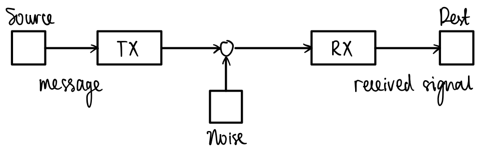
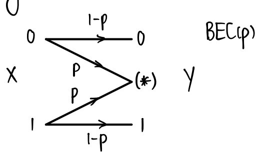
Digital Communication Systems



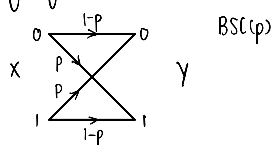
Binary Erasure Channel (BEC)



x: 0101001...

y: 0*01*0*...

Binary Symmetric Channel (BSC)



x: 0101001...

y: 0001000.. ← don't know location of corrupted/flipped bits

$$\left.\begin{array}{l} P(y=0|x=0) = P(y=1|x=1) = 1-p \\ P(y=*|x=0) = P(y=*|x=1) = p \end{array}\right\}\text{channel model}$$

Shannon showed that

$$\left.\begin{array}{l} C_{BEC}(p) = 1-p \text{ bits/ch use} \\ C_{BSC}(p) = 1-h(p) \text{ bits/ch use} \end{array}\right\}\text{how much info that gets across per channel use}$$

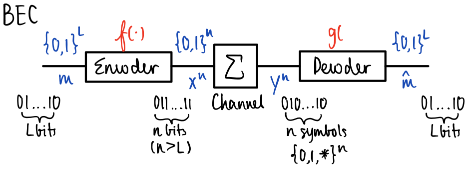
$$\boxed{C = \max_{p(x)} I(X,Y)}$$

Shannon showed his capacity results by

1/ establishing converse to comm reliably at a rate $R > C$

2/ achievable scheme that it is possible to comm at a rate $R \leq C$

BEC



$$P_e(n) = \max_{m \in \{0,1\}^L} P(\hat{m} \neq m)$$

$R = \frac{L}{n}$ is said to be achievable if $P_e(n) \to 0$ as $n \to \infty$

Capacity

The largest achievable rate for the channel is called its capacity.

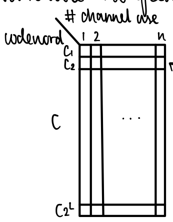
Theorem: The capacity of the BEC(p) channel is (1-p) bits/channel use.

① Proof: First we prove the converse, i.e. it is impossible to get $R > (1-p)$.

Even with feedback (where RX informs TX which location gets erased), the best TX can do is to resend the erased bits.

The channel erases a fraction p of the bits, it is impossible to communicate at a rate above (1-p) bits per ch use.

② Achievable: No feedback!



populate w/ indep fair coin flips

$M_n = 2^{Ln}$

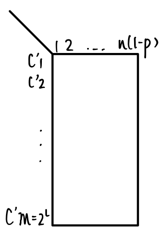
C is a $(2^L \times n)$ codebook consisting of $2^L = M$ entries of length n each, with each entry ~ iid $B(\frac{1}{2})$ RVs.

e.g. If msg 1 (of 2^L) $\Rightarrow X^n = (01010 \ldots 1)$
$Y^n = (0*01* \ldots 1)$

Main idea: If num of msgs (2^L) is not too large, i.e. R is small enough, then with high probability, one & only one codeword entry will be consistent w/ received output.

WLOG, we will assume that the last np bits were erased.
↳ transmitter doesn't know where erasures are

Truncated Codebook (C')



Decoding rule: Decoder looks at all possible message entries in C' & finds the only entry that is consistent w/ received information.
If there's a unique entry $\hat{m} = m \rightarrow$ success;
else if no unique match $\rightarrow$ error.

WLOG, assume m=1 sent (C'_1 sent).

$$P_e = P\{(C_2' = C_1') \cup (C_3' = C_1') \cup \ldots \cup (C_m' = C_1')\}$$
$$\leq \sum_{i=2}^{m} P(C_i' = C_1')$$
$$= (M-1)\, 2^{-n(1-p)}$$
$$< M\, 2^{-n(1-p)} \qquad M = 2^L = 2^{nR}$$
$$= 2^{nR}\, 2^{-n(1-p)}$$
$$= 2^{-n[(1-p)-R]}$$

$P_e \rightarrow 0$ as $n \rightarrow \infty$ if $(1-p) - R > 0 \Rightarrow R < 1-p$

If $R = 1-p-\epsilon$, $P_e < 2^{-n\epsilon}$

$n = 10{,}000$ $\quad$ $C = 5{,}000$ bits

$\epsilon = 0.01$ $\quad$ $R = 0.49 \times 10{,}000 = 4{,}900$ bits

$p = \frac{1}{2}$ $\quad$ $P_e < 2^{-100} \approx 0$

General: $C_{BEC} = \max_{0 \leq q \leq 1} [H(X) - H(X|Y)]$ $\qquad P(X=0) = q$

Show that max is attained when $q = \frac{1}{2}$.