MOOC: Computación y Criptografía Cuánticas

Lección 1: Modelo de Computación Cuántica

Soluciones a los ejercicios propuestos

Ejercicio 1.2. a) ¿Cuál es la probabilidad de obtener el estado $|0\rangle$ como estado resultante tras haber medido $u = 0.6|0\rangle - 0.8|1\rangle$ con la base B_1? ¿Y si se utiliza $B_\times$?

Recordemos que al medir un estado u, usando una base B, éste se proyecta sobre el subespacio generado por uno de los vectores de la base, por lo que el resultado será un vector paralelo a uno de los vectores de B y la probabilidad de cada resultado es el cuadrado del módulo de la amplitud correspondiente al expresar u como combinación lineal de los vectores de B.

Por tal motivo, la probabilidad de obtener el estado $|0\rangle$ al medir el estado $u = 0.6|0\rangle - 0.8|1\rangle$ con la base B_1 es 0.36.

Sin embargo la probabilidad de obtener el estado $|0\rangle$ al medir con $B_\times$ es nula, ya que $|0\rangle$ no es un estado de la base $B_\times$.

b) Determinar los posibles resultados de medir el estado u, con la base $B_\times$.

Para obtener el resultado de la medición, necesitamos expresar el estado u en función de los vectores de la base $B_\times$.

Como

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \qquad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

Se deduce que

$$u = 0.6|0\rangle - 0.8|1\rangle = \frac{0.6}{\sqrt{2}}(|+\rangle + |-\rangle) - \frac{0.8}{\sqrt{2}}((|+\rangle - |-\rangle) = \frac{-0.2}{\sqrt{2}}|+\rangle + \frac{1.4}{\sqrt{2}}|-\rangle$$

Por tanto el estado resultante tras la medición será $|+\rangle$, con probabilidad $\dfrac{(0.2)^2}{2} = 0.02$, o bien $|-\rangle$, con probabilidad $\dfrac{(1.4)^2}{2} = 0.98$.

Ejercicio 1.3.1 Pon otro ejemplo de estado entrelazado.

Cualquier estado de la forma $a|00\rangle + b|11\rangle$, con a y b números complejos no nulos tales que $|a|^2 + |b|^2 = 1$ es entrelazado.

También es entrelazado $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, ya que para que este estado fuera producto tensorial de dos estados de 1 qubit

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

debería ser $ac = 0$ y bd=0, $ad = 1/\sqrt{2}$, $bc = 1/\sqrt{2}$.

De la primera igualdad se deduce que puede ser $a = 0$ y entonces sería $ad = 0 \neq 1/\sqrt{2}$, o bien $c = 0$, y entonces sería $bc = 0 \neq 1/\sqrt{2}$.

Ejercicio 1.3.2 Estudiar cuál puede ser el estado resultante tras medir el segundo qubit del estado $u = 0.5(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, usando la base B_1.

El resultado de medir el segundo qubit puede ser 0 ó 1 con probabilidad $0.5^2 + 0.5^2 = 0.5$. En el primer caso el estado resulante es $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ y en el segundo es $\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$.

Ejercicio 1.5.1 Demuestra que $HXH = Z$ y $HZH = X$.

Basta multiplicar las matrices:

$$HXH = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2 & 0\\ 0 & -2\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = Z$$

Por otra parte

$$HZH = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = X$$

Teniendo en cuenta que la matriz H es unitaria, deduce del resultado anterior que para cualquier entero positivo k es $HZ^kH = X^k$

Como H es simétrica y real coincide con su transpuesta conjugada y por tanto $H^{-1} = H$ y $H^2 = I$.

Demostramos la igualdad pedida por inducción sobre k. Para $k = 1$, $HZH = X$, lo hemos visto en el apartado anterior. Supongamos ahora que $HZ^{k-1}H = X^{k-1}$ y se deduce:

$$HZ^kH = HZ^{k-1}ZH = HZ^{k-1}(HH)ZH = (HZ^{k-1}H)(HZH) = X^{k-1}X = X^k$$

Ejercicio 1.5.2 Determina U tal que $U^2 = Z$ y V tal que $V^2 = X$.

Como Z es una matriz diagonal, es fácil encontrar su raíz cuadrada $U = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$.

Para obtener V basta hacer $V = HUH$, ya que se tendrá

$$V^2 = (HUH)(HUH) = HU^2H = HZH = X.$$

En consecuencia $V = HUH = \frac{1}{2}\begin{pmatrix}1+i & 1-i\\ 1-i & 1+i\end{pmatrix}$.

Ejercicio 1.5.3 ¿Cuál es la imagen del estado $|01\rangle$ por la transformación de Walsh-Hadamard W_2?

Como $|01\rangle$ es el segundo vector de la base B_2, las coordenadas del vector $W_2(|01\rangle)$, respecto de la base B_2, son los números que aparecen en la segunda columna de la matriz de W_2. Por lo tanto

$$W_2(|01\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Ejercicio 1.5.4 Indica en cada caso si es posible encontrar dos puertas de un qubit cuyo producto tensorial transforme:

i) el estado $a|01\rangle + b|10\rangle$ en $a|11\rangle + b|00\rangle$.

Hay que negar el primer qubit y dejar igual el segundo. Por lo tanto la transformación es $X \otimes I$.

$$(X \otimes I)(a|01\rangle + b|10\rangle) = a|11\rangle + b|00\rangle$$

ii) el estado $|00\rangle$ en uno de la forma $a|00\rangle + b|10\rangle$.

Basta aplicar H en el primer qubit y dejar igual el segundo

$$(H \otimes I)(|00\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

iii) el estado $|00\rangle$ en uno de la forma $a|11\rangle + b|00\rangle$.

En este caso, solo sería posible en el caso $a = 0$ y $b = 1$, con la transformación identidad $I \otimes I$, o bien en el caso $a = 1$ y $b = 0$, con la negación en los dos qubits $X \otimes X$. Para el resto de los valroes de a y b el estado es entrelazado y no es posible ponerlo como imagen de $|00\rangle$ por una transformación que sea producto tensorial de dos transformaciones de un qubit.

Sí que se puede obtener haciendo la composición de $H \otimes I$ con una C_{NOT}.

Ejercicio 1.5.5 Escribe la matriz asociada a la puerta de Toffoly para la base

$$B_3 = [|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle].$$

Las columnas de la matriz son las coordenadas de las imágenes de los vectores de la base. La puerta de Toffoly cambia el tercer qubit cuando los dos primeros son iguales a 1.

$$\begin{array}{ll} T(|000\rangle) = |000\rangle, & T(|100\rangle) = |100\rangle \\ T(|001\rangle) = |001\rangle, & T(|101\rangle) = |101\rangle \\ T(|010\rangle) = |010\rangle, & T(|110\rangle) = |111\rangle \\ T(|011\rangle) = |011\rangle, & T(|111\rangle) = |110\rangle \end{array}$$

Por tanto la matriz es

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Ejercicio 1.5.6 Construye un circuito que transforme $a|000\rangle + b|100\rangle$ en $a|000\rangle + b|111\rangle$.

Con una puerta C_{12} se transforma $a|000\rangle + b|100\rangle$ en $a|000\rangle + b|110\rangle$ y ahora basta usar una puesta de Toffoly para conseguir $a|000\rangle + b|111\rangle$. El circuito por tanto es el de la siguiente figura: