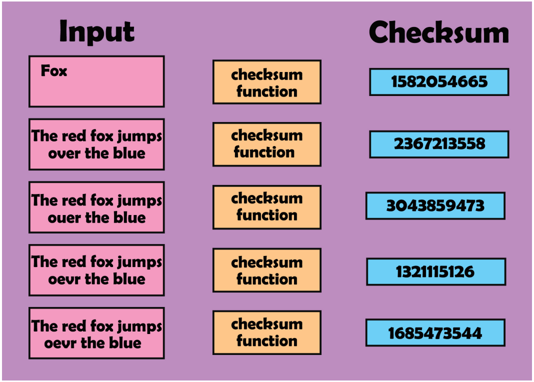
Course 6

Dimension

Prof. dr. Septimiu Crivei

Application: checksum function

Following [Klein], we present a checksum function for detecting corrupted files.



Theorem (Steinitz Theorem, Exchange Theorem)

Let V be a vector space over K, $X = (x_1, \ldots, x_m)$ a linearly independent list of vectors of V and $Y = (y_1, \ldots, y_n)$ a system of generators of V. Then:
(i) $m \leq n$.
(ii) m vectors of Y can be replaced by the vectors of X obtaining again a system of generators for V.

In Steinitz Theorem not necessarily the first m vectors of Y can be replaced by the m vectors of X.

Theorem

Any two bases of a vector space have the same number of elements.

Proof. [...]

Definition

Let V be a vector space over K. Then the number of elements of any of its bases is called the *dimension of V* and is denoted by $\dim_K V$ or simply by $\dim V$.

If $V = \{0\}$, then V has the basis $\emptyset$ and $\dim V = 0$.

(a) Let K be a field and $n \in \mathbb{N}^*$. Then $\dim_K K^n = n$.

(b) We have seen that the subspaces of $\mathbb{R}^3$ are $\{(0,0,0)\}$, any line containing the origin, any plane containing the origin and $\mathbb{R}^3$. Their dimensions are 0, 1, 2 and 3 respectively.

(c) Let K be a field and $n \in \mathbb{N}$. Then $\dim K_n[X] = n + 1$.

(d) Let K be a field. Then $\dim M_2(K) = 4$.
More generally, if $m, n \in \mathbb{N}$, $m, n \geq 2$, then $\dim M_{m,n}(K) = m \cdot n$.

(e) Consider the subspace

$$S = \{(x, y, z) \in \mathbb{R}^3 \mid x - y - z = 0\} = \langle (1,1,0), (1,0,1) \rangle$$

of the canonical real vector space $\mathbb{R}^3$. Since the vectors $(1,1,0)$ and $(1,0,1)$ are linearly independent, it follows that $B = ((1,1,0), (1,0,1))$ is a basis of S. Hence $\dim S = 2$.

(f) We have $\dim_{\mathbb{C}} \mathbb{C} = 1$ and $\dim_{\mathbb{R}} \mathbb{C} = 2$.

Theorem

Let V be a vector space over K. The following are equivalent:
(i) $\dim V = n$.
(ii) The maximum no. of linearly independent vectors in V is n.
(iii) The minimum no. of generators for V is n.

Proof. $(i) \Longrightarrow (ii)$ Assume that $\dim V = n$. Let $B = (v_1, \dots, v_n)$ be a basis of V. Then B is linearly independent in V. Since B is a system of generators for V, any linearly independent list in V must have at most n elements by Steinitz Theorem.

$(ii) \Longrightarrow (i)$ Assume (ii). Let $B = (v_1, \dots, v_m)$ be a basis of V and let $(u_1, \dots, u_n)$ be a linearly independent list in V. Since B is linearly independent, we have $m \leq n$ by hypothesis. Since B is a system of generators for V, we have $n \leq m$ by Steinitz Theorem. Hence $m = n$ and consequently $\dim V = n$.

$(i) \Longleftrightarrow (iii)$ Homework.

When linear independence = system of generators

Theorem

Let V be a vector space over K with $\dim V = n$ *and* $X = (u_1, \ldots, u_n)$ *a list of vectors in V. Then*

X *is linearly independent in* $V \iff X$ *is a system of generators for* V.

Proof. [...]

Corollary

Let $n \in \mathbb{N}$, $n \geq 2$. Then n vectors in K^n form a basis of the canonical vector space K^n if and only if thety are linearly independent if and only if the determinant consisting of their components is non-zero.

Completion to a basis

Theorem

Any linearly independent list of vectors in a vector space can be completed to a basis of the vector space.

Proof. [...]

Corollary

Let V be a vector space over K and $S \leq V$. Then:
(i) Any basis of S is a part of a basis of V.
(ii) $\dim S \leq \dim V$.
(iii) $\dim S = \dim V \iff S = V$.

Proof. Homework.

Example

The completion of a linearly independent list to a basis of the vector space is not unique.

The list (e_1, e_2), where $e_1 = (1, 0, 0)$ and $e_2 = (0, 1, 0)$, is linearly independent in the canonical real vector space $\mathbb{R}^3$.

It can be completed to the canonical basis of the space, namely (e_1, e_2, e_3), where $e_3 = (0, 0, 1)$.

On the other hand, since $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$, in order to obtain a basis of the space it is enough to add to our list a vector v_3 such that (e_1, e_2, v_3) is linearly independent. For instance, we may take $v_3 = (1, 1, 1)$, since the determinant consisting of the components of the three vectors is non-zero.

Decomposition theorem

Theorem

Let V be a vector space over K and let $S \leq V$. Then there exists $\overline{S} \leq V$ such that $V = S \oplus \overline{S}$. In particular,

$$\dim V = \dim S + \dim \overline{S}.$$

Proof. Let $(u_1, \ldots, u_m)$ be a basis of S. Then it can be completed to a basis $B = (u_1, \ldots, u_m, v_{m+1}, \ldots, v_n)$ of V. We consider

$$\overline{S} = \langle v_{m+1}, \ldots, v_n \rangle$$

and we prove that $V = S \oplus \overline{S}$ [...]. □

Remark

This is an important property of a vector space, allowing to split it in "smaller" subspaces, that can be studied easier and are used to derive information about the entire vector space.

Complement of a subspace

Definition

Let V be a vector space over K and $S \leq V$. Then a subspace $\overline{S}$ of V such that

$$V = S \oplus \overline{S}$$

is called a *complement of S in V*.

Note that a subspace may have more than one complement.

Consider the subspace $S = \langle e_1, e_2 \rangle$ of the canonical real vector space $\mathbb{R}^3$, where $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$. Then clearly (e_1, e_2) is a basis of S.

It can be completed to a basis of $\mathbb{R}^3$, with the vector $e_3 = (0, 0, 1)$ or with the vector $v_3 = (1, 1, 1)$. Following the proof of the above theorem, a complement in V of the subspace $S = \langle e_1, e_2 \rangle$ is $\langle e_3 \rangle$ or $\langle v_3 \rangle$.

Theorem

Let V and V' be vector spaces over K. Then

$$V \simeq V' \Longleftrightarrow \dim V = \dim V' .$$

Proof. $\boxed{\Longrightarrow}$ If $f : V \to V'$ is a K-isomorphism and $B = (v_1, \dots, v_n)$ is a basis of V, then one shows that $B' = f(B) = (f(v_1), \dots, f(v_n))$ is a basis of V'. [...]
$\boxed{\Longleftarrow}$ If $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ are bases of V and V' respectively, define a function $f : V \to V'$ in the following way. For every $v = k_1 v_1 + \cdots + k_n v_n \in V$ (where $k_1, \dots, k_n \in K$ are uniquely determined), define $f(v) = k_1 v'_1 + \cdots + k_n v'_n$. One proves that f is a K-isomorphism. [...]

Uniqueness of n-dimensional vector spaces up to isomorphism

We may immediately deduce the following result.

Theorem

Any vector space V over K with $\dim V = n$ *is isomorphic to the canonical vector space K^n over K.*

This result is a very important structure theorem, saying that, up to an isomorphism, *any finite dimensional vector space over K is, in fact, the canonical vector space K^n over K.* For instance, we have the K-isomorphisms $K_n[X] \simeq K^{n+1}$ and $M_{m,n}(K) \simeq K^{mn}$. Now we have an explanation why we have used so often the canonical vector spaces: not only because the operations are very nice and easily defined, but they are, up to an isomorphism, the only types of finite dimensional vector spaces.

Definition

Let $f : V \to V'$ be a K-linear map. Then:
(1) $\dim(\mathrm{Ker} f)$ is called the *nullity* of f, and is denoted by $\mathrm{null}(f)$.
(2) $\dim(\mathrm{Im} f)$ is called the *rank* of f, and is denoted by $\mathrm{rank}(f)$.

Next we present an important theorem relating the nullity and the rank of a linear map.

Theorem (First Dimension Theorem)

Let $f : V \to V'$ be a K-linear map. Then

$$\dim V = \dim(\mathrm{Ker} f) + \dim(\mathrm{Im} f)\,.$$

In other words, $\dim V = \mathrm{null}(f) + \mathrm{rank}(f)$.

Second Dimension Theorem

Theorem (Second Dimension Theorem)

Let V be a vector space over K and let S, T be subspaces of V. Then

$$\dim S + \dim T = \dim(S \cap T) + \dim(S + T)\,.$$

Corollary

Let V be a vector space over K, and let S and T be subspaces of V such that $V = S \oplus T$. Then

$$\dim V = \dim S + \dim T\,.$$

Extra: Checksum function I

Definition

Let $u = (x_1, \dots, x_n), v = (y_1, \dots, y_n) \in K^n$. Then the *dot-product* (or *scalar product*) of u and v is the scalar

$$u \cdot v = x_1 y_1 + \dots + x_n y_n \in K.$$

We give an example of a checksum function which may detect accidental random corruption of a file during transmission or storage.

Let $a_1, \dots, a_{64} \in \mathbb{Z}_2^n$ and let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^{64}$ be the $\mathbb{Z}_2$-linear map defined by

$$f(v) = (a_1 \cdot v, \dots, a_{64} \cdot v).$$

Suppose that v is a "file". We model corruption as the addition of a random vector $e \in \mathbb{Z}_2^n$ (the error), so the corrupted version of the file is $v + e$. We look for a formula for the probability that the corrupted file has the same checksum as the original file.

The checksum of the original file v is taken to be $f(v)$, hence the checksum of the corrupted file $v+e$ is $f(v+e)$.
The original file and the corrupted file have the same checksum if and only if $f(v) = f(v+e)$ if and only if $f(e) = 0$ if and only if $e \in \operatorname{Ker} f$.
Every vector space V over the field $\mathbb{Z}_2$ with $\dim V = n$ is isomorphic to $\mathbb{Z}_2^n$, hence it has 2^n vectors. In particular, $\operatorname{Ker} f$ has 2^k vectors, where $k = \dim(\operatorname{Ker} f)$.
If the error is chosen according to the uniform distribution, the probability that $v+e$ has the same checksum as v is the following:

$$P = \frac{\text{number of vectors in } \operatorname{Ker} f}{\text{number of vectors in } \mathbb{Z}_2^n} = \frac{2^k}{2^n}.$$

One may show that $\dim(\operatorname{Im} f)$ is close to $\min(n, 64)$. So if we choose $n \geq 64$, we may assume that $\dim(\operatorname{Im} f) = 64$.

Extra: Checksum function III

By the First Dimension Theorem, we have

$$k = \dim(\operatorname{Ker} f) = \dim \mathbb{Z}_2^n - \dim(\operatorname{Im} f) = n - 64.$$

Hence

$$P = \frac{2^{n-64}}{2^n} = \frac{1}{2^{64}},$$

and thus there is only a very tiny chance that the change is undetected.