MAT4430, Exercises-sheet 3, to be discussed 12.02.2026

Exercise This exercise is about the Hamming $(7,4)$-code from Lecture 5, see also [1, Section 4.3.2]. Here we use the channel $N = \mathrm{BSC}_p^7$, with $p \in [0,1]$, where $\mathcal{X} = \mathcal{Y} = \{0,1\}^7$.

(i) Read and understand the description of the code set $\mathcal{C}$ as a subset of $\{0,1\}^7$ in terms of the three intersecting circles from [1, Figure 4.4]. Pick any element from $\mathcal{C}$ different from $(1,0,0,1,1,1,0)$ and plot it in the diagram, similar to [1, Figure 4.5].

(ii) Recall that we obtain the code as all 7-bitstrings of the form $z \cdot G$, where $z = (b_1, b_2, b_3, b_4) \in \{0,1\}^4$ is multiplied from the right with G. Recall that we defined a decoder $\overline{D} : \mathcal{Y} \to \mathcal{C}$ by $\overline{D}(y) = y - e$, assuming that a vector $e \in \{0,1\}^7$ can be found with a single entry equal to 1. For $x \in \mathcal{C}$, we have that

$$P(x \notin \overline{D}(\mathcal{Y})) = \sum_{\{y \in \mathcal{Y} | \overline{D}(y) \neq x\}} N(y|x).$$

Find an expression for the right hand side, using the product formula for $N(y|x)$.

(iii) Consider the maximum-likelihood decoder $D : \mathcal{Y} \to \{0,1\}^4$ together with the encoder $E : \{0,1\}^4 \to \{0,1\}^7$ given by $E(z) = z \cdot G$, as described in (i), see also the list in [1, Section 4.3.2]. Show that D is a decoder for E if a single bit in $E(z)$ has been flipped. (Hint: How many powers of p and $1-p$ enter in $N(y|x)$, for $x = E(z)$?).

Estimate the probability of unsuccessful decoding for the triple (N, D, E) given in the form

$$\max_{b_1, \cdots, b_4 \in \{0,1\}} P(E(z) \notin D^{-1}(z)),$$

for $z = (b_1, \ldots, b_4)$.

References

[1] A. Muller-Hermes, Lecture notes on quantum information theory, 2025.