Universidad de La Laguna

Breve Introducción al Álgebra Lineal

Microcredencial en Introducción a la Computación Cuántica

Daniel Escanez-Exposito

Jorge Garcia-Diaz

Escuela Superior de Ingeniería y Tecnología

Grupo de Investigación en Criptología - CryptULL

La Laguna, 2025

Universidad de La Laguna

Breve Introducción al Álgebra Lineal

Microcredencial en Introducción a la Computación Cuántica

Daniel Escanez-Exposito
Correo electrónico - jescanez@ull.edu.es

Jorge Garcia-Diaz
Correo electrónico - jgarcidi@ull.edu.es

Escuela Superior de Ingeniería y Tecnología
Grupo de Investigación en Criptología - CryptULL

Microcredencial en Introducción a la Computación Cuántica

La Laguna, 2025

Índice general

A

Breve Introducción al Álgebra Lineal

En esta sección introduciremos los elementos básicos del Álgebra Lineal para seguir los capítulos de este libro, desde la noción de vector y escalar hasta estructuras más complejas. Se empezará con la intuición y diferencias entre escalares y vectores, para luego formalizar matemáticamente estos objetos gracias a los espacios vectoriales. Estos conceptos serán necesarios para trabajar y entender la computación e información cuántica.

A.1. Escalares y vectores

La principal diferencia entre un escalar y un vector no es más que la cantidad de información que manejan. Un escalar es simplemente un número, se suelen usar para describir variables que solo necesitan un dato: la temperatura ($25°C$), el precio de un café ($1'50$ €) o una constante matemática como π. Un escalar solo nos dice "cuánto" hay de algo (su magnitud).

En cambio, un vector almacena más información. Geométricamente, se puede visualizar un vector como una flecha: tiene una longitud (magnitud), una dirección y una punta sobre la dirección que indica su sentido. Para describir matemáticamente un vector se suele usar una colección ordenada de números. Por ejemplo el vector $(1, 2)$ es una flecha que avanza 1 unidad en el eje X y 2 en el eje Y. El vector $(10, \pi, \frac{1}{2})$ sería una flecha en un espacio de 3 dimensiones (ejes X, Y y Z).

Nota

Tanto los puntos como los vectores de espacios de d dimensiones se representan mediante colecciones ordenadas de d números, pero son objetos matemáticos distintos. Un punto indica una posición en el espacio, mientras que un vector se puede interpretar como movimiento (traslación) para los puntos en este espacio, pues tienen dirección, sentido y magnitud (distancia recorrida), pero estos carecen de posición en el espacio.

Teniendo en cuenta que los vectores definen traslaciones en los puntos de un espacio, podemos pensar en la encadenación (composición) de estas traslaciones o incluso en como encoger o expandir un vector. Esto se consigue mediante las operaciones básicas con vectores.

A.2. Operaciones básicas con vectores

Una vez definido el concepto de vector, surge la pregunta natural: ¿cómo se opera con ellos? Aunque existen diversas operaciones, hay dos fundamentales sobre las que se construye todo el Álgebra Lineal: la suma de vectores y la multiplicación por un escalar (o escalado).

A.2.1. Suma de vectores

Si se interpreta un vector como un desplazamiento, la suma de dos vectores equivale a realizar un movimiento seguido del otro.

Por ejemplo, supóngase que el vector $\vec{v} = (3, 1)$ representa un desplazamiento de "3 pasos al Este y 1 al Norte". Por otro lado, el vector $\vec{w} = (2, 4)$ representa "2 pasos al Este y 4 al Norte".

Si se efectúan ambos movimientos de manera consecutiva, el resultado final es un desplazamiento total de 5 pasos al Este $(3 + 2)$ y 5 pasos al Norte $(1 + 4)$. Matemáticamente, la suma se realiza componente a componente:

$$\vec{v} + \vec{w} = (3, 1) + (2, 4) = (5, 5)$$

Geométricamente, esto se visualiza mediante la llamada "regla del triángulo": se coloca la base del segundo vector en la punta del primero. El vector suma es la flecha que une el origen del primero con el final del último.

A.2.2. Multiplicación por un escalar

La segunda operación consiste en tomar un vector y multiplicarlo por un número (un escalar). Dado que un escalar representa una magnitud, al multiplicar un vector

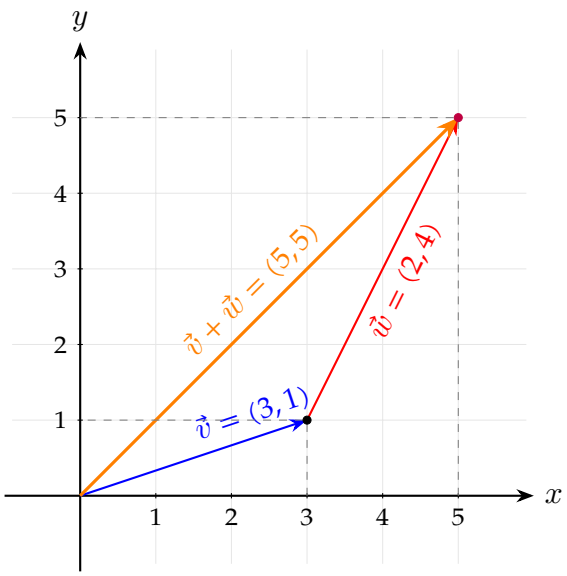

Figura A.1: *Interpretación geométrica de la suma de vectores.*

por un número, lo que se hace es "escalarlo": se modifica su longitud manteniendo la dirección original.

Se pueden distinguir tres casos principales:

- Si se multiplica por un número mayor que 1 (ej. 2), la flecha se alarga.
- Si se multiplica por un número entre 0 y 1 (ej. 0,5), la flecha se contrae.
- Si se multiplica por un número negativo (ej. -1), la flecha invierte su sentido, apuntando hacia el lado contrario.

Matemáticamente, esta operación se realiza multiplicando cada coordenada del vector por dicho número. Si $\vec{v} = (1,2)$:

$$2 \cdot \vec{v} = (2,4)$$

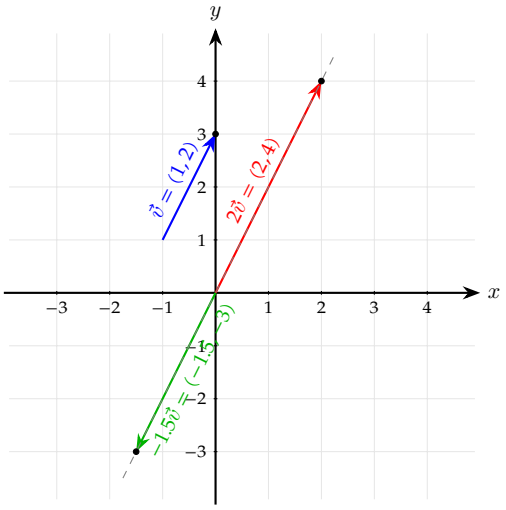

Figura A.2: *Interpretación geométrica del producto de un vector con un escalar.*

A.3. Números complejos

Hasta el momento, se ha trabajado bajo la asunción implícita de que los escalares pertenecen al conjunto de los números reales $(\mathbb{R})$. Este conjunto es suficiente para resolver muchas ecuaciones algebraicas y problemas geométricos cotidianos. Sin embargo, desde un punto de vista matemático estricto, los números reales presentan una limitación fundamental: no son algebraicamente cerrados.

Esta limitación se hace evidente al intentar resolver ecuaciones polinómicas muy sencillas. Considérese, por ejemplo, la ecuación:

$$x^2 - 1 = 0$$

Esta ecuación tiene dos soluciones claras en los números reales: $x = 1$ y $x = -1$. Geométricamente, estas soluciones corresponden a los puntos donde la parábola $y = x^2 - 1$ corta al eje horizontal.

Sin embargo, si se cambia ligeramente el signo de la constante, se obtiene:

$$x^2 + 1 = 0 \quad \Longrightarrow \quad x^2 = -1$$

No es difícil observar que el polinomio $x^2 + 1$ no tienes raíces reales, es por ellos que surgen los números complejos.

A.3.1. Definición y representación

En esencia, un número complejo c es un número que se puede expresar en la forma:

$$z = a + bi$$

donde a y b son números reales, e i es la **unidad imaginaria**.

La unidad imaginaria i es la solución a la ecuación $x^2 = -1$, por lo que se define como $i = \sqrt{-1}$, con la propiedad fundamental $i^2 = -1$.

- $a = \text{Re}(c)$, se denomina la **parte real** de c.
- $b = \text{Im}(c)$, se denomina la **parte imaginaria** de c.

Si $b = 0$, el número $z = a$ es simplemente un número real. Esto demuestra que el conjunto de los números reales $\mathbb{R}$ es un subconjunto de los números complejos $\mathbb{C}$.

Así como los números reales se representan en una recta numérica, los números complejos se pueden visualizar en un plano de dos dimensiones llamado **plano complejo**.

En este plano, el eje horizontal representa la parte real (a) y el eje vertical representa la parte imaginaria (b). Por lo tanto, el número complejo $z = a + bi$ se corresponde con el punto (a, b) en el plano.

A

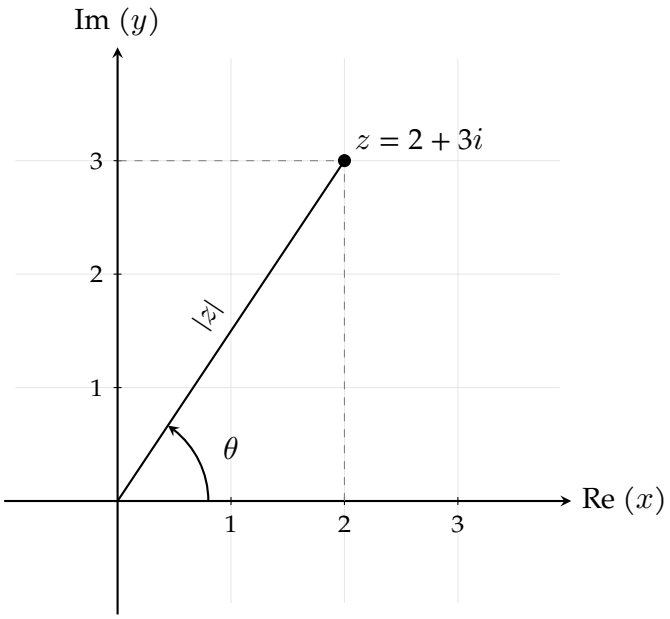

Figura A.3: *Representación geométrica de un número complejo.*

A.3.2. Operaciones con números complejos

Además de las operaciones aritméticas estándar (suma, resta, multiplicación y división), hay dos operaciones que son absolutamente esenciales para la computación cuántica: el conjugado complejo y el módulo.

Definición A.3.1 (Conjugado Complejo)**.** *El* ***conjugado complejo*** *de un número $z = a + bi$, denotado como z^* (o a veces $\bar{z}$), se obtiene cambiando el signo de la parte imaginaria:*

$$z^* = a - bi$$

Gráficamente, z^* es el simétrico de z con respecto al eje real. Esta operación es crucial para definir el producto interno (que se verá más adelante) y para la construcción de matrices hermíticas.

Definición A.3.2 (Módulo de un Número Complejo)**.** *El módulo (o magnitud) de un número complejo z, denotado $|c|$, es su distancia desde el origen $(0, 0)$ hasta el punto (a, b) en el plano complejo.*

Por el teorema de Pitágoras, esta distancia es:

$$|z| = \sqrt{a^2 + b^2}$$

Una propiedad extremadamente útil es que el módulo al cuadrado se puede calcular multiplicando el número por su conjugado:

$$|z|^2 = z \cdot z^* = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 - (b^2 i^2) = a^2 + b^2$$

Consejo

En computación cuántica, los escalares que describen los estados de un cúbit se llaman **amplitudes**, que se suelen denotar por $\alpha \in \mathbb{C}$. El módulo al cuadrado de una amplitud de probabilidad, $|z|^2$, representa la **probabilidad** real y medible de obtener un resultado específico. Dado que las probabilidades deben sumar 1, la normalización de los vectores cuánticos dependerá directamente de esta operación.

Definición A.3.3 (Fase de un Número Complejo)**.** *La fase ϕ es el ángulo del vector z respecto al eje real. Generalmente se usa* $\arctan(b/a)$*, pero si $a = 0$ (eje vertical), se define por casos:*

$$\phi = \begin{cases} \arctan\left(\frac{b}{a}\right) & si\ a > 0 \\ \arctan\left(\frac{b}{a}\right) + \pi & si\ a < 0, b \geq 0 \\ \arctan\left(\frac{b}{a}\right) - \pi & si\ a < 0, b < 0 \\ \frac{\pi}{2} & si\ a = 0, b > 0 \\ -\frac{\pi}{2} & si\ a = 0, b < 0 \end{cases}$$

A.3.3. Forma exponencial

Además de la forma cartesiana $z = a+bi$, un número complejo se puede representar por su *módulo* $|z|$ (su longitud) y su *argumento* θ (el ángulo que forma con el eje real).

Gracias a la **fórmula de Euler**, $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, cualquier número complejo z se puede escribir en forma exponencial (o polar):

$$z = |z|\,(\cos(\theta) + i\sin(\theta)) = |z|\,e^{i\theta}$$

El término $e^{i\theta}$ se denomina **fase**. Dos estados cuánticos que solo difieren en una fase global (ejemplo: $\mathbf{v}$ y $e^{i\theta}\mathbf{v}$) son físicamente indistinguibles. Sin embargo, las diferencias de fase *relativas* entre componentes de un vector son la causa del fenómeno de la **interferencia cuántica**, la principal fuente de la ventaja computacional cuántica.

A.4. Espacios vectoriales

Una vez que se entiende el concepto de vector, se está en condiciones de formalizar matemáticamente los vectores. Esto se consigue mediante los espacios vectoriales. Los espacios vectoriales se definen sobre otra estructura algebraica llamada cuerpos, que son básicamente conjuntos de escalares. No es necesario entender exactamente que es un cuerpo, ahora mismo basta con saber que los números reales $\mathbb{R}$ con la suma y el producto usual conforman un cuerpo al igual que los complejos $\mathbb{C}$.

Un espacio vectorial V sobre un cuerpo K es un conjunto no vacío de objetos (vectores) provisto de dos operaciones:

1. **Suma de vectores:** Una operación interna $+ : V \times V \to V$.
2. **Producto por escalar:** Una operación externa $\cdot : K \times V \to V$.

Estas operaciones deben satisfacer los siguientes axiomas para todo $u, v, w \in V$ y todo escalar $a, b \in K$:

- **Distributividad (vectorial):** $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$.
- **Distributividad (escalar):** $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$.
- **Asociatividad (producto de escalares):** $a(b\mathbf{v}) = (ab)\mathbf{v}$.
- **Elemento neutro (escalar 1_K):** El escalar 1_K (el "uno" del cuerpo K) cumple $1_K \cdot \mathbf{v} = \mathbf{v}$, $\forall \mathbf{v} \in V$.

> **Nota**
>
> No es necesario entender profundamente la teoría de anillos para trabajar en computación cuántica, pero basta con saber que un cuerpo K es un conjunto de elementos (que se denominan *escalares*) donde están bien definidas dos operaciones: suma $(+)$ y producto $(\cdot)$.
> Los ejemplos que usaremos son:
>
> - El cuerpo de los números reales: $(\mathbb{R}, +, \cdot)$.
> - El cuerpo de los números complejos: $(\mathbb{C}, +, \cdot)$.

A.4.1. Combinación lineal, generadores e independencia

Antes de definir formalmente una base, se deben introducir tres conceptos clave. En lo que sigue, se asume un espacio vectorial V sobre un cuerpo K.

Definición A.4.1 (Combinación Lineal)**.** *Un vector $\mathbf{v} \in V$ es una **combinación lineal** de un conjunto de vectores $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ (con $\mathbf{v}_i \in V$) si se puede expresar de la forma:*

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$$

donde $a_1, a_2, \dots, a_n$ son escalares del cuerpo K.

La idea de "generar" un espacio es poder construir cualquier vector del espacio usando un conjunto finito de "ladrillos" (otros vectores).

Definición A.4.2 (Sistema Generador)**.** *Se dice que un conjunto de vectores $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ es un **sistema generador** (o que genera) el espacio V, si todo vector $\mathbf{v} \in V$ se puede escribir como una combinación lineal de los vectores en S.*

Un sistema generador puede tener vectores "redundantes". Por ejemplo, en $\mathbb{R}^2$ (el plano), el conjunto $\{(1,0),(0,1),(1,1)\}$ genera el espacio, pero el vector $(1,1)$ es redundante, ya que se puede construir a partir de los otros dos. La independencia lineal formaliza la idea de un conjunto sin redundancias.

Definición A.4.3 (Conjunto Linealmente Independiente)**.** *Se dice que un conjunto de vectores $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ es **linealmente independiente** si la única forma de que su combinación lineal sea el vector cero ($\mathbf{0}$) es que todos los escalares sean cero. Es decir:*

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{0}_{\mathbf{v}} \quad \Longrightarrow \quad a_1 = a_2 = \cdots = a_n = 0_K$$

*Si existe una solución donde algún escalar a_i no es cero, se dice que el conjunto es **linealmente dependiente**.*

A.4.2. Bases y dimensión

El concepto de "base" une las dos propiedades anteriores: es el conjunto de vectores más pequeño y eficiente posible que aún puede generar el espacio completo.

Definición A.4.4 (Base de Espacio Vectorial)**.** *Un conjunto de vectores $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ es una **base** de un espacio vectorial V si cumple dos condiciones simultáneamente:*

1. *B es un sistema generador de V.*
2. *B es linealmente independiente.*

> **Consejo**
>
> La gran utilidad de una base es que permite representar cualquier vector $\mathbf{v} \in V$ como una combinación lineal de los vectores de la base de forma **única**.
> Es decir, para cualquier $\mathbf{v}$, existen escalares $a_1, \dots, a_n$ únicos tales que $\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$. Estos escalares $(a_1, \dots, a_n)$ se denominan las **coordenadas** (o componentes) del vector $\mathbf{v}$ en la base B.

Se puede demostrar que, aunque un espacio vectorial puede tener infinitas bases diferentes, *todas* las bases de un mismo espacio vectorial tienen el mismo número de vectores.

Definición A.4.5 (Dimensión de un Espacio Vectorial)**.** *Se denomina dimensión de un espacio vectorial V, denotado como $\dim(V)$, al número de vectores que componen cualquiera de sus bases.*

Ejemplo A.4.1 (La Base Canónica)**.** *El espacio vectorial $\mathbb{C}^n$ (listas de n números complejos) es fundamental en computación cuántica. Su base más simple es la **base canónica** (o base*

estándar), formada por n vectores:

$$\begin{aligned}\mathbf{e}_1 &= (1,0,0,\dots,0)\\ \mathbf{e}_2 &= (0,1,0,\dots,0)\\ &\vdots\\ \mathbf{e}_n &= (0,0,0,\dots,1)\end{aligned}$$

Dado que esta base tiene n vectores, la dimensión de $\mathbb{C}^n$ es n. Por ejemplo, el espacio de un qubit, $\mathbb{C}^2$, tiene dimensión 2.

A.5. Aplicaciones lineales

El álgebra lineal se centra casi exclusivamente en un tipo especial de aplicaciones que preservan la estructura del espacio vectorial. Estas se denominan **aplicaciones lineales**.

A.5.1. Aplicaciones

De forma general, una aplicación f de un conjunto A a un conjunto B, denotado por $f : A \to B$, es una regla que asigna a cada elemento de A un *único* elemento de B.

Definición A.5.1 (Aplicación)**.** *Una aplicación de un conjunto A a un conjunto B, denotada como:*

$$f : A \to B$$

es una aplicación si y solo si cumple las siguiente propiedad:

- *Existencia y unicidad de la imagen:*

$$\forall a \in A,\ \exists! b \in B : f(a) = b$$

> **Nota**
>
> En general, para una aplicación $f : A \to B$ se denomina al conjunto A como conjunto de salida (o dominio) y al conjunto B como conjunto de llegada. En particular, al conjunto $f(A) = \{b \in B \mid \exists a \in A : f(a) = b\}$.

En el contexto de este libro, los conjuntos A y B serán en su inmensa mayoría espacios vectoriales, V y W. Por lo tanto, una aplicación $T : V \to W$ es una regla que toma cada vector $\mathbf{v} \in V$ y le asigna un único vector $\mathbf{w} \in W$, que se denota como $T(\mathbf{v}) = \mathbf{w}$.

Sin embargo, la mayoría de las aplicaciones arbitrarias entre espacios vectoriales no son muy útiles para el álgebra lineal, ya que no respetan la estructura (la suma y el producto por escalar) que acabamos de definir.

A.5.2. Aplicaciones lineales

Intuitivamente, una aplicación es lineal si "respeta" las líneas de la cuadrícula: una cuadrícula de líneas rectas y paralelas se transforma en otra cuadrícula de líneas rectas y paralelas (aunque pueden haberse estirado, rotado o sesgado).

Formalmente, se definen de la siguiente manera:

Definición A.5.2 (Aplicación Lineal)**.** *Dados dos espacios vectoriales V y W sobre el mismo cuerpo K (por ejemplo, $\mathbb{C}$), se dice que una aplicación $T : V \to W$ es **lineal** si cumple las dos siguientes condiciones para todos los vectores $\mathbf{u}, \mathbf{v} \in V$ y todos los escalares $a \in K$:*

1. ***Aditividad* (*Preserva la suma*)*:***

$$T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$$

2. ***Homogeneidad* (*Preserva el producto por escalar*)*:***

$$T(a\mathbf{v}) = aT(\mathbf{v})$$

Estas dos condiciones son la piedra angular de todo el álgebra lineal. En computación cuántica, las puertas cuánticas (las operaciones que se aplican a los cúbits) son, de hecho, aplicaciones lineales de un tipo muy específico (unitarias) que operan sobre el espacio $\mathbb{C}^n$.

A.6. Representación matricial de aplicaciones lineales

Se ha establecido que las operaciones en computación cuántica son aplicaciones lineales. La gran utilidad de esto proviene de un resultado fundamental: *toda aplicación lineal entre espacios vectoriales de dimensión finita se puede representar mediante una matriz*.

A.6.1. Matriz de una aplicación lineal

Dada una aplicación lineal $T : V \to W$, ¿cómo se construye su matriz asociada?

El procedimiento se basa en ver cómo la aplicación T transforma los vectores de la **base** de V. Si se sabe qué le pasa a la base, se sabe qué le pasa a cualquier vector del espacio.

Supóngase que V tiene dimensión n y una base $B_V = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$, y que W tiene dimensión m y una base $B_W = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_m\}$.

El procedimiento es el siguiente:

1. **Transformar cada vector de la base de salida:** Se aplica T a cada vector $\mathbf{v}_j$ de la base de V para obtener un vector $T(\mathbf{v}_j)$ en W.
2. **Escribir el resultado en la base de llegada:** Como $T(\mathbf{v}_j)$ es un vector en W, se puede escribir como una combinación lineal única de los vectores de la base de W:

$$T(\mathbf{v}_j) = a_{1j}\mathbf{w}_1 + a_{2j}\mathbf{w}_2 + \cdots + a_{mj}\mathbf{w}_m$$

3. **Formar la matriz con las coordenadas:** Los escalares (coordenadas) de esta combinación lineal $(a_{1j}, a_{2j}, \dots, a_{mj})^T$ se convierten en la **columna** j de la matriz A.

Definición A.6.1 (Matriz Asociada)**.** *La matriz A de $m \times n$ asociada a la aplicación lineal T (respecto a las bases B_V y B_W) se forma usando los vectores de coordenadas de las imágenes de la base B_V como sus columnas:*

$$A = \begin{pmatrix} | & | & & | \\ [T(\mathbf{v}_1)]_{B_W} & [T(\mathbf{v}_2)]_{B_W} & \dots & [T(\mathbf{v}_n)]_{B_W} \\ | & | & & | \end{pmatrix}$$

Una vez que se tiene esta matriz A, la acción de la aplicación abstracta T sobre *cualquier* vector $\mathbf{v}$ es equivalente a la multiplicación de la matriz A por el vector de coordenadas de $\mathbf{v}$.

Ejemplo A.6.1. *Considérese la aplicación lineal $T : \mathbb{R}^2 \to \mathbb{R}^3$ definida por:*

$$T(x, y) = (x + y, x - y, 2y)$$

Se desea encontrar la matriz A asociada a T utilizando las bases canónicas para ambos espacios.

El espacio de salida es $V = \mathbb{R}^2$, con $\dim(V) = 2$. Su base canónica es $B_V = \{\mathbf{v}_1, \mathbf{v}_2\} = \{(1, 0), (0, 1)\}$. El espacio de llegada es $W = \mathbb{R}^3$, con $\dim(W) = 3$. Su base canónica es $B_W = \{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\} = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

La matriz A será de tamaño $\dim(W) \times \dim(V)$, es decir, 3×2.

Paso 1: Transformar la base de V

Se aplica T a cada vector de la base B_V:

$$T(\mathbf{v}_1) = T(1, 0) = (1 + 0, 1 - 0, 2 \cdot 0) = (1, 1, 0)$$
$$T(\mathbf{v}_2) = T(0, 1) = (0 + 1, 0 - 1, 2 \cdot 1) = (1, -1, 2)$$

Paso 2: Escribir los resultados en la base de W

Se expresan los vectores obtenidos como combinación lineal de la base B_W. Al ser B_W la base canónica, este paso es directo:

$$T(\mathbf{v}_1) = (1, 1, 0) = 1 \cdot \mathbf{w}_1 + 1 \cdot \mathbf{w}_2 + 0 \cdot \mathbf{w}_3$$
$$T(\mathbf{v}_2) = (1, -1, 2) = 1 \cdot \mathbf{w}_1 - 1 \cdot \mathbf{w}_2 + 2 \cdot \mathbf{w}_3$$

Las coordenadas obtenidas son:

$$[T(\mathbf{v}_1)]_{B_W} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad y \quad [T(\mathbf{v}_2)]_{B_W} = \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}$$

Paso 3: Formar la matriz

Se usan estas coordenadas como las columnas de la matriz A:

$$A = \begin{pmatrix} | & | \\ [T(\mathbf{v}_1)]_{B_W} & [T(\mathbf{v}_2)]_{B_W} \\ | & | \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 2 \end{pmatrix}$$

Esta es la matriz A (de 3×2) que representa a T respecto a las bases canónicas.

Ejemplo A.6.2. *Este ejemplo demuestra que la matriz asociada depende críticamente de las bases elegidas.*

Considérese $T : \mathbb{R}^2 \to \mathbb{R}^2$ definida por $T(x, y) = (2x, x + y)$. Se usará la misma base B para el espacio de salida y de llegada:

$$B = B_V = B_W = \{\mathbf{v}_1, \mathbf{v}_2\} = \{(1, 1), (1, -1)\}$$

Paso 1: Transformar la base de V

$$T(\mathbf{v}_1) = T(1, 1) = (2 \cdot 1, 1 + 1) = (2, 2)$$
$$T(\mathbf{v}_2) = T(1, -1) = (2 \cdot 1, 1 - 1) = (2, 0)$$

Paso 2: Escribir los resultados en la base de W (que es B)

Aquí se debe resolver un sistema de ecuaciones para encontrar las coordenadas.

Para $T(\mathbf{v}_1) = (2, 2)$:

$$(2, 2) = a\mathbf{v}_1 + b\mathbf{v}_2 = a(1, 1) + b(1, -1) = (a + b, a - b)$$

Se obtiene el sistema: $a + b = 2$ y $a - b = 2$. Resolviendo, se encuentra $a = 2, b = 0$. Por lo tanto, $[T(\mathbf{v}_1)]_B = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$.

Para $T(\mathbf{v}_2) = (2, 0)$:

$$(2, 0) = c\mathbf{v}_1 + d\mathbf{v}_2 = c(1, 1) + d(1, -1) = (c + d, c - d)$$

Se obtiene el sistema: $c + d = 2$ y $c - d = 0$. Resolviendo, se encuentra $c = 1, d = 1$. Por lo tanto, $[T(\mathbf{v}_2)]_B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Paso 3: Formar la matriz

$$A' = \begin{pmatrix} | & | \\ [T(\mathbf{v}_1)]_B & [T(\mathbf{v}_2)]_B \\ | & | \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

Nótese que A' es completamente diferente de la matriz que se obtendría para la misma T usando la base canónica, la cual sería $A = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$.

A.6.2. Operaciones matriciales

La representación matricial permite traducir operaciones abstractas entre aplicaciones lineales en operaciones algebraicas concretas con matrices. A continuación, se definen el producto matriz-vector y el producto de matrices desde esta perspectiva.

Evaluación de una aplicación: producto matriz-vector

Si la matriz A representa a la aplicación T, entonces evaluar la función T sobre un vector $\mathbf{v}$ equivale algebraicamente a multiplicar la matriz A por el vector de coordenadas de $\mathbf{v}$.

Si A es una matriz de $m \times n$ y $\mathbf{x}$ es un vector columna de $n \times 1$ (las coordenadas de $\mathbf{v}$), el producto $A\mathbf{x}$ genera un nuevo vector $\mathbf{y}$ de $m \times 1$ (las coordenadas de $T(\mathbf{v})$).

La regla de cálculo para la componente i-ésima del vector resultante es el producto escalar de la fila i de la matriz por el vector columna:

$$y_i = \sum_{j=1}^{n} A_{ij} x_j$$

Matricialmente:

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \dots & A_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Composición de aplicaciones: producto de matrices

Una de las operaciones más importantes en álgebra lineal (y fundamental en computación cuántica para la construcción de circuitos) es la composición de aplicaciones.

Sean dos aplicaciones lineales:

$$T : U \to V \quad \text{y} \quad S : V \to W$$

Supóngase que T tiene asociada la matriz B (de dimensiones $p \times n$) y S tiene asociada la matriz A (de dimensiones $m \times p$).

La composición $S \circ T$ es la aplicación que resulta de aplicar primero T y luego S:

$$(S \circ T)(\mathbf{u}) = S(T(\mathbf{u}))$$

El resultado fundamental es que la matriz asociada a la composición $S \circ T$ es el producto de las matrices A y B.

$$\text{Matriz de } (S \circ T) = A \cdot B$$

Para que este producto sea posible, el número de columnas de A debe coincidir con el número de filas de B (lo cual corresponde a la dimensión del espacio intermedio

V).

Definición A.6.2 (Producto de Matrices)**.** *Dada una matriz A de $m \times p$ y una matriz B de $p \times n$, el producto $C = AB$ es una matriz de $m \times n$ cuyos elementos se calculan mediante la suma:*

$$C_{ij} = \sum_{k=1}^{p} A_{ik} B_{kj}$$

Esto significa que el elemento en la fila i y columna j de la matriz producto se obtiene multiplicando la fila i de la primera matriz por la columna j de la segunda.

Ejemplo A.6.3. *Supónganse las matrices $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$.*

El producto AB representa la aplicación conjunta de la transformación asociada a B seguida de la asociada a A. El cálculo es:

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1(0) + 2(2) & 1(1) + 2(1) \\ 3(0) + 4(2) & 3(1) + 4(1) \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 8 & 7 \end{pmatrix}$$

*Es crucial notar que el producto de matrices, en general, **no es conmutativo** ($AB \neq BA$), lo que refleja el hecho de que el orden en que se aplican las transformaciones importa (físicamente, rotar y luego desplazar no es lo mismo que desplazar y luego rotar).*

A.7. Determinante, autovectores y autovalores

Una vez que las aplicaciones lineales se representan como matrices cuadradas (es decir, aplicaciones de un espacio a sí mismo, $T : V \to V$), se pueden estudiar propiedades intrínsecas de dicha transformación. El determinante, los autovalores y los autovectores son las herramientas fundamentales para este análisis.

A.7.1. Determinante de una matriz

El determinante es un número escalar especial que se puede calcular para cualquier matriz *cuadrada* (de tamaño $n \times n$). Se denota como $\det(A)$ o $|A|$.

Este número codifica información geométrica y algebraica fundamental sobre la transformación lineal T asociada a la matriz A.

Nota

Geométricamente, el valor absoluto del determinante $|\det(A)|$ representa el factor por el cual se escala el "volumen" (o el área en 2D) de una forma después de aplicar la transformación T.

- Si $|\det(A)| = 1$, la transformación preserva el volumen (como una rotación pura).
- Si $|\det(A)| > 1$, la transformación expande el volumen.
- Si $|\det(A)| < 1$, la transformación contrae el volumen.
- Si $\det(A) = 0$, la transformación "colapsa" el espacio a una dimensión inferior (por ejemplo, proyecta un plano sobre una recta), resultando en un volumen cero.

Cálculo del Determinante

Para una matriz de 2×2, el cálculo es directo:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \det(A) = ad - bc$$

Para matrices de 3×3 (usando la Regla de Sarrus):

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \implies \det(A) = a(ei - fh) - b(di - fg) + c(dh - eg)$$

En general, el cálculo del determinante de una matriz A de $n \times n$, el método consiste en reducir el problema a calcular determinantes de matrices más pequeñas $(n-1 \times n-1)$. Este proceso se repite hasta llegar a matrices de 2×2, cuyo determinante se sabe calcular.

Para ello, se necesitan dos definiciones:

Definición A.7.1 (Menor)**.** *Dada una matriz cuadrada A de $n \times n$, se define el **Menor** del elemento a_{ij} (el elemento en la fila i, columna j) como el determinante de la submatriz de $(n-1) \times (n-1)$ que se obtiene al **eliminar la fila** i **y la columna** j de la matriz A.*

Este menor se denota como M_{ij}.

Definición A.7.2 (Cofactor)**.** *El **Cofactor** del elemento a_{ij}, denotado como C_{ij}, es el menor M_{ij} multiplicado por un signo que depende de su posición:*

$$C_{ij} = (-1)^{i+j} M_{ij}$$

El término $(-1)^{i+j}$ genera un "patrón de tablero de ajedrez" de signos, donde la

esquina superior izquierda $(1,1)$ es positiva:

$$\begin{pmatrix} + & - & + & \dots \\ - & + & - & \dots \\ + & - & + & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

El determinante de A se puede calcular eligiendo cualquier fila o columna de la matriz. Se multiplica cada elemento de esa fila (o columna) por su cofactor correspondiente, y se suman los resultados.

Definición A.7.3 (Determinante por Cofactores)**.** *Si se expande por la fila i:*

$$\det(A) = \sum_{j=1}^{n} a_{ij}C_{ij} = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}$$

Si se expande por la columna j:

$$\det(A) = \sum_{i=1}^{n} a_{ij}C_{ij} = a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}$$

Ejemplo A.7.1. *Se usará la expansión por cofactores en la primera fila de una matriz general de 3×3:*

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

La fórmula para la fila 1 $(i = 1)$ es:

$$\det(A) = a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13}$$

Se calculan los tres cofactores:

- $C_{11} = (-1)^{1+1}M_{11} = +\det\begin{pmatrix} e & f \\ h & i \end{pmatrix} = (ei - fh)$
- $C_{12} = (-1)^{1+2}M_{12} = -\det\begin{pmatrix} d & f \\ g & i \end{pmatrix} = -(di - fg)$
- $C_{13} = (-1)^{1+3}M_{13} = +\det\begin{pmatrix} d & e \\ g & h \end{pmatrix} = (dh - eg)$

Se sustituyen los cofactores en la fórmula:

$$\det(A) = a(ei - fh) - b(di - fg) + c(dh - eg)$$

Se observa que esta es exactamente la misma fórmula que la Regla de Sarrus. Este método recursivo es la definición general subyacente.

Consejo

Dado que se puede elegir cualquier fila o columna para la expansión, el cálculo se simplifica enormemente si se elige la fila o columna que contenga la **mayor cantidad de ceros**.

La propiedad algebraica más importante del determinante está relacionada con la invertibilidad de una matriz.

Nota

Una matriz cuadrada A es **invertible** (es decir, existe una matriz inversa A^{-1} tal que $AA^{-1} = A^{-1}A = I$) si y solo si su determinante es distinto de cero:

$$\exists A^{-1} \iff \det(A) \neq 0$$

Si $\det(A) = 0$, se dice que la matriz es **singular** o no invertible.

A.7.2. Autovectores y autovalores

Al aplicar una transformación lineal (una matriz A) a un vector $\mathbf{v}$, el vector resultante $A\mathbf{v}$ generalmente cambia tanto su magnitud como su dirección.

Sin embargo, para la mayoría de las matrices cuadradas, existen ciertas direcciones "especiales". Al aplicar la transformación a un vector en una de estas direcciones, el vector resultante mantiene su dirección original, simplemente es escalado (estirado, encogido o invertido).

Estos vectores especiales se llaman **autovectores** (o vectores propios), y el factor por el cual son escalados se llama **autovalor** (o valor propio).

Definición A.7.4 (Autovector y Autovalor)**.** *Dado un espacio vectorial V y una aplicación lineal $T : V \to V$ representada por la matriz cuadrada A, se dice que un vector no nulo $\mathbf{v} \in V$ es un **autovector** de A si existe un escalar $\lambda \in K$ (que puede ser real o complejo) tal que:*

$$A\mathbf{v} = \lambda\mathbf{v}$$

*El escalar λ se denomina el **autovalor** asociado al autovector $\mathbf{v}$.*

Encontrar los autovectores de una matriz es encontrar los "ejes" fundamentales de la transformación que representa.

A.7.3. Cálculo de autovalores y autovectores

Para encontrar los autovalores y autovectores de una matriz A, se debe resolver la ecuación $A\mathbf{v} = \lambda\mathbf{v}$. Esta ecuación se puede reescribir:

$$A\mathbf{v} - \lambda\mathbf{v} = \mathbf{0}$$
$$A\mathbf{v} - \lambda I\mathbf{v} = \mathbf{0}$$
$$(A - \lambda I)\mathbf{v} = \mathbf{0}$$

donde I es la matriz identidad.

Se busca un vector $\mathbf{v}$ que *no* sea el vector cero ($\mathbf{v} \neq \mathbf{0}$) que resuelva esta ecuación.

Recordando la propiedad del determinante: si la matriz $(A - \lambda I)$ fuera invertible, la única solución para $\mathbf{v}$ sería $\mathbf{v} = (A - \lambda I)^{-1}\mathbf{0} = \mathbf{0}$.

Como se busca una solución no nula, se debe imponer que la matriz $(A - \lambda I)$ *no* sea invertible. Esto significa que su determinante debe ser cero.

Definición A.7.5 (Ecuación Característica)**.** *Los autovalores λ de una matriz A son las soluciones de la* ***ecuación característica****:*

$$\det(A - \lambda I) = 0$$

Al resolver esta ecuación (que resulta ser un polinomio en λ), se obtienen los autovalores.

> **Consejo**
>
> Este concepto es central en la mecánica cuántica. En ese dominio:
>
> - Las **matrices** (específicamente, matrices hermíticas) representan "Observables" (cosas que se pueden medir, como la posición o el spin).
> - Los **autovalores** (que para matrices hermíticas son siempre números reales) representan los únicos *resultados posibles* que se pueden obtener al realizar la medición.
> - Los **autovectores** representan los estados definidos del sistema que corresponden a esos resultados de medición.
>
> El acto de medir "fuerza" al sistema a colapsar en uno de los autovectores del observable.

Ejemplo A.7.2. *Considérese la matriz* $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

1. Encontrar Autovalores: *Se resuelve* $\det(A - \lambda I) = 0$.

$$A - \lambda I = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2-\lambda & 1 \\ 1 & 2-\lambda \end{pmatrix}$$

$$\begin{aligned} \det(A - \lambda I) &= (2-\lambda)(2-\lambda) - (1)(1) \\ 0 &= (2-\lambda)^2 - 1 \\ 1 &= (2-\lambda)^2 \\ \pm 1 &= 2 - \lambda \end{aligned}$$

Esto produce dos autovalores:

- $\lambda_1 = 2 - 1 = 1$
- $\lambda_2 = 2 - (-1) = 3$

2. Encontrar Autovectores: *Para cada autovalor, se resuelve* $(A - \lambda I)\mathbf{v} = \mathbf{0}$.
Para $\lambda_1 = 1$*:*

$$(A - 1I)\mathbf{v}_1 = \mathbf{0} \implies \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Esto lleva a la ecuación $x + y = 0$*. Cualquier vector que cumpla esto es un autovector. Tomando* $y = 1$*, se obtiene el autovector* $\mathbf{v}_1 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

Para $\lambda_2 = 3$*:*

$$(A - 3I)\mathbf{v}_2 = \mathbf{0} \implies \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Esto lleva a la ecuación $-x + y = 0$*. Tomando* $y = 1$*, se obtiene el autovector* $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

A.8. Matrices especiales en computación cuántica

No todas las matrices cuadradas son aptas para describir operaciones cuánticas. Las operaciones físicas imponen restricciones severas sobre las matrices que las representan. Esto da lugar a dos tipos de matrices de importancia capital: hermíticas y unitarias.

Para definirlas, primero se debe introducir una operación fundamental: la traspuesta conjugada.

A.8.1. Matriz transpuesta conjugada

La operación traspuesta conjugada (denotada por el símbolo †, conocido como "daga") es la generalización de la transposición simple al dominio de los números complejos.

La traspuesta conjugada de una matriz A, denotada $A^\dagger$, se calcula en dos pasos:

1. **Transposición** (A^T)**:** Se intercambian las filas por las columnas.

2. **Conjugación Compleja (A^*):** Se toma el conjugado complejo de cada elemento de la matriz (es decir, se cambia el signo de la parte imaginaria, $a + bi \to a - bi$).

La traspuesta conjugada $A^\dagger$ es el resultado de aplicar ambos pasos (en cualquier orden):

$$A^\dagger = (A^T)^* = (A^*)^T$$

Ejemplo A.8.1. *Si se tiene la matriz C:*

$$C = \begin{pmatrix} 1 & 2+i \\ 3i & 4 \end{pmatrix}$$

Su transpuesta C^T es:

$$C^T = \begin{pmatrix} 1 & 3i \\ 2+i & 4 \end{pmatrix}$$

Su traspuesta conjugada $C^\dagger$ (transponiendo y conjugando) es:

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

Con esta operación definida, se pueden introducir los tipos de matrices más importantes.

A.8.2. Matrices hermíticas

Las matrices hermíticas son la generalización de los números reales al mundo de las matrices. (Un número real es hermítico porque $z = z^*$ si y solo si z es real).

Definición A.8.1 (Matriz Hermítica)**.** *Una matriz cuadrada H se denomina hermítica si es igual a su propia traspuesta conjugada:*

$$H = H^\dagger$$

Esto implica que sus elementos deben cumplir $h_{ij} = h^*_{ji}$. En particular, los elementos de la diagonal ($i = j$) deben ser reales, ya que $h_{ii} = h^*_{ii}$.

Nota

Las matrices hermíticas son fundamentales porque representan observables, es decir, cualquier propiedad del sistema que se pueda medir (como la energía, la posición o el spin).
Esto se debe a una propiedad matemática crucial: *Todos los autovalores de una matriz hermítica son números reales.*
Esto es una necesidad física, ya que cuando se mide una propiedad, el resultado (el autovalor) debe ser un número real, como $+1$ o $-1/2$, y no un número complejo.

A.8.3. Matrices unitarias

Las matrices unitarias son la generalización de los números complejos de módulo 1 (como $e^{i\theta}$) al mundo de las matrices.

Definición A.8.2 (Matriz Unitaria)**.** *Una matriz cuadrada U se denomina unitaria si su matriz inversa es igual a su matriz traspuesta conjugada:*

$$U^{-1} = U^{\dagger}$$

De forma equivalente, una matriz es unitaria si multiplicarla por su traspuesta conjugada da la identidad:

$$UU^{\dagger} = U^{\dagger}U = I$$

Nota

Todos los autovalores de matrices unitarias tienen módulo 1, es decir, si λ es autovalor de U, entonces $\exists\theta \in [0, 2\pi)$ tal que:

$$\lambda = e^{i\theta}$$

Esta es una propiedad de gran utilidad.