Spring 2016

6.441 - Information Theory

Homework 7

Due: Tue, Apr 12, 2016 (in class)

Prof. Y. Polyanskiy

1 Reading (optional)

1. Read [1, Chapter 7]

2 Exercises

NOTE: Each exercise is 10 points. Only 3 exercises per assignment will be graded. If you submit more than 3 solved exercises please indicate which ones you want to be graded.

1 Consider a random transformation where $\mathcal{A} = \mathcal{B} = \{1, \dots, L\}$ and

$$P_{Y|X}(x|x) = P_{Y|X}([x+1]|x) = 1/2$$

with $[\ell]$ denoting modulo L, i.e. $[\ell] = \ell$ for $\ell \in \{1, \dots, L\}$ and $[L+1] = 1$.

1. Give the best upper bound you can find on the cardinality of a code with average error probability $\epsilon = 0.1$.
2. Let $L = 1024$. How many bits can be conveyed with zero error probability?
3. Compute the DT achievability bound with uniform P_X.
4. Let $L = 1024$. How many bits can be conveyed if we allow bit error rate equal to 0.1?

2 Consider a memoryless binary erasure channel with erasure probability 0.1 and blocklength equal to 10 (formally: $\mathcal{X} = \{0,1\}^{10}$, $\mathcal{Y} = \{0, 1, \mathtt{e}\}^{10}$ and $P_{Y|X}$ acts on $\mathcal{X}$ by erasing each bit independently with probability 0.1).

1. Find a lower bound on the bit error rate achievable by a code with rate 1/2 (i.e. a code with 32 codewords).
2. Find the smallest ϵ for which you can guarantee that a $(32, \epsilon)_{avg}$-code exists.

3 Bounds for the binary erasure channel (BEC). Consider a code with $M = 2^k$ operating over the blocklength n BEC with erasure probability $\delta \in [0, 1)$.

1. Show that regardless of the encoder-decoder pair:

$$\mathbb{P}[\text{error}|\#\text{erasures} = z] \ge \left|1 - 2^{n-z-k}\right|^+$$

2. Conclude by averaging over the distribution of z that the probability of error ϵ must satisfy

$$\epsilon \ge \sum_{\ell=n-k+1}^{n} \binom{n}{\ell} \delta^\ell (1-\delta)^{n-\ell} \left(1 - 2^{n-\ell-k}\right), \tag{1}$$

3. By applying the DT bound with uniform P_X show that there exist codes with

$$\epsilon \le \sum_{t=0}^{n} \binom{n}{t} \delta^t (1-\delta)^{n-t} 2^{-|n-t-k+1|^+} . \tag{2}$$

4. Fix $n = 500$, $\delta = 1/2$. Compute the smallest k for which the right-hand side of (1) is greater than 10^{-3}.
5. Fix $n = 500$, $\delta = 1/2$. Find the largest k for which the right-hand side of (2) is smaller than 10^{-3}.
6. Express your results in terms of lower and upper bounds on $\log M^*(500, 10^{-3})$.

4 Recall that in the proof of the DT bound we used the decoder that outputs (for a given channel output y) the first c_m that satisfies

$$\{i(c_m; y) > \log \beta\} . \tag{3}$$

One may consider the following generalization. Fix $E \subset \mathcal{X} \times \mathcal{Y}$ and let the decoder output the first c_m which satisfies

$$(c_m, y) \in E$$

By repeating the random coding and the steps in lectures show that the average probability of error satisfies

$$\mathbb{E}\left[P_e\right] \le \mathbb{P}[(X,Y) \notin E] + \frac{M-1}{2} \mathbb{P}[(\bar{X}, Y) \in E] ,$$

where

$$P_{XY\bar{X}}(a, b, \bar{a}) = P_X(a) P_{Y|X}(b|a) P_X(\bar{a}) .$$

Conclude that the optimal E is given by (3) with $\beta = \frac{M-1}{2}$.

5 A magician is performing card tricks on stage. In each round he takes a shuffled deck of 52 cards and asks someone to pick a random card N from the deck, which is then revealed to the audience. Assume the magician can prepare an arbitrary ordering of cards in the deck (before each round) and that N is distributed binomially on $\{0, \ldots, 51\}$ with mean $\frac{51}{2}$.

1. What is the maximal number of *bits per round* that he can send over to his companion in the room? (in the limit of infinitely many rounds)
2. Is communication possible if N were uniform on $\{0, \ldots, 51\}$? (In practice, however, nobody ever picks the top or the bottom ones)

6 [Wozencraft ensemble] Let $\mathcal{X} = \mathcal{Y} = \mathbb{F}_q^2$, a vector space of dimension two over Galois field with q elements. A Wozencraft code of rate 1/2 is a map parameterized by $0 \neq u \in \mathbb{F}_q$ given as $a \mapsto (a, a \cdot u)$, where $a \in \mathbb{F}_q$ corresponds to the original message, multiplication is over $\mathbb{F}_q$ and $(\cdot, \cdot)$ denotes a 2-dimensional vector in $\mathbb{F}_q^2$. We will show there exists u yielding a $(q, \epsilon)_{avg}$ code with

$$\epsilon \le \mathbb{E}\left[\exp\left\{-\left|i(X;Y) - \log\frac{q^2}{2(q-1)}\right|^+\right\}\right] \tag{4}$$

for the channel $Y = X + Z$ where X is uniform on $\mathbb{F}_q^2$, noise $Z \in \mathbb{F}_q^2$ has distribution P_Z and

$$i(a; b) \triangleq \log \frac{P_Z(b-a)}{q^{-2}} .$$

1. Show that probability of error of the code $a \mapsto (av, au) + h$ is the same as that of $a \mapsto (a, auv^{-1})$.
2. Let $\{X_a, a \in \mathbb{F}_q\}$ be a random codebook defined as

$$X_a = (aV, aU) + H \,,$$

with V, U – uniform over non-zero elements of $\mathbb{F}_q$ and H – uniform over $\mathbb{F}_q^2$, the three being jointly independent. Show that for $a \neq a'$ we have

$$P_{X_a, X'_a}(x_1^2, \tilde{x}_1^2) = \frac{1}{q^2(q-1)^2} 1\{x_1 \neq \tilde{x}_1, x_2 \neq \tilde{x}_2\}$$

3. Show that for $a \neq a'$

$$\begin{aligned} \mathbb{P}[i(X'_a; X_a + Z) > \log \beta] &= \frac{q^2}{(q-1)^2} \mathbb{P}[i(\bar{X}; Y) > \log \beta] - \frac{1}{(q-1)^2} \mathbb{P}[i(X; Y) > \log \beta] \\ &\leq \frac{q^2}{(q-1)^2} \mathbb{P}[i(\bar{X}; Y) > \log \beta] \,, \end{aligned}$$

where $P_{\bar{X}XY}(\bar{a}, a, b) = \frac{1}{q^4} P_Z(b - a)$.
4. Conclude by following the proof of the DT bound with $M = q$ that the probability of error averaged over the random codebook $\{X_a\}$ satisfies (4).

References

[1] T. Cover and J. Thomas, *Elements of Information Theory,* Second Edition, Wiley, 2006