MATH 525
Section 1.7 - Some Basic Algebra

August 28, 2020

Let $K = \{0, 1\}$ and define two operations on it, $+$ and $\cdot$, as follows:

$$\begin{cases} 0+0=0 \\ 0+1=1 \\ 1+0=1 \\ 1+1=0 \end{cases} \quad \text{and} \quad \begin{cases} 0\cdot 0=0 \\ 0\cdot 1=0 \\ 1\cdot 0=0 \\ 1\cdot 1=1 \end{cases}$$

$+$ and $\cdot$ are addition and multiplication modulo 2. Endowed with these two operations, K becomes a field.

Let n be a positive integer. Then

$$K^n = K \times K \times \cdots \times K = \{(v_1, \ldots, v_n) \mid v_i \in K, i = 1, \ldots, n\}.$$

In K^n, define addition componentwise, that is,

$$(v_1, v_2, \ldots, v_n) + (w_1, w_2, \ldots, w_n) = (v_1 + w_1, v_2 + w_2, \ldots, v_n + w_n),$$

for all $(v_1, v_2, \ldots, v_n), (w_1, w_2, \ldots, w_n) \in K^n$. The $+$ inside the parentheses are addition modulo 2.

Finally, define multiplication by scalar as

$$a \cdot (v_1, v_2, \ldots, v_n) = (av_1, av_2, \ldots, av_n)$$

for all $a \in K$ and for all $(v_1, v_2, \ldots, v_n) \in K^n$.

Endowed with these two operations, K^n becomes a vector space over K (the definition of vector space, normally learned in Linear Algebra, is reviewed on the next slide).

If v is sent and w is received, then $e = v + w$ is called the error pattern or error vector. The nonzero components of e indicate the positions where the errors have occurred. Example: $v = 010100, w = 011101$. Then

$$e = v + w = 001001 \text{ is the error pattern.}$$

Observe that the nonzero components of e indicate the positions where errors have occurred.

Definition (Review of Vector Spaces)

A vector space is a nonempty set V of objects, called vectors, on which are defined two operations, addition and multiplication by scalars[a], subject to the ten rules (axioms) listed below. The axioms must hold for all vectors $\vec{u}$, $\vec{v}$, and $\vec{w}$ in V and for all scalars c and d.

1. The sum of $\vec{u}$ and $\vec{v}$, denoted by $\vec{u} + \vec{v}$, is in V.
2. $\vec{u} + \vec{v} = \vec{v} + \vec{u}$.
3. $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$.
4. There is a zero vector $\vec{0}$ in V such that $\vec{u} + \vec{0} = \vec{u}$.
5. For each $\vec{u}$ in V, there is a vector $-\vec{u}$ in V such that $\vec{u} + (-\vec{u}) = \vec{0}$.
6. The scalar multiple of $\vec{u}$ by c, denoted by $c\vec{u}$, is in V.
7. $c(\vec{u} + \vec{v}) = c\vec{u} + c\vec{v}$.
8. $(c + d)\vec{u} = c\vec{u} + d\vec{u}$.
9. $c(d\vec{u}) = (cd)\vec{u}$.
10. $1\vec{u} = \vec{u}$.

[a] In our case, the scalars are 0 and 1, or the elements of the field $K = \{0, 1\}$.