

Error correcting codes

Exercise 1. Construction of a Reed-Solomon code

a. Build a Reed-Solomon code over the field \mathbb{F}_8 of dimension 3, able to correct 2 errors. Give the corresponding generating matrix.

b. What code does it correspond to when $k = 1$?

Exercise 2. Dual of a GRS code

Let $C_1 = \mathcal{C}_{\text{GRS}}(n, k, \mathbf{x}, \mathbf{v})$ be a Generalized Reed Solomon code over a field K .

a. What is a generating matrix G for C_1 ?

b. Let $L_i = \prod_{j \neq i} (x_i - x_j)$. Show that the vector $(\frac{1}{L_1}, \frac{1}{L_2}, \dots, \frac{1}{L_n})$ is in the right kernel of

the Vandermonde matrix $V = \begin{bmatrix} 1 & \dots & 1 \\ x_1 & \dots & x_n \\ \vdots & & \vdots \\ x_1^{n-2} & \dots & x_n^{n-2} \end{bmatrix}$

c. Deduce that there exist a vector $w \in (K^*)^n$ such that

$$H = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & & & \vdots \\ x_1^{n-k-1} & x_2^{n-k-1} & \dots & x_n^{n-k-1} \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \dots \\ w_n \end{bmatrix}$$

verifies $GH^T = 0$.

d. Deduce that the dual of any Generalized Reed-Solomon code is a Generalized Reed-Solomon code in the same evaluation points.

Exercise 3. Alternant codes

Let C be an alternant code over a field \mathbb{F}_q built from a GRS codes over \mathbb{F}_{q^m} with parameters (n, k) .

a. Prove that the minimum distance of C is $\geq n - k + 1$.

b. Prove that its dimension is $\geq n - (n - k)m$.

Exercise 4. Mc Eliece

Recall that the Mc Eliece cryptosystem based on a code C over a field \mathbb{K} is defined by:

- the private key is composed of a generator matrix $G \in \mathbb{K}^{k \times n}$ of a code with an efficient decoding algorithm up to t errors, an invertible matrix $S \in \mathbb{K}^{k \times k}$, a permutation matrix $P \in \mathbb{K}^{n \times n}$;
- the public key is (\hat{G}, t) where $\hat{G} = SGP$
- the encryption function: $E : m \mapsto m\hat{G} + e$ where e is sampled uniformly with $w_H(e) \leq t$

- a. Recall how the decryption algorithm works.
- b. When instantiated with a Reed-Solomon code of length 256 and dimension 224 over \mathbb{F}_{256} , what is the maximum value for t . What is the size in kilobytes of the public key?
- c. For an arbitrary field (no longer assuming \mathbb{F}_{256}), suppose that a same message m is sent twice using McEliece cryptosystem. An attacker, has then access to two different ciphertexts c_1 and c_2 for the same message m . Explain why the attacker can deduce, with high probability of success, k positions in c_1 at which the corresponding error e_1 is zero.
- d. Deduce that there is then a polynomial time algorithm (state its cost) to compute m , and therefore decode c_1 without knowing the private key.
- e. Explain how does this attack generalizes for the *related plaintext attack*: when the ciphertexts c_1 and c_2 correspond to plain texts which difference is known to the attacker.
- f. Propose a countermeasure for this attack.

Exercise 5. Niederreiter encryption scheme

An alternative to Mc Eliece encryption scheme was proposed by Niederreiter based on the duality between the generating matrix and the parity check matrix.

Hence the public key, is formed by a matrix

$$H^{\text{pub}} = SH^{\text{priv}}P$$

where $H^{\text{priv}} \in K^{(n-k) \times n}$ is the parity check matrix of a secret Goppa code with error correction capacity t ; $S \in K^{(n-k) \times (n-k)}$ is a non-singular matrix and $P \in K^{n \times n}$ is a permutation matrix.

- a. Recall what is the Syndrom decoding problem, and how it relates to correcting errors ?
A cipher text in a Niederreiter encryption scheme is a syndrom, and the decryption is done by solving the Syndrom decoding problem.
- b. Explain why isn't it possible to define encryption procedure in the same way as in Mc Eliece encryption scheme.
Instead, the plaintext should formatted as a n -dimensionnal vector with only t non-zero coefficients.
- c. Explain how to encrypt such plaintexts, and how does the decryption work.