# Information Theory Exercise Sheet #5

## (Error-Correcting Codes and Zero-Error Channel Coding)

University of Amsterdam, Master of Logic, Fall 2015
Lecturer: Christian Schaffner
TA: Mathias Madsen

Out: Wednesday, 25 November 2015
(due: Wednesday, 2 December 2015, 9:00)

1. **Error Probability of Repetition Code**

   (a) Show that the probability of error of $R_n$, the repetition code with $n$ repetitions, is

   $$p_e^{(n)} = \sum_{k=(n+1)/2}^{n} \binom{n}{k} f^k (1-f)^{n-k}$$

   when $n$ is odd and $R_n$ is used over a binary symmetric channel with error probability $f$.

   (b) Assuming $f = 0.1$, which of the terms in this sum is the biggest? How much bigger is it than the second-biggest term?

   (c) Use Stirling's approximation (see Exercise 12 in Series 1) to approximate $\binom{n}{k}$ in the largest term and find, approximately, the probability of error of the repetition code with $n$ repetitions.

   (d) Assuming $f = 0.1$, how many repetitions are required to get the probability of error down to $10^{-20}$? Answer: about 83

2. **Hamming codes**

   (a) Decode the following strings 1101011, 0110110, 0100111, 1111111 according to the $(2^4, 7)$-Hamming code.

   (b) Find some noise vectors that give the all-zero syndrome (that is, noise vectors that leave all the parity checks unviolated). How many such noise vectors are there?

3. **Another Linear Code** Consider the following linear code $C$ given by the generator matrix

$$G^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

(a) What is the parity check matrix $H$?

(b) How many bits can $C$ encode? How long are its codewords? How many different codewords are there?

(c) What is the minimal distance?

(d) Encode the strings 101, 111 according to $C$.

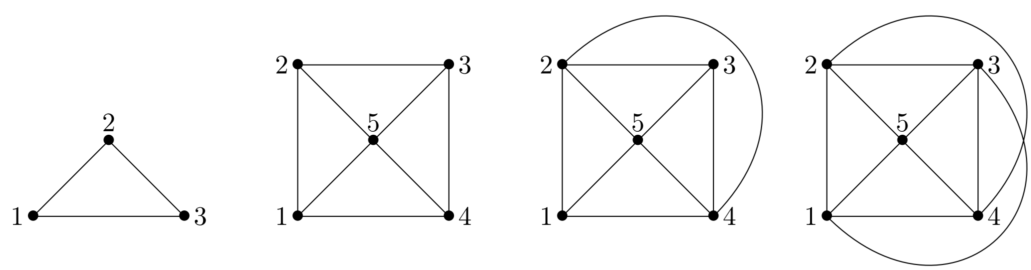
(e) Decode 1011010, 1110110, 1111110, and 1111111.

4. **Confusability Graphs from Channels** For each of the channels below, give the corresponding confusability graph.

   (a) $\mathcal{X} = \{1,2,3,4,5\}$, $\mathcal{Y} = \{a,b,c\}$, $P_{Y|X}(a|1) = P_{Y|X}(b|1) = P_{Y|X}(a|2) = P_{Y|X}(b|2) = \frac{1}{2}$, $P_{Y|X}(b|3) = \frac{1}{3}$, $P_{Y|X}(c|3) = \frac{2}{3}$, $P_{Y|X}(c|4) = P_{Y|X}(c|5) = 1$.

   (b) $\mathcal{X} = \{1,2,3,4,5\}$, $\mathcal{Y} = \{a,b,c,d\}$, $P_{Y|X}(a|2) = P_{Y|X}(b|2) = P_{Y|X}(c|2) = P_{Y|X}(a|4) = P_{Y|X}(c|4) = P_{Y|X}(d|4) = \frac{1}{3}$, $P_{Y|X}(b|3) = P_{Y|X}(c|3) = \frac{1}{2}$, $P_{Y|X}(a|1) = P_{Y|X}(d|5) = 1$.

5. **Channels from Confusability Graphs** For each of the confusability graphs below, describe one of the possible corresponding channels. Try to minimize the number of output symbols you are using.




(a) (b) (c) (d)

   (e) Can you argue that you reached the minimal number of outputs in (a), (b), (c), (d) ?

   (f) Show that for any confusability graph $G$ with no isolated vertices, there exists a corresponding channel with $|E(G)|$ output symbols.

6. **Shannon capacity of the complete graph.** A graph $G$ with $n$ vertices $V(G) = \{1,2,\ldots,n\}$ is called *complete* if it has edges between any two vertices, i.e. $\forall i \neq j : ij \in E(G)$.

   (a) Compute $\alpha(K_n)$, the independence number of the complete graph.

(b) Show that $K_n \boxtimes K_n = K_{n^2}$.

(c) Use (a) and (b) to prove that the Shannon capacity of $K_n$ is 0.

Note that this result formally confirms the intuition that channels whose confusability graphs are complete are useless for zero-error communication, because all symbols can possibly be confused with each other.

7. **Disjoint graphs.** For two graphs $G$ and $H$, the graph $G + H$ is defined as the disjoint union of the two graphs[1]. Formally, assuming without loss of generality that $V(G) \cap V(H) = \emptyset$, then $V(G + H) = V(G) \cup V(H)$ and $E(G + H) = E(G) \cup E(H)$.

   For a graph $G$, the disjoint union of $t$ copies of $G$ is denoted as $G^{+t}$. Similarly, we write $G^{\boxtimes t}$ for the $t$-time strong product of $G$ with itself.

   (a) Prove that $\alpha(G + H) = \alpha(G) + \alpha(H)$.

   (b*) Prove that for any three graphs $G, H, L$, it holds that

   $$(G + H) \boxtimes L = (G \boxtimes L) + (H \boxtimes L)$$

   and for the same reason, it also holds that

   $$G \boxtimes (H + L) = (G \boxtimes H) + (G \boxtimes L)\,.$$

   (c) Use (b) to derive that for any natural number $k \in \mathbb{N}$, $(G + G)^{\boxtimes k} = (G^{\boxtimes k})^{+2^k}$.

8. **Zero-Error Capacity of "Same-Parity Channel"** Let $\mathcal{X} = \mathcal{Y} = \{1, 2, 3, 4, 5, 6\}$. In this exercise, we compute the zero-error Shannon capacity of the noisy channel with transition probabilities $P_{Y|X}(y|x) = 1/3$ if and only if $x \equiv y \mod 2$.

   (a) Give the confusability graph $G$ of the noisy channel $P_{Y|X}$ described above.

   (b) Use 7.(c) and 6.(a) and 6.(b) to show that the Shannon capacity of $G$ is 1.

Homework is exercises 3, 4, 5, 8.

[1] You can think of $G + H$ as $G$ and $H$ "next to each other".