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 relative entropy)**.** Let $p, q \in \mathcal{P}(\Sigma_A)$ denote probability distributions and $N : \Sigma_B \to \mathcal{P}(\Sigma_C)$ a classical channel. Show that

$$D(N(p)\|N(q)) \leqslant D(p\|q).$$

(**Hint:** Use an inequality from the previous sheet.)

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

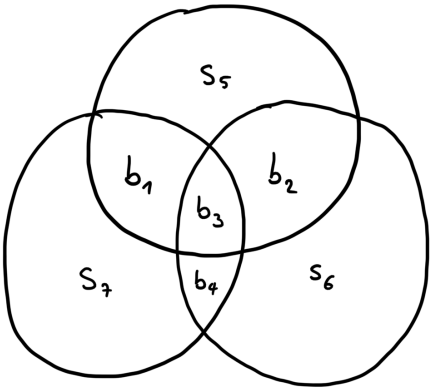


FIGURE 1. Defining codewords of the $(7, 4)$-Hamming code.

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
$$p_e = \max_{b_1,\dots,b_4} P(\mathrm{BSC}_p^{\times 7}(E(b_1,b_2,b_3,b_4)) \notin D^{-1}(b_1,b_2,b_3,b_4)).$$
(3) Compare the performance of the $(7,4)$-Hamming code to the 3-repetition code. Which code is better?

Excercise 4 (Information transmission and compression)**.** Consider the noiseless channel $N : \Sigma \to \mathcal{P}(\Sigma)$ such that $N(x) = \delta_x$ for every $x \in \Sigma$. Recall the notion of a (n, M, δ)-coding scheme consisting of a pair of functions $E : \{1,\dots,M\} \to \Sigma^n$ and $D : \Sigma^n \to \{1,\dots,M\}$ such that
$$\min_{m\in M} \mathrm{Prob}\left(N^{\times n} \circ E(m) \in D^{-1}(\{m\})\right) \geqslant 1-\delta.$$
Show that there is no sequence of (n, M_n, δ_n)-coding schemes such that $\delta_n \to 0$ as $n \to \infty$ and $\lim_{n\to\infty} \log(M_n)/n > \log(\Sigma)$.

(**Hint:** Relate this problem to data compression.)