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 ?

Solution : $n_5 = 5$; $k_5 = 3$.

2. Construire à partir de G_5 une matrice de contrôle H_5 de C_5.

Solution : $H_5 = \left(\begin{array}{ccc|cc} 4 & 3 & 2 & 1 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{array}\right)$

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.

Solution : On obtient H_5' à partir de H_5 en ajoutant la deuxième ligne de H_5 à la première. H_5' étant obtenue à partir de H_5 par opérations élémentaires sur les lignes, c'est donc 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 ?

Solution : Les colonnes de H_5' ne sont pas nulles, donc $d_5 \geq 2$. Deux colonnes quelconques de H_5' ne sont pas proportionnelles, car les colonnes sont distinctes et le premier coefficient de chaque colonne est 1 (pour être proportionnelles, deux colonnes devraient donc être égales). On a donc $d_5 \geq 3$. Enfin on sait que $d_5 \leq n_5 - k_5 + 1 = 3$ d'où $d_5 = 3$. C_5 est un code MDS car $d_5 = n_5 - k_5 + 1$.

5. Soit $x_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \in (\mathbb{F}_5)^5$.

   (a) Calculer le syndrome de $s_5 = S(x_5) = H_5' \times x_5$.

Solution : $S(x_5) = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 3 \end{pmatrix}$.

   (b) Montrer qu'il existe un unique $c_5 \in C$ tel que $d(c_5, x_5) \leq 1$ et le déterminer.

Solution : Le syndrome de x_5 égale 2 fois la deuxième colonne de H'.

Donc le mot de code $c_5 = x_5 - \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ appartient à C_5.

De plus comme la distance minimum de C_5 est 3, c_5 est bien l'unique élément de C_5 à distance ≤ 1 de x_5.

(c) Déterminer $m_5 \in (\mathbb{F}_5)^3$ tel que $c_5 = G_5 \times m_5$.

Solution : Les coordonnées de m_5 sont les trois premières coordonnées de c_5 : $m_5 = \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}$.

6. Soit $x'_5 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 4 \end{pmatrix} \in (\mathbb{F}_5)^5$.

(a) Calculer le syndrome de $s'_5 = S(x'_5) = H'_5 \times x'_5$.

Solution : $S(x'_5) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

(b) Montrer qu'il existe pas de mot de code $c'_5 \in C_5$ tel que $d(c'_5, x'_5) \leq 1$.

Solution : $S(x'_5) \neq 0$ donc $x'_5 \notin C_5$. De plus s'il existait $c'_5 \in C_5$ tel que $d(c'_5, x'_5) = 1$, alors $S(x'_5)$ serait égal à un multiple d'une colonne de H'_5. Mais la première coordonnée de $S(x'_5)$ est nulle alors que toutes les colonnes de H'_5 ont une première coordonnée non nulle. Il ne peut donc exister $c'_5 \in C_5$ tel que $d(c'_5, x'_5) = 1$.

(c) Le code C_5 est-il parfait ?

Solution : Le code C_5 n'est pas parfait car, d'après la question qui précède, il existe au moins un élément de $(\mathbb{F}_5)^5$ qu'on ne peut pas décoder.

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 $\mathbb{Z}$.

Solution : $1 + 2 + \cdots + (p-1) = \dfrac{p(p-1)}{2} = pq$ est bien un multiple de p dans $\mathbb{Z}$.

8. Montrer que $1 + 2 + \cdots + (p-2) = 1$ dans $\mathbb{F}_p$.

Solution : De ce qui précède, $1 + 2 + \cdots + (p-1) = 0$ dans $\mathbb{F}_p$, donc $1 + 2 + \cdots + (p-2) = 1 - p = 1$ dans $\mathbb{F}_p$.

9. Exprimer, en fonction de q, la valeur de l'inverse de 2 dans $\mathbb{F}_p$.

Solution : On a dans $\mathbb{F}_p$: $2q = -1$ donc $2(q+1) = 1$ et donc l'inverse de 2 dans $\mathbb{F}_p$ est $q + 1 = \dfrac{p+1}{2}$.

Partie III — Le cas général

Soit maintenant G, la matrice à coefficients 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 ?

Solution : $n = p$ et $k = p - 2$.

11. Construire à partir de G une matrice de contrôle H de C.

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

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.

Solution : La solution est la même que pour la question 3. On obtient H' à partir de H en ajoutant la deuxième ligne de H à la première. H' étant obtenue à partir de H par opérations élémentaires sur les lignes, c'est donc 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.)

Solution : $S(x_1) = \begin{pmatrix} p \\ 1 + 2 + \cdots + (p-1) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. (La deuxième coordonnée est nulle d'après la question 7.) Comme $S(x_1)$ est nulle, cela montre que $x_1 \in C$.

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

Solution : Les coordonnées de m_1 sont les $p - 2$ premières coordonnées de c_1 : $m_1 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \in (\mathbb{F}_p)^{p-2}$.

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 ?

Solution : La solution est la même que pour la question 4. Les colonnes de H' ne sont pas nulles, donc $d \geq 2$. Deux colonnes quelconques de H' ne sont pas proportionnelles, car les colonnes sont distinctes et le premier coefficient de chaque colonne est 1 (pour être proportionnelles, deux colonnes devraient donc être égales). On a donc $d \geq 3$. Enfin on sait que $d \leq n - k + 1 = 3$ d'où $d = 3$. C est un code MDS car $d = n - k + 1$.

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

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

Solution : $S(x_2) = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ q+1 \end{pmatrix}$.

(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.)

Solution : Le syndrome de x_2 égale 2 fois la q-ième colonne de H'.

Donc le mot de code $c_2 = x_2 - 2 \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ p-2 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix}$ appartient à C.

(La première coordonnée non nulle de c_2 est la q-ième. Les coordonnées de c_2 d'indices 1 à $q-1$, ainsi que celle d'indices $q+1$ à $p-2$, sont toutes nulles.

De plus comme la distance minimum de C est 3, c_2 est bien l'unique élément de C à distance ≤ 1 de x_2.

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

Solution : Les coordonnées de m_2 sont les $p-2$ premières coordonnées de c_2 : $m_2 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ p-2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in (\mathbb{F}_p)^{p-2}$.

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 $d(x, c) = 1$.

Solution : Les colonnes de H' sont tous les vecteurs $\begin{pmatrix} 1 \\ a \end{pmatrix}$ avec $a \in \mathbb{F}_p$. Or $S(x) = u \begin{pmatrix} 1 \\ u^{-1}v \end{pmatrix}$. C'est donc un multiple d'une colonne de H'. Soit i l'indice de cette colonne.

En soustrayant u à la i-ième coordonnée de x, on obtient un élément c de C tel que $d(x, c) = 1$.

De plus comme la distance minimum de C est 3, c est bien l'unique élément de C à distance ≤ 1 de x.

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 $d(x, c) \leq 1$.

Solution : La solution est la même que pour la question 6b. $S(x) \neq 0$ donc $x \notin C$. De plus, s'il existait $c \in C$ tel que $d(c, x) = 1$, alors $S(x)$ serait égal à un multiple d'une colonne de H'. Mais la première coordonnée de $S(x)$ est nulle alors que toutes les colonnes de H' ont une première coordonnée non nulle. Il ne peut donc exister $c \in C$ tel que $d(c, x) \leq 1$.

18. Le code C est-il parfait ?

Solution : La solution est la même que pour la question 6c. Soit $x = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ p-1 \end{pmatrix} \in (\mathbb{F}_p)^p$ On a $S(x) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Il existe donc au moins un élément de $(\mathbb{F}_p)^p$ qu'on ne peut pas décoder. Le code C n'est donc pas parfait.