Non-linearity for $\mathbb{F}_2$-vector spaces

Giacomo Borin

Università di Trento

October 22, 2021

Definition

Given two vector spaces V and W on the **same field** k, then a map

$$f : V \to W$$

is linear if for all $v, v' \in V$ and $\lambda, \mu \in k$ we have

$$f(\lambda v + \mu v') = \lambda f(v) + \mu f(v')$$

An example of linear map are the combinations of sum and multiplication by a constant, like for the matrices.

Question

Then why are the sum $\mod n$ for $n \neq 2$ not linear?

The problem is that we are passing from string of bits (vectors in $\mathbb{F}_2^k$) to numbers in $\mathbb{Z}_n$ (this is an object that we mathematicians use to indicate the numbers modulo n : $\{0, 1, \ldots, n-1\}$).

So in this way we **change the defining field** between the two spaces, against the definition.

A simple example

Let's see with a simple example of how this can create problems.

Example function

Consider the map f that sends a string of three bits $(b_0, b_1, b_2) = v \in \mathbb{F}_2^3$ to the element:

$$b_0 + b_1 + 2b_2 \mod 4$$

and then converts it to a string of 2 bits $f(v) = (c_0, c_1) \in \mathbb{F}_2^2$

A simple example

First of all we can see with a simple calculation that (sadly or luckly) f is not linear.

Define $s_1 = (1, 1, 0)$ and $s_2 = (0, 1, 1)$, thus $s_1 + s_2 = (1, 0, 1)$, so:

$$
\begin{aligned}
f((1, 1, 0)) &= 1 + 1 + 0 \mod 4 = 2 = (1, 0) \\
f((0, 1, 1)) &= 0 + 1 + 2 \mod 4 = 3 = (1, 1) \\
f((1, 0, 1)) &= 1 + 0 + 2 \mod 4 = 3 = (1, 1)
\end{aligned}
$$

Example

Now we can evaluate

$$f(s_1) + f(s_2) = (1,0) + (1,1) = (0,1)$$

that its different from

$$f(s_1 + s_2) = f((1,0,1)) = (1,1)$$

So f **is not linear**

The function f seems very *regular*, so where is the problem?

The base field

The problem is that part of the computations have been done out of our defining field $\mathbb{F}_2$, observe that the map f pass through 3 steps:

1. We pass from seeing (b_0, b_2, b_2) as bits to seeing them as integers
2. We perform some linear calculations in $\mathbb{Z}_4 = \{\, 0, 1, 2, 3\}$
3. We convert elements of $\{\, 0, 1, 2, 3\}$ to a string of 2 bits.

The first and the third passage cannot be linear since the vector spaces are defined on different fields

Here a simple diagram of the map

$$\mathbb{F}_2^3 \xrightarrow[\text{(not linear)}]{1} \mathbb{Z}_4^3 \xrightarrow{2} \mathbb{Z}_4 \xrightarrow[\text{(not linear)}]{3} \mathbb{F}_2^2$$

Remarks

Remark I

You can also observe that $\mathbb{Z}_4$ is not a field (2 is not invertible) so $\mathbb{Z}_4^3$ is not a vector space, but this is not a problem since mathematicians created objects that preserve a concept of linearity in these cases, called **Ring modules**

Remark II

You should remember from linear algebra that another simple way to lose linearity is to add a non zero constant term c: for example $g : \mathbb{F}_2 \to \mathbb{F}_2$ that maps $b \mapsto b \oplus 1$ is not linear (prove it!)