Course 8

Matrix of a list of vectors, matrix of a linear map

Prof. dr. Septimiu Crivei

Applications: Hill cipher, image transformations

We present the Hill cipher, which was the first application of linear algebra to cryptography, based on operations with invertible matrices.

We analyze image transformations: rotation of 2D-images with an angle around the origin.

Matrix of a list of vectors I

Definition

Let V be a vector space over K, $B = (v_1, \ldots, v_n)$ a basis of V and $X = (u_1, \ldots, u_m)$ a list of vectors in V. Let

$$\begin{cases} u_1 = a_{11}v_1 + a_{12}v_2 + \cdots + a_{1n}v_n \\ u_2 = a_{21}v_1 + a_{22}v_2 + \cdots + a_{2n}v_n \\ \dots\dots\dots\dots\dots\dots \\ u_m = a_{m1}v_1 + a_{m2}v_2 + \cdots + a_{mn}v_n \end{cases}$$

be the unique writings of the vectors in X as linear combinations of vectors of the basis B, for some $a_{ij} \in K$.

Matrix of a list of vectors II

Definition

The *matrix of the list of vectors* X in the basis B is the matrix having as its rows the coordinates of the vectors in X in the basis B, that is,

$$[X]_B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Example

Consider the canonical basis $B = (e_1, e_2, e_3, e_4)$ and the list $X = (u_1, u_2, u_3)$ in the canonical real vector space $\mathbb{R}^4$, where

$$\begin{cases} u_1 & = (1, 2, 3, 4) \\ u_2 & = (5, 6, 7, 8) \\ u_3 & = (9, 10, 11, 12) \end{cases}.$$

Since the coordinates of a vector in the canonical basis are just its components, we get

$$[X]_B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}.$$

Dimension of the generated subspace

Theorem

Let V be a vector space over K, $B = (v_1, \ldots, v_n)$ a basis of V and $X = (u_1, \ldots, u_m)$ a list of vectors in V having the matrix A in the basis B. Then:
(i) $\dim\langle X\rangle = \mathrm{rank}(A)$.
(ii) A basis of $\langle X\rangle$ is the list of non-zero row-vectors $(c_1, \ldots, c_r)$ of an echelon form C equivalent to A.

Example

Let us determine the dimensions of the subspaces S, T, $S+T$ and $S\cap T$ of the canonical real vector space $\mathbb{R}^4$, where

$$S = \langle(-3,5,-1,1),(-1,1,0,1),(1,1,-1,-3)\rangle\,,$$
$$T = \langle(1,0,2,0),(2,1,-1,2)\rangle\,.$$

We have $\dim S = \dim T = 2$. Furthermore, $S+T=\langle S\cup T\rangle$. We write the matrix of $S\cup T$ in the canonical basis and we have

$$\begin{pmatrix} -3 & 5 & -1 & 1 \\ -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -3 \\ 1 & 0 & 2 & 0 \\ 2 & 1 & -1 & 2 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 1 & -1 & -3 \\ 0 & -1 & 3 & 3 \\ 0 & 0 & 5 & 4 \\ 0 & 0 & 0 & 33 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then $\dim(S+T)=4$ and a basis of $S+T$ consists of the non-zero row-vectors from the echelon form, that is, $((1,1,-1,-3),(0,-1,3,3),(0,0,5,4),(0,0,0,33))$. Finally, $\dim(S\cap T) = \dim S + \dim T - \dim(S+T) = 2+2-4 = 0$.

Matrix of a vector

It is more convenient to define it as a column-matrix in order to avoid formulas involving transposes.

Definition

Let V be a vector space over K, $v \in V$ and $B = (v_1, \ldots, v_n)$ a basis of V. If $v = k_1 v_1 + \cdots + k_n v_n$ $(k_1, \ldots, k_n \in K)$ is the unique writing of v as a linear combination of the vectors of the basis B, then the *matrix* of v in the basis B is $[v]_B = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$.

Example

Consider the vector $v = (1, 2, 3)$ in the canonical real vector space $\mathbb{R}^3$, and let E be the canonical basis. Then $[v]_E = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

Definition

Let $f : V \to V'$ be a K-linear map, $B = (v_1, \dots, v_n)$ a basis of V and $B' = (v'_1, \dots, v'_m)$ a basis of V'. Then we can uniquely write the vectors in $f(B)$ as linear combinations of the vectors of the basis B', say

$$\begin{cases} f(v_1) = a_{11}v'_1 + a_{21}v'_2 + \cdots + a_{m1}v'_m \\ f(v_2) = a_{12}v'_1 + a_{22}v'_2 + \cdots + a_{m2}v'_m \\ \dots\dots\dots\dots\dots\dots \\ f(v_n) = a_{1n}v'_1 + a_{2n}v'_2 + \cdots + a_{mn}v'_m \end{cases}$$

for some $a_{ij} \in K$.

Matrix of a linear map II

Definition

Then the *matrix of the K-linear map f* in the bases B and B' is the matrix having as its columns the coordinates of the vectors of $f(B)$ in the basis B', that is,

$$[f]_{BB'} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

If $V = V'$ and $B = B'$, then we simply denote $[f]_B = [f]_{BB'}$.

We have to emphasize that we put the coordinates on the columns of the matrix of a linear map and not on the rows as we did for the matrix of a list of vectors.

Example

Consider the $\mathbb{R}$-linear map $f : \mathbb{R}^4 \to \mathbb{R}^3$ defined by

$$f(x, y, z, t) = (x + y + z, y + z + t, z + t + x), \ \forall (x, y, z, t) \in \mathbb{R}^4 .$$

Let $E = (e_1, e_2, e_3, e_4)$ and $E' = (e'_1, e'_2, e'_3)$ be the canonical bases in $\mathbb{R}^4$ and $\mathbb{R}^3$ respectively. Since

$$\begin{cases} f(e_1) = f(1,0,0,0) = (1,0,1) = e'_1 + e'_3 \\ f(e_2) = f(0,1,0,0) = (1,1,0) = e'_1 + e'_2 \\ f(e_3) = f(0,0,1,0) = (1,1,1) = e'_1 + e'_2 + e'_3 \\ f(e_4) = f(0,0,0,1) = (0,1,1) = e'_2 + e'_3 \end{cases}$$

it follows that the matrix of f in the bases E and E' is

$$[f]_{EE'} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} .$$

Property of the matrix of a linear map I

Theorem

Let $f : V \to V'$ be a K-linear map, $B = (v_1, \ldots, v_n)$ a basis of V, $B' = (v'_1, \ldots, v'_m)$ a basis of V' and $v \in V$. Then

$$[f(v)]_{B'} = [f]_{BB'} \cdot [v]_B \, .$$

Proof. Let $[f]_{BB'} = (a_{ij}) \in M_{m,n}(K)$. Let

$$v = \sum_{j=1}^{n} k_j v_j ,$$

$$f(v) = \sum_{i=1}^{m} k'_i v'_i$$

for some $k_i, k'_i \in K$.

Property of the matrix of a linear map II

On the other hand, using the definition of the matrix of f in the bases B and B', we have

$$f(v) = f\left(\sum_{j=1}^{n} k_j v_j\right) = \sum_{j=1}^{n} k_j f(v_j)$$
$$= \sum_{j=1}^{n} k_j \left(\sum_{i=1}^{m} a_{ij} v'_i\right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} k_j\right) v'_i\,.$$

But the writing of $f(v)$ as a linear combination of the vectors of the basis B' is unique, hence we must have $k'_i = \sum_{j=1}^{n} a_{ij} k_j$ for every $i \in \{1, \ldots, m\}$. Therefore, $[f(v)]_{B'} = [f]_{BB'} \cdot [v]_B$. $\square$

Theorem

Let $f : V \to V'$ be a K-linear map. Then $\mathrm{rank}(f) = \mathrm{rank}([f]_{BB'})$, *where B and B' are any bases of V and V' respectively.*

Proof. Let $B = (v_1, \dots, v_n)$ and $[f]_{BB'} = A$. We have:

$$\begin{aligned}\mathrm{rank}(f) &= \dim(\mathrm{Im} f) = \dim f(V) = \dim f(\langle v_1, \dots, v_n\rangle) \\ &= \dim\langle f(v_1), \dots, f(v_n)\rangle = \mathrm{rank}(\ A^T) = \mathrm{rank}(A) = \mathrm{rank}([f]_{BB'})\end{aligned}$$

Now take some other bases $B_1 = (u_1, \dots, u_n)$ of V and B_1' of V' and denote $[f]_{B_1B_1'} = A_1$. Then

$$\begin{aligned}\mathrm{rank}([f]_{B_1B_1'}) &= \mathrm{rank}(A_1) = \mathrm{rank}(\ A_1^T) = \dim\langle f(u_1), \dots, f(u_n)\rangle \\ &= \dim(\mathrm{Im} f) = \dim\langle f(v_1), \dots, f(v_n)\rangle = \mathrm{rank}([f]_{BB'}).\end{aligned}$$

Example

Consider the $\mathbb{R}$-linear map $f : \mathbb{R}^4 \to \mathbb{R}^3$ defined by

$$f(x, y, z, t) = (x + y + z, y + z + t, z + t + x), \ \forall (x, y, z, t) \in \mathbb{R}^4 .$$

Let $E = (e_1, e_2, e_3, e_4)$ and $E' = (e'_1, e'_2, e'_3)$ be the canonical bases in $\mathbb{R}^4$ and $\mathbb{R}^3$ respectively. By a previous example it follows that

$$[f]_{EE'} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} .$$

Now it follows that $\mathrm{rank}(f) = \mathrm{rank}([f]_{EE'}) = 3$.

Connection between linear maps and matrices I

Theorem

Let V, V' and V'' be vector spaces over K with $\dim V = n$, $\dim V' = m$ *and* $\dim V'' = p$ *and let* $B = (v_1, \dots, v_n)$, $B' = (v'_1, \dots, v'_m)$ *and* $B'' = (v''_1, \dots, v''_p)$ *be bases of V, V' and V'' respectively. Then* $\forall f, g \in \mathrm{Hom}_K(V, V')$, $\forall h \in \mathrm{Hom}_K(V', V'')$ *and* $\forall k \in K$, *we have*

$$[f+g]_{BB'} = [f]_{BB'} + [g]_{BB'} \,,$$
$$[kf]_{BB'} = k \cdot [f]_{BB'} \,,$$
$$[h \circ f]_{BB''} = [h]_{B'B''} \cdot [f]_{BB'} \,.$$

Proof. Let $[f]_{BB'} = (a_{ij}) \in M_{m,n}(K)$, $[g]_{BB'} = (b_{ij}) \in M_{m,n}(K)$ and $[h]_{B'B''} = (c_{ki}) \in M_{pm}(K)$. Then

$$f(v_j) = \sum_{i=1}^{m} a_{ij} v'_i \,, \quad g(v_j) = \sum_{i=1}^{m} b_{ij} v'_i \,, \quad h(v'_i) = \sum_{k=1}^{p} c_{ki} v''_k$$

Connection between linear maps and matrices II

$\forall j \in \{1, \ldots, n\}$, $\forall i \in \{1, \ldots, m\}$. Then $\forall k \in K$, $\forall j \in \{1, \ldots, n\}$ we have

$$(f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^{m} a_{ij} v'_i + \sum_{i=1}^{m} b_{ij} v'_i = \sum_{i=1}^{m} (a_{ij} + b_{ij}) v'_i \,,$$

$$(kf)(v_j) = kf(v_j) = k \cdot \left(\sum_{i=1}^{m} a_{ij} v'_i \right) = \sum_{i=1}^{m} (k a_{ij}) v'_i \,,$$

hence $[f+g]_{BB'} = [f]_{BB'} + [g]_{BB'}$ and $[kf]_{BB'} = k \cdot [f]_{BB'}$.
Finally, $\forall j \in \{1, \ldots, n\}$ we have

$$(h \circ f)(v_j) = h(f(v_j)) = h\left(\sum_{i=1}^{m} a_{ij} v'_i \right) = \sum_{i=1}^{m} a_{ij} h(v'_i)$$

$$= \sum_{i=1}^{m} a_{ij} \left(\sum_{k=1}^{p} c_{ki} v''_k \right) = \sum_{k=1}^{p} \sum_{i=1}^{m} (c_{ki} a_{ij}) v''_k \,,$$

hence $[h \circ f]_{BB''} = [h]_{B'B''} \cdot [f]_{BB'}$. $\square$

Theorem

Let V and V' be vector spaces over K with $\dim V = n$ and $\dim V' = m$, and let B and B' be bases of V and V' respectively. Then the map

$$\varphi : \mathrm{Hom}_K(V, V') \to M_{m,n}(K), \quad \varphi(f) = [f]_{BB'}\,, \ \forall f \in \mathrm{Hom}_K(V, V')$$

is an isomorphism of vector spaces.

Proof. We have seen that $\mathrm{Hom}_K(V, V')$ is a vector space over K with respect to the following addition and scalar multiplication: $\forall f, g \in \mathrm{Hom}_K(V, V')$ and $\forall k \in K$, $f + g, k \cdot f \in \mathrm{Hom}_K(V, V')$, where $\forall x \in V$,

$$(f+g)(x) = f(x) + g(x)\,,$$
$$(kf)(x) = kf(x)\,.$$

Also, $M_{m,n}(K)$ is a vector space over K. It follows that φ is a K-linear map.
Finally, let us prove that φ is bijective. Consider $B = (v_1, \ldots, v_n)$ and $B' = (v'_1, \ldots, v'_m)$. Let $f, g \in \mathrm{Hom}_K(V, V')$ be such that $\varphi(f) = \varphi(g)$. Then $[f]_{BB'} = [g]_{BB'} = (a_{ij}) \in M_{m,n}(K)$, hence

$$f(v_j) = a_{1j}v'_1 + a_{2j}v'_2 + \cdots + a_{mj}v'_m = g(v_j)\,,$$

$\forall j \in \{1, \ldots, n\}$. We have seen that two K-linear maps are equal if and only if they have the same values at all vectors of a basis.
Hence $f = g$, which shows that φ is injective. Now let $A = (a_{ij}) \in M_{m,n}(K)$, seen as a list of column-vectors $(a^1, \ldots, a^n)$,

An isomorphism of vector spaces III

where $a^j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$. Define a K-linear map $f : V \to V'$ on the basis of the domain by

$$f(v_j) = a_{1j}v'_1 + \cdots + a_{mj}v'_m \,,$$

$\forall j \in \{1, \ldots, n\}$. Then $\varphi(f) = [f]_{BB'} = (a_{ij}) = A$. Thus, φ is surjective. $\square$

Remarks

This isomorphism allows us to work with matrices instead of linear maps, which is much easier from a computational point of view.

Under this isomorphism, the kernel and the image of a linear map $f : V \to V'$, where V and V' are vector spaces over K with $\dim(V) = n$ and $\dim(V') = m$, and bases B and B' respectively, correspond to the so-called *null space* and to the *column space* of its associated matrix $A = [f]_{BB'} \in M_{m,n}(K)$ respectively.

Thus, the *null space* of A consists of vectors $x \in K^n$ such that $Ax = 0$, while the *column space* of A consists of all linear combinations of the columns of A.

A vector $b \in K^m$ belongs to the column space of A if and only if the system $Ax = b$ has a solution.

By the First Dimension Theorem it follows that the sum of the dimensions of the null space and the column space of A equals n.

Theorem

Let V be a vector space over K with $\dim V = n$, and let B be a basis of V. Then the map

$$\varphi : \mathrm{End}_K(V) \to M_n(K), \quad \varphi(f) = [f]_B\,,\ \forall f \in \mathrm{End}_K(V)$$

is an isomorphism of vector spaces and of rings.

Proof. Note that $(\mathrm{End}_K(V), +, \circ)$ and $(M_n(K), +, \cdot)$ are rings. The required isomorphisms follow by the above theorem. □

Corollary

Let $f \in \mathrm{End}_K(V)$. Then $f \in \mathrm{Aut}_K(V) \Longleftrightarrow \det([f]_B) \neq 0$, where B is any basis of V.

Proof. $f \in \mathrm{Aut}_K(V) \Leftrightarrow f$ is invertible in $(\mathrm{End}_K(V), +, \circ) \Leftrightarrow [f]_B$ is invertible in $(M_n(K), +, \cdot) \Leftrightarrow \det([f]_B) \neq 0$. □

Extra: Hill cipher I

Let $n \in \mathbb{N}^*$ and consider the canonical vector space $V = \mathbb{Z}_2^n$ over $\mathbb{Z}_2$ with canonical basis E. The vectors of V may be identified with n-bit binary strings. Suppose that Alice needs to send an n-bit plaintext $p \in \mathbb{Z}_2^n$ to Bob.

Hill cipher:

1. (*Key establishment*) Alice and Bob randomly choose an invertible matrix $K \in M_n(\mathbb{Z}_2)$ as a key, and compute its inverse.
2. (*Encryption*) Alice computes the ciphertext c according to the formula $[c]_E^T = [p]_E^T \cdot K$.
3. (*Decryption*) Bob computes the plaintext p according to the formula $[p]_E^T = [c]_E^T \cdot K^{-1}$.

The Hill cipher is nowadays insecure.

Extra: Hill cipher II

Alice wants to send the message $p = (1, 0, 1) \in \mathbb{Z}_2^3$ to Bob.
Alice and Bob agree on the matrix K and its inverse:

$$K = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in M_3(\mathbb{Z}_2), \quad K^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_2).$$

Alice encrypts the message by computing the ciphertext c as:

$$[c]_E^T = [p]_E^T \cdot K = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}.$$

Bob decrypts the message by computing the plaintext p as:

$$[p]_E^T = [c]_E^T \cdot K^{-1} = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}.$$

Extra: Image transformations I

Suppose that we have a 2D-image that we want to rotate counterclockwise with θ degrees around the origin. By such a rotation, the point of coordinates $(1,0)$ becomes the point of coordinates $(\cos\theta, \sin\theta)$, while the point of coordinates $(0,1)$ becomes the point of coordinates $(-\sin\theta, \cos\theta)$.
We look for an $\mathbb{R}$-linear map $f : \mathbb{R}^2 \to \mathbb{R}^2$ satisfying the following conditions:

$$f(1,0) = (\cos\theta, \sin\theta),$$
$$f(0,1) = (-\sin\theta, \cos\theta).$$

Recall that every linear map is determined by its values at the elements of a basis (the canonical basis in our case). Hence the matrix of the linear map f in the canonical basis E of the canonical real vector space $\mathbb{R}^2$ is:

$$[f]_E = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

For any point $v = (x, y) \in \mathbb{R}^2$ of a 2D-image, its corresponding point in the rotated image is computed as $f(v) = (x', y') \in \mathbb{R}^2$, where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = [f(v)]_E = [f]_E \cdot [v]_E = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

For instance, for a counterclockwise rotation of 90^0 around the origin one has the matrix:

$$[f]_E = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$