Linear Algebra

Berkant Ustaoğlu

CRYPTOLOUNGE.NET

Vector Spaces

Vector space over complex numbers

Definition (vector space)

A *vector space* over $\mathbb{C}$ is a non-empty set $\mathbf{V}$ of elements called *vectors* along with two operations

- *vector addition* denoted by $\oplus$

$$\oplus : \mathbf{V} \times \mathbf{V} \to \mathbf{V}$$

- *scalar vector multiplication* denoted by $\odot$

$$\odot : \mathbb{C} \times \mathbf{V} \to \mathbf{V}$$

Definition (vector space (con't))

1. $\forall \vec{v} \in \mathbf{V}, \forall \vec{u} \in \mathbf{V},$
$$\vec{u} \oplus \vec{v} = \vec{v} \oplus \vec{u}$$
2. $\forall \vec{v} \in \mathbf{V}, \forall \vec{u} \in \mathbf{V}, \forall \vec{w} \in \mathbf{V},$
$$(\vec{u} \oplus \vec{v}) \oplus \vec{w} = \vec{u} \oplus (\vec{v} \oplus \vec{w})$$
3. $\exists ! \vec{0} \in \mathbf{V}, \forall \vec{v} \in \mathbf{V}$
$$\vec{0} \oplus \vec{v} = \vec{v}$$
4. $\forall \vec{v} \in \mathbf{V}, \exists ! \vec{u} \in \mathbf{V}$
$$\vec{v} \oplus \vec{u} = \vec{0}$$
   often $\vec{u} = \vec{-v}$

Vector space over complex numbers

Definition (vector space)

5. $\forall \vec{v} \in \mathbf{V}$

$$1 \odot \vec{v} = \vec{v}$$

6. $\forall \vec{v} \in \mathbf{V}$, $\forall \alpha \in \mathbb{C}$, $\forall \beta \in \mathbb{C}$

$$\alpha \odot (\beta \odot \vec{v}) = (\alpha\beta) \odot \vec{v}$$

7. $\forall \vec{v} \in \mathbf{V}$, $\forall \vec{u} \in \mathbf{V}$, $\forall \alpha \in \mathbb{C}$

$$\alpha \odot (\vec{u} \oplus \vec{v}) = (\alpha \odot \vec{v}) \oplus (\alpha \odot \vec{u})$$

8. $\forall \vec{v} \in \mathbf{V}$, $\forall \alpha \in \mathbb{C}$, $\forall \beta \in \mathbb{C}$

$$(\alpha + \beta) \odot \vec{v} = (\alpha \odot \vec{v}) \oplus (\beta \odot \vec{v})$$

Examples and counterexamples

- Euclidean space
- $\mathbb{C}^2$ with standard operations
- matrices
- planes through origin in 3D
- all functions defined in an interval $[a, b]$
- vectors with integer components
- vectors with components where $x \neq y$
- continuous functions defined in an interval $[a, b]$

Examples and counterexamples

- all sequences
- all sequences with finite support
- polynomials
- polynomials of degree at most n $\mathbf{P}_n$
- a set with single element z where $\alpha z = z$ and $z + z = z$; here z is the zero vector
- polynomials that evaluate to 1 at 2
- $\{a\cos x + b\sin x \mid a, b \in \mathbb{C}\}$

Crazy Vector Space[1]

$$\mathbf{V} = \left\{ \left(\begin{array}{c} x \\ y \end{array} \right) \mid x, y \in \mathbb{C} \right\}$$ with:

vector addition

$$\left(\begin{array}{c} x_1 \\ y_1 \end{array} \right) \oplus \left(\begin{array}{c} x_2 \\ y_2 \end{array} \right) = \left(\begin{array}{c} x_1 + x_2 - 4 \\ y_1 + y_2 - 3 \end{array} \right)$$

scalar vector multiplication

$$\alpha \odot \left(\begin{array}{c} x \\ y \end{array} \right) = \left(\begin{array}{c} \alpha x - 4\alpha + 4 \\ \alpha y - 3\alpha + 3 \end{array} \right)$$

---

[1] credit: R. A. Breezer

Verifications: preliminary

1. $\mathbf{V}$ is non-empty
2. $\oplus$ is closed
3. $\odot$ is closed

Axiom 1

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 - 4 \\ y_1 + y_2 - 3 \end{pmatrix}$$

$$= \begin{pmatrix} x_2 + x_1 - 4 \\ y_2 + y_1 - 3 \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

Axiom 2

$$\left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right] \oplus \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 - 4 \\ y_1 + y_2 - 3 \end{pmatrix} \oplus \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}$$

$$= \begin{pmatrix} [x_1 + x_2 - 4] + x_3 - 4 \\ [y_1 + y_2 - 3] + y_3 - 3 \end{pmatrix} = \begin{pmatrix} x_1 + [x_2 + x_3 - 4] - 4 \\ y_1 + [y_2 + y_3 - 3] - 3 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 + x_3 - 4 \\ y_2 + y_3 - 3 \end{pmatrix} = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \left[\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}\right]$$

Axiom 3

$$\exists! \vec{0} \in \mathbf{V}, \forall \vec{v} \in \mathbf{V} : \vec{0} \oplus \vec{v} = \vec{v}$$

want $\begin{pmatrix} s \\ t \end{pmatrix}$ s.t. $\begin{pmatrix} s \\ t \end{pmatrix} \oplus \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$ for any $\begin{pmatrix} x \\ y \end{pmatrix}$

$$\begin{pmatrix} s \\ t \end{pmatrix} \oplus \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} s + x + 4 \\ t + y + 3 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

so

$$\begin{aligned} s + x - 4 &= x & \Rightarrow s &= 4 \\ t + y - 3 &= y & \Rightarrow t &= 3 \end{aligned}$$

Axiom 3

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix} \oplus \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 + x - 4 \\ 3 + y - 3 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Thus

$$\vec{0} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

Axiom 4

$$\forall \vec{v} \in \mathbf{V}, \exists! \vec{u} \in \mathbf{V} : \vec{v} + \vec{u} = \vec{0}$$

Given $\begin{pmatrix} x \\ y \end{pmatrix}$ want unique $\begin{pmatrix} z \\ w \end{pmatrix}$ such that

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \oplus \begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} x+z-4 \\ y+w-3 \end{pmatrix}$$

$$\begin{aligned} x+z-4 &= 4 \quad &\Rightarrow z = 8-x \\ y+w-3 &= 3 \quad &\Rightarrow w = 6-y \end{aligned}$$

Axiom 4: example

Given $\begin{pmatrix} 9 \\ 2 \end{pmatrix}$ additive inverse is $\begin{pmatrix} -1 \\ 4 \end{pmatrix}$

$$\begin{pmatrix} 9 \\ 2 \end{pmatrix} \oplus \begin{pmatrix} -1 \\ 4 \end{pmatrix} = \begin{pmatrix} 9-1-4 \\ 2+4-3 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

Axiom 5

$$\forall \vec{v} \in \mathbf{V}, 1 \odot \vec{v} = \vec{v}$$

Recall

$$\alpha \odot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x - 4\alpha + 4 \\ \alpha y - 3\alpha + 3 \end{pmatrix}$$

Then

$$1 \odot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \times x - 4 \times 1 + 4 \\ 1 \times y - 3 \times 1 + 3 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Axiom 6

$$\forall \vec{v} \in \mathbf{V}, \forall \alpha \in \mathbb{C}, \forall \beta \in \mathbb{C} : \alpha \odot (\beta \odot \vec{v}) = (\alpha\beta) \odot \vec{v}$$

$$\alpha \odot \left[\beta \odot \begin{pmatrix} x \\ y \end{pmatrix} \right] = \alpha \odot \begin{pmatrix} \beta x - 4\beta + 4 \\ \beta y - 3\beta + 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha(\beta x - 4\beta + 4) - 4\alpha + 4 \\ \alpha(\beta y - 3\beta + 3) - 3\alpha + 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha\beta x - 4\alpha\beta + 4 \\ \alpha\beta y - 3\alpha\beta + 3 \end{pmatrix} = (\alpha\beta) \odot \begin{pmatrix} x \\ y \end{pmatrix}$$

Axiom 7

$$\forall \vec{v} \in \mathbf{V}, \forall \vec{u} \in \mathbf{V}, \forall \alpha \in \mathbb{C}, \alpha \odot (\vec{v} \oplus \vec{u}) = (\alpha \odot \vec{v}) \oplus (\alpha \odot \vec{u})$$

$$\alpha \odot \left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right] = \alpha \odot \begin{pmatrix} x_1 + x_2 - 4 \\ y_1 + y_2 - 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha(x_1 + x_2 - 4) - 4\alpha + 4 \\ \alpha(y_1 + y_2 - 3) - 3\alpha + 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha x_1 + \alpha x_2 - 4\alpha - 4\alpha + 4 \pm 4 \\ \alpha y_1 + \alpha y_2 - 3\alpha - 3\alpha + 3 \pm 3 \end{pmatrix}$$

Axiom 7

$$\forall \vec{v} \in \mathbf{V}, \forall \vec{u} \in \mathbf{V}, \forall \alpha \in \mathbb{C}, \alpha \odot (\vec{v} \oplus \vec{u}) = (\alpha \odot \vec{v}) \oplus (\alpha \odot \vec{u})$$

$$\alpha \odot \left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right]$$

$$= \begin{pmatrix} \alpha x_1 + \alpha x_2 - 4\alpha - 4\alpha + 4 + 4 - 4 \\ \alpha y_1 + \alpha y_2 - 3\alpha - 3\alpha + 3 + 3 - 3 \end{pmatrix}$$

$$= \begin{pmatrix} (\alpha x_1 - 4\alpha + 4) + (\alpha x_2 - 4\alpha + 4) - 4 \\ (\alpha y_1 - 3\alpha + 3) + (\alpha y_2 - 3\alpha + 3) - 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha x_1 - 4\alpha + 4 \\ \alpha y_1 - 3\alpha + 3 \end{pmatrix} \oplus \begin{pmatrix} \alpha x_2 - 4\alpha + 4 \\ \alpha y_2 - 3\alpha + 3 \end{pmatrix}$$

Axiom 7

$$\forall \vec{v} \in \mathbf{V}, \forall \vec{u} \in \mathbf{V}, \forall \alpha \in \mathbb{C}, \alpha \odot (\vec{v} \oplus \vec{u}) = (\alpha \odot \vec{v}) \oplus (\alpha \odot \vec{u})$$

$$\alpha \odot \left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right]$$

$$= \begin{pmatrix} \alpha x_1 - 4\alpha + 4 \\ \alpha y_1 - 3\alpha + 3 \end{pmatrix} \oplus \begin{pmatrix} \alpha x_2 - 4\alpha + 4 \\ \alpha y_2 - 3\alpha + 3 \end{pmatrix}$$

$$= \left[\alpha \odot \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \right] \oplus \left[\alpha \odot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right]$$

Axiom 8

$$\forall \vec{v} \in \mathbf{V}, \forall \alpha \in \mathbb{C}, \forall \beta \in \mathbb{C}, (\alpha + \beta) \odot \vec{v} = (\alpha \odot \vec{v}) \oplus (\beta \odot \vec{v})$$

$$(\alpha + \beta) \odot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (\alpha + \beta)x - 4(\alpha + \beta) + 4 \\ (\alpha + \beta)y - 3(\alpha + \beta) + 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha x + \beta x - 4\alpha - 4\beta + 4 \\ \alpha y + \beta y - 3\alpha - 3\beta + 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha x - 4\alpha + 4 + \beta x - 4\beta + 4 - 4 \\ \alpha y - 3\alpha + 3 + \beta y - 3\beta + 3 - 3 \end{pmatrix}$$

Axiom 8

$$\forall \vec{v} \in \mathbf{V}, \forall \alpha \in \mathbb{C}, \forall \beta \in \mathbb{C}, (\alpha + \beta) \odot \vec{v} = (\alpha \odot \vec{v}) \oplus (\beta \odot \vec{v})$$

$$(\alpha + \beta) \odot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x - 4\alpha + 4 + \beta x - 4\beta + 4 - 4 \\ \alpha y - 3\alpha + 3 + \beta y - 3\beta + 3 - 3 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha x - 4\alpha + 4 \\ \alpha y - 3\alpha + 3 \end{pmatrix} \oplus \begin{pmatrix} \beta x - 4\beta + 4 \\ \beta y - 3\beta + 3 \end{pmatrix}$$

$$= \left[\alpha \odot \begin{pmatrix} x \\ y \end{pmatrix}\right] \oplus \left[\beta \odot \begin{pmatrix} x \\ y \end{pmatrix}\right]$$

multiplication by zero

Theorem

$$\forall \vec{v} \in \mathbf{V}, 0\vec{v} = \vec{0}$$

CVS example

$$0 \odot \begin{pmatrix} 9 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \times 9 \\ 0 \times 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

CVS example

$$0 \odot \begin{pmatrix} 9 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \times 9 - 4 \times 0 + 4 \\ 0 \times 2 - 3 \times 0 + 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

multiplication by negative one

Theorem

$$\forall \vec{v} \in \mathbf{V}, (-1)\vec{v} = \vec{-v}$$

CVS example

$$(-1) \odot \begin{pmatrix} 9 \\ 2 \end{pmatrix} = \begin{pmatrix} (-1) \times 9 \\ (-1) \times 2 \end{pmatrix} = \begin{pmatrix} -9 \\ -2 \end{pmatrix} \neq \begin{pmatrix} -1 \\ 4 \end{pmatrix}$$

CVS example

$$(-1) \odot \begin{pmatrix} 9 \\ 2 \end{pmatrix} = \begin{pmatrix} (-1) \times 9 - 4 \times (-1) + 4 \\ (-1) \times 2 - 3 \times (-1) + 3 \end{pmatrix} = \begin{pmatrix} -1 \\ 4 \end{pmatrix}$$

CVS example

$$0 \odot \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \times 4 - 4 \times 0 + 4 \\ 0 \times 3 - 3 \times 0 + 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

scalar times the zero vector

Theorem

$$\forall \alpha \in \mathbb{C} : \alpha\vec{0} = \vec{0}$$

CVS example

$$\alpha \odot \vec{0} = \begin{pmatrix} \alpha \times 0 \\ \alpha \times 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

CVS example

$$\alpha \odot \vec{0} = \alpha \odot \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} \alpha \times 4 - 4 \times \alpha + 4 \\ \alpha \times 3 - 3 \times \alpha + 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$