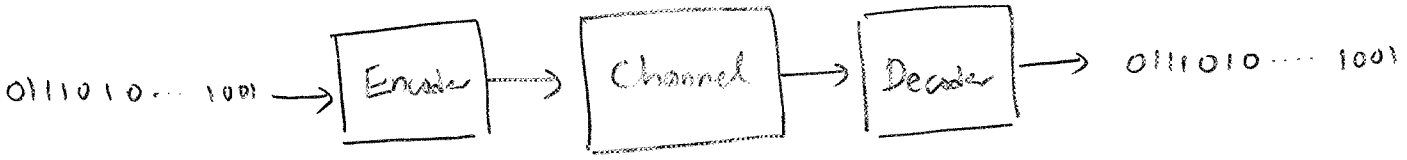
CHAPTER II : LINEAR ALGEBRA (REVIEW)



Encoder takes the stream of input bits and breaks them into blocks of length k bits. It then converts each block of k bits into a coded block of n bits, achieving a transmission rate of $\boxed{\frac{k}{n} = R}$.

To encode k information bits, we need 2^k unique codewords. Each codeword is n-bits long.

If there was no structure in choosing the codewords, then the encoder will need

$2^k \cdot n$ bits long lookup table.

In practice k is large, 500 is common

$\Rightarrow 2^k \cdot n \geq 2^{500} \cdot 500 \approx 10^{152}$ bits

$\approx 3 \times 10^{144}$ Mbits

So we need some structure on our codes. Linearity is one very computationally tractable and mathematically elegant structure. To understand it, we need some mathematical machinery.

Detour : Review of Linear Algebra

Galois Field GF(2)

(Read about Galois online. You will enjoy it)

Galois field GF(2) consists of two elements $\{0,1\}$ and two binary operations

multiplication

$\cdot$	0	1
0	0	0
1	0	1

addition

$+$	0	1
0	0	1
1	1	0

This is, basically, addition & multiplication modulo 2.

Notation

$\mathbb{F} = \{0,1\}$ ← Field

$\mathbb{F}^n = \{0,1\}^n$ ← set of all n-tuples with components from $\mathbb{F}$

Definition : BINARY BLOCK CODES

An (n, M) binary block code $\mathbb{C}$ is a collection of M binary n-tuples over $\mathbb{F}$. For our example $(7,4)$ Hamming code, we have

$$M = 2^4$$
$$n = 7$$

Definition : Rate of Code The rate of (n,M) code $\mathbb{C}$ is defined as

$$R = \frac{\log_2 M}{n}$$

$$R = \frac{4}{7} \text{ for } (7,4) \text{ code}$$

Our next major concept is that vector spaces. It will allow us to manipulate and study string of bits. For example

block of bits
1 0 1 0 ⟶ vector $[1\ 0\ 1\ 0]$

this is a 4-dim vector with elements in GF(2)

$\Rightarrow [1\ 0\ 1\ 0] \in \mathbb{F}^4$

The space of such vectors is called vector space with operations from GF(2) to manipulate the elements of the space.

DEFINITION: VECTOR SPACES

Let $\mathbb{V}$ be the set of elements (vectors) and $\mathbb{F}$ denote a field. Two operations are defined: '+' between the elements of $\mathbb{V}$ and '.' between elements of $\mathbb{F}$ and $\mathbb{V}$. The set $\mathbb{V}$ is called a vector space over the field $\mathbb{F}$ if it satisfies the following conditions:

(1) $\mathbb{V}$ is a commutative group under addition
That means if $v_1, v_2, v_3 \in \mathbb{V}$, then

(a) $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ [associative]

(b) There is an $e \in \mathbb{V}$ such that [identity]
$$e + v_1 = v_1 + e = v_1$$

(c) There is an element v_1' s.t. [inverse]
$$v_1 + v_1' = v_1' + v_1 = e$$

(d) $v_1 + v_2 = v_2 + v_1$ [Commutative]

(2) For an element $a \in \mathbb{F}$ and $v \in \mathbb{V}$
$a \cdot v \in \mathbb{V}$ [Scalar multiplication]

(3) For any $v_1, v_2 \in \mathbb{V}$ and $a, b \in \mathbb{F}$ [distributive laws]
$$a \cdot (v_1 + v_2) = a \cdot v_1 + a \cdot v_2$$
$$(a+b) \cdot v_1 = a \cdot v_1 + b \cdot v_1$$

(4) For any $v \in \mathbb{V}$ and $a, b \in \mathbb{F}$ [associative law]
$$(a \cdot b) \cdot v = a \cdot (b \cdot v)$$

(5) Let 1 be the unit element of $\mathbb{F}$, then for any
$v \in \mathbb{V}$, $1 \cdot v = v$

Example: $\mathbb{F} = \{0,1\}$, $\mathbb{V} = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} : a_i \in \mathbb{F} \right\}$

- vector addition: $(v+w)$ is defined elementwise

$$v = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} \qquad w = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix}$$

$$v+w = \begin{bmatrix} v_1+w_1 \\ v_2+w_2 \\ v_3+w_3 \end{bmatrix}$$ all additions are mod 2, inherited for GF(2)

- scalar multiplication $a \cdot v$ is also elementwise

$$a \cdot v = \begin{bmatrix} a \cdot v_1 \\ a \cdot v_2 \\ a \cdot v_3 \end{bmatrix}$$ everything mod 2

Next we consider another key concept which we will use repeatedly use while studying linear codes.

Theorem (Vector Subspace): Let S be a non-empty subset of $\mathbb{V}$ over a field $\mathbb{F}$. Then S is a subspace of $\mathbb{V}$ if the following are satisfied:

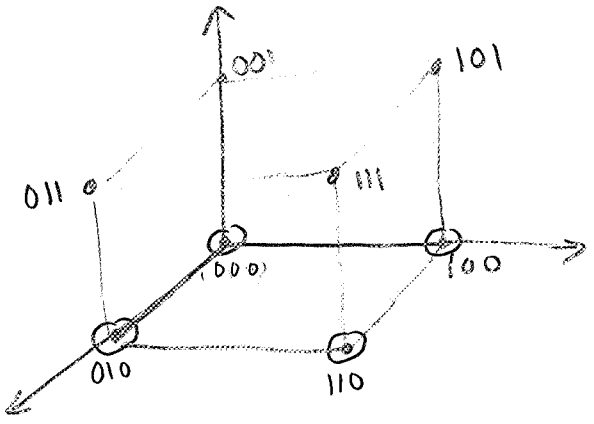
(a) For any two vectors, $v, w \in S$, $v+w \in S$

(b) For any $a \in \mathbb{F}$ and $v \in S$, $a \cdot v \in S$

Basically S is a vector space by itself. It just sits in a bigger vector space.

Example : $\mathbb{F} = \{0, 1\}$, $\mathbb{V} = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} : a_i \in \mathbb{F} \right\}$

$$S = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ 0 \end{bmatrix} : a_i \in \mathbb{F} \right\}$$



• : part of $\mathbb{V}$

⊙ : part of S

You can check that S is a subspace, sum of any two vectors in S is also in S, and scalar products with 0 & 1 are also in S.

There are subtle differences between vector spaces over finite fields (fields which have only finite number of elements) and infinite fields like set of real numbers.

(1) All vectors are their own additive inverses for $\mathbb{F} = GF(2)$
ie. for all $v \in \mathbb{V}$, $v + v = 0$

(In $\mathbb{R}^n$, $v + (-v) = 0$)

(2) Vector spaces over finite fields have only finite number of elements. So additions & multiplications "loopback", so you always stay on those finite set of points.

Let's consider some more properties of vector subspaces.

The first one concerns the linear combination of elements from the vector space.

Theorem: Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space $\mathbb{V}$ over a field $\mathbb{F}$. The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of $\mathbb{V}$.

$$\mathbb{L} = \{ a_0 v_0 + a_1 v_1 + \ldots + a_{k-1} v_{k-1} : a_i \in \mathbb{F} \}$$

is a subspace of $\mathbb{V}$

Related to linear combination of vectors, another important concept will be that of linear dependence & independence.

Definition (Linear Dependence): A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space $\mathbb{V}$ over a field $\mathbb{F}$ is said to be linearly dependent if and only if there exist k scalars $a_1, a_2, \ldots, a_k \in \mathbb{F}$, not <u>all</u> zero

$$\ni \quad a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = \underline{0}$$

Definition (Linear Independence): A set of vectors $v_1, v_2, \ldots, v_k$ are linearly independent if they are not linearly dependent. That is

$$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0$$

Unless $a_1 = a_2 = \ldots = a_k = 0$

Example : The three vectors $[1\ 1\ 0]$, $[0\ 0\ 1]$, $[1\ 1\ 1]$ are linearly dependent

$$1\cdot[1\ 1\ 0] + 1\cdot[0\ 0\ 1] + 1\cdot[1\ 1\ 1] = [0\ 0\ 0]$$

But $[1\ 0\ 0]$, $[0\ 1\ 0]$, $[0\ 0\ 1]$ are linearly independent.

The concept of linear independence immediately leads to the next main concept of basis of a vector space.

Definition (BASIS) : In any vector space or subspace, there exists at least one set B of linearly independent vectors which span the whole space. That is, all vectors in that space can be expressed as a linear combination of vectors in B. The number of vectors in B is the dimension of the vector space.

Example : $\{[1\ 0\ 0], [0\ 1\ 0], [0\ 0\ 1]\}$ & $\{[0\ 1\ 1], [1\ 0\ 1], [1\ 1\ 0]\}$ are both basis for $\mathbb{V} = \mathbb{E}^3$

Definition (Inner Product): Inner product of $\underline{u}$ and $\underline{v}$ is defined as

$$\underline{u} \cdot \underline{v} = u_1 \cdot v_1 + u_2 \cdot v_2 + \cdots + u_n v_n$$

All operations performed modulo-2.

- If $\underline{u} \cdot \underline{v} = 0$, then $\underline{u}, \underline{v}$ are orthogonal
- $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$
- $\underline{v} \cdot (\underline{v} + \underline{w}) = \underline{u} \cdot \underline{v} + \underline{u} \cdot \underline{w}$
- $(a\underline{u}) \cdot \underline{v} = a(\underline{u} \cdot \underline{v})$

The last main concept is that of dual (or null) space

Definition (DUAL SPACE): Let S be a k-dimensional subspace of $\bar{V}$. Define

$$S_d = \{ \underline{v} \in \bar{V} : \underline{v} \cdot \underline{u} = 0 \text{ for all } \underline{u} \in S \}$$

[Exercise: Verify S_d is a subspace of $\bar{V}$]

S_d is called the <u>dual space</u> of S

Theorem (Dimension Theorem): $\dim(S) + \dim(S_d) = \dim(\bar{V})$

MATRICES

The concept of basis, linear independence, orthogonality etc. all come together very nicely when things are arranged in matrices. A $k \times n$ matrix over a field is a rectangular array with k rows & n columns

$$G = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & & & & g_{1,n-1} \\ \vdots & & & & \vdots \\ g_{k-1,1} & & & & g_{k-1,n-1} \end{bmatrix}_{k \times n}$$

where each of the $g_{ij} \in \mathbb{F}$.

You can also arrange the matrix entries by its k rows $\underline{g}_0, \underline{g}_1 \cdots, \underline{g}_{k-1}$ as

$$G = \begin{bmatrix} \underline{g}_0 \\ \underline{g}_1 \\ \vdots \\ \underline{g}_{k-1} \end{bmatrix}$$

each row is a vector of dim $1 \times n$, $\mathbb{F}^n$

Using matrices & vectors, linear combination of vectors can be naturally represented as vector-matrix multiplication

$$\underline{v} \cdot G = [v_0 \; v_1 \cdots v_{k-1}] \begin{bmatrix} \underline{g}_0 \\ \underline{g}_1 \\ \vdots \\ \underline{g}_{k-1} \end{bmatrix}$$

$$= v_0 \underline{g}_0 + v_1 \underline{g}_1 + \cdots + v_{k-1} \underline{g}_{k-1}$$

If $\{\underline{g}_0, \underline{g}_1, \ldots \underline{g}_{k-1}\}$ is a linearly independant set, then the rank of this matrix is k (assuming $k \leq n$). Also the set of vectors span a subspace of dimension k. This subspace is called the ROW SPACE of matrix G, S.

Let S_d be the dual space of row space S. Since S_d is a subspace itself, it will have a dimension $n-k$ (dimension theorem), which implies that there exists $\underline{h}_0, \underline{h}_1, \ldots, \underline{h}_{n-k-1}$ which are linearly independent and span S_d.

Arrange $\underline{h}_0, \underline{h}_1, \ldots, \underline{h}_{n-k-1}$ in a matrix

$$H = \begin{bmatrix} \underline{h}_0 \\ \underline{h}_1 \\ \vdots \\ \underline{h}_{n-k-1} \end{bmatrix}_{(n-k)\times n}$$

Remember the row space of $H = S_d$ is orthogonal/dual of rowspace of $G = S$, we have

$$\underline{g}_i \cdot \underline{h}_j = 0 \quad \forall \; i,j$$

In matrix notation

$$G H^T = 0$$

(H^T: transpose of matrix)

We are now ready to study encoding/decoding of linear codes