EXERCISES 2

Excercise 1 (Probabilistic method)**.** In this exercise, you should try to find a probabilistic proof for a statement in linear algebra. Consider vectors $v_1, \dots, v_n \in \mathbb{R}^n$ with Euclidean norms $\|v_i\|_2 = 1$. We want to show that there exist signs $\epsilon_1, \dots, \epsilon_n \in \{-1, +1\}$ such that

$$\|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|_2 \leqslant \sqrt{n}.$$

(1) Choose random signs $\epsilon_1, \dots, \epsilon_n \in \{-1, +1\}$ uniformly and independently and consider the random variable

$$N = \|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|_2^2.$$

Compute the expectation value $\mathbb{E}[N]$ and conclude the desired statement.

(2) Show that there also exist signs $\epsilon_1, \dots, \epsilon_n \in \{-1, +1\}$ such that

$$\|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|_2 \geqslant \sqrt{n}.$$

Excercise 2 (Data processing inequality for the mutual information)**.** Let $p_{AB} \in \mathcal{P}(\Sigma_A \times \Sigma_B)$ denote a joint distribution and $N : \Sigma_B \to \mathcal{P}(\Sigma_C)$ a classical channel. Show that

$$I(A:B)_{p_{AB}} \geqslant I(A:C)_{q_{AC}},$$

where $q_{AC} \in \mathcal{P}(\Sigma_A \times \Sigma_C)$ is the distribution given by

$$q_{AC}(x,z) = \sum_{y \in \Sigma_B} N(z|y) p_{AB}(x,y).$$

Excercise 3 (The $(7,4)$-Hamming code)**.** The $(7,4)$-Hamming code encodes four bits of information into seven bits as follows. To bits $b_1, b_2, b_3, b_4 \in \{0,1\}$ we assign the codeword

$$E(b_1, b_2, b_3, b_4) = (b_1, b_2, b_3, b_4, s_1, s_2, s_3),$$

with bits s_1, s_2, s_3 such that each of the four circles in the diagram depicted in Figure 1 contains an even number of 1s. Check your understanding by verifying

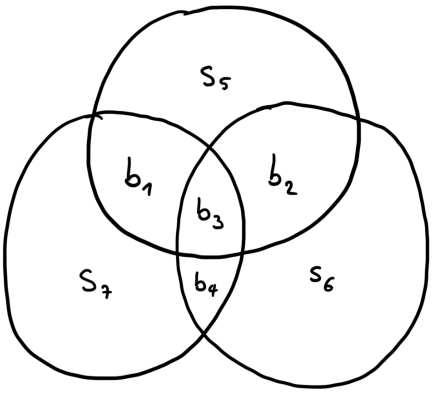


FIGURE 1. Defining codewords of the $(7,4)$-Hamming code.

that

$$E(1001) = (1001110).$$

In the following, we will study the performance of this code under the binary symmetric channel BSC_p for $p \in [0, 1/2]$.

(1) Find a simple rule to describe the maximum-likelihood decoder D for the $(7, 4)$-Hamming code and show that it corrects any single bit-flip.
(2) Compute the probability of a decoding error

$$p_e = \max_{b_1,\ldots,b_4} P(\mathrm{BSC}_p^{\times 7}(E(b_1, b_2, b_3, b_4)) \notin D^{-1}(b_1, b_2, b_3, b_4)).$$

(3) Compare the performance of the $(7, 4)$-Hamming code to the 3-repetition code. Which code is better?

Excercise 4 (The channel mutual information)**.** To quantify how noisy a classical channel is we introduce the *channel mutual information*. Let $N : \Sigma_A \to \mathcal{P}(\Sigma_B)$ denote a classical channel and consider the quantity

$$I(N) = \max_{p_A \in \mathcal{P}(\Sigma_A)} I(A : B)_{p_{AB}^N},$$

where for a given $p_A \in \mathcal{P}(\Sigma_A)$ the distribution $p_{AB}^N \in \mathcal{P}(\Sigma_A \times \Sigma_B)$ is given by

$$p_{AB}^N(x, y) = p_A(x)N(y|x).$$

The distribution p_{AB}^N can be understood as the joint distribution of inputs and outputs when input symbols chosen from a distribution $p_A \in \mathcal{P}(\Sigma_A)$ are send through the channel N.

(1) Compute the channel mutual information $I(\mathrm{BSC}_p)$ for the binary symmetric channel $\mathrm{BSC}_p : \{0, 1\} \to \mathcal{P}(\{0, 1\})$ introduced in the lecture.
(2) Compute the channel mutual information $I(\mathrm{Erase}_p)$ for the binary erasure channel $\mathrm{Erase}_p : \{0, 1\} \to \mathcal{P}(\{0, 1\})$ introduced in the lecture.
(3) Show that we have $I(N) = 0$ for a classical channel $N : \Sigma_A \to \mathcal{P}(\Sigma_B)$ if and only if the channel N is constant, i.e., there exists a probability distribution $q \in \mathcal{P}(\Sigma_B)$ such that $N(x) = q$ for every $x \in \Sigma_A$.