Class 24

$\{0,1\}^n \longrightarrow \boxed{\text{Channel}} \longrightarrow \{0,1\}^n$

Channel : For input x & output y

$d_H(x,y) \le t$. $(t \le n)$

Lemma: Let $\mathcal{C} \subseteq \{0,1\}^n$.

Let $\underbrace{d_{min}(\mathcal{C})}_{\text{min distance of code } \mathcal{C}} \triangleq \min\limits_{\substack{\underline{c},\underline{c}' \in \mathcal{C} \\ \underline{c} \neq \underline{c}'}} d_H(\underline{c},\underline{c}')$

$d_{min}(\mathcal{C}) \geq 2t+1$ iff $\mathcal{C}$ can correct any t errors in the communication, under the min distance decoder

Proof:

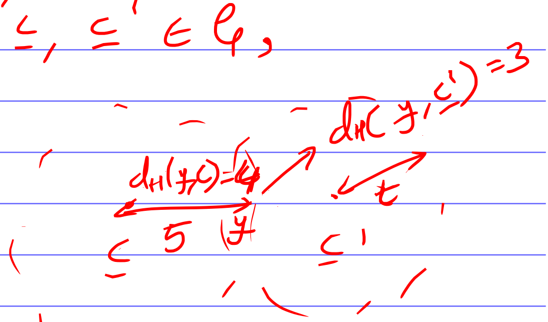
If part:

Gn: $\mathcal{C}$ can correct any t errors in the commn under MDD.

Tp: $d_{min}(\mathcal{C}) \geq 2t+1$

Gn statement implies that for any distinct $\underline{c}, \underline{c}' \in \mathcal{C}$,

$B_t(\underline{c}) \cap B_t(\underline{c}') = \phi \longrightarrow (1)$



where $B_t(\underline{c})$ = Hamming ball of radius t

$\triangleq \{ \underline{x} \in \{0,1\}^n : d_H(\underline{x},\underline{c}) \le t \}$

$\longrightarrow \left(\text{No. } |B_t(\underline{c})| = \sum\limits_{i=0}^{t} \binom{n}{i} \right)$

By (1) it is clear that

This proves if part. $\left\{ \begin{array}{l} d_H(\underline{c},\underline{c}') > 2t. \\ \forall\ \underline{c},\underline{c}' \in \mathcal{C} \text{ such that } \underline{c} \neq \underline{c}' \end{array} \right.$ (Proof of this is by contradiction

Suppose $d(\underline{c},\underline{c}') \le 2t$

Then $\exists\, \underline{y}$ such that $d_H(\underline{c},\underline{y}) \le t$ & $d_H(\underline{c}',\underline{y}) \le t$)

Please complete proof of only-If part.

Terminology:

"Size" of the code $= |\mathcal{C}|$

"Length of the code" = "Block length" $= n$ (= length of each codeword)

Lemma above relates the error correcting capability of the code with the min-distance

$\longrightarrow$ Min dist calculation has nothing to do with channel.

$\downarrow$

This suggests that code design can be theoretically done independent of the channel & its performance can be tested based on its min distance. $\Longleftarrow$ Suppose code has min-distance $= d$, then it can be used on a channel for correcting upto $\left\lfloor \frac{d-1}{2} \right\rfloor$

Lemma (Hamming bound (upper bound on size of code based on given min distance))

Let $\mathcal{C}$ be any code with $d_{min}(\mathcal{C}) = d$.

Then

$$|\mathcal{C}| \leq \frac{2^n}{\left(\sum_{i=0}^{t} \binom{n}{i}\right)} \qquad \text{where } t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

$2^n \longrightarrow$ Total no of vectors

$\left(\sum_{i=0}^{t} \binom{n}{i}\right) \longrightarrow$ size of each ball of radius t.

Proof follows as we can pick at most one codeword per ball.

Linear codes: [over $\mathbb{F}_2$ → $(\{0,1\}, +, \cdot)$ → 'field' of 2 elements / binary 'field'.]

$+$ ↑ XOR (addition over integers but modulo 2) $(1+1=0)$

Definition: "A linear code over $\mathbb{F}_2$" of length n is a subset $\mathcal{C} \subseteq \mathbb{F}_2^n$ and also a subspace of the vector space $\mathbb{F}_2^n$.

$\Rightarrow \forall\, a,b \in \mathbb{F}_2,\ \forall\, \underline{c_1}, \underline{c_2} \in \mathcal{C}$

$$a\,\underline{c_1} + b\,\underline{c_2} \in \mathcal{C}.$$

Since only nontrivial values of a, b above are $a=1$ & $b=1$

> Recollect: $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2$ (of dimension n)
> ↑ field of scalars
>
> Note: For $a,b \in \mathbb{F}_2$, $\underline{v_1}, \underline{v_2} \in \mathbb{F}_2^n$
> $a\,\underline{v_1} + b\,\underline{v_2} \in \mathbb{F}_2^n$
> component-wise add in $\mathbb{F}_2$ / scalar multiplication

$\Leftrightarrow \mathcal{C}$ is a subspace of $\mathbb{F}_2^n$ iff

$$\forall\, c_1, c_2 \in \mathcal{C}, \text{ we have } \underline{c_1 + c_2} \in \mathcal{C}.$$

> Recollect:
> "-1" in $\mathbb{F}_2$ represents additive inverse of 1, which is 1 itself
> $\Rightarrow \underline{c_1} - \underline{c_2} = \underline{c_1} + \underline{c_2}$

Lemma: If $\mathcal{C}$ is a linear code, then

$$d_{\min}(\mathcal{C}) = \min_{\underline{c} \neq 0,\ \underline{c} \in \mathcal{C}} w_H(\underline{c}).$$

where $w_H(\underline{c})$ = no. of non-zero positions in $\underline{c}$. (Hamming wt of vector $\underline{c}$.)

Class 25:

Proof: By definition

$$d_{\min}(\mathcal{C}) \triangleq \min_{\substack{\underline{c_1}, \underline{c_2} \in \mathcal{C} \\ \underline{c_1} \neq \underline{c_2}}} d_H(\underline{c_1}, \underline{c_2})$$

$$\min_{\substack{\underline{c_1}, \underline{c_2} \in \mathcal{C} \\ c_1 \neq c_2}} d_H(\underline{c_1}, \underline{c_2}) = \min_{\substack{\underline{c_1}, \underline{c_2} \in \mathcal{C} \\ \underline{c_1} \neq \underline{c_2}}} w_H(\underline{c_1} - \underline{c_2})$$

$$= \min_{\substack{\underline{c} \neq \underline{0} \\ \underline{c} \in \mathcal{C}}} w_H(\underline{c})$$

Ex:
$\underline{c_1} = (1,1,1,0,0,0)$
$\underline{c_2} = (1,0,1,1,0,1)$
$\underline{c_1} - \underline{c_2} = (0,1,0,-1,0,-1)$
$= (0,1,0,1,0,1)$

Take away: For Linear Code $d_{\min}(\mathcal{C}) =$ min wt of non-zero codeword

Aside: $\mathbb{F}_2$, $\mathbb{F}_2^n$

Elements of $\mathbb{F}_2$ are $\{0, 1\}$.

Operations in $\mathbb{F}_2$: Addition & Multiplication

AND

a	b	a·b
0	0	0
1	0	0
0	1	0
1	1	1

For any $a, b \in \mathbb{F}_2$

$a+b \in \mathbb{F}_2$

we want to "define" an addition

(we use XOR)

XOR

a	b	a+b
0	0	0
0	1	1
1	0	1
1	1	0

(add inverse of 0 = 0)

additive inverse of 1 = 1

Note that subtracting in $\mathbb{F}_2$ is exactly addition with inverse

Take 2 elements of $\mathbb{F}_2^n$:

These are called n-tuples

$(a_1, \ldots, a_n) : a_i \in \mathbb{F}_2$

$(b_1, \ldots, b_n) : b_i \in \mathbb{F}_2^n$

(+ in $\mathbb{F}_2$)

$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) \stackrel{\Delta}{=} (a_1 + b_1, \ldots, a_n + b_n)$

adding component-wise

Scalar Multiplication in $\mathbb{F}_2^n$: $a\,(b_1, \ldots, b_n) \stackrel{\Delta}{=} (a \cdot b_1, \ldots, a \cdot b_n)$

$\in \mathbb{F}_2$

componentwise in $\mathbb{F}_2$

Recall from linear algebra: Every subspace of a vector space has a basis.

(linearly independent set of vectors from the subspace which span the subspace)

So linear code $\mathcal{C}$ will have a basis:

Ex 1: Suppose $\mathcal{C} = \mathbb{F}_2^n$.

→ Then any set of n linearly ind. vectors from $\mathbb{F}_2^n$ will work as a basis of $\mathcal{C}$.

→ In particular we can choose standard basis

$\underline{e_1} \stackrel{\Delta}{=} (1, 0, \ldots, 0)$, $\underline{e_2} \stackrel{\Delta}{=} (0, 1, \ldots, 0)$, $\ldots$, $\underline{e_n} \stackrel{\Delta}{=} (0, \ldots, 0, 1)$

Ex 2: Repetition code

$$\mathcal{C} = \{ (0,0,\ldots,0), (1,\ldots,1) \}$$ → Easy to check this is a linear code.

Basis for $\mathcal{C}$ = $\{ (1,\ldots,1) \}$ → $\boxed{\text{Dimension} = 1 \; \downarrow \; \text{encodes 1 bit}}$

Ex 3: Suppose $B = \{g_1, \ldots, g_k\}$ are a set of linearly independent vectors in $\mathbb{F}_2^n$. What is a linear code $\mathcal{C}$ for which B is a basis?

Fix $\mathcal{C} = \text{span}(B) \triangleq \left\{ \sum_{i=1}^{k} \alpha_i g_i : \forall \alpha_i \in \mathbb{F}_2 \right\}$

Every vector here must be unique since B forms a linearly independent set

set of all linear combinations of vectors in B.

Note that $|\mathcal{C}| = 2^k$.

k = dimension of code $\mathcal{C}$ $\left(k = \log_2 |\mathcal{C}|\right)$

Rate of this code $= \dfrac{k}{n}$.

This code encodes k bits

Message vector $(\alpha_1, \ldots, \alpha_k) \xrightarrow{\text{encoded}} \sum_{i=1}^{k} \alpha_i g_i$ → Codeword

$$\xrightarrow{\text{Encoder}} \text{codeword} = \underset{1\times k}{(\alpha_1, \ldots, \alpha_k)} \underset{k\times n}{G}$$

↓

Linear operation (easy to implementation)

where G matrix $= k \times n = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$