Feuille de révisions

Classification des 16 éléments du corps $GF(16)$ en carrés successifs.

Soit $GF(16)$ le corps à 16 éléments, décrit par la table ci-dessous où α est racine de $X^4 + X + 1$. On sait que $GF(16)$ est un espace vectoriel sur $GF(2) = \{0, 1\}$, avec pour base $\mathcal{B} = \{1, \alpha, \alpha^2, \alpha^3\}$ et que $\beta^{15} = 1$ pour tout élément non nul β.
1) Montrer que les éléments $\beta = \alpha^5$ et $\gamma = \alpha^{10}$ vérifient $\beta^2 = \gamma$ et $\gamma^2 = \beta$ et qu'ils sont les racines du polyôme $X^2 + X + 1$; déduire que l'on a la décomposition suivante :

$$X^2 + X + 1 = (X - \beta)(X - \gamma)$$

2) Soit K l'ensemble $\{0, 1, \beta, \gamma\}$. Montrer que tout élément de K est racine de $X^4 - X$. Déduire que $X^4 - X$ est produit de 4 monômes que l'on précisera.
3) Montrer que l'addition ou la multiplication de deux éléments de K est encore un élément de K. Ecrire explicitement les tables d'addition et de multiplication pour K.
4) Montrer que α^3 est racine du polynôme $X^5 - 1$, ainsi que ses carrés successifs : $\alpha^6, \alpha^{12}, \alpha^9$. Décomposer $X^4 + X^3 + X^2 + X + 1$ en produit de 4 monômes.
5)Considérons le graphe G ayant pour sommets les 15 éléments non nuls de $GF(16)$ avec un arc de x vers y quand $y = x^2$. Désignons par $C(x)$ la composante fortement connexe de x.
a) Montrer qu'il y a un cycle de G passant par les 4 sommets : $\alpha^3, \alpha^6, \alpha^{12}$ et α^9. Déduire $C(\alpha^3)$.
b) Représenter le graphe de G par un dessin. Déterminer ses composantes fortement connexes. Que peut-on dire du graphe réduit ? De ses composantes faiblement connexes ?
c) Montrer que les composantes de α et de α^7 sont formées des racines de $X^4 + X + 1$ et de $X^4 + X^3 + 1$ respectivement. Décomposer ces deux polynômes en produit de 4 monômes.
6) Montrer que l'application qui à x fait correspondre $y = x^2$ est une application linéaire de $GF(16)$ dans lui- même, conidéré comme un espace vectoriel sur $GF(2)$. Préciser la matrice M de f par rapport à la base $\mathcal{B}$.
7) Montrer que M est inversible. Calculer son inverse. Justifier que tout élément y de $GF(16)$ admet une racine carrée unique $r(y)$. Déterminer $r(y)$ pour $y = 1, \alpha, \alpha^2, \alpha^3$. Quelle est la matrice de r par rapport à la base $\mathcal{B}$?

Feuille d'exercices n^{o}1 : Problèmes d'affectation

Exercice 1

Soit à résoudre le problème d'affectation de matrice des coûts :

$$A = \begin{pmatrix} 4 & 3 & 5 \\ 3 & 6 & 3 \\ 7 & 3 & 8 \end{pmatrix}$$

$a_{i,j}$ représente le coût d'affectation de l'ouvrier O_i à la tâche T_j.
1) Décomposer A en somme de 3 matrices : $A = C+L+R$ où C est colonnes-constantes, L lignes-constantes et R comporte un zéro au moins par rangée.
2) Donner un minorant du coût de toute affectation.
3) Montrer ensuite que toute affectation où O_3 ne fait pas T_2 coûte au moins 13. Conclure.

Exercice 2

Soit à résoudre le problème d'affectation de matrice des coûts :

$$A = \begin{pmatrix} 2 & 8 & 6 & 3 & 6 \\ 4 & 13 & 9 & 20 & 10 \\ 3 & 3 & 5 & 22 & 14 \\ 5 & 6 & 11 & 11 & 18 \\ 1 & 9 & 15 & 14 & 18 \end{pmatrix}$$

Ses coûts représentent des frais de déplacements de 5 inspecteurs vers des chantiers (en ligne k figurent les frais de l'inspecteur I_k vers les chantiers C_1, C_2, C_3, C_4 et C_5). On veut affecter un inspecteur et un seul à chaque chantier de façon à minimiser la somme des coûts des 5 déplacements.
1) Décomposer A en somme de 3 matrices : $A = C+L+R$ dans $M_{5,5}(\mathbb{R}^+)$où C est colonnes-constantes, L lignes-constantes et R comporte un zéro au moins par rangée.
2) Donner un minorant m du coût de toute affectation (m =coût par rapport à $C + L$).
3) Quel est le "deuxième minimum" r dans la ligne 5 de R ? Déduire que $(m + r)$ est un minorant du coût de toute affectation où I_5 ne va pas en C_1.
4) Si le cinquième inspecteur va en C_1, la sous-matrice correspondante S de R obtenue en éliminant la ligne 5 et la colonne 1 se décompose comme en 1), soit $S = C' + L' + R'$. Préciser. Déduire l'affectation de moindre coût dans ce sous-problème. Conclure.

Feuille d'exercices n^{o}2 : Les corps

Exercice 1

Construction explicite du corps à 16 éléments.

1) Dans $\mathbb{Z}_2[X]$, ensemble des polynômes à coefficients dans $\mathbb{Z}_2 = \{0, 1\}$, montrer que

a) $Q(X) = X^2 + X + 1$ est irréductible

b) $P(X) = X^4 + X + 1$ est irréductible

2) On choisit P comme modulo et on considère $GF(2^4) = \mathbb{Z}_2[X]_{/(X^4+X+1)}$. Ecrire la table des décompositions des éléments de $GF(2^4)$.

Exercice 2

Description matricielle du corps à 8 éléments.

Soit $F = GF(8)$ le corps à 8 éléments. C'est un espace vectoriel sur $GF(2) = \{0, 1\}$, avec pour base $\mathcal{B} = \{1, \alpha, \alpha^2, \alpha^3\}$, où α est racine de $X^3 + X + 1 = 0$. Tout élément z de F s'écrit de manière unique sous forme $z = (a + b\alpha + c\alpha^2)$ où a, b, c sont dans $GF(2)$; a, b, c sont ses "composantes binaires".
1) Calculer les composantes binaires du produit $zz^{'}$ où $z = (a + b\alpha + c\alpha^2)$ et $z^{'} = (a + b\alpha + c\alpha^2)$.
2) Dans l'ensemble $M_{3,3}(GF(2))$ des matrices carrées 3×3 à coefficients dans $GF(2)$. On note I la matrice identité et A la matrice suivante

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Calculer la matrice A^2 et montrer que $A^3 = A + I$.
3) Soit M l'application qui à tout élément $z = (a + b\alpha + c\alpha^2)$ de F fait correspondre la matrice : $M(z) = (aI + bA + cA^2)$. Préciser en fonction de a, b, c les coefficients de $M(z)$. Montrer que M est injective, que $M(z+z)^{'} = M(z) + M(z^{'})$ et $M(zz)^{'} = M(z)M(z^{'})$.
4) Montrer que pour tout entier k, on a $M(\alpha^k) = A^k$; en déduire que $A^7 = I$ et que toute puissance de A est égale à l'une des 7 matrices suivantes : $I, A, A^2, A^3, A^4, A^5, A^6$.
5) Montrer que A^3 a pour inverse A^4 et que $A^4 = A + A^2$. Calculer les coefficients de A^4. Déterminer de même les inverses des matrices A et A^2.
6) Calculer les matrices A^{59} et A^{222} et les produits suivants :

$P = (A+I)(A^2+A+I)$, $Q = (A^2+I)(A+I)^{141}$ et $R = (A^2+A+I)(A+I)^{23}$.
Méthode conseillée : se ramener à des puissances de A ou de α.

Feuille d'exercices n^{o}3 : Les codes

Exercice 1

Construction d'un code 2-correcteur.

Soit $\mathcal{C}$ le code de matrice de vérification

$$H = \begin{pmatrix} A | I_7 \end{pmatrix}$$

avec

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

1) Montrer que $C = \{Y / HY^T = 0\}$ est un sous-espace-vectoriel de $\mathbb{Z}_2^{10}$. Préciser sa dimension.
2) Donner une base de C (utiliser la matrice génératrice).
3) Montrer que tout système de 4 vecteurs colonnes de H est libre. Déduire que l'on peut toujours corriger 2 erreurs.
4) Montrer que dans C tout vecteur non nul a un support qui compte au moins $d = 5$ éléments.
5) Peut-on corriger 3 erreurs ?
6) Montrer que l'ensemble $\mathcal{C}^+$ des mots pairs de $\mathcal{C}$ est un sous-espace vectoriel de dimension 2 avec lequel on peut détecter 3 erreurs.
6) Montrer que l'ensemble $\hat{\mathcal{C}}$ des mots $\hat{Y}$ de $\mathcal{C}$ tels que $H\hat{Y}^T = 0$ est un sous-espace vectoriel de dimension 3. Donner son cardinal et une base. Combien d'erreurs peut-on corriger ?

Exercice 2

Indépendance et capacité de correction d'un code.

Soit $\mathcal{C}$ le code binaire dont la matrice de vérification de parité H est la suivante

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Pour tout mot binaire Y, on note $w(Y)$ son poids.
Si $Y = (y_1y_2y_3y_4y_5y_6y_7y_8)$ est un mot binaire de longueur 8, le produit $S = HY^T$ est un mot binaire de longueur 4 et de poids compris entre 0 et 4.
1) Montrer qu'étant donné un mot binaire Y de longueur 8 et de poids p,
a) si p est impair, alors le poids du produit $w(S)$ vaut 1 ou 3 ;
b) si $p = 2$, alors le poids du produit $w(S)$ vaut 2 ou 4.
2) Déduire que 3 colonnes quelconques de H forment un système libre.
3) Soit un mot binaire S de longueur 4. Montrer que
a) si S est de poids 1 ou 3, alors il existe un et un seul mot Y de poids 1 et de longueur 8 tel que $HY^T = S$;
b) si S est de poids 2 ou 4, alors il existe plusieurs mots Y de poids 2 et de longueur 8 tels que $HY^T = S$ (on précisera les solutions Y de l'équation matricielle $HY^T = S$ dans le cas où $S = (1100)$ et $S = (1111)$). Note : on déduit que $\mathcal{C}$ permet de corriger 1 erreur et de détecter 2 erreurs. Mais on ne peut pas reconstituer le mot initial quand il y a 2 erreurs.
4) Soit $\mathcal{C}$ l'ensemble des mots du code (caractérisés par $HY^T = 0$). Montrer que $\mathcal{C}$ est de dimension 4, qu'il contient le vecteur $\mathbf{1} = (11111111)$ et que tout mot Y de $\mathcal{C}$ distinct de $\mathbf{1}$ et de 0 est de poids $w(Y) = 4$. (indication : Y et $\mathbf{1} - Y$) sont de poids > 2 d'après la question 1)).

Exercice 3

Le code 1-correcteur de longueur 6 généré par $(I, A + I)$.

Soit $\mathcal{C}$ le code binaire dont la matrice génératrice est G définie par

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

1) Montrer que G est de rang plein et qu'elle admet deux inverses à droite distincts. Déterminer la dimension de $\mathcal{C}$ et sa matrice de vérification H.
2) Dans H, montrer que tout système lié de vecteurs lignes contient au minimum 3 vecteurs.
3) Trouver 3 vecteurs distincts Y, Y' et Z de poids respectifs 2, 2 et 1 tels que $YH = Y'H = ZH$.
4) Déduire que $\mathcal{C}$ permet de corriger une erreur mais pas de détecter 2 erreurs.
5) Montrer que l'ensemble $\mathcal{C}^+$ des mots pairs de $\mathcal{C}$ contient exactement 3 mots non nuls que l'on écrira et qu'ils sont de poids 4. Trouver K matrice 6×4 à coefficients dans $GF(2)$ telle que l'on ait $KY^T = 0$ si et seulement si $Y \in \mathcal{C}^+$ pour tout vecteur Y de longueur 6.
6) Montrer que $\mathcal{C}^+$ permet de détecter 2 erreurs mais pas de les corriger.

Feuille d'exercices n^{o}4 : Les graphes

Exercice 1

Réduction d'une matrice en changeant l'ordre des indices et calcul d'inverse de matrices.

Pour toute matrice carrée M de $\mathcal{M}_{n*n}$ notons $G(M)$ le graphe associé c'est à dire le graphe simple dont les sommet sont les indices $i = 1, 2, 3, 4, 5, 6$ avec un arc de i vers j si et seulement si le coefficient a_{ij} est non nul. Soit $R(M)$ le graphe réduit de $G(M)$.
1) Représenter par un dessin les graphes $G(N)$ et $R(N)$ correspondant à la matrice N suivante :

$$N = \begin{pmatrix} 11 & 0 & -3 & -4 & 11 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 3 & 5 & -1 & -1 & 2 & 2 \\ 3 & 2 & 0 & -1 & 3 & 1 \\ 0 & 0 & -2 & 0 & 0 & 3 \end{pmatrix}$$

Classer les 6 indices par composantes fortement connexes de $G(N)$ et répartir les composantes par niveaux de $R(N)$.
2) Vérifier que la composante fortement connexe J contenant l'indice 5 est "sans arc rentrant".
3) Déduire une matrice de permutation Q telle que $N^{'} = Q^t N Q$.

Exercice 2

Matrices d'adajacence d'un graphe et composantes connexes

Soit G le graphe ci-dessous.
1) Ecrire sa matrice booléenne d'adajacence B. Déterminer les puissances booléennes $(I + B)^k$ pour $k > 1$. A partir de quel rang la suite des $(I + B)^k$ est-elle stationnaire ?
2) Calculer la matrice booléenne P de la relation de précédence de G et déterminer les composantes fortement connexes de G.
3) Décrire le graphe réduit R de G. Répartir ses sommets par niveaux.

Exercice 3

Trigonalisation par blocs d'une matrice à coefficients réels.

1) Présicer le graphe G associé à la matrice C suivante :

$$C = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 & 5 \\ -4 & -8 & 0 & 6 & 6 & 2 \\ 4 & 7 & 4 & -3 & -6 & 7 \\ 0 & 0 & 0 & -1 & 0 & 1 \\ 3 & 5 & 0 & -1 & -7 & 6 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{pmatrix}$$

Réordonner les 6 indices par composantes fortement connexes de G et par niveaux du graphe réduit de G.
2) Déduire une matrice de permutation Q telle que Q^tCQ soit trigonale par blocs avec tous les zéros de Q^tCQ au-dessous de la diagonale principale. Calculer explicitement les coefficients de Q^tCQ.

Exercice 4

Soit G le graphe suivant :
Soient A sa matrice d'adjacence et B sa matrice booléenne d'adjacence.
1) Préciser A. Calculer A^2 et A^3. Combien y a-t-il de termes non nuls ?
2) Montrer que la suite de matrices $(I + B)^k$ est stationnaire à partir d'un certain rang r et interpréter le terme général de $(I + B)^r$.

Exercice 5

Situation d'un graphe à circuit.

Soit G le graphe suivant :
Soient A sa matrice d'adjacence et B sa matrice booléenne d'adjacence.
1) Montrer que les puissances A^k et B^k de A et B ne sont jamais nulles.
2) Montrer que la suite des B^k est périodique à parti d'un certain rang.
3) Déduire que la suite des $(I + B)^k$ est stationnaire à partir d'un certain rang.