Exercice - 72 - **ENS ULC** 2011 - 2015

On considère une $A \in \mathfrak{M}_{n,p}(\mathbb{Z})$ où $p > n$.

On s'intéresse au système linéaire diophantien : $AX = 0_{\mathfrak{M}_{n,1}(\mathbb{Z})}$.

1 Calculer, en fonction de A, un $R > 0$ tel que l'on soit certain de trouver une solution non-triviale : X telle que $\|X\|_\infty \leqslant R$.

2 Vous pourriez finalement montrer que le nombre

$$R \overset{\text{déf}}{=} (p\|A\|_\infty)^{\frac{n}{p-n}}$$

convient !

Solution.
Soit $R \in \mathbb{N}^*$.
On pose $A \overset{\text{déf}}{=} (a_{i,j})_{1\leqslant i\leqslant n,\, 1\leqslant j\leqslant p}$

On veut pouvoir assurer l'existence d'une solution (non triviale) dans la boule $B_{\|.\|_\infty}(0, R)$.

— *Méthode 1 :*
On pose [1]

$$\phi \overset{\text{déf}}{=} \mathbb{Z}^p \to \mathbb{Z}^n,\ X \mapsto AX$$

— $\phi_{|[\![-R,R]\!]^p}$ est à valeurs dans $[\![-pR\|A\|_\infty, pR\|A\|_\infty]\!]^n$:
En effet : Pour tout $X \overset{\text{déf}}{=} (x_1, \cdots, x_p) \in [\![-R, R]\!]^p$,

$$\forall i \in [\![1, n]\!],\ |[AX]_i| = \left|\sum_{k=1}^{p} a_{ik}x_k\right| \leqslant \sum_{k=1}^{p} |a_{ik}x_k| \leqslant \|A\|_\infty \sum_{k=1}^{p} |x_k| \leqslant \|A\|_\infty pR$$

Une condition suffisante de non injectivité de $\phi_{|[\![-R,R]\!]^p}$ corestreinte à $[\![-pR\|A\|_\infty, pR\|A\|_\infty]\!]^n$ est que le cardinal d'une partie de l'ensemble de départ soit strictement supérieur au cardinal de l'ensemble d'arrivée, soit :

— **Approche 1** [2] **:**

$$(2R)^p > (2Rp\|A\|_\infty + 1)^n$$

ce qui sera a fortiori [3] le cas si :

$$(2R)^p > (2Rp\|A\|_\infty + 2R)^n$$

i.e :

$$R > \frac{1}{2}(p\|A\|_\infty + 1)^{\frac{n}{p-n}}$$

— **Approche 2** [4] (pour retomber sur le rayon de l'énoncé) :

$$(2R + 1)^p > (2Rp\|A\|_\infty + 1)^n$$

ce qui sera a fortiori le cas si [5] :

$$(2R + 1)^p > ((2R + 1)p\|A\|_\infty)^n$$

1. on confondra, à partir de maintenant, $\mathfrak{M}_{p,1}(\mathbb{Z})$ (resp. $\mathfrak{M}_{n,1}(\mathbb{Z})$) et $\mathbb{Z}^p$ (resp $\mathbb{Z}^n$), par commodité d'écriture
2. la partie en question est $([\![-R, R]\!]\backslash\{0\})^p$, de cardinal $(2R)^p$
3. car $R \geqslant 1$
4. la partie est l'ensemble de départ entier, de cardinal $(2R + 1)^p$
5. On peut loisiblement supposer que $p\|A\|_\infty \geqslant 1$, sinon A est identiquement nulle, et n'importe quel rayon entier strictement positif conviendra.

i.e :

$$2\mathrm{R}+1 > (p\|\mathrm{A}\|_\infty)^{\frac{n}{p-n}}$$

i.e :

$$\mathrm{R} > \frac{1}{2}(p\|\mathrm{A}\|_\infty)^{\frac{n}{p-n}} - \frac{1}{2}$$

et enfin [6] :

$$\mathrm{R} \geqslant \frac{1}{2}(p\|\mathrm{A}\|_\infty)^{\frac{n}{p-n}}$$

Ladite non injectivité permet de conclure, puisqu'elle assure l'existence de deux vecteurs $\mathrm{X}, \mathrm{Y} \in [\![-\mathrm{R}, \mathrm{R}]\!]^p$ distincts tels que $\mathrm{AX} = \mathrm{AY}$.
En posant $\mathrm{Z} \overset{\text{déf}}{=} \mathrm{X} - \mathrm{Y} \neq 0$, $\mathrm{AZ} = 0$ et $\mathrm{Z} \in [\![-\mathrm{R}, \mathrm{R}]\!]^p$.

— *Méthode 2 (M.Guelfi) :*
Pour tout $\mathrm{X} \overset{\text{déf}}{=} (x_1, \cdots, x_p) \in [\![-\mathrm{R}, \mathrm{R}]\!]^p$,

$$\forall i \in [\![1, n]\!],\ -\mathrm{R}\sum_{k=1}^{p} a_{ik}^- \leqslant [\mathrm{AX}]_i = \sum_{k=1}^{p} a_{ik}x_k \leqslant \mathrm{R}\sum_{k=1}^{p} a_{ik}^+$$

Donc pour tout $i \in [\![1, n]\!]$, $[\mathrm{AX}]_i \in [\![-\mathrm{R}\sum_{k=1}^{p} a_{ik}^-, \mathrm{R}\sum_{k=1}^{p} a_{ik}^+]\!]$, d'où :

$$\mathrm{AX} \in \prod_{i=1}^{n} [\![-\mathrm{R}\sum_{k=1}^{p} a_{ik}^-,\ \mathrm{R}\sum_{k=1}^{p} a_{ik}^+]\!]$$

peut prendre

$$\mathrm{card}\left(\prod_{i=1}^{n} [\![-\mathrm{R}\sum_{k=1}^{p} a_{ik}^-,\ \mathrm{R}\sum_{k=1}^{p} a_{ik}^+]\!]\right) = \prod_{i=1}^{n}\left(\mathrm{R}\sum_{k=1}^{p} a_{ik}^- + \mathrm{R}\sum_{k=1}^{p} a_{ik}^+ + 1\right) = \prod_{i=1}^{n}\Big(\mathrm{R}\underbrace{\sum_{k=1}^{p}|a_{ik}|}_{\text{noté } \Lambda_i} + 1\Big)$$

valeurs possibles.
Donc la fonction

$$[\![-\mathrm{R}, \mathrm{R}]\!]^p \to \mathbb{Z}^n,\ \mathrm{X} \mapsto \mathrm{AX}$$

peut être corestreinte à un ensemble de cardinal $\prod_{i=1}^{n}(\mathrm{R}\Lambda_i + 1)$

De la même manière que précédemment, une condition suffisante de non injectivité de cette fonction corestreinte est que le cardinal d'une partie [7] de l'ensemble de départ soit strictement supérieur au cardinal de l'ensemble d'arrivée, i.e :

$$\prod_{i=1}^{n}(\mathrm{R}\Lambda_i + 1) < (\mathrm{R}+1)^p \qquad \circledast$$

— **Approche 1** (pour retomber sur le rayon de l'énoncé) :
Or :

$$\prod_{i=1}^{n}(\mathrm{R}\Lambda_i + 1) \leqslant \prod_{i=1}^{n}(\mathrm{R}p\|\mathrm{A}\|_\infty + 1) \leqslant \prod_{i=1}^{n}((\mathrm{R}+1)p\|\mathrm{A}\|_\infty) \leqslant ((\mathrm{R}+1)p\|\mathrm{A}\|_\infty)^n$$

donc avoir $((\mathrm{R}+1)p\|\mathrm{A}\|_\infty)^n < (\mathrm{R}+1)^p$, i.e : $\mathrm{R} > (p\|\mathrm{A}\|_\infty)^{\frac{n}{p-n}} - 1$, suffit [8].

6. car R est entier
7. $[\![0, \mathrm{R}]\!]^p$, cette fois
8. à assurer, via $\circledast$, la non injectivité de la fonction précédemment posée.

— **Approche 2** (pour faire mieux que le rayon de l'énoncé) :
Or :

$$\prod_{i=1}^{n}(\mathrm{R}\Lambda_i+1)\leqslant\prod_{i=1}^{n}(\mathrm{R}\Lambda_i+\Lambda_i)\leqslant(\mathrm{R}+1)\prod_{i=1}^{n}\Lambda_i$$

donc avoir $(\mathrm{R}+1)\prod_{i=1}^{n}\Lambda_i<(\mathrm{R}+1)^p$, i.e : $\mathrm{R}>\left(\prod_{i=1}^{n}\Lambda_i\right)^{\frac{1}{p-1}}-1$, suffit.

On conclut de la même manière que dans la *Méthode 1*.

Sur l'existence de solutions non triviales

Remarquons que la dimension, dans[a] $\mathfrak{M}_{p,1}(\mathbb{R})$, de l'espace des solutions est celle de l'intersection de n hyperplans, soit $p-n>0$.
Il y a donc nécessairement des solutions non triviales dans $\mathfrak{M}_{p,1}(\mathbb{R})$. Mais ces considérations d'algèbre linéaire ne permettent pas de rendre compte de la situation "arithmétique" dans laquelle on se trouve.

a. on "plonge" $\mathbb{Z}$ dans le corps $\mathbb{R}$, qui nous permet de profiter de l'algèbre linéaire.

□