Introducción a la computación cuántica

Trabajo Fin de Grado

Autora:
María del Mar Villasana Alcaraz

Tutor:
Juan Antonio López Ramos

Grado en Matemáticas

Julio, 2020
Universidad de Almería

Índice general

Abstract in English

In this paper we attempt to give an introduction to the theory of quantum computing, a branch of computing currently in progress that takes advantage of the knowledge of quantum mechanics, the part of physics that studies atomic and subatomic particles, to overcome the limitations of classical computing.

Initially, we will review some concepts of basic linear algebra that it is essential to know to approachother new ones related to quantum computing based mostly on matrix operations.

In the first chapter we also present the Hilbert spaces that form the basis of quantum systems.

In a second part, the concepts "ket" and "bra" are defined and the meaning of the latter is justified by the Riesz representation theorem that relates each vector space to its dual. Just as the basic unit of information in classical computing is the bit, at the quantum level we define the qubits that we represent in the Bloch sphere. These can be presented together giving rise to a system in composition of many qubits. The main operators on which the properties collected by the quantum postulates are based are introduced below, rules that relatethe operation of computing with mathematical concepts.

To conclude this part we focus from the point of view of quantum architecture, the matrix operands defined above; now implemented as gates that transform the input of qubits into output.

Finally and once the foundations of quantum computing are established, we dedicate a chapter to cryptography where we describe the classic approach of this discipline and how the appearance of protocols, such as BB84, and of certain quantum algorithms such as Shor's, that solve efficiently the mathematical problems on which current security systems are based, have a great influence in modern researching lines in cryptography.

Resumen en español

En este trabajo pretendemos dar una introducción a la teoría de la computación cuántica, una rama de la informática en progreso actualmente que aprovecha el conocimiento de la mecánica cuántica, la parte de la física que estudia las partículas atómicas y subatómicas, para superar las limitaciones de la informática clásica.

Inicialmente repasaremos algunos de los conceptos básicos del álgebra lineal que resulta fundamental conocer para abordar otros nuevos relacionados con la computación cuántica basados en su mayoría en las operaciones matriciales.

En el primer capítulo presentamos también los espacios de Hilbert que constituyen la base de los sistemas cuánticos.

En una segunda parte, se definen los conceptos "ket" y "bra" y se justifica el significado de este último mediante el teorema de representación de Riesz que relaciona cada espacio vectorial con su dual. Al igual que la unidad básica de información en computación clásica es es el bit, a nivel cuántico se definen los qubits que representamos en la esfera de Bloch. Estos pueden presentarse juntos dando lugar a un sistema en composición de muchos qubits. A continuación se introducen los principales operadores en los que se basan las propiedades que recogen los postulados cuánticos, reglas que relacionan el funcionamiento de la computación cuántica con conceptos matemáticos.

Para concluir esta parte enfocamos desde el punto de vista de la arquitectura cuántica, los operadores matriciales definidos; ahora implementados como compuertas que transforman la entrada de qubits produciendo una salida.

Finalmente y una vez establecidas las bases de la computación cuántica, dedicamos un capítulo a la criptografía donde describimos el enfoque clásico de esta disciplina y cómo la aparición de protocolos, como el BB84, y de ciertos algoritmos cuánticos como el de Shor, que resuelven de manera eficiente los problemas matemáticos en los que se basan los actuales sistemas de seguridad, tienen una gran influencia en las líneas actuales de investigación criptográfica.

1 Introducción

La computación sufrió un gran avance en 1947 con el desarrollo del transistor, un dispositivo electrónico que procesa la información de entrada obteniendo una respuesta como salida.

En los años posteriores, este campo continuó un potencial crecimiento y fue en 1965 cuando Gordon Moore, cofundador de Intel (principal fabricante de microprocesadores y semiconductores del mundo), predijo que cada año se duplicaría el número de transistores por unidad de superficie que pueden incluirse en un microprocesador [8]. Diez años después, Moore modificó su estimación inicial ampliando el periodo a dos años.

Dicha predicción es lo que se conoce como la Ley de Moore que, aunque no es una ley propiamente dicha sino más bien una tendencia empírica, se ha venido cumpliendo de manera que hoy en día es posible anexionar cientos de millones de transistores en cada milímetro cuadrado de un circuito integrado.

El proceso dota a los ordenadores modernos de mayor rapidez, al realizar más operaciones por unidad de tiempo, y de un menor consumo de energía. Pero ¿podemos continuar eternamente miniaturizando el tamaño de estos dispositivos?

Los transistores son básicamente interruptores que bloquean o permiten el paso de electrones en una dirección. Actualmente su tamaño se mide en nanómetros, la millonésima parte de un milímetro y ya se han conseguido fabricar de sólo dos nanómetros lo que equivale a diez átomos de diámetro.

En estas escalas atómicas y subatómicas, las leyes deterministas de la física clásica dejan de ser válidas y la materia se rige por reglas cuánticas de carácter probabilístico es decir, si en el mundo clásico una partícula se encuentra en un lugar y en un tiempo concreto, desde el enfoque cuántico coexisten muchos estados con una cierta probabilidad. La medición realizada hace que esas probabilidades desaparezcan y encontremos la partícula en uno de los estados posibles. Al medir estamos influyendo en el estado final de la partícula.

En el caso de los transistores, es probable que un electrón que debería permanecer confinado a un lado de la barrera interna de este dispositivo, "aparezca" o "se transfiera" al lado opuesto. Es decir, el electrón parece haber atravesado la barrera. Es lo que conocemos como efecto túnel. De esta forma la corriente o señal eléctrica puede pasar por canales donde no debería circular y el microchip deja de funcionar correctamente.

Por tanto, no es posible continuar disminuyendo el tamaño de estos mecanismos. Una solución a este problema, que constituye la motivación principal de este trabajo, es el uso de la computación cuántica que se basa en la mecánica cuántica para realizar los cálculos necesarios para el funcionamiento de los dispositivos.

El desarrollo de este nuevo paradigma permite a los ordenadores además un aumento de la eficiencia en los cálculos pues, como en el caso de la posición de los electrones en el transistor, la unidad básica de información podrá encontrarse en muchos estados diferentes simúltanemente, de modo que las máquinas cuánticas procesan información paralelamente superando a las clásicas que lo hacen de forma secuencial.

Uno de los descubrimientos más importantes del siglo XX realizado por John von Neumann y recogido en su libro *Mathematical Foundations of Quantum Mechanics* es que toda la mecánica cuántica puede ser descrita en base a conceptos algebraicos.
Será por tanto el objetivo central de este trabajo el desarrollo de los contenidos del álgebra lineal y operadores estudiados a lo largo del grado para ser aplicados a esta rama de la computación en clara progresión.

En este primer capítulo nos centraremos en conceptos básicos y resultados elementales a los que recurriremos más adelante.
El cuerpo de números $\mathbb{K}$ notará indistintamente tanto a los números reales $\mathbb{R}$ como a los complejos $\mathbb{C}$. Los elementos del cuerpo $\mathbb{K}$ se denominan escalares y los de un espacio vectorial V vectores.

1.1 Conceptos generales del Álgebra Lineal

Comenzaremos introduciendo los conceptos de espacio y subespacio vectoriales, que son los elementos u objetos básicos del álgebra. El espacio más interesante para nosotros será el espacio complejo finito dimensional que notaremos $\mathbb{C}^n$ el espacio de todas las $n-uplas$ $x = (x_1, \ldots, x_n)$ de números complejos. Definimos también la base y la dimensión de un espacio vectorial.

Definición 1.1. *Un espacio vectorial sobre $\mathbb{K}$ es un conjunto $V \neq \emptyset$ provisto de dos operaciones:*

I *La suma definida de $V \times V$ en V, que denotaremos por $+ : (u, v) \to u + v$, $u, v \in V$, que satisface las siguientes propiedades:*

(a) Asociatividad:
$$(u + v) + w = u + (v + w) \quad \forall u, v, w \in V$$

(b) Conmutatividad:
$$u + v = v + u$$

(c) Existencia de elemento neutro:
$$\exists 0_V \in V : 0_V + v = v$$

(d) Existencia de elemento opuesto o simétrico:
$$\forall v \in V \quad \exists -v : v + (-v) = 0_V$$

II *El producto por escalares definido de $\mathbb{K} \times V$ en V, que denotaremos por $\cdot : (\alpha, v) \to \alpha v \quad \alpha \in \mathbb{K}$, satisfaciendo las siguientes propiedades:*

(a) Es distributivo respecto a la suma por vectores:
$$\alpha(u + v) = \alpha u + \alpha v$$

(b) Es distributivo respecto a la suma por escalares:
$$(\alpha + \beta)u = \alpha u + \beta u$$

(c) *Pseudoasociatividad:*

$$(\alpha\beta)u = \alpha(\beta u)$$

(d) *Existencia de elemento unidad para el producto por escalares:*

$$1v = v$$

donde 1 denota la unidad en $\mathbb{K}$ del producto por escalares.

Definición 1.2. *Un subconjunto $M \neq \emptyset$ de un espacio vectorial V se dice que es un subespacio vectorial de V si $\alpha v, u+v \in M \quad \forall \alpha \in \mathbb{K}$ y $u, v \in M$*

Definición 1.3. *Una base B de un espacio vectorial V finito dimensional es un conjunto de vectores $\{v_1, \ldots, v_n\}$ no todos nulos, linealmente independiente, i.e., si $c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$ entonces $c_i = 0 \quad \forall i = 1, \ldots, n$, de forma que todo vector de V puede expresarse como combinación única de los vectores de B .*

Decimos que una base es un conjunto de vectores linealmente indepediente y sistema generador del espacio V.

Introducimos el lema de Zorn, que no es más que una reformulación del axioma de elección (ver [10, Section 16], [21, Section 7.3]), que nos será de utilidad en el desarrollo de la demostración del teorema posterior.

Axioma de Elección: Sea I un conjunto arbitrario y $\{A_i\}_{i\in I}$ una familia de conjuntos no vacíos entonces se puede elegir un elemento de cada conjunto A_i.

Lema 1.1 (Lema de Zorn)**.** *Sea A un conjunto parcialmente ordenado. Si toda cadena $C \subseteq A$ tiene cota superior, entonces A tiene un elemento maximal.*

Se dice que A es un conjunto parcialmente ordenado si existe una relación binaria en A, $\leq$, tal que satisface las propiedades reflexiva, ($a \leq a \quad \forall a \in A$), antisimétrica, ($a \leq b, b \leq a \Rightarrow a = b \quad \forall a, b \in A$) y transitiva, ($a \leq b, b \leq c \Rightarrow a \leq c \quad \forall a, b, c \in A$).

Considerando A parcialmente ordenado por $\leq$ y $S \subset A$ con el orden heredado de A, se dice que $m \in A$ es una cota superior de S en caso de que $s \leq m \quad \forall s \in S$.

Una cadena en A es un subconjunto $C \subseteq A$ tal que, bajo el mismo orden heredado, C es un conjunto totalmente ordenado, es decir, dados $a, b \in C \Rightarrow a \leq b \vee b \leq a$.

La cadena puede escribirse $C = \{c_i\}_{i\in I}$, donde I es un conjunto totalmente ordenado y $c_i \in A$, con $c_i \leq c_j \Leftrightarrow i \leq j$.

Teorema 1.1. *Sea V un espacio vectorial no nulo con un conjunto linealmente independiente, S, entonces existe una base B de V tal que $S \subset B$.*

Demostración:

Sea $\mathcal{F} = \{A \subset V : S \subset A$, A linealmente independiente$\}$. Claramente $\mathcal{F} \neq \emptyset$ pues $S \in \mathcal{F}$.

Sea $\mathcal{G} = \{A_i : i \in I\}$ familia indexada de $\mathcal{F}$, totalmente ordenada por la relación de inclusión $\subset$ y sea $A = \cup_{i\in I} A_i$, veamos que A es linealmente independiente. De no ser así, existiría una combinación $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ con algún α_i no nulo y $\{v_1, \ldots, v_n\} \subset A$. Por estar totalmente ordenado $\mathcal{G}$, existiría un i_0 con $\{v_1, \ldots, v_n\} \in A_{i0}$ pero entonces A_{i_0} no sería linealmente independiente lo cual es absurdo pues $A_{i_0} \in \mathcal{F}$, con lo que $A = \cup_{i\in I} A_i$ es linealmente independiente.

Por ser A linealmente independiente y $S \subset A$ entonces $A \in \mathcal{F}$ y $A_i \subset A$, luego A es cota superior de $\mathcal{G}$.

Aplicando el lema 1.1, $\mathcal{F}$ tiene un elemento maximal, B. Veamos que B es base de V.
Como $B \subset \mathcal{F}$, B es linealmente independiente, además $S \subset B$. Veamos ahora que B es sistema generador del espacio V. Por reducción al absurdo, si no lo fuera existiría $v \in V - \langle B \rangle$, donde $\langle B \rangle$ es el subespacio generado por B, luego $B \cup \{v\}$ es linealmente independiente por lo que $B \cup \{v\} \in \mathcal{F}$ y $B \subsetneq B \cup \{v\}$ en contra de la maximilidad de B, con lo que B es una base que contiene a S.

■

Corolario 1.1.1 (Teorema de existencia de la base)**.** *Todo espacio vectorial contiene una base.*

Demostración:

Si $V \neq \{0\}$, $\exists v \in V$ no nulo, basta elegir el conjunto linealmente independiente $S = \{v\}$. Si $V = \{0\}$, $B = \emptyset$ es base de V.

■

Llamamos dimensión del espacio vectorial V y lo denotamos $dim_{\mathbb{K}}(V)$, al número de vectores de cualquiera de sus bases. Para comprobar que es siempre la misma, independientemente de la base escogida, enunciamos el siguiente lema.

Lema 1.2. *Sean V un espacio vectorial, $S \subset V$ y $u, v \in V$. Si $v \in \langle S \cup \{u\} \rangle - \langle S \rangle$, entonces $u \in \langle S \cup \{v\} \rangle$.*

Demostración:

Por hipótesis, $v \in \langle S \cup \{u\} \rangle - \langle S \rangle$, entonces existen x_i, $i = 1, \ldots, m$ y x escalares y $s_1, \ldots, s_m$ elementos de S tales que

$$v = x_1 s_1 + \cdots + x_m s_m + xu$$

En caso de que $x = 0$, se tiene que $v \in \langle S \rangle$, lo que es absurdo. De este modo $x \neq 0$, de donde se tiene que

$$u = x^{-1} v - (x^{-1} x_1) s_1 - \cdots - (x^{-1} x_m) s_m$$

es decir, $u \in \langle S \cup \{v\} \rangle$.

■

Teorema 1.2 (Teorema de la dimensión de la base)**.** *Todas las bases de un espacio vectorial V tienen el mismo cardinal.*

Demostración:

Nos restringiremos al caso en que el espacio sea finito, es decir, las bases tienen un número finito de vectores, pues, como veremos más adelante, los resultados aplicados a la teoría de la computación cuántica no usan espacios de dimensión infinita.

Sean $B = \{u_1, \ldots u_n\}$ y $B' = \{v_1, \ldots, v_m\}$ dos bases del espacio V. Supongamos en primer lugar que $m < n$. Como B es una base, se tiene $v_1 = x_1 u_1 + \cdots + x_n u_n$. Dado que v_1 no es cero, $\exists x_i$, $i = 1, \ldots, n$, no nulo. Sea pues $x_1 \neq 0$.

En este punto hemos de tener en cuenta que no puede tenerse que $v_1 \in \langle\{u_2,\dots,u_n\}\rangle$, dado que entonces, como $v_1 = x_1u_1 + \cdots + x_nu_n$ y, al mismo tiempo $v_1 = y_2u_2 + \cdots + y_nu_n$, restando se sigue que $x_1u_1 + (x_2 - y_2)u_2 + \cdots + (x_n - y_n)u_n = 0$, lo que es absurdo pues B es un conjunto linealmente independiente.

De este modo, $v_1 \in \langle\{u_2,\dots,u_n\} \cup \{u_1\}\rangle - \langle\{u_2,\dots,u_n\}\rangle$, de donde, aplicando el lema anterior, se sigue que $u_1 \in \langle\{v_1,u_2,\dots u_n\}\rangle$.

Ahora bien, $\{u_2,\dots,u_n\}$ es un conjunto linealmente independiente y como $v_1 \notin \{u_2,\dots,u_n\}$, se tiene que $\{v_1,u_2,\dots,u_n\}$ es un conjunto linealmente independiente. Como además se tiene que u_1 se escribe como combinación lineal de $\{v_1,u_2,\dots,u_n\}$, se sigue que $V = \langle\{v_1,u_2,\dots,u_n\}\rangle$ y así, $\{v_1,u_2,\dots,u_n\}$ es una base de V.

Si repetimos el razonamiento anterior, se sigue que $\{v_1,\dots,v_m,u_{m+1},\dots,u_n\}$ es una base de V. Pero como $B' = \{v_1,\dots,v_m\}$ es una base de V, necesariamente u_{m+1} es combinación lineal de los elementos de B' y así tenemos una contradicción. Por tanto, no puede ser que $m < n$.

Supongamos ahora que $m > n$. Razonando exactamente del mismo modo obtendríamos igualmente una contradicción y así se tiene que $m = n$.

En caso de que B' tenga un número infinito de vectores. Razonando del mismo modo, es posible construir una base $B'' = B \cup S$, donde $B = \{u_1,\dots,u_n\}$ y S es un subconjunto (no vacío) de B'. Como B es base de V y $S \neq \emptyset$, se sigue que B'' es un conjunto linealmente dependiente dado que cualquier elemento de S se expresará como combinación lineal de los elementos de B, lo cual es una contradicción.

■

1.2 Definición de producto escalar y norma

Producto escalar. Producto interno.

El producto interno es una generalización del producto escalar utilizado en espacios euclídeos, que permite a partir de dos vectores de espacio complejo $\mathbb{C}^n$, obtener un número complejo.

Definición 1.4. *Sea V un espacio vectorial sobre $\mathbb{C}$ y $u,v,w \in V$, la función $\langle\cdot,\cdot\rangle$ definida de $V \times V$ sobre $\mathbb{C}$:*

$$\langle u,v\rangle = u_1\overline{v_1} + u_2\overline{v_2} + \cdots + u_n\overline{v_n}$$

es un producto interno sobre $\mathbb{C}$ si satisface las siguientes propiedades:

1. *Es simétrica respecto a su conjugado:*

$$\langle u,v\rangle = \overline{\langle v,u\rangle}$$

2. *Es lineal en el primer argumento:*

$$\langle z\cdot u,v\rangle = z\cdot\langle u,v\rangle \quad y \quad \langle u+w,v\rangle = \langle u,v\rangle + \langle w,v\rangle \quad \forall z \in \mathbb{C} \tag{1.1}$$

3. *Es semidefinida positiva:*

$$\langle v,v\rangle \geq 0 \; y \; \langle v,v\rangle = 0 \Leftrightarrow v = 0_V$$

Por lo anterior, el espacio V es un espacio con producto interior.

Ejemplo 1.2.1. El espacio $\mathbb{C}^n$ con el producto interno definido por:

$$\langle x, y\rangle = \sum_{k=1}^{N} x_k \overline{y_k} \quad x = (x_1, \ldots, x_n), \quad y = (y_1, \ldots, y_n)$$

es un espacio con producto interior.

Notemos que para probar todas las propiedades nos limitaremos a hacerlo sobre $\mathbb{C}$ considerando $x \equiv u$ y $y \equiv v$. La prueba se extiende por linealidad.

1. De la izquierda de la igualdad tenemos: $\langle u, v\rangle = u \cdot \overline{v}$ y de la parte derecha $\overline{\langle v, u\rangle} = \overline{(v \cdot \overline{u})} = \overline{v} \cdot u$. En las últimas dos igualdades hemos aplicado la definición, que el conjugado del producto de dos complejos es el producto de sus conjugados y el conjugado del conjugado es el propio número complejo.

2. Comprobemos la linealidad en el primer argumento. Por definición de producto escalar $\langle z \cdot u, v\rangle = z \cdot u \cdot \overline{v} = z \cdot \langle u, v\rangle$. Aplicando también la definición, $\langle u + w, v\rangle = (u + w) \cdot \overline{v} = u\overline{v} + w\overline{v} = \langle u, v\rangle + \langle w, v\rangle$.

   Además, de la linealidad en el primer argumento se deduce la conjugación lineal en el segundo: $\langle u, z \cdot v\rangle = \overline{\langle z \cdot v, u\rangle} = \overline{z \cdot \langle v, u\rangle} = \overline{z} \cdot \overline{\langle v, u\rangle} = \overline{z} \cdot \langle u, v\rangle$

3. Veamos que es semidefinida positiva. $\langle v, v\rangle = v \cdot \overline{v} = (c + di) \cdot (c - di) = c^2 + d^2$, que por ser suma de cuadrados, es mayor o igual a 0. En caso de ser 0, $c^2 = -d^2$ por lo que $d = c = 0$ y así $v = 0$.

Norma de un vector

El concepto de norma en un espacio vectorial sobre un cuerpo $\mathbb{K}$ es una generalización del concepto del valor absoluto en $\mathbb{R}$ y del módulo en $\mathbb{C}$.

Definición 1.5. *Una norma en un espacio vectorial V sobre un cuerpo $\mathbb{K}$ es una aplicación $\|\cdot\|: V \to \mathbb{R}$ dada por $u \to \| u \|$ que:*

1. *Es no degenerada:*
$$\forall u \in V, \ \| u \| = 0 \Leftrightarrow u = 0_V$$

2. *Verifica la desigualdad triangular:*
$$\| u + v \| \leq \| u \| + \| v \|$$

3. *Es absolutamente homogénea:*
$$\| zu \| = | z | \| u \| \quad \forall z \in \mathbb{K}$$

Un espacio normado es un espacio vectorial V con producto interno en el que hemos fijado una norma definida por dicho producto.

Ejemplo 1.2.2. Sea V un espacio vectorial sobre $\mathbb{C}$ con un producto interno $\langle \cdot, \cdot \rangle$. Sea la aplicación $\| \cdot \|: V \to \mathbb{R}$ definida por:

$$\| u \| = \sqrt{\langle u, u \rangle}$$

es una norma para el espacio vectorial V. Veamos que satisface las propiedades de la definición 1.5:

1. Si $\| u \| = 0 \Rightarrow \sqrt{\langle u, u \rangle} = 0$ de donde aplicando la propiedad 3 de la definición 1.4 por la cual el producto interno es semidefinido positivo, se tiene $u = 0_V$

2. Elevando al cuadrado la parte izquierda de la igualdad:

$$\begin{aligned} \| u + v \|^2 &= \langle u + v, u + v \rangle = (u + v) \cdot \overline{(u + v)} \\ &\underset{(1)}{=} (u + v) \cdot (\overline{u} + \overline{v}) = u\overline{u} + v\overline{v} + u\overline{v} + v\overline{u} \\ &= \langle u, u \rangle + \langle v, v \rangle + \langle u, v \rangle + \langle v, u \rangle = \| u \|^2 + \| v \|^2 + |\langle u, v \rangle| \cdot |\langle v, u \rangle| \\ &\underset{(2)}{\leq} \| u \|^2 + \| v \|^2 + 2 \| u \| \cdot \| v \| = (\| u \| + \| v \|)^2 \end{aligned}$$

   donde en (1) hemos aplicado la propiedad de los números complejos de que el conjugado de la suma es la suma de los conjugados y en (2) hemos utilizado que $|\langle v, u \rangle| \leq \| u \| \cdot \| v \|$ que se conoce como **desigualdad de Cauchy-Schwartz**.

3. $$\| zu \| = \sqrt{\langle zu, zu \rangle} \underset{(1)}{=} \sqrt{z\langle u, zu \rangle} \underset{(2)}{=} \sqrt{z\overline{\langle zu, u \rangle}} \underset{(3)}{=} \sqrt{z^2 \cdot \langle u, u \rangle} = | z | \, \| u \|$$

No obstante debemos tener presente que en cada espacio vectorial se pueden definir normas diferentes dando lugar a distintos espacios normados.

Cada espacio V con el producto interno definido como en 1.4 es también un espacio normado. La implicación contraria no es siempre cierta. Para verlo, introducimos el siguiente teorema.

Teorema 1.3 (Teorema de Jordan-Von Neumann)**.** *Sea* $\| \cdot \|: V \to \mathbb{R}$ *una norma con* V *un* $\mathbb{K}$ *espacio vectorial. Equivalen:*

1. $\| \cdot \|$ *está inducida por un producto interno.*

2. $\| \cdot \|$ *satisface la siguiente igualdad conocida como Ley del Paralelogramo*

$$\| x + y \|^2 + \| x - y \|^2 = 2(\| x \|^2 + \| y \|^2) \tag{1.2}$$

Demostración:

Veamos 1. $\Rightarrow$ 2.

$$\begin{aligned} \| x + y \|^2 &= \langle x + y, x + y \rangle = \langle x, x + y \rangle + \langle y, x + y \rangle = \overline{\langle x + y, x \rangle} + \overline{\langle x + y, y \rangle} \\ &= \langle y, y \rangle + \langle x, x \rangle + \langle y, x \rangle + \langle x, y \rangle = \langle y, y \rangle + \langle x, x \rangle + \langle x, y \rangle + \overline{\langle x, y \rangle} \\ &= \langle y, y \rangle + \langle x, x \rangle + 2Re\langle x, y \rangle \end{aligned} \tag{1.3}$$

$$\begin{aligned}\| x-y \|^2 &= \langle x-y, x-y\rangle = \langle x, x-y\rangle - \langle y, x-y\rangle = \overline{\langle x-y, x\rangle} - \overline{\langle x-y, y\rangle} \\ &= \langle x,x\rangle - \langle x,y\rangle - \langle y,x\rangle + \langle y,y\rangle = \langle x,x\rangle + \langle y,y\rangle - \Big(\langle x,y\rangle + \overline{\langle x,y\rangle}\Big) \\ &= \langle y,y\rangle + \langle x,x\rangle - 2Re\langle x,y\rangle \end{aligned} \tag{1.4}$$

donde hemos aplicado que si $z \in \mathbb{C}$, entonces $z + \bar{z} = 2Re(z)$. Sumando (1.3) y (1.4) obtenemos $2\langle x,x\rangle + 2\langle y,y\rangle = 2\Big(\| x \|^2 + \| y \|^2 \Big)$ como queríamos probar.

Probaremos ahora la implicación contraria. Por lo anterior anterior tenemos

$$\frac{\| x+y \|^2}{4} - \frac{\| x-y \|^2}{4} = Re\langle x,y\rangle \tag{1.5}$$

Supongamos $x = a + bi$ y $y = c + di$. Entonces

$$\begin{aligned}\langle x,y\rangle &= \langle a+bi, c+di\rangle = (a+bi)\cdot(c-di) = (ac-bd) + (-ad-bc)i \\ \langle x,iy\rangle &= \langle a+bi, -d+ci\rangle = (a+bi)\cdot(-d-ci) = (-ad-bc) + (ac+bd)i\end{aligned}$$

Por lo que $Im\langle x,y\rangle = Re\langle x,iy\rangle$ y de (1.5)

$$\langle x,y\rangle = \frac{1}{4}\Big[\| x+y \|^2 - \| x-y \|^2 \Big] + \frac{i}{4}\Big[\| x+iy \|^2 - \| x-iy \|^2 \Big],$$

que satisface

$$\begin{aligned}\langle x,x\rangle &= \frac{1}{4}\Big[\| 2x \| \Big] + \frac{i}{4}\Big[\| x+ix \|^2 - \| x-ix \|^2 \Big] \\ &= \frac{1}{4}\Big[\| 2x \| \Big] + \frac{i}{4}\Big[|1+i|^2 \cdot \| x \|^2 - |1-i|^2 \cdot \| x \|^2 \Big] \\ &= \| x \|^2\end{aligned}$$

Ahora comprobamos que $\langle \cdot, \cdot \rangle$ es producto interno.

Es semidefinida positiva: $\langle x,x\rangle = \| x^2 \| \geq 0$ y $\langle x,x\rangle = 0 \Leftrightarrow x = 0$, y simétrica respecto a su conjugado,

$$\begin{aligned}\langle x,y\rangle &= \frac{1}{4}\Big[\| x+y \|^2 - \| x-y \|^2 \Big] + \frac{i}{4}\Big[\| x+iy \|^2 - \| x-iy \|^2 \Big] = \\ &= \frac{1}{4}\Big[\| y+x \|^2 - \| y-x \|^2 \Big] + \frac{i}{4}\Big[\| y-ix \|^2 - |-i|^2 \| y+ix \|^2 \Big] = \\ &= \frac{1}{4}\Big[\| y+x \|^2 - \| y-x \|^2 \Big] - \frac{i}{4}\Big[\| y+ix \|^2 - \| y-ix \|^2 \Big] = \\ &= \overline{\langle y,x\rangle}\end{aligned}$$

Para la linealidad en la primera variable, veamos en primer lugar que se cumple la igualdad

$$Re\Big(2\langle u,v\rangle\Big) = Re\Big(\langle u+w,v\rangle + \langle u-w,v\rangle\Big) \tag{1.6}$$

Por la ecuación (1.5)

$$\begin{aligned}Re\Big(\langle u+v,w\rangle\Big) &= \frac{1}{4}\Big(\| u+v+w \|^2 - \| u+v-w \|^2 \Big) \\ Re\Big(\langle u-v,w\rangle\Big) &= \frac{1}{4}\Big(\| u-v+w \|^2 - \| u-v-w \|^2 \Big)\end{aligned}$$

Luego sumando las expresiones anteriores

$$\frac{1}{4}\Big(2\parallel u+w\parallel^2+2\parallel v\parallel^2-2\parallel u-w\parallel^2-2\parallel v\parallel^2\Big)=$$
$$\frac{1}{4}\Big(2\parallel u+w\parallel^2-2\parallel u-w\parallel^2\Big)=\frac{1}{2}\Big(\parallel u+w\parallel^2-\parallel u-w\parallel^2\Big)=2Re\langle u,v\rangle$$

Por tanto

$$Re\Big(\langle u+v,w\rangle+\langle u-v,w\rangle\Big)=Re\Big(\langle u+v,w\rangle\Big)+Re\Big(\langle u-v,w\rangle\Big)=2Re\langle u,v\rangle=Re\Big(2\langle u,v\rangle\Big)$$

Como corolario se tiene

$$Im\Big(2\langle u,v\rangle\Big)=Im\Big(\langle u+w,v\rangle+\langle u-w,v\rangle\Big) \tag{1.7}$$

De (1.6) y (1.7), $2\langle u,v\rangle=\langle u+w,v\rangle+\langle u-w,v\rangle$. En particular si $u=w$, $2\langle u,v\rangle=\langle 2u,v\rangle+\langle 0,v\rangle=\langle 2u,v\rangle$.

Sea $x=u+w$, $y=u-w$,

$$\langle x,z\rangle+\langle y,z\rangle=\langle u+w,z\rangle+\langle u-w,z\rangle=2\langle u,z\rangle=\langle 2u,z\rangle=\langle x+y,z\rangle$$

Veamos ahora que se verifica

$$\lambda\langle x,y\rangle=\langle \lambda x,y\rangle \tag{1.8}$$

Distinguiendo casos:

- Si $\lambda\equiv n\in\mathbb{N}$ lo haremos por inducción. Consideramos

$$\langle nx,y\rangle=\langle (n-1)x+x,y\rangle=\langle (n-1)x,y\rangle+\langle x,y\rangle$$

Para $n=1$ y $n=2$ es obvio. Suponemos cierto para n y demostramos para $n+1$.

$$\langle (n+1)x,y\rangle=\langle nx+x,y\rangle=\langle nx,y\rangle+\langle x,y\rangle=n\langle x,y\rangle+\langle x,y\rangle=(n+1)\langle x,y\rangle$$

- Si $\lambda\equiv r\in\mathbb{Q}^+$, dado que $\left\langle\frac{1}{n}x,y\right\rangle=\frac{1}{n}\langle x,y\rangle$, sin más que tomar $x\equiv\frac{1}{n}x$ en el caso anterior $\left\langle n\cdot\frac{1}{n}x,y\right\rangle=n\left\langle\frac{1}{n}x,y\right\rangle$ luego $\frac{1}{n}\left\langle n\cdot\frac{1}{n}x,y\right\rangle=\left\langle\frac{1}{n}x,y\right\rangle$. Si $r=0$, $\langle 0,y\rangle=0=0\langle x,y\rangle$

- Si $\lambda\in\mathbb{R}$ y $\lambda\geq 0$, existe una sucesión $\{r_n\}\in\mathbb{Q}^+$ tal que $r_n\to\lambda$, por lo que $r_n\langle x,y\rangle\to\lambda\langle x,y\rangle$. Si $\lambda<0$, $\langle\lambda x,y\rangle-\lambda\langle x,y\rangle=\langle\lambda x,y\rangle+\langle-\lambda x,y\rangle=\langle\lambda x+(-\lambda x)y\rangle=0$ luego $\langle\lambda x,y\rangle=\lambda\langle x,y\rangle$.

■

Ejemplo 1.2.3. Sea $\ell^2=\left\{x=(x_1,\dots,x_n):x_n\in\mathbb{C},\sum_{n=1}^{\infty}|x_n|^p\leq\infty\right\}$, con $p\neq 2$, no es espacio con producto interno.

Si consideramos por ejemplo $x=(1,1,0\dots)$ y $y=(1,-1,0\dots)$, se tiene $\parallel x\parallel=\parallel y\parallel=2^{\frac{1}{p}}$ y $\parallel x+y\parallel=\parallel x-y\parallel=2$ luego $8=\parallel x+y\parallel^2+\parallel x-y\parallel^2\neq 2(\parallel x\parallel)^2+(\parallel y\parallel)^2=16$.

Por lo tanto, al no verificarse la Ley del Paralelogramo, por el teorema anterior, no es un espacio con producto interno.

1.3 Bases ortogonales y ortonormales

Una de las consecuencias más importantes de tener un espacio con producto interno, es la posibilidad de definir la ortogonalidad vectorial.

Un vector v cuya longitud es 1, i.e., que verifica $\| v \| = 1$ es un vector unitario. También nos referimos a él como vector normalizado.

Definición 1.6. *Decimos que una base B del espacio V es ortogonal si $\langle v_i, v_j \rangle = 0 \ \forall i \neq j$ y $v_i, v_j \in B$, i.e., todos sus vectores son ortogonales dos a dos.*

Definición 1.7. *Si la base B del espacio V satisface la definición 1.6 y además todos sus vectores son unitarios, entonces B es una base ortonormal.*

El siguiente resultado, que nos asegura la existencia de una base ortonormal para cualquier espacio vectorial de dimensión finita V sobre el que haya definido un producto escalar, permite también obtener un procedimiento recursivo para el cálculo de dicha base a partir de cualquier otra.

Proposición 1.1. ***Método de Ortonormalización de Gram-Schmidt.***
Sea $(V, \langle \cdot, \cdot \rangle)$ un espacio vectorial con producto interno, $\{v_1, \ldots, v_n\}$ una base de V y $L(v_1, \ldots, v_k)$ el subespacio generado por k vectores. Existe una base ortonormal $\{w_1, \ldots, w_n\}$ de forma que

$$L(v_1, \ldots, v_k) = L(w_1, \ldots, w_k) \qquad \forall 1 \leq k \leq n$$

Demostración:

Construiremos una base ortogonal $\{z_1, \ldots, z_n\}$ satisfaciendo:

$$L(z_1, \ldots, z_k) = L(v_1, \ldots, v_k) \qquad \forall 1 \leq k \leq n$$

Normalizando los vectores de dicha base obtendremos la base ortonormal que buscamos.

Para construir los vectores seguiremos un procedimiento recursivo:

1° Consideramos el primer vector $z_1 = v_1$, con lo que $L(z_1) = L(v_1)$.

2° Buscamos z_2 que verifique la ortogonalidad, i.e., $\langle z_1, z_2 \rangle = 0$ y que $L(z_1, z_2) = L(v_1, v_2)$. Esto último se tiene únicamente si $z_2 = av_1 + bv_2$ Suponiendo $b = 1$

$$0 = \langle z_1, z_2 \rangle = \langle v_1, v_2 + av_1 \rangle = \langle v_1, v_2 \rangle + a\langle v_1, v_1 \rangle$$

y así

$$a = \frac{-\langle v_1, v_2 \rangle}{\| v_1 \|^2}$$

Obteniendo

$$z_2 = v_2 - \frac{\langle v_1, v_2 \rangle}{\| v_1 \|^2} \cdot v_1 = v_2 - \frac{\langle z_1, v_2 \rangle}{\| z_1 \|^2} \cdot z_1$$

3° Construidos $z_1, \ldots, z_r \in V$ tales que:

i) $\langle z_i, z_j \rangle = 0$ si $i \neq j$

ii) $L(z_1,\dots,z_k) = L(v_1,\dots,v_k) \qquad \forall 1 \le k \le r$

Sea el vector

$$z_{r+1} = v_{r+1} - \sum_{i=1}^{r} \frac{\langle z_i, v_{r+1}\rangle}{\| z_i \|^2} \cdot z_i$$

i) $L(z_1,\dots,z_r,z_{r+1}) = L(z_1,\dots,z_r,v_{r+1}) = L(v_1,\dots,v_r,v_{r+1})$

ii) Para $j \le r$:

$$\begin{aligned}
\langle z_j, z_{r+1}\rangle &= \langle z_j, v_{r+1} - \sum_{i=1}^{r} \frac{\langle z_i, v_{r+1}\rangle}{\| z_i \|^2} \cdot z_i\rangle \\
&= \langle z_j, v_{r+1}\rangle - \sum_{i=1}^{r} \frac{\langle z_i, v_{r+1}\rangle}{\| z_i \|^2} \cdot \langle z_j, z_i\rangle \\
&= \langle z_j, v_{r+1}\rangle - \frac{\langle z_j, v_{r+1}\rangle}{\| z_j \|^2} \cdot \langle z_j, z_j\rangle \\
&= 0
\end{aligned}$$

Luego z_{r+1} satisface las propiedades requeridas y obtenemos la base ortogonal que buscábamos.

Finalmente, considerando $w_i = \frac{z_i}{\|z_i\|}$ para cada $1 \le i \le n$, el conjunto $\{w_1,\dots,w_n\}$ es base ortonormal de V que satisface lo pedido.

■

1.4 Espacios de Hilbert

Según uno de los postulados de la computación cuántica, asociado a todo sistema físico encontramos un espacio de Hilbert, es decir, un espacio vectorial complejo con producto interno normalizado, que es el espacio de estados de dicho sistema.

En matemáticas, los espacios de Hilbert son la generalización más natural y cercana en el ámbito de las "dimensiones infinitas" de nuestra geometría euclidiana clásica y han sido, hasta ahora, los espacios más útiles en las aplicaciones para el análisis funcional y el álgebra lineal.

A pesar de que los espacios de Hilbert serían de muy poco valor si no fuera por las infinitas dimensiones, algunas ideas físicas que desarrollaremos sólo se pueden estudiar considerando espacios finitos.

En particular, para el estudio de los espacios vectoriales complejos que surgen en la computación e información cuántica, nos centraremos en la dimensión finita.

Previamente a la definición de espacio de Hilbert, introducimos los conceptos de sucesión convergente y sucesión de Cauchy.
Sea $\{x_n\} = (x_1,\dots,x_n)$ una sucesión de vectores del espacio vectorial V, si se verifica (1.9) decimos que converge en norma a un vector $v \in V$, y si se verifica (1.10) decimos

que dicha sucesión es de Cauchy. Si toda sucesión de Cauchy converge, decimos que el espacio V es completo.

$$\lim_{n\to\infty} \| x_n - v \| = 0 \Leftrightarrow \forall \epsilon \geq 0, \exists N_\epsilon \in \mathbb{N} : \quad \| x_n - v \| \leq \epsilon \quad \forall n \geq N_\epsilon \tag{1.9}$$

$$\forall \epsilon \geq 0, \exists N_\epsilon \in \mathbb{N} : \quad \| x_n - x_m \| \leq \epsilon \quad \forall n, m \geq N_\epsilon \tag{1.10}$$

Definición 1.8. *Un espacio prehilbertiano es un espacio vectorial dotado de un producto interno. Un espacio de Hilbert es un espacio prehilbertiano completo con la norma definida por el producto interno.*

Todos los espacios vectoriales tienen bases finitas. Una de las principales ventajas de los espacios de Hilbert de dimensión finita frente a los que no la tienen, es la posibilidad de describir bases ortonormales. Una base $B_{\mathcal{H}}$ para un espacio de Hilbert $\mathcal{H}$ es un subconjunto maximal ortonormal de $\mathcal{H}$.

A partir de ahora, cuando hagamos referencia a un espacio de Hilbert $\mathcal{H}$ de dimensión finita n, nos estaremos refiriendo al espacio de Hilbert $\mathbb{C}^n$, con el producto interno estudiado anteriormente.

Teorema 1.4. *Sea $\mathcal{H}$ un espacio de Hilbert, todo subconjuto finito o numerable que sea ortonormal es linealmente independiente.*

Demostración:

Lo probaremos para un subconjunto finito. La demostración para un conjunto numerable es análoga. Para el caso finito, sea $\{x_1, \ldots, x_n\}$ un subconjunto ortonormal y sea $x \in \mathcal{H}$ tal que $x = \sum_{k=1}^{n} \lambda_k x_k$ entonces

$$\lambda_j \underset{(1)}{=} \left\langle \sum_{k=1}^{n} \lambda_k x_k, x_j \right\rangle = \langle x, x_j \rangle$$

En (1) hemos aplicado si $j = k$ se tiene $\langle \lambda_j x_j, x_j \rangle = \lambda_j \langle x_j, x_j \rangle = \lambda_j$ y si por el contrario $j \neq k$ entonces $\langle \lambda_k x_k, x_j \rangle = \lambda_k \langle x_k, x_j \rangle = 0$. Considerando $x = 0$, $\langle 0, x_j \rangle = 0$ para todo $j = 1, \ldots, n$, luego el subconjunto $\{x_1, \ldots, x_n\}$ es linealmente independiente.

■

1.5 Producto tensorial de espacios vectoriales.

Sea V un $\mathbb{K}$–espacio vectorial y $W \subset V$ un subespacio suyo. Definimos la relación de equivalencia

$$v_1 \equiv v_2 \Leftrightarrow v_1 - v_2 \in W \qquad \forall v_1, v_2 \in W$$

que particiona al conjunto V en clases de equivalencia

$$\overline{v} = \{u \in V : u \equiv v\} = v + W = \{v + w, w \in W\}$$

y el conjunto de dichas clases de equivalencia es lo que conocemos como espacio vectorial cociente de V por W, es decir,

$$V/W = \{\overline{v} : v \in V\}$$

Si $u+W$ y $v+W$ son elementos de V/W y $k \in \mathbb{K}$, es inmediato comprobar que tiene estructura de espacio vectorial con la suma y el producto por escalares definidos respectivamente por

$$(u+W)+(v+W) = (u+v)+W$$
$$k(u+W) = ku+W$$

Esta suma está bien definida dado que si $u+W = u'+W$ y $v+W = v'+W$, entonces $(u+v)+W = (u'+v')+W$ dado que $u-u', v-v' \in W$ y así $(u+v)-(u'+v') \in W$.

Además, dado que $u+W = u'+W$, entonces $ku-ku' = k(u-u') \in W$, por ser W un subespacio vectorial de V con lo que se comprueba que el producto también está bien definido.

Construcción y base del producto tensorial

Si consideramos el producto $V \times W$ como conjunto podemos definir el espacio vectorial

$$K(V\times W) = \left\{ \sum_i^n \alpha_i \cdot z_{(e_i,f_i)} : n \in \mathbb{N}, \alpha_i \in \mathbb{K}, (e_i,f_i) \in V \times W \right\}$$

donde $e_{(e,f)}$ son los vectores que constituyen una base ortonormal de $V\times W$ considerado como espacio vectorial y R es subespacio de $K(V\times W)$ generado por las relaciones de equivalencia

$$\begin{aligned} z_{(e_1+e_2,f)} &\equiv z_{(e_2,f)} + z_{(e_1,f)} \\ z_{(e,f_1+f_2)} &\equiv z_{(e,f_1)} + z_{(e,f_2)} \\ cz_{(e,f)} &\equiv z_{(ce,f)} \equiv z_{(e,cf)} \end{aligned}$$

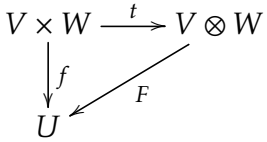
El producto tensorial de los espacios vectoriales V y W es entonces el espacio vectorial cociente

$$V \otimes W = K(V\times W)/R$$

Sea la aplicación $t : V \times W \to V \otimes W$, que asigna a cada elemento (v,w) su clase de equivalencia en $V\otimes W$, que denotaremos por $v\otimes w$. A partir de las relaciones anteriores que determinan el producto tensor, se sigue inmediatamente que t es una aplicación bilineal, es decir, si $a,b \in \mathbb{K}$ y $v_1,v_2 \in V, w_1,w_2 \in W$

$$t(av_1+bv_2,w) = at(v_1,w)+bt(v_2,w)$$
$$t(v,aw_1+bw_2) = at(v,w_1)+bt(v,w_2)$$

Teorema 1.5. *Sea U un $\mathbb{K}$-espacio vectorial. Entonces para cualquier aplicación bilineal $f : V \times W \to U$, existe una única aplicación lineal $F : V \otimes W \to U$ tal que satisfaciendo $F \circ t = f$, donde F viene dada por $F(v\otimes w) = f(v,w)$ que hace que el siguiente diagrama conmute.*



La existencia de F es lo que constituye la propiedad universal del producto tensorial.

Demostración:

La función f definida sobre la base canónica $V \times W$ de $K(V \times W)$ induce una única transformación lineal $F' : K(V \times W) \to U$ definida por $F'(v,w) = f(v,w)$.

Definimos ahora la función $F(\overline{z}) = F'(z)$, donde $z \in K(V \times W)$. En particular, si $z = z_{(e_i,f_i)}$ es un vector de la base que notaremos como $z = (v,w)$ para simplificar la notación, entonces $F(v \otimes w) = F'(v,w) = f(v,w)$.

Para demostrar que F está bien definida ha de probarse que dos elementos iguales en $V \otimes W$ tienen la misma imagen. Para ello nos basta probar que se conservan las relaciones que definen dicho producto tensor. De este modo,

$$\begin{aligned} F[(v \otimes w) + (v' \otimes w)] = F[(v+v') \otimes w] = F'(v+v', w) = f(v+v', w) \\ = f(v,w) + f(v',w) = F'(v,w) + F'(v',w) = F(v \otimes w) + F(v' \otimes, w) \end{aligned}$$

$$F(kv \otimes w) = F(k(v \otimes w)) = F'(kv, w) = f(kv, w) = kf(v,w) = kF(v \otimes w)$$

Por ser f bilineal se tiene $F[(v \otimes w) + (v \otimes w')] = F(v \otimes w) + F(v \otimes w')$ y $F(v \otimes kw) = kF(v \otimes w)$ Como F' es K-lineal, F es una transformación lineal y $F \circ t(v,w) = F(v \otimes w) = f(v,w)$, con lo que $F \circ t = f$.

Finalmente, veamos la unicidad de F. Suponemos $G : V \otimes W \to U$, tal que $G \circ t = f$. Como G es una transformación lineal basta considererar el caso $v \otimes w$, entonces $G \circ t(v,w) = f(v,w) = G(v \otimes w)$ por lo que $G \equiv F$.

■

Teorema 1.6. *Sean los conjuntos $B_V = \{e_1, \ldots, e_n\}$ y $B_W = \{f_1, \ldots, f_m\}$ las bases de los espacios vectoriales V y W de dimensiones n y m respectivamente. Entonces $B_V \otimes B_W = \{e_i \otimes f_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ es una base del espacio $V \otimes W$ y por lo tanto $dim_{\mathbb{K}}(V \otimes W) = nm$.*

Demostración:

Consideramos el $K-$espacio vectorial U^{nm} de dimension nm y $Z = \{z_{11}, \ldots, z_{1m}, z_{21} \ldots, z_{2m}, \ldots, z_{n1} \ldots, z_{nm}\}$ su base canónica. Definimos la transformación lineal T y la función lineal f como

$$\begin{aligned} T : U^{nm} \to K(V \times W) \qquad f : V \otimes W \to U^{nm} \\ z_{ij} \to e_i \otimes f_j \qquad f(v,w) = e_1 f_1 z_{11} + e_1 f_m z_{1m} + \cdots + e_n f_1 z_{n1} + e_n f_m z_{nm} \end{aligned}$$

donde $v = \sum_i^n v_i e_i$ y $w = \sum_j^m w_j f_j$. Por el teorema 1.5 existe una transformación lineal $F : V \otimes W \to U^{nm}$ definida por $F(v \otimes w) = f(v,w)$. Además $F \circ T = I_{U^{nm}}$ y $T \circ F = I_{V \otimes W}$. Por ello T es isomorfismo de espacios vectoriales con lo que $B_V \otimes B_W$ es base de $V \otimes W$ y $dim_{\mathbb{K}}(V \otimes W) = nm$.

■

Por el teorema anterior cualquier vector en $V \otimes W$ queda descrito por los vectores de la base $e_i \otimes f_j$ cuyos coeficientes son $v_i w_j$ por lo que es bilineal, es decir lineal en V y en W.

$$v \otimes w = \Big(\sum_i^n v_i e_i \Big) \otimes \Big(\sum_j^m w_j f_j \Big) = \sum_i^n \sum_j^m v_i w_j \Big(e_i \otimes f_j \Big)$$

Considerando $n = 2$ y $m = 3$, expresando como vectores columna

$$\vec{e_1} \otimes \vec{f_1} = \left(\begin{array}{c} 1 \\ 0 \\ 0 \\ \hline 0 \\ 0 \\ 0 \end{array}\right), \quad \ldots, \quad \vec{e_2} \otimes \vec{f_3} = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ \hline 0 \\ 0 \\ 1 \end{array}\right) \Rightarrow \vec{v} \otimes \vec{w} = \left(\begin{array}{c} v_1 w_1 \\ v_1 w_2 \\ v_1 w_3 \\ \hline v_2 w_1 \\ v_2 w_2 \\ v_2 w_3 \end{array}\right)$$

Producto de Kronecker

Una matriz A no es más que una transformación lineal de un espacio vectorial V en otro. Para el desarrollo de sus aplicaciones en la computación cuántica, nos limitaremos a considerar $A : V \to V$ tal que $\vec{v} \to A\vec{v}$ o de forma equivalente

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \to \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

En el espacio $V \otimes W$ la matriz A actúa sobre el espacio V sin afectar a W. Lo representamos como la matriz $A \otimes I$ donde I es la matriz identidad. Si consideramos $n = 2$ y $m = 3$, entonces $dim(A) = n \times n = 2 \times 2$ y $dim(I) = m \times m = 3 \times 3$

$$(A \otimes I)(\vec{v} \otimes \vec{w}) = \left(\begin{array}{ccc|ccc} a_{11} & 0 & 0 & a_{12} & 0 & 0 \\ 0 & a_{11} & 0 & 0 & a_{12} & 0 \\ 0 & 0 & a_{11} & 0 & 0 & a_{12} \\ \hline a_{21} & 0 & 0 & a_{22} & 0 & 0 \\ 0 & a_{21} & 0 & 0 & a_{22} & 0 \\ 0 & 0 & a_{21} & 0 & 0 & a_{22} \end{array}\right) \left(\begin{array}{c} v_1 w_1 \\ v_1 w_2 \\ v_1 w_3 \\ \hline v_2 w_1 \\ v_2 w_2 \\ v_2 w_3 \end{array}\right) = \left(\begin{array}{c} (a_{11} v_1 + a_{12} v_2) w_1 \\ (a_{11} v_1 + a_{12} v_2) w_2 \\ (a_{11} v_1 + a_{12} v_2) w_3 \\ \hline (a_{21} v_1 + a_{22} v_2) w_1 \\ (a_{21} v_1 + a_{22} v_2) w_2 \\ (a_{21} v_1 + a_{22} v_2) w_3 \end{array}\right)$$

Es decir, $(A \otimes I)(\vec{v} \otimes \vec{w}) = (A\vec{v}) \otimes \vec{w}$, donde la matriz A unicamente actúa sobre el vector $\vec{v} \in V$. De forma similar si consideramos la matriz $B : W \to W$ tal que $\vec{w} \to B\vec{w}$ actúa sobre $V \otimes W$ como $(I \otimes B)$ y $dim(B) = m \times m = 3 \times 3$ y $dim(I) = n \times n = 2 \times 2$

$$(I \otimes B)(\vec{v} \otimes \vec{w}) = \left(\begin{array}{ccc|ccc} b_{11} & b_{12} & b_{13} & 0 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & 0 & 0 & 0 \\ b_{31} & b_{32} & b_{33} & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & b_{11} & b_{12} & b_{13} \\ 0 & 0 & 0 & b_{21} & b_{22} & b_{23} \\ 0 & 0 & 0 & b_{31} & b_{32} & b_{33} \end{array}\right) \left(\begin{array}{c} v_1 w_1 \\ v_1 w_2 \\ v_1 w_3 \\ \hline v_2 w_1 \\ v_2 w_2 \\ v_2 w_3 \end{array}\right) = \left(\begin{array}{c} v_1(b_{11} w_1 + b_{12} w_2 + b_{13} w_3) \\ v_1(b_{21} w_1 + b_{22} w_2 + b_{23} w_3) \\ v_1(b_{31} w_1 + b_{32} w_2 + b_{33} w_3) \\ \hline v_2(b_{11} w_1 + b_{12} w_2 + b_{13} w_3) \\ v_2(b_{21} w_1 + b_{22} w_2 + b_{23} w_3) \\ v_2(b_{31} w_1 + b_{32} w_2 + b_{33} w_3) \end{array}\right)$$

Luego $(I \otimes B)(\vec{v} \otimes \vec{w}) = \vec{v} \otimes (B\vec{w})$, donde la matriz B unicamente actúa sobre el vector $\vec{w} \in V$.

Por lo anterior, sean A_1, A_2 matrices que actúan sobre V y B_1, B_2 sobre W,

$$\begin{aligned} (A_1 \otimes I)(A_2 \otimes I) &= (A_1 A_2) \otimes I \\ (I \otimes B_1)(I \otimes B_2) &= I \otimes (B_1 B_2) \\ (A \otimes I)(I \otimes B) &= (AI) \otimes (IB) = A \otimes B \\ (A \otimes B)(\vec{v} \otimes \vec{w}) &= (A\vec{v}) \otimes (B\vec{w}) \end{aligned}$$

Siendo la matriz $A \otimes B$

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & \cdots & a_{11}b_{1m} & \cdots & \cdots & a_{1n}b_{11} & \cdots & a_{1n}b_{1m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{11}b_{m1} & \cdots & a_{11}b_{mm} & \cdots & \cdots & a_{1n}b_{m1} & \cdots & a_{1n}b_{mm} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1}b_{11} & \cdots & a_{n1}b_{1m} & \cdots & \cdots & a_{nn}b_{11} & \cdots & a_{nn}b_{1m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1}b_{m1} & \cdots & a_{n1}b_{mm} & \cdots & \cdots & a_{nn}b_{m1} & \cdots & a_{nn}b_{mm} \end{pmatrix}$$

2

Computación cuántica

2.1 Definición de bra y ket de vectores

Una vez introducidos los principales conceptos algebraicos, a lo largo de los siguientes capítulos, utilizaremos la notación de los espacios vectoriales en mecánica cuántica que simplifica de manera notable la formalización de los mismos: la notación bra-ket o notación de Dirac que debe su nombre al científico Paul Dirac, constructor de la moderna teoría cuántica.

Al igual que en el ámbito de las matemáticas y la física, un vector $v = (v_1, v_2, \ldots, v_n)$ correspondiente a un espacio vectorial V de dimensión n se representa como $\vec{v}$, la representación

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \tag{2.1}$$

es lo que se conoce como "ket" y denota un vector en un espacio de Hilbert $\mathcal{H}$.

A continuación, para justificar la utilización del concepto de "bra", introducimos el concepto de espacio dual y funcional lineal.

Definición 2.1. *Sea $\mathbb{K}$ cuerpo sobre el que se ha definido un producto interno $\langle \cdot, \cdot \rangle$ y V espacio vectorial de dimensión finita sobre el cuerpo $\mathbb{K}$, un funcional lineal es una aplicación T que lleva vectores de V en escalares y verifica*

$$\begin{aligned} T(u+v) &= T(u) + T(v) \qquad \forall u, v \in V \\ T(kv) &= kT(v) \qquad \forall v \in V, k \in \mathbb{K} \end{aligned}$$

Teorema 2.1 (Teorema de representación de Riesz)**.** *Sea $T : \{V \to \mathbb{K}\}$ un funcional lineal, entonces existe un único $w \in V$ tal que*

$$T(v) = \langle v, w \rangle \qquad \forall v \in V \tag{2.2}$$

Demostración:

Sea $\{e_1, \ldots, e_n\}$ una base ortonormal del espacio V. Pretendemos encontrar w tal que $T(e_k) = \langle e_k, w \rangle \quad \forall k = 1, \ldots n$. Por ser $\{e_1, \ldots, e_n\}$ base, podemos escribir

$$w = w_1 e_1 + \cdots + w_n e_n \tag{2.3}$$

Luego $\langle w, e_j \rangle = \langle w_1 e_1, e_j \rangle + \cdots + \langle w_j e_j, e_j \rangle + \cdots + \langle w_n e_n, e_n \rangle = w_j$ donde hemos multiplicado escalarmente (2.3) por e_j y se ha considerado $\langle e_j, e_j \rangle = 1$ y $\langle e_i, e_j \rangle = 0$ ambas igualdades por ser base ortonormal. Por tanto

$$w = \langle w, e_1 \rangle e_1 + \cdots + \langle w, e_n \rangle e_n \tag{2.4}$$

Por la simetría respecto a su conjugado del producto interno, se tiene $\overline{T(e_k)} = \langle w, e_k \rangle$, luego sustituyendo en (2.4)

$$w = \overline{T(e_1)}e_1 + \cdots + \overline{T(e_n)}e_n \tag{2.5}$$

Por otra parte si $v = \sum_{i=1}^{n} v_i e_i$ resulta

$$T(v) = T(\sum_{i=1}^{n} v_i e_i) = \sum_{i=1}^{n} v_i T(e_i) \tag{2.6}$$

Así, por (2.5) y (2.6) y aplicando la simetría respecto a su conjugado del producto escalar y que es lineal en la primera variable, se tiene

$$\langle v, w \rangle = \langle \sum_{i=1}^{n} v_i e_i, \sum_{i=1}^{n} \overline{T(e_i)} e_i \rangle = \sum_{i=1}^{n} v_i \langle e_i, \sum_{i=1}^{n} \overline{T(e_i)} e_i \rangle \tag{2.7}$$

$$= \sum_{i=1}^{n} v_i \overline{\overline{T(e_i)}} \langle e_i, e_i \rangle = \sum_{i=1}^{n} v_i T(e_i) = T(v) \tag{2.8}$$

Supongamos que existen $w_1, w_2 \in V$ tales que $T(v) = \langle v, w_1 \rangle = \langle v, w_2 \rangle, \forall v \in V$. Entonces

$$\overline{\langle w_1, v \rangle} = \overline{\langle w_2, v \rangle}$$

implica que

$$0 = \overline{\langle w_1, v \rangle} - \overline{\langle w_2, v \rangle} = \overline{\langle w_1, v \rangle - \langle w_2, v \rangle}$$

de donde

$$\langle w_1, v \rangle - \langle w_2, v \rangle = \langle w_1 - w_2, v \rangle = 0, \ \forall v \in V$$

en particular, para $v = w_1 - w_2$, y así $w_1 - w_2 = 0$, de donde $w_1 = w_2$.

■

Definición 2.2. *Sean V, T y $\mathbb{K}$ en las condiciones del teorema 2.1, al conjunto $V^* = \{T : V \to \mathbb{K}\}$ lo llamamos espacio dual de V.*

Teorema 2.2. *Sea $\mathcal{H}$ un espacio de Hilbert sobre el cuerpo $\mathbb{K}$ de dimensión finita y sea $\mathcal{H}^*$ su espacio dual. Entonces $\phi : \mathcal{H} \to \mathcal{H}^*$ definida por $\phi(v)(w) = \langle w, v \rangle$ para $\forall v, w \in \mathcal{H}$, verifica*

$$\phi(v_1 + v_2)(w) = \phi(v_1)(w) + \phi(v_2)(w) \qquad \forall v_1, v_2 \in \mathcal{H}$$
$$\phi(kv)(w) = \overline{k}\phi(v)(w) \qquad \forall k \in \mathbb{K}$$

Demostración:

Por el teorema de representación de Riesz, ϕ es biyectiva. En concreto, es sobreyectiva, dado que para cualquier $T \in \mathcal{H}^*$, existe $v \in \mathcal{H}$ tal que $T(-) = \langle -, v \rangle$. Por otro lado, es inyectiva como consecuencia de la unicidad de dicho $v \in \mathcal{H}$.

Sean ahora $v_1, v_2 \in \mathcal{H}$. Entonces, para cualquier $w \in \mathcal{H}$, por ser el producto interno lineal en la primera variable, se tiene que

$$\phi(v_1 + v_2)(w) = \langle w, v_1 + v_2 \rangle = \overline{\langle v_1 + v_2, w \rangle} = \overline{\langle v_1, w \rangle} + \overline{\langle v_2, w \rangle}$$
$$= \langle w, v_1 \rangle + \langle w, v_2 \rangle = \phi(v_1)(w) + \phi(v_2)(w)$$

Análogamente, sean $v \in \mathcal{H}$ y $k \in \mathbb{K}$. Entonces

$$\phi(kv)(w) = \langle w, kv\rangle = \overline{\langle kv, w\rangle} = \overline{k\langle v, w\rangle} = \overline{k}\langle w, v\rangle$$

■

Como hemos visto, el teorema de representación de Riesz nos asegura que a cada vector de un espacio de Hilbert $\mathcal{H}$, es posible asociarle un funcional lineal en su espacio dual $\mathcal{H}^*$, es decir, que existe una biyección entre ambos espacios y por tanto son isomorfos.

Es por ello que para cada ket $|v\rangle$ podemos considerara su vector dual $\langle v| \in \mathcal{H}^*$ que denominaremos bra.

2.2 Definición de qubit

La unidad básica de información procesada en computación clásica es el *bit* que puede representar el 0 ó el 1. De manera análoga, en computación cuántica, el sistema más simple y elemental de información es el bit cuántico, más conocido como qubit por su denominación del inglés, *quantum bit*.

Al igual que un bit, el qubit puede encontrarse en los estados 0 ó 1, sin embargo también existe la posibilidad de encontrarlo que lo que llamamos *superposición*, que no es más que la combinación lineal de ambos estados.

Estado de un qubit

Completando el primer postulado de la computación cuántica, sobre el *espacio de estados* que ya introdujimos en la sección 1.4, un sistema físico esta completamente descrito por su vector de estados que es un vector unitario en el espacio de estados.

Como ya adelantábamos, cada qubit $|\psi\rangle$ es un sistema cuántico, por lo que, por el postulado anterior, queda representado por un vector de estado en el espacio de Hilbert $\mathcal{H}$.

Definición 2.3. *Sea $|\psi\rangle$ el estado de un qubit, podemos expresarlo como*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.9}$$

Donde α y β son números complejos y $\{|0\rangle, |1\rangle\}$ es una base ortonormal conocida como base computacional, tal que

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.10}$$

Podemos decir que equivalen al 0 y el 1 en la computación clásica. Nótese que $\{|0\rangle, |1\rangle\}$ es sólo una de las posibles bases para los estados de un qubit.

Como introducíamos, al contrario que ocurre con los bits, los qubits pueden existir en un estado continuo entre el 0 y el 1 hasta que son observados, es decir, cuando medimos un qubit, sólo obtendremos 0 ó 1 como resultado posible.

Según las leyes de la mecanica cuántica, los coeficientes α y β de la definición 2.3 son las amplitudes del estado del qubit, cuyos cuadrados nos indican la probabilidades

de que el qubit se encuentre en los estados 0 y 1 respectivameete, por lo que se verifica la *condición de normalización*

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.11}$$

Dicha condición justifica que el vector que describe el estado de un qubit sea unitario y por ello consideremos un espacio vectorial normalizado, es decir un espacio de Hilbert.

Esfera de Bloch

Además de la definición 2.3, en la que un qubit queda caracterizado como vector en un espacio de Hilbert bidimensional, veamos una descripción gráfica de él.

Dado que en 2.9, α y β son números complejos, empleando $e^{i\phi} = cos(\phi) + isen(\phi)$ ó formula de Euler por la cual cualquier número complejo $z = |z| \cdot e^{i\phi} = |z| \cdot (cos(\phi) + isen(\phi))$ tenemos

$$|\psi\rangle = |\alpha|\, e^{i\phi_\alpha} |0\rangle + |\beta|\, e^{i\phi_\beta} |1\rangle, \tag{2.12}$$

donde el qubit viene dado en función de $|\alpha|$, $|\beta|$, ϕ_α y ϕ_β, parámetros reales.

Invarianza respecto a la fase global

Para la expresión de un número complejo $z = |z| \cdot e^{i\phi}$, el valor $e^{i\phi}$ es la fase de dicho número complejo. Como hemos visto anteriormente, en la expresión (2.12) las únicas cantidades medibles son las probabilidades $|\alpha|^2$ y $|\beta|^2$, por lo que para ver la invarianza respecto a la fase global de $|\psi\rangle$ bastará ver la de dichas cantidades.

$$|\alpha e^{i\phi_\alpha}|^2 = \overline{\alpha e^{i\phi_\alpha}} \cdot \alpha e^{i\phi_\alpha} = \overline{\alpha}\alpha \cdot e^{i\phi_\alpha} e^{-i\phi_\alpha} = \overline{\alpha}\alpha = |\alpha|^2 \tag{2.13}$$

Análogamente para β, por lo que podemos multiplicar libremente por $e^{-i\phi_\alpha}$

$$|\psi\rangle e^{-i\phi_\alpha} = (|\alpha|\,|0\rangle + |\beta|\, e^{i(\phi_\beta - \phi_\alpha)} |1\rangle) = |\alpha|\,|0\rangle + |\beta|\, e^{i\phi} |1\rangle \tag{2.14}$$

donde $\phi \equiv \phi_\beta - \phi_\alpha$ con lo que hemos expresado el qubit dependiendo de $|\alpha|$, $|\beta|$ y ϕ.

Representación esférica

Dado que $\beta \in \mathbb{C}$, $\beta = x + iy$, la condición de normalización podemos expresarla como

$$1 = |\alpha|^2 + |x + iy|^2 = \alpha^2 + x^2 + y^2 \tag{2.15}$$

lo que no es más que la ecuación de una esfera unitaria en el espacio real 3-dimensional.

Considerando las coordenadas esféricas respecto a los ángulos $0 \leq \phi < 2\pi, 0 \leq \theta \leq \pi$.

$$\begin{aligned} x &= cos(\phi)sen(\theta) \\ y &= sen(\phi)sen(\theta) \\ z &= cos(\theta) = \alpha \end{aligned}$$

y sustituyendo en 2.14

$$\begin{aligned}|\psi\rangle &= |\alpha|\,|0\rangle + |x+iy|^2\,|1\rangle \\ &= cos(\theta)\,|0\rangle + \Big(cos(\phi)sen(\theta) + isen(\phi)sen(\theta)\Big)|1\rangle \\ &= cos(\theta)\,|0\rangle + sen(\theta)e^{i\phi}|1\rangle\end{aligned}$$

Recordemos las fórmulas del seno y del coseno de la resta de dos ángulos:

$$\begin{aligned}cos(\pi-\theta) &= cos(\pi)cos(\theta) + sen(\pi)sen(\theta) \\ &= -cos(\theta) \qquad (2.16)\\ sen(\pi-\theta) &= sen(\pi)cos(\theta) - cos(\pi)sen(\theta) \\ &= sen(\theta) \qquad (2.17)\end{aligned}$$

Si consideramos un estado $|\psi'\rangle$, en el lado opuesto de la esfera tendrá coordenadas $(1, \pi-\theta, \phi+\pi)$.

$$\begin{aligned}|\psi'\rangle &= cos(\pi-\theta)\,|0\rangle + sen(\pi-\theta)e^{i(\phi+\pi)}|1\rangle \\ &= -cos(\theta)\,|0\rangle + sen(\theta)e^{i(\phi+\pi)}|1\rangle \qquad (2.18)\\ &= -cos(\theta)\,|0\rangle - sen(\theta)e^{i\phi}|1\rangle \qquad (2.19)\\ &= -|\psi\rangle\end{aligned}$$

donde en 2.18 hemos aplicado 2.16 y 2.17 y en 2.19 la identidad de Euler $e^{i\pi}+1=0$.

Hemos comprobado que cualquier estado en la mitad inferior de la esfera, es el opuesto de otro en la semiesfera superior. Obsérvese que si $\theta = 0$, $|\psi\rangle = |0\rangle$, estado que corresponde al polo norte de la esfera y si $\theta = \pi/2$, $|\psi\rangle = e^{i\phi}|1\rangle$, correspondiente a un punto en el ecuador.

Por lo anterior, y para no repetir estados, consideramos $0 \leq \theta \leq \pi/2$ en lugar de $0 \leq \theta \leq \pi$. Por lo tanto el estado más general de un qubit se escribe como

$$|\psi\rangle = cos\Big(\frac{\theta}{2}\Big)|0\rangle + e^{i\phi}sen\Big(\frac{\theta}{2}\Big)|1\rangle \qquad (2.20)$$

que representa un punto es una esfera 3-dimensional que conocemos como esfera de Bloch. Los estados $|0\rangle$ y $|1\rangle$ del bit clásico corresponden a los polos norte y sur de la esfera y las correspondientes probabilidades a un punto en el segmento que une ambos polos.

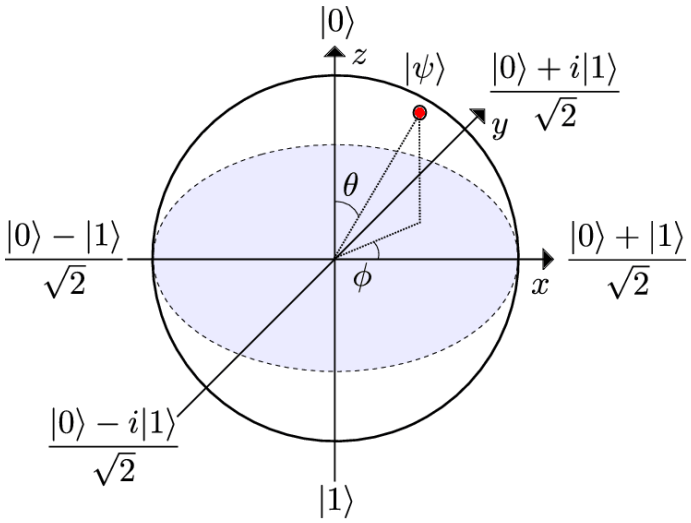


Figura 2.1: *Esfera de Bloch*

Una de las ventajas de la esfera de Bloch como vemos en la figura 2.1, es que nos permite representar la superposición de los estados del qubit en la base $\{|+\rangle, |-\rangle\}$, donde $|+\rangle \equiv \big(|0\rangle + |1\rangle\big)/\sqrt{2}$ y $|-\rangle \equiv \big(|0\rangle - |1\rangle\big)/\sqrt{2}$ con lo que a partir de la expresión 2.3

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \tag{2.21}$$

2.3 Composición y entrelazamiento de un sistema

Dado que la cantidad de información que representa un qubit es muy pequeña, suele ser necesario trabajar con sistemas formados por más de una sola partícula o qubit.

Según las leyes de la mecánica cuántica, si representamos por $|\psi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ el estado de un qubit que no es más que un vector en un espacio de Hilbert $\mathcal{H}_i, i = 1, \ldots, n$, entonces el espacio de estados del sistema compuesto por n qubits $\mathcal{H}$ es el producto tensor de los espacios de estados de cada uno de los qubits que lo forman.

Como veíamos, cada espacio de Hilbert tendrá asociada una base $\{|0\rangle, |1\rangle\}$ por lo que $dim(\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n) = 2^n$. Considerando $n = 2$, $|i\rangle \otimes |j\rangle \equiv |ij\rangle$ con $i, j \in \{0, 1\}$, el estado de un qubit en el sistema $\mathcal{H}_1 \otimes \mathcal{H}_2$ vendrá dado por

$$\begin{aligned} |\psi\rangle &= (|\psi_1\rangle \otimes |\psi_2\rangle) = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\ &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle \end{aligned}$$

donde $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ es la base en la notación de Dirac para el espacio 4-dimensional $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Ejemplo 2.3.1. Considerando el siguiente 2-qubit veamos que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

$$|\psi\rangle = \frac{1}{4}|00\rangle + \frac{\sqrt{3}}{4}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{3}{4}|11\rangle$$

Han de verificarse las ecuaciones

$$\alpha_1\alpha_2 = \frac{1}{4} \qquad \alpha_1\beta_2 = \frac{\sqrt{3}}{4} \qquad \beta_1\alpha_2 = \frac{\sqrt{3}}{4} \qquad \beta_1\beta_2 = \frac{3}{4} \tag{2.22}$$

De la primera y segunda obtenemos $\alpha_2 = \frac{1}{4\alpha_1}$ y $\beta_2 = \frac{\sqrt{3}}{4\alpha_1}$. Además, por la condición de normalización que satisface cualquier qubit $|\alpha_2|^2 + |\beta_2|^2 = 1$, sustituyendo lo anterior resulta

$$\left(\frac{1}{4\alpha_1}\right)^2 + \left(\frac{\sqrt{3}}{4\alpha_1}\right)^2 = 1 \Rightarrow \frac{4}{16\alpha_1^2} = 1 \Rightarrow \alpha_1^2 = \frac{1}{4} \Rightarrow \alpha_1 = \frac{1}{2}$$

De las ecuaciones de (2.22) se tiene por tanto $\alpha_1 = \alpha_2 = \frac{1}{2}$ y $\beta_1 = \beta_2 = \frac{\sqrt{3}}{2}$ y concluimos

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$

Sin embargo, no siempre podremos expresar un sistema compuesto por dos qubits como el producto tensor de dos qubits individuales.

Definición 2.4. *Sea $|\psi\rangle$ el estado de un sistema compuesto por n qubits, en caso de que estos interactúen entre sí no es posible obtener $|\psi_i\rangle$, $i = 1, \dots n$ tales que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots |\psi_n\rangle$. En este caso decimos que el estado $|\psi\rangle$ es un estado entrelazado.*

La mayoría de los estados de dos qubits son entrelazados. Por ejemplo el estado

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.23}$$

es el *estado de Bell* o par *EPR* porque fue introducido por Einstein, Podolsky y Rosen en 1935.

Es fácil ver que es entrelazado ya que no existen α_1, α_2, β_1 y β_2 tales que $\alpha_1\alpha_2 = \beta_1\beta_2 = \frac{1}{\sqrt{2}}$ y $\alpha_1\beta_2 = \alpha_2\beta_1 = 0$. Dicho estado junto con

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

constituye una base para un sistema de dos particulas entralazadas.

2.4 Operadores y representación matricial

Para abordar los postulados que asientan las bases de la teoría de la computación cuántica, en esta sección aplicaremos el concepto de operador en un espacio de Hilbert para definir algunos tipos concretos de operadores que intervienen en dichos postulados así como la visión de los tipos de productos vectoriales en la notación de Dirac.

Un operador en un espacio de Hilbert $\mathcal{H}$ es una transformación $A : \mathcal{H} \to \mathcal{H}$ del espacio vectorial en sí mismo, es decir, envía vectores de $\mathcal{H}$ en vectores de $\mathcal{H}$.

Puesto que, como hemos visto en la sección (2.1), un ket es un vector en un espacio de Hilbert, podemos definir operadores en dicho espacio.

Definición 2.5. *Sea $|\psi\rangle$ un ket, definimos el operador A como la transformación que convierte dicho ket en otro que definimos como $|\phi\rangle$*

$$A|\psi\rangle = |\phi\rangle \tag{2.24}$$

Análogamente si $\langle\mu|$ y $\langle\nu|$ son bras,

$$A\langle\mu| = \langle\nu| \tag{2.25}$$

Diremos que A es lineal si verifica:

$$A(a_1|\psi\rangle + a_2|\phi\rangle) = a_1(A|\psi\rangle) + a_2(A|\phi\rangle) \tag{2.26}$$

Cabe destacar el operador identidad $I|\psi\rangle = |\psi\rangle$ y el operador idénticamente nulo $N|\psi\rangle = 0$.

Producto interno y externo

Como consecuencia de los teoremas 2.1 y 2.2 veíamos que dado un ket $|\phi\rangle = \sum_j^n \phi_j|\gamma_j\rangle$, podemos considerar su correspondiente bra como $\langle\phi| = \sum_j^n \overline{\phi_j}\langle\gamma_j|$. El producto interno del ket $|\psi\rangle = \sum_i^n \psi_i|\gamma_i\rangle$ y el bra $\langle\phi|$ es por tanto $\Big\langle\langle\phi|, |\psi\rangle\Big\rangle$ que por convenio notaremos:

$$\langle\phi|\psi\rangle = \Big\langle \sum_j^n \overline{\phi_j}\langle\gamma_j|, \sum_i^n \psi_i|\gamma_i\rangle\Big\rangle = \sum_{ij}^n \overline{\phi_j}\psi_i\Big\langle\langle\gamma_j|, |\gamma_i\rangle\Big\rangle = \sum_{ij}^n \overline{\phi_j}\psi_i \cdot \delta_{ij} \tag{2.27}$$

$$= \sum_i^n \overline{\phi_i}\psi_i = (\overline{\phi_1}, \overline{\phi_2}, \ldots, \overline{\phi_n}) \cdot \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} = \overline{\phi_1}\psi_1 + \overline{\phi_2}\psi_2 + \cdots + \overline{\phi_n}\psi_n \tag{2.28}$$

El resultado anterior es un número real y hemos considerado la función conocida como delta de Kronecker: $\delta_{ij} = \langle\gamma_i|\gamma_j\rangle$ que tomará los valores 1 ó 0 según sea $i = j$ o $i \neq j$ respectivamente.

De 2.28 vemos como el bra de un ket o vector columna de $\mathcal{H}$, no es más que su transposición como vector fila y el conjugado de cada uno de sus componentes.

$$\langle\phi| = |\phi\rangle^\dagger = \overline{(|\phi\rangle^T)} = (\overline{\phi_1}, \overline{\phi_2}, \ldots, \overline{\phi_n}) \in \mathcal{H}^*$$

A continuación presentamos el producto externo. Un operador que, haciendo uso del producto interno, convierte un vector o ket del espacio $\mathcal{H}$ en otro.

Sean $\langle\psi'| \in \mathcal{H}^*$ y $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ definimos $|\phi\rangle\langle\psi'|$ como

$$(|\phi\rangle\langle\psi'|)(|\psi\rangle) = \langle\psi'|\psi\rangle|\phi\rangle \tag{2.29}$$

donde el producto externo es el operador que actúa sobre el ket $|\psi\rangle$, o lo que es lo mismo, el resultado de multiplicar el número complejo $\langle\psi'|\psi\rangle$ por el ket $|\phi\rangle$.

Representación matricial

Como hemos visto, cualquier ket de un espacio de Hilbert de dimensión n puede ser representado mediante un vector columna; por tanto, por la definición 2.5, cualquier operador puede ser representado en forma de matriz, es decir, la acción de un operador sobre un ket no es más que la multiplicación por una matriz.

Proposición 2.1. *Sea el operador lineal $A : \mathcal{H} \to \mathcal{H}$ donde $\{|\gamma_1\rangle,\ldots,|\gamma_n\rangle\}$ es una base ortonormal de $\mathcal{H}$. Entonces para cada i y j desde 1 hasta n , existe un A_{ij}*

$$A = \sum_{ij} A_{ij}\langle\gamma_j|\gamma_i\rangle = \sum_{ij} A_{ij}|\gamma_i\rangle\langle\gamma_j| \tag{2.30}$$

La matriz A cuadrada $n \times n$ es lo que llamamos la representación matricial del operador A.

Demostración:

En efecto, sean los kets $|\psi\rangle = \sum_j^n \psi_j|\gamma_j\rangle$ y $|\phi\rangle = \sum_i^n \phi_i|\gamma_i\rangle$, como hemos visto en la definición 2.5,

$$|\phi\rangle = A|\psi\rangle = A\sum_j^n \psi_j|\gamma_j\rangle = \sum_j^n \psi_j A|\gamma_j\rangle \tag{2.31}$$

Por otra parte, $\phi_i = \langle\gamma_i|\phi\rangle$ y sustituyendo (2.31) obtenemos:

$$\phi_i = \langle\gamma_i|\sum_j^n \psi_j A|\gamma_j\rangle = \sum_j^n \psi_j\langle\gamma_i|A|\gamma_j\rangle = \sum_j^n A_{ij}\psi_j$$

donde hemos notado $A_{ij} = \langle\gamma_i|A|\gamma_j\rangle$ el elemento en la fila i columna j de la representación matricial del operador A.

$$A = \begin{pmatrix} \langle\gamma_1|A|\gamma_1\rangle & \langle\gamma_1|A|\gamma_2\rangle & \cdots & \langle\gamma_1|A|\gamma_n\rangle \\ \langle\gamma_2|A|\gamma_1\rangle & \langle\gamma_2|A|\gamma_2\rangle & \cdots & \langle\gamma_2|A|\gamma_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle\gamma_n|A|\gamma_1\rangle & \cdots & & \langle\gamma_n|A|\gamma_n\rangle \end{pmatrix}$$

■

Operador adjunto y hermítico

Si A es un operador, consideramos el operador adjunto o hermítico conjugado al operador

$$A^\dagger = \overline{(A^T)} \tag{2.32}$$

donde, en su expresión matricial A^T denotará la matriz traspuesta de A y por $\overline{(A^T)}$ denotamos el conjugado de cada uno de sus componentes.

Por ejemplo:

$$\begin{pmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{pmatrix}^\dagger = \begin{pmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{pmatrix} \tag{2.33}$$

Teniendo en cuenta que $\langle\phi|A^\dagger = (A|\phi\rangle)^\dagger$ se tiene la siguiente definición equivalente a 2.32

Definición 2.6. *Sea A un operador lineal en un espacio de Hilbert $\mathcal{H}$, entonces el adjunto u operador hermítico conjugado de A es tal que para todo $|\psi\rangle$ y $|\phi\rangle \in \mathcal{H}$*

$$\langle\phi|A^\dagger|\psi\rangle = \langle\psi|A|\phi\rangle \tag{2.34}$$

En caso de que un operador coincida con su conjugación hermitíca, decimos que es hermítico, hermitiano o autoadjunto.

Dada la ecuación, $A|\phi\rangle = \lambda|\phi\rangle$ decimos que $|\phi\rangle$ es el autovector o vector propio asociado al autovalor o valor propio λ. Entonces si A es hermítico verifica:

1. *Sus autovalores son números reales.*

$$\begin{aligned} A|\phi\rangle = \lambda|\phi\rangle &\Rightarrow \langle\phi|A|\phi\rangle = \lambda\langle\phi|\phi\rangle \\ &\underset{(1)}{\Rightarrow} \overline{\lambda}\langle\phi|\phi\rangle = \langle\phi|A^\dagger|\phi\rangle = \lambda\langle\phi|\phi\rangle \end{aligned}$$

   donde en (1) hemos traspuesto y conjugado. Dado que $\overline{\lambda} = \lambda$, $\lambda \in \mathbb{R}$

2. *Los autovectores correspondientes a valores propios distintos son ortogonales entre sí.*

   Sean $|\phi_i\rangle$ y $|\phi_j\rangle$ vectores propios asociado a los valores propios λ y μ respectivamente. Entonces

$$\begin{aligned} (A|\phi_i\rangle)^\dagger = (\lambda|\phi_i\rangle)^\dagger = \langle\phi_i|A = \overline{\lambda}\cdot\langle\phi_i| = \lambda\cdot\langle\phi_i| \\ \Rightarrow \langle\phi_i|A|\phi_j\rangle = \lambda\cdot\langle\phi_i|\phi_j\rangle \end{aligned} \tag{2.35}$$

   Dado que $A|\phi_j\rangle = \mu|\phi_j\rangle$ de (2.35), se tiene $\langle\phi_i|\mu|\phi_j\rangle = \lambda\cdot\langle\phi_i|\phi_j\rangle$, luego $(\lambda-\mu)\langle\phi_i|\phi_j\rangle = 0$ y dado que $\lambda \neq \mu$, necesariamente $\langle\phi_i|\phi_j\rangle = 0$, por lo que son ortogonales.

Operador proyección

Una importante clase de operadores hermíticos son los operadores proyección o proyectores.

Definición 2.7. *Sea $\mathcal{H}$ un espacio de Hilbert de dimensión n, $\mathcal{X}$ un subespacio de dimensión m con $m \leq n$ y $\{|\gamma_1\rangle,\ldots,|\gamma_m\rangle\}$ una base ortonormal para $\mathcal{X}$. Entonces para cada $|\phi\rangle \in \mathcal{H}$, $|\phi\rangle = \sum_{i=1}^m \phi_i|\gamma_i\rangle$*

$$P_{\mathcal{X}}(|\phi\rangle) = \sum_{i=1}^m \phi_i|\gamma_i\rangle = \sum_{i=1}^m \langle\gamma_i|\phi\rangle|\gamma_i\rangle = |\phi\rangle\sum_{i=1}^m |\gamma_i\rangle\langle\gamma_i| \tag{2.36}$$

es la proyección en el subespacio $\mathcal{X}$ del ket $|\phi\rangle$. $P_{\mathcal{X}} = \sum_{i=1}^m |\gamma_i\rangle\langle\gamma_i|$ es lo que conocemos como proyector u operador proyección sobre el subespacio $\mathcal{X}$.

Nótese que en la segunda igualdad hemos aplicado $\phi_i = \langle\gamma_i|\phi\rangle$.

Si consideramos $\mathcal{Y}$ otro subespacio de $\mathcal{H}$ de dimensión l y $\{|\gamma_1\rangle,\ldots,|\gamma_l\rangle\}$ una base ortonormal, el operador proyección satisface las siguiente propiedades:

1. Idempotencia: $P^2 = \sum_{i=1}^m |\gamma_i\rangle\langle\gamma_i|\cdot|\gamma_i\rangle\langle\gamma_i| = \sum_{i=1}^m |\gamma_i\rangle\langle\gamma_i| = P$

2. Ortogonalidad: $P_{\mathcal{X}}P_{\mathcal{Y}} = \sum_{i=1}^m\sum_{i=1}^l |\gamma_i\rangle\langle\gamma_i|\cdot|\gamma_j\rangle\langle\gamma_j| = P_{\mathcal{Y}}P_{\mathcal{X}} = 0$

Resolución de la Identidad

En caso de considerar todo el espacio, $P_{\mathcal{H}} = \sum_{i=1}^{n} |\gamma_i\rangle\langle\gamma_i| \equiv I$, es decir, la suma de los proyectores asociados a una base ortonormal es igual a la identidad. La anterior expresión es lo que denominamos *resolución de la identidad* o *relación de cierre*.

Siendo el operador A, podemos obtener los elementos de la matriz que lo representa.

$$A = I \cdot A \cdot I = \Big(\sum_{i=1} |\gamma_i\rangle\langle\gamma_i| \Big) A \Big(\sum_{j=1} |\gamma_j\rangle\langle|\gamma_j \Big) = \sum_{i,j} \langle\gamma_i|A|\gamma_j\rangle |\gamma_i\rangle\langle\gamma_j|$$

La expresión anterior coincide con la ya obtenida en la proposición 2.1.

Medición de un sistema cuántico

Hemos visto que el estado del sistema cuántico más simple, que es el qubit, está descrito por un vector en un espacio de Hilbert. Si queremos medir ciertas propiedades de dicho sistema, este deja de estar aislado y su comportamiento durante la medición vendrá descrito por un operador.

Lo deseable es que los valores obtenidos sean reales. Como hemos comprobado, los autovalores de un operador hermítico lo son, y dado que cualquier medición de una variable o propiedad de un sistema físico es el valor propio del operador correspondiente queda patente la conveniencia de aplicar este tipo de operadores que llamaremos "Observables" en la medición del estado de un sistema cuántico.

Así pues, si consideramos el operador u observable A actuando sobre el espacio de estados que deseamos medir,

$$A|\gamma_i\rangle = i|\gamma_i\rangle \Rightarrow A = i|\gamma_i\rangle\langle\gamma_i| = iP_i \tag{2.37}$$

donde P_i es el proyector en el subespacio propio del operador A asociado al valor propio i que será la correspondiente medida.

Sea el ket que representa el estado inicial $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, los posibles valores de salida del sistema son $|0\rangle$ ó $|1\rangle$ con probabilidades α ó β respectivamente. En general, si consideramos como el estado inicial en un sistema cuántico,

$$|\phi\rangle = \sum_{i=1}^{n} \phi_i |\gamma_i\rangle \qquad \forall \phi_i \in \mathbb{C}$$

los posibles estados finales son $|\gamma_i\rangle$ con probabilidades $|\phi_i|^2$. Dado que $\phi_i = \langle\gamma_i|\phi\rangle$ se tiene

$$|\phi_i|^2 = \overline{\phi_i}\phi_i = \langle\phi|\gamma_i\rangle\langle\gamma_i|\phi\rangle = \langle\phi|P_i|\phi\rangle \tag{2.38}$$

donde hemos aplicado la definición 2.7 de operador proyección. De lo anterior, podemos obtener $|\gamma_i\rangle$, el estado final en el que se encontrará el sistema tras efectuar su medición.

$$P_i|\phi\rangle = |\phi_i|^2|\phi\rangle \Rightarrow |\gamma_i\rangle\langle\gamma_i| \cdot |\phi\rangle = |\phi_i|^2|\phi\rangle \Rightarrow |\gamma_i\rangle = \frac{P_i|\phi\rangle}{\langle\gamma_i|\phi\rangle} = \frac{P_i|\phi\rangle}{\sqrt{\langle\phi|P_i|\phi\rangle}} \tag{2.39}$$

Es decir que la medida i proyecta el estado inicial del sistema $|\phi\rangle$ sobre uno de los subespacios ortogonales correspondientes a los operadores proyección P_i con una probabilidad igual al cuadrado del módulo de la amplitud del estado inicial.

Operadores unitarios

Aunque es evidente que cualquier sistema interactúa al menos de forma mínima con otro, hay algunos que de los que puede darse una aproximación bastante precisa considerándolos como sistemas cerrados. En cualquier caso todo sistema constituye una parte de un sistema cerrado más grande (el universo) cuya evolución es unitaria.

Definición 2.8. *Sea A un operador, su operador inverso es A^{-1} tal que $A \cdot A^{-1} = A^{-1} \cdot A = I$. Un operador U se dice unitario si su adjunto es igual a su inverso es decir $U^\dagger = U^{-1}$ por lo que*

$$U^\dagger \cdot U = U \cdot U^\dagger = I$$

Si U es unitario se verifica:

1. *Sus valores propios son todos ± 1.*

   Sea $U|\phi\rangle = \lambda|\phi\rangle$

   $$\Big(U|\phi\rangle\Big)^\dagger \cdot U|\phi\rangle = \Big(U|\phi\rangle\Big)^\dagger \cdot \lambda|\phi\rangle = \Big(\lambda|\phi\rangle\Big)^\dagger \cdot \lambda|\phi\rangle \Rightarrow U^\dagger \cdot U\langle\phi|\phi\rangle = \overline{\lambda} \cdot \lambda\langle\phi|\phi\rangle$$

   Dado que U es unitario $\overline{\lambda} \cdot \lambda = 1 \Rightarrow |\lambda|^2 = 1 \Rightarrow \lambda = \pm 1$

2. *Si U es también hermítico se cumple $U^2 = I$*

   Por la definición de operador hermítico $U^\dagger = U$ y dado que es unitario $U^\dagger \cdot U = I$ por lo que $U \cdot U = I$.

3. *El producto escalar permanece invariante bajo la acción de U. Como consecuencia, todo operador unitario conserva la norma asociado a dicho producto.*

   $$U\Big(\langle\phi|\psi\rangle\Big) = \Big\langle U\langle\phi|, U|\psi\rangle\Big\rangle = \langle\phi|\psi\rangle$$

   donde hemos aplicado que $U|\phi\rangle = |\phi\rangle$ por la propiedad 1. Por lo tanto,

   $$\| U\langle\phi| \| = \sqrt{\Big\langle U|\phi\rangle, U|\phi\rangle\Big\rangle} = \sqrt{\langle\phi|\phi\rangle} = \| |\phi\rangle \| \tag{2.40}$$

Dado que conserva el producto interno, también la norma asociada a este, que no es más que la longitud del vector. De este modo, los operadores unitarios actúan en el espacio de Hilbert de una manera análoga a las rotaciones en el espacio euclideo, las cuales mantienen el módulo de un vector, y el ángulo entre dos vectores.

Estado de un sistema cuántico

Según uno de los postulados de la mecánica cuántica, la evolución temporal del estado $|\psi\rangle$ un sistema cerrado vendrá descrita por la ecuación de Schrödinger

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \tag{2.41}$$

En la ecuación anterior, $\hbar$ es una constante física conocida como constante de Planck y H es un operador hermitiano llamado Hamiltoniano que representa la energía total

del sistema. Si consideramos hamiltonianos independientes del tiempo, la solución de la anterior ecuación en los tiempos $t_0 = 0$ y $t_1 \equiv t$ vendrá dada por:

$$|\psi(t)\rangle = e^{\frac{-iH(t-0)}{\hbar}}|\psi(0)\rangle = e^{\frac{-iHt}{\hbar}}|\psi(0)\rangle \tag{2.42}$$

Sea $e^{\frac{-iHt}{\hbar}} \equiv U$ entonces $U^\dagger \equiv e^{\frac{iH^\dagger t}{\hbar}}$. Dado que por ser H operador hermitiano satisface $H = H^\dagger$, se tiene $U = e^{\frac{-iH^\dagger t}{\hbar}}$ de donde si el operador N denota el operador idénticamente nulo

$$U \cdot U^\dagger = e^{\frac{-iH^\dagger t}{\hbar}} \cdot e^{\frac{iH^\dagger t}{\hbar}} = e^N = I \tag{2.43}$$

la ecuación anterior coincide con la definición 2.8 por lo que concluimos que el operador $e^{\frac{-iHt}{\hbar}}$ es en efecto unitario. Es por ello que si $|\psi(0)\rangle$ es el estado del sistema en el tiempo t_0 y $|\psi(t)\rangle$ en el tiempo t se cumple

$$|\psi(t)\rangle = U|\psi(0)\rangle$$

es decir, que la evolución de un sistema cuántico cerrado (estrictamente aislado sin intercambio de energía con su medio ambiente) queda descrita por la acción de un operador unitario.

2.5 Arquitectura cuántica

En computación clásica la información puede ser procesada mediante las llamadas compuertas, puertas computacionales o puertas lógicas que implementan funciones, es decir, expresiones que contienen operaciones actuando sobre los posibles estados de un bit 0 ó 1. Debido a que el dominio de dichas funciones es el conjunto $\{0,1\}$, su comportamiento vendrá dado por la lógica binaria.

Álgebra de Boole. Lógica binaria

Definición 2.9. *Un álgebra de Boole es un conjunto $\mathfrak{B}$ provisto de tres operaciones:*

I *La suma definida de $\mathfrak{B}\times\mathfrak{B}$ en $\mathfrak{B}$, que denotaremos por $\oplus$:*

$$\forall (a,b) \in \mathfrak{B}\times\mathfrak{B},\ \exists! c \in \mathfrak{B} : c = a \oplus b$$

II *El producto definido de $\mathfrak{B}\times\mathfrak{B}$ en $\mathfrak{B}$, que denotaremos por $\odot$:*

$$\forall (a,b) \in \mathfrak{B}\times\mathfrak{B},\ \exists! c \in \mathfrak{B} : c = a \odot b$$

III *El complemento definido de $\mathfrak{B}$ en $\mathfrak{B}$, que denotaremos por $\sim$:*

$$\forall a \in \mathfrak{B},\ \exists! b \in \mathfrak{B} : b = \sim a$$

que satisfacen las siguientes propiedades:

(a) Asociatividad: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ *y* $(a \odot b) \odot c = a \odot (b \odot c)$

(b) Conmutatividad: $a \oplus b = b \oplus a$ *y* $a \odot b = b \odot a$

(c) *Existencia de elemento neutro:* $\exists \emptyset, U \in \mathfrak{B} : a \oplus \emptyset = a \quad y \quad \forall a \in \mathfrak{B}, a \odot U = a$

(d) *Existencia de complemento:* $\exists \sim a \in \mathfrak{B} : a \oplus \sim a = U \quad y \quad a \odot \sim a = \emptyset$

La lógica binaria es el caso particular de un álgebra de Boole en la que se considera $\mathfrak{B} = \{0, 1\}$, $U \equiv 1$ y $\emptyset \equiv 0$.

Un circuito cuántico constará de compuertas cuánticas, operadores que permiten manipular la información, transformando el estado de un qubit.

Dichos operadores evolución han de satisfacer la condición de normalización 2.11 lo que equivale a conservar la longitud del vector que representa cada ket en la esfera de Bloch. Es por ello por lo que consideraremos las compuertas cuánticas como operadores unitarios en su expresión matricial.

Compuertas de un qubit

Matrices de Pauli

Una compuerta con n entradas puede representarse con una matriz de grado 2^n.

Aunque, como hemos visto, cualquier matriz unitaria 2×2 representa una compuerta operando sobre un qubit; en computación clásica la única compuerta que permite un único bit de entrada es la puerta NOT que corresponde a la operación de complemento. Es decir, si el bit de entrada es 1, el de salida será 0 y viceversa.

Su equivalente en computación cuántica es la matriz X, que forma parte de las tres matrices de Pauli: X, Y, y Z que, junto con la matriz identidad, constituyen una base ortonormal del espacio de Hilbert.

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Su actuación sobre la base computacional clásica es la siguiente

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i|1\rangle \qquad Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0\rangle$$

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

Proposición 2.2. *Sea U un operador unitario y hermitiano e I el operador identidad entonces*

$$e^{-i\theta U} = cos(\theta)I - isen(\theta)U$$

Demostración:

Sea A un operador cualquiera, la exponenciación de la matriz que lo representa vendrá dada por

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + \frac{A}{1!} + \frac{A^2}{2!} + \cdots + \frac{A^n}{n!} + \cdots$$

En nuestro caso $A \equiv -i\theta U$ y como hemos visto en la propiedad 2 de los operadores unitarios $U^2 = I$, luego

$$\begin{aligned} e^{-i\theta U} &= I - i\theta U + (-i)^2\frac{(\theta U)^2}{2!} + (-i)^3\frac{(\theta U)^3}{3!} + (-i)^4\frac{(\theta U)^4}{4!} + (-i)^5\frac{(\theta U)^5}{5!} + (-i)^6\frac{(\theta U)^6}{6!} + \cdots \\ &= I - i\theta U - \frac{(\theta U)^2}{2!} + i\frac{(\theta U)^3}{3!} + \frac{(\theta U)^4}{4!} - i\frac{(\theta U)^5}{5!} - \frac{(\theta U)^6}{6!} + \cdots \\ &= I - \Big(\frac{(\theta U)^2}{2!} - \frac{(\theta U)^4}{4!} + \frac{(\theta U)^6}{6!} - \cdots\Big) - i\Big(\theta U - \frac{(\theta U)^3}{3!} + \frac{(\theta U)^5}{5!}\cdots\Big) \\ &= I\Big(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \cdots\Big) - iU\Big(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots\Big) \end{aligned} \tag{2.44}$$

Además el desarrollo en serie del seno y del coseno vienen dados por

$$sen(x) = \sum_{k=0}^{\infty}\frac{(-1)^k x^{2k+1}}{(2k+1)!} = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots$$
$$cos(x) = \sum_{k=0}^{\infty}\frac{(-1)^k x^{2k}}{(2k)!} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots$$

y sustituyendo en 2.44 obtenemos lo que se quería comprobar.

■

Dado que $X^2 = Y^2 = Z^2 = I$, si aplicamos la proposición anterior a las matrices de Pauli,

$$e^{\frac{-i\theta X}{2}} = cos(\theta/2)\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - isen(\theta/2)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}cos(\theta/2) & -isen(\theta/2)\\ -isen(\theta/2) & cos(\theta/2)\end{pmatrix} \equiv R_x(\theta)$$
$$e^{\frac{-i\theta Y}{2}} = cos(\theta/2)\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - isen(\theta/2)\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} = \begin{pmatrix}cos(\theta/2) & -sen(\theta/2)\\ sen(\theta/2) & cos(\theta/2)\end{pmatrix} \equiv R_y(\theta)$$
$$e^{\frac{-i\theta Z}{2}} = cos(\theta/2)\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - isen(\theta/2)\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}cos(\theta/2) - isen(\theta/2) & 0\\ 0 & cos(\theta/2) + isen(\theta/2)\end{pmatrix} \equiv R_z(\theta)$$

Por lo que partir de la exponenciación de las matrices X, Y y Z hemos obtenido los operadores $R_x(\theta)$, $R_y(\theta)$ y $R_z(\theta)$ que representan las rotaciones de ángulo θ en torno a los ejes x, y y z respectivamente.

La relevancia de las matrices de Pauli reside en que cualquier operador unitario actuando sobre un qubit, es decir, cualquier matriz 2×2 unitaria, puede ser expresado como producto de las anteriores rotaciones.

Teorema 2.3. *Sea U cualquier matriz unitaria de rango 2, existen a, b, c y d números reales tales que para cuales quiera dos ejes l y m no paralelos en la esfera de Bloch se verifica*

$$U = e^{ia}\, R_l(b)\, R_m(c)\, R_l(d) \tag{2.45}$$

Demostración:

Nos restringiremos al caso $l \equiv z$ y $m \equiv y$. Considerando entonces

$$R_z(b) = \begin{pmatrix}e^{-\frac{ib}{2}} & 0\\ 0 & e^{\frac{ib}{2}}\end{pmatrix}, \quad R_y(c) = \begin{pmatrix}cos(c/2) & -sen(c/2)\\ sen(c/2) & cos(c/2)\end{pmatrix}, \quad R_z(d) = \begin{pmatrix}e^{-\frac{id}{2}} & 0\\ 0 & e^{\frac{id}{2}}\end{pmatrix}$$

y aplicando a la ecuación (2.45) dada en el teorema

$$e^{ia}\cdot\begin{pmatrix} e^{-\frac{ib}{2}}cos(c/2) & -e^{-\frac{ib}{2}}sen(c/2)\\ e^{-\frac{ib}{2}}sen(c/2) & e^{-\frac{ib}{2}}cos(c/2)\end{pmatrix}\begin{pmatrix} e^{-\frac{id}{2}} & 0\\ 0 & e^{\frac{id}{2}}\end{pmatrix} = e^{ia}\cdot\begin{pmatrix} e^{-\frac{id}{2}}\left[e^{-\frac{ib}{2}}cos(c/2)\right] & e^{\frac{id}{2}}\left[-e^{-\frac{ib}{2}}sen(c/2)\right]\\ e^{-\frac{id}{2}}\left[e^{-\frac{ib}{2}}sen(c/2)\right] & e^{\frac{id}{2}}\left[e^{-\frac{ib}{2}}cos(c/2)\right]\end{pmatrix} =$$

$$e^{ia}\cdot\begin{pmatrix} e^{\frac{-i}{2}(d+b)}cos(c/2) & -e^{\frac{-i}{2}(b-d)}sen(c/2)\\ e^{\frac{-i}{2}(d-b)}sen(c/2) & e^{\frac{i}{2}(d+b)}cos(c/2)\end{pmatrix} = \begin{pmatrix} e^{\frac{i}{2}(a-d-b)}cos(c/2) & -e^{\frac{i}{2}(a+d-b)}sen(c/2)\\ e^{\frac{i}{2}(a-d+b)}sen(c/2) & e^{\frac{i}{2}(a+d+b)}cos(c/2)\end{pmatrix} \equiv U$$

Para facilitar los cálculos, sean $\alpha = \frac{a-d-b}{2}$, $\beta = \frac{a+d-b}{2}$, $\gamma = \frac{a-d+b}{2}$ y $\delta = \frac{a+d+b}{2}$, de lo anterior,

$$\begin{aligned} U\cdot U^{\dagger} &= \begin{pmatrix} e^{i\alpha}cos(c/2) & -e^{i\beta}sen(c/2)\\ e^{i\gamma}sen(c/2) & e^{i\delta}cos(c/2)\end{pmatrix}\begin{pmatrix} e^{-i\alpha}cos(c/2) & e^{-i\gamma}sen(c/2)\\ -e^{-i\beta}sen(c/2) & e^{-i\delta}cos(c/2)\end{pmatrix}\\ &= \begin{pmatrix} cos^2(c/2)+sen^2(c/2) & \left[e^{i(\alpha-\gamma)}-e^{i(\beta-\delta)}\right]cos(c/2)\cdot sen(c/2)\\ \left[e^{i(\gamma-\alpha)}-e^{i(\delta-\beta)}\right]cos(c/2)\cdot sen(c/2) & cos^2(c/2)+sen^2(c/2)\end{pmatrix}\end{aligned}$$

Nótese que $e^{i(\alpha-\gamma)} = e^{-ib} = e^{i(\beta-\delta)}$ y $e^{i(\gamma-\alpha)} = e^{ib} = e^{i(\delta-\beta)}$, por lo que sustituyendo en la expresión anterior resulta $U\cdot U^{\dagger} = \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix} \equiv I$, con lo que U es un operador unitario.

■

Puertas cambio de fase y Hadamard

Otra matriz de especial importancia es la matriz cambio de fase que representaremos con la letra P.

$$P \equiv \begin{pmatrix} 1 & 0\\ 0 & e^{i\theta}\end{pmatrix} \tag{2.46}$$

Como vimos en la sección 2.2, un qubit $|\psi\rangle$ en el estado $\alpha|0\rangle + \beta|1\rangle$ puede verse como un punto de coordenadas (θ,ϕ) en la esfera de Bloch siendo $\alpha = cos(\theta/2)$ y $\beta = e^{i\phi}sen(\theta/2)$. Por lo tanto,

$$P|\psi\rangle = \begin{pmatrix} 1 & 0\\ 0 & e^{i\theta}\end{pmatrix}\begin{pmatrix} \alpha\\ e^{i\phi}\beta\end{pmatrix} = \begin{pmatrix} \alpha\\ e^{i(\theta+\phi)}\beta\end{pmatrix}$$

modificándose de esta forma la fase relativa $e^{i\phi}$ del qubit de entrada.

Además $e^{i\pi} = cos(\pi) + isen(\pi) = -1$, luego la matriz de Pauli Z, no es más que la matriz de cambio de fase con $\theta = \pi$. Si consideramos $\theta = \pi/2$ y $\theta = \pi/4$ obtenemos las matrices S y T. A la compuerta que representa esta última se la conoce históricamente como *puerta* $\pi/8$, pues como vemos, salvo una fase global, es igual a la matriz en la que aparece $e^{\pm i\pi/8}$ en su diagonal principal.

$$S \equiv \begin{pmatrix} 1 & 0\\ 0 & e^{i\pi/2}\end{pmatrix} = \begin{pmatrix} 1 & 0\\ 0 & i\end{pmatrix} \qquad\qquad T \equiv e^{i\pi/8}\begin{pmatrix} e^{-i\pi/8} & 0\\ 0 & e^{-i\pi/8}\end{pmatrix} = \begin{pmatrix} 1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$$

Obviamente se verifica la relación $T^2 = S$, pues la matriz T se corresponde a una rotación de 45° y al aplicarla dos veces equivale a una de 90°.

Aunque es aplicable a sistemas de más de un qubit, presentamos en esta sección la compuerta de Hadamard, que denotaremos con la letra H.

$$H \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.47}$$

Es de gran importancia en computación cuántica, pues permite transformar el estado de un qubit en superposicón de estados.

Recordemos que ya en la sección 2.2 presentábamos la base $\{|+\rangle, |-\rangle\}$, donde $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ y $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$ que es conocida como base de Hadamard, pues se origina por aplicación de la matriz de Hadamard a los estados de la base clásica $\{|0\rangle, |1\rangle\}$

$$H|0\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$$

$$H|1\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

El teorema 2.3 concede a la computación de lo que se denomina universalidad, es decir, cualquier compuerta cuántica para 1 qubit puede ser representada mediante la combinación de las matrices R_x, R_y y R_z. También el conjunto $G = \{HTHT, THTH\}$ y $\{H, T\}$ son conjuntos de puertas universales.

Sin embargo, para poder generalizar este hecho a varios qubits, es preciso la definición de otras compuertas cuánticas.

Compuertas de 2 qubits

Como decíamos en la seccion 2.3, el conjunto $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ es la base en la notación de Dirac del espacio cuántico $\mathcal{H} \otimes \mathcal{H}$ por lo que, dado que es un espacio 4-dimensional, los operadores unitarios que actúan sobre sistemas compuestos de dos qubits serán matrices 4×4.

Compuerta Hadamard

Comenzaremos aplicando la puerta de Hadamard que hemos visto para qubits individuales ambos en el estado $|0\rangle$ a dos qubits de forma

$$(H \otimes H)(|0\rangle \otimes |0\rangle) = H|0\rangle \otimes H|0\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

La generalización a n qubits produce una salida que es la superposición ponderada de los estados $i = 1, \ldots, n$ que forman la base de sistema compuesto, es decir,

$$H|0\rangle \overset{n}{\otimes \cdots \otimes} H|0\rangle = \frac{1}{\sqrt{2}}\Big((|0\rangle + |1\rangle) \overset{n}{\otimes \cdots \otimes} (|0\rangle + |1\rangle)\Big) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2n-1} |i\rangle$$

Puertas CNOT y U-controladas

Una de las compuertas fundamentales para sistemas de 2 qubits es la compuerta NOT controlada o CNOT (controlled not). La entrada para este operador será de dos qubits, el de salida u *objetivo* que notaremos t sobre el cuál se aplicara la matriz NOT sólo en caso de que el qubit *de control*, c sea $|1\rangle$, si este es $|0\rangle$, el qubit objetivo conservará su estado inicial.

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle \qquad |10\rangle \to |11\rangle \qquad |11\rangle \to |10\rangle \tag{2.48}$$

Si consideramos $|ct\rangle$ como el estado de ambos qubits a la entrada y $\oplus$ la suma módulo 2, la representación genérica del operador $CNOT$ vendrá dada como

$$CNOT(|c,t\rangle) = |c, c \oplus t\rangle \qquad c,t \in \{0,1\}$$

De las ecuaciones de (2.48) obtengamos la representación matricial de esta compuerta.

$$\begin{aligned} CNOT &\equiv |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \\ &= \begin{pmatrix}1\\0\\0\\0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix} + \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix} + \begin{pmatrix}0\\0\\1\\0\end{pmatrix}\begin{pmatrix}0 & 0 & 0 & 1\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\begin{pmatrix}0 & 0 & 1 & 0\end{pmatrix} \\ &= \begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} + \begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} + \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&0&0\end{pmatrix} + \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \end{aligned}$$

La matriz anterior la podemos expresar como suma

$$\begin{aligned} CNOT \equiv \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} &= \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} + \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \\ &= \begin{pmatrix}1&0\\0&0\end{pmatrix} \otimes \begin{pmatrix}1&0\\0&1\end{pmatrix} + \begin{pmatrix}0&0\\0&1\end{pmatrix} \otimes \begin{pmatrix}0&1\\1&0\end{pmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \end{aligned}$$

Donde I denota la matriz identidad de orden 2 y X es la compuerta NOT presentada anteriormente que actúa sobre 2 qubits. Por lo tanto es posible construir cualquier compuerta controlada de la forma $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$, siendo U es el operador unitario que actuará sobre el qubit objetivo si y sólo si el estado del qubit de entrada del qubit de control es 1.

Puerta SWAP

Si aplicamos el operador CNOT intercambiando en cada una de las sucesivas aplicaciones el qubit de control con el objetivo, obtenemos el intercambio de los valores de dichos qubits, es decir,

$$\begin{aligned} |a,b\rangle &\to |a, a \oplus b\rangle \\ &\to |a \oplus b, a \oplus (a \oplus b)\rangle = |a \oplus b, b\rangle \\ &\to |b, (a \oplus b) \oplus b\rangle = |b, a\rangle \end{aligned}$$

En particular,

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |10\rangle \qquad |10\rangle \to |01\rangle \qquad |11\rangle \to |11\rangle$$

Esta compuerta se denomina SWAP (del inglés "intercambiar") y su representación matricial donde cada columna es el vector de salida correspondiente

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

Podemos concluir que el conjunto de las puertas de Hadamard, S, T y CNOT permite construir cualquier circuito que opere sobre un sistema compuesto por n qubits. Esto se debe a que cualquier circuito puede ser expresado en función de operadores unitarios y dicho conjunto de operadores permite implementar cualquiera de estos operadores. En otras palabras el conjunto es universal.

3

Criptografía cuántica

3.1 Introducción. Criptografía clásica

La criptografía como su nombre indica significa "escritura oculta" y tiene entre sus objetivos el de la confidencialidad, es decir, presentar la información de forma que sea ininteligible para cualquier entidad no autorizada a conocerla.

Para ello se emplea un criptosistema que es una séxtupla (m, c, k, k', E, D) que combina el mensaje o mensajes que se desea codificar o proteger m, con una clave o conjunto de claves k, mediante una aplicación, $E : m \times k \to c$ algoritmo de encriptado, generando una mensaje cifrado c. k' es el conjunto de claves que permiten recuperar la información original y $D : c \times k' \to m$ es una aplicación denominada algoritmo de desencriptado o descifrado y que permite, dado un mensaje cifrado, por medio de la clave adecuada, obtener la información originalmente protegida mediante E.

Antes de abordar la criptografía desde el punto de vista de la teoría cuántica, veamos a modo de introducción una clasificación y algunos ejemplos de los métodos clásicos más usuales.

Simétrica o de clave privada

Los cifrados simétricos requieren del uso de una única clave que servirá tanto en la encriptación como en la desencriptación del mensaje. Es decir, $k = k'$.

El más conocido es *el cifrado de Vernam* ya que fue inventado por Gilbert Vernam, ingeniero de ATT (American Telephone and Telegraph) en 1918 publicándose en 1926.

Cifrado de Vernam

Si queremos enviar un mensaje, texto en claro, m que será un código binario de ceros y unos a un receptor, generamos una clave aleatoria k también binaria de forma que el mensaje cifrado c vendrá dado por $c = m \oplus k$, donde $\oplus$ es la suma módulo 2. El receptor realiza la operación $c \oplus k$ obteniendo m.

Ejemplo 3.1.1. Deseamos cifrar el texto $m \equiv QUBIT$ y nuestra clave es $k \equiv MATHS$. A cada letra (prescindiremos de la ñ) le hacemos corresponder un número comenzando por el 1 y lo expresamos en binario $A \equiv 1 \equiv_2 00001, B \equiv 2 \equiv_2 00010, \ldots, Z \equiv 26 \equiv_2 11010$. Representamos el proceso:

Encriptación					
Mensaje m	Q	U	B	I	T
$m\,(mod\,2)$	10001	10101	00010	01001	10100
Clave k	M	A	T	H	S
$k\,(mod\,2)$	01101	00001	10100	01000	10011
$c\,(mod\,2)$	11100	10100	10110	00001	00111

Desencriptación					
$c\,(mod 2)$	11100	10100	10110	00001	00111
Clave k	M	A	T	H	S
$k\,(mod 2)$	01101	00001	10100	01000	10011
$c \oplus k = m$	10001	10101	00010	01001	10100
Mensaje m	Q	U	B	I	T

Este tipo de cifrado es el único que se ha probado [19] que es totalmente seguro siempre que la clave sea al menos tan larga que el mensaje, aleatoria y de un sólo uso (de ahí que también se le conozca como *libreta de un solo uso*). Estas características hacen que su implementación sea costosa ya que requiere generar grandes secuencias de números aleatorios que además han de ser diferentes para cada mensaje y transmitidas mediante un canal seguro.

Estándar de encriptación

En 1997, la entidad estadounidense *NIST* (*National Institute of Standards and Technology*), llevó a cabo un proceso abierto de selección para sustituir el entonces método estándar de encriptación de datos *DES* por el nuevo *AES* (*Advanced Encryption Standard*).

El algoritmo ganador fue *Rijndael* [3], creado por Vincent Rijmen y Joan Daemen, matemático e ingeniero eléctronico respectivamente de la Universidad Católica de Lovaina. Actualmente es el método más utilizado en el mundo por administraciones, bancos e industria pues no se conoce hasta el momento ningún ataque convencional ponga en peligro su uso.

El algoritmo se basa en sustituciones, permutaciones y transformaciones lineales, que se repiten un número determinado de veces, llamadas rondas, según la longitud de la clave y que son realizadas sobre matrices de 4×4 bytes. En una primera etapa (*AddRoundKey)* se genera una clave de cifrado y a partir de ella se calcula para cada ronda una clave. Cada ronda tiene cuatro fases excepto la última en la que se prescinde de la tercera. Las fases son:

- *SubBytes*: cada byte del bloque inicial es reeemplazado con otro mediante transformaciones no lineales según una tabla de búsqueda preestablecida.
- *ShiftRows*: los bytes en cada fila son rotados de forma cíclica.
- *MixColumns*: cada columna es multiplicada por un polinomio.
- *AddRoundKey*: cada byte del bloque se combina con la clave correspondiente a esta ronda que se ha generado en la primera etapa.

Asimétrica o de clave pública

Como hemos visto, los sistema simétricos presentan lo que conocemos como *problema de distribución de clave* pues son seguros actualmente si, entre otros requisitos, se garantiza la distribución secreta de una clave, en otras palabras, conocer el algoritmo empleado para generar dicha clave no amenaza la privacidad del mensaje cifrado.

La solución a este problema viene de la mano de la criptografía asimétrica introducida en 1976 por Whitfield Diffie y Martin Hellman [6]. En su artículo proponen el siguiente método que emplea dos claves diferentes una privada y otra que se hace pública, sin comprometer la seguridad de la primera y por tanto el protocolo permite acordar una clave común mediante un canal no necesariamente seguro.

Dos usuarios se ponen de acuerdo en un primo p considerando el grupo multiplicativo $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p : \exists b \in \mathbb{Z}_p, ab = 1\}$ y un g generador de $\mathbb{Z}_p^*$ cuyas potencias originan dicho grupo multiplicativo siendo p y g públicos. Ambos seleccionan respectivamente dos enteros x e y, los cuales mantienen en secreto, e intercambian los valores g^x y g^y en $\mathbb{Z}_p$. Las claves públicas serán (g, p, g^x) y (g, p, g^y). A continuación, usando las claves privadas x e y calculan el valor o clave común $(g^x)^y = (g^y)^x \in \mathbb{Z}_p$.

Este protocolo basa su seguridad en la dificultad de resolver lo que se conoce como logaritmo discreto, es decir, dados p, g y x es sencillo calcular g^x, sin embargo no lo es encontrar el valor x dado g^x.

Algoritmo RSA

El algoritmo RSA [18] fue inventado por Rivest, Shamir y Adleman y es el primer algoritmo de tipo asimétrico o clave pública que se introdujo. Supongamos que A quiere enviar un mensaje M a B. Entonces se lleva a cabo el siguiente proceso:

- Generación de claves: Sea la función de Euler $\varphi(n) = |\{q \in \mathbb{Z}^+ : q < n, (q, n) = 1\}|$ que representa el cardinal del conjunto de todos los enteros menores y coprimos con n, B escoge p y q primos y calcula $\varphi(n) = (p-1)(q-1)$ por las propiedades de dicha función. Considerando e tal que $(e, \varphi(n)) = 1$, la clave pública será el par (n, e) donde n es la base y e el exponente de cifrado, y sea d tal que $e \cdot d = 1 (mod\, n)$, (n, d) es la clave privada.

- Cifrado: B comunica a A su clave pública y guarda en secreto la clave privada. A divide el mensaje M en bloques m de un tamaño menor que n y calcula el mensaje cifrado como $c = m^e (mod\, n)$.

- Descifrado: B recibe c de A y calcula m como $m = c^d (mod\, n)$. Esto es posible ya que $c^d = (m^e)^d = m^{ed} = m (mod\, n)$.

La seguridad que ofrece se debe a que a día de hoy no se conoce ningún algoritmo capaz de factorizar un número entero que sea producto de dos primos lo suficientemente grandes. Por lo tanto la velocidad del progreso tecnológico pone en peligro este sistema.

ElGamal y curvas elípticas

El algoritmo de ElGamal [7] fue introducido por Taher ElGamal. En su origen, fue ideado para el caso del grupo multiplicativo $\mathbb{Z}_p^*$, con p un número primo, aunque posteriormente se comprobó su utilidad para cualquier grupo cíclico $G = \{1, g, g^2, \ldots, g^{n-1}\}$, por lo que al igual que la idea de Diffie y Hellman, se basa en la dificultad de cálculo de k logaritmo discreto en base g de a siendo $a = g^k$ cualquier elemento del grupo G. Si suponemos que A quiere enviar un mensaje a B el algoritmo en general es el siguiente:

- Generación de claves: Se toma un entero positivo a, tal que $1 < a < n$ y se calcula $g^a \in G$. La clave pública la constituye la terna (G, g, g^a), mientras que la clave privada es a.

- Encriptación: B cifra un mensaje m para A. Toma un k $1 < k < n$ y calcula $h = g^k (mod\, n)$ y $\alpha = m\dot{(}g^a)^k$. El mensaje cifrado es la tupla $c = (h, \alpha)$.

- Desencriptación: A descifra el mensaje usando su clave privada a, pues $h^{-a} \cdot \alpha (mod\, p) = (g^k)^{-a} \cdot m \cdot g^{ak} (mod\, p) = m (mod\, p)$

Posteriormente, Victor Miller [16] y Neil Koblitz [13] sugirieron como apropiado el grupo de puntos de una curva elíptica como base para el criptosistema de ElGamal, en lo que hoy conocemos como criptografía con curvas elípticas (*ECC*), del inglés, *Elliptic Curve Cryptography*.

Esta idea proviene del hecho de que es posible sumar dos puntos de una curva elíptica obteniendo como resultado otro punto de la curva. Es decir, cada línea que la corta en dos puntos, la corta además exactamente en un tercero. La seguridad de este criptosistema se basa en la complejidad de resolver el logaritmo elíptico, es decir si E es una curva elíptica, dado un punto $Q = n \cdot P$, $\forall n \in \mathbb{N}$ en ella, obtener el punto P.

3.2 Distribución de clave cuántica.

Los principios por los que se rige la física cuántica hacen posible el desarrollo de nuevos métodos que garanticen la seguridad en la transmisión de información, utilizando la mecánica cuántica en lugar de algoritmos númericos tradicionales para distribuir la clave privada, por lo que solemos referirnos a ellos genericamente como métodos cuánticos de distribución de clave o *QKD*, del inglés, *Quantum Key Distribution*.

De forma general, en la implementación de QKD se utilizan dos canales mediante los cuales los usuarios se transmiten la información: un canal clásico de comunicación como puede ser Internet o una línea telefónica y uno cuántico un cable de fibra óptica si dicha informacion se transmite en forma de fotones polarizados. Es importante señalar que, dado que la verificación de la clave y de no existencia de perturbaciones ya sea por errores en el canal o presencia de espías tiene lugar después del intercambio inicial, los datos confidenciales no viajan directamente a través del canal cuántico sino que se usa para intercambiar información que carece de relevancia con la única finalidad de garantizar la seguridad en la comunicación.

Como ya introdujimos al hablar de la medición en un sistema cuántico, cualquier objeto cuántico al ser observado modifica su estado de forma inevitable. Este es el principio en el que se basa la QKD, de forma que si la información ha sido interceptada por un posible espía se modificará y posteriormente, mediante el uso de un canal clásico, los usuarios percibirán dichas incongruencias en la transmision mediante el canal cuántico. Si por el contrario se valida la seguridad y privacidad de la comunicación, la clave es segura y se puede usar para encriptar o cifrar datos.

No clonación

La información clásica se codifica mediante bits que como hemos visto pueden tomar los valores 0 ó 1. El hecho de un qubit pueda encontrarse en lo que definíamos en la sección 2.2 como superposición de estados es lo que, en oposición a lo que ocurre con la información clásica, hace que resulte imposible copiar qubits. Este hecho fue descubierto en 1982 por Wootters y Zurek y es lo que conocemos como el teorema de no clonación que se deriva directamente de que las transformaciones en un sistema cuántico son unitarias.

Teorema 3.1 (Teorema de no clonación)**.** *Sean $\mathcal{H}_A$ y $\mathcal{H}_B$ los espacios de estados de dos sistemas cuánticos A y B, no existe un operador unitario U tal que cualquier $|\psi\rangle$ estado inicial del sistema A pueda ser copiado en el sistema B con estado inicial $|\phi\rangle$.*

Demostración:

Si consideramos el sistema compuesto $\mathcal{H}_A \otimes \mathcal{H}_B$, el estado inicial de dicho sistema será $|\psi\rangle \otimes |\phi\rangle$.

Supongamos existe U operador unitario tal que para cualesquiera $|\psi\rangle$ y $|\varphi\rangle$, dos estados iniciales distintos de $\mathcal{H}_A$

$$U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |\phi\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Si efectuamos el producto interno de los miembros a ambos lados de las anteriores ecuaciones

$$\begin{aligned}(\langle\phi| \otimes \langle\varphi|)\, U^\dagger U\, (|\psi\rangle \otimes |\phi\rangle) = \langle\varphi| \otimes \langle\varphi||\psi\rangle \otimes |\psi\rangle \Rightarrow \\ \langle\phi| \otimes \langle\varphi||\psi\rangle \otimes |\phi\rangle = \langle\varphi|\psi\rangle \otimes \langle\varphi|\psi\rangle \Rightarrow \\ \langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2 \end{aligned} \tag{3.1}$$

donde hemos aplicado que $UU^\dagger = 1$ por ser U unitario, la propiedad distributiva del producto tensor y que el estado $|\phi\rangle$ está normalizado.

Nótese que la última igualdad (3.1) será cierta si $\langle\varphi|\psi\rangle \in \{0, 1\}$. Si $\langle\varphi|\psi\rangle = 1$ entonces $|\psi\rangle = |\varphi\rangle$ pero hemos supuesto que son estados diferentes. Si $\langle\varphi|\psi\rangle = 0$ entonces ambos estados son ortogonales en contra de la arbitrariedad de la elección de ambos. ■

BB84

Dado que hemos probado que para que sea posible clonar estados en un sistema cuántico estos han de ser ortogonales, resulta imposible hacerlo para estados desconocidos. Este hecho junto con la perturbación que sufre un sistema cuántico al ser observado, permitió a Charles Bennett de la compañía IBM y a Gilles Brassad, profesor en la Universidad de Montreal desarrollar en 1984 el primer protocolo de criptografía cuántica o *QKD* que hoy en día conocemos como *BB84* [2] por las iniciales de sus creadores y el año de publicación.

Debido a que un fotón puede verse como un qubit, ya que es el estado de un sistema cuántico representado por un vector espacio de Hilbert bidimensional; emisor y

receptor intercambiarán, a través de un sistema cuántico, fotones individuales cuyos estados polarizados sirven para codificar los valores de un bit.

Consideremos como bases de dicho espacio de Hilbert $\mathcal{H}$ las ya estudiadas en la sección 2.2: $\oplus \equiv \{|0\rangle, |1\rangle\}$ que se identifica con la polarización horizontal (0 °) y vertical (90 °) respectivamente y $\otimes \equiv \{|+\rangle, |-\rangle\}$ correspondiente a las polarizaciones diagonales (±45°). Nótese que dado que $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ y $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, los 4 estados correspondientes a ambas bases no son mutuamente ortogonales lo que mantiene la validez del teorema 3.1.

Supongamos que se desea establecer un canal seguro de comunicación usando el protocolo *BB84* entre un emisor y un receptora los que llamaremos Alice y Bob. Veamos cuáles serán los pasos a seguir:

1º Alice envía a través del canal cuántico una serie de bits en forma de fotones polarizados eligiendo aleatoriamente una de las bases anteriores de forma que por convenio el bit 0 se corresponderá con los estados $|0\rangle$ y $|+\rangle$ y el bit 1 con $|1\rangle$ y $|-\rangle$.

2º Bob selecciona de forma aleatoria una de las bases $\otimes$ o $\oplus$ en las cuáles medirá cada uno de los fotones que viajan a través del canal. La secuencia obtenida por Bob es lo que conocemos como clave en bruto.

3º Utilizando el canal clásico, Alice le comunica a Bob cuáles han sido las bases en las que ha polarizado los fotones enviados y Bob por su parte las utilizadas en la observación de cada qubit.

4º Si Bob ha medido en la base contraria a la de Alice, dicho fotón colapsará tomando el estado 0 ó 1 con igual probabilidad por lo que esta información puede coincidir o no con la polarización de Alice. Por ello Alice y Bob sólo conservarán los fotones en los cuales la base usada por Bob para medirlo coincida con la de Alice. Los bits correspondientes constituyen la clave pulida o privada.

Ejemplo 3.2.1. Supongamos que Alice envía el fotón $|+\rangle$ cuya polarización vendrá representada por el bit 0. Si Bob escoge la misma base $\otimes$, es decir, proyecta sobre el subespacio generado por $\{|+\rangle, |-\rangle\}$, aplica el operador de Hadamard

$$H(0) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

obteniendo como resultado el mismo fotón enviado por Alice.

Si consideramos que Alice envía $|1\rangle$ y Bob emplea esta misma base, aplica entonces la matriz identidad

$$I(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle$$

Sin embargo, si Bob emplea la base $\otimes$ obtendrá $H(1) = |+\rangle$ obteniendo un valor de 0 al contrario del bit enviado por Alice pero también puede obtener $H(1) = |-\rangle$ coincidiendo así el valor del bit, que es 1, pero no el estado de la polarización del fotón por ser distintas las bases.

Resumamos el intercambio de una cadena de 8 fotones constituida por los 4 anteriores y otros que añadimos.

Bit enviado por Alice	0	1	1	1	1	0	0	1
Base usada por Alice	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$
Qubit enviado	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Base usada por Bob	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$
Qubit obtenido	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$
Bit recibido por Bob	0	1	0	1	0	0	0	1
¿Coinciden las bases?	Sí	Sí	No	No	No	Sí	No	Sí
Bit compartido	0	1				0		1

Espionaje

En el caso del intercambio de Diffie y Hellman definido en la sección de criptografía con clave pública, supongamos que existe un espía, Eve, que interviene de forma activa del siguiente modo.

Una vez que Alice y Bob intercambian g^x y g^y respectivamente, Eve, toma su propio valor z, intercepta ambos valores y calcula $(g^x)^z$ y $(g^y)^z$. Además envía a Alice y a Bob el valor g^z por lo que calculan respectivamente $(g^z)^x$ y $(g^z)^y$. De este modo, Alice y Bob creen compartir una clave secreta de comunicación, mientras que lo que en realidad ocurre es que Eve comparte una clave con Alice y otra con Bob. Así Eve podrá leer cualquier comunicación, que Alice y Bob piensan que es secreta entre ambos y, posteriormente, una vez leída, reenviarla usando la clave correspondiente.

Este ataque, conocido comunmente como “Man-in-the-middle", en el caso del protocolo BB84 no puede llevarse a cabo sin que Alice y Bob detecten la existencia de Eve.

Una vez Alice y Bob han obtenido la clave privada, escogerán la mitad de los bits de dicha clave y establecerán una cantidad a partir de la cual, si al revelarlos mediante el canal público sus valores no coinciden, abortan el intercambio. En el caso en que coincidan estas comparaciones, tras desechar los valores que han hecho públicos, la clave secreta estaría constituida por la cuarta parte de los bits iniciales enviados por Alice.

Para Eve la única forma de obtener la información que Alice envía a Bob será interceptar el qubit enviado ya que de lo contrario, Bob no recibiría ningún envío de Alice y cancelarían la comunicación. Por el teorema de no clonación, Eve no podrá copiar el qubit de Alice para enviarlo a Bob y tampoco podrá medirlo en cualquier base sin modificar su estado. Por ello la única alternativa es elegir aletoriamente una de las dos bases de forma que coincida con la base utiliza por Alice.

En el segundo caso del ejemplo anterior, si Eve, antes de que Bob mida el fotón enviado por Alice, escoge la base $\otimes$, obtiene $|+\rangle$ o $|-\rangle$ y dado que la base elegida por Bob es $\oplus$ este puede medir $|1\rangle$, en cuyo caso coincide con el bit inicial enviado por Alice, o $|0\rangle$ con lo que al comparar Alice el bit enviado 1 con el recibido por Bob 0, ambos no coincidirían aunque sus bases hayan sido las mismas por lo que detectarían pertubaciones en la comunicación. Si suponemos la presencia de Eve en el intercambio de 8 bits anterior entonces,

Bit enviado por Alice	0	1	1	1	1	0	0	1
Base usada por Alice	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$
Qubit enviado	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Base usada por Eve	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Qubit enviado	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$
Base usada por Bob	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$
Qubit obtenido	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$
Bit recibido por Bob	0	0	0	1	0	0	0	1
¿Coinciden las bases?	Sí	Sí	No	No	No	Sí	No	Sí
¿Bit revelado?	No	Sí				Sí		No

Donde de los 4 bits (primero, segundo, sexto y octavo) compartidos en la clave privada, Alice y Bob publican los valores del segundo y del sexto detectando la presencia de Eve o ruidos en la comunicación por lo que desechan la validez de la clave que constituyen los bits primero y octavo.

Aunque por lo expuesto en esta sección podríamos pensar que el protocolo BB84 ofrece una solución definitiva al problema de la distribución de clave, esto no es así dado que en dicho protocolo se lleva a cabo una discusión sobre las bases utilizadas a través del canal de comunicación clásico y un impostor podría hacer creer a estos comunicantes que no ha habido interferencias mediante un ataque *Man-in-the-middle*.

Este problema se resolvería añadiendo información a la discusión de las bases para certificar la procedencia lícita pero en un futuro es de esperar el desarrollo de ordenadores cuánticos capaces de atacar esta información cifrada por métodos tradicionales.

3.3 Algoritmos cuánticos

Uno de los principales motivos para trabajar en el desarrollo de la información y computación cuántica es la posibilidad que ofrece de simular y resolver problemas más rápidamente que los ordenadores clásicos. Para ello se sirve de algoritmos, secuencias de transformaciones u operadores que llevan a cabo medidas de un sistema cuántico usando las propiedades de interferencia y paralelismo cuánticos que introduciremos mediante el algoritmo de Deutsch.

Algoritmo de Deutsch

En 1985, David Deutsch desarrolló el primer algoritmo cuántico [5] que, aunque no tiene amplias aplicaciones prácticas, supuso el primer ejemplo de la mejora exponencial en la resolución de problemas clásicos mediante computación cuántica.

El propósito del algoritmo es determinar si una función de un qubit $f : \{0,1\} \to \{0,1\}$ es constante (f_0 y f_1), es la función identidad (f_x) o es la función complemento ($f_{\overline{x}}$).

x	f_0	f_1	f_x	$f_{\overline{x}}$
0	0	1	0	1
1	0	1	1	0

Las funciones cambio de estado y la funcion identidad se denominan balanceadas porque la salida puede tomar los valores 0 ó 1 con igual probabilidad.

El problema por tanto sería evaluar $f(0) \oplus f(1)$. Si el resultado es 0 entonces $f(0) = f(1)$ con lo que f es la función constante y si el resultado es 1 entonces $f(0) \neq f(1)$ y f es balanceada. En el caso de hacerlo de forma tradicional, obviamente necesitaremos al menos dos aplicaciones de la función f sin embargo este algoritmo permite hacerlo evaluando $f(x)$ para varios valores de x simultáneamente. Esta propiedad es lo que conocemos como paralelismo cuántico.

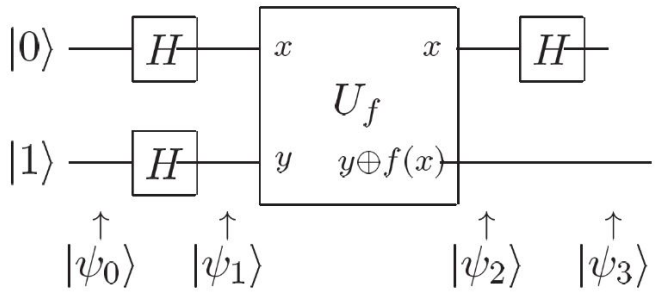
Sea la transformación unitaria para dos qubits $|x\rangle, |y\rangle$ definida como

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle \tag{3.2}$$

Si $|y\rangle = |0\rangle$, el resultado será $f(x)$. Para la aplicación del paralelismo cuántico consideramos el qubit en superposición de estados mediante la implementación de la compuerta de Hadamard, si $|y\rangle = 1$, $H|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ y aplicando U_f

$$\begin{aligned} U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= U_f\left(\left(\frac{|x\rangle|0\rangle}{\sqrt{2}}\right) - \left(\frac{|x\rangle|1\rangle}{\sqrt{2}}\right)\right) = \frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}} \\ &= |x\rangle\left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) = |x\rangle(-1)^{f(x)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned} \tag{3.3}$$

donde para obtener la última igualdad si $f(x) = 0$ entonces $|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$, si $f(x) = 1$ se obtendría $|x\rangle\left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right) = -|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$. Veamos el circuito que implementa el algoritmo de Deutsch



donde $|\psi_1\rangle = H(|\psi_0\rangle) = H|01\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{|0\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{|1\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$ por aplicación de la compuerta de Hadamard a las entradas $|\psi_0\rangle = |0\rangle$ y $|\psi_0\rangle = |1\rangle$ respectivamente. Empleando U_f

$$\begin{aligned} |\psi_2\rangle = U_f(|\psi_1\rangle) &= U_f\left(\frac{|0\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) + U_f\left(\frac{|1\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= \frac{(-1)^{f(0)}|0\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{(-1)^{f(1)}|1\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \\ &= (-1)^{f(0)}\left(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned} \tag{3.4}$$

Nótese para la obtención de la última igualdad

$$(-1)^{f(0)} \cdot \left((-1)^{f(0)\oplus f(1)}\right) = (-1)^{f(0)} \cdot (-1)^{f(0)} \cdot (-1)^{f(1)} \tag{3.5}$$

Si $f(0) = 1$ la expresión (3.5) quedaría como $(-1) \cdot (-1) \cdot (-1)^{f(1)} = (-1)^{f(1)}$ y si $f(0) = 0$, $1 \cdot 1 \cdot (-1)^{f(1)} = (-1)^{f(1)}$

En (3.4), como introducíamos:

- Si f es función constante $f(0) = f(1) \Rightarrow f(0) \oplus f(1) = 0$ luego

$$|\psi_2\rangle = (-1)^{f(0)} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$
$$\Rightarrow |\psi_3\rangle = (-1)^{f(0)} H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(0)}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Si f es balanceada $f(0) \neq f(1) \Rightarrow f(0) \oplus f(1) = 1$ y

$$|\psi_2\rangle = (-1)^{f(0)} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$
$$\Rightarrow |\psi_3\rangle = (-1)^{f(0)} H\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(0)}|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Para la obtención de $|\psi_3\rangle$, aplicar la compuerta de Hadamard al primer qubit no es más que el cálculo de la interferencia respecto a dicho qubit; matemáticamente la suma de las amplitudes de probabilidad.

En el caso de f constante, $H\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = |0\rangle$ decimos que la interferencia es positiva respecto al estado $|0\rangle$ y negativa respecto de $|1\rangle$ pues las amplitudes iniciales se suman (1/2 para el estado 0 y 1) y la amplitud final 1 pasa a ser la del estado 0 lo que significa que estamos seguros de encontrar 0 al realizar la medición como estado del primer qubit. Si f es balanceada, la interferencia es positiva respecto al estado $|1\rangle$ y negativa respecto de $|0\rangle$ pues las amplitudes iniciales se cancelan con lo que mediremos para el primer qubit en el estado 1.

Como hemos visto el cálculo de la interferencia sobre el primer qubit permite el cálculo de las salidas del circuito y con ello deducir una propiedad global de la función.

El algoritmo de Shor. Impacto en la criptografía

Fue en 1994 cuando Peter Shor propuso un algoritmo [20] basado en métodos cuánticos para factorizar enteros como producto de primos.

Su idea fue sustituir el problema de dicha factorización por el de encontrar el periodo de una función $f(n) := a^n \, (mod\, N)$ donde $a \in \{1, 2, \ldots, N-1\}$ es primo relativo con N. Dicho periodo es el menor $n \neq 0$ para el cuál $f(n) = 1$ y se conoce también como el orden de a en $\mathbb{Z}_N$.

Hallar los factores primos de un entero N se reduce a encontrar cualquiera de ellos; veamos como hacerlo.

Ejemplo 3.3.1. Supongamos que $N = 15$.

1º Elegimos un $a < N$, por ejemplo $a = 11$

2º Si $(a, N) \neq 1$, a es ya un factor no trivial de N y hemos terminado. Dado que $(a, N) = (11, 15) = 1$, continuamos.

3º Calculamos el orden de a, es decir, sea $n = 1, 2, \ldots$, efectuamos $f(n) = a^n \, (mod\, N)$ hasta que $f(n) = 1$.

Si $n = 1$, $11^1 \, (mod 15) = 11$. Si $n = 2$, $11^2 \, (mod 15) = 1$ por lo que 2 es el orden de 11 en $\mathbb{Z}_{15}$.

4º Si $(a^{n/2} - 1, N)$ o $(a^{n/2} + 1, N)$ no son 1, son entonces factores de N. En caso contrario, regresamos a 1º. Dado que $(11^{2/2} - 1, 15) = (10, 15) = 5$ y $(11^{2/2} + 1, 15) = (12, 15) = 3$, podemos concluir $15 = 3 \cdot 5$

En 1995 Grover desarrolló el algoritmo de búsqueda cuántica [9] que hoy lleva su nombre y que da respuesta al problema de, dada una función $f : A \to \{0, 1\}$, siendo A el espacio o conjunto de búsqueda con $N = 2^n$ elementos, encontrar $x \in A$: $f(x) = 1$. Dicho algoritmo permite reducir el costo en computación clásica de 2^n operaciones a $\sqrt{2^n}$.

Sin embargo, el algoritmo de Shor supone un impacto mucho mayor que cualquier otro desarrollado en base a métodos cuánticos, pues resuelve el problema de factorizar números y el cálculo del logaritmo discreto; problemas que, a día de hoy, son intratables desde el punto de vista clásico.

Como veíamos anteriormente, la factorización de números enteros, constituye la base para la seguridad del algoritmo RSA y el cálculo del logaritmo discreto en $\mathbb{Z}_p$, base para el criptosistema de ElGamal. Incluso el algoritmo de ElGamal para curvas elípticas puede verse afectado dado que existen reducciones del problema del logaritmo elíptico al problema del logaritmo discreto sobre $\mathbb{Z}_p$ como [14].

En definitiva, Shor desarrolló el algoritmo que pone de manifiesto la superioridad cuántica en cuanto a la capacidad de acabar con las bases de la criptografía actual.

4

Conclusiones

La ley de Moore mantiene aún su validez desde que fue enunciada hace 55 años. Sin embargo, en 2007, el propio Moore predijo que en los siguientes diez o quince años su ley dejaría de cumplirse.

Actualmente, como ya explicábamos al comienzo, este proceso está llegando a su fin, pero la física cuántica se abre paso como un nuevo modelo tecnológico.

Las matemáticas nos permiten explicar y predecir el comportamiento de la materia a escalas subatómicas, por lo que a lo largo de este trabajo se ha desarrollado un resumen conciso y autocontenido de los conceptos algebraicos fundamentales para el estudio de la computación cuántica basada en las propiedades de la superposición, que describe cómo una partícula puede estar en diferentes estados a la vez y el entrelazamiento cuántico consistente en la correlación de dos partículas que aunque esten separadas, la actuación sobre una altera el estado de la otra.

El nuevo paradigma cuántico supone grandes avances en los campos de la inteligencia artificial, los drones o la red 5G y en múltiples áreas de la bioinformática y biomedicina como el diseño de fármacos y tratamientos personalizados genéticamente; así como en la investigación del ADN. En economía, mejoran las inversiones y los sistemas de detección de fraude y en transporte se optimizan rutas y planificación del tráfico y ya existen aviones que implementan la métodología cuántica.

A pesar de estas y otras muchas aplicaciones, cabe destacar el enorme impacto que supone el desarrollo cuántico sobre la criptografía y por ende sobre las tecnologías en las que esta tiene un rol más relevante, como la seguridad informática o ciberseguridad, las telecomunicaciones o el Blockchain. La programación cuántica supondrá grandes avances en la resolución problemas de cifrado de la información y encriptación de datos.

Hemos visto que el único método criptográfico clásico que se ha probado es totalmente seguro depende de la distribución de una única clave por lo que esta ha de trasmitirse mediante un canal seguro.

La solución viene de la mano de la criptografía cuántica mediante el sistema de distribución de clave cuántica (QKD) que garantiza la confidencialidad gracias a la imposibilidad de clonar un sistema cuántico. El BB84 fue el primer protocolo cuántico desarrollado para la distribución segura de una clave y se basa en la propiedad de entrelazamiento de un sistema cuántico permitiendo que los comunicantes perciban la presencia de posibles espías en el proceso.

Actualmente, el sistema criptográfico dominante es el que conocemos como asimétrico o de clave pública que emplea dos claves esquivando así el problema de la distribución segura de una única clave. La seguridad de los algoritmos de este tipo se basa en la dificultad de la resolución de ciertos problemas como el cálculo del logaritmo discreto o, en el caso del algoritmo RSA, la factorización de números lo suficientemente grandes.

En 1994, Peter Shor presentó un algoritmo capaz de resolver estos problemas rompiendo el sistema criptográfico más empleado, lo que motivó el estudio de otros algoritmos cuánticos así como de la tecnología necesaria para construir ordenadores cuánticos lo suficientemente potentes que permitan implementarlos. El algoritmo de Shor

hace necesario el desarrollo de métodos convencionales que resistan los posibles ataques cuánticos.

Todas las grandes empresas tecnológicas ya se han posicionado respecto a la computación cuántica y trabajan en la creación de ordenadores lo suficientemente potentes. IBM desarrolló en 2016 su primer prototipo de procesador de 5 qubits, y en 2017 el 'IBM Q' de 20 qubits, el primer sistema con esta capacidad al alcance de cualquier usuario. A principios de 2019, la compañía anunció el primer ordenador cuántico para uso científico y comercial, el 'Q System One' y en septiembre consiguió desarrollar el que a día de hoy es el ordenador cuántico más grande y potente operando a nivel comercial con 53 qubits disponible en la nube para sus clientes. Por su parte Google, tan sólo un mes después del anuncio por parte de IBM, hizo público un sistema progamable denominado Sycamore [1] también de 53 qubits capaz de ejecutar en 200 segundos una tarea que a la mejor de las supercomputadoras clásicas del mundo, la Summit, construida por IBM abría tardado en completar alrededor de 10.000 años. Con este experimento, Google anunció haber alcanzado la supremacía cuántica. Sin embargo IBM argumenta [2] que los cálculos en el dispositivo clásico serían realizados en 2 días y medio siendo mucho más de 200 segundos pero ya no serían inabordables con ordenadores actuales, que es el concepto que se utiliza para definir la supremacía cuántica.

Estos continuos avances hacen parecer que antes de lo que pensamos los primeros ordenadores cuánticos domésticos serán una realidad. Sin embargo, aún hemos de lidiar con dificultades en el desarrollo del marco cuántico. El principal desafío al que hacer frente es el problema de la decoherencia que consiste en que al interactuar con el entorno, el sistema se modifica perdiendo información pues deja de estar en superposición de estados y se comporta como un sistema clásico. Por ello es necesario ejecutar cualquier algoritmo antes del tiempo de decoherencia; es decir, antes de que el qubit pierda sus propiedades cuánticas. Para conseguir este aislamiento del sistema, los ordenadores cuánticos han de trabajar a -273 ° C y en condiciones de vacío. Además se hace necesario permitir la interacción entre qubits para poder crear estados entrelazados. Para corregir los errores fruto de la decoherencia se incrementa el número de qubits, aumentando así la dificultad de mantener la estabilidad y aislamiento del sistema. Esto constituye el problema de escalabilidad de los sistemas cuánticos.

En definitiva, aunque en caso de desarrollarse la computación cuántica acabaría con las bases de los actuales sistemas de seguridad de Internet (Internet Protocol), redes privadas VPN (Virtual private net), firma digital y certificados digitales; la sensibilidad de los sistemas y las condiciones de aislamiento que precisan hacen que a medio plazo no se espere disponer de prototipos lo suficientemente potentes para amenazar los sistemas convencionales.

Cabe destacar que el cambio de paradigma no consiste en que los ordenadores cuánticos sean más rápidos realizando las mismas tareas que los actuales, sino que resuelvan ciertas operaciones de forma diferente, que en muchos casos resulta ser más eficiente, es decir, en menos tiempo o utilizando muchos menos recursos computacionales. Es por ello, por lo que al menos a medio plazo, la computación cuántica coexistirá con los métodos clásicos.

[1] https://www.nature.com/articles/s41586-019-1666-5

[2] https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

Bibliografía

[1] S. Akama. *Elements of Quantum Computing: History, Theories and Engineering Applications*. Springer, (2015).

[2] C. H. Bennett, G. Brassard. *Quantum Criptography: Public key distribution and Coin Tossing*. Int. Conf. on Computers, Systems and Signal Processing. Bangalore, India, 175-179, (1984).

[3] J. Daemen, V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, (2002).

[4] F. De Lima Marquezino, R. Portugal, C. Lavor. *A Primer on Quantum Computing*. SpringerBriefs in Computer Science. Springer, (2019).

[5] D. Deutsch. *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*. Proceedings of the Royal Society of London A, vol. 400, 97–117, (1985).

[6] W. Diffie, M. E. Hellman. *New directions in cryptography*. IEEE Transactions on Information Theory, vol. 22, no. 6, 644-654, (1976).

[7] T. ElGamal. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Transactions on Information Theory, vol. 31, no. 4, 469-472, (1985).

[8] M. Gordon. *Cramming More Components onto Integrated Circuits*, Electronics Magazine. Vol. 38, No. 8 (April 19, 1965).

[9] L.K. Grover. *A fast quantum mechanical algorithm for database search*. Proc. of the 28th ACM Symposium on Theory of Computing, 212–219, (1996).

[10] P. R. Halmos. *Naive Set Theory*. Van Nostrand, Nueva York (1960).

[11] J. D. Hidary. *Quantum Computing: An Applied Approach*. Springer, (2019).

[12] P. Kaye, R. Laflamme, M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, (2007).

[13] N. Koblitz. *Elliptic curve cryptosystems*. Mathematics of Computation, vol. 48, no. 177, 203-209, (1987).

[14] A. Menezes, S. Vanstone, T. Okamoto. *Reducing elliptic curve logarithms to logarithms in a finite field*. STOC' 91, Proceedings of the 23rd annual ACM symposium on Theory of Computing, 80-89, (1991).

[15] D. McMahon. *Quantum computing explained*. John Wiley & Sons, Inc. IEEE Computer Society, (2008).

[16] V. Miller. *Use of elliptic curves in cryptography*. H.C. Williams (Ed.): Advances in Cryptology - CRYPT0' 85, Springer Lecture Notes in Computer Science vol. 218, 418-426, (1985).

[17] M. Nielsen, I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, (2010).

[18] R. Rivest, A. Shamir, L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, vol. 21, no. 2, 120-126, (1978).

[19] C. E. Shannon. *Communication theory of secrecy systems*. Bell System Technical Journal, vol. 28, no. 4, 656-715, (1949).

[20] P. Shor. *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134, IEEE Computer Society, Washington (1994).

[21] R. L. Vaught. *Set Theory. An Introduction.* Birkhauser, Boston (1985).

[22] B. Zygelman. *A First Introduction to Quantum Computing and Information*. Springer (2018).