REMINDERS

1. HW 3 out this Th and due 2 weeks after that (Mar 28)
   → Delay in HW 2 grading (during spring break)

2. 2-page report due in 3 weeks (April 2)
   → You can submit early & get comments sooner after submission

3. 2nd round of proof reading starts today
   → Make sure you're aware when your 2nd proof reading is due

RECAP:

Big Q: Optimal tradeoff between R & S (recall: worst-case noise model due to Hamming)

\[
\begin{align*}
R & \quad 1 \\
S & \quad 1 \\
\end{align*}
\]

TODAY: Proof reader → Amy

→ Revisit the worst-case noise model.
→ Noise model pioneered by Shannon

Memoryless (i.e., noise model acts independently on each transmitted symbol)

(Fully specified) random noise.

Shannon's '48 paper:

1. Noisy channel: (Channel coding) Our setup so far except noise is not worst-case (stochastic noise)
2. Noiseless channel: (Source coding) No noise during transmission ⇒ do compression.

Generic setup:
In Shannon's setup, we can accept and decode source and channel coding/decoding & optimize separately.

Source coding: notion of entropy as the "right" notion of compressibility was introduced.

**Shannon's noise model**

\[ X \rightarrow \text{channel} \rightarrow Y \]

Memoryless: same noise function acts on all the symbols transmitted.

For us, \( X, Y \): discrete.

Transition matrix \( X \rightarrow X \rightarrow (\cdot, \cdot) = M = \text{Pr}(Y|X) \)

1. **Binary Symmetric Channel (BSC)**

\[ X = Y = \{0, 1\} \]

\[
\begin{array}{c|cc}
& 0 & 1 \\
0 & 1-p & p \\
1 & p & 1-p \\
\end{array}
\]

= each bit gets flipped \( w.p. p \).

\[ Q: \text{Assume } 0 \leq p \leq \frac{1}{2}. \]

A: flip all bit received & use scheme for \( 0 \leq p \leq \frac{1}{2} \).
2) \(q\)-ary symmetric channel (qSCp) \((q=2 \rightarrow BSCp)\)

\[0 \leq p \leq \frac{1}{q}\]

\[X = Y = \{0, 1\}\]

\[\Pr[X \neq Y] = \left\{ \begin{array}{ll}
1-p & \text{if } y = x \\
p & \text{if } y \neq x
\end{array} \right.\]

So far \(X = Y\)

3) Binary erasure channel (BEC\(\alpha\)) \(0 \leq \alpha \leq 1\)

\(X = \{0, 1\} \text{} ; \ Y = \{0, 1, ?\}\)

- Each bit independent
- Gets flipped with prob \(\alpha\).

Error correction: \((BSCp) \rightarrow \text{some non-zero prob that transmitted codeword gets changed to another codeword.}\)

\(BEC\alpha \rightarrow \text{some non-zero prob that all symbols get erased.}\)

\(\text{Every message is decoded correctly w.p. } 1 - f(n)\)

\(\lim_{n \to \infty} f(n) = 0\) Ideally: \(f(n) = 2^{-\alpha(n)}\)

Shannon's general result:

\[R \text{ vs errors} \rightarrow \text{error parameter} \ p; \ qSCp\]

\(\alpha; \ \text{BEC}\)

\(\text{Shannon's thm: } \forall C \leq 1, \ 0 \leq R < C \Rightarrow \text{reliable communication.}\)

\(\text{For any } R > C \Rightarrow \text{is not possible}\)

\(C:\ \text{capacity of channel}\)

Next: Above for \(BSCp\)
Shannon's Capacity Thm for BSCp

0 \leq p < \frac{1}{2}, \ 0 \leq \epsilon \leq \frac{1}{2} - p

Following are true for large enough n:

1. \exists \delta > 0, an encoding function \ E : \{0,1\}^k \rightarrow \{0,1\}^n\ 
   a decoding \ D : \{0,1\}^n \rightarrow \{0,1\}^k \ 
   \forall m \in \{0,1\}^k, \ \Pr[D(\tilde{E}(m) + \epsilon) \neq m] \leq 2^{-\delta n}

2. If \ k \geq \lceil (1-H(p) + \epsilon) n \rceil \text{ then } \forall \ E : \{0,1\}^k \rightarrow \{0,1\}^n \ 
   D : \{0,1\}^n \rightarrow \{0,1\}^k \ 
   \exists m \in \{0,1\}^k \text{ s.t. } \ 
   \Pr[D(E(m) + \epsilon) \neq m] \geq \frac{1}{2} \quad (\epsilon \text{ can make this } \geq 1 - 2^{-\delta n})

⇒ \text{ Capacity of BSCp : } 1 - H(p)

\{SCp : 1 - H_q(p) \} \text{ same reason as GV bound: upper/lower bounds for Voq (p, n)}

Pf (sketch) of part 1:

Via probabilistic method: Pick E at random:

\[ \forall m \in \{0,1\}^k, \ E(m) \text{ is uniformly random } \in \{0,1\}^n \]

\[ \text{ independent choices for different } m \]

2 steps:

Step 1: For any \ m \in \{0,1\}^k, \text{ for random } E \text{ prob of decoding error is } 2^{-2(n) + \delta n}

⇒ \exists \text{ good } E \text{ for a fixed } m

Step 2: Show similar result \[ \forall m \in \{0,1\}^n \text{, } \exists E \text{ s.t. } \text{ involves cropping half of codewords } (k \rightarrow k^*). \]
2 sources of randomness:
1. Choice of \( E \) for prob. method
2. Randomness in BSCp noise \( \rightarrow \) contributes to decoding error prob.