Noisy-Channel Theorem: Converse

In the previous section, we showed that any rate strictly below the channel capacity is achievable. Here, we show that one cannot do better: rates strictly above the channel capacity are not achievable. Specifically, codes with such rates suffer from non-negligible error probabilities.

Theorem: Shannon's noisy-channel coding theorem (converse)

On a discrete memoryless channel with capacity C, any code with rate $R > C$ has average probability of error $p_e^{(n)} \geq 1 - \frac{C}{R} - \frac{1}{nR}$.

Proof

For a code with rate $R > C$, let W be uniformly distributed over all possible messages, let X^n describe the encoding of the message (and the input to the channel), let Y^n describe the output of the channel, and $\hat{W}$ the decoding of that output.

The average probability of error, $p_e^{(n)}$, is equal to $P[W \neq \hat{W}]$, the probability that the original message differs from the decoded message. Note that $W \to X^n \to Y^n \to \hat{W}$ forms a Markov chain.

As a first step, we show that the mutual information between the message W and the channel output Y^n is upper bounded by $n \cdot C$, that is, there is a limit to the amount of information that can get through the channel. To see this, first observe that

$$\begin{aligned}
H(Y^nW) &= H(Y^nW) + H(X^n \mid Y^nW) && \text{(since } W \text{ determines } X \\
&= H(X^nY^nW) && \text{(chain ru} \\
&= H(X^{n-1}Y^{n-1}W) + H(Y_n \mid X^nY^{n-1}W) + H(X_n \mid X^{n-1}Y^{n-1}W) && \text{(chain ru} \\
&= H(X^{n-1}Y^{n-1}W) + H(Y_n \mid X^nY^{n-1}W) && \text{(since } W \text{ determines } X \\
&= H(X^{n-1}Y^{n-1}W) + H(Y_n \mid X_n) && \text{(memoryle} \\
&= \dots && \text{(repe} \\
&= H(W) + \sum_{i=1}^{n} H(Y_i \mid X_i).
\end{aligned}$$

Therefore,

$$\begin{aligned}
I(W;Y^n) &= H(W) + H(Y^n) - H(Y^nW) && \text{(entropy diagram)} \\
&= H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid X_i) && \text{(by the above derivation)} \\
&\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i \mid X_i) \\
&= \sum_{i=1}^{n} I(X_i;Y_i) \\
&\leq n \cdot C.
\end{aligned}$$

Now that we have established that $I(W;Y^n)$ is upper bounded by $n \cdot C$, we can show that the code with rate R induces a considerable error probability:

$$\begin{aligned} R &= \frac{\log|\mathcal{W}|}{n} \\ &= \frac{1}{n}H(W) \\ &= \frac{1}{n}(H(W \mid Y^n) + I(W;Y^n)) \\ &\leq \frac{1}{n}(H(W \mid Y^n) + n \cdot C) \\ &\leq \frac{1}{n}\left(1 + P[W \neq \hat{W}] \cdot n \log|\mathcal{W}| + n \cdot C\right) \\ &= \frac{1}{n} + P[W \neq \hat{W}] \cdot R + C, \end{aligned}$$

where the second inequality is an application of Fano's inequality. Dividing both sides by R and rearranging, we get the desired inequality:

$$p_e^{(n)} = P[W \neq \hat{W}] \geq 1 - \frac{C}{R} - \frac{1}{nR}.$$

This theorem shows that if Alice and Bob try to communicate using a code with a rate $R > C$, their probability of error will be bounded away from zero by a constant factor of $1 - \frac{C}{R}$ (for big n, the last term in the inequality becomes insignificant). This error probability worsens for a bigger difference between R and C.