Después de haber visto los principios de la mecánica cuántica, vamos a empezar con el protagonista de la computación cuántica que es el *qubit*. Aunque todavía habrá algunas referencias físicas para motivar, los conceptos primordiales serán puramente matemáticos, concretamente pertenecientes al álgebra lineal, con una notación algo singular.

La base física de la computación cuántica es que hay algunas magnitudes que no solo están cuantizadas, sino que toman un número finito de valores. El ejemplo paradigmático es el *espín*[1]. Resulta que un electrón, al igual que otras partículas subatómicas, se comporta como un pequeño imán y es posible hacer mediciones cuánticas para detectar si tal imán apunta hacia arriba, estado que indicamos con $|\uparrow\rangle$, o si apunta hacia abajo, estado representado por $|\downarrow\rangle$. En general, el estado de espín (para ser preciso, el de espín 1/2, que es el del electrón) es de la forma

$$|\Psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle \qquad a, b \in \mathbb{C}.$$

Desde el punto de vista clásico podríamos entender que los imanes pueden tener direcciones oblicuas y que, de alguna forma, a y b tienen información acerca de la inclinación hacia arriba y hacia abajo. Sin embargo, desde el punto de vista cuántico, suponiendo siempre el estado normalizado, $|a|^2+|b|^2 = 1$, los números $|a|^2$ y $|b|^2$ son las probabilidades de que en la medición obtengamos $|\uparrow\rangle$ o $|\downarrow\rangle$. Hay dos grados de libertad correspondientes a a y b, por tanto el espacio de Hilbert natural del que nos habla el primer postulado es $\mathbb{C}^2$ con el producto escalar usual. En matemáticas usaríamos los vectores de la base canónica en lugar de $|\uparrow\rangle$ y $|\downarrow\rangle$, y en computación cuántica, que es el tema que nos ocupa, se usan $|0\rangle$ y $|1\rangle$. En definitiva,

$$|\uparrow\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad \text{y} \qquad |\downarrow\rangle = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

Un *qubit* no es otra cosa que un vector unitario en $\mathbb{C}^2$, representando así un estado de espín en concordancia con el postulado 1. Con la notación de la computación cuántica, un qubit es un estado de la forma

$$|\Psi\rangle = a|0\rangle + b|1\rangle \qquad \text{con} \quad a, b \in \mathbb{C} \quad \text{tales que} \quad |a|^2 + |b|^2 = 1. \tag{1}$$

Un *bit* tradicional solo puede tomar dos valores: 0 y 1, mientras que un qubit puede tomar toda una circunferencia compleja de valores. En principio contiene mucha más información. Sin embargo, por lo que sabemos del postulado 3, cuando accedemos a un qubit con una medición que decida entre $|0\rangle$ y $|1\rangle$, colapsará en uno de estos dos estados con cierta probabilidad. De algún modo se transformará en un bit tradicional que no permite recuperar el estado del qubit. Aparentemente solo podemos acceder a resultados probabilistas y no se ve la utilidad de la computación cuántica. Ya veremos cómo escapar de esta paradoja.

[1] Siguiendo el DRAE uso esta forma castellanizada del término en inglés *spin*, aunque la verdad es que ni es muy común ni me gusta demasiado. Tú haz lo que prefieras en tu trabajo.

Comencemos con un ejercicio prácticamente trivial para comprobar que estás entendiendo la notación.

1) Cuando decidimos entre $|0\rangle$ y $|1\rangle$, los operadores de medición del postulado 3 son P_0 y P_1 dados por las proyecciones ortogonales sobre los subespacios generados por $|0\rangle$ y $|1\rangle$, respectivamente. Escríbelos como matrices 2×2.

Al multiplicar un qubit aislado por un número complejo de módulo 1, el estado no varía, por ello se puede suponer $a \in \mathbb{R}_{\geq 0}$ en (1). A veces se incluye en el postulado 1 la invariancia de los estados al multiplicar por números de módulo 1 porque es un hecho general en mecánica cuántica que deriva de que hay diferentes formas de normalizar. En la hoja anterior apareció indirectamente cuando elegimos la constante real positiva al definir Ψ_n.

2) Demuestra que

$$(\cos\varphi \operatorname{sen}\theta, \operatorname{sen}\varphi \operatorname{sen}\theta, \cos\theta) \longmapsto \cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \operatorname{sen}\frac{\theta}{2}|1\rangle$$

con $\theta \in [0, \pi]$, $\varphi \in [0, 2\pi)$ establece una biyección entre los puntos de S^2, la superficie esférica unidad en $\mathbb{R}^3$, y los qubits (1) considerados iguales si difieren en multiplicar por un número complejo de módulo 1.

Cuando S^2 se utiliza para parametrizar qubits, se dice que es la *esfera de Bloch*. Su motivación, viene de la física del espín. Hagamos una pequeña digresión en este sentido para introducir unas matrices importantes en computación cuántica. Si en vez de hacer un experimento para estudiar si el imán del electrón apunta hacia arriba, dirección $(0, 0, 1)$, o hacia abajo, dirección $(0, 0, -1)$, se hace para ver si apunta en cierta dirección $\vec{n} \in \mathbb{R}^3$, con $\|\vec{n}\| = 1$, o su opuesta; la teoría dice que los dos posibles estados son los autovectores normalizados de la matriz $\vec{n} \cdot \vec{\sigma}$ definida como $n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3$ con σ_j las *matrices de Pauli*:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \text{y} \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Es también muy común llamarlas σ_x, σ_y y σ_z. Para $\vec{n} = (0, 0, 1)$, se tiene $\vec{n} \cdot \vec{\sigma} = \sigma_3$ y es obvio que $|0\rangle$ y $|1\rangle$ son autovectores normalizados con autovalores 1 y -1. Por eso al estudiar el espín (por ejemplo, en [5]) se escribe a veces $|+\rangle$ y $|-\rangle$ en vez de $|\uparrow\rangle$ y $|\downarrow\rangle$.

3) Sea $\vec{n} \in \mathbb{R}^3$ un vector arbitrario. Prueba que los autovalores de $\vec{n} \cdot \vec{\sigma}$ son siempre 1 y -1 y que los autovectores respectivos son ortogonales. Indicación: Esto no debería requerir apenas ninguna cuenta. Para la segunda parte piensa en algún teorema de álgebra lineal que hable de la ortogonalidad de los autovectores.

4) Si escribimos $\vec{n} = (\cos\varphi \operatorname{sen}\theta, \operatorname{sen}\varphi \operatorname{sen}\theta, \cos\theta)$, comprueba que el autovector con autovalor 1 es, salvo multiplicar por constantes, $\cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \operatorname{sen}\frac{\theta}{2}|1\rangle$.

5) Calcula los dos qubits asociados a direcciones opuestas del eje X y escribe las matrices de los operadores de medición correspondientes.

La posibilidad de hacer diferentes tipos de mediciones es crucial en computación cuántica. Nos da control sobre el tipo de estados en que colapsa un qubit tras la medición.

Dada cualquier base ortonormal de $\mathbb{C}^2$ las proyecciones sobre cada uno de sus dos vectores (sobre los subespacios que generan) dan lugar a operadores de medición válidos en el postulado 3 (¿ves claro que su suma es la identidad?) y dependiendo de la base elegida, un qubit colapsará con ciertas probabilidades en cada uno de estos vectores. Estas probabilidades vienen dadas por el módulo al cuadrado del producto escalar porque el producto escalar es la "longitud" de la proyección. En fórmulas:

$$\langle\Psi|P_{\vec{v}}|\Psi\rangle = \big\langle\Psi|\langle\vec{v}|\Psi\rangle\vec{v}\big\rangle = \big|\langle\Psi|\vec{v}\rangle\big|^2.$$

Por ejemplo, si medimos el qubit $\frac{1}{\sqrt{3}}|0\rangle + \frac{1+i}{\sqrt{3}}|1\rangle$ usando la base canónica $\big\{|0\rangle, |1\rangle\big\}$ colapsará en $|0\rangle$ con probabilidad $\frac{1}{3}$ y en $|1\rangle$ con probabilidad $\frac{1}{3}|1+i|^2 = \frac{2}{3}$.

6) Comprueba que $\left\{\frac{2+i}{3}|0\rangle + \frac{2}{3}|1\rangle, -\frac{2i}{3}|0\rangle + \frac{1+2i}{3}|1\rangle\right\}$ es una base ortonormal y calcula la probabilidad de que el qubit del párrafo anterior colapse en el segundo elemento de la base al emplearla para hacer mediciones.

Aunque trabajar con un solo qubit tiene un recorrido muy limitado, es suficiente para diseñar un sistema criptográfico probabilista virtualmente inexpugnable. Te doy como referencia principal una que lo explica con polarización de fotones. Simplemente cada vez que leas fotón debes entender qubit y los símbolos con las dobles flechas tienen el siguiente significado:

$$|\updownarrow\rangle = |0\rangle, \qquad |\leftrightarrow\rangle = |1\rangle, \qquad |\nwarrow\!\!\searrow\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big), \qquad |\swarrow\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big).$$

7) Lee el protocolo de *distribución de claves cuánticas* en [2, §3.2] y escribe unos párrafos explicándolo[2]. Al principio seguramente te parecerá lioso, insiste hasta que lo entiendas. No te extiendas mucho, limítate a reseñar las ideas fundamentales.

Se aspira a que los ordenadores cuánticos operen con muchos qubits simultáneamente, cuya base física son sistemas cuánticos de partículas. Según el postulado 4, el modelo matemático es el *producto tensorial*. Más allá de lo que diga la definición rigurosa de este concepto [4], se puede identificar cada elemento del producto tensorial $\mathbb{C}^m \otimes \mathbb{C}^n$ con un elemento de $\mathbb{C}^{mn}$ por medio de la regla:

$$(v_1, v_2, \ldots, v_m)^t \otimes (w_1, w_2, \ldots, w_n)^t = (v_1w_1, v_1w_2, \ldots, v_1w_n, v_2w_1, v_2w_2, \ldots, v_mw_n)^t.$$

[2] Si prefieres una fuente donde no haya que traducir de polarizaciones a qubits, mira [3, §12.6.3], aunque para mi gusto en [2] está mejor.

Es decir, se hacen todos los productos y se ordenan con el orden lexicográfico en los índices. Piensa que esto no está tan lejos de lo hecho en la hoja anterior con el producto de las funciones de onda: allí multiplicábamos cada $\Psi(x)$ por todos los valores de $\widetilde{\Psi}$ y aquí multiplicamos cada coordenada de $\vec{v}$ por todas las de $\vec{w}$. Lo crucial en ambos casos es que se tenga

$$\langle \vec{v} \otimes \vec{w}, \vec{a} \otimes \vec{b} \rangle = \langle \vec{v}, \vec{a} \rangle \langle \vec{w}, \vec{b} \rangle.$$

8) Escribe alguna línea explicando por qué con la definición anterior se cumple esta relación.

El producto tensorial no es conmutativo, pero sí asociativo y distributivo con respecto a la suma. En computación cuántica se suele abreviar $|m\rangle \otimes |n\rangle$ como $|mn\rangle$. Por ejemplo, el resultado de operar $\left(\left(\frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle\right) \otimes |1\rangle\right) \otimes |0\rangle$ se escribe como $\frac{3}{5}|010\rangle - \frac{4}{5}|110\rangle$.

El espacio de Hilbert correspondiente a dos qubits es[3] $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$ y una base es la canónica de $\mathbb{C}^4$, que se expresa como productos tensoriales de los elementos de las bases canónicas de los factores:

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad |01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

El estado de un sistema de dos qubits viene dado por:

$$(2) \quad |\Psi\rangle = a_{00}|00\rangle + a_{10}|10\rangle + a_{01}|01\rangle + a_{11}|11\rangle \qquad \text{con} \quad |a_{00}|^2 + |a_{10}|^2 + |a_{01}|^2 + |a_{11}|^2 = 1.$$

En general, el estado de un sistema de n qubits, lo que en computación cuántica se llama un *registro* de n qubits, es un elemento de $\mathbb{C}^{2^n}$ y se representa como

$$|\Psi\rangle = \sum_{b \in \mathcal{B}_n} a_b |b\rangle \qquad \text{con} \quad \sum_{b \in \mathcal{B}_n} |a_b|^2$$

donde $\mathcal{B}_n$ es el conjunto de todas las cadenas de longitud n formadas por ceros y unos, lo que corresponde a todos los números naturales entre 0 y $2^n - 1$ escritos en binario y completados con ceros a la izquierda hasta n dígitos si es necesario. Con esta identificación y un ligero abuso de notación, lo anterior se escribe como $|\Psi\rangle = \sum_{b=0}^{2^n-1} a_b |b\rangle$.

9) Con esta notación, prueba que si tenemos un registro de m qubits $|\Psi\rangle = \sum_{b=0}^{2^m-1} a_b |b\rangle$ y otro de n qubits, $|\Phi\rangle = \sum_{b=0}^{2^n-1} \alpha_b |b\rangle$, entonces $|\Psi\rangle \otimes |\Phi\rangle = \sum_{b=0}^{2^m-1} \sum_{\beta=0}^{2^n-1} a_b \alpha_\beta |2^n b + \beta\rangle$.

Se define el producto tensorial $T \otimes S$ de dos endomorfismos $T : V \longrightarrow V$ y $S : W \longrightarrow W$ de espacios vectoriales sobre $\mathbb{C}$ de la manera obvia: $T \otimes S$ aplica $\vec{v} \otimes \vec{w}$ en $T(\vec{v}) \otimes S(\vec{w})$ para cada $\vec{v} \in V$ y $\vec{w} \in W$ y se extiende por linealidad.

[3] Un matemático riguroso con una definición más formal del producto tensorial, escribiría $\cong$ en vez de $=$.

10) Halla la matriz de $\sigma_1 \otimes \sigma_2$ y calcula la imagen de $\frac{1}{3}|00\rangle - \frac{2i}{3}|01\rangle + \frac{2}{3}|11\rangle$ por este operador.

Después de la base canónica, la base más importante de $\mathbb{C}^2 \otimes \mathbb{C}^2$ en computación cuántica es la base $\big\{|\Phi_0\rangle, |\Phi_1\rangle, |\Phi_2\rangle, |\Phi_3\rangle\big\}$ formada por los llamados *estados de Bell* donde

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \qquad \text{y} \qquad |\Phi_j\rangle = \big(I \otimes \sigma_j\big)|\Phi_0\rangle \quad \text{para } j = 1,\, 2,\, 3$$

con I la identidad (en $\mathbb{C}^2$).

11) Expresa $|\Phi_1\rangle$, $|\Phi_2\rangle$ y $|\Phi_3\rangle$ en términos de la base canónica $\big\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\big\}$.

Un registro de n qubits se dice que está *entrelazado* si no es producto tensorial de n qubits. Por ejemplo, en el caso $n = 2$ significa que (2) no es de la forma $\big(a|0\rangle + b|1\rangle\big) \otimes \big(c|0\rangle + d|1\rangle\big)$. Cualquiera que sea $n \geq 2$, casi todos los registros de n qubits están entrelazados, aunque solo hay un criterio simple para decidirlo cuando $n = 2$.

12) Demuestra que (2) está entrelazado si y solo si $a_{00}a_{11} - a_{10}a_{01} \neq 0$.

En cierto modo, la manera de resolver la paradoja señalada al principio consiguiendo que un ordenador cuántico sirva para hacer cálculos deterministas, pasa por considerar mediciones parciales de estados entrelazados.

Digamos que consideramos el $|\Phi_0\rangle$ de los estados de Bell y queremos medir solo el primer qubit. Entonces los operadores de medición deben ser $M_0 = P_0 \otimes I$ y $M_1 = P_1 \otimes I$ con P_0 y P_1 las proyecciones sobre $|0\rangle$ y $|1\rangle$ (en rigor, sobre los subespacios que generan), que ya aparecieron en un problema anterior. Tras la medición, el estado colapsará en $|00\rangle$ con probabilidad $1/2$ y en $|11\rangle$ con probabilidad $1/2$. Esto lleva una situación curiosa, aunque no hemos medido el segundo qubit, porque no hemos proyectado sobre el segundo factor del producto tensorial, con toda certeza sabemos que coincide con el primero. Si ambos qubits están espacialmente muy lejos, parece increíble que la medición de uno de ellos afecte instantáneamente a que el otro esté totalmente determinado. Esta es la base de la *paradoja de Einstein-Podolsky-Rosen* (mira [2, §3.5] o [1, §2.5] si tienes curiosidad). Cuando uno parte de un estado no entrelazado, los qubits se pueden medir con independencia, sin que uno afecte al otro. De ahí el nombre.

Para ver que lo has entendido, te propongo un par de ejercicios que involucran la base ortonormal

$$\big\{|\Psi_\alpha\rangle, |\Psi_\alpha^\perp\rangle\big\} \qquad \text{con} \quad |\Psi_\alpha\rangle = \cos\alpha\,|0\rangle + \operatorname{sen}\alpha\,|1\rangle \quad \text{y} \quad |\Psi_\alpha^\perp\rangle = -\operatorname{sen}\alpha\,|0\rangle + \cos\alpha\,|1\rangle$$

y las proyecciones ortogonales sobre ellos que denotamos con P_α y $P_\alpha^\perp$.

13) Explica por qué $M_0 = P_\alpha \otimes I$ y $M_1 = P_\alpha^\perp \otimes I$ son operadores de medición de acuerdo con el postulado 3, es decir, ambos son proyecciones ortogonales y su suma es la identidad.

Demuestra que tras la medición correspondiente a estos operadores el estado de Bell $|\Phi_0\rangle$ colapsa a $|\Psi_\alpha\rangle \otimes |\Psi_\alpha\rangle$ o a $|\Psi_\alpha^\perp\rangle \otimes |\Psi_\alpha^\perp\rangle$ y halla con qué probabilidades.

14) Supongamos ahora que medimos los dos qubits examinando si el primero es $|\Psi_\alpha\rangle$ y el segundo es $|\Psi_\beta\rangle$, esto es, $M_0 = P_\alpha \otimes P_\beta$ es uno de los operadores de medición. Muestra que la probabilidad de que $|\Phi_0\rangle$ colapse a $|\Psi_\alpha\rangle \otimes |\Psi_\beta\rangle$ es $\frac{1}{2}\cos^2(\alpha - \beta)$.

Tarea a entregar. Debes escribir un documento que combine las soluciones de los ejercicios anteriores. Te recomiendo que cuentes algo acerca del espín para motivar. En [5] y [1] tienes más información al respecto. La extensión es libre siempre que no superes las 7 páginas con el formato de esta hoja o de la plantilla. Si ves que te pasas mucho de la extensión reduce lo que consideres oportuno de la parte de la esfera de Bloch conservando las matrices de Pauli. Antes de suprimir otras cosas, consúltame. En cualquier caso, como te he dicho, no te extiendas con lo de la distribución de claves cuánticas. El documento debe dar lugar a un segundo capítulo de tu TFG llamado *Qubits y entrelazamiento* o algo parecido.

Referencias

[1] F. Chamizo. Un poco de física cuántica para chicos listos de primero (del grado de física o matemáticas). `http://matematicas.uam.es/~fernando.chamizo/physics/files/qf.pdf`, 2015.

[2] M. Nakahara and T. Ohmi. *Quantum computing*. CRC Press, Boca Raton, FL, 2008. From linear algebra to physical realizations.

[3] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[4] Wikipedia contributors. Tensor product — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Tensor_product&oldid=1180992747`, 2023. [Online; accessed 23-October-2023].

[5] B. Zwiebach. Quantum physics I. MIT OpenCourseWare, `https://ocw.mit.edu/courses/physics/8-04-quantum-physics-i-spring-2016/`, 2016.