Linear Algebra

Berkant Ustaoğlu

CRYPTOLOUNGE.NET

Linear dependence and independence

Linear combination

Definition (linear combination)

A vector $\vec{u}$ is said to be *linear combination* of $\vec{v_1}, \vec{v_2}, \ldots, \vec{v_n}$ if there exists constants $\alpha_1, \ldots, \alpha_n$ such that

$$\vec{u} = \sum_{i=1}^{n} \alpha_i \vec{v_i} = \alpha_1 \vec{v_1} + \cdots + \alpha_n \vec{v_n}$$

2×2 matrices

$$\begin{pmatrix} -1 & -12 \\ 2 & 21 \end{pmatrix} = 2\begin{pmatrix} -2 & -10 \\ 0 & 5 \end{pmatrix} + 3\begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} + (-1)\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

2×2 matrices

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \alpha \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} + \beta \begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix} + \gamma \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 2 \end{pmatrix} = 2\begin{pmatrix} 1 \\ 0 \end{pmatrix} + 5\begin{pmatrix} 0 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$= 2\begin{pmatrix} 1 \\ 0 \end{pmatrix} + (-2)\begin{pmatrix} 0 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix} \neq \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

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

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

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

CVS example

$$\left[0 \odot \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] \oplus \left[0 \odot \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right] = \begin{pmatrix} 0 \times 1 - 4 \times 0 + 4 \\ 0 \times 0 - 3 \times 0 + 3 \end{pmatrix} \oplus \begin{pmatrix} 0 \times 0 - 4 \times 0 + 4 \\ 0 \times 0 - 3 \times 0 + 3 \end{pmatrix}$$

$$= \begin{pmatrix} 4 \\ 3 \end{pmatrix} \oplus \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

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

Linear combination

Theorem

If $\vec{u}$ is linear combination of a subset of $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_k$ then it is linear combination of all the vectors.

2×2 matrices

$$\begin{aligned} \begin{pmatrix} -1 & -12 \\ 2 & 21 \end{pmatrix} = & 2 \begin{pmatrix} -2 & -10 \\ 0 & 5 \end{pmatrix} + 3 \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} \\ & + (-1) \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + 0 \begin{pmatrix} 4 & 2 \\ 2 & -5 \end{pmatrix} \\ & + 0 \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix} + (-1) \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

CVS example

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \left[\frac{-1}{2} \odot \begin{pmatrix} 12 \\ 9 \end{pmatrix}\right] \oplus \left[\frac{1}{3} \odot \begin{pmatrix} -8 \\ -6 \end{pmatrix}\right]$$

$$= \left[\frac{-1}{2} \odot \begin{pmatrix} 12 \\ 9 \end{pmatrix}\right] \oplus \left[\frac{1}{3} \odot \begin{pmatrix} -8 \\ -6 \end{pmatrix}\right] \oplus \left[1 \odot \begin{pmatrix} 4 \\ 3 \end{pmatrix}\right]$$

$$\begin{aligned}
8 =& 5\sin^2 x + 3\sin^2 x^2 + 5\cos^2 x + 3\cos^2 x^2 \\
=& 5\sin^2 x + 3\sin^2 x^2 + 9\sin^2 x^3 - 9\sin^2 x^4 \\
& + 5\cos^2 x + 3\cos^2 x^2 + 9\cos^2 x^3 - 9\cos^2 x^4
\end{aligned}$$

Linear combination

Theorem

If $\vec{u}$ *is linear combination of* $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_k$ *and each* $\vec{v}_i$ *is a linear combination of* $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_s$ *then* $\vec{u}$ *is a linear combination of* $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_s$*.*

$\mathbb{C}^4$ example

$$\begin{pmatrix} -1 \\ 4 \\ 2 \\ 6 \end{pmatrix} = 2 \begin{pmatrix} -2 \\ 7 \\ 0 \\ 2 \end{pmatrix} + 3 \begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix} + (-1) \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} -2 \\ 7 \\ 0 \\ 2 \end{pmatrix} = -2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 7 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + 2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$\mathbb{C}^4$ example

$$\begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - 3 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + 1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$\mathbb{C}^4$ example

$$\begin{pmatrix} -1 \\ 4 \\ 2 \\ 6 \end{pmatrix} = -\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 4\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + 6\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

CVS example

$$
\begin{aligned}
\begin{pmatrix} 6 \\ 7 \end{pmatrix} &= \left[2 \odot \begin{pmatrix} 8 \\ 11 \end{pmatrix}\right] \oplus \left[2 \odot \begin{pmatrix} 1 \\ -3 \end{pmatrix}\right] \\
&= \left(2 \odot \left[(-4) \odot \begin{pmatrix} 3 \\ 1 \end{pmatrix}\right]\right) \oplus \left(2 \odot \left[3 \odot \begin{pmatrix} 3 \\ 1 \end{pmatrix}\right]\right) \\
&= \left((2 \times (-4)) \odot \begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \oplus \left((2 \times 3) \odot \begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\
&= (2 \times (-4) + 2 \times 3) \odot \begin{pmatrix} 3 \\ 1 \end{pmatrix} \\
&= -2 \odot \begin{pmatrix} 3 \\ 1 \end{pmatrix}
\end{aligned}
$$

Linear dependence

Definition (linear (in)dependence)

Let $\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}$ be a set of vectors. If

$$a_1\vec{v_1} + a_2\vec{v_2} + \cdots + a_k\vec{v_k} = \vec{0} \quad \Rightarrow \quad a_1 = a_2 = \cdots = a_k = 0$$

then the vectors $\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}$ are called *linearly independent* otherwise they are *linearly dependent*.

$\mathbb{C}^4$ example

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} x_1 + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} x_2 + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} x_3 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} x_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Linear dependence

Theorem

The standard basis vectors are linearly independent, in other words the columns and rows of I are linearly independent.

$\mathbb{C}^2$ example

Are $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$ linearly dependent?

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix} x_1 + \begin{pmatrix} 1 \\ 1 \end{pmatrix} x_2 + \begin{pmatrix} 2 \\ 2 \end{pmatrix} x_3 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

- $x_1 = x_2 = x_3 = 0$ is solution
- $x_1 = 0$, $x_2 = 1$ and $x_3 = -1$ is another solution

$\mathbb{C}^2$ example

Are $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ linearly dependent?

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix} x_1 + \begin{pmatrix} 1 \\ 1 \end{pmatrix} x_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

1. $x_1 = 0$ and $x_2 = 0$ is the *only* solution

CVS example

Are $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ linearly dependent?

$$\left[\alpha \odot \begin{pmatrix} 4 \\ 3 \end{pmatrix}\right] \oplus \left[\beta \odot \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right] = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

look at

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

- $\alpha = 0$ and $\beta = 0$ is a solution
- $\alpha = 7$ and $\beta = 0$ is a solution

CVS example

Is $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ linearly dependent?

$$\alpha \odot \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

look at

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

- $\alpha = 0$ is a solution
- $\alpha = 7$ is a solution

$\mathbb{C}^2$ example

Is $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ linearly dependent?

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

- $\alpha = 0$ is the *only* solution

functions

- Are the functions $p_0(x) = x^0$, $p_1(x) = x^1$ and $p_2(x) = x^2$ linearly dependent or independent?
- Are the functions $5x^0$, $\sin^2 x$ and $3\cos^2 x$ linearly dependent or independent?

Linear dependence

Theorem

Let $\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}$ *be collection of vectors. If* $k = 1$ *the system of vectors is linearly dependent if and only if* $\vec{v_1} = \vec{0}$*.*

Linear dependence

Theorem

Let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_k$ *be collection of vectors. If for some* $1 \leq i \leq k$ *we have that* $\vec{v}_i = \vec{0}$ *then the system of vectors is linearly dependent.*

Linear dependence

Theorem

Let $\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}$ be collection of vectors. If for some $1 \leq i \neq j \leq k$ we have that $\vec{v_i} = \vec{v_j}$ then the system of vectors is linearly dependent.

Linear dependence

Theorem

Let $\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}$ be collection of linearly dependent vectors and $k > 1$. Then there is an index i such that $\vec{v_i}$ can be written as a linear combination of the remaining vectors.

A sufficient condition

Theorem

Let $A : \vec{a_1}, \vec{a_2}, \ldots, \vec{a_s}$ *and* $B : \vec{b_1}, \vec{b_2}, \ldots, \vec{b_k}$ *be two system of vectors. Suppose that for each* $1 \leq i \leq s$ *we have that* $\vec{a_i}$ *is a linear combination of* $\vec{b_1}, \vec{b_2}, \ldots, \vec{b_k}$. *Suppose also* $s > k$ *then the vectors in* A *are linearly dependent.*

$\vec{b}$'s independent

$$\begin{pmatrix} 2 & 0 \\ -3 & 3 \end{pmatrix} = 2\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - 3\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + 3\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 4 & 4 \end{pmatrix} = 2\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 4\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + 4\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 2\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + 2\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 3\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$\vec{b}$s dependent

$$\begin{pmatrix} 8 & 8 \\ 3 & 3 \end{pmatrix} = 2\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} - 3\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + 3\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 3 \\ 6 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + 4\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 5 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + 3\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + 2\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 3 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + 2\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix} = 2\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} - 3\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} +0\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix} = 0\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + 0\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} +3\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$s \geq k$

$$\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} = 2\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} - 3\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad +0\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 4 \\ 4 & 0 \end{pmatrix} = 0\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + 0\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad +3\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Basis

Definition (basis)

Let $\mathbf{V}$ be a vector space, the set of vectors $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_d\}$ is a *basis* for $\mathbf{V}$ if every vector in $\mathbf{V}$ can be represented as a linear combination of the vectors in $\mathbf{B}$ and the vectors in $\mathbf{B}$ are linearly independent.

2×2 matrices

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

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

$$\begin{pmatrix} 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Different basis

Theorem

Let $\mathbf{B}_1$ *and* $\mathbf{B}_2$ *be two distinct basis for a vector space* $\mathbf{V}$*. Then the number of vectors in* $\mathbf{B}_1$ *and* $\mathbf{B}_2$ *is the same.*

Dimension

Definition (dimension)

Let $\mathbf{B}$ be a basis for a vector space $\mathbf{V}$, then the size of $\mathbf{B}$ is called the *dimension* of $\mathbf{V}$.

Different basis

Theorem

Let $\vec{e_1}, \ldots, \vec{e_n}$ be linearly independent. Suppose

1. $\vec{u} = a_1\vec{e_1} + \cdots + a_n\vec{e_n}$ *and*
2. $\vec{u} = b_1\vec{e_1} + \cdots + b_n\vec{e_n}$.

Then

$$a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$$