Homework 11
Science de l'information

Problem 1

Let $F = F_7$. Consider the system of linear equations

$$\begin{aligned} x_1 + 3x_2 + 2x_3 &= 2, \\ 4x_1 + 4x_2 + 4x_3 &= 2, \\ 3x_1 + x_2 + 3x_3 &= 0. \end{aligned}$$

(a) Write this system in matrix form as $\mathbf{A}\mathbf{x}^{\mathbf{T}} = \mathbf{u}^{\mathbf{T}}$. What are $\mathbf{A}, \mathbf{x}, \mathbf{u}$, and what are their dimensions ?

(b) Consider the matrix $\mathbf{A}$ first as a matrix over the integers. You can check that it has determinant equal to -8. What is the determinant of $\mathbf{A}$ if you consider it as a matrix over F_7?

(c) Show that the system can be solved uniquely over F_7.

(d) Solve the system over F_7 using Gaussian elimination.

(e) If you had to solve an $n \times n$ system. How complex is Gaussian elimination, i.e., how many elementary operations (addition, multiplication, etc.) will you need ?

Problem 2

We consider a binary code generated by the matrix

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

This means that

$$C = \{x : x = uG, u \in F_2^4\}.$$

(a) Is the word $(1, 0, 1, 0, 1, 0, 1)$ a codeword?

(b) How many codewords are generated by this code? Give a list of them.

(c) Assume that you receive the word $(?, ?, 0, 1, 1, 1, 1)$ where the first two components have been erased. You would like to reconstruct the codewords. Can this be done and how could you proceed. What is the complexity of your approach?

(d) Let C be the vector space of the words generated by this code, and let $C^{\perp}$ be its dual. Find $C^{\perp}$ (give the list of all its elements).

(e) Give a basis for the vector space $C^{\perp}$. Such a basis is usually denoted by the matrix H. It is called the parity-check matrix of the code C.

Problem 3

Let $r \geq 2$ be an arbitrary integer. Consider all non-zero binary vectors of length r and list them as the column of a matrix, called $\mathbf{H}_r$.

(a) What is the size of the matrix $\mathbf{H}_r$ as a function of r?

(b) Assumethat the vectors are in $\mathbb{F}_2$. Let t be the minimum number of columns of $\mathbf{H}_r$ which are linearly dependent, i.e., there exist columns indicated by $h_{i_1}, h_{i_2}, \ldots, h_{i_t}$ and binary numbers $c_1, c_2, \ldots, c_t$ such that

$$\sum_{j=1}^{t} c_j h_{i_j} = 0.$$

Prove that $t = 3$ for any $r \in \mathbb{N}$.

(c) Proof that $\mathbf{H}_r$ is a full-rank matrix. (HINT: recall that the columns of $\mathbf{H}_r$ are ALL the non-zero binary r-tuples. Try to arrange these columns in a particular way so that the left-most $r \times r$ matrix has rank r.)

(d) Given the fact that $\mathbf{H}_r$ is a full-rank matrix, find the size of the right kernel of $\mathbf{H}_r$, that is the number of vectors $\mathbf{x}$ which satisfy $\mathbf{H}_r \cdot \mathbf{x} = \mathbf{0}$.

(e) Define the code $\mathcal{C}_r$ as the set of vectors $\mathbf{x}$ is part (c). Show that this code is linear. Find the codeword length, dimension, minimum distance and the rate of the code.