Vector space V over a field K

$+ : V \times V \to V$

$\cdot : K \times V \to V$

$(V, +)$ Abelian group

$(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$

$\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$

$\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$

$1 \cdot v = v$

Standard example of a vector space is K^n with

$$(x_i)_{i=1,\dots,n} + (y_i)_{i=1,\dots,n} := (x_i + y_i)_{i=1,\dots,n}$$

$$\alpha \cdot (x_i)_{i=1,\dots,n} := (\alpha x_i)_{i=1,\dots,n}$$

For a K-vector space V a subset U is called a vector subspace or a linear subspace if

$0 \in U$ and $\alpha a + \beta b \in U$ for all $\alpha, \beta \in K$ and all $a, b \in U$.

In other words, U is a vector subspace of V if the operations of V can be restricted to U in the sense

$+ : U \times U \to U$ as a restriction of $+ : V \times V \to V$

and $\cdot : K \times U \to U$ a a restriction of $\cdot : K \times V \to V$

In this case, U becomes a vector space under these restricted operations.

One way to define a vector subspace of K^n is by $U = \{x \in K^n : Ax = 0\}$, where $A \in K^{m \times n}$.

This is one possible way to fix a linear code, when K is a finite field. We introduced our Hamming code this way.

One can also generate vector subspaces by a system of vectors, say, if we have $a_1, \ldots, a_\ell \in V$ then

$\alpha_1 a_1 + \ldots + \alpha_\ell a_\ell$ is called the linear combination of $a_1, \ldots, a_\ell$ with the coefficients $\alpha_1, \ldots, \alpha_\ell \in K$.

The set of all such linear combinations is called the linear hull or the K-linear hull or the span or the K-span of $a_1, \ldots, a_\ell$:

$$\underbrace{\text{lin}_K}(a_1, \ldots, a_\ell) := \{ \alpha_1 a_1 + \ldots + \alpha_\ell a_\ell : \alpha_1, \ldots, \alpha_\ell \in K \}$$

the subscript K can be omitted if it's clear what K is.

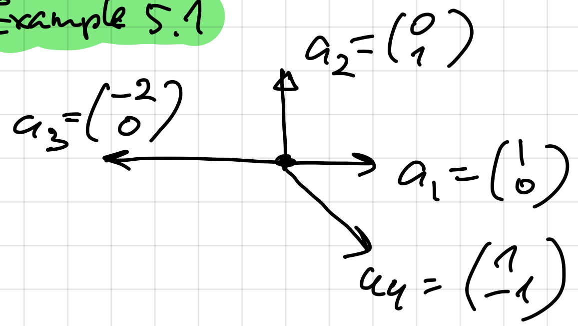
When we generate linear hulls, there might be vectors in the system that are redundant. Because of this we introduce the notion of linear independence.

Vectors $a_1, \ldots, a_\ell$ are called linearly independent if the linear combination $\alpha_1 a_1 + \ldots + \alpha_\ell a_\ell$ can only be zero when all of the coefficients $\alpha_1, \ldots, \alpha_\ell \in K$ are zero. In this case, ℓ is said to be the dimension of $\text{lin}(a_1, \ldots, a_\ell)$.

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$ are called the standard unit vectors in K^n.

If $a_1, \ldots, a_\ell$ are linearly independent, then $a_1, \ldots, a_\ell$ is called a <u>basis</u> of $\text{lin}(a_1, \ldots, a_\ell)$.

Example 5.1

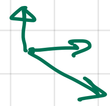


$K = \mathbb{R}$

$$\mathrm{lin}(a_1, a_2, a_3, a_4) = \mathbb{R}^2$$

linear dependencies among the vectors $a_1, \dots, a_4$ (some of the linear dependencies)

$$-a_1 + a_2 + a_4 = 0$$



$$2a_1 + a_3 = 0$$

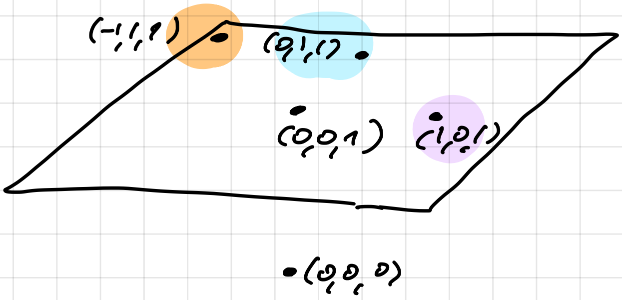
$$2a_2 + a_3 + 2a_4 = 0$$

$$\underbrace{\mathrm{lin}(a_2, a_3)}_{\text{basis}} = \underbrace{\mathrm{lin}(a_1, a_2)}_{\text{basis}} = \underbrace{\mathrm{lin}(a_3, a_4)}_{\text{basis}} = \underbrace{\mathrm{lin}(a_2, a_4)}_{\text{basis}} = \underbrace{\mathrm{lin}(a_1, a_4)}_{\text{basis}} = \mathbb{R}^2$$

Example 5.2

$$a_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad a_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad a_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \quad \text{in } K = \mathbb{R}.$$

$$\underbrace{\mathrm{lin}(a_1, a_2, a_3)}_{\text{basis, but how do we see this?}} = \mathbb{R}^3?$$



Let's solve $\alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

$$\alpha_1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \alpha_3 \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Updownarrow$$

$$\begin{cases} \alpha_1 - \alpha_3 = 0 \\ \alpha_2 + \alpha_3 = 0 \\ \alpha_1 + \alpha_2 + \alpha_3 = 0 \end{cases}$$

$$\begin{cases} \alpha_1 = \alpha_3 \\ \alpha_2 = -\alpha_3 \\ \alpha_1 + \alpha_2 + \alpha_3 = 0 \end{cases}$$

$$\begin{cases} \alpha_1 = \alpha_3 \\ \alpha_2 = -\alpha_3 \\ \alpha_3 - \alpha_3 + \alpha_3 = 0 \end{cases} \iff \alpha_1 = \alpha_2 = \alpha_3 = 0$$

$\Rightarrow$ a_1, a_2, a_3 linearly independent.

Example 5.3 $K = \mathbb{Z}_2$

$$a_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

linearly dependent, because

$$a_1 + a_2 + a_3 = 0$$

Let us look at all $\alpha_1, \alpha_2, \alpha_3 \in K$ such that $\alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 = 0$. That is, let's look at the set:

$$\{ (\alpha_1, \alpha_2, \alpha_3) \in K^3 : \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 = 0 \}$$

$$= \{ 000, 111 \}$$

$$\mathrm{lin}(a_1, a_2, a_3) = K^2$$

a_1, a_2 Basis

a_1, a_3 Basis

a_2, a_3 Basis.

5.1.2 Linear maps and matrices

For K-vector space V and W a map $F: V \to W$ is called K-linear or (just) linear if

$$F(\alpha a + \beta b) = \alpha F(a) + \beta F(b)$$

for all $\alpha, \beta \in K$ and $a, b \in V$.

A matrix $A \in K^{m \times n}$ gives rise to the linear map $x \mapsto Ax$ from $K^n \to K^m$ and the linear map $u \mapsto uA$ from $K^m \to K^n$.

The set $im(F) = \{ F(v) : v \in V \}$ is called the image of F. It is a vector subspace of W.

The set $ker(F) = \{ v \in V : F(v) = 0 \}$ is called the kernel of F. This is a vector subspace of V.

Example 5.4 $K = \mathbb{Z}_2$.

$$ENC(x_1, x_2) = (x_1, x_2, x_1, x_2, x_1 + x_2)$$

this is a linear map.

$im(ENC) = \{ 00000, 10101, 01011, 11110 \}$

This is a K-vector subspace of K^5.

$$\mathrm{ENC}(x_1, x_2) = x_1 \cdot \mathrm{ENC}(1,0) + x_2 \cdot \mathrm{ENC}(0,1)$$
$$= x_1 \cdot (1,0,1,0,1) + x_2 \cdot (0,1,0,1,1)$$

$$\Rightarrow \mathrm{im}(\mathrm{ENC}) = \mathrm{lin}\,(\underbrace{(1,0,1,0,1), (0,1,0,1,1)})$$

linearly independent, which you can see by looking at their first two components:

$(1, 0, \ldots\ldots)$
$(0, 1, \ldots\ldots)$

Remark 5.5 In the language of linear maps, one can give a linear code in two ways: as the image of a linear map and as a kernel of a linear map.

Theorem 5.6 For a linear map $F: V \to W$ on K-vector spaces V and W with V having a finite dimension $n \in \mathbb{N}$ one has

$$\dim \mathrm{im}(F) = \dim(V) - \dim(\ker(F)),$$

or in other way:

$$\dim \mathrm{im}(F) + \dim \ker(F) = \dim(V).$$