Combinatória e Teoria de Códigos
Exam - 05/07/2019

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.

2

1. Consider a channel with input alphabet $X = \{a, b, c, d\}$, output $Y = \{1, 2, 3, 4\}$ and forward channel probability matrix (for the given orders of X and Y)

$$M = \begin{pmatrix} 1-s & s & 0 & 0 \\ s & 1-s & 0 & 0 \\ 0 & 0 & 1-t & t \\ 0 & 0 & t & 1-t \end{pmatrix}$$

where $0 \leq s, t, \leq 1$ are two parameters.
Suppose moreover that X has a probability distribution of the form $\{\frac{p}{2}, \frac{p}{2}, \frac{1-p}{2}, \frac{1-p}{2}\}$ (again, for the given order of X).

a) (1.0) Define and compute the entropy $H(Y)$ and the conditional entropy $H(Y|X)$;
b) (2.5) Find, for input probability distributions of the form given above, the value of p that maximizes the mutual information of the channel.

Note: Use the base 2 logarithm in your computations.

2. 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) (2.5) Decode, if possible, each of the following output strings

$$(1, a, a, *, 0, 1), \qquad (a, *, 1, *, a, a^2)$$

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.

3. Let C be a $[n, k]$ code over $\mathbb{F}_4$ with weight enumerator $W_C(z) = \sum_{i=0}^{n} A_i z^i$. Prove that

a) (2.0) the number of vectors with weight n in $C^\perp$ is $\sum_{j=0}^{n} (-1)^j 3^{n-j} A_j$;
b) (1.0) if C has only codewords of even weight, then $C^\perp$ contains some codeword with weight n.

4. Let C be the code over $\mathbb{F}_9 = \mathbb{F}_3[a]$, where $a^2 = a + 1$, defined by

$$C = \{(u(1), u(a), \cdots, u(a^7)) : u(x) \in P_4\}.$$

a) (3.0) Decode, determining the locator polynomial, $v = (1, a^2, 2a^2, a^3, 1, 0, a, 2a)$.
b) (2.0) Determine a generator matrix for the trace code $Tr(C)$.

5. Consider the following generator matrices of binary $[3, 2]$ convolutional codes:

$$G_1 = \begin{bmatrix} 1+D & D & 1+D^2 \\ 0 & D & 1+D \end{bmatrix} \qquad G_2 = \begin{bmatrix} 1 & 0 & D \\ 0 & D & 1+D \end{bmatrix}$$

a) (2.0) Are G_1 and G_2 basic and/or reduced?
b) (2.0) The following string is received as the output of a finite message encoded by G_2:

$$r = 001 \quad 101 \quad 011 \quad 010 \quad 111 \quad 101 \quad 100 \quad 010$$

Apply Viterbi's algorithm to find the codewords at minimal distance from r.