Introduction to Coding Theory
2023-2024 - Homework 1

1. Apply Huffman's algorithm to construct q-ary codes with the prescribed probability distributions:
   a) $q = 3$, $P = \{0.3, 0.1, 0.1, 0.1, 0.1, 0.06, 0.05, 0.05, 0.05, 0.04, 0.03, 0.02\}$;
   b) $q = 4$, $P = \{0.3, 0.1, 0.1, 0.1, 0.1, 0.06, 0.05, 0.05, 0.05, 0.04, 0.03, 0.02\}$;

2. Suppose that $\{c_1, \cdots, c_n\}$ is an optimal binary prefix code for the probability distribution $\{p_1, \cdots, p_n\}$ satisfying $p_i > p_{i+1}$ for all $1 \leq i < n$. Find constants $0 < b < a < 1$ such that
   i) if $p_1 > a$ then the length of c_1 is 1;
   ii) if $p_1 < b$ then the length of c_1 is at least 2.
   Are your constants optimal with respect to those conditions?

3. Let C be the linear $[10, 5]$ code over$\mathbb{F}_3$ with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 1 & 0 \end{bmatrix}.$$

   a) Encode the message $(1, 2, 0, 2, 0)$;
   b) Compute the minimal distance of C;
   c) Decode, by syndrome decoding, the output $(1, 0, 2, 2, 0, 1, 2, 1, 0, 0)$

4. Let C be the code over $\mathbb{F}_3$ with parity-check matrix

$$H = \begin{bmatrix} 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 & 0 & 0 & 1 \end{bmatrix}$$

   and let

$$u = (\ 1 \quad 0 \quad 0 \quad ? \quad 0 \quad 0 \quad 2 \quad 0\ ), \qquad v = (\ 1 \quad 0 \quad 1 \quad 2 \quad ? \quad ? \quad 0 \quad 1\ )$$

   be outputs. Discuss the possible decoding of u and v.

5. Suppose that C is a binary $[31, 22, 5]$-linear code.
   a) Determine the number of cosets of C and the number of coset leaders with weight 0, 1 and 2;
   b) Determine, for each coset, an upper bound for the number of words of weight 3 contained in it;
   d) Show that the previous computations lead to a contradiction.

6. Let C be the code over $\mathbb{F}_3$ with parity-check matrix

$$H = \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \end{bmatrix}$$

   a) Determine the minimal distance of C and show it corrects any error pattern with weight 1 and also the error patterns

$$aa000000,\ 0aa00000,\ 00aa0000,\ 000aa000,$$

$$0000aa00,\ 00000aa0,\ 000000aa,\ a000000a,$$

   for $a \in \{1, 2\}$.
   b) Decode the outputs 11111112 and 11211200.

7. A q-ary Hamming code, ie a Hamming code over $\mathbb{F}_q$ (a field with q elements) is defined by a parity-check matrix H whose columns are representatives of the different 1-dimensional subspaces of $\mathbb{F}_q^m$, for some $m > 0$; we denote this code as $\mathcal{H}_m(q)$.
   a) Show that $\mathcal{H}_m(q)$ is a $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3]$-code.
   b) Compute the dimension and minimal distance of the dual of $\mathcal{H}_m(q)$.
   Hint: Use the form of the generator matrix H to compute the number of zero entries in a given codeword uH.