6/1/2020 **Lecture 1** (Introduction, Course Plan).

Course Syllabus

→ Introduction & motivation (1 lecture)
→ Block Codes, linear Codes (2).
→ Bounds on the Codes (2)
→ Finite fields preliminaries (2)
→ Cyclic Codes, Reed Solomon, BCH Codes (2)
→ Convolutional Codes, LDPC Codes (2)
→ Application to distributed storage, Computing (2)

Reference Textbook

→ Introduction to Coding Theory, Ron Roth (check with the library).

→ Shu Lin & Costello
→ Huffman & VeraPless.

Tutorials (Every week) → starts on 15th Jan.
Slot is Friday 3:30 to 5PM.
Arvind Rameshwar (PhD, IISc).

Course Evaluation

- Assignments (6 of them, 5 of which are graded) - 30%.

  (Solutions of the assignment will be discussed in the tutorial class → After the due date of the submission).

- 2 Quizzes - 20% (Each 10%).

  (1st Quiz on Jan 31st, 2nd on Feb 14) → both are Sundays.

- Final Exam - 20%
- Term Paper (groups of 3 or 4) - 20%
- Viva - 10%

  ↳ Will be after last class which is Feb 20.

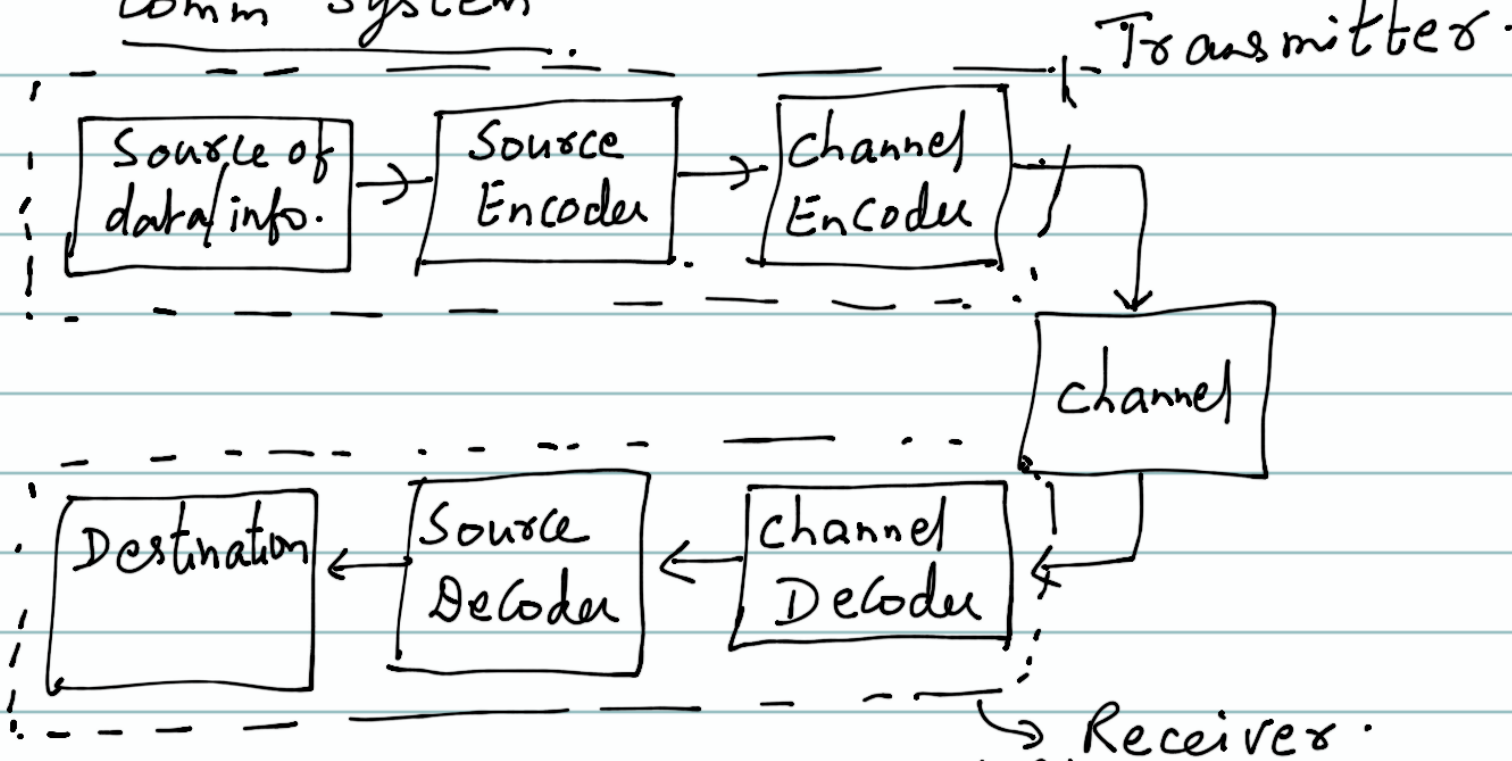
Motivation

Communication System

Examples:- ① Telephones, mobiles, TV, mails (Comm in space).

② CD, DVDs, flash drives, (Memory info). (Comm in time)

Block diagram / (back bone) of a Comm System



Source of data/info → Txt file.
→ Audio file
→ Image.

Source Encoder:- Compresses data and converts into bits. (bit stream) → Removes Redundancy

sequence of source symbols

Example:- Zip a bunch of files.

There is natural redundancy present in the data

Source Decoder:- Converts the bit stream back into source symbols.

We will not deal with source encoder & decoder more in the course.

(
Zip → Lempel Ziv 77/78 algorithm
Compression of images (JPEG) → Huffman algorithm
).

Channel Encoder:- Takes as input the bit stream → introduces redundancy in a controlled fashion. →

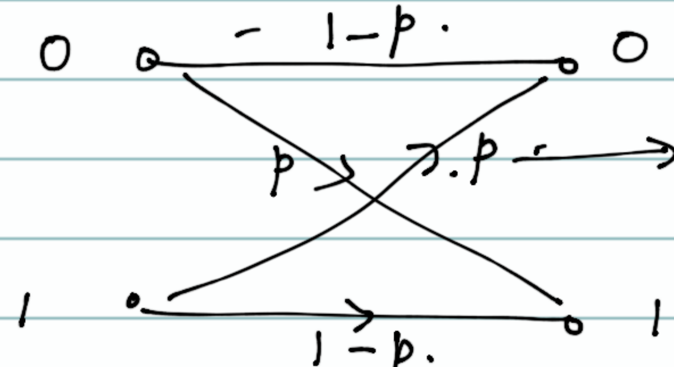
Why are adding this redundancy?
Because there is channel which is coming ahead which will corrupt your message.

Desirable → To be able to correctly/reliably receive the message.

Channel Decoder:- Receives the corrupted **Codeword** and tries to **guess** whatever was sent by the trasmitter

Examples of Channel Models

Binary Symmetric channel

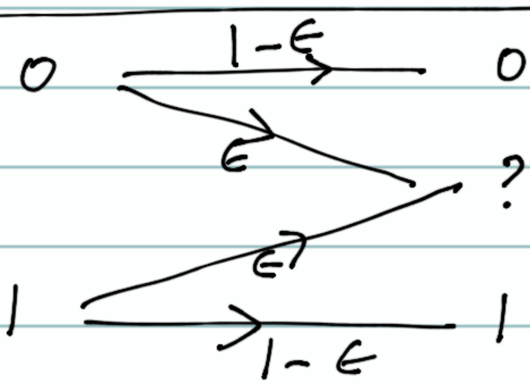


→ **Cross over probability**

0010 $\xrightarrow{\text{Flips each bit}}$ independently with prob p.

At the receiver, you can get any of the 16 possible combinations.

Binary Erasure channel



0010 → 16 outputs possible

Channel Encoder

Input bit stream $\rightarrow$ Channel Encoder $\rightarrow$

$\rightarrow$ splits the i/p bit stream into blocks of size k (bits). $\rightarrow$ Each block of size k. is mapped to a block of size n. bits $\rightarrow$.

$\underline{\underline{n > k}}$

<u>0 0 1 0 0 1 1 1</u>

Simple example of a channel encoder is a repetition code — 3-fold repetition

$k = 1, \quad n = 3$

00100111 $\longrightarrow$ 000 000 111 000 000 111 111 111

8 bits $\longrightarrow$ 24 bits.

$\underline{u}$ $\rightarrow$ Channel Encoder $\longrightarrow$ $\underline{c}$ (n bits)

$\underline{u}$ $\downarrow$ k bits (message).

$\underline{c}$ $\downarrow$ Codeword.

k bit message $\underline{u} \rightarrow 2^k$ distinct messages are possible.

How many distinct codewords should the encoder map to?

No. of distinct codewords $= 2^k$.

Channel Encoder map is a one-one function.

$$\begin{array}{l} 0 \searrow \\ \quad\ \ 000. \\ 1 \nearrow \end{array}$$

A code is the collection (as a set) of all possible codewords.

$(000, 111)$

$0 \rightarrow 000$

$1 \rightarrow 111$

Let's say the received vector is $110. \rightarrow$ What's your guess of transmitted vector? (depends on the flipping probability).

<u>Maximum likelihood decoding</u> $\rightarrow$ <u>Best channel decoder for any channel</u>

Probability of error calculations assuming your channel is BSC.

Assume $p = 0.1$.

Decoding Rules

Received Vector (corrupted) $\longrightarrow$ Codewords. (Messages are in one-one map with the codewords).

3-fold repetition code

000	001	010	011	100	101	110	111
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
000	000	000	111	000	111	111	111

Even when you make your best guess, there is a chance that you are in error.

$$\xrightarrow{\underline{c}} \boxed{\text{Channel}} \xrightarrow{\underline{y}} \boxed{\text{Channel Decoder}} \xrightarrow{\hat{\underline{c}}}$$

Error Event: $\{ \underline{c} \neq \hat{\underline{c}} \}$.

$P(\underline{c} \neq \hat{\underline{c}})$.

$$P(\underline{c} \neq \hat{\underline{c}})$$

$$= P(\underline{c} \neq \hat{\underline{c}} \mid \underline{c} = 000) \cdot P(\underline{c} = 000)$$

$$+ P(\underline{c} \neq \hat{\underline{c}} \mid \underline{c} = 111) \, P(\underline{c} = 111).$$

(Using total prob. theorem)

$$P(\underline{c} = 000) = P(\underline{u} = 0) = \frac{1}{2} = P(\underline{c} = 111) = P(\underline{u} = 1)$$

$$P(\underline{c} \neq \hat{\underline{c}} \mid \underline{c} = 000).$$

$$= P(\underline{y} = 110 \mid \underline{c} = 000) + P(\underline{y} = 011 \mid \underline{c} = 000)$$

$$+ P(\underline{y} = 101 \mid \underline{c} = 000)$$

$$+ P(\underline{y} = 111 \mid \underline{c} = 000).$$

$$= p \cdot p \cdot (1-p) + p \cdot p \cdot (1-p)$$

$$+ p \cdot p(1-p) + p \cdot p \cdot p.$$

$$= p^3 + 3p^2(1-p).$$

$$P(\underline{c} \neq \hat{\underline{c}} \mid \underline{c} = 111)$$

$$= p^3 + 3p^2(1-p)$$

$$P(\underline{c} \neq \hat{\underline{c}}) = p^3 + 3p^2(1-p).$$

Uncoded (Not using channel Code)

$\longrightarrow \quad P(\underline{c} \neq \hat{\underline{c}}) = 0.1$

3-fold repetition

$\longrightarrow \quad P(\underline{c} \neq \hat{\underline{c}}) = 3p^2(1-p) + p^3$

$= 0.028.$

Prob. of error decreases by employing a nontrivial channel code.

Metric for reliability is probability of error.

5-fold $\longrightarrow P_e^5$

7-fold $\longrightarrow P_e^7$

$$P_e^1 > P_e^3 > P_e^5 > P_e^7$$

As a system designer, for a target prob. of error, choose the repetition factor.