Université de Rennes 1 — Année universitaire 2020-2021
Licence de mathématiques
Module Anneaux et arithmétique

Feuille de TD n°3 bis

Exercice 3 bis.1

Soit $\mathbf{K}$ un corps, n et k des entiers strictement positifs avec $k \leqslant n$, E le $\mathbf{K}$-espace vectoriel $\mathbf{K}^n$ et F un sous-espace vectoriel de E de dimension k. Soit $\pi \colon \mathbf{K}^n \to \mathbf{K}^{k-1}$ la projection sur les $k-1$ premières coordonnées. Montrer que $\pi_{|F}$ n'est pas injective. En déduire la borne de Singleton.

Exercice 3 bis.2

Soit $\mathscr{C}$ un code linéaire et H une matrice de contrôle de $\mathscr{C}$. Soit d l'unique entier strictement positif vérifiant la propriété suivante :

1. il existe d colonnes de H qui forment un système lié ;
2. tout sous-ensemble de colonnes de H de cardinal $d-1$ est un système libre

Montrer que d est la distance minimale de $\mathscr{C}$.

Exercice 3 bis.3

1. Vérifier que la distance de Hamming est bien une distance.
2. Soit A un ensemble fini de cardinal q et $n \geqslant 1$ un entier. Soit $t \geqslant 1$ un entier. Montrer que le nombre d'éléments d'une boule de rayon t de A^n (pour la distance de Hamming) est
$$N(q,n,t) = \sum_{k=0}^{t} \binom{n}{k} (q-1)^k.$$
3. Soit $1 \leqslant k \leqslant n$ un entier et $A^k \cong \mathscr{C} \subset A^n$ un code. Soit $t \geqslant 1$ un entier. Montrer que $\mathscr{C}$ est t-correcteur si et seulement si les boules de rayon t centrée en les éléments de $\mathscr{C}$ sont deux à deux disjointes. Montrer que si $\mathscr{C}$ est t-correcteur alors $N(q,n,t) \leqslant q^{n-k}$ (*borne de Hamming*).
4. Le code $\mathscr{C}$ est dit *parfait* s'il existe un entier $t \geqslant 1$ tel que les boules de rayon t centrée en les éléments de $\mathscr{C}$ forment une partition de A^n. Montrer qu'un tel entier t est alors unique et est le plus grand entier t' tel que $\mathscr{C}$ est t'-correcteur. Montrer que le code $\mathscr{C}$ est parfait si et seulement s'il existe un entier $t \geqslant 1$ tel que $\mathscr{C}$ est t-correcteur et on a l'égalité
$$N(q,n,t) = q^{n-k}.$$
5. *Codes de Hamming binaires :* soit r un entier et $n = 2^r - 1$. Soit M une matrice à r colonnes et $2^r - 1$ lignes dont l'ensemble des lignes coïncide avec $\mathbf{F}_2^r \setminus \{0\}$. Soit
$$\mathscr{C} := \{x \in \mathbf{F}_2^n, \quad x \cdot M = 0\}.$$
Déterminer les paramètres de $\mathscr{C}$. Montrer que $\mathscr{C}$ est 1-correcteur parfait.
6. Lister les éléments du code de Hamming binaire de paramètres $[7,4,3]$ (qui est historiquement l'un des premiers codes non triviaux introduits). Soit $y \in \mathbf{F}_2^7$ un mot transmis comprenant une erreur. Montrer que le syndrome de y est la ligne de M dont l'indice correspond à la position de l'erreur.

7. *Codes de Hamming q-aires :* soit $\mathbf{K}$ un corps de cardinal q, r un entier. Soit $\mathcal{L} \subset \mathbf{K}^r$ une partie maximale de $\mathbf{K}^r$ telle que deux éléments de $\mathcal{L}$ ne sont pas colinéaires. Soit M la matrice à r colonnes dont l'ensemble des lignes coïncide avec $\mathcal{L}$. Explicitez le cas $q = 3$, $r = 2$. Soit
$$\mathscr{C} := \{x \in \mathbf{K}^n, \quad x \cdot M = 0\}.$$
Donner les paramètres de $\mathscr{C}$. Montrer que $\mathscr{C}$ est 1-correcteur parfait.

Exercice 3 bis.4

1. Soit $\mathbf{K}$ un corps fini de cardinal q et α un générateur de $\mathbf{K}^\times$. Soit $2 \leqslant d \leqslant q-1$ un entier et $\mathcal{I}$ l'idéal de $\mathbf{K}[X]$ engendré par le polynôme
$$g(X) := \prod_{i=1}^{d-1}(X - \alpha^i).$$
Montrer que $\mathcal{I}$ définit un code cyclique sur $\mathbf{K}$ de paramètres $[q-1, q-d, d]$ (donc de type MDS). Expliciter une base du code pour les paramètres suivants : $[3, 2, 2]$ et $[8, 7, 2]$.
2. Soit $\mathbf{K}$ un corps, $\alpha \in \mathbf{K}^\times$ et n l'ordre multiplicatif de α. Soit $m(X)$ et $u(X)$ des éléments de $\mathbf{K}[X]$ de degré au plus $n-1$. Montrer que les deux propriétés suivantes sont équivalentes :
   (a) on a $n \cdot m(X) = \sum_{i=0}^{n-1} u(\alpha^i) X^i$;
   (b) on a $u(X) = \sum_{i=0}^{n-1} m(\alpha^{-i}) X^i$.
3. Soit $\mathbf{K}$ un corps de cardinal q et $2 \leqslant k \leqslant q-1$ un entier. Soit $\mathbf{K}[X]_{\leqslant k-1}$ l'ensemble des polynômes à coefficients dans $\mathbf{K}$ de degré au plus $k-1$. Choisissons une énumération $\{x_i\}_{0 \leqslant i \leqslant q-2}$ des éléments de $\mathbf{K}^\times$. On considère l'application qui à $u \in \mathbf{K}[X]_{\leqslant k-1}$ associe $(u(x_i))_{0 \leqslant i \leqslant q-2}$. Montrer que son image est un code de paramètres $[q-1, k, q-k]$ (donc de type MDS). Comment ce code est-il relié à celui de la première question ?

Exercice 3 bis.5

Soit $\mathbf{K}$ un corps fini, n un entier positif tel que que n et $q := [\mathbf{K}]$ sont premiers entre eux, r l'ordre de $[q]_n$ dans $(\mathbf{Z}/n\mathbf{Z})^\times$. Soit $\mathbf{L}$ un corps à q^r éléments contenant $\mathbf{K}$ et $\alpha \in \mathbf{L}^\times$ un élément d'ordre n. Pour toute partie Σ de $\mathbf{Z}/n\mathbf{Z}$, on note
$$g_\Sigma := \prod_{i \in \Sigma}(X - \alpha^i) \in \mathbf{L}[X]$$

1. On veut montrer que g_Σ est à coefficient dans $\mathbf{K}$ si et seulement si Σ est stable par multiplication par q.
   (a) Soit A, B des anneaux et $\varphi\colon A \to B$ un morphisme. Soit I un ensemble fini, $(a_i)_{i \in I}$ des éléments de A. Écrivons
   $$\prod_{i \in I}(X - a_i) = \sum_{k \geqslant 0} b_k X^k, \quad (b_k) \in A^{(\mathbf{N})}$$
   Vérifier (sans calculs...) qu'on a
   $$\prod_{i \in I}(X - \varphi(a_i)) = \sum_{k \geqslant 0} \varphi(b_k) X^k, \quad (b_k) \in A^{(\mathbf{N})}$$

(b) Conclure en utilisant le morphisme $x \mapsto x^q$.

2. On suppose en outre qu'il existe $\nu \in \mathbf{Z}/n\mathbf{Z}$ et $2 \leqslant d \leqslant n$ un entier positif tels que

$$\{\nu + [i]_n\}_{0 \leqslant i \leqslant d-2} \subset \Sigma$$

On veut montrer que le code cyclique $\mathscr{C}$ de $\mathbf{K}[X]/\langle X^n - 1\rangle$ engendré par g est de distance minimale au moins d. Soit $P \in \mathbf{K}[X]$ un multiple de g de degré au plus $n-1$ et ayant *au plus* $d-1$ coefficients non nul. Traduire la condition que P est un multiple de g en un système linéaire d'inconnues les coefficients de P dont la matrice est une matrice de Vandermonde. Conclure que P est nul, puis conclure quant à la distance minimale de $\mathscr{C}$.

3. On suppose que $\mathbf{K} = \mathbf{F}_2$ et $n = 2^r - 1$. Soit

$$g := \prod_{i=0}^{r-1} (X - \alpha^{2^i}).$$

Vérifier que $g \in \mathbf{F}_2[X]$. Déterminer les paramètres du code cyclique engendré par g. Comparer avec les codes de Hamming binaires de l'exercice 3 bis.3.

4. On suppose que $n = \frac{q^r-1}{q-1}$ et que n et $q-1$ sont premiers entre eux. Soit

$$g =: \prod_{i=0}^{r-1} (X - \alpha^{q^i}).$$

Vérifier que $g \in \mathbf{K}[X]$. Déterminer les paramètres du code cyclique engendré par g ; on pourra comparer ce code avec le code de Hamming q-aire analogue de l'exercice 3 bis.3.