EE 121 – Intro to Digital Communication Spring 2016

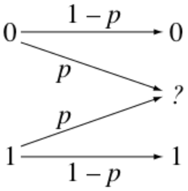
Homework 3

Assigned: Thur, 2/18/16 Due: Thur, 2/25/16

Instructor: Omur Ozel *GSI: Preetum Nakkiran*

1 Binary Erasure Channel Capacity

In this problem, we will explore the capacity of the binary erasure channel (BEC). The channel model of BEC_p is: Each bit is independently erased with probability p, and transmitted otherwise. This is represented by the following diagram (where the symbol ? denotes an erasure).



For example, if the 6 bits $\vec{x} = 110010$ are transmitted, they may be received as $\vec{y} = 1?0?10$. Note that in this model, the receiver knows the location of any erasures (it is not a *deletion channel*).

Intuitively, we would expect the erasure channel BEC_p to have higher capacity than the error channel BSC_p. Since we expect p fraction of bits to be dropped in the BEC_p channel, we may hope for a channel capacity of $1-p$. (Certainly if we transmit n bits across the channel and p fraction of them are dropped, we cannot hope to transmit more than $(1-p)n$ message bits). In fact, we will show that rates less than $1-p$ are achievable across the BEC_p channel, using similar random coding argument as the BSC_p case.

To be more precise: Let n be the blocklength, $p < 1$ the erasure probability of BEC_p, and any rate $R < 1-p$. Let $\mathcal{C}_n$ be a codebook containing 2^{nR} codewords, corresponding to (nR)-bit messages. We will show that: If codebook $\mathcal{C}_n$ is picked at random, and a codeword/message $c \in \mathcal{C}_n$ is picked at random, transmitted across the channel, and received as y, then it is possible to define a decoder such that

$$\Pr_{\mathcal{C}_n, c, y}[\text{Decode(y)} \neq c] \to 0$$

Where the notation $\Pr[\ldots] \to 0$ means a probability goes to 0 exponentially fast in n, ie $\Pr[\ldots] = 2^{-\Omega(n)}$. For this problem, you can get partial credit for showing error probabilities go to 0, not necessarily exponentially fast. (This will still yield the same capacity, but the results will be weaker).

(a) First, show that for any $\varepsilon > 0$, the channel will erase at most $(p+\varepsilon)$ fraction of bits with high probability. That is,

$$\Pr[\#\text{ bits erased} > (p+\varepsilon)n] \to 0$$

Thus, if a codeword c is sent across the channel, it will be received with $\leq (p+n)n$ erasures with high probability (this is somewhat analogous to the "decoding box / noise ball / typical set" around a codeword in the BSC argument).

(b) Consider the following decoder: On input the received message $\vec{y}$ (with erasures), search the codebook $\mathcal{C}$ for all "candidate codewords", which match the received $\vec{y}$ on all non-erased locations. In the below example, if $\vec{y}$ was received and c_1, c_2, c_3 were codewords, then c_1 and c_2 would be candidate codewords for $\vec{y}$, while c_3 would not be.

$$\begin{aligned}\vec{y} &= 1?0?10\\ \vec{c}_1 &= 110010\\ \vec{c}_2 &= 100110\\ \vec{c}_3 &= 010110\end{aligned}$$

If there is only one candidate codeword, the decoder picks this. Otherwise, it picks at random from the set of candidate codewords. [1] Indeed, this is the optimal decoder.

To analyze the probability of decoding error, note that the event {decoding fails} is contained in the union of the following two error events:

- Error Event 1: Channel erases more than $(p+\varepsilon)n$ bits.
- Error Event 2: Channel erases at most $(p+\varepsilon)n$ bits, but in the random codebook $\mathcal{C}$, there is more than 1 candidate codeword for the received y.

By the first part, the probability of Error Event 1 occurring goes to 0. We need to show that the probability of Error Event 2 goes to 0 as well.

Suppose the codebook $\mathcal{C}$ is sampled at random, i.e. each codeword in $\mathcal{C}$ is chosen iid uniform over $\{0,1\}^n$. Suppose codeword $c_i \in \mathcal{C}$ is transmitted across the channel, and received as y with $\leq (p+\varepsilon)n$ erasures. For a fixed $j \neq i$, bound the probability that codeword c_j is a also candidate codeword for y. That is, show

$$\Pr_{c_j}[c_j \text{ is a candidate codeword for received } y] = 2^{-\Omega(n)}$$

Note, the probability here is just over the random choice of codeword c_j (for a fixed choice of c_i, and fixed erasure pattern of $\leq (p+\varepsilon)n$ erasures). Then, using by the union bound over all 2^{nR} other codewords in $\mathcal{C}$, bound the probability that there is more than 1 candidate codeword for y. That is, show

$$\Pr_{\mathcal{C}}[\exists c_j \neq c_i \text{ that is candidate codeword for received } y] \to 0$$

How large can the rate R be for this probability to go to 0? (Recall the codebook is of size 2^{nR}, corresponding to sending an (nR)-bit message).

Thus, by the union bound over Error Events 1 and 2, we have shown the probability of decoding error goes to zero for any rate $R < 1-p$. Operationally, this means we can map an (nR)-bit message to n bits, to reliable communicate across the binary erasure channel at any rate $R < 1-p$.

(c) *(Remark, no need to write an answer).* The above argument shows that, on average over all codebooks and all sent messages, the probability of decoding error goes to zero exponentially fast. Convince yourself that this also implies the existence of good codebooks, where all messages have exponentially low probability of decoding error. (This follows from exactly the same reasoning as in the random coding argument for the binary error channel).

(d) Plot the capacity of the binary symmetric channel $C = 1 - H(p)$, together with the capacity of the binary erasure channel $C = 1-p$, as a function of the error/erasure probability p. Comment.

2 Binary Errors and Erasures

Here we will explore more connections between correcting for errors and correcting for erasures.

Recall that a code $\mathcal{C} \subset \{0,1\}^n$ is *t-error-correcting* if it can correct for all patterns of $\leq t$ errors. And similarly a code is *t-erasure-correcting* if it can correct for all patterns of $\leq t$ erasures.

(a) Show that a code $\mathcal{C}$ is $2t$-erasure correcting if and only if $\mathcal{C}$ is t-error-correcting. *(Hint: consider the minimum-distance).*

[1] This is not necessary; the decoder could just declare an error if multiple candidates are found without affecting the error probability much.

(b) Now let us show a more robust version of the above. Let $\mathcal{C} \subset \{0,1\}^n$ be an arbitrary code that is good for the binary symmetric channel BSC_p. Show that $\mathcal{C}$ is also good for the erasure channel BEC_{2p}.

More precisely, suppose there exists a decoder D for the code $\mathcal{C}$, such that if a uniformly random codeword $c \in \mathcal{C}$ is sent across BSC_p, then $\Pr_{c \in \mathcal{C}, BSC}[\{\text{decoding error}\}] \leq \varepsilon$. Then, show that there exists a (possibly randomized) decoder D' such that, if a uniformly random codeword $c \in \mathcal{C}$ is sent across BEC_{2p}, we will have $\Pr_{c \in \mathcal{C}, BEC}[\{\text{decoding error}\}] \leq \varepsilon$.

Note that the code $\mathcal{C}$ may be arbitrary, and you should only use the decoder D in a black-box way. *(Hint: Try to define D' to reduce the BEC_{2p} channel to a BSC_p channel).*

3 A Binary Code

Consider a binary code $\mathcal{C}$ spanned by the following rows

$$\begin{gathered} 010100 \\ 110010 \\ 001100 \\ 011000 \end{gathered}$$

(a) What is the size of $\mathcal{C}$? What is the rate of $\mathcal{C}$? What is the minimum weight of $\mathcal{C}$?

(b) How many errors can this code detect, correct? How many erasures can this code correct?

(c) Identify all correctable and non-correctable errors.

(d) Determine the generator matrix for $\mathcal{C}$ in the form $G = [\ I \mid P\ ]$.