Linear Block Codes

How to make communication reliable?
Channel Coding

Two types of chennel codes
- Block codes
- Convolutional codes

Block codes

- Binary seq. of length k mapped into seq. of length n $(n \geq k)$

How do we send the n bits
Use BPSK, QPSK, FSK
(Do we have to send the n bits together?)

- Block codes are memoryless:
Each set of k bits is independent from the next sequence of k bits.
Sequence of codewords indep. of each other.

Convolutional Codes:

Code rate:

Defined by $R_c = \frac{k}{n}$

represents the info bits sent in transmission of a binary symbol over channel

(Given a seq. of k bits mapped into a seq. of n bits, How does the entropy of the codewords differ?)

$$n > k \Rightarrow R_c < 1.$$

General Properties of linear block codes

A binary block code C consists of a set of M vectors of length n

$$C_m = \begin{bmatrix} c_{m1} \\ c_{m2} \\ \vdots \\ c_{mn} \end{bmatrix}$$

How many possible codewords 2^n (n bits)

We choose only 2^k of them (k bits)

A block of k info bits is mapped into a codeword of length n selected from the set of 2^k codewords

This is called an (n, k) block code with rate $R_c = \frac{k}{n}$.

Why "Linear" block codes

Linearity guarantees easy implementation

~~Linear~~ For a linear block code,

for any two code words c_1 ~~&~~ c_2

$c_1 + c_2$ is a codeword

(The all zero vector is a codeword – Why?)

Generator & Parity Check Matrices

mapping from k bits to n bits can be represented by a $k \times n$ "Generator matrix" G

$1 \le m \le 2^k$

$$\underbrace{c_m}_{\text{corresponding codeword}} = \underbrace{u_m}_{\text{info sequence}} \underbrace{G}_{k \times n}$$

$$G = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}$$

g_1 is a codeword – why?
what info sequence "generates" it?

Thus, the code word correspond to the input seq. $u_m = (u_{m1}, \dots, u_{mk})$ is

$$c_m = [u_{m1} \dots u_{mk}] G$$
$$= \sum_{i=1}^{k} u_{mi} g_i$$

$\Rightarrow$ codewords is the set of lin combination of rows of G

$\Rightarrow$ ~~C~~codewords is the row space of G

systematic code

If G has the following structure

$$G = [\underbrace{I_k}_{\text{identity matrix } k \times k} \,|\, \underbrace{P}_{\text{size } k \times n-k}]$$

Resulting lin. block code is systematic

$$c_m = [u_1, u_2, \dots, u_k] G$$
$$= [u_1, u_2, \dots, u_k] [I_k | P]$$
$$= [\underbrace{u_1, u_2, \dots, u_k}_{\text{info seq. } (k)} \,|\, \underbrace{[u_1, u_2, \dots, u_k] P}_{\text{Parity check bits } (n-k)}]$$

provides redundancy against errors.

Any linear block code has a systematic equivalent

i.e. pub

$$G = [\, I_k \mid P \,]$$

by elementary row & column operations

Codewords are of dimension k in n-dimensional space

$\Rightarrow$ orthogonal complement is of dim. $(n-k)$ in n-dim. space

Let H be corresponding matrix (of dim $n-k \times n$).

$n-k \times n$

Then for any codeword

$$c H^t = 0 .$$

Rows of G are codewords

$\Rightarrow$

$$G H^t = 0$$

~~For~~ systematic codes

$$G = [\, I_k \mid P \,]$$

then

$$H = [\, \underset{n-k \times k}{P^t} \mid \underset{n-k \times n-k}{I_{n-k}} \,]$$

Check that

<u>Ex</u>

$$G = [\, I_4 \mid P \,] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Let $u = (u_1, u_2, u_3, u_4)$ be the info

$c_1 = u_1$

$c_2 = u_2$

$c_3 = u_3$

$c_4 = u_4$

$c_5 = u_1 + u_2 + u_3$

$c_6 = u_2 + u_3 + u_4$

$c_7 = c_1 + c_2 + c_4$

Syndrome & Standard Array Decoding

Let c_m be the transmitted codeword

y be the received codeword

$$y = c_m + \underset{\uparrow}{e} \text{ error binary vector}$$

Let's kalculate yH^t

$$yH^t = c_m H^t + eH^t$$

$$\Rightarrow \underset{\uparrow}{s} = eH^t.$$

syndrome vector (of dim. $(n-k)$) of the error pattern

s is a characteristic of the error pattern

If $s = 0 \Rightarrow$ error pattern = code word

$\Rightarrow$ undetected error

Error remains undeteted if it is equal one of the codeword

There are $2^k - 1$ such patterns

There are a total $2^n - 1$ error patterns

of which $2^k - 1$ are undetected

$c_1 = 0$	c_2	c_3	--	c_{2^k}
e_2	$c_2 + e_2$	$c_3 + e_2$	--	$c_{2^k} + e_2$
⋮				
$e_{2^{n-k}}$	$c_2 + e_{2^{n-k}}$	$c_3 + e^{n-k}$	--	$c_{2^k} + e^{n-k}$

Example

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

info seq. $[u_1 \; u_2]$

Possible sequences

[0 0]
[1 0]
[0 1]
[1 1]

00000   10101   01011   11110

d_{min} for the code $= 3$

coset leader

00001
00010
00100
01000
10000
11000
10010

There exists a one-to-one correspondence between coset leaders & syndromes

Decoding:

find the error sequence of min weight

Such that

$$s = y H^t = e_j H^t$$

Each s corresponds to a single coset leader

Once you find the syndrome, find the corresponding coset leader.

coset

Add the coset leader