Combinatória e Teoria de Códigos
Exam - Part 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

1. (3.0) - Consider the transmission channel with input alphabet $\{x_1, x_2, x_3\}$, output alphabet $\{y_1, y_2, y_3\}$, and forward probabilities $p(y_j|x_i)$ given by the matrix

$$\begin{bmatrix} \frac{1}{6} & \frac{1}{3} & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{1}{2} & \frac{1}{6} & \frac{1}{3} \end{bmatrix}$$

Given the input probability distribution

$$p(x_1) = \frac{1}{2}, \qquad p(x_2) = p(x_3) = \frac{1}{4}$$

determine the best decision scheme for the decoding of a length 1 message and the associated average and maximum probabilities of error.

2. - Let C be a $[n, k]$ binary code with the property that, for any $1 \leq i \leq n$, exactly half of the codewords satisfy $c_i = 0$.

a) (2.0) Show that each coset has the same property.

b) (2.0) Let M be the $2^k \times n$ matrix whose rows are the codewords. Summing the entries in two ways show that the covering radius of C satisfies $cr(C) \leq \lfloor n/2 \rfloor$.

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

$$cr(C) = \min\{r | \forall x \in \mathbb{F}_q^n \, \exists c \in C \text{ such that } d(x, c) \leq r\}.$$

3. - Let C be the hexacode over $\mathbb{F}_4 = \mathbb{F}_2[a] = \{0, 1, a, a^2\}$, where $a^2 = a + 1$, with generator matrix

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

a) (3.0) Decode, if possible, the following output string:

$$(a, a, *, 1, a^2, a).$$

where $*$ denotes an erasure.

b) (2.0) Recall that the weight of a coset is the weight of any of its coset leaders. Show that all cosets of C have weight less or equal than 2 and that each coset of weight 2 has exactly 3 coset leaders, with mutual disjoint supports.

4. - Let C be a $[n,k]$ code over $\mathbb{F}_4$, with weight distribution $W_C(x) = \sum_{i=0}^{n} A_i x^i$.

a) (2.0) Show that the number of vectors of weight n in $C^\perp$ is $\sum_{i=0}^{n} A_i 3^{n-i}(-1)^i$.

b) (1.0) Show that, if all codewords $c \in C$ have even weight then $C^\perp$ contains some vector with weight n.

5. - Let $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$ where $\alpha^2 = \alpha + 1$. Consider the code C with generator matrix

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

a) (2.0) Prove that C is self-dual with respect to the Hermitian inner product $< x, y >= \sum_{i=1}^{6} x_i y_i^3$;

b) (3.0) Prove that C is 1-error correcting and decode, by syndrome decoding, the message $u = (\alpha, 1, 2\alpha, 2\alpha, 1, \alpha + 1)$.