MPRI **Year 2021–22**

Module 2.13.2 : Error correcting codes and applications to cryptography

Mid-term exam, November 25, 2021

You have 1h30.
You can write your answers either in french or in english.

Exercise 1. Let $C \subseteq \mathbb{F}_2^n$ be the linear code with generator matrix :

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

1. Give the dimension of C. Deduce the number of codewords in C.
2. Prove that C has only codewords of even weight.
3. Prove that $C^\perp$ has only codewords of even weight (*Hint : do not try to compute* $C^\perp$).
4. Let $P_C(x,y)$ be the weight enumerator of C, that is to say :

$$P_C(x,y) := \sum_{j=0}^{6} A_j(C) x^j y^{6-j} \qquad \text{where} \qquad \forall j \in \{0,\dots,6\},\ A_j(C) := |\{\mathbf{c} \in C \mid w_H(\mathbf{c}) = j\}|.$$

   Prove that $P_C(x,y) = P_C(y,x)$ and $P_{C^\perp}(x,y) = P_{C^\perp}(y,x)$.
5. Prove that
$$P_C(x,y) = P_{C^\perp}(x,y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6.$$
6. Deduce that the polynomial $P(x,y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6$ satisfies
$$P(x,y) = P(y-x, y+x).$$
7. However, do we have $C = C^\perp$? Justify your answer.

Exercise 2.

1. Prove that the only linear binary cyclic codes of length 11 are the codes $\{0\}, \mathbb{F}_2^{11}$, the repetition code and the parity code.

Caution. In the sequel, we consider linear codes over $\mathbb{F}_4$ and no longer over $\mathbb{F}_2$ as in the previous question.

2. Compute the minimal nonempty cyclotomic classes for $\mathbb{F}_4^{11}$. That is to say the smallest nonempty parts of $\mathbb{Z}/11\mathbb{Z}$ stable by multiplication by 4.
3. Deduce the number of cyclic codes of length 11 over $\mathbb{F}_4$ (including the codes $\{0\}$ and $\mathbb{F}_4^{11}$).
4. Prove that there exist two cyclic codes in $\mathbb{F}_4^{11}$ of dimension 6 and minimum distance $\geqslant 4$.

Turn the page please.

Exercise 3. In this exercise, any code is linear. In $\mathbb{F}_2^n$, the Hamming ball of centre $\mathbf{c}$ and radius ℓ, *i.e.* the set of words at distance less than or equal to ℓ from $\mathbf{c}$ is denoted $\mathbb{B}_H(\mathbf{c}, \ell)$. The number of words in such a ball is denoted by $V(n, \ell)$. We recall the existence of a function H_2 satisfying

$$\forall \rho \in [0, 1/2],\ \forall \mathbf{c} \in \mathbb{F}_2^n, \quad 2^{nH_2(\rho) - o(n)} \leqslant V(n, \rho n) \leqslant 2^{nH_2(\rho)}.$$

A code $C \subseteq \mathbb{F}_2^n$ is said to be (ρ, L)*–list decodable* if for any $\mathbf{y} \in \mathbb{F}_2^n$, we have

$$|\mathbb{B}_H(\mathbf{y}, \rho n) \cap C| \leqslant L.$$

1. Explain the rationale behind the terminology "list decodable".
2. Let C be a code of dimension k and $0 < \rho < 1/2$. Let $\mathbf{y}$ be a uniformly random word of $\mathbb{F}_2^n$ and consider the random variable $Z_{C,\rho} = |\mathbb{B}_H(\mathbf{y}, \rho n) \cap C|$. Prove that its expectation (mean) satisfies
$$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) = 2^{k-n} \cdot V(n, \rho n).$$
3. Let $\varepsilon > 0$. Prove that, for large enough n, any code $C \subseteq \mathbb{F}_2^n$ of dimension $n(1 - H_2(\rho) + \varepsilon)$ satisfies
$$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) \geqslant 2^{\frac{\varepsilon n}{2}}.$$
4. A code is said ρ–list decodable if it is (ρ, L)–list decodable where L is polynomial in n. Deduce from the previous results that, for large enough n, no code of dimension $n(1 - H_2(\rho) + \varepsilon)$ is ρ–list decodable.
5. To which result in your course, the previous result can be compared ? How do these results differ from each other ?

Exercise 4. Any code in the exercise is linear. Recall that a code $C \subseteq \mathbb{F}_q^n$ is said to be MDS if C has parameters $[n, k, n - k + 1]$. For any $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, we call *support of* $\mathbf{y}$ the set

$$\mathrm{Supp}(\mathbf{y}) := \{i \in \{1, \ldots, n\} \mid y_i \neq 0\}.$$

1. Let $C \subseteq \mathbb{F}_q^n$, be an MDS code of dimension k. Prove that for any $J \subseteq \{1, \ldots, n\}$ such that $|J| = n - k + 1$, there exists $\mathbf{c}_J \subseteq C$ such that
$$\mathrm{Supp}(\mathbf{c}_J) = J.$$
2. Prove that $\mathbf{c}_J$ is unique up to multiplication by a scalar.
3. Let $C' \subseteq \mathbb{F}_q^n$ be a code of dimension k and $\mathbf{c} \in C' \setminus \{0\}$ with weight $r \leqslant n - k$. Let $J \supseteq \mathrm{Supp}(\mathbf{c})$ be such that $|J| = n - k$. Prove that there **cannot exist** for all $i \in \{1, \ldots, n\} \setminus J$ a word $\mathbf{c}_{J \cup \{i\}} \in C'$ with support $J \cup \{i\}$.
4. Deduce that : *A code $C \subseteq \mathbb{F}_q^n$ of dimension k is MDS if and only if, for all $J \subseteq \{1, \ldots, n\}$ such that $|J| = n - k + 1$, there exists a codeword $\mathbf{c}_J \in C$ with support J.*
5. Given two codes $C, D \subseteq \mathbb{F}_q^n$, denote
$$C * D := \mathrm{Span}_{\mathbb{F}_q} \{(c_1 d_1, \ldots, c_n d_n) \mid (c_1, \ldots, c_n) \in C,\ (d_1, \ldots, d_n) \in D\}.$$
Prove that if C and D are MDS and $\dim C * D = \dim C + \dim D - 1$, then $C * D$ is MDS.