Solutions du Partiel du 17 novembre 2014

Exercice 1 (Calcul d'une distribution de poids)**.** 1. Étant donné que pour tout code C, on a

$$\dim C + \dim C^{\perp} = n.$$

Si $C = C^{\perp}$, nécessairement, n est pair et la dimension de C est $\frac{n}{2}$.

2. Le fait qu'il soit auto dual signifie entre autres que

$$\begin{aligned} \forall c \in C,\ \langle c, c\rangle &= 0 \\ \sum_{i=1}^{n} c_i^2 &= 0 \\ \sum_{i=1}^{n} c_i &= 0, \end{aligned}$$

ce qui entraîne que c est de poids pair.

3. Le polynôme énumérateur des poids est en toute généralité de la forme :

$$P_C^{\sharp}(x,y) = a_0y^6 + a_1xy^5 + a_2x^2y^4 + +a_3x^3y^3 + a_4x^4y^2 + a_5x^5y + a_6x^6. \tag{1}$$

Par ailleurs, d'après la question précédente, le code n'a que des mots de poids pair, ce qui implique $a_1 = a_3 = a_5 = 0$. De plus, $a_0 = 1$ car le seul mot de poids 0 est le mot nul qui appartient à C car il est linéaire. Le fait que $a_6 \in \{0, 1\}$ vient de ce que le seul mot de poids 6 est le mot (1 1 1 1 1 1) donc suivant s'il appartient ou non à C, on a $a_6 = 0$ ou $a_6 = 1$. Enfin, comme C est de dimension 3 (car autodual, c.f. question 1.), on a $|C| = 2^3 = 8$ et

$$\begin{aligned} |C| &= \sum_{i=0}^{6} |\{c \in C \mid w_H(c) = i\}| \\ &= 1 + a_2 + a_4 + a_6. \end{aligned}$$

4. La transformée de McWilliams appliquée à $P_C^{\sharp}$ montre que le coefficient en x^6 de $P_C^{\sharp}(y-x, x+y)$ est égal à $1 + a_2 + a_4 + a_6 \neq 0$ (= $|C|$ d'après la question précédente). Par conséquent, comme C est autodual, $P_C^{\sharp}(x,y) = \frac{1}{|C|}P_C^{\sharp}(y-x, x+y)$ et donc, le terme en x^6 de $P_C^{\sharp}$ est égal à 1. Ce qui entraîne que $(1\ 1\ 1\ 1\ 1\ 1) \in C$.

5. Comme $(1\ 1\ 1\ 1\ 1\ 1) \in C$, pour tout mot $c \in C$ de poids 2, $(1\ 1\ 1\ 1\ 1\ 1) + c$ est également dans C et est de poids 4. L'application $C \to (1\ 1\ 1\ 1\ 1\ 1) + c$ est une bijection de l'ensemble des mots de poids 2 dans l'ensemble des mots de poids 4. D'où $a_2 = a_4$.

Remarque : Plus généralement, le fait que $(1\ 1\ 1\ 1\ 1\ 1) \in C$ *entraîne que* $P_C^{\sharp}$ *est* réversible, *i.e.* $P_C^{\sharp}(x,y) = P_C^{\sharp}(y,x)$.

6. D'après les questions précédentes, on a obtenu le système de relations suivant :

$$\left\{\begin{array}{ccc} a_6 & = & 1 \\ a_2 & = & a_4 \\ 1+a_2+a_4+a_6 & = & 8 \end{array}\right.$$

Par conséquent, on en déduit que $a_2 = a_4 = 3$ et donc

$$P_C^\sharp(x,y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6.$$

Exercice 2. 1. $\{0\}, \{1,3,9\}, \{2,6,5\}, \{4,12,10\}, \{7,8,11\}$.

2. Considérons la classe cyclotomoique obtenue par réunion des classes $\{2,6,5\}$ et $\{7,8,11\}$. Elle contient 4 entiers consécutifs, à savoir : $5,6,7,8$. D'après la borne BCH, le code correspondant est de distance minimale supérieure ou égale à 5. Par ailleurs, le polynôme générateur du code cyclique correspondant a 6 racines distinctes dans l'extension cyclotomique, il est donc de degré 6. La dimension du code cyclique correspondant est de fait égale à 7.
3. Le corps $\mathbb{F}_{27}$ contient toutes les racines 13-èmes de l'unité. En effet, dans ce corps on a

$$X^{q-1} - 1 = X^{26} - 1 = \prod_{a \in \mathbb{F}_{27}^\times} (X - a).$$

Donc, $\mathbb{F}_{27}$ contient toutes les racines 26-èmes de l'unité. À fortiori, il contient toutes les racines 13-èmes puisque 13 divise 26. Ces racines 13-èmes s'obtiennent d'ailleurs en prenant les carrés des racines 26-èmes. De fait, les classes cyclotomiques sont dans ce cas les singletons $\{a\}$ pour tout $a \in \mathbb{Z}/13\mathbb{Z}$. Une autre façon de le voir est que la multiplication par 27 dans $\mathbb{Z}/13\mathbb{Z}$ n'est autre que la multiplication par 1 car $27 \equiv 1 \mod 13$.
4. L'ensemble $\{1,2,3,4\}$ (par exemple) est une classe cyclotomique 27–aire modulo 13. Donc le code cyclique associé est de distance minimale $\geqslant 5$ et a un polynôme générateur de degré 4. Il est donc de dimension 9. D'après la borne de Singleton, il est de distance exactement 5 et est de fait MDS.

Exercice 3 (Une borne sur les paramètres d'un code)**.** 1. Supposons l'existence d'un second vecteur $c' \neq c$ tel que $p(c') = 0$. Cela signifie que le support de c' est contenu dans $\{1,\dots,d\}$ et comme $c' \neq c$ par hypothèse, il a donc son support strictement contenu dans cet ensemble. De ce fait son poids est strictement inférieur à d ce qui implique que $c' = 0$ par définition de la distance minimale.

2. D'après la question précédente, le noyau de la restriction de p à C est de dimension 1 sur $\mathbb{F}_2$. D'après le théorème du rang, son image est de dimension $k-1$.
3. L'inégalité (i) vient de ce que $v \in C$, $v \neq 0$ (car il est de poids $\geqslant d'$) donc $w_H(v) \geqslant d$. L'inégalité (ii) vient de ce que $c - v \in C$ (par linéarité), $c + v \neq 0$ car v a des coefficients non nuls parmi les $v_{d+1},\dots,v_n$ et que tous les $c_{d+1},\dots,c_n$ sont nuls. On obtient alors (ii) à partir de $w_H(c+v) \geqslant d$ et en notant que $w_H(c+v) = d - a + d'$.
4. Si on additionne les inégalités (i) et (ii), on obtient : $2d' \geqslant d$.
5. Nous allons démontrer ce résultat par récurrence sur k. Si $k = 1$, on a de façon évidente que $d \leqslant n$. Soit maintenant $k > 1$ et supposons le résultat vrai pour tout code de dimension $< k$. Comme le code $p(C)$ est de longueur $n - d$ et de dimension $k - 1$, on peut appliquer l'hypothèse de récurrence à $p(C)$. On obtient

$$n - d \geqslant \sum_{i=0}^{k-2} \frac{d'}{2^i}$$

Puis en utilisant le résultat de la question précédente, à savoir que $d' \geqslant \frac{d}{2}$, on en déduit :

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

6. Les matrices suivantes conviennent :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Plus généralement, on prend le code engendré par les mots c, c' ou $c_i = 1$ pour $1 \leqslant i \leqslant 2a$ et $c_i = 0$ sinon et $c'_i = 1$ pour $a + 1 \leqslant i \leqslant n$ et $c'_i = 0$ sinon.

7. De la borne on obtient

$$n \geqslant d \sum_{i=0}^{k-1} \frac{1}{2^i}$$
$$1 \geqslant \delta \frac{1 - \frac{1}{2^k}}{1 - \frac{1}{2}}$$
$$\frac{1}{2} \underbrace{\frac{1}{1 - \frac{1}{2^k}}}_{\longrightarrow 1} \geqslant \delta.$$

8. Ce résultat est moins précis : la borne de Plotkin asymptotique dit que $R \leqslant 1 - 2\delta$. Comme $R \geqslant 0$ cela entraîne $\delta \leqslant \frac{1}{2}$. En fait, le résultat obtenu est strictement moins bon que la borne de Plotkin dès lors que $R > 0$.