Corrigé de l'examen

Mercredi 15 mai 2019.
Durée 2h. Aucun document autorisé

Solution 1. —

1. (a) *Déterminer le nombre d'éléments de* $\mathbf{F}_{64}^*$
   $\mathbf{F}_{64}^*$ contient 63 éléments.
   (b) *Pour chaque ordre possible d, donner le nombre d'éléments de* $\mathbf{F}_{64}^*$*, d'ordre d.*
   $\mathbf{F}_{64}^*$ est un groupe cyclique. Il contient $\varphi(d)$ éléments d'ordre d si d divise 63. Les diviseurs de 63 sont $1,3,7,9,21,63$. On a $\varphi(3)=2$, $\varphi(7)=6$, $\varphi(9)=6$, $\varphi(21)=12$, $\varphi(63)=36$. Il contient donc 1 élément d'ordre 1, 2 éléments d'ordre 3, 6 éléments d'ordre 9, 12 éléments d'ordre 21, 36 éements d'ordre 63.
2. Soit $P = X^6+X^3+1 \in \mathbf{F}_2[X]$.
   (a) *Montrer que P divise* X^9-1 *dans* $\mathbf{F}_2[X]$
   On a $X^9-1 = (X^3-1)\cdot P$ donc P divise X^9-1.
   (b) *En déduire que P a toutes ses racines dans* $\mathbf{F}_{64}$.
   P divise X^9-1 dans $\mathbf{F}_2[X]$ donc dans $\mathbf{F}_{64}[X]$. P divise donc $X^{63}-1=(X^9)^7-1$ dans $\mathbf{F}_{64}[X]$. Les racines de P sont parmi les racines de $X^{63}-1$ qui sont exactement les 63 éléments de $\mathbf{F}_{63}^*$.
3. (a) *Montrer que* α *est d'ordre 9 dans* $\mathbf{F}_{64}^*$.
   On a $\alpha^9-1=(\alpha^3-1)P(\alpha)=0$. Donc $\alpha^9=1$ mais $\alpha^3=1+\alpha^6\neq 1$ car $\alpha\neq 0$, donc α est d'ordre 9.
   (b) *Quel est le degré du polynôme minimal de* α *sur* $\mathbf{F}_2$ *?*
   Soit M_α de degré d le polynôme minimal de α. Alors $\overline{X}\in\mathbf{F}_2[X]/(M_\alpha)$ est racine de P et est donc d'ordre 9. Donc $9 \mid 2^d-1$, c'est-à-dire, $\mathrm{ord}_9(2) \mid d$ (l'ordre de 2 dans $(\mathbf{Z}/9\mathbf{Z})^*$ divise d). Mais $\mathrm{ord}_9(2)=6$ donc $6 \mid d$ et $d=6$. *On pouvait aussi utiliser directement le résultat du cours : le degré du polynôme minimal de* α *d'ordre N sur* $\mathbf{F}_p$ *est l'ordre de q dans* $(\mathbf{Z}/N\mathbf{Z})^*$ *(lorsque* $(p,N)=1$*).*
   (c) *En déduire que P est irréductible dans* $\mathbf{F}_2[X]$.
   Si α est une racine de P alors $M_\alpha \mid P$ donc $P=M_\alpha$ est irréductible.
4. (a) *Montrer que* $\mathcal{B}=(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5)$ *est une base du* $\mathbf{F}_2$*-espace vectoriel* $\mathbf{F}_{64}$.
   Si $\sum_{i=0}^5 u_i\alpha^i=0$ alors $Q=\sum_{i=0}^5 u_iX^i$ annule α et donc $M_\alpha=P$ divise Q, donc $Q=0$.
   (b) *Montrer que les racines de P sont* $\{\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8\}$.
   Si $P(\gamma)=0$ alors $P(\gamma^2)=P(\gamma)^2=0$. On déduit que $\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^{16}=\alpha^7,\alpha^{32}=\alpha^5$ sont 6 racines distinctes de P. Ce sont les racines de P.
   (c) *Écrire les racines de P dans la base* $\mathcal{B}$.
   On a $\alpha=\alpha$, $\alpha^2=\alpha^2$, $\alpha^4=\alpha^4$, $\alpha^8=\alpha^5+\alpha^2$, $\alpha^7=\alpha+\alpha^4$, $\alpha^5=\alpha^5$.
5. Soit $\beta=1+\alpha$.
   (a) *Montrer que* $\beta^{21}=1+\alpha^3$.
   On a

$$\begin{aligned}\beta^{21} &= \beta\cdot\beta^4\cdot\beta^{16}=(1+\alpha)\cdot(1+\alpha^4)\cdot(1+\alpha^{16})\\ &= 1+\alpha+\alpha^4+\alpha^{16}+\alpha^5+\alpha^{17}+\alpha^{20}+\alpha^{21}\\ &= 1+\alpha+\alpha^4+\alpha^7+\alpha^5+\alpha^8+\alpha^2+\alpha^3\\ &= 1+\alpha P(\alpha)+\alpha^2P(\alpha)+\alpha^3=1+\alpha^3.\end{aligned}$$

(b) *En déduire que* β *est d'ordre 63.*
On a $\beta^{21} \neq 1$ donc β n'est pas d'ordre divisant 21 ni d'ordre 9 (les 6 racines de P sont d'ordre 9), donc est d'ordre 63.

(c) *Déterminer le polynôme minimal de* β *sur* $\mathbf{F}_2[X]$.
On a $P(1+\beta)=0$ donc $Q(X)=P(1+X)=X^6+X^4+X^3+X+1$ est le polynôme minimal de β. Il est de degré 6. *On avait aussi que* $\mathrm{ord}_{63}(2)=6$.

6. **Question bonus :** *Déterminer le nombre de polynôme unitaires irréductibles de degré 6 de* $\mathbf{F}_2[X]$.
Les éléments de $\mathbf{F}_{64}$ dont le polynôme minimal est de degré 6 sont ceux qui ne sont ni dans $\mathbf{F}_8$, ni dans $\mathbf{F}_4$. Il en reste $36+6+12=54$. Mais chaque polynôme irréductible de degré 6 a 6 racines dans $\mathbf{F}_{64}$. Il y a donc $54/6=9$ polynômes irréductibles de degré 6 dans $\mathbf{F}_2[X]$.

Solution 2. —

1. Soit $\mathcal{C}$ le code correcteur de longueur 4 sur $\mathbf{F}_3$:

$$\{(u+v,u-v,2u,2v); u,v \in \mathbf{F}_3\}$$

(a) *Quelle est la dimension de* $\mathcal{C}$ *?*
Une base de $\mathcal{C}$ est $\big((1,1,2,0),(1,-1,0,2)\big)$. La dimension est 2.

(b) *Écrire une matrice génératrice G de* $\mathcal{C}$.
On peut prendre $G=\begin{pmatrix}1 & 1 & 2 & 0\\ 1 & -1 & 0 & 2\end{pmatrix}$. En faisant des opérations élémentaires sur les lignes de G, on obtient $G \sim \begin{pmatrix}2 & 0 & 2 & 2\\ 1 & -1 & 0 & 2\end{pmatrix} \sim \begin{pmatrix}2 & 0 & 2 & 2\\ 0 & 2 & 2 & 1\end{pmatrix} = 2\begin{pmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 1 & 2\end{pmatrix}$.
C'est-à-dire $\Big((1,0,1,1),(0,1,1,2)\Big)$ est une base de $\mathcal{C}$.

(c) *Montrer que* $H=G$ *est également une matrice de contrôle de* $\mathcal{C}$.
Une matrice de contrôle est de dimension $(n-k)\times n = 2\times 2$, de rang $n-k=2$ et doit vérifier $H\cdot {}^tG = 0$. G est bien de rang 2 et vérifie $G\cdot {}^tG = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

(d) *En déduire les paramètres de* $\mathcal{C}$ *(longueur, dimension, distance minimale).*
Pour déterminer la distance minimale on doit calculer le nombre minimal de colonnes liées de H. Les colonnes sont non-nulles donc $d>1$. Les colonnes ne sont pas proportionnelles donc $d>2$. On a aussi $H_1+H_2-H_3=0$ donc $d=3$.
$\mathcal{C}$ est un $[4,2,3]_3$ code. Sa capacité de correction est $t=(d-1)/2=1$.

(e) $\mathcal{C}$ *est-il MDS ?*
Oui, on a $n+1=k+d=5$.

2. (a) *Quel est le cardinal d'une boule de rayon 1 dans* $(\mathbf{F}_3)^4$ *?*
La boule $B(0,1)$ contient son centre $(0,0,0,0)$ et 8 éléments à une distance 1 de l'origine (choisir 1 valeur non nulle parmi 2 sur 1 coordonnée parmi 4). Le cardinal d'une boule de rayon 1 est 9.

(b) *En déduire que* $\mathcal{C}$ *est un code parfait.*
$\mathcal{C}$ est parfait car les boules de rayon 1 sont disjointes ($d=3$) et leur réunion est de cardinal 81, c'est-à-dire, le cardinal de $(\mathbf{F}_3)^4$.

(c) *Le mot* $x=(1,1,1,1)$ *appartient-il à* $\mathcal{C}$ *?*
Calculons le syndrome $s(x)=H{}^tx = H_1+H_2+H_3+H_4 = G_1+G_2+G_3+G_4 = \begin{pmatrix}0\\ 1\end{pmatrix} = H_2 = H(e_2)$. On déduit que le syndrome de x n'est pas nul donc $x \notin \mathcal{C}$.

(d) *Trouver le mot du code* $c \in \mathcal{C}$ *le plus proche de x.*
On a $s(x)=H_2=s((0,1,0,0))$, donc $x=c+e_2$ et $c=x-e_2=(1,0,1,1)$. La distance $w(x-c)$ vaut 1.