Information and coding theory

Exercise sheet n° 6 :

6-1. We define a Hamming code with the 4×6 parity matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & h_{1,6} \\ 1 & 1 & 0 & 0 & 0 & h_{2,6} \\ 0 & 1 & 1 & 0 & 0 & h_{3,6} \\ 1 & 0 & 0 & 1 & 0 & h_{4,6} \end{pmatrix}.$$

(a) If one choses $h_{1,6} = h_{2,6} = h_{3,6} = h_{4,6} = 1$, determine the list of codewords. What is the amount of information and parity bits ? How many errors does this code correct ?

(b) Show that the variables $h_{1,6}, h_{2,6}, h_{3,6}, h_{4,6}$ cannot be chosen in a way such that this code corrects a single error and detects as well (without correcting them) two errors.

Help : For a minimal Hamming distance x all sets of $x-1$ columns of H have to be linearly independent.

6-2. *Generator of a Hamming code.* We call a $k \times n$ matrix G with k linearly independent rows (codewords) a generator of a binary code (n, k). Each of the 2^k codewords can be thus expressed in terms of a linear combination of the rows of G.

(a) Determine the parity matrix of the code with the generator

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Which are the correction and/or detection properties of this code ?

(b) The same question as (a) for the generator

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}.$$

6-3. *Hamming code.* Show that a Hamming code corrects up to $e-1$ errors and detects (but does not necessarily correct) up to e errors *if and only if* all sets of $2e-1$ columns of the parity matrix are linearly independent.

6-4. Optional. Show that the minimal distance of a Hamming code is equal to d *if and only if* all non-zero codewords have at least d bits equal to 1, and at least one of them has *exactly* d bits equal to 1.