Exercises n° 4, Cyclic and BCH codes

Exercise 1. In this exercise, we give an alternative proof of the BCH bound using the discrete Fourier Transform.

Let n be an integer and $\mathbb{F}_q$ a finite field with q prime to n. Let $\mathbb{F}_q(\zeta_n)$ be a finite extension of $\mathbb{F}_q$ containing all the n–th roots of 1, ζ_n denotes a primitive n–th root of 1. The discrete Fourier transform is defined as

$$\mathcal{F} : \left\{ \begin{array}{ccc} \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) & \longrightarrow & \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \\ f & \longmapsto & \sum_{i=0}^{n-1} f(\zeta_n^{-i}) X^i \end{array} \right. .$$

1. Prove that $\mathcal{F}$ is an $\mathbb{F}_q$–linear map.
2. Prove that
$$\sum_{i=0}^{n-1} \zeta_n^{ij} = \left\{ \begin{array}{ccc} n & \text{if} & n|j \\ 0 & \text{else} & \end{array} \right. .$$
3. Prove that $\mathcal{F}$ is an isomorphism with inverse:
$$\mathcal{F}^{-1} : \left\{ \begin{array}{ccc} \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) & \longrightarrow & \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \\ f & \longmapsto & \frac{1}{n} \sum_{i=0}^{n-1} f(\zeta_n^{i}) X^i \end{array} \right. .$$
Indication: it suffices to prove that $\mathcal{F}^{-1}(\mathcal{F}(X^i)) = X^i$ for all $i = 0, \dots, n-1$.
4. For all $f, g \in \mathbb{F}_q(\zeta_n)[X]/(X^n - 1)$, denote by $f \star g$ the coefficientwise product:
$$\text{if } f = \sum_{i=0}^{n-1} f_i X^i \text{ and } g = \sum_{i=0}^{n-1} g_i X^i, \text{ then } f \star g = \sum_{i=0}^{n-1} f_i g_i X^i.$$
Prove that for all $f, g \in \mathbb{F}_q(\zeta_n)[X]/(X^n - 1)$, then
   (i) $\mathcal{F}(fg) = \mathcal{F}(f) \star \mathcal{F}(g)$;
   (ii) $\mathcal{F}(f \star g) = \frac{1}{n} \mathcal{F}(f)\mathcal{F}(g)$;
   (iii) $\mathcal{F}^{-1}(fg) = n(\mathcal{F}^{-1}(f) \star \mathcal{F}^{-1}(g))$;
   (iv) $\mathcal{F}^{-1}(f \star g) = \mathcal{F}^{-1}(f)\mathcal{F}^{-1}(g)$;

5. Let $g \in \mathbb{F}_q[X]/(X^n - 1)$ be a nonzero polynomial vanishing at $1, \zeta_n, \ldots, \zeta_n^{\delta-2}$ (in particular, it vanishes at $\delta - 1$ roots of $X^n - 1$ with consecutive exponents). Prove that

$$\mathcal{F}^{-1}(g) \equiv X^{\delta-1} h(X) \mod (X^n - 1)$$

   for some $h \in \mathbb{F}_q(\zeta_n)[X]$ where h is nonzero and has degree $\leqslant n - \delta$.

6. Using $\mathcal{F}(\mathcal{F}^{-1}(g))$ prove that g has at least δ nonzero coefficients.

7. Prove that of $g \in \mathbb{F}_q[X]/(X^n - 1)$ vanishes at $\zeta_n^a, \zeta_n^{a+1}, \ldots, \zeta_n^{a+\delta-2}$, then g also has at least δ nonzero coefficients.

8. Conclude.

Exercise 2 (A decoding algorithm for BCH codes)**.** Let $\mathbb{F}_q$ be a finite field and n be an integer prime to q. Let $\mathbb{F}_q(\zeta_n)$ be the smallest extension of $\mathbb{F}_q$ containing all the n–th roots of 1. Let $g \in \mathbb{F}_q[x]$ be a polynomial of degree $< n$ vanishing at $\zeta_n, \ldots, \zeta_n^{\delta-1}$ for some positive integer δ. Let C be the BCH code with generating polynomial g. The BCH bound asserts that C has minimum distance at least equal to δ. We will prove that the code is t–correcting, where $2t + 1 = \delta$ if δ is odd and $2t + 1 = \delta - 1$ if δ is even.

Let $y \in \mathbb{F}_q^n$ be a word such that

$$y = c + e$$

where $c \in C$ and e is a word of weight f with $f \leqslant t$. In what follows, all the words of $\mathbb{F}_q^n$ are canonically associated to polynomials in $\mathbb{F}_q[z]/(z^n - 1)$. For instance

$$e(z) = e_{i_1} z^{i_1} + \cdots + e_{i_f} z^{i_f}$$

where the e_{i_j}'s are nonzero elements of $\mathbb{F}_q$.

We introduce some notation and terminology.

- The *syndrome* polynomial $S \in \mathbb{F}_q(\zeta_n)[z]$:

$$S(z) \stackrel{\text{def}}{=} \sum_{i=1}^{2t} y(\zeta_n^i) z^{i-1}.$$

- The *error locator polynomial* $\sigma \in \mathbb{F}_q(\zeta_n)[z]$

$$\sigma(z) \stackrel{\text{def}}{=} \prod_{j=1}^{f} (1 - \zeta_n^{i_j} z).$$

1. Among the polynomials S and σ, which one is known and which one is unknown from the point of view of the decoder?

2. Prove that
$$S(z) = \sum_{i=1}^{2t} e(\zeta_n^i) z^{i-1}$$
and hence depends only on the error vector e.

3. Let ω be the polynomial defined as
$$\omega(z) \stackrel{\text{def}}{=} \sum_{j=1}^{f} e_{i_j} \zeta_n^{i_j} \prod_{k \neq j} (1 - \zeta_n^{i_k} z)$$

   Prove that

   (i) $\deg \omega < t$;

   (ii) $S(z)\sigma(z) \equiv \omega(z) \mod (z^{2t})$;

   (iii) σ and ω are prime to each other.

   Indication: to prove that two polynomials are prime to each other, it is sufficient to prove that no root of one is a root of the other.

4. Prove that if another pair (σ', ω') of polynomials satisfying $\deg \sigma' \leqslant t$, $\deg \omega' < t$ and $S(z)\sigma'(z) \equiv \omega'(z) \mod (z^{2t})$ then, there exists a polynomial $C \in \mathbb{F}_q(\zeta_n)[z]$ such that $\sigma' = C\sigma$ and $\omega' = C\omega$.

5. Let h be the largest integer such that $z^h | S(z)$. Prove that $h < t$. Deduce that the greatest common divisor of S and z^{2t} has degree $< t$.

6. By proceeding to the extended Euclidian algorithm to the pair (S, z^{2t}), there exist sequences of polynomials $P_0 = z^{2t}, P_1 = S, P_2, \ldots, P_r$ with $\deg P_0 > \deg P_1 > \deg P_2 > \cdots$ where P_r is the GCD of (S, z^{2t}) and $A_0, A_1, \ldots$ $B_0, B_1, \ldots$ such that for all i,
$$P_i = A_i S + B_i z^{2t}.$$

   Prove the existence of a polynomial C and an index i such that $P_i = C\omega$ and $A_i = C\sigma$.

   Remark : Actually a deeper analysis of extends Euclid algorithm makes possible to prove that C has degree 0 *and Equals* $B_i(0)$.

7. Describe a decoding algorithm for decoding BCH codes. What is its complexity?

Exercise 3. The goal of the exercise is to observe the strong relations between BCH and Reed-Solomon codes. Let $\mathbb{F}_q$ be a finite field and n be an integer prime to q.

1. We first consider the case $n = q - 1$.

   (a) Prove that if $n = q - 1$ then $\mathbb{F}_q$ contains all the n–th roots of 1.

Let ζ_n be such an n–th root, from now on the elements of $\mathbb{F}_q \setminus \{0\}$ are denoted by $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$.

(b) Then, in this situation, describe the minimal cyclotomic classes and the cyclotomic classes in general.

(c) Still in case where $n|(q-1)$, let C be a BCH whose set of roots contains $\zeta_n, \ldots, \zeta_n^{\delta-1}$. Prove that C has dimension $n-\delta+1$. Then prove that C is MDS.

(d) Let C' be the generalised Reed–Solomon code $C' \stackrel{\text{def}}{=} \mathbf{GRS}_{\delta-1}(\mathbf{x}, \mathbf{x})$ where $\mathbf{x} \stackrel{\text{def}}{=} (1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1})$. Recall that this code is defined as the image of the map

$$\left\{ \begin{array}{ccc} \mathbb{F}_q[z]_{<\delta-1} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(1),\ \zeta_n f(\zeta_n),\ \zeta_n^2 f(\zeta_n^2), \ldots,\ \zeta_n^{n-1} f(\zeta_n^{n-1})) \end{array} \right. .$$

Prove that $C' = C^{\perp}$.

Indication : a nice basis for C' can be obtained from the images by the above map of the monomials $1, z, z^2, \ldots, z^{\delta-2}$.

(e) Conclude that C is a generalised Reed Solomon (GRS in short) code.

2. Now, consider the general case : n is prime to q and C denotes the BCH code whose set of roots contains $\zeta_n, \ldots, \zeta_n^{\delta-1}$. Prove that C is contained in the subfield subcode of a GRS code with minimum distance δ.

3. Deduce from that a decoding algorithm based on the decoding of the GRS code. Compare its complexity with that of the algorithm presented in Exercise 2.