Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

# ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Examen terminal, le 16 mai 2013, 13h30–16h30

CORRIGE et BAREME

**Question de cours. (4 pts)** Soit $n$ l'ordre $|G|$ de $G$. Pour $d \in \mathbb{N}^\star$, soit $N_d$ le nombre d'éléments de $G$ d'ordre $d$. D'après le Théorème de Cauchy, l'ordre de tout élément de $G$ divise $n$. Il s'ensuit que

$$\sum_{d|n} N_d = n.$$

Montrons que $N_d \leq \varphi(d)$ pour tout diviseur $d$ de $n$. En effet, supposons qu'il existe un élément $\xi \in G$ d'ordre $d$. Les éléments $\xi^0, \ldots, \xi^{d-1}$ sont donc $d$ racines distinctes du polynôme $X^d - 1$ dans $K$. Or, tout polynôme de degré $d$ dans $K[X]$ possède au plus $d$ racines dans $K$. Il s'ensuit que tout élément $\zeta$ de $K$ d'ordre $d$ est de la forme $\xi^i$, avec $i \in \{0, \ldots, d-1\}$. Comme l'ordre de $\zeta$ est égal à l'ordre de $\xi$, les entiers naturels $i$ et $d$ sont premiers entre eux. Par conséquent, $N_d \leq \varphi(d)$, pour tout diviseur $d$ de $n$.

Comme

$$\sum_{d|n} (\varphi(d) - N_d) = \sum_{d|n} \varphi(d) - \sum_{d|n} N_d = n - n = 0$$

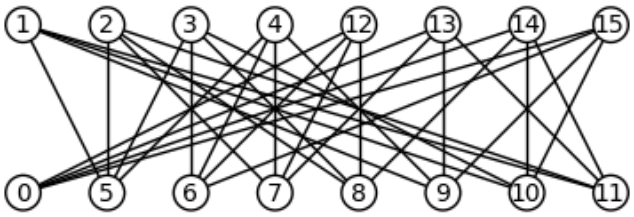
et $\varphi(d) - N_d \geq 0$ pour tout diviseur $d$ de $n$, on a $\varphi(d) - N_d = 0$, pour tout diviseur $d$ de $n$. En particulier, $N_n = \varphi(n) \neq 0$, ce qui veut dire que $G$ contient au moins un élément d'ordre $n$. Un tel élément est un générateur de $G$, et $G$ est donc cyclique.

**Exercice 1. (4 pts)** Notons $G$ le graphe en question. Soit $X$ l'ensemble des sommets de $G$ reliés à 0 par un chemin de longueur paire. Soit $Y$ l'ensemble des sommets de $G$ reliés à 0 par un chemin de longueur impaire. On voit que

$$0, 5, 6, 7, 8, 9, 10, 11 \in X \quad \text{et} \quad 1, 2, 3, 4, 12, 13, 14, 15 \in Y.$$

Dessinons le graphe $G$ en mettant ces deux collections de sommets de part et d'autre (voir le graphe ci-dessous). On constate que $G$ est bien biparti et que

$$X = \{0, 5, 6, 7, 8, 9, 10, 11\} \quad \text{et} \quad Y = \{1, 2, 3, 4, 12, 13, 14, 15\}.$$




**Exercice 2. (4 pts) a. (0,5 pt)** La longueur du code $C$ est la dimension sur $\mathbb{F}_5$ de l'espace vectoriel ambiant $\mathbb{F}_5^5$, i.e., 5.

**b. (0,5 pt)** La dimension du code $C$ est la dimension sur $\mathbb{F}_5$ de $C$ comme espace vectoriel. Remarquons que l'application $\varphi$ est injective car un polynôme non nul de degré $\leq 2$ possède au plus 2 racines. Comme $\varphi$ est injective, $\dim C = \dim \mathbb{F}_5[X]_{\leq 2} = 3$.

**c. (0,5 pt)** Un polynôme non nul de degré $\leq 2$ possède au plus 2 racines. Il s'ensuit que $\varphi(P)$ a au moins 3 coordonnées non nulles, i.e., le poids de Hamming $w(\varphi(P))$ de $\varphi(P)$ satisfait $w(\varphi(P)) \geq 3$, pour tout $P \in \mathbb{F}_5[X]_{\leq 2}$, avec $P \neq 0$. De plus, $w(\varphi(X(X-1))) = 3$. Par conséquent, la distance minimale de $C$ est égale à 3.

**d. (0,5 pt)** $[\frac{1}{2}(d-1)] = 1$ car $d = 3$ d'après le c.

**e. (1 pt)** Prenons la base $1, X, X^2$ de $C$. Son image

$$u = (\bar{1}, \bar{1}, \bar{1}, \bar{1}, \bar{1}),\ v = (\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}),\ w = (\bar{0}, \bar{1}, \bar{4}, -\bar{1}, \bar{1})$$

est une base de $C$. Une matrice génératrice de $C$ est donc

$$G = \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} & \bar{1} & \bar{1} \\ \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{0} & \bar{1} & \bar{4} & \bar{4} & \bar{1} \end{pmatrix}.$$

**f. (1 pt)** Pour déterminer une matrice de parité de $C$, on cherche des équations linéaires portant sur $t = (a, b, c, d, e) \in \mathbb{F}_5^5$ pour que $t \in C$. Supposons que $t \in C$. Il existe donc $x, y, z \in \mathbb{F}_5$ tels que $xu + yv + zw = t$. Cela donne lieu à un système de 5 équations en 3 inconnues qu'on résoud par la

métode de Gauss :

$$\left\{\begin{array}{rcrcrcl} x & & & & & = & a \\ x & + & y & + & z & = & b \\ x & + & \bar{2}y & + & \bar{4}z & = & c \\ x & + & \bar{3}y & + & \bar{4}z & = & d \\ x & + & \bar{4}y & + & z & = & e \end{array}\right. \Leftrightarrow$$

$$\left\{\begin{array}{rcrcrcl} x & & & & & = & a \\ & & y & + & z & = & b-a \\ & & \bar{2}y & + & \bar{4}z & = & c-a \\ & & \bar{3}y & + & \bar{4}z & = & d-a \\ & & \bar{4}y & + & z & = & e-a \end{array}\right. \Leftrightarrow$$

$$\left\{\begin{array}{rcrcrcl} x & & & & & = & a \\ & & y & + & z & = & b-a \\ & & & & \bar{2}z & = & c-\bar{2}b+a \\ & & & & z & = & d-\bar{3}b+\bar{2}a \\ & & & & \bar{2}z & = & e-\bar{4}b+\bar{3}a \end{array}\right. \Leftrightarrow$$

$$\left\{\begin{array}{rcrcrcl} x & & & & & = & a \\ & & y & + & z & = & b-a \\ & & & & z & = & d-\bar{3}b+\bar{2}a \\ & & & & 0 & = & -\bar{2}d+c+\bar{4}b-\bar{3}a \\ & & & & 0 & = & e-\bar{2}d+\bar{2}b-a \end{array}\right.$$

Du coup, il existe $x, y, z \in \mathbb{F}_5$ tels que $xu + yv + zw = t$ si et seulement si

$$\left\{\begin{array}{rcrcrcrcl} -\bar{3}a & + & \bar{4}b & + & c & - & \bar{2}d & = & 0 \\ -a & + & \bar{2}b & & & - & \bar{2}d & + & e & = & 0 \end{array}\right.$$

Cette dernière condition est donc équivalente à la condition $(a, b, c, d, e) \in C$. Autrement dit, la matrice

$$H = \begin{pmatrix} -\bar{3} & \bar{4} & \bar{1} & -\bar{2} & \bar{0} \\ -\bar{1} & \bar{2} & \bar{0} & -\bar{2} & \bar{1} \end{pmatrix}$$

est une matrice de parité pour $C$.

**Exercice 3. (8 pts) a. (0,5 pt)** Si $\mathcal{C}$ est une partition de $[n]$ de cardinal 0, on a $\mathcal{C} = \emptyset$ et $[n] = \bigcup \mathcal{C} = \emptyset$. D'où $S_0([n]) = 0$ lorsque $n \geq 1$. Comme la collection vide est bien une partition de $[0]$, on a bien $S_0([0]) = 1$.

**b. (0,5 pt)** Soit $n \geq 1$. Si $\mathcal{C}$ est une partition de $[n]$ de cardinal 1, alors $\mathcal{C} = \{F\}$ avec $F \neq \emptyset$ et $[n] = \bigcup \mathcal{C} = F$. Comme la collection $\{[n]\}$ est bien une partition de $[n]$ lorsque $n \neq 0$, on a bien $S_1([n]) = 1$ pour $n \geq 1$. Comme l'ensemble vide ne contient aucun sous-ensemble non vide, l'ensemble $[0]$ ne possède aucune partition de cardinal $\geq 1$. Il s'ensuit que $S_1([0]) = 0$.

**c. (1 pt)** Soit $n \geq 1$. Toute partition de $[n]$ en 2 sous-ensembles est de la forme $\{F, F^c\}$, où $F$ est un sous-ensemble propre de $[n]$, i.e., $F \neq \emptyset$ et

$F \neq [n]$. (Rappelons que $F^c$ désigne le complémentaire de $F$ dans $[n]$.) Or, $[n]$ contient $2^n - 2$ sous-ensembles propres. De plus, les partitions $\{F, F^c\}$ et $\{F^c, (F^c)^c\}$ sont égales. Du coup,

$$S_2([n]) = \frac{2^n - 2}{2} = 2^{n-1} - 1.$$

**d. (1 pt)** Soit $\mathcal{C}$ une partition de $[n]$ en $k$ sous-ensembles. De deux choses une : soit $\{n\} \in \mathcal{C}$, soit $\{n\} \notin \mathcal{C}$.

Dans le premier cas, $\mathcal{C} \setminus \{\{n\}\}$ est une partition de $[n-1]$ en $k-1$ sous-ensembles. De plus, cela établit une correspondance entre les partitions de $[n]$ en $k$ sous-ensembles dont l'un est égal à $\{n\}$, d'une part, et les partitions de $[n-1]$ en $k-1$ sous-ensembles. En particulier, le nombre de telles partitions de $[n]$ est $S_{k-1}([n-1])$.

Dans le deuxième cas, la trace $\mathcal{C}'$ de $\mathcal{C}$ sur $[n-1]$ définie par

$$\mathcal{C}' = \{F \cap [n-1] \mid F \in \mathcal{C}\}$$

est une partition de $[n-1]$ en $k$ sous-ensembles. Si on note $\mathcal{C}' = \{F_1, \ldots, F_k\}$, les partitions $\mathcal{C}$ de $[n]$ en $k$ sous-ensembles qui ont trace $\mathcal{C}'$ sur $[n-1]$ sont

$$\{F_1 \cup \{n\}, \ldots, F_k\}, \ldots, \{F_1, \ldots, F_k \cup \{n\}\}.$$

En particulier, le nombre de telles partitions de $[n]$ est égal à $kS_k([n-1])$.

Au final, on a donc bien $S_k([n]) = kS_k([n-1]) + S_{k-1}([n-1])$.

**e. (1 pt)** On calcule

$$D(F_k) = \sum_{n\geq 0} \frac{S_k([n])}{n!} D(X^n) = \sum_{n\geq 1} \frac{S_k([n])}{n!} nX^{n-1} = \sum_{n\geq 1} \frac{S_k([n])}{(n-1)!} X^{n-1} = \sum_{n\geq 1} \frac{kS_k([n-1]) + S_{k-1}([n-1])}{(n-1)!} X^{n-1}$$

d'après le d. Du coup,

$$D(F_k) = \sum_{n\geq 1} \frac{kS_k([n-1])}{(n-1)!} X^{n-1} + \sum_{n\geq 1} \frac{S_{k-1}([n-1])}{(n-1)!} X^{n-1} = k\sum_{n\geq 1} \frac{S_k([n-1])}{(n-1)!} X^{n-1} + F_{k-1} = kF_k + F_{k-1}.$$

**f. (2 pts)** Pour $k \in \mathbb{N}$, soit $G_k$ la série formelle définie par $G_k = \frac{1}{k!}(\exp -1)^k$. On montre par récurrence que $F_k = G_k$ pour tout $k$. D'après le a, $F_0 = 1$. Comme $G_0 = 1$ également, on a bien $F_0 = G_0$.

Supposons que $F_{k-1} = G_{k-1}$ pour $k \geq 1$. Montrons que $F_k = G_k$. Remarquons que l'équation différentielle $DH = kH + F_{k-1}$, portant sur des séries formelles $H$, a au plus une solution avec $H(0) = 0$. Comme $F_k$ en est

une d'après le e et le b, il suffit de montrer que $G_k$ en est une également avec $G_k(0) = 0$. Or, on a bien $G_k(0) = 0$. De plus

$$DG_k = \frac{1}{k!}k(\exp -1)^{k-1}\exp = k\frac{1}{k!}(\exp -1)^{k-1}(\exp -1)+k\frac{1}{k!}(\exp -1)^{k-1} = kG_k + \frac{1}{(k-1)!}(\exp -1)^{k-1} = kG_k + G_{k-1} = kG_k + F_{k-1},$$

d'après l'hypothèse de récurrence. Cela montre bien que $F_k = G_k$.

**g. (2 pts)** D'après le f et la formule du binôme,

$$F_k = \frac{1}{k!}(\exp -1)^k = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\exp(X)^i = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\exp(iX) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\sum_{n\geq 0}\frac{i^n}{n!}X^n = \sum_{n\geq 0}\frac{\frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n}{n!}X^n.$$

Il s'ensuit que

$$S_k([n]) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n.$$