Partiel du 17 novembre 2014

Durée 1h30, Documents autorisés. Bon courage !

Exercice 1 (Calcul d'une distribution de poids)**.** Un code $C \subseteq \mathbb{F}_q^n$ est dit *autodual* si $C = C^\perp$.

1. Montrer qu'un code autodual est nécessairement de longueur n paire et de dimension $\frac{n}{2}$.
2. Montrer qu'un code **binaire** autodual n'a que des mots de poids pair.
3. Soit $C \subseteq \mathbb{F}_2^6$ un code autodual **binaire** de longueur 6. Montrer que son polynôme (homogène) énumérateur des poids est de la forme
$$P_C^\sharp(x,y) = y^6 + a_2x^2y^4 + a_4x^4y^2 + a_6x^6. \qquad (\star)$$
où $a_6 \in \{0,1\}$ et $1 + a_2 + a_4 + a_6 = 8$.
4. À l'aide de la formule de McWilliams, montrer qu'un tel code contient nécessairement le mot (1 1 1 1 1 1 1). *Conseil : évitez de développer le polynôme $P_C^\sharp(y-x, y+x)$ cela vous évitera des calculs fastidieux. Contentez vous de calculer son coefficient en x^6.*
5. Déduire de la question précédente que $a_2 = a_4$.
6. Donner la distribution des poids d'un code autodual binaire de longueur 6.

Exercice 2. On cherche à étudier les codes cycliques contenus dans $\mathbb{F}_3^{13}$. On rappelle que les classes cyclotomiques q–aires modulo 13 sont les parties de $\mathbb{Z}/13\mathbb{Z}$ stables par multiplication par q.

1. Donner la liste des classes cyclotomiques modulo 13 qui sont minimales pour l'inclusion.
2. En déduire l'existence d'un code cyclique contenu dans $\mathbb{F}_3^{13}$ de dimension 7 et distance minimale supérieure ou égale à 5. Vous devrez préciser la classe cyclotomique associée (obtenue comme une union de classes cyclotomiques minimales).
3. Si l'on se place maintenant sur $\mathbb{F}_{27}$ quelles sont les classes cyclotomiques modulo 13 (cette fois-ci il s'agira des parties de $\mathbb{Z}/13\mathbb{Z}$ stables par multiplication par 27).
4. Montrer qu'il existe des codes cycliques MDS contenus dans $\mathbb{F}_{27}^{13}$.

Exercice 3 (Une borne sur les paramètres d'un code)**.** *Dans tout cet exercice les codes sont des codes linéaires binaires (i.e. des sous-espaces vectoriels de $\mathbb{F}_2^n$).* Soit $C \subset \mathbb{F}_2^n$ un code de paramètres $[n,k,d]$ (n désignant sa longueur, k sa dimension et d sa distance minimale. Quitte à permuter les coordonnées, (ce qui n'a pas d'influence sur les poids), on peut supposer que le mot $c = (1\cdots1\ 0\cdots\cdots0)$ de poids d tel que $c_1 = \cdots = c_d = 1$ et $c_{d+1} = \cdots = c_n = 0$ appartient à C. On introduit également l'application de poinçonnage
$$p : \left\{ \begin{array}{ccc} \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^{n-d} \\ (x_1,\ldots,x_n) & \longmapsto & (x_{d+1},\ldots,x_n) \end{array} \right. .$$

1. Montrer que c est l'unique vecteur de $C \setminus \{0\}$ tel que $p(c) = 0$.
2. Montrer que l'image C' de C par p est de dimension $k-1$.

3. Soit d' la distance minimale de C' (l'image de C par p). Soit $v \in C$ un mot tel que $p(v) \in C'$ soit de poids d'. Soit $a \stackrel{\text{def}}{=} w_H(v) - d'$. Notons qu'il existe $u \in \mathbb{F}_2^d$ tel que v s'écrit $v = (u|p(v))$ où "|" désigne la concaténation des mots. Dans ce contexte, a n'est autre que le poids de u.

   Montrer les inégalités suivantes

   (i) $a + d' \geqslant d$;

   (ii) $d - a + d' \geqslant d$.

   Indication ; on utilisera le fait que p est linéaire et $p(c) = 0$.

4. En déduire que $d' \geqslant \frac{d}{2}$.

5. Montrer que pour tout code C de paramètres $[n, k, d]$ on a

$$n \geqslant \sum_{i=0}^{k-1} \frac{d}{2^i}. \tag{E}$$

6. Donner une matrice génératrice d'un code binaire $[6, 2, 4]$ et d'un $[9, 2, 6]$. En déduire que la borne (E) est optimale pour $k = 2$ et n multiple de 3. Autrement dit que pour tout entier $a > 0$, il existe un code binaire $[3a, 2, 2a]$.

7. Soit $(C_\ell)_{\ell \in \mathbb{N}}$ une suite de codes de paramètres $[n_\ell, k_\ell, d_\ell]$ telle que $(n_\ell)_\ell$ et $(k_\ell)_\ell$ tendent vers l'infini et telle que la suite $(d_\ell/n_\ell)_\ell$ converge vers un réel δ. Montrer que $\delta \leqslant \frac{1}{2}$.

8. Le résultat précédent est-il plus précis, moins précis ou aussi précis que la borne de Plotkin asymptotique ?