Arithmétique et Applications, Combinatoire et Graphes.

Epreuve de mai 2019 – Solutions

1. $f(x) = x^2 + 2 \in \mathbb{F}_5[x]$

$f(0) = 2$, $f(1) = 3$, $f(2) = 1$, $f(3) = 1$, $f(4) = 3$ donc pas de facteur linéaire et $f$ est irréductible.

Soit $K = \mathbb{F}_5[x]/(f(x))$ alors $|K| = 25$ et $|K^*| = 24$ donc si $f(x)$ primitif, l'ordre de $a = \bar{x}$ est 24

On calcule son ordre :

$a^2 = -2 = 3 \pmod 5$

$1, a, a^2 = 3, a^3 = 3a, a^4 = 3a^2 = 9 = 4, a^5 = 4a, a^6 = 4a^2 = 12 = 2, a^7 = 2a,$

$a^8 = 2a^2 = 6 = 1 \pmod 5$

Donc l'ordre de $a$ est 8, pas 24, et $f(x)$ n'est pas primitif.

2. Matrice d'adjacence

$$M = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Le nombre de "1" est égal au nombre d'arêtes.

$$M^2 = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&1&1 \\ 0&1&1&0 \end{pmatrix}\begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&1&1 \\ 0&1&1&0 \end{pmatrix} = \begin{pmatrix} 0&0&1&0 \\ 1&0&1&1 \\ 0&1&2&1 \\ 1&0&2&1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 0&0&1&0 \\ 1&0&1&1 \\ 0&1&2&1 \\ 1&0&2&1 \end{pmatrix}\begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&1&1 \\ 0&1&1&0 \end{pmatrix} = \begin{pmatrix} \cdot&\cdot&\cdot&\cdot \\ \cdot&\cdot&\cdot&\cdot \\ \cdot&\cdot&\cdot&\cdot \\ \cdot&\cdot&*&\cdot \end{pmatrix}$$

On s'intéresse au coefficient * dans $M^3$ qui correspond au nombre de chemins allant de 4 à 3 : il s'agit de $(0\,0\,2\,1)\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 3$.

3. On applique l'algorithme de Havel-Hakimi

$(5, 3, 2, 2, 1, 1, 1, 1, 1, 1)$

$\downarrow$

$(2, 1, 1, 0, 0, 1, 1, 1, 1)$

$2$

$(2, 1, 1, 1, 1, 1, 1, 0, 0)$

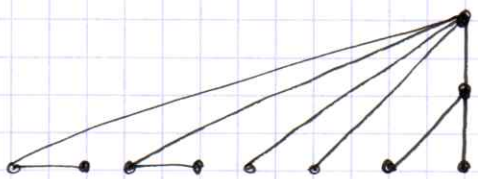
$\downarrow$

$(0, 0, 1, 1, 1, 1, 0, 0)$

$2$

$(1, 1, 1, 1, 0, 0, 0, 0)$ manifestement graphique

On construit un graphe correspondant



3 cont.

$(4, 3, 2, 1, 1, 1, 1, 1, 1, 1)$

$\downarrow$

$(2, 1, 0, 0, 1, 1, 1, 1, 1)$

$\downarrow$ ?

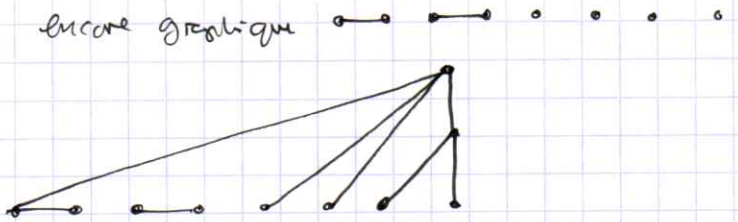
$(3, 1, 1, 1, 1, 1, 1, 0, 0)$

$\downarrow$

$(0, 0, 1, 1, 1, 1, 0, 0)$

$\downarrow$ ?

$(1, 1, 1, 1, 0, 0, 0, 0)$ encore graphique



Graphe correspondant :



Ce graphe n'est pas connexe.

Est-il possible de construire un graphe connexe ?

Pour ça il faut que le nombre d'arêtes soit $\geq n-1 = 9$

Mais $\sum$ degrés $= 2|A|$ et $\sum$ degrés $= 4+3+2+7 = 16$

d'où $|A| = 8$.

Il n'est pas possible de construire un graphe connexe avec la suite de degrés.

4. $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$

(a) $p(0) = 1$, $p(1) = 1$ — pas de facteur linéaire ; $p(x)$ est irréductible.

$K = \mathbb{F}_2[x] / (p(x))$ contient $2^3 = 8$ éléments.

$x^3 + x + 1 = (x+1)(x^2+x+1) + x$

$x^2 + x + 1 = (x+1)x + 1$

$1 = x^2 + x + 1 + (x+1)x = x^2 + x + 1 + (x+1)\left[x^3 + x + 1 + (x+1)(x^2+x+1)\right]$

$= (x+1)(x^3+x+1) + \left[1 + (x+1)^2\right](x^2+x+1)$

$= \underbrace{(x+1)(x^3+x+1)}_{0 \text{ dans } K} + \left[x^2\right](x^2+x+1)$

$x^2$ est l'inverse multiplicatif de $x^2 + x + 1$

vérification $x^2(x^2+x+1) = x^4 + x^3 + x^2 = x(x+1) + x + 1 + x^2 = 1$ ($x^3 = x+1$)

(b) $|K^*| = 7$ nombre premier, puisque l'ordre de $a = \overline{x}$ divise $|K^*|$ et l'ordre de $a$ n'est pas 1, il s'ensuit que $a$ engendre $K^*$ et $p(x)$ est primitif.

(c) On calcule les polynômes minimaux de $a$ et de $a^2$ $(a = \overline{xe})$

Alors $M_1(x) = p(x)$ est le polynôme minimal de $a$ (il est unitaire irréductible)

Par Frobenius :

$p(a^2) = p(a)^2 = 0$, d'où $p(x)$ annule $a^2$ et

$M_2(x) = p(x)$ est aussi le polynôme minimal de $a^2$.

Alors le polynôme générateur $g(x) = ppcm\{M_1(x), M_2(x)\} = p(x)$.

Le code $\mathcal{C} = (g(x)) \lhd \mathbb{F}_2[x]/(x^7+1)$ est engendré par

$\{g(x), xg(x), x^2g(x), x^3g(x)\}$ : il est de dimension 4.

(d) On calcule les syndrômes : $r(x) = 1 + x^2 + x^3 + x^5 + x^6$

$$s_1 = r(a) = 1 + a^2 + a^3 + a^5 + a^6 = a^2$$

$$= 1 + a^2 + a + 1 + a^2 + a + 1 + a^2 + 1$$

$$= a^2$$

$$s_2 = r(a^2) = r(a)^2 \quad \text{(Frobenius)}$$

$$= a^4$$

| | |
|---|---|
| $a$ | $a$ |
| $a^2$ | $a^2$ |
| $a^3$ | $a+1$ |
| $a^4$ | $a^2+a$ |
| $a^5$ | $a^3+a^2 = a^2+a+1$ |
| $a^6$ | $a^3+a^2+a = a^2+1$ |
| $a^7$ | $a^3+a = 1$ |

Equation fondamentale : $s_1\sigma_1 = s_2$

c'est à dire : $a^2\sigma_1 = a^4 \Longrightarrow \sigma_1 = a^2$

Polynôme localisateur d'erreurs : $E(z) = z + \sigma_1 = z + a^2$

Racine $z = a^2$

Erreur $e(x) = x^2$ et $c(x) = r(x) - e(x) = 1 + x^3 + x^5 + x^6$

ce qui correspond au mot $c = (1\,0\,0\,1\,0\,1\,1)$

On remarque que $c(x) = x^6 + x^5 + x^3 + 1 = x^3(x^3+x+1) + x^2(x^3+x+1) + x(x^3+x+1) + x^3 + x + 1$

$= (x^3 + x^2 + x + 1)g(x)$ est bien combinaison de la base.

5. $G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} l_1 \\ l_2 \\ l_3 \end{matrix}$

Le code est $C = \{0, l_1, l_2, l_3, l_1+l_2, l_1+l_3, l_2+l_3, l_1+l_2+l_3\}$

$= \{000000000, 110010101, 001011110, 011110010, 111001011, 101100111,$
$010101100, 100111001\}$

(b) Afin de calculer la matrice de control $H$, on change de base afin d'écrire $G$ sous la forme $\tilde{G} = (I_3 \mid P)$

Puis une matrice de control $\tilde{H}$ par $\tilde{G}$ est $\tilde{H} = (P^t \mid I_6)$

et enfin on revient à la base originale pour trouver $H$ :

$$\tilde{G} = \left(\begin{array}{ccc|cccccc} 1&0&0&0&1&1&1&0&1 \\ 0&1&0&1&1&0&1&1&0 \\ 0&0&1&1&1&1&0&1&0 \end{array}\right)$$

avec l'échange entre $C_3 \leftrightarrow C_4$

$C_6 \leftrightarrow C_2$

où $C_j$ est la colonne $j$

$$\tilde{H} = \left(\begin{array}{ccc|cccccc} 0&1&1&1&0&0&0&0&0 \\ 1&1&1&0&1&0&0&0&0 \\ 1&0&1&0&0&1&0&0&0 \\ 1&1&0&0&0&0&1&0&0 \\ 0&1&1&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&1 \end{array}\right)$$

$$H = \left(\begin{array}{ccc|cccccc} 0&0&1&1&0&1&0&0&0 \\ 1&0&0&1&1&1&0&0&0 \\ 1&1&0&1&0&0&0&0&0 \\ 1&0&0&0&0&1&1&0&0 \\ 0&0&0&1&0&1&0&1&0 \\ 1&0&0&0&0&0&0&0&1 \end{array}\right)$$

(c) La distance minimale est la norme de Hamming (le nombre de 1) la plus petite parmi les mots de $C$ non nuls : $c_{1010100}$

- il s'agit de $d = 4$.

La code est $t$ correcteur par $t < \frac{d}{2} = 2$

c'est à dire $C$ est 1-correcteur.

(d)

| erreurs de poids $\leq 1$ | syndrome (colonnes de $H^t$) |
|---|---|
| 0000000000 | $(0\,0\,0\,0\,0\,0)^t$ |
| 1000000000 | $(0\,1\,1\,1\,0\,1)^t$ |
| 0100000000 | $(0\,0\,1\,0\,0\,0)^t$ |
| 0010000000 | $(1\,0\,0\,0\,0\,0)^t$ |
| 0001000000 | $(1\,1\,1\,0\,1\,0)^t$ |
| 0000100000 | $(0\,1\,0\,0\,0\,0)^t$ |
| 0000010000 | $(1\,1\,0\,1\,1\,0)^t$ |
| 0000001000 | $(0\,0\,0\,1\,0\,0)^t$ |
| 0000000100 | $(0\,0\,0\,0\,1\,0)^t$ |
| 0000000001 | $(0\,0\,0\,0\,0\,1)^t$ |

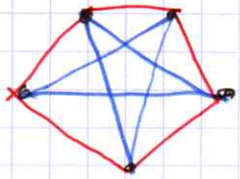
(e) On calcule $Hr_1^t = \begin{pmatrix} 0&0&1&1&0&1&0&0&0 \\ 1&0&0&1&1&1&0&0&0 \\ 1&1&0&1&0&0&0&0&0 \\ 1&0&0&0&0&1&1&0&0 \\ 0&0&0&1&0&1&0&1&0 \\ 1&0&0&0&0&0&0&0&1 \end{pmatrix} \begin{pmatrix} 1\\1\\1\\1\\0\\1\\1\\1\\0 \end{pmatrix} = \begin{pmatrix} 0\\1\\0\\1\\0\\1 \end{pmatrix}$ pas un syndrome donc $r_1$ pas corrigible

$Hr_2^t = \begin{pmatrix} \\ \\ \\ \\ \\ \\ \end{pmatrix} \begin{pmatrix} 1\\0\\1\\0\\0\\1\\1\\0\\1 \end{pmatrix} = \begin{pmatrix} 0\\0\\1\\0\\0\\0 \end{pmatrix}$ il s'agit du syndrome associé à l'erreur $e_2 = 010000000$

on corrige $r_2$ en

$C_2 = r_2 + e_2 = 111001011$

6. (a) La coloration suivante du graphe complet $K_5$ ne contient ni un triangle rouge ni un triangle bleu :



et donc $R(3,3) \geq 6$.

$= (V, A)$

On montre que toute coloration de $K_6$ rouge/bleue contient soit un triangle rouge soit un triangle bleu.

On fixe un sommet $x$ quelconque :

Soit $R_x = \{y \in V : xy \text{ rouge}\}$

$B_x = \{y \in V : xy \text{ bleu}\}$

Puisque $|R_x| + |B_x| = 5$ il faut que soit $|R_x| \geq 3$ soit $|B_x| \geq 3$.

Supposons $|R_x| \geq 3$.

Sans perdre la généralité, on suppose $x = 1$ et que $2, 3, 4 \in R_x$

Donc les arêtes $12, 13, 14$ sont rouges.

Si aucune des arêtes $23, 24, 34$ est rouge on aurait un triangle rouge, par exemple si $23$ rouge, $123$ est un triangle rouge.

D'autre part, si $23, 24, 34$ sont toutes bleues, on aurait un triangle bleue : $234$.

Dans tous les cas, il y a un triangle bleu.

De même si $|B_x| \geq 3$.

(b) Soit $X$ l'ensemble de sommets de $K_{17}$ et soit

$R_x = \{y \in X \mid xy \text{ rouge}\}$

$B_x = \{y \in X \mid xy \text{ bleue}\}$

$V_x = \{y \in X \mid xy \text{ verte}\}$

Alors $|R_x| + |B_x| + |V_x| = 16$ et donc au moins un parmi $|R_x|, |B_x|, |V_x|$ est $\geq 6$.

Supposons $|R_x| \geq 6$.

Sans perdre la généralité $x = 1$, et $2, 3, 4, 5, 6, 7 \in R_x$

Si une des arêtes $ij$ $(i, j \in \{2, 3, 4, 5, 6, 7\}, i \neq j)$ est rouge, alors $1ij$ est un triangle rouge, sinon, le sous-graphe complet engendré par $2, 3, 4, 5, 6, 7$ est colorié avec les deux couleurs bleu et vert.

Par la partie (a), il contient soit un triangle vert soit un triangle bleu.

Dans tous les cas il existe un triangle monochrome.

De même si $|B_x| \geq 6$ ou $|V_x| \geq 6$

//