MPRI **Year 2015–16**

Module 2.13.2 : Error correcting codes and applications to cryptography

Mid term exam, December, 3 2015

You have 1h30. Your personal lecture notes, the online lecture notes and the exercise sheets together with the solutions are authorised

The two exercises are independent.

Exercice 1. Let $C \subseteq \mathbb{F}_q^n$ be a linear code. The *covering radius* of C is defined as the integer

$$\rho := \max_{y \in \mathbb{F}_q^n} \min_{c \in C} d_H(y, c).$$

Equivalently, it is the maximal distance between a word of $\mathbb{F}_q^n$ and the code C.

1. Prove that
$$\bigcup_{c \in C} \mathbf{B}_H(c, \rho) = \mathbb{F}_q^n.$$
2. What is the covering radius of a Hamming code ?
3. Let $(C_s)_{s \in \mathbb{N}}$ be a sequence of codes with parameters $[n_s, k_s, d_s]$ such that $\lim_{s \to +\infty} n_s = +\infty$ and such that the sequence $(\frac{k_s}{n_s})$ converges to a real number $R \in [0,1]$. Let ρ_s be the covering radius of C_s and assume that the sequence $(\frac{\rho_s}{n_s})$ converges to $P \in [0,1]$. Prove that
$$H_q(P) \geqslant 1 - R.$$
4. Prove that for any code $C \subseteq \mathbb{F}_q^n$ of dimension k, the covering radius of C is less than or equal to $n - k$. *Hint : One can proceed to Gaussian elimination.*

We will now focus on the covering radius of Reed–Solomon codes. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be an n-tuple of distinct elements of $\mathbb{F}_q$. Remind that for all $0 < k \leqslant n$,

$$\mathbf{RS}_k(\alpha) := \{(f(\alpha_1), \dots, f(\alpha_n)) \mid f \in \mathbb{F}_q[X],\ \deg f < k\}.$$

5. Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree k and $y_f := (f(\alpha_1), \dots, f(\alpha_n))$. Prove that the distance from y_f to $\mathbf{RS}_k(\alpha)$ satisfies
$$\min_{c \in \mathbf{RS}_k(\alpha)} d_H(y_f, c) = n - k.$$
6. Deduce that the covering radius of $\mathbf{RS}_k(\alpha)$ is $n - k$ and that, for every polynomial f of degree k, the distance between $(f(\alpha_1), \dots, f(\alpha_n))$ and $\mathbf{RS}_k(\alpha)$ equals this radius.
7. Assume that for all i, $\alpha_i \neq 0$. Prove that the distance between $(\alpha_1^{-1}, \dots, \alpha_n^{-1})$ and the code $\mathbf{RS}_k(\alpha)$ equals the covering radius of the code.

Continued next page please.

Exercice 2. In this exercise, $m > 1$ denotes an integer, $x_1, \dots, x_n$ is a tuple of distinct elements of $\mathbb{F}_{2^m}$ and $g \in \mathbb{F}_{2^m}[X]$ is a polynomial such that for all $i \in \{1, \dots, n\}$, we have $g(x_i) \neq 0$. To any $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_2^n$, we associate the polynomial[1] $\pi_{\mathbf{c}} := \prod_{i=1}^n (X - x_i)^{c_i}$. We define the **binary** code

$$\Gamma(\mathbf{x}, g) := \{\mathbf{c} \in \mathbb{F}_2^n \mid g \text{ divise } \pi'_{\mathbf{c}}\},$$

where $\pi'_{\mathbf{c}}$ denotes the derivative of $\pi_{\mathbf{c}}$.

The objective of the exercise is to study the parameters of these codes. Let us emphasize again that even if $g \in \mathbb{F}_{2^m}[X]$ and $x_1, \dots, x_n \in \mathbb{F}_{2^m}$, the code $\Gamma(\mathbf{x}, g)$ is **binary** (its elements are in $\mathbb{F}_2^n$).

1. For all $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_2^n$ we denote by $\mathbf{c} \cap \mathbf{c}' := (u_1, \dots, u_n)$ the vector with entries :
$$\forall i \in \{1, \dots, n\}, \quad u_i = \begin{cases} 1 & \text{if } c_i = c'_i = 1 \\ 0 & \text{otherwise.} \end{cases}$$
Prove that for all $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_2^n$, we have
$$\pi_{\mathbf{c}} \pi_{\mathbf{c}'} = \pi_{\mathbf{c}+\mathbf{c}'} \pi_{\mathbf{c} \cap \mathbf{c}'}^2$$
2. Prove that for all $\mathbf{c} \in \mathbb{F}_2^n \setminus \{0\}$, g is coprime to $\pi_{\mathbf{c}}$.
3. Use the previous results to prove that $\Gamma(\mathbf{x}, g)$ is linear.
Remark : Since the code is binary, proving that it is linear consists only in proving that the sum of two codewords is a codeword.
4. Prove that the minimum distance of $\Gamma(\mathbf{x}, g)$ is larger than or equal to $\deg(g) + 1$.
5. Prove that if $f \in \mathbb{F}_{2^m}[X]$, then f' is a square, i.e. there exists $a \in \mathbb{F}_{2^m}[X]$ such that $f' = a^2$.
6. Prove that if g is squarefree, then $\Gamma(\mathbf{x}, g) = \Gamma(\mathbf{x}, g^2)$. Deduce in that particular case a better lower bound for the minimum distance of $\Gamma(\mathbf{x}, g)$.

If you did everything well up to here, you'll have 20/20. The remaining questions are bonus questions.

7. Let $\mathbb{F}_{2^m}(X)$ be the field of rational fractions with coefficients in $\mathbb{F}_{2^m}$. For any $f \in \mathbb{F}_{2^m}(X)$, we denote by f' its derivative. Let ψ be the map :
$$\psi : \begin{cases} \mathbb{F}_{2^m}(X)^\times & \rightarrow & \mathbb{F}_{2^m}(X) \\ f & \mapsto & \frac{f'}{f}. \end{cases}$$
Prove that for all $f, g \in \mathbb{F}_{2^m}(X)^\times$, we have $\psi(fg) = \psi(f) + \psi(g)$.
8. Let
$$h : \begin{cases} \mathbb{F}_2^n & \rightarrow & \mathbb{F}_{2^m}(X) \\ \mathbf{a} & \mapsto & \frac{\pi'_{\mathbf{a}}}{\pi_{\mathbf{a}}}. \end{cases}$$
Prove that h is $\mathbb{F}_2$–linear and injective.
Hint : One can start by proving that for all $f \in \mathbb{F}_{2^m}[X]$, $f' = 0$ if and only if f is a square.
9. Let $E, E_g \subseteq \mathbb{F}_{2^m}(X)$ be the $\mathbb{F}_{2^m}$–vector spaces
$$E = \left\{ \frac{f(X)}{\prod_{i=1}^n (X - x_i)} \;\middle|\; f \in \mathbb{F}_{2^m}[X]_{<n} \right\}, \quad E_g = \left\{ \frac{f(X)g(X)}{\prod_{i=1}^n (X - x_i)} \;\middle|\; f \in \mathbb{F}_{2^m}[X]_{<n-\deg(g)} \right\}.$$
What are the $\mathbb{F}_{2^m}$–dimensions of E and E_g ? and their $\mathbb{F}_2$–dimensions ?
10. Prove that h has its image contained in E.
11. Prove that $\Gamma(\mathbf{x}, g)$ has $\mathbb{F}_2$–dimension larger than or equal to $n - m \deg g$.
Hint : One can start by proving that $\Gamma(\mathbf{x}, g)$ is isomorphic (as an $\mathbb{F}_2$–vector space) to $E_g \cap Im(h)$.

---

1. We allow ourselves the following abuse of language : we denote by c_i the integer 0 if $c_i = 0$ in $\mathbb{F}_2$ and 1 if $c_i = 1$