Université Pierre et Marie Curie

2M120 – Éléments d'arithmétique

Examen partiel du 26 octobre 2016

Durée : 1 heure 30 minutes

**Aucun document n'est autorisé. L'utilisation de tout appareil électronique (tel que calculatrices, téléphones portables, montres connectées, etc.) est interdite. Ceux-ci doivent être rangés dans les sacs et mis en position éteinte.**

Les correcteurs tiendront compte de la qualité de la rédaction et de la précision des raisonnements.

## Partie I — Un cas particulier

Soit $G_5 = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 2 & 3 \\ 3 & 2 & 1 \end{array}\right)$ à coefficients $\boxed{\text{dans } \mathbb{F}_5}$ et $C_5$ le code linéaire de matrice génératrice $G_5$.

1. Quelle est la longueur $n_5$ de $C_5$ ? Quelle est sa dimension $k_5$ ?
2. Construire à partir de $G_5$ une matrice de contrôle $H_5$ de $C_5$.
3. Montrer que la matrice $H'_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$ est également une matrice de contrôle de $C_5$.
4. À l'aide de $H'_5$, déterminer la distance minimum $d_5$ de $C_5$ ainsi que sa capacité de correction $t_5$. $C_5$ est-il un code MDS ?
5. Soit $x_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \in (\mathbb{F}_5)^5$.
   (a) Calculer le syndrome de $s_5 = S(x_5) = H'_5 \times x_5$.
   (b) Montrer qu'il existe un unique $c_5 \in C$ tel que $d(c_5, x_5) \leq 1$ et le déterminer.
   (c) Déterminer $m_5 \in (\mathbb{F}_5)^3$ tel que $c_5 = G_5 \times m_5$.
6. Soit $x'_5 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 4 \end{pmatrix} \in (\mathbb{F}_5)^5$.
   (a) Calculer le syndrome de $s'_5 = S(x'_5) = H'_5 \times x'_5$.
   (b) Montrer qu'il existe pas de mot de code $c'_5 \in C_5$ tel que $d(c'_5, x'_5) \leq 1$.
   (c) Le code $C_5$ est-il parfait ?

## Partie II — Préliminaire au cas général

Soit $p \geq 3$ un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ le corps à $p$ éléments. On écrit $p$ sous la forme $p = 2q + 1$ où $q$ est un nombre entier.

7. Montrer que $1 + 2 + \cdots + (p-1)$ est un multiple de $p$ dans $\mathbb{Z}$.
8. Montrer que $1 + 2 + \cdots + (p-2) = 1$ dans $\mathbb{F}_p$.
9. Exprimer, en fonction de $q$, la valeur de l'inverse de 2 dans $\mathbb{F}_p$.

## Partie III — Le cas général

Soit maintenant $G$, la matrice à coefficients $\boxed{\text{dans } \mathbb{F}_p}$ à $p$ lignes et $p-2$ colonnes :

$$G = \left(\begin{array}{ccccc} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ \hline 1 & 2 & \cdots & p-3 & p-2 \\ p-2 & p-3 & \cdots & 2 & 1 \end{array}\right)$$

et $C$ le code linéaire sur $\mathbb{F}_p$ de matrice génératrice $G$.

10. Quelle est la longueur $n$ de $C$ ? Quelle est sa dimension $k$ ?
11. Construire à partir de $G$ une matrice de contrôle $H$ de $C$.
12. Montrer que la matrice $H'$, à 2 lignes et $p$ colonnes :

$$H' = \left(\begin{array}{ccccc|cc} 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ 2 & 3 & \cdots & p-2 & p-1 & 0 & 1 \end{array}\right)$$

est également une matrice de contrôle de $C$.

13. Soit $c_1 = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \in (\mathbb{F}_p)^p$.

(a) Calculer le syndrome de $s_1 = S(c_1) = H' \times c_1$ et montrer que $c_1 \in C$.
(On pourra utiliser le résultat de la question 7 pour simplifier l'expression de $s_1$.)

(b) Déterminer $m_1 \in (\mathbb{F}_p)^{p-2}$ tel que $c_1 = G \times m_1$.

14. À l'aide de $H'$, déterminer la distance minimale $d$ de $C$, ainsi que sa capacité de correction $t$.
$C$ est-il un code MDS ?

15. Soit $x_2 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix} \in (\mathbb{F}_p)^p$.

(a) Calculer le syndrome de $s_2 = S(x_2) = H' \times x_2$.

(b) Montrer qu'il existe un unique $c_2 \in C$ tel que $d(c_2, x_2) = 1$ et le déterminer.
(On pourra utiliser le résultat de la question 9.)

(c) Déterminer $m_2 \in (\mathbb{F}_p)^{p-2}$ tel que $c_2 = G \times m_2$.

16. Soit $x \in (\mathbb{F}_p)^p$ tel que $S(x) = H' \times x = \begin{pmatrix} u \\ v \end{pmatrix}$ avec $u \neq 0$ dans $\mathbb{F}_p$.
Montrer qu'il existe un unique $c \in C$ tel que $d(x, c) = 1$.

17. Soit $x \in (\mathbb{F}_p)^p$ tel que $S(x) = H' \times x = \begin{pmatrix} 0 \\ v \end{pmatrix}$ avec $v \neq 0$ dans $\mathbb{F}_p$.
Montrer qu'il n'existe pas de mot de code $c \in C$ tel que $d(x, c) \leq 1$.

18. Le code $C$ est-il parfait ?