Codes correcteurs 1 — 2018–2019
Prof. M. Borello — Université Paris 8

CONTRÔLE CONTINU N° 1

NOM Prénom : .....

Numéro d'étudiant : .....

Barême : Ex1-10 points, Ex2-10 points.

Exercice 1. *Donner la liste des codes cycliques binaires de longueur* 8*, en précisant leurs paramètres. Parmi ces codes, y en a-t-il un qui est autodual ?*

Solution : $x^8+1=(x+1)^8$ dans $\mathbb{F}_2[x]$. Ainsi, les polynômes générateurs des idéaux $\mathcal{C}_i$ dans $\mathbb{F}_2[x]/\langle x^8+1\rangle$, i.e. des codes cycliques binaires non nuls de longueur 8, sont $g_i(x)=(x+1)^i$ pour $i\in\{0,1,2,\dots,7\}$. Notons que

$$\{0\}\subset\mathcal{C}_7\subset\mathcal{C}_6\subset\mathcal{C}_5\subset\mathcal{C}_4\subset\mathcal{C}_3\subset\mathcal{C}_2\subset\mathcal{C}_1\subset\mathcal{C}_0=\mathbb{F}_2^8,$$

de manière que $\mathrm{d}(\mathcal{C}_i)\geq\mathrm{d}(\mathcal{C}_j)$ si $i\geq j$. On fait la liste des codes non triviaux.

(1) $g_1(x)=(x+1)$ engendre le code de parité $\mathcal{C}_1$ de paramètres $[8,7,2]$.

(2) $g_2(x)=x^2+1$ engendre le code $\mathcal{C}_2$ qui a dimension $8-2=6$ et distance minimale 2 (en effet, $g_2(x)$ a poids 2 et $\mathrm{d}(\mathcal{C}_2)\geq\mathrm{d}(\mathcal{C}_1)=2$).

(3) $g_3(x)=x^3+x^2+x+1$ engendre le code $\mathcal{C}_3$ qui a dimension $8-3=5$ et distance minimale 2 (en effet, $g_3(x)+xg_3(x)$ a poids 2 et $\mathrm{d}(\mathcal{C}_3)\geq\mathrm{d}(\mathcal{C}_2)=2$).

(4) $g_4(x)=x^4+1$ engendre le code $\mathcal{C}_4$ qui a dimension $8-4=4$ et distance minimale 2 (en effet, $g_4(x)$ a poids 2 et $\mathrm{d}(\mathcal{C}_4)\geq\mathrm{d}(\mathcal{C}_3)=2$).

(5) $g_5(x)=x^5+x^4+x+1$ engendre le code $\mathcal{C}_5$ qui a dimension $8-5=3$ et distance minimale 4 (on peut le calculer en faisant une liste des 8 mots à partir d'une matrice génératrice).

(6) $g_6(x)=x^6+x^4+x^2+1$ engendre le code $\mathcal{C}_6$ qui a dimension $8-6=2$ et distance minimale 4 (on peut le calculer en faisant une liste des 4 mots à partir d'une matrice génératrice)

(7) $g_7(x)=x^7+x^6+x^5+x^4+x^3+x^2+x+1$ engendre le code $\mathcal{C}_7$ qui a dimension $8-7=1$ et distance minimale 8 (c'est le code de répétition).

Le seul code qui peut être autodual est $\mathcal{C}_4$, en ayant dimension $4=8/2$. En fait, il l'est (une manière de le voir est la suivante : le dual d'un code cyclique est cyclique, donc le dual de $\mathcal{C}_4$ est un code cyclique de dimension $8-4=4$, i.e. lui-même, le seul avec ces propriétés).

Exercice 2. *On veut factoriser* x^5-1 *sur* $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$ (*avec* $\alpha^2=\alpha+1$).

a) *Quel est l'ordre* m *de* 4 *dans* $(\mathbb{Z}/5\mathbb{Z})^*$ *?*

b) *Soit* β *une racine du polynôme irréductible* $x^2+\alpha x+1\in\mathbb{F}_4[x]$. *Montrer que* β *est une racine primitive* 5*-ième de l'unité dans*

$$\mathbb{F}_{16}=\mathbb{F}_4[\beta]=\mathbb{F}_4[x]/\langle x^2+\alpha x+1\rangle.$$

c) *Donner les classes cyclotomiques modulo* 5 *sur* $\mathbb{F}_4$ *et les polynômes minimaux correspondants.*

Solution :

a) On a $4\neq 1$ dans $(\mathbb{Z}/5\mathbb{Z})^*$ et $4^2=16\equiv 1 \bmod 5$, de manière que $m=2$ est l'ordre de 4 dans $(\mathbb{Z}/5\mathbb{Z})^*$.

b) On doit montrer que l'ordre de $\beta\neq 1$ dans le groupe $\mathbb{F}_{16}^*$ est 5. On a

$$\beta^5=\beta(\beta^2)^2=\beta(\alpha\beta+1)^2=\beta(\alpha^2\beta^2+1)=\beta((\alpha+1)(\alpha\beta+1)+1)=\ldots=1,$$

ce qui montre le résultat.

c) Les classes cyclotomiques modulo 5 sur $\mathbb{F}_4$ et les polynômes minimaux correspondants sont

- $C_0=\{0\}$ et $M_0(x)=x-\beta^0=x-1$;
- $C_1=\{1,4\}$ et $M_1(x)=(x-\beta)(x-\beta^4)=x^2+\alpha x+1$;
- $C_2=\{2,3\}$ et $M_2=(x-\beta^2)(x-\beta^3)=x^2+(\alpha+1)x+1$.