MPRI **Année 2021–22**

Module 2.13.2 : Codes correcteurs d'erreurs et applications à la cryptographie

Partiel du 25 novembre 2021

Vous avez 1h30.
Vous pouvez répondre en français ou en anglais.

Exercice 1. Soit $C \subseteq \mathbb{F}_2^n$ le code linéaire binaire de matrice génératrice

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

1. Donner la dimension de C. En déduire le nombre de mots de C.
2. Montrer que C n'a que des mots de poids pair.
3. Montrer que $C^\perp$ n'a que des mots de poids pair (*Hint : ne cherchez pas à calculer* $C^\perp$).
4. Soit $P_C(x, y)$ l'énumérateur des poids de C, autrement dit

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

   Montrer que $P_C(x, y) = P_C(y, x)$ et $P_{C^\perp}(x, y) = P_{C^\perp}(y, x)$.
5. Montrer que
$$P_C(x,y) = P_{C^\perp}(x,y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6.$$
6. En déduire que le polynôme $P(x, y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6$ vérifie
$$P(x,y) = \frac{1}{8} P(y - x, y + x).$$
7. A-t-on pour autant $C = C^\perp$? Justifier votre réponse.

Exercice 2.

1. Montrer que les seuls codes linéaires cycliques binaires de longueur 11 sont les codes $\{0\}, \mathbb{F}_2^{11}$, le code de répétition et le code de parité.

Attention. Dans ce qui suit, on considère des codes linéaires sur $\mathbb{F}_4$ et non plus sur $\mathbb{F}_2$ comme dans la question précédente.

2. Calculer les classes cyclotomiques non vides minimales pour $\mathbb{F}_4^{11}$. Autrement dit les plus petites parties non vides de $\mathbb{Z}/11\mathbb{Z}$ stables par multiplication par 4.
3. En déduire le nombre de codes cycliques de longueur 11 sur $\mathbb{F}_4$ (y compris les codes $\{0\}$ et $\mathbb{F}_4^{11}$).
4. Montrer qu'il existe deux codes cycliques dans $\mathbb{F}_4^{11}$ de dimension 6 et de distance minimale $\geqslant 4$.

Tournez la page s.v.p.

Exercice 3. Dans cet exercice, tous les codes sont linéaires. Dans $\mathbb{F}_2^n$, la boule de Hamming de centre $\mathbf{c}$ et de rayon ℓ, *i.e.* l'ensemble des mots dont la distance à $\mathbf{c}$ inférieure ou égale à ℓ est notée $\mathbb{B}_H(\mathbf{c}, \ell)$. Le nombre de mots dans une telle boule est noté $V(n, \ell)$. On rappelle l'existence d'une fonction H_2 telle que

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

On dit qu'un code $C \subseteq \mathbb{F}_2^n$ est (ρ, L)–*décodable en liste* si pour tout $\mathbf{y} \in \mathbb{F}_2^n$, on a

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

1. Justifiez en quelques mots la terminologie "décodable en liste".
2. On se donne un code C de dimension k et un réel $0 < \rho < 1/2$. Soit $\mathbf{y}$ un mot aléatoire uniforme de $\mathbb{F}_2^n$ et on considère la variable aléatoire $Z_{C,\rho} = |\mathbb{B}_H(\mathbf{y}, \rho n) \cap C|$. Montrer que son espérance vérifie
$$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) = 2^{k-n} \cdot V(n, \rho n).$$
3. Soit $\varepsilon > 0$. Montrer que pour n suffisamment grand, tout code $C \subseteq \mathbb{F}_2^n$ de dimension $n(1 - H_2(\rho) + \varepsilon)$ vérifie
$$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) \geqslant 2^{\frac{\varepsilon n}{2}}.$$
4. On dit qu'un code est ρ–décodable en liste s'il est (ρ, L)–décodable en liste avec L qui est polynomial en n. Déduire de ce qui précède que pour n suffisamment grand, aucun code de dimension $n(1-H_2(\rho)+\varepsilon)$ n'est ρ–décodable en liste.
5. À quel résultat du cours ce résultat peut-il être comparé ? En quoi les résultats diffèrent-ils ?

Exercice 4. Tous les codes dans cet exercice sont linéaires. On rappelle qu'un code $C \subseteq \mathbb{F}_q^n$ est dit MDS si C a pour paramètres $[n, k, n-k+1]$. Pour tout $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, on appellera *support de* $\mathbf{y}$ l'ensemble

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

1. Soit $C \subseteq \mathbb{F}_q^n$, un code MDS de dimension k. Montrer que pour tout $J \subseteq \{1, \ldots, n\}$ tel que $|J| = n-k+1$, il existe un mot $\mathbf{c}_J \subseteq C$ tel que
$$\mathrm{Supp}(\mathbf{c}_J) = J.$$
2. Montrer que $\mathbf{c}_J$ est unique à multiplication près par un scalaire.
3. Soit $C' \subseteq \mathbb{F}_q^n$ un code de dimension k et $\mathbf{c} \in C' \setminus \{0\}$ de poids $r \leqslant n-k$. Soit $J \supseteq \mathrm{Supp}(\mathbf{c})$ tel que $|J| = n-k$. Montrer qu'il ne **peut pas exister** pour tout $i \in \{1, \ldots, n\} \setminus J$ un mot $\mathbf{c}_{J\cup\{i\}} \in C'$ de support $J \cup \{i\}$.
4. En déduire le résultat suivant : *Un code $C \subseteq \mathbb{F}_q^n$ de dimension k est MDS si et seulement si pour tout $J \subseteq \{1, \ldots, n\}$ tel que $|J| = n-k+1$ alors il existe un mot $\mathbf{c}_J \in C$ de support J.*
5. Étant donnés deux codes $C, D \subseteq \mathbb{F}_q^n$, on note
$$C * D := \mathrm{Span}_{\mathbb{F}_q}\left\{(c_1 d_1, \ldots, c_n d_n) \mid (c_1, \ldots, c_n) \in C,\ (d_1, \ldots, d_n) \in D\right\}.$$
Montrer que si C et D sont MDS et $\dim C * D = \dim C + \dim D - 1$, alors $C * D$ est MDS.