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.

   Réponse : Le code est de dimension 3 (si on remplace la ligne 3 par ligne 1+ ligne 3 on a une matrice échelonnée). Il y a donc $2^3 = 8$ mots.

2. Montrer que C n'a que des mots de poids pair.

   Réponse : Cela revient à prouver que le mot (1 1 1 1 1 1) est dans le noyau de G, ce qui est le cas.

3. Montrer que $C^\perp$ n'a que des mots de poids pair (*Hint : ne cherchez pas à calculer* $C^\perp$).

   Réponse : On vérifie que (1 1 1 1 1 1) est dans C, c'est en effet la troisième ligne de G.

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 $P_{C^\perp}(x, y) = P_{C^\perp}(y, x)$.

   Réponse : Du fait que (1 1 1 1 1 1) est dans C et dans $C^\perp$, à tout mot $x \in C$ (resp. $C^\perp$) de poids r correspond le mot $(1\ 1\ 1\ 1\ 1\ 1) + x$ de poids $6 - r$. Aussi pour tout $r \in \{0,\dots,6\}$ il y a une correspondance bijective entre les mots de C (resp $C^\perp$) de poids r et les mots de C (resp. $C^\perp$) de poids $6 - r$. On en déduit cette propriété de symétrie des énumérateurs de poids P_C et $P_{C^\perp}$.

5. Montrer que

$$P_C(x,y) = P_{C^\perp}(x,y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6.$$

   Réponse : Le code C contient 0 et (1 1 1 1 1 1) qui sont respectivement les seuls mots de poids 0 et 6. Il n'a que des mots de poids pair, aussi les seuls autres poids possibles sont 2 et 4. D'après la question précédente, il y a autant de mots de poids 2 que de mots de poids 4. Comme il y a 8 mots en tout, on en déduit qu'il y a 3 mots de poids 2 et 3 mots de poids 4 dans C. Le code dual $C^\perp$ vérifie la même propriété, exactement pour les mêmes raisons.

6. En déduire que le polynôme $P(x,y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6$ vérifie

$$P(x,y) = \frac{1}{8}P(y-x, y+x).$$

Réponse : C'est une conséquence immédiate de la formule de McWilliams.

7. A-t-on pour autant $C = C^\perp$? Justifier votre réponse.

Réponse : Non, le mot (1 1 0 0 0 0) est dans C mais pas dans $C^\perp$.

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.

Réponse : Les classes cyclotomiques minimales sont $\{0\}$ et $\{1,2,4,8,5,10,9,7,3,6\}$ Aussi en longueur 11, les seuls codes linéaires cycliques sont :
- $\mathbb{F}_2^{11}$ correspondant à $\emptyset$;
- 0 correspondant à $\mathbb{Z}/11\mathbb{Z}$ tout entier ;
- Le code de répétition, correspondant à $\{1,2,4,8,5,10,9,7,3,6\}$;
- Le code de parité correspondant à $\{0\}$.

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.

Réponse : $\{0\}, \{1,4,5,9,3\}, \{2,8,10,7,6\}$.

3. En déduire le nombre de codes cycliques de longueur 11 sur $\mathbb{F}_4$ (y compris les codes $\{0\}$ et $\mathbb{F}_4^{11}$).

Réponse : Il y en a $2^3 = 8$.

4. Montrer qu'il existe deux codes cycliques dans $\mathbb{F}_4^{11}$ de dimension 6 et de distance minimale $\geqslant 4$.

Réponse : Le code associé à la classe cyclotomique $\{1,4,5,9,3\}$ est de dimension $11-5=6$. De plus, d'après la borne BCH, il est de distance minimale $\geqslant 4$ car la classe cyclotomique contient 3 éléments consécutifs : $3,4,5$.

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".

   Réponse : Pour tout mot reçu, la liste des mots de code à distance inférieure à ρn est de cardinal inférieur ou égalà à L. Autrement dit, pour tout mot reçu le problème de décodage en liste admet au plus L solutions.

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

   $$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) = 2^{k-n} \cdot V(n, \rho n).$$

   Réponse : On peut reformuler $Z_{C,\rho}$ en

   $$Z_{C,\rho} = \sum_{\mathbf{c} \in C} \mathbf{1}_{\mathbf{c} \in \mathbb{B}_H(\mathbf{y}, \rho n).}$$

   Par conséquent,

   $$\mathbb{E}(Z_{C,\rho}) = \sum_{\mathbf{c} \in C} \mathbb{P}(c \in \mathbb{B}_H(\mathbf{y}, \rho n)) = \sum_{\mathbf{c} \in C} \frac{V(n, \rho n)}{2^n} = 2^{k-n} V(n, \rho n).$$

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

   $$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) \geqslant 2^{\frac{\varepsilon n}{2}}.$$

   Réponse : Pour $n \gg 0$, on a $V(n, \rho n) \geqslant 2^{nH_2(\rho) - \frac{\varepsilon n}{2}}$. Donc, d'après la question précédente :

   $$\mathbb{E}_{\mathbf{y}}(Z_{C,\rho}) = 2^{n(1-H_2(\rho)+\epsilon)-n} \cdot V(n, \rho n) \geqslant 2^{n(1-H_2(\rho)+\epsilon)-n} \cdot 2^{nH_2(\rho) - \frac{\varepsilon n}{2}} = 2^{\frac{\varepsilon n}{2}}$$

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.

   Réponse : D'après ce qui précède, à au moins un mot $\mathbf{y}$ correspond une liste $C \cap \mathbb{B}_H(\mathbf{y}, \rho n)$ de cardinal supérieur à $2^{\frac{\varepsilon n}{2}}$, autrement dit une liste de taille exponentielle.

5. À quel résultat du cours ce résultat peut-il être comparé ? En quoi les résultats diffèrent-ils ?

   Réponse : Ce résultat peut être comparé à la seconde partie du théorème de Shannon affirmant l'impossibilité de décoder des codes de rendement strictement supérieur à $1 - H_2(\rho)$. Mais le théorème de Shannon affirme simplement qu'un décodeur échouera avec une probabilité élevée. Cet énoncé affirme qu'au moins une instance du problème du décodage en listes aura un ensemble de solution de taille exponentielle.

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
$$\mathrm{Supp}(\mathbf{c}_J) = J.$$

   Réponse : Si l'on se donne une matrice génératrice de C. Par élimination Gaussienne, on peut construire un mot de code non nul dont les $k-1$ entrées dans $\{1, \ldots, n\} \setminus J$ sont nulles. Un tel mot est de poids $\leqslant n-k+1$ et de support inclus dans J. Par définition d'un code MDS, ce mot est en fait de poids exactement $n-k+1$ et donc de support J.

2. Montrer que $\mathbf{c}_J$ est unique à multiplication près par un scalaire.

   Réponse : Supposons qu'il y ait deux mots $\mathbf{c}, \mathbf{c}'$ non colinéaires de support J. Soit $i \in J$ et $\lambda \in \mathbb{F}_q^\times$ tel que $\mathbf{c}_i = \lambda \mathbf{c}'_i$. Alors le mot $\mathbf{c}_i - \lambda \mathbf{c}'_i$ est dans C et a support inclus dans $J \setminus \{i\}$, ce qui contredit la propriété MDS.

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 $J \cup \{i\}$.

   Réponse : Supposons que de tels mots existent. Alors les mots, $\mathbf{c}_{J\cup\{i\}}$ pour $i \in \{1, \ldots, n\} \setminus J$ ainsi que le mot $\mathbf{c}$ forment une famille libre (quitte à réorganiser les indices, ils forment une famille échelonnée). De fait, le code C est de dimension k et contiendrait $k+1$ mots linéairement indépendants. Il y a donc contradiction.

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.*

   Réponse : Le "seulement si" a été prouvé dans la question 1 . Pour la réciproque, on remarque que si un code vérifie la propriété "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" alors, d'après la question 3, il ne peut pas avoir de mot de poids $\leqslant n-k$. Il est donc MDS.

5. Étant donnés deux codes $C, D \subseteq \mathbb{F}_q^n$, on note
$$C * D := \mathrm{Span}_{\mathbb{F}_q} \{(c_1 d_1, \ldots, c_n d_n) \mid (c_1, \ldots, c_n) \in C,\ (d_1, \ldots, d_n) \in D\}.$$
   Montrer que si C et D sont MDS et $\dim C * D = \dim C + \dim D - 1$, alors $C * D$ est MDS.

   Réponse : Soit $J \subseteq \{1, \ldots, n\}$ de cardinal $n - \dim C - \dim D + 2$ et notons $\bar{J}$ son complémentaire, qui est de cardinal $\dim C + \dim D - 2$. On va montrer l'existence dans $C * D$ d'un mot de code de support J. Pour cela on subdivise $\bar{J}$ en deux sous-ensembles dusjoints $\bar{U}, \bar{V}$ de cardinaux respectifs $\dim C - 1$ et $\dim D - 1$. Leurs complémentaires respectifs sont notés U, V. D'après la question 1, il existe $\mathbf{c} \in C$ de support U et $\mathbf{d} \in D$ de support V. Le mot $\mathbf{c} * \mathbf{d} \in C * D$ a précisément pour support J.
   Le raisonnement qui précède est vrai pour tout J de cardinal $n - \dim C - \dim D + 2$. On en déduit, d'après la question 4, que le code $C * D$ est MDS.