# ÉPREUVE DE MATHÉMATIQUES-INFORMATIQUE

(Epreuve commune aux ENS : Lyon et Cachan - Groupes M, I et MP)

Durée : 3 heures

*L'usage de calculatrices électroniques de poche à alimentation autonome, non imprimantes et sans document d'accompagnement, est autorisé. Cependant, une seule calculatrice à la fois est admise sur la table ou le poste de travail, et aucun échange n'est autorisé entre les candidats.*

## Définitions et notations

L'objet du problème est l'étude d'un algorithme de résolution d'équations diophantiennes linéaires. Les questions peuvent être traitées indépendamment, à condition d'admettre les résultats des questions qui précèdent.

Certaines questions, plus difficiles, sont indiquées par le signe (*) . Bien que leur lecture soit utile à la bonne compréhension du sujet, il est conseillé de ne les aborder qu'en fin de copie.

$\mathcal{M}(m,n)$ désignera l'ensemble des matrices à $m$ lignes et $n$ colonnes dont les coefficients sont dans $\mathbb{Z}$, ensemble des entiers relatifs. $\mathcal{V}(n)$ est l'ensemble des vecteurs à $n$ lignes et à coefficients dans $\mathbb{N}$, ensemble des entiers naturels. $\mathcal{V}(n)$ est donc l'ensemble des matrices de $\mathcal{M}(n,1)$ dont tous les coefficients sont positifs ou nuls. Les matrices et les vecteurs sont partiellement ordonnés suivant l'ordre produit de l'ordre habituel sur les entiers: si $A = (a_{i,j})_{1\leq i\leq m, 1\leq j\leq n} \in \mathcal{M}(m,n)$ et $B = (b_{i,j})_{1\leq i\leq m, 1\leq j\leq n} \in \mathcal{M}(m,n)$,

$$A \leq B \qquad \text{si et seulement si} \qquad \forall 1 \leq i \leq m, \forall 1 \leq j \leq n, a_{i,j} \leq b_{i,j}$$

On appelle *système diophantien linéaire homogène* un système d'équations

$$AX = 0$$

où $A \in \mathcal{M}(m,n)$ est une matrice non nulle. ($X$ est un vecteur de $n$ *inconnues*). Une *solution* d'un tel système est un vecteur $V \in \mathcal{V}(n)$ tel que $AV = 0$. Une solution *minimale* est une solution non nulle $V$ telle que, pour tout autre solution non nulle $W$, $W \leq V \Rightarrow W = V$.

Un sous-ensemble $E$ de $\mathcal{V}(n)$ est dit *stable* si

1. pour tous éléments $v_1, v_2 \in E$, $v_1 + v_2 \in E$
2. pour tous éléments $v_1, v_2 \in E$, si $v_1 \geq v_2$, alors $v_1 - v_2 \in E$

Soit $E$ un sous-ensemble stable de $\mathcal{V}(n)$, un ensemble $E' \subseteq E$ est appelé *système générateur* de $E$ si

$$\forall V \in E, \exists k \in \mathbb{N}, \exists \lambda_1, \ldots, \lambda_k \in \mathbb{N}, \exists V_1, \ldots, V_k \in E',\ V = \sum_{i=1}^{k} \lambda_i V_i$$

Pour $1 \leq i \leq n$, on note $E_i \in \mathcal{V}(n)$ le vecteur dont les composantes sont toutes nulles, sauf la $i$ème qui vaut 1.

Si $V = (v_i)_{1\leq i\leq n}, W = (w_i)_{1\leq i\leq n}$ sont des vecteurs de $\mathcal{V}(n)$, $V \cdot W$ désigne leur *produit scalaire* $\sum_{i=1}^{n} v_i w_i$. La *norme* d'un vecteur $V \in \mathcal{V}(n)$ est définie par $\|V\| = \sqrt{V \cdot V}$. Ces opérations sont définies de manière identique sur les vecteurs de $\mathbb{R}^n$ et $\mathbb{Q}^n$.

Dans tout le problème, on se fixe une matrice $A \in \mathcal{M}(m,n)$.

## Partie 1. Préliminaires

Soit $S$ l'ensemble des solutions du système homogène $AX = 0$.

**Question 1.1.** *Montrer que $S$ est stable.*

**Question 1.2.** *Soit $M$ l'ensemble des solutions minimales du système homogène $AX = 0$. Montrer que $M$ est un système générateur de $S$.*

**Question 1.3.** *(*) Si $E$ est un sous-ensemble de $\mathcal{V}(n)$, montrer que l'ensemble des éléments minimaux de $E$ pour $\geq$ est fini (on pourra raisonner par récurrence sur $n$). En déduire que $S$ admet un système générateur fini.*

Cette question montre l'existence d'un ensemble fini de générateurs de $S$ sans donner explicitement une manière de le construire. L'objet de tout ce problème est de donner une preuve constructive de ce résultat en étudiant un algorithme qui calcule explicitement le système de générateurs.

**Question 1.4.** *Donner explicitement ce système générateur dans le cas où $A = (2; -1)$.*

## Partie 2. Un algorithme de résolution des systèmes homogènes

Soit $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n} \in \mathcal{M}(m, n)$. On considère l'algorithme suivant (que nous appelerons $\mathcal{A}$ dans la suite) qui construit deux ensembles de vecteurs $\mathcal{E}$ et $\mathcal{F}$ et dépend d'une fonction **Choisir** non précisée pour l'instant.

$\mathcal{E} = \emptyset$ et $\mathcal{F} = \{E_1, \ldots, E_n\}$ {Initialisation}
Tant que $\mathcal{F} \neq \emptyset$ Faire
début
**Choisir** $T \in \mathcal{F}$ et le retirer de $\mathcal{F}$
S'il existe $U \in \mathcal{E} \cup \mathcal{F}$ tel que $U \leq T$,
Alors ne rien faire
Sinon
Si $AT = 0$ alors ajouter $T$ à $\mathcal{E}$ {$T$ est une solution}
Sinon ajouter à $\mathcal{F}$ l'ensemble $\{T + E_i \mid 1 \leq i \leq n, (AT) \cdot (AE_i) < 0\}$
{ Retour vers l'origine}
fin

On note $\mathcal{E}_k$ et $\mathcal{F}_k$ les valeurs de $\mathcal{E}$ et $\mathcal{F}$ respectivement après $k$ passages dans la boucle.

**Question 2.1.** *Exécuter l'algorithme pas à pas dans le cas où $A = (3, -2, -1)$. (On précisera la fonction* **Choisir** *utilisée. Le nombre d'étapes de calcul dépend de celle-ci. A titre indicatif il peut y avoir 16 étapes de calcul).*

**Question 2.2.** *Montrer que, pour tous $k, k'$ tels que $k > k'$, si $V \in \mathcal{F}_k$, alors il existe $W \in \mathcal{F}_{k'}$, $W \leq V$.*

**Question 2.3.** *Montrer que $\mathcal{A}$ est correct, c'est à dire que, pour tout $k$, pour tout $V \in \mathcal{E}_k$, $V$ est une solution de $AX = 0$.*

Pour $k \geq 0$, on dira que $V$ *est sélectionné à l'étape* $k$ si $V \in \mathcal{F}_k$,$V \notin \mathcal{F}_{k+1}$ et $\forall U \in \mathcal{F}_k \cup \mathcal{E}_k$, $U \neq V \Rightarrow U \not\leq V$.

**Question 2.4.** *Montrer que, pour $p \geq 1$, si $V \in \mathcal{F}_{k+p}$ et $W$ est sélectionné à $k$, alors $W \not\geq V$.*

**Question 2.5.**

1. (*) *Montrer que, si $V$ est une solution non nulle de $AX = 0$, alors, pour tout $k$, il existe un vecteur $W \in \mathcal{E}_k \cup \mathcal{F}_k$ tel que $V \geq W$.*
2. *En déduire que, si $W$ est sélectionné à $k$, alors, pour toute solution non nulle $V$ de $AX = 0$ telle que $V$ est distinct de $W$, $W \not\geq V$.*
3. *Montrer que, pour tout $k$, tout vecteur de $\mathcal{E}_k$ est une solution minimale de $AX = 0$.*

La fonction **Choisir** est *équitable* si elle ne repousse pas indéfiniment le choix d'un vecteur de $\mathcal{F}$, c'est-à-dire si, pour tout $k$ et pour tout vecteur $V$ de $\mathcal{F}_k$, il existe un $k' > k$ tel que $V \notin \mathcal{F}_{k'}$.

**Question 2.6.** *Montrer que, si* **Choisir** *est équitable, alors l'algorithme est complet, c'est-à dire que, pour toute solution minimale $V$ de $AX = 0$, il existe un entier $k$ tel que $V \in \mathcal{E}_k$.*

## Partie 3. Terminaison de l'algorithme

**Question 3.1.** *Dans cette question (et cette question seulement) on suppose que $m = 1$.*

1. *Montrer que, pour tout $V \in \mathcal{F}_k$, $\|AV\|$ reste borné par un nombre qui ne dépend pas de $k$, mais seulement des coefficients de $A$. (Indication: on pourra considérer le coefficient de $A$ dont la valeur absolue est maximale).*
2. *En déduire que l'algorithme se termine. (Indication: on pourra utiliser les questions 3 de la partie 1 et 5 de la partie 2.)*

L'objet des deux questions qui suivent est de montrer la terminaison de l'algorithme pour $m$ quelconque. Pour cela, on raisonne par l'absurde et on suppose dans ces deux questions que l'algorithme ne se termine pas.

Si $V \in \mathcal{V}(n)$, $S(V)$ désigne l'ensemble $\{V + E_i \mid (AV) \cdot (AE_i) < 0\}$ s'il existe un $k$ tel que $V$ est sélectionné à l'étape $k$ et $S(V)$ est l'ensemble vide sinon. $S$ est étendu aux ensembles par $S(\mathcal{E}) = \bigcup_{V \in \mathcal{E}} S(V)$. On définit aussi $S^k(\mathcal{E})$ par récurrence sur $k$: $S^0(\mathcal{E}) = \mathcal{E}$ et $S^{k+1}(\mathcal{E}) = S(S^k(\mathcal{E}))$.
Enfin, on note $S^*(\mathcal{E}) = \bigcup_{k \geq 0} S^k(\mathcal{E})$

**Question 3.2.** *Montrer l'existence d'une suite infinie $(V_i)_{i \in \mathbb{N}}$ telle que*

- $V_0 \in \{E_1, \ldots, E_n\}$
- *pour tout $i$, il existe un $k_i$ tel que $V_i$ est sélectionné à l'étape $k_i$*

– *pour tout $i$, il existe $j_i \in \{1, \ldots, n\}$ tel que $V_{i+1} = V_i + E_{j_i}$*

*Pour cela, on pourra construire $(V_i)_{i\in\mathbb{N}}$ par récurrence en conservant la propriété que $S^*(V_i)$ est infini.*

**Question 3.3.** *Soit une suite $(V_i)_{i\in\mathbb{N}}$ construite comme à la question précédente.*

1. *Montrer que*
$$\lim_{i\to+\infty} \frac{\|AV_i\|}{i} = 0$$
2. *Soit $U_i = \frac{V_i}{i}$. Montrer qu'il existe une sous-suite $U_{i_j}$ qui converge vers un vecteur $l$ non nul de $\mathbb{R}^n$ tel que $Al = 0$ et dont toutes les composantes sont positives ou nulles.*
3. *(*) Montrer qu'il existe un vecteur non nul $l' \in \mathbb{Q}^n$, dont toutes les composantes sont positives ou nulles et tel que $Al' = 0$ et $\|l - l'\| < 1$.*
4. *En déduire l'existence d'une solution non nulle $l'' \in \mathcal{V}(n)$ telle que $\exists j_0, \forall j > j_0, V_{i_j} > l''$. En conclure une contradiction et donc la terminaison de l'algorithme.*

**Question 3.4.**

*Certains calculs de l'algorithme sont redondants. Proposer une modification de l'algorithme (qui reste correcte complète et termine) telle que, pour tous $k \neq k'$*

$$(\mathcal{F}_{k+1} \setminus \mathcal{F}_k) \cap (\mathcal{F}_{k'+1} \setminus \mathcal{F}_{k'}) = \emptyset$$

*Appliquer ce nouvel algorithme sur l'exemple suivant (15 étapes de calcul):*

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$