Théorèmes de transfert

1 Dualité

Théorème 1 *Soit $A \in M_{n,m}(\mathbb{R})$. Pour chaque $P \in \mathbb{Z}^n$ et $Q \in \mathbb{Z}^m \backslash \{0\}$ tel que $\|AQ+P\|_\infty \leq 1$, il existe $P^* \in \mathbb{Z}^m$ et $Q^* \in \mathbb{Z}^n \backslash \{0\}$ tels que*

$$\begin{aligned} \|Q^*\|_\infty &\leq C \|Q\|_\infty^{\frac{m}{n+m-1}} \|AQ+P\|_\infty^{\frac{1-m}{n+m-1}} \\ \left\| {}^tAQ^* - P^* \right\|_\infty &\leq C \|Q\|_\infty^{\frac{1-n}{n+m-1}} \|AQ+P\|_\infty^{\frac{n}{n+m-1}} \end{aligned}$$

et

$$\|Q^*\|_\infty^n \left\| {}^tAQ^* - P^* \right\|_\infty^m \leq C \left(\|Q\|_\infty^m \| AQ+P\|_\infty^n\right)^{\frac{1}{n+m-1}}$$

où la constante C ne dépend que de n et m.

Démonstration. Soit $A \in M_{n,m}(\mathbb{R})$. Pour chaque $t > 0$, considérons le réseau Λ_t de $\mathbb{R}^{n+m}$ dont une base est donnée par les vecteurs colonnes de la matrice

$$\begin{pmatrix} t^m Id_n & 0 \\ 0 & t^{-n} Id_m \end{pmatrix} \begin{pmatrix} Id_n & A \\ 0 & Id_m \end{pmatrix} = \begin{pmatrix} t^m Id_n & t^m A \\ 0 & t^{-n} Id_m \end{pmatrix}.$$

Dans la suite nous noterons un réseau par la matrice dont les vecteurs colonnes forment une base de ce réseau. Le déterminant de Λ_t est 1. Les éléments de Λ_t sont les vecteurs de la forme

$$\begin{pmatrix} t^m Id_n & t^m A \\ 0 & t^{-n} Id_m \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} t^m(X+AY) \\ t^{-n} Y \end{pmatrix}$$

où $X \in \mathbb{Z}^n$ et $Y \in \mathbb{Z}^m$. Cherchons le réseau Λ_t^* dual du réseau Λ_t. Sa matrice est donnée par

$$\Lambda_t^* = {}^t\Lambda_t^{-1} = \begin{pmatrix} t^{-m} Id_n & 0 \\ -t^n\, {}^tA & t^n Id_m \end{pmatrix}.$$

Soit $P \in \mathbb{Z}^n$ et $Q \in \mathbb{Z}^m$. Posons $\alpha = \|Q\|_\infty^m \|AQ+P\|_\infty^n$ et choisissons t minimisant la norme du vecteur $\Lambda_t \begin{pmatrix} P \\ Q \end{pmatrix}$ on obtient $t^m \|AQ+P\|_\infty = t^{-n} \|Q\|_\infty$ i.e. $t = \left(\frac{\|Q\|}{\|AQ+P\|}\right)^{\frac{1}{n+m}}$. Pour la norme $\|.\|_\infty$, nous avons $\lambda_1(\Lambda_t) \leq t^m \|AQ+P\|_\infty = t^{-n} \|Q\|_\infty$. Comme la norme max est équivalente à la norme euclidienne nous avons d'après le théorème de Malher sur le réseau dual,

$$\lambda_{n+m}^* \geq c_1 (t^m \|AQ+P\|_\infty)^{-1} = c_1 (t^{-n} \|Q\|_\infty)^{-1}$$

où c_1 est une constante strictement positive qui ne dépend que de m et n. D'après le théorème des minima de Minkowski on a

$$(\lambda_1^*)^{n+m-1} \lambda_{n+m}^* \leq c_2 \det \Lambda_t^* = c_2$$

où c_2 ne dépend que de $m+n$. Par conséquent

$$\lambda_1^* \leq c_3 (t^m \|AQ+P\|_\infty)^{\frac{1}{n+m-1}}$$

et il existe $(P^*, Q^*) \in \mathbb{Z}^m \times \mathbb{Z}^n$ différent du couple nul tel que la norme max de

$$\Lambda_t^* \begin{pmatrix} Q^* \\ P^* \end{pmatrix} = \begin{pmatrix} t^{-m} Id_n & 0 \\ -t^n\, {}^tA & t^n Id_m \end{pmatrix} \begin{pmatrix} Q^* \\ P^* \end{pmatrix} = \begin{pmatrix} t^{-m} Q^* \\ t^n (P^* - {}^tAQ^*) \end{pmatrix}$$

soit plus petite que $c_3 (t^m \|AQ + P\|_\infty)^{\frac{1}{n+m-1}}$. Nous obtenons donc

$$\begin{cases} \|Q^*\|_\infty \leq c_3 t^m (t^m \|AQ + P\|_\infty)^{\frac{1}{n+m-1}} \\ \|P^* - {}^tAQ^*\|_\infty \leq c_3 t^{-n} (t^m \|AQ + P\|_\infty)^{\frac{1}{n+m-1}} =\leq c_3 t^{-n} (t^{-n} \|Q\|_\infty)^{\frac{1}{n+m-1}} \end{cases}.$$

Posons $r = \|AQ + P\|_\infty$ et $q = \|Q\|_\infty$. Comme $t = \left(\frac{q}{r}\right)^{\frac{1}{n+m}}$, on obtient

$$\begin{aligned} \|Q^*\|_\infty &\leq c_3 \left(\frac{q}{r}\right)^{\frac{m}{n+m}} \left(\left(\frac{q}{r}\right)^{\frac{m}{n+m}} r \right)^{\frac{1}{n+m-1}} = c_3 q^{\frac{m}{n+m}(1+\frac{1}{n+m-1})} r^{-\frac{m}{n+m}(1+\frac{1}{n+m-1})+\frac{1}{n+m-1}} \\ &= c_3 q^{\frac{m}{n+m-1}} r^{\frac{1-m}{n+m-1}} \end{aligned}$$

et

$$\begin{aligned} \left\|P^* - {}^tAQ^*\right\|_\infty &\leq c_3 \left(\frac{q}{r}\right)^{\frac{-n}{n+m}} \left(\left(\frac{q}{r}\right)^{\frac{-n}{n+m}} q \right)^{\frac{1}{n+m-1}} = c_3 \,(q)^{\frac{-n}{n+m}(1+\frac{1}{n+m-1})+\frac{1}{n+m-1}} \,(r)^{\frac{n}{n+m}(1+\frac{1}{n+m-1})} \\ &= c_3 q^{\frac{1-n}{n+m-1}} r^{\frac{n}{n+m-1}}. \end{aligned}$$

Si $Q^* = 0$ on peut prendre $Q^{*'} = (1, 0, ..., 0)$ et $P^{*'}$ tel que $\left\|P^{*'} - {}^tAQ^{*'}\right\|_\infty \leq 1$. On a alors

$$\left\|Q^{*'}\right\|_\infty \leq 1 \leq c_3 q^{\frac{m}{n+m-1}} r^{\frac{1-m}{n+m-1}}$$

car $r \leq 1$ et $q \geq 1$ (c_3 peut être choisie ≥ 1) et

$$\left\|P^{*'} - {}^tAQ^{*'}\right\|_\infty \leq 1 \leq \|P^*\|_\infty$$

et la conclusion du théorème est valable. Finalement, on voit que

$$\|Q^*\|_\infty^n \left\|P^* - {}^tAQ^*\right\|_\infty^m \leq c_3^2 q^{\frac{mn+m(1-n)}{n+m-1}} r^{\frac{n(1-m)+mn}{m+n-1}} = c_4 \,(q^m r^n)^{\frac{1}{n+m-1}}. \square$$

Corollaire 1 *Soit $A \in M_{n,m}(\mathbb{R})$. La matrice A est mal approchable ssi sa transposée ${}^tA$ est mal approchable.*

Démonstration. L'inégalité

$$\|Q^*\|_\infty^n \left\| {}^tAQ^* - P^* \right\|_\infty^m \leq C \left(\|Q\|_\infty^m \left\| {}^tAQ - P \right\|_\infty^n \right)^{\frac{1}{n+m-1}}$$

montre que si A n'est pas mal approchable alors la transposée de A ne l'est pas non plus. $\square$

Corollaire 2 *Soit K un sous corps de $\mathbb{R}$ de dimension $m+1$ sur $\mathbb{Q}$. Si $1, \alpha_1, ..., \alpha_m$ est une base de K sur $\mathbb{Q}$ alors la forme linéaire (la matrice ligne) $\theta = (\alpha_1, ..., \alpha_n)$ est mal approchable.*

2 Transfert entre les approximations homogènes et les approximations non homogènes

Théorème 2 *Soit $A \in M_{n,m}(\mathbb{R})$, $R > 0$ et $\alpha > 0$ tels que pour tout $Q \in \mathbb{Z}^m \backslash \{0\}$ on ait*

$$\|Q\|_\infty \leq R \Rightarrow \forall P \in \mathbb{Z}^n,\ \|AQ+P\|_\infty \geq \alpha R^{-\frac{m}{n}}.$$

Alors pour tout $X \in \mathbb{R}^n$ il existe $Q \in \mathbb{Z}^m$ et $P \in \mathbb{Z}^n$ tels que

$$\|AQ+P-X\|_\infty \leq C\alpha^{\frac{n(1-n)}{n+m}} \times R^{-\frac{m}{n}} \text{ et } \|Q\|_\infty \leq \alpha^{-n}R$$

où C est une constante qui ne dépend que de m et n.

Démonstration. Soit $A \in M_{n,m}(\mathbb{R})$, R et α vérifiant les hypothèses du théorème. Pour chaque $t > 0$, considérons le réseau Λ_t defini par la matrice

$$\Lambda_t = \begin{pmatrix} t^m Id_n & t^m A \\ 0 & t^{-n} Id_m \end{pmatrix}.$$

Cherchons t maximisant $\lambda_1(\Lambda_t)$ sachant que $\|Q\|_\infty \leq R \Rightarrow \forall P \in \mathbb{Z}^n,\ \|AQ+P\|_\infty \geq \alpha R^{-\frac{m}{n}}$. Il suffit de choisir t tel que $t^{-n}R = t^m \alpha R^{-\frac{m}{n}}$ on obtient $t = \alpha^{\frac{-1}{n+m}} R^{\frac{1}{n+m}(1+\frac{m}{n})} = \alpha^{\frac{-1}{n+m}} R^{\frac{1}{n}}$. Pour cette valeur de t on a pour tout $Q \neq 0$

$$\left\|\Lambda_t \begin{pmatrix} P \\ Q \end{pmatrix}\right\|_\infty = \left\|\begin{pmatrix} t^m(AQ+P) \\ t^{-n}Q \end{pmatrix}\right\|_\infty \geq \begin{cases} \|t^m(AQ+P)\|_\infty \geq t^m \alpha R^{-\frac{m}{n}} \text{ si } \|Q\|_\infty \leq R \\ \|t^{-n}Q\|_\infty \geq t^{-n}R \text{ si } \|Q\|_\infty \geq R \end{cases}$$

et pour $Q = 0$ et $P \neq 0$

$$\left\|\Lambda_t \begin{pmatrix} P \\ 0 \end{pmatrix}\right\|_\infty = \left\|\begin{pmatrix} t^m P \\ 0 \end{pmatrix}\right\|_\infty \geq t^m \geq t^m \alpha R^{-\frac{m}{n}}$$

car $\alpha R^{-\frac{m}{n}} \leq 1$ (en effet, $\forall Q,\ \exists P,\ \|AQ+P\|_\infty \leq 1$). On en déduit que

$$\lambda_1(\Lambda_t) \geq t^{-n}\alpha R^{-\frac{m}{n}} = t^{-n}R.$$

D'après le théorème des minima on a

$$\begin{aligned} \lambda_{n+m}(\Lambda_t) &\leq C\lambda_1(\Lambda_t)^{-(n+m-1)} = C_1 \left((\alpha^{\frac{-1}{n+m}} R^{\frac{1}{n}})^{-n} R\right)^{1-(n+m)} \\ &= C_1 \alpha^{\frac{n(1-n-m)}{n+m}}. \end{aligned}$$

Pour tout X de $\mathbb{R}^{n+m}$ il existe $Y \in \Lambda_t$ tel que $d(X,Y) \leq \lambda_1 + ... + \lambda_{n+m} \leq C_2 \lambda_{n+m}$. Par conséquent pour tout $X \in \mathbb{R}^n$ il existe $(P,Q) \in \mathbb{Z}^n \times \mathbb{Z}^m$ tel que

$$\left\|\Lambda_t \begin{pmatrix} P \\ Q \end{pmatrix} - \begin{pmatrix} t^m X \\ 0 \end{pmatrix}\right\|_\infty \leq C_2 \lambda_{n+m} \leq C_3 \alpha^{\frac{n(1-n-m)}{n+m}}$$

d'où

$$\|Q\|_\infty \leq C_3 \alpha^{\frac{n(1-n-m)}{n+m}} t^n = C_3 \alpha^{\frac{n(1-n-m)}{n+m}} (\alpha^{\frac{-1}{n+m}} R^{\frac{1}{n}})^n = \alpha^{-n}R$$

et

$$\|AQ+P-X\|_\infty \leq C_3 t^{-m} \alpha^{\frac{n(1-n-m)}{n+m}} = C_3 \alpha^{\frac{n(1-n-m)}{n+m}} (\alpha^{\frac{-1}{n+m}} R^{\frac{1}{n}})^{-m} = C_3 \alpha^{\frac{n(1-n)}{n+m}} R^{-\frac{m}{n}}. \square$$

"**Réciproque" :**

Théorème 3 *Soit $A \in M_{n,m}(\mathbb{R})$, $R > 0$ et $\varepsilon > 0$. Supposons que pour tout $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{R}^n$ il existe $Q = (q_1, ..., q_m) \in \mathbb{Z}^m$ et $P \in \mathbb{Z}^n$ tels que*

$$\|Q\|_\infty \leq R \text{ et } \|AQ + P - \alpha\|_\infty < \varepsilon.$$

Alors il n'existe pas d'éléments $Q^* \in \mathbb{Z}^n$ et $P^* \in \mathbb{Z}^m$ tels que

$$\|Q^*\|_\infty \leq R^* \text{ et } \left\| {}^tAQ^* + P^* \right\| \leq \varepsilon^*$$

avec $R^* = (4n\varepsilon)^{-1}$ et $\varepsilon^* = (4mR)^{-1}$.

Démonstration. Supposons que Q^* et P^* existent. Choisissons un $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{R}^n$ tels que ${}^tQ^*\alpha = \frac{1}{2}$. Alors il existent $P \in \mathbb{Z}^n$ et $Q \in \mathbb{Z}^m$ tel que

$$\begin{aligned}
\frac{1}{2} &= \left\|{}^tQ^*\alpha\right\| = \left\|{}^tQ^*(\alpha - (AQ+P) + (AQ+P))\right\| \\
&\leq \left\|{}^tQ^*(\alpha - (AQ+P))\right\| + \left\|{}^tQ^*(AQ+P))\right\| \\
&= \left\|{}^tQ^*(\alpha - (AQ+P))\right\| + \left\|({}^tQ^*A + {}^tP^*)Q\right\| \\
&< n \left\| {}^tQ^* \right\|_\infty \|\alpha - AQ - P\|_\infty + m \left\| {}^tAQ^* + P^* \right\|_\infty \|Q\|_\infty \leq \frac{1}{4} + \frac{1}{4}. \square
\end{aligned}$$

Théorème 4 *Soit $A \in M_{n,m}(\mathbb{R})$. Les quatres propositions suivantes sont équivalentes*
1. *A est mal approchable.*
2. *${}^tA$ est mal approchable.*
3. *Il existe une constante $C_1 \geq 0$ telle que $\forall \alpha \in \mathbb{R}^n$, $\forall R > 0$, $\exists Q \in \mathbb{Z}^m$, $\exists P \in \mathbb{Z}^n$,*

$$\|Q\|_\infty \leq R \text{ et } \|AQ + P - \alpha\|_\infty \leq C_1 R^{-\frac{m}{n}}.$$

4. *Il existe une constante $C_2 \geq 0$ telle que $\forall \beta \in \mathbb{R}^m$, $\forall R > 0$, $\exists Q^* \in \mathbb{Z}^n$, $\exists P^* \in \mathbb{Z}^m$,*

$$\|Q^*\|_\infty \leq R \text{ et } \left\| {}^tAQ^* + P^* - \beta \right\|_\infty \leq C_2 R^{-\frac{n}{m}}.$$

Démonstration. D'après le premier corollaire **1**$\Longleftrightarrow$**2.** D'après le théorème 2 on a **1**$\Rightarrow$**3** et **2**$\Rightarrow$**4**. Supposons **3.** Soit $R > 0$, $Q^* \in \mathbb{Z}^n \backslash \{0\}$ et $P^* \in \mathbb{Z}^m$. Utilisons le théorème précedent avec $\varepsilon = C_1 R^{-\frac{m}{n}}$. On obtient

$$\|Q^*\|_\infty \leq (4nC_1 R^{-\frac{m}{n}})^{-1} \Rightarrow \left\| {}^tAQ^* + P^* \right\| > (4mR)^{-1}$$

d'où avec $R = (\frac{1}{4nC_1} \|Q^*\|_\infty)^{\frac{n}{m}}$

$$\left\| {}^tAQ^* + P^* \right\| > (4mR)^{-1} = (4m(\frac{1}{4nC_1} \|Q^*\|_\infty)^{\frac{n}{m}})^{-1} = c \|Q^*\|_\infty^{-\frac{n}{m}}$$

et ${}^tA$ est mal approchable. On démontre de même que **4** implique **1.** $\square$