Exercice 3 –

1) Soit $P(X) = X^6 + X^5 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Effectuer les divisions euclidiennes dans $\mathbb{F}_2[X]$ de $P(X)$ par $X^2 + X + 1$, $X^3 + X + 1$ et $X^3 + X^2 + 1$.

2) En déduire que $P(X)$ est irréductible dans $\mathbb{F}_2[X]$. On identifie $\mathbb{F}_{64}$ à $\mathbb{F}_2[X]/(P(X))$.

3) Quels sont les sous-corps de $\mathbb{F}_{64}$?

4) Soit α la classe de X dans $\mathbb{F}_{64}$. Montrer que $\alpha^5 + \alpha^3 + \alpha^2$ appartient à un sous-corps strict K de $\mathbb{F}_{64}$. Exprimer les éléments de K comme polynômes en α de degrés inférieurs strictement à 6.

5) Montrer que $\alpha^3 + \alpha^2$ appartient à un sous-corps strict L de $\mathbb{F}_{64}$. Exprimer les éléments de L comme polynômes en α de degrés inférieurs strictement à 6.

6) Soit $(s_i)_{i\geqslant 0} \in (\mathbb{F}_2)^{\mathbb{N}}$ définie par $s_0 = s_1 = s_2 = s_3 = s_4 = 0$, $s_5 = 1$ et par la relation

$$s_{i+6} = s_{i+5} + s_{i+2} + s_{i+1} + s_i \quad \text{(pour tout } i \geqslant 0\text{)}.$$

Expliquer pourquoi $(s_i)_{i\geqslant 0}$ est périodique de période $r \leqslant 63$.

7) Calculer les premiers termes de $(s_i)_{i\geqslant 0}$ et en déduire r.

8) Le polynôme $P(X)$ est-il primitif ?

9) Rappeler pourquoi $P(X)$ divise $X^{63} - 1$ dans $\mathbb{F}_2[X]$.

10) Soit $\mathcal{C}$ le code binaire cyclique de longueur 63 et de polynôme générateur $P(X)$. Quelle est la dimension de $\mathcal{C}$? Quel est son cardinal ?

11) Quels sont les paramètres de $\mathcal{C}$?

12) Calculer α^8 et α^{11} comme polynômes en α de degrés inférieurs strictement à 6. En déduire un élément non nul de $\mathcal{C}$ de poids minimum.

Exercice 4 –

1) Montrer que dans $\mathbb{F}_8$, tout élément distinct de 0 et 1 est un élément primitif.

2) Expliquer pourquoi dans $\mathbb{F}_8[X]$ le polynôme $X^3 + X + 1$ est scindé à racines simples. Soit α une de ses racines dans $\mathbb{F}_8$.

3) On considère dans $\mathcal{M}_{3,7}(\mathbb{F}_8)$ la matrice

$$M = \begin{pmatrix} \alpha^2+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2 & 1 & 0 & 0 \\ 0 & \alpha^2+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2 & 1 & 0 \\ 0 & 0 & \alpha^2+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2 & 1 \end{pmatrix}.$$

Montrer que les lignes de cette matrice sont linéairement indépendantes sur $\mathbb{F}_8$.

4) Soit $\mathcal{C}$ le code linéaire de matrice génératrice M. Quel est le cardinal de $\mathcal{C}$?

5) Montrer que $(1, 0, 0, \alpha^2+1, \alpha^2+\alpha+1, \alpha^2+\alpha+1, \alpha^2) \in \mathcal{C}$ et en déduire que $\mathcal{C}$ est cyclique.

6) Quel est le polynôme générateur $g(X)$ de $\mathcal{C}$?

7) Vérifier que $g(X) = (X-1)(X-\alpha)(X-\alpha^2)(X-\alpha^3)$ et en déduire que l'on a bien $g(X) \mid X^7 - 1$ dans $\mathbb{F}_8[X]$.

8) Soit $c = (c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ un mot non nul de $\mathcal{C}$. Montrer que si $P(X) = \sum_{i=0}^{6} c_i X^i \in \mathbb{F}_8[X]$, on a $P(1) = P(\alpha) = P(\alpha^2) = P(\alpha^3) = 0$.

9) En déduire que $\omega(c) > 4$.

10) Quelle est la distance minimale de $\mathcal{C}$? Quel est l'ordre de la condition de décodage de $\mathcal{C}$ (le nombre d'erreurs que l'on peut corriger) ?

11) Soit $\mathcal{C}^\perp$ le dual de $\mathcal{C}$. Quel est le cardinal de $\mathcal{C}^\perp$?

12) On sait par le cours que $\mathcal{C}^\perp$ est un code cyclique. Quel est son polynôme générateur ?

13) Quelle est la distance minimale de $\mathcal{C}^\perp$?