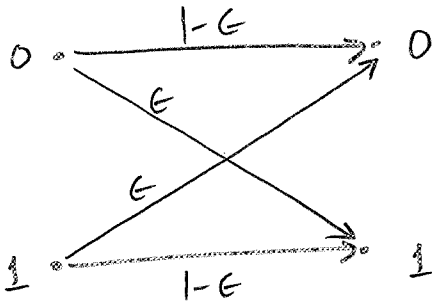
ELEC 541

CHAPTER I : INTRODUCTION

Our focus will be to communicate reliably over noisy communication channels.

A commonly encountered channel is

Binary Symmetric Channel ("Bit-flipping" channel)



Input bit Output bit

CORRECT RECEPTION

$$\text{Prob}(0|0) = \text{Prob}(1|1) = 1-\epsilon$$

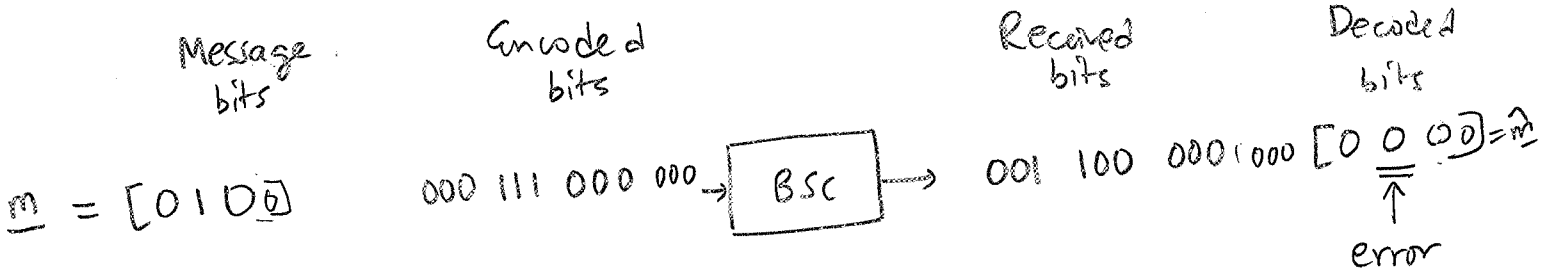
ERROR IN OUTPUT

$$\text{Prob}(1|0) = \text{Prob}(0|1) = \epsilon$$

Thus ϵ fraction of bits are received in error. How do we communicate reliably over such a channel ?

Repetition Code : For every input bit, send $(2k+1)$ bits. Then use a majority rule at the receiver to decide on what was sent

Consider $k=1$.



Message bits, $\underline{m} = [m_0\ m_1\ m_2\ m_3]$

Decoded bits, $\hat{\underline{m}} = [\hat{m}_0\ \hat{m}_1\ \hat{m}_2\ \hat{m}_3]$

Probability of error in decoding a bit in error,

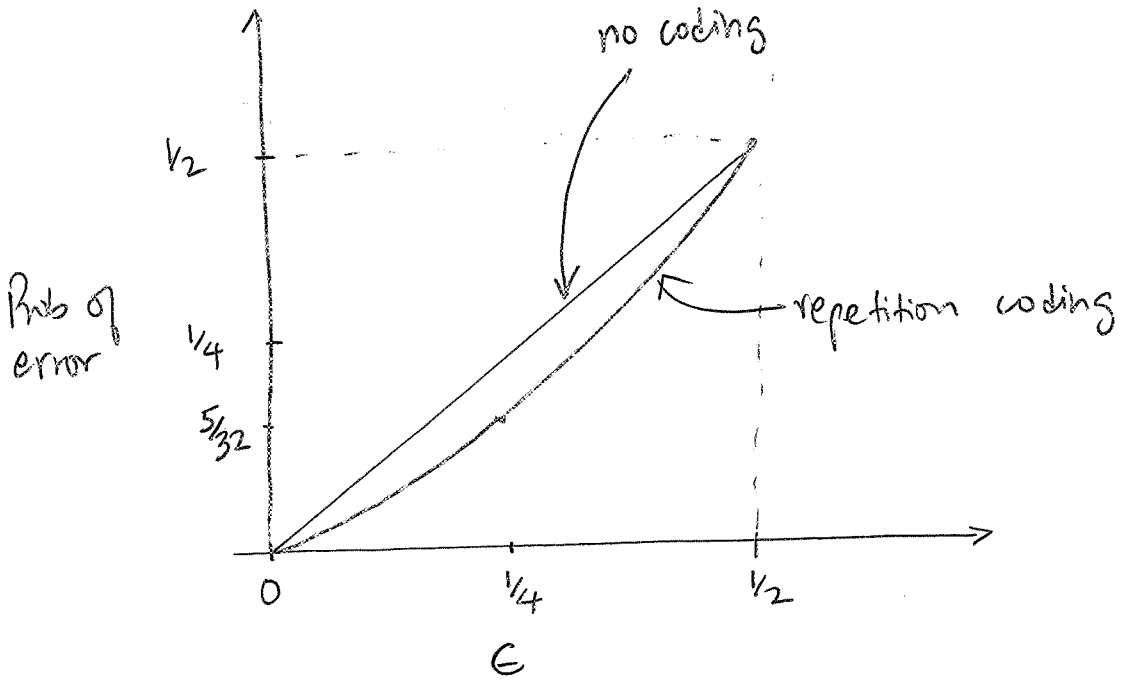
$$\text{Prob}(m_i \neq \hat{m}_i) = \text{Prob}(\text{at least 2 bits are flipped})$$

Consider $m_1 = 0 \longrightarrow 000$

what are the error events ?

$000 \longrightarrow$	0	1 1	$\epsilon^2(1-\epsilon)$
	1	1 0	$\epsilon^2(1-\epsilon)$
	1	0 1	$\epsilon^2(1-\epsilon)$
	1	1 1	ϵ^3

$$\text{Total probability error} = 3\epsilon^2(1-\epsilon) + \epsilon^3$$
$$= \epsilon^2[3 - 3\epsilon + \epsilon]$$
$$= \epsilon^2[3 - 2\epsilon]$$



So repetition coding can reduce the end-to-end error probability.

However, by having to send every bit three time, we can only send at a rate 1/3 of the uncoded system. $\left[\text{Rate} = \frac{\text{input bit}}{\text{output bits}} = \frac{1}{3}\right]$

With repetition coding, we can make it more reliable by increasing k but rate decreases as $\frac{1}{k}$.

In the limit, as $k \to \infty$

Prob of error $\to 0$

Rate of information $= \frac{1}{k} \to 0$

Yes, we are more reliable
but we are not really sending any information

Can we do better?

Hamming Code

Take 4 input bits $[m_0\ m_1\ m_2\ m_3]$

$$b_0 = m_1 + m_2 + m_3 \quad \text{(binary addition)}$$

$$b_1 = m_0 + m_2 + m_3$$

$$b_2 = m_0 + m_1 + m_3$$

Send $[m_0\ m_1\ m_2\ m_3\ b_0\ b_1\ b_2]$

$[0\ 1\ 0\ 0\ 1\ 0\ 1]$

Let's cause an error by flipping one of the bits

Received $[\underset{\hat{m}_0}{1}\ \underset{\hat{m}_1}{1}\ \underset{\hat{m}_2}{0}\ \underset{\hat{m}_3}{0}\ \underset{\hat{b}_0}{1}\ \underset{\hat{b}_1}{0}\ \underset{\hat{b}_2}{1}]$

Receiver checks if all the equations are satisfied

$$\hat{m}_1 + \hat{m}_2 + \hat{m}_3 = 1 = \hat{b}_0 \quad \checkmark \Rightarrow (\hat{m}_1, \hat{m}_2, \hat{m}_3) \text{ are correct}$$

$$\left.\begin{aligned} \hat{m}_0 + \hat{m}_2 + \hat{m}_3 &= 1 \neq \hat{b}_1 \quad \times \\ \hat{m}_0 + \hat{m}_1 + \hat{m}_3 &= 0 \neq \hat{b}_2 \quad \times \end{aligned}\right\} \Rightarrow \hat{m}_0 \text{ is in error}$$

This scheme can correct one error (and no more).

Compared to repetition code

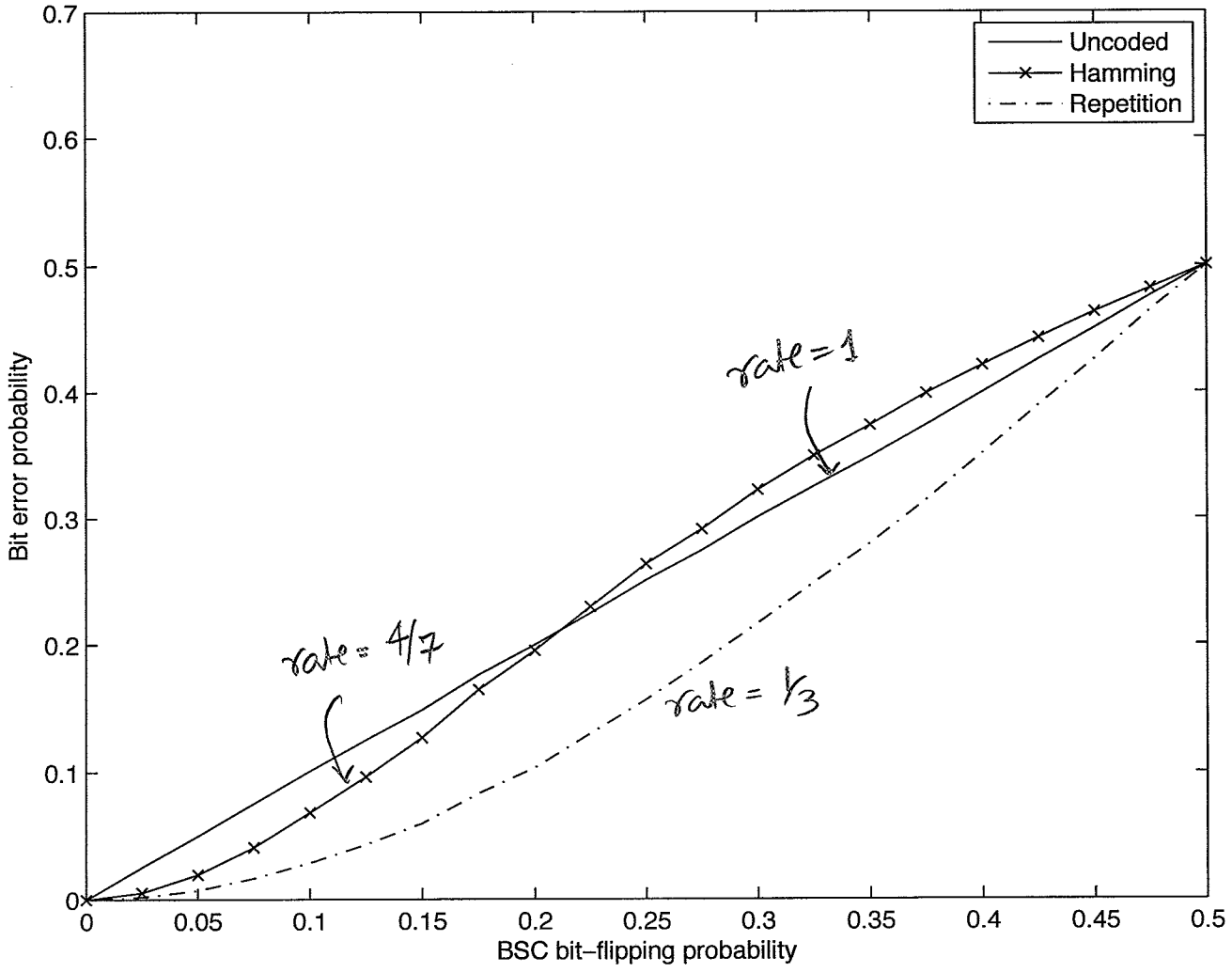
- Rate of Hamming code $= \frac{4}{7} > \frac{4}{12}$
- Both are guaranteed to correct upto one (1) error. Repetition code can correct some 2-errors and 3-errors but not all.

See plot on next page detailing performance of Hamming and repetition codes, compared to uncoded system.

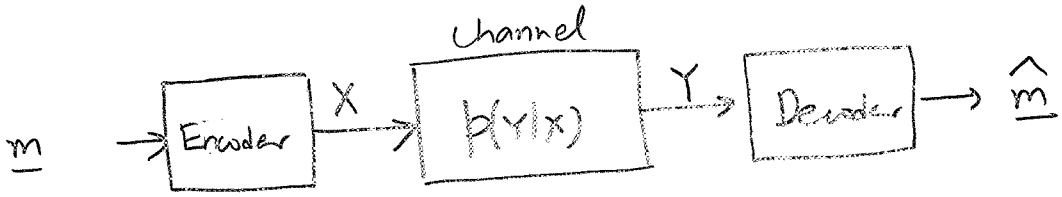
- Is this the best we can do?
- What is a systematic way to correct errors?

We will answer these questions in this class

But before we do that, we will state the fundamental result which gave birth to error correcting codes.


Uncoded
Hamming
Repetition
Bit error probability
BSC bit–flipping probability
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.05
0.15
0.25
0.35
0.45
rate = 1
rate = 4/7
rate = 1/3

Shannon's Channel Capacity Theorem



For every channel $p(y|x)$, the capacity of the channel is given

$$C = \max_{p(x)} I(X;Y)$$

where $I(X;Y)$ is the mutual information between input X and output Y.

[Details in ELEC 535: Information Theory]

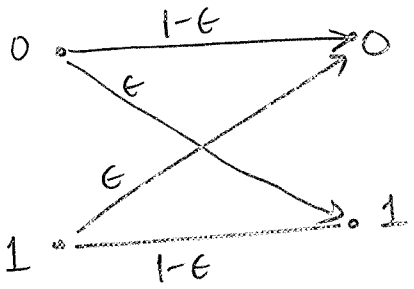
The key claim is that transmission rate

$$R = \frac{\text{information bits}}{\text{transmitted bits}} \longrightarrow \underbrace{C}_{\text{capacity}} > 0$$

And $P_e \longrightarrow 0$

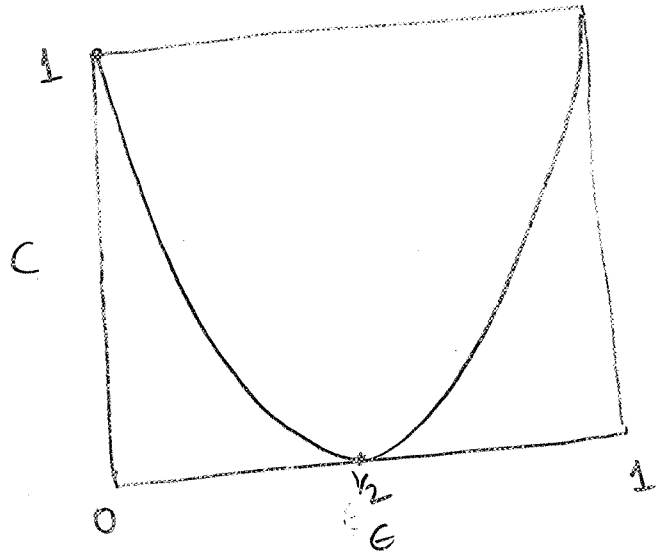
The trick is to encode using longer and longer blocks of data together. We will see how long block codes can get us both data rates and reliability

Capacity of BSC



$$\boxed{C = 1 - h_2(\epsilon)}$$

where $h_2(\epsilon) = \epsilon \log_2 \frac{1}{\epsilon} + (1-\epsilon) \log_2 \left(\frac{1}{1-\epsilon}\right)$



If $\epsilon = 0$ or 1, the decoder knows the input X without any doubt. Hence we can send at 1 bits/sec

For $\epsilon = 1/2$, the channel output Y is like an outcome of coin toss. As a result, no information can be received reliably.

Loosely speaking, coding theory can be divided into two streams of thoughts

Deterministic Codes:
- ("Short") block codes
- convolutional codes
- trellis coded modulation

"Random" codes:
- ("Long") block codes
- turbo codes

Random coding are inspired by Shannon's proof of coding theorem, and represent our best known codes today.