

Exercises

CODING THEORY

Annamaria Iezzi and Elisa Lorenzo García

25/07/25

Exercise 1. Consider the *even weight code* $C \subset \mathbb{F}_q^n$ with $n \geq 2$, defined as the set of all vectors in \mathbb{F}_q^n with even weight. Compute the parameters n , q , M , k , redundancy, d , $R = k/n$. Check that it is a linear code only for $q = 2$ and give a generator matrix in this case.

Exercise 2. Prove that the binary ($q = 2$) even weight code with length n and the $[n, 1, n]$ -repetition code are dual.

Exercise 3. Explain the decoding in the magic trick that Elisa performed to guess a number after 7 yes/no questions.

Exercise 4. We start by defining the following codes:

Definition. Set $n = \frac{q^r - 1}{q - 1}$ with $r \geq 2$. Define $H_r(q)$ as a $r \times n$ matrix over \mathbb{F}_q with non-zero columns and such that no 2 columns are linearly dependent. We define the q -ary *Hamming code* $\mathcal{H}_r(q)$ as the linear code having $H_r(q)$ as parity check matrix. The q -ary *simplex code* $\mathcal{S}_r(q)$ is the code having $H_r(q)$ as generator matrix.

Prove that the q -ary Hamming code $\mathcal{H}_r(q)$ has parameters $[n, n-r, 3]$ for $r \geq 2$ and that the q -ary simplex code $\mathcal{S}_r(q)$ is a constant weight code with parameters $\left[\frac{q^r - 1}{q - 1}, r, q^r - 1 \right]$.

Exercise 5. Prove that the code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 3 & 3 \\ 0 & 1 & 0 & 2 & 2 & 4 \\ 0 & 0 & 1 & 3 & 1 & 3 \end{pmatrix}$$

over \mathbb{F}_5 is self-dual.

Exercise 6. Give an example of a $[4, 2]_3$ self-dual code and show that there is no $[6, 3]_3$ self-dual code.

Exercise 7.

- (a) Prove that if the cyclic shift (by one position) of each row of the generator matrix is a codeword then the code is cyclic.
- (b) Consider the Hamming code $[7, 4, 3]_2$ with the following systematic generator matrix:

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

Prove that it is not a cyclic code.

Exercise 8. Describe all the cyclic codes of length 7 over \mathbb{F}_2 by giving a generator matrix for each of them.

Exercise 9.

Let \mathbb{F}_8 be the finite field with 8 elements, constructed as an extension of \mathbb{F}_2 using an irreducible polynomial of degree 3. Let α be a generator of the multiplicative group $\mathbb{F}_8 \setminus \{0\}$.

Consider the Reed–Solomon code $C = \text{RS}(7, 3) \subseteq \mathbb{F}_8^7$ defined as follows:

The code C consists of all evaluations of polynomials $f(x) \in \mathbb{F}_8[x]$ of degree at most 2 at the 7 nonzero elements of \mathbb{F}_8 , i.e., at the points $\alpha, \alpha^2, \dots, \alpha^7 = 1$.

- (a) Find the codewords corresponding to $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$.
- (b) Construct a generator matrix for the code C .
- (c) Show that C is cyclic and find its generator polynomial.
- (d) Let $q = p^r$, with p a prime number and let α be a generator of the multiplicative group $\mathbb{F}_q \setminus \{0\}$. Prove more in general that the Reed-Solomon code $\text{RS}(q-1, k) \subseteq \mathbb{F}_q^{q-1}$ obtained as evaluation of polynomials in $\mathbb{F}_q[x]$ of degree at most $k-1$ at $\alpha, \alpha^2, \dots, \alpha^{q-1} = 1$ is a cyclic code.