

Homework problem set 5

Your homework must be handed in **electronically via Moodle before Friday December 9th, 20:00h**. This deadline is strict and late submissions are graded with a 0. At the end of the course, the lowest of your 6 weekly homework grades will be dropped. You are strongly encouraged to work together on the exercises, including the homework. However, after this discussion phase, you have to write down and submit your own individual solution. Numbers alone are never sufficient, always motivate your answers.

Problem 1: Hadamard code (12pt)

For two k -bit strings x and y , the inner product is defined as

$$\langle x, y \rangle := \sum_{i=1}^k x_i \cdot y_i \quad \text{mod } 2.$$

Note that the inner product of two strings is a single bit. The k -bit Hadamard code is defined such that the codeword of x is the concatenation of all possible inner products with x , i.e.

$$\text{enc}(x) := (\langle x, y \rangle)_{y \in \{0,1\}^k}.$$

Here, the y are ordered [lexicographically](#).

- (a) **(1pt)** Find the codewords for 010 and 1101 using the 3-bit and 4-bit Hadamard codes respectively.
- (b) **(2pt)** Give the explicit generator matrix G^T for $k = 3$. Describe how to construct the generator matrix for arbitrary k .
- (c) **(2pt)** For a fixed non-zero $x \in \{0,1\}^k$, what is the probability that a uniformly random $y \in \{0,1\}^k$ is such that $\langle x, y \rangle = 1$?
- (d) **(1pt)** Use (c) to find the minimal distance of the k -bit Hadamard code.

There is some unnecessary redundancy in the Hadamard code. For example, the first bit of $\text{enc}(x)$ is always 0, regardless of what x is. The *punctured* k -bit Hadamard code attempts to solve this. It considers only the inner products with strings y such that $y_1 = 1$:

$$\text{enc}'(x) := (\langle x, y \rangle)_{y \in \{1\} \times \{0,1\}^{k-1}}$$

- (e) **(3pt)** Find the minimal distance of the punctured k -bit Hadamard code using a similar approach as in (c) and (d).
- (f) **(2pt)** Compute the rates of the k -bit Hadamard code and the punctured k -bit Hadamard code as a function of k . Which is better?
- (g) **(1pt)** What goes wrong if we try to puncture this code again? The doubly punctured k -bit Hadamard code is defined by

$$\text{enc}''(x) := (\langle x, y \rangle)_{y \in \{1\} \times \{1\} \times \{0,1\}^{k-2}}$$

Problem 2: Shannon capacity of the complete graph (6pt)

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

- (a) **(2pt)** Compute $\alpha(K_n)$, the independence number of the complete graph of size n .
- (b) **(2pt)** Show that $K_n \boxtimes K_n = K_{n^2}$.
Hint: the \LaTeX command for \boxtimes is `\boxtimes` (in the `amssymb` package). See also [Detexify](#).
- (c) **(2pt)** 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.

Problem 3: Disjoint graphs (5 + 2 pt)

For two graphs G and H , the graph $G + H$ is defined as the disjoint union of the two graphs. Formally, assuming without loss of generality that $V(G) \cap V(H) = \emptyset$, then $V(G + H) = V(G) \cup V(H)$ and $E(G + H) = E(G) \cup E(H)$. (You can think of $G + H$ as G and H “next to each other”).

(a) (2pt) Prove that $\alpha(G + H) = \alpha(G) + \alpha(H)$.

★ (2 bonus points) 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

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

(b) (3pt) Use ★ to derive that for any natural number $k \in \mathbb{N}$, $(G + G)^{\boxtimes k} = (G^{\boxtimes k})^{+2^k}$.

Problem 4: Same-parity channel (6pt)

Let $\mathcal{X} = \mathcal{Y} = \{1, 2, 3, 4, 5, 6\}$. In this exercise, you will 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 and y have the same parity (i.e. $x \equiv y \pmod{2}$).

(a) (2pt) Give the confusability graph G of the noisy channel $P_{Y|X}$ described above.

(b) (4pt) Compute the Shannon capacity of G .

Hint: use several results from the previous two exercises.