20/1/2021    Lecture 4 (Linear Block Codes)

**Recap**

→ Parameters of a block code
$(n, M, d)$ $\mathbb{F}$ – Code alphabet.

→ $R = \frac{1}{n} \log_q |M|$

→ MAP & ML decoders are optimal

→ Error detection and error correction capability of a block code.
Error detection → Upto $d-1$ errors
Error correction $\xrightarrow{\text{Upto}}$ $\lfloor \frac{d-1}{2} \rfloor$ errors

Erasure Correction capability of a code.
→ You can correct upto $(d-1)$ erasures

$$\underline{c} \longrightarrow \boxed{\text{Channel}} \longrightarrow \underline{y}$$

Claim:- Consider a $(n, M, d)$ block code. There exists a decoder for $\mathbb{C}$ which corrects upto $(d-1)$ erasures.

Proof:- Let $t$ be the no. of erasures where $t \leq d-1$.
Pick the codeword which matches $\underline{y}$ in

the $(n-t)$ positions.

If there exists a unique codeword, which satisfies the above condition; then it has to be codeword which was transmitted.

$(n-t)$ positions have to be same for two codewords $\underline{c}_1$ and $\underline{c}_2$

In that case $d_H(\underline{c}_1, \underline{c}_2) \leq t \leq d-1$

By the defn of minimum distance, the above. Case cannot happen.

---

## Linear Block Codes

Motivation: Why linearity is important

→ Block code doesn't have any structure.

→ Encode or decode block codes → Look Up Table.

$k = 50, 100$ → Length of the message

$\underline{M = 2^{50}}$. → Size of the look up table is in general exponential.

→ Efficient encoding and decoding of a code.

# Vector Spaces

A vector space $(V, +, \mathbb{F}, \cdot)$ is a set of vectors, $\mathbb{F}$ is said to a field (elements of $\mathbb{F}$ are also referred to as scalars)

$+ \rightarrow$ vector addition

$\cdot \rightarrow$ scalar multiplication.

(i) $(V, +)$ forms an abelian group $\rightarrow$ closure, commutativity, associativity, additive identity & additive inverse.

$$\underline{a} \in V, \quad \underline{b} \in V, \quad \underline{a}+\underline{b} \in V$$

$$\underline{a}+\underline{b} = \underline{b}+\underline{a}$$

$$\underline{a}+(\underline{b}+\underline{c}) = (\underline{a}+\underline{b})+\underline{c}$$

$$\exists\ \underline{0}, \text{ s.t. } \underline{a}+\underline{0} = \underline{a} \quad \forall\ \underline{a} \in V.$$

For every $\underline{a}$, $\exists(-\underline{a})$ s.t. $\underline{a}+(-\underline{a}) = \underline{0}$

(ii) Closure under scalar multiplication.

$$\alpha \in \mathbb{F}, \quad \underline{a} \in V, \quad \alpha \cdot \underline{a} \in V.$$

(iii) Multiplication with identity.

$$1 \in \mathbb{F}, \quad \underline{a} \in V, \quad 1 \cdot \underline{a} = \underline{a}$$

(iv) Associative under scalar multiplication.

$$c_1(c_2\underline{a}) = (c_1 c_2)\underline{a}$$

(v) Distributive property.

$$c \cdot (\underline{a} + \underline{b}) = c \cdot \underline{a} + c \cdot \underline{b}$$

## Examples of Vector spaces

$\rightarrow (\mathbb{R}^n, +, \mathbb{R}, \cdot)$

$\rightarrow (\mathbb{F}_2^n, +, \mathbb{F}_2, \cdot)$

Vector addition

$\rightarrow (a_1, a_2, \ldots, a_n)$

$(b_1, b_2, \ldots, b_n)$

Component wise addition.

$c \cdot (a_1, \ldots, a_n)$

$= (ca_1, ca_2, \ldots, ca_n)$

$\rightarrow (\mathbb{F}[x], +, \mathbb{F}, \cdot)$

$\downarrow$

vector space of polynomials with coefficients drawn from field $\mathbb{F}$.

$\rightarrow (\mathbb{R}^{m \times n}, +, \mathbb{R}, \cdot)$

## Subspace of a vector space

A subspace of a vector space $(V, +, \mathbb{F}, \cdot)$ is a subset $W$ of $V$ s.t.

$(W, +, \mathbb{F}, \cdot)$ is also a vector space in itself.

# Basis, Dimension of a Vector Space

A basis of a vector space $(V, +, \mathbb{F}, \cdot)$ is a collection $\{\underline{a}_1, \underline{a}_2, \dots\}$ s.t.

(a) the set is linearly independent

(b). the set spans the vector space V.

→ $\{\underline{a}_1, \underline{a}_2, \dots\}$ is said to be linearly independent if.

$$\sum_i c_i \underline{a}_i = \underline{0}_v \implies c_i = 0 \ \forall i$$

→ Every element in the vector space. V. can be written as a linear combination of $\{\underline{a}_1, \underline{a}_2, \dots\}$.

**Basis** → Maximal linearly independent set
→ Minimal Spanning set.

A vector space V can have multiple bases.

If the no. of elements in the basis of a vector is finite, then every basis will have the same no. of elements. → That unique no. is called dimension of v.s.

# Linear Block Codes

A linear block code of blocklength $n$ is any subspace of the vector space $(\mathbb{F}_2^n, +, \mathbb{F}_2, \cdot)$

Block Codes $\rightarrow$ $(n, \underline{M}, d)$ over $\mathbb{F}$.

Linear Block Codes $\rightarrow$ $(n, k, d)$ over $\mathbb{F}$ (here we are just considering $\mathbb{F}_2$)

$k$ is the dimension of a linear block code - is its dimension as a subspace of $(\mathbb{F}_2^n, +, \mathbb{F}_2, \cdot)$.

How are $M$ and $k$ related?

$M = q^k$ where $q$ is the size of the field.

$M = 2^k$ is the case of $\mathbb{F}_2$.

## Minimum Distance of a linear block Code

$$d_{min} = \min_{\substack{\underline{x}, \underline{y} \in \mathbb{C} \\ \underline{x} \neq \underline{y}}} d_H(\underline{x}, \underline{y}).$$

**Lemma:** The minimum distance $d_{min}$ of a linear block Code $\mathbb{C}$ is equal to minimum Hamming weight $w_{min}$ of a non zero codeword in $\underline{C}$.

$$w_H(101101) = 4$$

**Proof:**

$$\boxed{d_{min} = w_{min}}$$

$$w_{min} = \min_{\substack{\underline{x} \in \mathbb{C} \\ \underline{x} \neq 0}} w_H(\underline{x}) = \min_{\substack{\underline{x} \in \mathbb{C} \\ \underline{x} \neq \underline{0}}} d_H(\underline{x}, \underline{0})$$

$(0, \ldots, 0) = \underline{0} \in \mathbb{C}$ because $\mathbb{C}$ is a subspace.

First part: $d_{min} \leq w_{min}$.

Second part: $w_{min} \leq d_{min}$.

Say $d_H(\underline{x}, \underline{y}) = d_{min}$

$\underline{x} \in \mathbb{C}$, $y \in \mathbb{C}$, then $\underline{x} + \underline{y} \in \mathbb{C}$ (linearity).

$$\omega_H(\underline{x}+\underline{y}) = d_{min}$$ → which means $d_{min}$ is the Hamming wt of some codeword

$$\Rightarrow \quad \omega_{min} \le d_{min}.$$

From first & second parts, it follows that $d_{min} = \omega_{min}$.

## Generator matrix of a linear block code

Let $\mathbb{C}$ be a $(n, k, d)$ code.
Then any $k \times n$ matrix $G$ whose rows are a basis for $\mathbb{C}$ is called generator matrix for $\mathbb{C}$.

→ A code can in general have more than one generator matrix.

→ $\underline{u} \rightarrow \boxed{\text{Encoder}} \rightarrow \underline{c}$

$$\boxed{\underset{1\times n}{\underline{c}} = \underset{1\times k}{\underline{u}} \cdot G_{k\times n}}$$

→ Matrix multiplication
→ Much less complex than look up tables.

## Repetition Code

$$(0 \ldots 0) \quad \underline{\underline{(1 \ldots 1)}}$$

$$(n, 1, n)$$

Generator matrix of repetition code