en el sitio $(i+1)$.

3. Generador de números al azar. Un método de generar una sucesión de enteros pseudoazarosos es comenzar con un entero N_0, $0 \leq N_0 < n$ y aplicar repetidamente la regla:

$$N_{k+1} = (1N_k + m) \mathrm{mod\, n},$$

   donde, $1, m, n$ son enteros fijos y $k = 1, 2, 3, ...$, para obtener los números $N_1, N_2, ..., N_k$.

El problema con la generación de estos números es que sus salidas son periódicas. Demuestre la aseveración anterior. (Sugerencia, considere p.ej., el generador $N_{k+1} = (6N_k+7) \bmod 5$, con $N_0 = 2$). Para evitar las limitantes que estos generadores presentan se proponen los llamados "generadores de registro desplazado". Considere el siguiente (en representación binaria):

$$N_k = N_{k-i} XOR N_{k-j}.$$

donde XOR es la negación condicionada:

$$\begin{aligned} XOR|00> &= |00> \\ XOR|01> &= |01> \\ XOR|10> &= |11> \\ XOR|11> &= |10> \end{aligned}$$

Produzca una sucesión al azar de no menos de 8 dígitos.

4. Considere la matriz $M = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Pruebe que es unitaria. Aplíquela a los qubits sencillos cero y uno. Sea ahora un registro de $n-$qubits cero y uno, y sea W la matriz (una transformación) que es la composición de M aplicada a cada uno de los $n-$qubits en sucesión. (Como matriz M es aproximadamente diagonal en bloques con copias de M localizadas en las posiciones adecuadas cerca de la diagonal y con $1'$s en lo que reste de la diagonal y $0'$s llenando el resto de la matriz). Generalice el resultado para los qubits sencillos y responda a) ¿Qué superposición resultaría de aplicar W a los $n-$bits $|0>$? b) Responda lo mismo para los qubits $|1>$. (Este caso es sólo ligeramente más complicado que el anterior.)

5. Una computadora cuántica factoriza el número 15 de la ecuación

$$f(x) = x^a \bmod 15$$

usando el algoritmo de Shor. La máquina necesita 8 qubits para la exponenciación modular y 12 para el algoritmo mismo en un total de 20 qubits. Comenzando con el valor al azar $x = 4$, el periodo de la exponenciación modular se calcula fácilmente de $4^a \bmod 15 = 1$. Sea el periodo $r = a = 2$ que satisface la ecuación anterior. El espectro de Fourier forma picos en $|0>$ y en $|128>$ con igual probabilidad, comprobados en varias corridas. En otras corridas con $x = 11$, se tiene: $11^2 \bmod 15 = 1$. En este caso las mediciones muestran el pico más alto en el espectro para el valor $|128>$. Con $128/2^8 = 1/2 = \lambda/r$ se concluye que el periodo r fue escogido correctamente. Calcule los factores de 15.

6. Considere la siguiente
Definición.- *Un lenguaje L está en NQP sii existe una máquina cuántica de Turing Q y un polinomio p tal que*

$$x \in L \iff Pr[Q \text{ acepte } x \text{ en } p(|x|) \text{ pasos}] \neq 0.$$

En donde NQP se ha definido como el análogo a la clase NP clásica. Analice y discuta su contenido y significado.

7. Un sistema de criptografía cuántica permite a dos personas, Alice y Bob, intercambiar una clave secreta. Alice usa un transmisor para enviar fotones en una de cuatro polarizaciones: $0, 45, 90$, o 135 grados, escogidas al azar. Bob usa un receptor para medir la polarización ya sea en la base rectilínea (0 y 90) o en la base diagonal (45 y 135) ya que de acuerdo a la leyes de la mecánica cuántica no puede medir en ambas bases al mismo tiempo. Describa los pasos necesarios para intercambiar la información suponiendo que no haya espías durante su intercambio.