§1 Lecture 01-08

Definition 1.1. Vector space is a special kind of abelian group that can multiply by scalars. For a general vector space, the scalars are members of a field F, in which case V is called a vector space over F.

§1.1 Codes

Definition 1.2 (Codes)**.** A subset of the field $\mathbb{F}_2^n$

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$$

There are various features you would like a good code to have.

1. Capacity: Cardinality of sigma should be large relative to the cardinality of $\mathbb{F}_2^n$ which is 2^n.

2. Redundancy: Often data is transmitted over noisy channels, so single bits can occasionally be corrupted. One feature you would like to have is being able to detect these corruptions.
   Do this by defining Hamming distance. Let $v, w \in \mathbb{F}_2^n$. $d(v, w) = \#$ of j such that $v_j \neq w_j$.

   $$v = (v_1, \ldots, v_n)$$
   $$w = (w_1, \ldots, w_n)$$

   One bit is flipped you may fall out of sigma which may be detected.
   K-bit error detection. If $v \in \Sigma$, then

   $$\{w | d(v, w) \leq k\} \cap \Sigma = \{v\}$$

3. Computational Efficiency: Algorithms for converting elements of Σ into the acutal data you are trying to communicate should be efficient.

   Definition 1.3. Σ is a linear code if it is a vector subspace of $\mathbb{F}_2^n$. (Closed under addition). All you really have to check if closure under addition.
   Scalar multiplication is really no requirement at all because multiplying by 0 just means Σ must contain 0. And multiplying by 1 just gives you the element back.

§1.2 Function Spaces

Let x be a set, and F a field.
Let $\mathbb{F}(x, F)$ be the set of functions from x to F.

$$f_1, f_2 \in \mathbb{F}, \quad (f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$f \in \mathbb{F}, \quad (\lambda f)(x) = \lambda \cdot f(x)$$

§1.2.1 Linear subspaces of function spaces

1. Function with compact support
   x is a topological space.

Definition 1.4 (Compact Support)**.** $f : x \to$ has compact support if $\exists B \subset x$, B compact, such that $(f(x) = 0)(\forall x \notin B)$

If f_1 is supported on B_1 and f_2 on B_2, then $f_1 + f_2$ is supported on $B_1 \cup B_2$.

Linearly supported is closed under addition. And scalar multiplication as well

Special Case: x has discrete topology. Then compact sets are finite.

$\mathbb{F}_0(x, F)$ is the set of compactly supported F-valued functions on x. $F_0(x, F) \leq F(x, F)$.

§1.3 Linear Transformations

Definition 1.5 (Linear Transformation)**.** A linear transformation from V to W (V, W vector spaces over F) is a function $T : V \to W$ such that $\forall v_1, v_2 \in V$

$$T(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 T(v_1) + \lambda_2 T(v_2)$$

T is group homomorphism with additional feature that it respects scalar multiplication. $T(\lambda v) = \lambda T(v)$

Consequences:

$$T(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 T(v_1) + \cdots + \lambda_n T(v_n)$$

Now we can consider the set of all these linear transformations.

Note 1.6.

1. $\hom_F(V, W)$ represents the set of all linear transformations from V to W (V and W are vector spaces).

2. A linear transformation from V to itself is called endomorphism of V.

$$\mathrm{End}_F(V) = \hom_F(V, V)$$

3. $\hom(V, W)$ is a vector space! (this makes sense because if T_1 and T_2 are linear, so is $\lambda_1 T_1 + \lambda_2 T_2$)

4. $\mathrm{End}(V)$ is also endowed with an internal multiplication in addition to the addition arising from the vector space. The product $T_1 T_2 = T_1 \circ T_2$ or $T_1 T_2(v) = T_1(T_2(v))$. On the other hand you cannot compose elements of $\hom_F(V, W)$.

   Distributive Laws
   Composition of functions is always associative
   But not necesarily commutative.
   $\mathrm{End}(V)$ is a ring and a vector space over the field F!

   Definition 1.7. A vector space over F which is also a ring is called an F-algebra.

A ring R gives rise to two groups, namely

1. $(R, +, 0)$ is an abelian group.

2. $(R^{\times}, \times, 1)$ is a group.

$$\text{End}(V)^{\times} = \text{Aut}_F(V)$$

Note 1.8. Last value in $(R, +, 0)$ indicates the identity element.

Definition 1.9 (Automorphism)**.** An invertible linear transformation from V to V is called an automortphism of V.

Definition 1.10 (Dual Space)**.** Linear transformation from V to F where F is a vector space over itself.

$\hom_F(V, F) = V^*$ is called the dual space of V. We will talk about it in more detail on Monday.