Combinatória e Teoria de Códigos
2020-21 - Teste I

1. Instructions

You are to work on this examination by yourself. Any hint of collaborative work will be considered as evidence of academic dishonesty. You are not to have any outside contacts concerning this subject, except myself.

This being a take-home examination, you are expected to hand back a legible document, in terms of the presentation of your answers. Results proven in the course notes may be quoted indicating simply the file and result number (e.g. Notes I, Theorem 10); if you use theorems or other results from other sources, you must identify this source and state them in full, including the proof.

Justify all the steps and include the results of computations. The use of a computer for algebraic computations (factorization of polynomials, tables of powers of primitive elements, solutions of linear equations, etc.) must be indicated. Simple numerical computations (e.g. computing the numerical value of an entropy) may be done with the use of a computer without explicitly mentioning it.

The questions are written in English but the answers may be written either in Portuguese or in English.

The Test has a total grade of 20. The grade of each question is displayed after the question number.

2. Test

1. Consider an alphabet with $m > 1$ symbols $\{x_1, \cdots, x_m\}$, to be encoded by a binary Huffman's algorithm. In what follows, denote by s_i the length of codeword associated to x_i, $s = \max\{s_i : 1 \le i \le m\}$, and by n_k the number of codewords of length k.

a) Assume that the symbols x_i occur with probability $1/m$.

i) (1.0) Determine s in terms of m; for what values of m is $n_s = m$?

ii) (1.0) Prove that $n_{s-1} + n_s = m$ and determine those values.

b) (1.5) Assume now that the probabilities $p_i = p(x_i)$ satisfy

$$p_1 > p_2 > \cdots > p_m;$$

Find additional conditions on the p_i that imply $s_1 = 1$ and $s_m = m - 1$.

2. (3.0) Consider the memoryless channel with input $\{0, 1\}$ and output $\{0, 1, ?\}$, and transition matrix

$$\begin{pmatrix} 1/2 & 0 & 1/2 \\ 1/4 & 1/2 & 1/4 \end{pmatrix}.$$

Let the input probability distribution be $p(x = 0) = p$ and $p(x = 1) = 1 - p$.

Determine the channel capacity in bits (ie, using $\log_2$) and the value of p for which it is achieved.

3. Let C be the $[11, 6]$ linear code over $\mathbb{F}_3$ with generator matrix $[I_6 \,|\, A]$ where I_6 is the identity matrix of dimension 6 and

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

a) (1.5) Determine the minimal distance d of C and justify that C is a perfect code.

b) (1.5) Decode the output $u = \{0, 2, 1, 1, 2, 2, 0, 2, 1, 1, 0\}$.

c) (1.5) Decode the output $u = \{2, 0, 2, 1, 0, 0, ?, 2, 2, ?, 1\}$.

4. (3.0) Show that a $[15, 8, 5]$ binary code C can not exist, in the following way:
Justify that C would have a basis $\{c_1, \cdots, c_8\}$ such that $w(c_1) = 5$.
Let C' be the subcode generated by $\{c_2, \cdots, c_8\}$; consider the punctured code $C'^{[S]}$, where S is the support (ie, the set of non-zero coordinates) of c_1.

5. (3.0) Show that a linear code with length n and minimal distance d over a field $\mathbb{F}_N$ is MDS if and only if for any set $S = \{i_1, \cdots, i_d\}$ of coordinates there exists a codeword with support S. How many codewords exist with the same support S ($|S| = d$)?

6. Recall that the covering radius of a $[n, k, d]$ code C over $\mathbb{F}_q$ is defined as

$$\rho(C) = \min\{r : \forall x \in \mathbb{F}_q^n \; \exists c \in C \text{ such that } \operatorname{dist}(x, c) \leq r\}.$$

a) (2.0) Show that $\rho(C)$ may be defined by each of the following
   i) $\rho(C) = \max_S \min\{w(x) : x \in S\}$, where S denotes a coset of C;
   ii) if H is a parity-check matrix for C, $\rho(C)$ is the minimum s such that any $u \in \mathbb{F}_q^{n-k}$ is a linear combination of some s columns of H.

b) (1.0) Prove that if C a binary even code and C^* denotes the puncturing of C at some fixed but arbitrary coordinate, then $\rho(C^*) = \rho(C) - 1$.