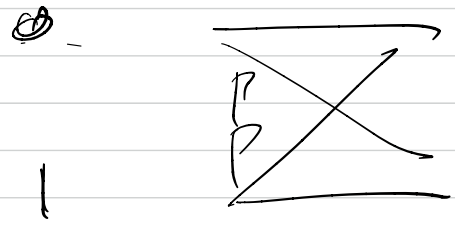
Information Theory & Coding

Nov 23, 2020

Linear Codes :

Binary Symmetric Channels :



$0 \leq p \leq \frac{1}{2}$

$enc : \{1, \ldots, M\} \longrightarrow \{0,1\}^n$

range of this function $= \{ enc(m) : m = 1.., M \}$

$\subseteq \{0,1\}^n$

$\mathcal{C}$

This enc is said to be the "encoder for a linear code" if $\mathcal{C}$ is a vector space over the scalar field $\{0,1\}$.

$\equiv$ ① if $x \in \mathcal{C}$ then $0 \cdot x \in \mathcal{C}$

② if $x, y \in \mathcal{C}$ then $x + y \in \mathcal{C}$.

$x = (x_1 \ldots x_n)$

$ax = (ax_1, \ldots, ax_n)$

$\equiv$ (① $0 \in \mathcal{C}$)

[② $x \alpha y \in \mathcal{C}$ $x+y \in \mathcal{C}$]

$x+y = (x_1+y_1, \dots, x_n+y_n)$

where $x = (x_1, \dots, x_n)$

$y = (y_1, \dots, y_n)$

mod-2 addition

$0+0 = 0$

$1+1 = 0$ ←

$1+0 = 1$

$0+1 = 1$

Because $x+x = 0$, we can replace our definition of being a vector space over $\{0,1\}$ by the following condition

$x, y \in \mathcal{C} \Rightarrow x+y \in \mathcal{C}$.

↳ elementwise mod 2 sum.

Ex: $\mathcal{C} = \{000\}$ is a linear code.

Ex: $\mathcal{C} = \{011, 110\}$ is not a linear code

Ex: $\mathcal{C} = \{000, 011, 110\}$ is not a c.c.

Ex: $C = \{000, 011, 110, 101\}$ is a linear code

$$C = \{ u_1(011) + u_2(110) : u_1 \in \{0,1\}, \; u_2 \in \{0,1\} \}$$

$$C = \text{span}\{011, 110\}$$

Ex: Let $H = \begin{bmatrix} 1&0&0&0&1&1&1 \\ 0&1&0&1&0&1&1 \\ 0&0&1&1&1&0&1 \end{bmatrix}$ } 3

7

$$C = \{ (x_1 \dots x_7) \in \{0,1\}^7 : H \begin{bmatrix} x_1 \\ \vdots \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \}$$

$= \ker(H) = \text{Null space}(H)$. (mod 2)

Question: is C a vector space? Yes.

Suppose $x, y \in C \equiv Hx = 0, \; Hy = 0$.

Then $z = x + y$ satisfies $Hz = Hx + Hy = 0$

$\Rightarrow z \in C$.

Elements of $\mathcal{C}$ are exactly the sequences $(x_1 \dots x_7)$ that satisfy

$$\begin{bmatrix} 1 & & & & 1 & 1 & 1 \\ & 1 & & 1 & & 1 & 1 \\ & & 1 & 1 & 1 & & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \hline x_4 \\ \vdots \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\iff \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix} \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\iff \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} & 1 & 1 & 1 \\ 1 & & 1 & 1 \\ 1 & 1 & & 1 \end{bmatrix} \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}.$$

$\Rightarrow$ $\mathcal{C}$ contains exactly 16 elements.

(one for each choice of $\begin{bmatrix} x_4 \\ \vdots \\ x_7 \end{bmatrix} \in \{0,1\}^4$)

Fact (to be shown in exercises):

If $\mathcal{C}$ is a vector space over $\{0,1\}$ then $|\mathcal{C}| = 2^k$ for some $k = 0, 1, 2, \dots$

Fact: Given a $\mathcal{C}$ which is a vector space over $\{0,1\}$, we can find vectors $g_1, \dots, g_k$ s.t

$$\mathcal{C} = \text{span}\{g_1, \dots, g_k\}$$

$$= \left\{ \underbrace{\sum_{i=1}^{k} u_i g_i}_{\text{linear combination}} : u_i \in \{0,1\} \right\}$$

& $\{g_i\}$ are linearly independent.

(proven in the exercises).

We call such $\{g_1, \dots, g_k\}$ to be the "generator" of $\mathcal{C}$.

Note:

$$\underbrace{\sum_{i=1}^{k} u_i g_i}_{\text{linear combination}} = \underbrace{\begin{bmatrix} \uparrow & & \uparrow \\ g_1 & \cdots & g_k \\ \downarrow & & \downarrow \end{bmatrix}}_{G} \begin{pmatrix} u_1 \\ \\ u_k \end{pmatrix}$$

So:

$$\mathcal{C} = \underbrace{\{Gu : u \in \{0,1\}^k\}}_{= \text{range}(G)}.$$

Moreover for any matrix G, its range is a vector space.

$x = Gu$, $y = Gv$

$\Rightarrow x + y = G(u+v) \Rightarrow x+y \in \mathcal{C}$

G is called a generator matrix.

Remember also? For any matrix H,

$\mathcal{C} = \{x : Hx = 0\}$ is a vector space

$= \text{Kernel}(H) = \text{Null-space}(H)$.

Moreover (Fact) for any vector space $\mathcal{C}$ we can find H s.t $\mathcal{C} = \text{Ker}(H)$.

Pf: By the "previous fact": Given $\mathcal{C}$ we can find G s.t $\mathcal{C} = \{Gu : u \in \{0,1\}^k\}$.

Now use column operations of G to put it in triangular form:

Aside: Ex: $G = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$

$\text{range}(G) = \text{range}\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}\right)$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = g_1 u_1 + g_2 u_2 = (g_1 + g_2) u_1$$

$$+ g_2 u_2 - g_2 u_1$$

$$= (g_1 + g_2) u_1 + g_2 (u_2 + u_1)$$

$$= \underbrace{\begin{bmatrix} g_1 + g_2 & g_2 \end{bmatrix}} \begin{pmatrix} u_1 \\ u_1 + u_2 \end{pmatrix}$$

$\underbrace{\quad}$ $g_1 \quad g_2$

So column operations don't change the range of a matrix.

$\Rightarrow$ By column operations we can put G in the following form:

$$G = \begin{bmatrix} I \\ - - - \\ A \end{bmatrix}$$

up to a permutation of the rows.

Ex: $G = \begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

So: $G = [\text{perm}] \begin{bmatrix} I \\ A \end{bmatrix}$

$\Rightarrow$ elements y the range satisfy

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (p \times m) \begin{pmatrix} I_k \\ \hline A \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

$$= (p \times m) \begin{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} \\ \hline A \begin{pmatrix} u_1 \\ u_k \end{pmatrix} \end{pmatrix}$$

$$= (p \times m)^{-1} \begin{pmatrix} x_1 \\ \\ x_n \end{pmatrix} = \begin{pmatrix} u_1 \\ \vdots \\ u_k \\ \hline A \begin{pmatrix} u_1 \\ u_k \end{pmatrix} \end{pmatrix}$$

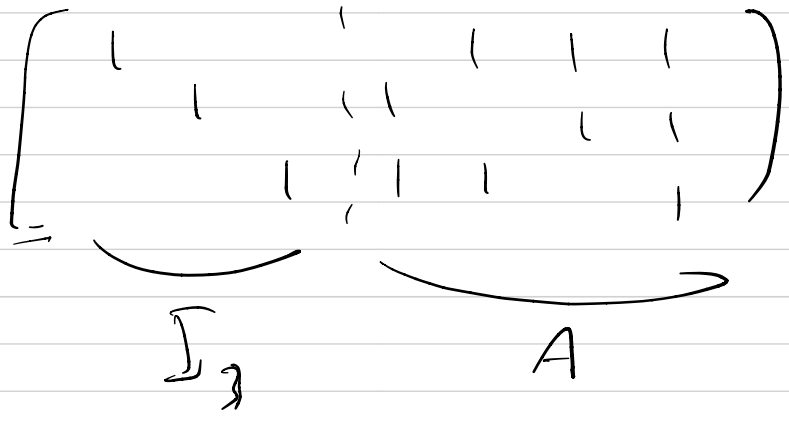
$$= \underbrace{\begin{pmatrix} A & I \end{pmatrix} (p \times m)^{-1}}_{H} \begin{pmatrix} x_1 \\ \\ x_n \end{pmatrix} = A \begin{pmatrix} u_1 \\ u_k \end{pmatrix} + A \begin{pmatrix} u_1 \\ u_k \end{pmatrix} = 0$$

$$= Hx = 0 \ldots, \text{ so we have found } H$$

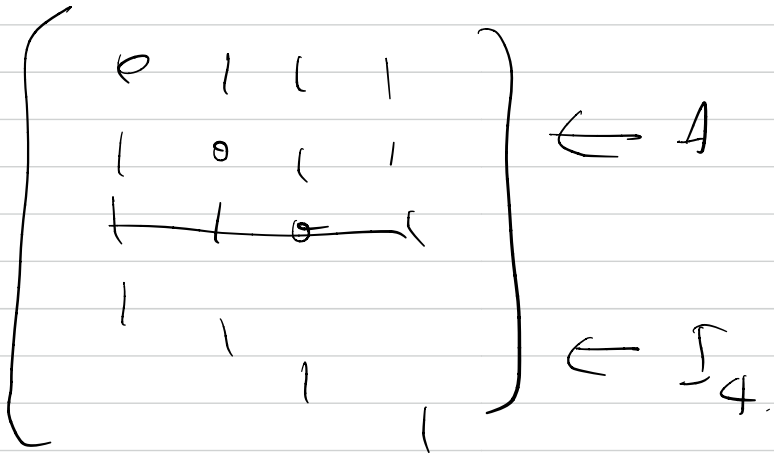
s.t. $\text{range}(G) = \ker(H)$.

G: generator matrix,

H: parity check matrix.

Ex : $H =$ 

I_3 A

$G =$ 

$\leftarrow A$

$\leftarrow I_4$

$K_{er}(H) = Range(G)$.

$$\{ x \in \{0,1\}^7 \text{ s.t } Hx = 0 \}$$

$$= \{ Gu : u \in \{0,1\}^4 \}.$$

Observe : with $G = \underbrace{[\quad]}_{k}\}n$ having linearly independent columns has rank $= k$. Thus if $u \neq u'$ then $Gu \neq Gu'$. (otherwise

$$G(\underbrace{u+u'}_{v}) = 0 \Rightarrow \sum_i v_i g_i = 0$$

with $v \neq 0$, contradicts the lin. indep of the g_i's.).

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

We also have

Thm: if $\mathcal{C}$ is linear, then

$$d_{min}(\mathcal{C}) = \min\{ w_H(x) : x \in \mathcal{C}, x \neq 0 \}$$

$$\triangleq w_{min}(\mathcal{C}).$$

Remark: $d_{min}(\mathcal{C}) = \min_{\substack{x, x' \in \mathcal{C} \\ x \neq x'}} d_H(x, x')$

$$w_H(x) = \sum_{i=1}^{n} \mathbb{1}\{x_i \neq 0\} \quad \text{with } x = (x_1 \dots x_n)$$

Pf: we will prove $d_{min}(\mathcal{C}) \leq w_{min}(\mathcal{C})$ & $\geq$.

for the 1st: let $x \in \mathcal{C}$ have $w_H(x) = w_{min}(\mathcal{C})$.

$x \neq 0$.

then $d_{min}(\mathcal{C}) \leq d_H(x, 0) = w_H(x) = w_{min}(\mathcal{C})$.

for the 2nd, let $x, x' \in \mathcal{C}$, $x \neq x'$ & $d_H(x, x') = d_{min}$.

then $d_{min}(\mathcal{C}) = d_H(x, x') = w_H(x \oplus x')$

$= w_H($ codeword $) \geq w_{min}(\mathcal{C})$. //

$\neq 0$

Corollary: Suppose $\mathcal{C} = \ker(H)$, and

Suppose any s columns of H are linearly

independent. $\Rightarrow d_{min}(\mathcal{C}) > s$.

Pf: Suppose $w_H(x) = w_{min}(\mathcal{C})$ $x \in \mathcal{C}$. then

$Hx = 0$ $\sum_i h_i x_i = 0$

i ↑ Colum of H

Contains $w_H(x)$ terms. But no

linear combination of $\leq s$ columns of H can be zero.

$\Rightarrow w_H(x) > s$. //

Moreover if some t columns of H are linearly

dependent, than $d_{min}(\mathcal{C}) \leq t$.

Pf: Suppose $h_1 \dots h_t$ are linearly dep.

then $\exists (x_1 \dots x_t) \neq (0 \dots 0)$ s.t

$\sum_{i=1}^{t} h_i x_i = 0$ now the vector

$x = (\underbrace{x_1 \dots x_t}\ 0\ 0\ 0 \dots) \in \{0,1\}^n$ satisfies

① $Hx = 0$ (i.e. $x \in \mathcal{C}$),

② $x \neq 0$ & $w_H(x) \leq t$

$\Rightarrow d_{min}(\mathcal{C}) = w_{min}(\mathcal{C}) \leq w_H(x) \leq t$. //

To illustrate there::

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Columns of H are all distinct, and non-zero.

$\Rightarrow$ any two columns are lin. independent.

$\Rightarrow$ $d_{min} > 2$.

also the three cols are linearly dep

$\Rightarrow$ $d_{min} \leq 3$ $\Rightarrow$ $d_{min} = 3$.

Since $G = \left[\begin{array}{c} I_4 \\ \hline \cdots \end{array}\right]$ has rank = 4, thus

code has 16 codewords.

The code above defined by

$$H = \left[\begin{array}{ccc} & & \\ & & \\ & & \end{array}\right] \Big\} 3$$

7

is called (7, 4, 3) Hamming code

n = 7, 4 codewords, d_{min} = 3

We can generalize this in the following way:

$$H = \left[\begin{array}{c|c} I_r & A \\ \hline \cdots & \end{array}\right] \Big\} r \text{ rows}$$

r

$2^r - 1$ columns : all dim = r

non-zero binary vectors

$$G = \left[\begin{array}{c} A \\ \hline I_k \end{array}\right] \qquad k = 2^r - 1 - r$$

This code has

2^k codewords $(k = 2^r - 1 - r)$

each $n = 2^r - 1$ dimensional

$d_{min} = 3$, called the

$(2^r - 1,\ 2^r - r - 1,\ 3)$ Hamming code,

capable of correcting a single bit flip.

Suppose $x \in \mathcal{C}$ (i.e., $Hx = 0$) is sent.

$y = x + z$ with $w_H(z) \le 1$.

$\uparrow$ mod 2

$Hy = Hx + Hz = Hz = \begin{cases} 0 & z = 0 \\ h_i & z = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix} \leftarrow i\text{th} \end{cases}$

$Hx = 0$

If we choose $H =$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

1 2 7

If we receive $y = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ we can form

$Hy = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ & conclude that $z = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ ← 4th.

So the transmitted codeword was

$x = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$.