MAD 6607: Coding Theory

Edoardo Persichetti Test 1 Solutions

Make sure you explain all your answers clearly and in detail. Answers such as "2" or "Yes" will be treated as incomplete and won't receive full credit.

Exercise 1 A simple definition of linear code over a generic finite field would be the following.

"A linear code over a finite field $\mathbb{F}_q$ is a set $\mathcal{C}$ of vectors $c \in \mathbb{F}_q^n$ called *codewords* which satisfy the condition $Hc^T = 0$ for a certain $r \times n$ matrix H over $\mathbb{F}_q$ called *parity-check matrix*".

Exercise 2 Consider the code $\mathcal{C}$ given by the following generator matrix.

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

a) $\mathcal{C}$ has length $n = 7$ (number of columns of G) and dimension $k = 3$ (number of rows of G).

b) We have $\mathcal{C} = \{0000000, 0110011, 0100101, 1000011, 0010110, 1110000, 1100110, 1010101\}$. The simplest way to obtain these is to multiply all possible messages (binary vectors of length 3) by the generator matrix. In total there are $2^k = 2^3 = 8$ codewords.

c) The minimum distance of this code corresponds to the lowest weight of its codewords, hence we have $d = 3$. So this code can correct $\lfloor \frac{d-1}{2} \rfloor = 1$ error.

d) We row-reduce and in particular all we need to do is replace the third row with the sum of the second and third row. Thus:

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

e) A parity-check matrix can be found from the systematic generator by transposing the non-identity part and adjoining a new identity matrix on the right (respecting dimension and co-dimension).

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

f) To verify that H is a parity-check matrix we can simply check that $H \cdot G^T = \mathbf{0}$.

Exercise 3 Consider again the code $\mathcal{C}$ and suppose to receive the word $y = 1010111$.

a) After multiplying with H we find that the syndrome of y is the vector 0010.

b) Notice that this is in fact the sixth column of H, and corresponds to the syndrome of the vector 0000010, which is the coset leader. Thus we have $c = y - e = 1010111 - 0000010 = 1010101$ (which was one of the codewords we had listed).

Exercise 4 We extend the code $\mathcal{C}$ by adding an overall parity check, and write the new parity-check matrix below.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Doing so we obtain a $[8, 3, 4]$ code.

Exercise 5 Given a code $\mathcal{C}$ the dual code $\mathcal{C}^{\perp}$ is defined as the set $\{u : u \cdot v = 0, v \in \mathcal{C}\}$. In our example, we get a code of length 7 and dimension 4, generated by H (list of codewords omitted). It is easy to verify that $\mathcal{C}$ is not even weakly self-dual since for instance the codeword 1000011 (first row) is not orthogonal to 0100101 (second row), or equivalently, that for instance neither of those vectors is a codeword of $\mathcal{C}^{\perp}$.

Exercise 6 This code has parameters $n = (q^r - 1)/(q - 1)$ and length $k = n - r$ with minimum distance 3, and in our case we have $q = 3, r = 2$, so we are going to build a $[4, 2, 3]$ code. Since parity-check matrices of Hamming codes have pairwise linearly independent columns, we can choose any such 4 columns, for instance

$$H' = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \text{ or } H'' = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}$$

Let's choose H'' since it is in systematic form. For this choice of parity-check matrix, we have $\mathcal{H}_2 = \{0000, 0111, 1021, 1102\}$ and $\mathcal{H}_2^T = \{0000, 1210, 2201, 0111\}$ and so clearly this is not even weakly self-dual.