Sommes de carrés de polynômes

Aurélie FISCHER
Anne-Laure POUPON

Juin 2006

Sujet d'exposé proposé par Philippe BIANE

Résumé

Un polynôme de $\mathbb{R}[X]$ s'écrit comme une somme de carrés si et seulement s'il ne prend que des valeurs positives. Qu'en est-il de polynômes en plusieurs indéterminées ? Le XVII^e problème de Hilbert concernait l'expression de tels polynômes comme somme de carrés. En fait, de nombreux polynômes positifs ne sont pas somme de carrés. Cependant, on a des résultats d'écriture comme somme de carrés de polynômes à indéterminées non commutatives, lorsqu'ils sont positifs dans un sens à définir.

Les polynômes non commutatifs sont évalués en substituant aux indéterminées des opérateurs bornés ou des matrices.

Un polynôme à coefficents dans $\mathbb{C}$, prenant des valeurs positives quels que soit les opérateurs unitaires en lesquels on l'évalue s'écrit comme une somme de carrés. On peut également faire le test avec les opérateurs hermitiens.

Si pour toute matrice réelle de toute taille, l'évaluation du polynôme donne une matrice positive, on dit que le polynôme est « positif au sens matriciel ». On a : un polynôme symétrique est « positif au sens matriciel » si et seulement si ce polynôme est somme de carrés.

Table des matières

1 Introduction

1.1 Le problème dans $\mathbb{R}[X]$ et $\mathbb{R}[X_1, ..., X_n]$

Soit P un polynôme de $\mathbb{R}[X]$ tel que, pour chaque x, $P(x)$ est positif. Les racines de P sont donc de multiplicité paire, et P se factorise :

$$P(X) = a^2 \prod (X - a_i)^2 \prod ((X - b_i)^2 + c_i^2)$$

En utilisant l'identité de Lagrange $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2(ad - bc)^2$ et en écrivant $(X - a_i)^2 = (X - a_i)^2 + 0^2$, on obtient par récurrence que P s'écrit $P = P_1^2 + P_2^2$.

Tout polynôme positif de $\mathbb{R}[X]$ s'écrit donc comme somme de carrés de polynômes.

Cette conclusion est-elle encore vérifiée pour les polynômes à plusieurs variables ? Hilbert a observé que ce n'est pas le cas. Par exemple, le polynôme $P(X, Y) = X^2Y^2(X^2 + Y^2 - 1) + 1$ est toujours positif sur $\mathbb{R}^2$, mais ne s'écrit pas comme somme de carrés de polynômes.

En 1900, le XVII^e problème que Hilbert pose lors de sa célèbre conférence au congrès international des mathématiciens est le suivant : est-il possible d'écrire un polynôme positif à n variables comme somme de carrés de fractions rationnelles (à défaut de pouvoir l'écrire comme somme de carrés de polynômes) ? Une réponse positive à ce problème a été apportée en 1926, par E. Artin.

En se plaçant dans le cadre des polynômes non commutatifs, J. W. Helton et S. McCullough, se sont intéressés, entre 2000 et 2002, à l'expression de polynômes positifs comme somme de carrés de polynômes.

1.2 Deux approches complémentaires

Nous montrerons tout d'abord une version de la factorisation de Fejer-Riesz, qui s'applique aux séries formelles à coefficients dans $\mathbb{C}$, à partir des travaux de S. McCullough ([1]). Grâce à ce théorème, il suffit de vérifier qu'une série formelle à variables matricielles est positive sur toutes les matrices unitaires ou toutes les matrices hermitiennes pour savoir qu'elle s'écrit comme un carré hermitien.

Nous nous attacherons ensuite à démontrer un théorème similaire, mais valable pour des polynômes symétriques à coefficients réels (le théorème s'applique en fait également dans $\mathbb{C}$). Ce dernier théorème, prouvé par J. W. Helton ([2]), permet d'implémenter un test de positivité pour les polynômes avec une complexité acceptable.

2 Une version de la factorisation de Fejer-Riesz

2.1 Cas de la dimension 1

Le théorème de factorisation de Fejer-Riesz affirme qu'un polynôme trigonométrique f en une variable, avec $f(e^{i\theta}) = \sum_{-n}^{n} a_j e^{ij\theta}$, positif sur le cercle unité, s'écrit comme le module au carré d'un polynôme g de la forme $g(e^{i\theta}) = \sum_{0}^{n} b_j e^{ij\theta}$. On peut même choisir ce polynôme extérieur au sens de Beurling (i.e. tel qu'il ne s'annule pas sur le disque unité ouvert).

La démonstration est simple : nécessairement si $f(e^{i\theta}) \geq 0 \ \forall \theta \in [0, 2\pi]$, alors $\overline{a_j} = a_{-j}$. Par conséquent,

$$f(z) = \overline{f(1/\bar{z})}$$

ce qui signifie que les zéros et les pôles de la fonction sont symétriques par rapport au cercle unité. Alors on peut écrire $z^n f(z) = cz^\nu \prod_j (z-\lambda_j)^2 \prod_k (z-\mu_k)(z^{-1}-\frac{1}{\overline{\mu_k}})$, avec c constante non nulle, $|\lambda_j| = 1$ et $\mu_k > 1$. On en déduit

$$f(e^{i\theta}) = |f(e^{i\theta})| = |c| \prod_j |e^{i\theta} - \lambda_j|^2 \prod_k \frac{|e^{i\theta} - \mu_k|^2}{|\mu_k|^2},$$

ce qui donne bien le résultat souhaité, et g n'a aucun zéro dans le disque unité ouvert.

M. Rosenblum et J. Rovnyak ont démontré un résultat identique mais avec des polynômes à coefficients dans $\mathcal{L}(\mathcal{C})$, algèbre des fonctions linéaires bornées d'un espace de Hilbert $\mathcal{C}$ ([6]), en utilisant un théorème de Krein « amélioré ». On a un théorème similaire pour la factorisation des séries formelles à plusieurs variables, que nous allons maintenant démontrer.

2.2 Théorème et plan de la démonstration

On définit tout d'abord $\mathcal{G}_m^n$ comme l'ensemble des mots de longueurs au plus n engendrés par g_1,...,g_m puis $\mathcal{H}_m^n$ comme l'ensemble des mots h de la forme $v^{-1}w$, où v et w appartiennent à $\mathcal{G}_m^n$. On choisit un ensemble $U = (U_1, \ldots, U_m)$ d'opérateurs unitaires et on définit U^h de manière canonique par $(U_{i_1} \ldots U_{i_k})^{-1} U_{j_1} \ldots U_{jl}$, où $(g_{i_1} \ldots g_{i_k})^{-1} g_{j_1} \ldots g_{jl} = h$

Soit $\mathcal{U}$ l'ensemble des opérateurs unitaires sur un espace de Hilbert séparable, $\mathcal{C}$ un espace de Hilbert et $\mathcal{L}(\mathcal{C})$ l'ensemble des opérateurs bornés sur $\mathcal{C}$. On cherche à montrer que toute série formelle à m variables de degré au plus n positive sur $\mathcal{U}^m$ s'écrit comme un carré hermitien. Le même théorème vaut dans le cas où l'on remplace $\mathcal{U}$ par $\mathcal{S}$ ensemble des matrices hermitiennes, et en remplaçant l'inverse par l'adjoint.

Théorème 1. *Soient m et n des entiers positifs et pour tout $h \in \mathcal{G}_m^n$, soit $A_h \in \mathcal{L}(\mathcal{C})$. Si*

$$A(U) = \sum_{h \in \mathcal{H}_m^n} U^h \otimes A_h$$

est positif sur $\mathcal{U}^m$ (i.e. s'il envoie tout m-uplet de matrices de la forme M^*M sur des matrices positives), alors il existe un espace de Hibert auxiliaire $\mathcal{E}$ et $B(U) = \sum_{v \in \mathcal{G}_m^n} U^v \otimes B_v$, où $B_v \in \mathcal{L}(\mathcal{C}, \mathcal{E})$ tels que

$$A(U) = B(U)^* B(U)$$

Par ailleurs, la dimension de $\mathcal{E}$ est au plus $dim(\mathcal{C}) \sum_0^n m^j$.

L'intérêt de ce théorème est qu'il suffit de vérifier qu'une telle série formelle est positive sur l'ensemble des matrices unitaires ou hermitiennes pour montrer qu'il est un carré hermitien. Cette simplification n'apporte pas grand-chose sur le plan algorithmique, mais peut être utile d'un point de vue théorique.

On pose $l = \sum_0^n m^j$, qui est le cardinal de $\mathcal{G}_m^n$, et V_m^n l'espace de Hilbert de base $\mathcal{G}_m^n$. Alors $\mathcal{L}(V_m^n)$ s'identifie naturellement avec $\mathfrak{M}_l$, ensemble des matrices de taille $l \times l$. Soit $E_{v,w}$ la matrice avec un 1 en position (v, w) et des 0 partout ailleurs.

Définition. On appelle *matrice de Toeplitz* (resp. *matrice de Haenkel*) toute matrice $(T_{v,w})_{v,w \in \mathcal{G}_m^n} \in \mathcal{L}(V_m^n)$ telle que $T_{v,w}$ ne dépend que de $v^{-1}w$ (resp. ${}^t vw$). L'ensemble de ces matrices est noté T_m^n (resp. H_m^n).

On pose $e(h) = \sum_{v^{-1}w=h} E_{v,w}$. Alors $\{e(h), h \in \mathcal{H}_m^n\}$ est une base de $\mathcal{T}_m^n$. On pose ensuite l'application linéaire $\phi : T_m^n \to \mathcal{L}(\mathcal{C})$ par $\phi(e(h)) = A_h$.

Définition. On dit qu'une application linéaire ϕ à valeurs matricielles sur une $\mathbb{C}^*$-algèbre A est *positive* si $\forall X \in A, \phi(X^*X) \geq 0$. On dit qu'une application linéaire $\phi : \mathcal{S} \to \mathcal{L}(\mathcal{C})$ est *complètement positive* si $\forall k, 1_k \otimes \phi : \mathfrak{M}_k \otimes \mathcal{S} \to \mathfrak{M}_k \otimes \mathcal{L}(\mathcal{C})$ est positive.

De manière équivalente, on peut définir $\phi_k : \mathfrak{M}_k(\mathcal{S}) \to \mathfrak{M}_k(\mathcal{L}(\mathcal{C}))$, et dire que ϕ est complètement positive si ϕ_k est positive pour tout k. Le produit tensoriel revient en quelque sorte à « restreindre »l'application de ϕ à des matrices de taille k.

Théorème 2. *L'application ϕ est complètement positive*

Pour montrer cela, on utilise le théorème suivant :

Théorème 3. *Si $T \in \mathfrak{M}_k \otimes T_m^n$ est positive, alors il existe $U = (U_1, \ldots, U_m)$ m-uplet d'opérateurs unitaires sur un espace de Hilbert $\mathcal{K}$ de dimension au plus $k \sum_0^n m^j$ et un opérateur $V : \mathbb{C}^k \to \mathcal{K}$ tels que*

$$T_{v,w} = V^* U^{v^{-1}w} V$$

$\forall |v|, |w| \leq n$.

La démonstration de ce théorème est reportée plus loin. Soit $T \in \mathfrak{M}_k \otimes T_m^n$, T est alors positive. On pose $t(u) = T_{v^{-1}w}$, avec $u = v^{-1}w$ (cette définition est cohérente puisque T est un opérateur de Toeplitz). On a alors $T = t(u) \otimes e(u)$, et en utilisant le théorème, il existe un m-uplet U de matrices unitaires et un opérateur V vérifiant $t(u) = V^* U^{v^{-1}w} V, \forall |u| \leq 2n$. On en déduit

$$\begin{aligned}
(1_k \otimes \phi)(T) &= 1_k \otimes \phi(\sum_h t(h) \otimes e(h)) \\
&= \sum t(h) \otimes \phi(e(h)) \\
&= \sum t(h) \otimes A_h \\
&= \sum V^* U^h V \\
&= (V \otimes 1_{\mathcal{C}})^* (\sum_h U^h \otimes A_h)(V \otimes 1_{\mathcal{C}})
\end{aligned}$$

qui est une matrice positive, donc $1_k \otimes \phi$ est positive pour tout k, donc ϕ est complètement positive.

On cherche ensuite à prolonger ϕ sur l'ensemble des matrices de taille l (c'est ce qui permet de ne vérifier la positivité du polynômes que sur un ensemble plus restreint). Pour cela, on utilise le théorème d'extension d'Arveson, qui est une généralisation du théorème de Krein aux fonctions complètement positives, et qui utilise la structure de $\mathbb{C}^*$-algèbre de $\mathfrak{M}_l$.

Théorème 4 (Arveson)**.** *Si $\mathcal{S} \subset \mathfrak{M}_l$ est fermé et auto-adjoint (i.e. stable par passage à l'auto-adjoint), et contient une matrice inversible définie positive, et si ϕ est une application linéaire complètement positive sur $\mathcal{S}$, alors on peut prolonger ϕ en une fonction complètement positive sur $\mathfrak{M}_l$.*

L'ensemble T_m^n vérifiant les hypothèses du théorème d'Arveson (il contient l'identité), on peut prolonger ϕ en une fonction $\tilde{\phi}$ complètement positive de $\mathfrak{M}_l$ vers $\mathcal{L}(\mathcal{C})$.

Or on a une caractérisation simple des applications complètement positives, due à Choi :

Théorème 5. *$\phi : \mathfrak{M}_l \to \mathcal{L}(\mathcal{C})$ est complètement positive si et seulement si*

$$(phi(E_{\alpha,\beta}))_{\alpha,\beta\in\mathcal{G}_m^n} \in \mathcal{L}(\oplus^l\mathcal{C})$$

est positive, avec $E_{\alpha,\beta}$ la matrice avec un 1 en position (α,β) et des 0 partout ailleurs.

Par conséquent (décomposition de Cholesky), il existe des opérateurs

$$B_v : \mathcal{C} \to \oplus^l\mathcal{C} \text{ vérifiant } B_v^*B_w = \bar{\phi}(E_{v,w}) \in \mathcal{L}(\oplus^l\mathcal{C}).$$

On en déduit :

$$\begin{aligned} A_h &= \phi(e(h)) \\ &= \phi(\sum_{h=v^{-1}w} E_{v,w}) \\ &= \sum_{h=v^{-1}w} \bar{\phi}(E_{v,w}) \\ &= \sum_{h=v^{-1}w} B_v^*B_w \end{aligned}$$

On réintroduit cette formule dans l'expression de la série formelle, et on obtient :

$$\begin{aligned} A(U) &= \sum_h U^h \otimes A_h \\ &= \sum_h U^h \otimes \sum_{h=v^{-1}w} B_v^*B_w \\ &= \sum_{v,w} U^{v^{-1}w} \otimes B_v^*B_w \\ &= B(U)^*B(U) \end{aligned}$$

avec les notations du théorème.

Le même schéma de démonstration s'applique exactement aux matrices de Haenkel, en remplaçant tous les inverses par des transposées. Comme le théorème de factorisation des matrices de Haenkel s'applique aux matrices définies positives cette fois, on l'applique à une matrice $H + \epsilon G$ avec $\epsilon > 0$ et on fait tendre ϵ vers 0.

2.3 Précision sur le théorème d'Arveson

En fait, l'hypothèse habituelle est que $\mathcal{S}$ contienne l'identité. Mais si $\mathcal{S}$ contient une matrice inversible P définie positive, on décompose P sous la forme X^*X et on pose $\mathcal{T} = (X^{-1})^*\mathcal{S}X^{-1}$. $\mathcal{T}$ vérifie les hypothèses du théorème d'Arveson

et contient l'identité, donc $\psi(M) = \phi(X^*MX)$ complètement positive sur $\mathcal{T}$ se prolonge sur $\mathfrak{M}_l$ en une application encore complètement positive, notée $\tilde{\psi}$. Alors $\tilde{\phi}(M) = \tilde{\psi}((X^{-1})^*MX^{-1})$ prolonge ϕ en une application complètement positive. Donc l'hypothèse que $\mathcal{S}$ contient une matrice définie positive suffit.

On peut trouver une démonstration du théorème d'Arveson dans [7].

2.4 Expression des matrices de Haenkel et de Toeplitz

On a utilisé un théorème de factorisation des opérateurs de Toeplitz. Pour le prouver, on a besoin d'un lemme qui prolonge d'un cran les opérateurs de $\mathfrak{M}_k \otimes T_m^n$:

Lemme 1. *Soit $T \in \mathfrak{M}_k \otimes T_m^n$. Si T est positive, alors il existe $R \in \mathfrak{M}_k \otimes T_m^{n+1}$ tel que R est positif et $R_{v,w} = T_{v,w}$, $\forall v, w \in \mathcal{G}_m^n$.*

Pour cela, on utilise un théorème reliant les graphes et les aplications positives. Un graphe sera dit *triangulé* si il ne contient pas de boucles de longueur 4 ou plus. Un sous-graphe H d'un graphe G sera appelé une *clique* si toutes les arêtes dans G qui relient des sommets de H sont encore présentes dans H.

Une matrice *partiellement positive subordonnée* à un graphe G est un ensemble P de matrices de taille k indexé par les arêtes de G tel que pour toute clique C de G, la matrice de matrices $(P_{v,w})_{(v,w)\in C}$ est positive.

Théorème 6. *Si G est un graphe triangulé et P une matrice partiellement positive subordonnée à G, alors il existe $k \times k$ matrices P_x indexées par toutes les arêtes réelles ou virtuelles entre des sommets de G, telles que (P_x) soit positive.*

Démonstration du lemme. Soit G le graphe de sommets $V = \mathcal{G}_m^{n+1}$ et d'arêtes $A = \{(v,w)\colon v^{-1}w \in \mathcal{H}_m^n\}$. Alors $(v,w) \in A$ si et seulement si $|v|, |w| \leq n$ ou $v = g_j v'$ et $w = g_j w'$. Les cliques maximales de G sont $\mathcal{G}_m^n$ et les $g_j\mathcal{G}_m^n$, et il n'y a pas d'arête reliant $\{g_j w\colon |w| = n\}$ et $\{g_l w\colon |w| = n\}$ si $j \neq l$.

Montrons maintenant que G est triangulé. On suppose que $L = v_1, \ldots, v_k$ est un ensemble de sommets de taille supérieure ou égale à 4. Si tous les v_j sont dans $\mathcal{G}_m^n$, puisque $\mathcal{G}_m^n$ est une clique, L ne peut pas être une boucle. On peut donc supposer par exemple que $v_1 = g_1 w_1$, avec $|w_1| = n$. Dans ce cas, $v_2 = g_1 w_2$ et $v_k = g_1 w_k$, avec $|w_2|, |w_k| \leq n$. Alors v_2 et v_k sont voisins et L n'est pas une boucle de longueur supérieure à 4. G est donc triangulé.

On pose $t(h) = t(v^{-1}w) = T_{v,w}$. La matrice R vérifiant $R_{v,w} = t(v^{-1}w)$ est partiellement positive subordonnée à G. Sur les cliques maximales,

$$(R_{v,w})_{v,w\in g_j\mathcal{G}_m^n} = (R_{g_j v', g_j w'})_{v',w'\in\mathcal{G}_m^n} = (T_{v',w'})_{v',w'\in\mathcal{G}_m^n}$$

On déduit du théorème qui précède l'existence de $(R_{v,w})_{v,w\in\mathcal{G}_m^n}$ positive, ce qui prouve le lemme. □

On peut maintenant prouver le théorème suivant :

Théorème 7. *Si $T \in \mathfrak{M}_k \otimes T_m^n$ est positive, alors il existe $U = (U_1, \ldots, U_m)$ m-uplet d'opérateurs unitaires sur un espace de Hilbert $\mathcal{K}$ de dimension au plus $k\sum_0^n m^j$ et un opérateur $V : \mathbb{C}^k \to \mathcal{K}$ tels que*

$$T_{v,w} = V^* U^{v^{-1}w} V$$

$\forall |v|, |w| \leq n$.

Démonstration. Par récurrence en appliquant le lemme qui précède, on sait qu'il existe $R_{v,w}$ matrice de taille k qui prolonge T telle que pour chaque N, $(R_{v,w})_{|v|,|w|\leq N}$ est positive. On note $\mathfrak{V}$ l'espace vectoriel de base $\mathcal{G}_m$, et $H(G)$ l'espace de Hilbert obtenu en quotientant $\mathbb{C}^k \otimes \mathfrak{V}$ par le moyau de la forme positive $[\sum x_w \otimes w, \sum y_v \otimes v] = \sum \langle R_{v,w} x_w, y_v \rangle]$.

On définit les opérateurs déplacements S_j denses dans $H(G)$ par $S_j \sum x_w \otimes w = \sum x_w \otimes g_j w$. On a alors :

$$\begin{aligned}
[S_j \sum x_w \otimes w, S_j \sum y_v \otimes v] &= [\sum x_w \otimes g_j w, \sum y_v \otimes g_j v] \\
&= \left\langle \sum R_{g_j v, g_j w} x_w, y_v \right\rangle \\
&= \left\langle \sum R_{v,w} x_w, y_v \right\rangle \\
&= [\sum x_w \otimes w, \sum y_v \otimes v]
\end{aligned}$$

Ceci montre que les S_j sont des isométries et donc s'étendent en une isométrie sur $H(G)$. Il existe un espace de Hilbert $K(G)$ contenant $H(G)$ et des opérateurs unitaires U_j sur $K(G)$ tels que $H(G)$ est invariant par les U_j et ces derniers prolongent les S_j.

On définit $V : \mathbb{C}^k \to K(G)$ par $Vx = x \otimes e$ et on obtient pour $|v|, |w| \leq n$,

$$\begin{aligned}
\left\langle V^* U^{v^{-1}w} V x, y \right\rangle &= \langle U^w x \otimes e, U^v y \otimes e \rangle \\
&= \langle S^w x \otimes e, S^v y \otimes e \rangle \\
&= \langle x \otimes w, y \otimes v \rangle \\
&= \langle R_{v,w} x, y \rangle \\
&= \langle T_{v,w} x, y \rangle
\end{aligned}$$

On en déduit donc que $V^* U^{v^{-1}w} V = T_{v,w}$. □

En ce qui concerne les matrices de Haenkel, on a les énoncés suivants :

Théorème 8. *Soit $H \in \mathfrak{M}_k \otimes H_m^n$. Si H est définie positive (seul changement par rapport aux matrices de Toeplitz), alors il existe un m-uplet S d'opérateurs hermitiens sur un espace de Hilbert $\mathcal{K}$ de dimension au plus $k\sum_0^n m^j$ et un opérateur $V : \mathbb{C}^k \to \mathcal{K}$ tel que*

$$H_{v,w} = V^* S^t v w V$$

pour tous $v, w \in \mathcal{G}_m^n$.

Une fois montré le lemme qui suit, la démonstration du théorème est exactement identique à celle du théorème sur les matrices de Toeplitz.

Lemme 2. *Soit $H \in \mathfrak{M}_k \otimes H_m^n$. Si H est définie positive, alors il existe $G, G' \in \mathfrak{M}_k \otimes H_m^{n+1}$ qui prolongent H telles que :*

- *G' est définie positive*
- *G est positive et pour tout $x = \sum_{|w|=n+1} x_w \otimes w \in \mathfrak{C}^k \otimes V_m^n$, il existe $y = \sum |w| \leq n y_w \otimes w$ tel que $G(x - y) = 0$.*

Démonstration. On pose $G_{v,w} = 0 = G'_{v,w}$ pour $|^t vw| = 2n + 1$. On considère V_m^n comme un sous-espace de V_m^{n+1}, et son orthogonal est l'ensemble de mots de longueurs exactement $n + 1$.

On pose $X : \mathfrak{C}^k \otimes (V_m^n)^\perp \to \mathfrak{C}^k \otimes V_m^n$ par

$$\langle X(x \otimes w), y \otimes v \rangle = \langle G_{v,w} x, y \rangle$$

Soit $Y = X^* H^{-1} X$. On définit, pour $|v|, |w| = n + 1$:

$$\langle G_{v,w} x, y \rangle = \langle Y(x \otimes w), y \otimes v \rangle$$

Alors la matrice de Haenkel

$$G = \begin{pmatrix} H & X \\ X^* & Y \end{pmatrix} = \begin{pmatrix} H^{1/2} \\ X^* H^{-1/2} \end{pmatrix} \begin{pmatrix} H^{1/2} & H^{-1/2} X \end{pmatrix}$$

est positive.

Pour $G(x - y) = 0$, $y = X^* H - 1X$ convient. On pose $G'_{^t vw} = G_{^t vw} + \delta_{v,w} I$, où $\delta_{v,w}$ est le symbole de Kronecker. G' est bien définie positive, ce qui conclut la démonstration. □

Grâce à ce lemme, on peut montrer de plus par récurrence que $\mathfrak{M}_k \otimes H_m^n$ contient une matrice définie positive.

3 Factorisation d'un polynôme symétrique positif au sens matriciel

3.1 Notations

Définition. Un polynôme Q est une somme de mots sur $X_1, X_2, ..., X_n, {}^t X_1, {}^t X_2, ..., {}^t X_n$, affectés de coefficients. Ce système de $2n$ générateurs est clos par l'involution « transposée » notée ^{t}. On note $X = \{X_1, X_2, ..., X_n\}$ et, de même, $X^T = \{{}^t X_1, {}^t X_2, ..., {}^t X_n\}$. Pour alléger les notations, on écrit simplement $Q(X)$ au lieu de $Q(X, {}^t X)$.

Un polynôme Q, symétrique en X et ${}^t X$, est dit « positif au sens matriciel » lorsque la subsitution dans Q de n'importe quelles matrices réelles $\chi_1, ..., \chi_n, {}^t \chi_1, ..., {}^t \chi_n$ de n'importe quelle taille, aux indéterminées $X_1, ..., X_n, {}^t X_1, ..., {}^t X_n$ donne une matrice $Q(\chi_1, ..., \chi_n, {}^t \chi_1, ..., {}^t \chi_n)$ positive.

Exemple. Soit $Q(X) = X_1^2 + {}^t (X_1^2) + {}^t X_2 X_2$. Pour des matrices de taille 1, $Q(\chi)$ est positive car on a une somme scalaire de carrés.

Qu'en est-il pour les matrices de taille 2 ? Prenons, par exemple,

$$\chi_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \chi_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On obtient :

$$Q(\chi) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

qui n'est pas positive. Donc $Q(X)$ n'est pas positif au sens matriciel.

On dit qu'un polynôme est somme de carrés lorsqu'il s'écrit :

$$Q(X) = \sum_i^t h_i(X) h_i(X)$$

où chaque h_i est un polynôme en X et ${}^t X$.

On remarque que si Q s'écrit sous cette forme, alors $Q(\chi) \geq 0 \quad \forall \chi$

Montrons que la réciproque est vraie : un polynôme symétrique positif au sens matriciel est somme de carrés. La méthode consiste en un argument de dualité, grâce à l'équivalence d'une condition portant sur les matrices et d'une condition portant sur une forme linéaire définie sur les matrices.

3.2 La représentation de Gram

Soit Q un polynôme symétrique non commutatif. On suppose qu'il est positif au sens matriciel et on souhaite montrer qu'il est somme de carrés. Le degré de Q est un entier pair $2d$. On note $\nu(d)$ le nombre de monômes sur $X_1, X_2, ..., X_n, {}^tX_1, {}^tX_2, ..., {}^tX_n$ de degré $\leq d$.

Notons $V^d(X)$ le vecteur composé de tous les monômes de degré $\leq d$, rangés dans l'ordre lexicographique en classant systématiquement les X_i avant les ${}^tX_i$.

Exemple. Pour $X = \{X_1, X_2\}$, $V^2(X)$ est le vecteur colonne de composantes :

$$\{I, X_1, X_2, {}^tX_1, {}^tX_2, X_1^2, X_1X_2, X_1^tX_1, X_1^tX_2, X_2X_1, ..., ({}^tX_2)^2\}$$

Théorème 9 (Représentation de Gram)**.** *On peut écrire le polynôme Q sous la forme :*

$$Q(X) = {}^t V^d(X) M_Q V^d(X), \text{ où } M_Q \in \mathfrak{S}_p(\mathbb{R})$$

Démonstration. Si M est un monôme unitaire en X et ${}^tX$ de degré $\leq 2d$, alors on peut écrire M comme produit de monômes de degré $\leq d$:

$$M = M_g M_d$$

On a $[{}^tV^d(X)]_i = M_g$ et $[V^d(X)]_j = M_d$ pour un certain i et un certain j.

Supposons $i \neq j$. On constate que $M + {}^t M = {}^t V^d(X) E'_{ij} V^d(X)$ où E'_{ij} est la matrice symétrique ayant tous ses coefficients nuls sauf ceux en position ij et ji qui valent 1.

$$\begin{aligned}
\text{En effet, } {}^tV^d(X)E'_{ij}V^d(X) &= \begin{pmatrix} V^d(X)_i \\ V^d(X)_j \end{pmatrix}^t \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} V^d(X)_i \\ V^d(X)_j \end{pmatrix} \\
&= {}^tV^d(X)_j V^d(X)_i + {}^t V^d(X)_i V^d(X)j \\
&= {}^tM_d^t M_g + M_g M_d \\
&= {}^tM + M \\
\text{Si } i = j, \ {}^tV^d(X)E'_{ii}V^d(X) &= {}^tV^d(X)_i V^d(X)_i \\
&= M_g M_d \\
&= M
\end{aligned}$$

Ainsi, tant que la décomposition $M = M_g M_d$ n'est pas symétrique, on peut prendre une matrice E'_{ij} ayant tous ses termes diagonaux nuls. Par contre, lorsque le degré de M est 0 ou que M est symétrique de degré $2d$, on a ${}^tM_g = M_d$ et E'_{ii} a tous ses coefficients nuls sauf le coefficient diagonal d'indice i qui est 1.

En écrivant le polynôme symétrique Q comme combinaison linéaire de termes de la forme ${}^tM + M$, on a la représentation désirée avec M_Q combinaison linéaire des $E'ij$. □

Quand on substitue à X un ensemble de matrices χ, on note

$$\chi^{(j)}, j = \{0, ..., \nu(d-1)\}$$

les composantes de $V^d(\chi)$.

Exemple. En reprenant l'exemple précédent, on a : $\chi^{(0)} = Id$, $\chi^{(1)} = \chi_1$, $\chi^{(5)} = \chi_1^2$, $\chi^{(8)} = \chi_1^t \chi_2$ et ainsi de suite.

3.3 Passage au problème dual

On peut montrer qu'il n'y a pas unicité de la représentation de Gram. Si on parvient à « rendre M_Q positive », alors la décomposition de Cholesky de M_Q permet de conclure que Q est somme de carrés.

Étant donné $M_Q \in \mathfrak{S}_p(\mathbb{R})$ et $\mathcal{B}$ un sous-espace vectoriel de $\mathfrak{S}_p(\mathbb{R})$, on souhaite montrer qu'il existe une matrice $B \in \mathcal{B}$ telle que $M = M_Q + B$ soit positive.

On utilise le produit scalaire sur $\mathfrak{S}_p(\mathbb{R})$ défini par la trace : $\langle A, B \rangle = \text{tr } AB$.

On a $\mathcal{B}^\perp = \{A \in \mathfrak{S}_p(\mathbb{R}) \colon \text{tr } AB = 0 \ \ \forall B \in \mathcal{B}\}$ et on note $\mathcal{B}^{\perp +} = \mathcal{B}^\perp \cap \{\text{matrices positives}\}$

On résout notre problème en passant par le problème dual. Soit ℓ_{M_Q} la forme linéaire continue définie sur $\mathcal{B}^\perp$ par :

$$\ell_{M_Q}(A) = \text{tr } M_Q A$$

Théorème 10 (Dualité)**.** *Soit $\mathcal{B}$ un sous-espace vectoriel de $\mathfrak{S}_p(\mathbb{R})$ et $M_Q \in \mathfrak{S}_p(\mathbb{R})$. Si $\mathcal{B}^{\perp +}$ contient une matrice inversible, les conditions suivantes sont équivalentes :*

1. *Il existe $B \in \mathcal{B}$ telle que $M = M_Q + B$ soit positive.*
2. *$\ell_{M_Q} \geq 0$ sur $\mathcal{B}^{\perp +}$*

Démonstration. Supposons tout d'abord qu'il existe $B \in \mathcal{B}$ telle que $M = M_Q + B \geq 0$. Soit $A \in \mathcal{B}^{\perp +}$. On a :

$$\ell_{M_Q}(A) = \text{tr } M_Q A = \text{tr } (M_Q + B)A = \text{tr } MA \geq 0$$

car M et A sont positives.

Supposons maintenant que $\ell_{M_Q} \geq 0$ sur $\mathcal{B}^{\perp +} = \mathcal{B}^\perp \cap \{\text{matrices positives}\}$. On utilise une variante du théorème de Hahn-Banach, le théorème de prolongement de Krein [5], qui dit que l'on peut étendre à tout l'espace une forme linéaire positive définie sur un sous-espace.

Les hypothèses du théorème de Krein sont satisfaites :

– $N \geq 0$ et $-N \geq 0$ impliquent $N = 0$

– Si $N \in \mathfrak{S}_p(\mathbb{R})$, il existe $A \in \mathcal{B}^{\perp +}$ telle que $A - N \geq 0$. En effet, il existe $\tilde{A} \in \mathcal{B}^{\perp +}$ inversible ; c'est une matrice définie positive, donc comme pour tout vecteur $Z \neq 0$, ${}^tZAZ \neq 0$, on a, pour un certain λ, $\lambda\tilde{A} - N \geq 0$.

Donc la forme linéaire ℓ_{M_Q} s'étend en une forme linéaire $\tilde{\ell}$ qui prend des valeurs positives sur les matrices positives.

On représente $\tilde{\ell}$: d'après le théorème de Riesz-Fréchet, $\exists\,!\ M \in \mathfrak{S}_p(\mathbb{R})$ telle que

$$\tilde{\ell}(A) = \text{tr } MA \qquad \forall A \in \mathfrak{S}_p(\mathbb{R})$$

On remarque que $M \geq 0$. En effet, $\forall A \geq 0$, $\tilde{\ell}(A) = \sum_{i,j=0}^{p-1} m_{ij}a_{ij} \geq 0$ et pour Z vecteur de composantes z_i avec $i = 0, ..., p-1$, ${}^tZMZ = \sum_{i,j=0}^{p-1} z_i z_j m_{ij}$. Soit A_Z la matrice de terme général $z_i z_j$: $\forall Y$, ${}^tYMY = \sum_{k,q=0}^{p-1} z_k z_q y_k y_q = \Big(\sum_{k=0}^{p-1} z_k y_k\Big)^2 \geq 0$ donc A_Z est positive $\forall Z$, d'où $\forall Z$, ${}^tZMZ = \text{tr } MA \geq 0$.

Alors $\forall A \in \mathcal{B}^{\perp}, 0 = \tilde{\ell}(A) - \ell_{M_Q}(A) = \text{tr } MA - \text{tr } M_QA = \text{tr } (M - M_Q)A$

Donc $B = M - M_Q \in \mathcal{B}^{\perp\perp} = \mathcal{B}$ et on a trouvé une matrice positive $M = M_Q + B$ avec $B \in \mathcal{B}$. □

On note A_v la matrice de terme général $a_{kl} = v_k \cdot v_l$.

Soit $\mathcal{A}_{V^d,q} = \{A_{V^d(\chi)v_0}$ avec χ ensemble de matrices de $\mathfrak{M}_q(\mathbb{R})$ et $v_0 \in \mathbb{R}^q\}$

Pour $\chi = \{\chi_1, \chi_2, ..., \chi_n, {}^t\chi_1, {}^t\chi_2, ..., {}^t\chi_n\}$ donné, $A_{V^d(\chi)v_0}$ est la matrice A_v avec $v = V^d(\chi)v_0$, c'est-à-dire le vecteur formé des $\chi^0 v_0, ..., \chi^{\nu(d-1)}v_0$.

Théorème 11. *On a :*

$$\ell_{M_Q}(A) = tr\ M_QA \geq 0 \qquad \forall A \in \mathcal{A}_{V^d,q}$$

Démonstration. Fixons $N \in \mathfrak{M}_p(\mathbb{R})$. Pour χ avec composantes $\chi_t \in \mathfrak{M}_q(\mathbb{R})$ avec $|t| \in 1, ..., n$ et $v_0 \in \mathbb{R}^q$, on a $V^d(\chi)v_0 \in \mathfrak{M}_{qp}(\mathbb{R})$

Alors : $\ell_N(A_{V^d(\chi)v_0}) = \text{tr } NA_{V^d(\chi)v_0} = \sum_{i,j=0}^{p-1} n_{ij}\ v_i \cdot v_j = {}^t\, v_0^t V^d(\chi) N V^d(\chi) v_0$

Donc

$$\ell_{M_Q}(A_{V^d(\chi)v_0}) = \text{tr } M_QA_{V^d(\chi)v_0} = {}^t\, v_0^t V^d(\chi) M_Q V^d(\chi) v_0 = {}^t\, v_0 Q(\chi) v_0 \geq 0$$

car Q est positif au sens matriciel. □

On souhaite appliquer ce qui précède à $\mathcal{B} = \mathcal{B}_{V^d}$ défini comme suit :

$$\mathcal{B}_{V^d} = \{B \in \mathfrak{S}_p(\mathbb{R}) \colon {}^tV^d(X)BV^d(X) = 0\}$$

On note :

$$\mathcal{B}_{V^d,q} = \{B \in \mathfrak{S}_p(\mathbb{R}) \colon {}^tV^d(\chi)BV^d(\chi) = 0 \quad \forall \chi \in \mathfrak{M}_q(\mathbb{R})\}$$

et

$$(\mathcal{B}_{V^d,q})^{\perp +} = (\mathcal{B}_{V^d,q})^{\perp} \cap \{\text{matrices positives}\}$$

3.4 Matrices fondamentales et caractérisation de $\mathcal{B}_{V^d}$

Définition. On appelle « matrice fondamentale » toute matrice symétrique F vérifiant, pour un certain ensemble de couples $\{(i,j),(k,l)\}$,

$$\begin{aligned} F_{ij} &= -F_{kl} \\ F_{ji} &= -F_{lk} \\ F_{st} &= 0 \text{ ailleurs} \end{aligned}$$

Soit $\mathcal{F}(\{(i,j),(k,l)\})$ l'ensemble des matrices fondamentales pour $\{(i,j),(k,l)\}$. Si $(i,j) = (k,l)$, $\mathcal{F}(\{(i,j),(k,l)\})$ ne contient que la matrice nulle.

On associe les monômes vérifiant ${}^tV^d(X)_iV^d(X)_j =^t V^d(X)_kV^d(X)_l$ aux matrices fondamentales correspondantes.

Lemme 3. *L'espace vectoriel $\mathcal{B}_{V^d}$ est engendré par les matrices fondamentales.*

Démonstration.

$${}^tV^d(X)BV(X) = \sum_{u,s=0}^{p-1} b^t_{us}V^d(X)_uV^d(X)_s$$

est une somme de monômes donc cette quantité est nulle si et seulement si le coefficient de chaque monôme est nul. On considère un monôme $\mu(X)$ que l'on peut écrire de r manières différentes :

$$\mu(X) =^t V^d(X)_{i_l}V^d(X)_{j_l} \qquad\qquad l \in \{1,...,r\}$$

Pour que disparaissent les termes en $\mu(X)$ dans la somme, il faut que leurs coefficients vérifient

$$\sum_{l=1}^{r} b_{i_lj_l} = 0$$

$$\text{Soit } E_{\mu(X)} = \Big\{(b_{i_1j_1}, ..., b_{i_rj_r})\colon \sum_{l=1}^{r} b_{i_lj_l} = 0\Big\}$$

C'est un espace vectoriel, qui est engendré par le sous-espace $\mathcal{E}_{\mu(X)}$ formé des éléments ayant exactement deux coefficients non nuls, par exemple les coefficients d'indices $i_{l_u}j_{l_u}$ et $i_{l_s}j_{l_s}$. B étant symétrique, le coefficient de $\mu(X)$ est annulé si et seulement si celui de ${}^t\mu(X)$ l'est. En fait, chaque vecteur de $\mathcal{E}_{\mu(X)}$ correspond aux matrices fondamentales $\mathcal{F}(\{(i_{l_u}, j_{l_u}), (i_{l_s}, j_{l_s})\})$ pour $\mu(X)$. Ici, on demande $(i_{l_u}, j_{l_u}) \neq (i_{l_s}, j_{l_s})$.

Une matrice fondamentale F de $\mathcal{F}(\{(i_{l_u}, j_{l_u}), (i_{l_s}, j_{l_s})\})$ est dans $\mathcal{B}_{V^d}$, car

$$\begin{aligned}
{}^tV^d(X)FV^d(X) &= \sum_{u,s=0}^{p-1} F^t_{us} V^d(X)_u V^d(X)_s \\
&= F^t_{i_{l_u}j_{l_u}} V^d(X)_{i_{l_u}} V(X)_{j_{l_u}} + F^t_{i_{l_s}j_{l_s}} V^d(X)_{i_{l_s}} V(X)_{j_{l_s}} \\
&\quad + F^t_{j_{l_u}i_{l_u}} V^d(X)_{j_{l_u}} V(X)_{i_{l_u}} + F^t_{j_{l_s}i_{l_s}} V^d(X)_{j_{l_s}} V(X)_{i_{l_s}} \\
&= [F_{i_{l_u}j_{l_u}} + F_{i_{l_s}j_{l_s}}]\mu(X) + [F_{j_{l_u}i_{l_u}} + F_{j_{l_s}i_{l_s}}]\mu(X) = 0
\end{aligned}$$

Soit P_μ l'ensemble de toutes les paires de couples d'entiers associés au monôme $\mu(X)$, les deux couples d'une paire n'étant jamais égaux. L'espace vectoriel engendré par les matrices fondamentales provenant des $E_{\mu(X)}$ lorsqu'on balaie tous les monômes $\mu(X)$ est $\mathcal{B}_{V^d}$, c'est-à-dire :

$$\mathcal{B}_{V^d} = \text{vect}\{\mathcal{F}(\{(i,j),(k,l)\})\colon \{(i,j),(k,l)\} \in P_\mu \text{ pour un certain monôme } \mu\}$$

□

3.5 Lien entre $\mathcal{A}_{V^d,q}$ et $\mathcal{B}_{V^d,q}$

D'après ce que l'on vient de voir, $\mathcal{B}_{V^d}$ est de la forme

$$\mathcal{B}^{\mathcal{P}} = \text{vect } (\mathcal{F}(\{(i,j),(k,l)\})\colon \{(i,j),(k,l)\} \in P \text{ et } P \in \mathcal{P})$$

avec $\mathcal{P}$ un ensemble d'ensembles P de paires de couples d'entiers entre 0 et $p-1$. On appellera un tel $\mathcal{P}$ une « collection de paires de couples ».

On note

$$\mathcal{A}^{\mathcal{P}} = \bigcap_{P\in\mathcal{P}} \{A_v\colon v \in \mathbb{R}^{rp} \text{ tel que } v_i \cdot v_j = v_k \cdot v_l \ \ \forall\{(i,j),(k,l)\} \in P, P \in \mathcal{P}\}$$

Lemme 4. *Soit $\mathcal{P}$ une collection de paires de couples.*

$$(\mathcal{A}^{\mathcal{P}})^{\perp} = \mathcal{B}^{\mathcal{P}} \quad (1)$$

$$\mathcal{A}^{\mathcal{P}} = (\mathcal{B}^{\mathcal{P}})^{\perp+} \quad (2)$$

(3) *Si $q \geq p$, l'ensemble $(\mathcal{B}^{\mathcal{P}})^{\perp +}$ ne contient aucune matrice inversible si et seulement si $\exists Z \in \mathbb{R}^p$, de coordonnées z_i, avec*

$$\sum_{j=0}^{p-1} v_j z_j = 0 \qquad \forall v \text{ tel que } v_i \cdot v_j = v_k \cdot v_l \;\; \forall \{(i,j),(k,l)\} \in P, P \in \mathcal{P}$$

Démonstration. 1. Écrivons :

$$(\mathcal{A}^{\mathcal{P}})^{\perp} = \text{vect } \left\{ \{A_v \colon v_i \cdot v_j = v_k \cdot v_l, v \in \mathbb{R}^{rp}\}^{\perp} \colon \{(i,j),(k,l)\} \in P \text{ et } P \in \mathcal{P} \right\}$$

Caractérisons l'ensemble $\mathfrak{a}^{\perp} = \{A_v \colon v_i \cdot v_j = v_k \cdot v_l, v \in \mathbb{R}^{rp}\}^{\perp} \subset \mathfrak{S}_p(\mathbb{R})$.
Une matrice symétrique $B \in \mathfrak{a}^{\perp}$ si et seulement si tr $BA_v = 0 \;\; \forall v \in \mathbb{R}^{rp}$ avec $v_i \cdot v_j = v_k \cdot v_l$.

$$\begin{aligned} 0 &= \text{tr } BA_v = \sum_{s,t=0}^{p-1} b_{st}[A_v]_{st} = \sum_{s,t=0}^{p-1} b_{st} \;\; v_s \cdot v_t \\ &= 2(b_{ij} + b_{kl}) v_i \cdot v_j + \sum_{\substack{s,t=0 \\ (s,t) \neq (i,j),(j,i),(k,l),(l,k)}}^{p-1} b_{st} \;\; v_s \cdot v_t \end{aligned}$$

Comme $r \geq p$, on peut choisir une famille assez riche de v vérifiant

$$v_i \cdot v_j = v_k \cdot v_l$$

pour avoir :

$$\begin{aligned} b_{ij} + b_{kl} &= 0 \\ b_{st} &= 0 \text{ pour } (s,t) \neq (i,j),(j,i),(k,l),(l,k) \end{aligned}$$

On a ainsi $\mathfrak{a}^{\perp} = \mathcal{F}(\{(i,j),(k,l)\})$, donc $(\mathcal{A}^{\mathcal{P}})^{\perp} = \mathcal{B}^{\mathcal{P}}$

2. La suite de la démonstration nécessite un lemme.

Lemme 5 (Représentation par q-vecteur)**.** *Si $A \in \mathfrak{S}_p(\mathbb{R})$ est une matrice positive de rang q, on peut l'écrire comme $A_v \in \mathfrak{S}_p(\mathbb{R})$ pour un certain v de composantes $v_0, ..., v_{p-1}$ dans $\mathbb{R}^q$.*

Démonstration. Soit $A \in \mathfrak{S}_p(\mathbb{R})$ positive. Par la décomposition de Cholesky $A = LD^tL$, A a une représentation :

$$A = \sum_{j=1}^{p} u^j ({}^t u^j)$$

avec $u^j \in \mathbb{R}^p$ vecteur colonne de composantes réelles $u_0^j, ..., u_{p-1}^j$. Si A n'est pas inversible de rang q, certains u^j intervenant dans la somme sont combinaison linéaire d'autres u^j, d'où une écriture équivalente :

$$A = \sum_{j=1}^{q} w^j ({}^t w^j)$$

Soit v le vecteur de composantes :

$$w_0^1, ..., w_0^q, w_1^1, ..., w_1^q, ..., w_{p-1}^1, ..., w_{p-1}^q$$

On définit des sous-vecteurs en posant $v_k = (w_k^1, ..., w_k^q)$
Montrons que $\forall (k,l), a_{kl} = v_k \cdot v_l$: on aura $A = A_v$.

$$A = \begin{pmatrix} w_0^1 \\ w_1^1 \\ \vdots \\ w_{p-1}^1 \end{pmatrix} (w_0^1, ..., w_{p-1}^1) + ... + \begin{pmatrix} w_0^q \\ w_1^q \\ \vdots \\ w_{p-1}^q \end{pmatrix} (w_0^q, ..., w_{p-1}^q)$$

Donc $a_{kl} = w_k^1 w_l^1 + w_k^2 w_l^2 + ... + w_k^q w_l^q = v_k \cdot v_l$ □

Maintenant, pour compléter la preuve du lemme 4, on considère

$$A \in (\mathcal{B}^{\mathcal{P}})^{\perp +} \subset \mathfrak{S}_p(\mathbb{R})$$

qui possède une représentation par r-vecteur d'après le lemme 5, puisque $\mathrm{rg}(A) \leq p \leq r$: pour un certain $v \in \mathbb{R}^{rp}, A = A_v$.
Par définition de $\mathcal{B}^{\perp}$, les composantes $v_j \in \mathbb{R}^r$ vérifient

$$\forall \{(i,j),(k,l)\} \in P, P \in \mathcal{P}, \quad v_i \cdot v_j = v_k \cdot v_l$$

Donc, on a $(\mathcal{B}^{\mathcal{P}})^{\perp +} \subset \mathcal{A}^{\mathcal{P}}$. Comme les matrices de $\mathcal{A}^{\mathcal{P}}$ sont positives et que $(\mathcal{A}^{\mathcal{P}})^{\perp} = \mathcal{B}^{\mathcal{P}}$, on a $\mathcal{A}^{\mathcal{P}} \subset (\mathcal{B}^{\mathcal{P}})^{\perp +}$ d'où l'égalité.

3. Montrons que si l'ensemble $(\mathcal{B}^{\mathcal{P}})^{\perp +} = \mathcal{A}^{\mathcal{P}}$ ne contient aucune matrice inversible, alors $\exists Z \in \mathbb{R}^p$ non nul, de coordonnées z_i, avec

$$\sum_{j=0}^{p-1} v_j z_j = 0 \qquad \forall v \text{ qui vérifie } v_i \cdot v_j = v_k \cdot v_l \ \ \forall P \in \mathcal{P}.$$

On remarque que $(\mathcal{B}^{\mathcal{P}})^{\perp +}$ est un cône : si A^1 et A^2 appartiennent à $(\mathcal{B}^{\mathcal{P}})^{\perp +}$, il en est de même de $A^1 + A^2$. La positivité entraîne

$$\ker(A^1 + A^2) = \ker(A^1) \cap \ker(A^2)$$

$\ker\left(\sum_i A^i\right) = \bigcap_i \ker A^i$ en prenant toutes les matrices de $(\mathcal{B}^{\mathcal{P}})^{\perp+}$: si aucune n'est inversible, il existe $\mathcal{N} \subset \mathbb{R}^p$ non trivial tel que $\mathcal{N} \subset \bigcap_i \ker A^i$

Soit $Z \neq 0$ dans $\mathbb{R}^p$, tel que $Z \in \ker(A_v)$:

$$0 = A_v \;\; Z \cdot Z = \sum_{i=0}^{p-1} \left[\sum_{j=0}^{p-1} v_i \cdot v_j \;\; z_j \right] z_i = \left\| \sum_{j=0}^{p-1} v_j z_j \right\|^2$$

Donc

$$\sum_{j=0}^{p-1} v_j z_j = 0 \qquad \forall v \text{ qui vérifie } v_i \cdot v_j = v_k \cdot v_l \;\; \forall P \in \mathcal{P}.$$

□

Donc pour $q \geq p$,

$$\mathcal{A}_{V^d,q} \subset (\mathcal{B}_{V^d,q})^{\perp+} \subset \mathfrak{S}_p(\mathbb{R})$$

En remarquant que $\mathcal{B}_{V^d,q} = \mathcal{B}_{V^d}$, on a $\mathcal{A}_{V^d,q} \subset (\mathcal{B}_{V^d})^{\perp+} \subset \mathfrak{S}_p(\mathbb{R})$

Théorème 12. *Pour r assez grand,*

$$\overline{\{V^d(\chi)v_0 \colon \chi \subset \mathfrak{M}_r(\mathbb{R}) \text{ , } v_0 \in \mathbb{R}^r\}} = \{v \in \mathbb{R}^{rp} \textit{ vérifiant } \mathcal{R}\cdot\}$$

Démonstration. Soit $v \in \mathbb{R}^{qp}$ vérifiant $\mathcal{R}\cdot$; on note v_0 sa première composante.

1. Si $v_0 \neq 0$ et si les $v_{(j)}$, $|j| \in \{0, ..., d-1\}$ sont linéairement indépendants, v s'écrit $V^d(\chi)v_0$.
   En effet, $\forall t \in \{0, ..., n\}$, on définit χ_t et $\hat{\chi}_{-t}$ sur les $v_{(j)}$, $|j| \in \{0, ..., d-1\}$ par :
   $$\chi_t v_{(j)} = v_{(\{t\}*j)} \text{ et } \hat{\chi}_{-t} v_{(j)} = v_{((-\{t\})*j)}$$
   Donc, χ_t et $\hat{\chi}_{-t}$ sont définis sur le sous-espace $\mathcal{S}^{d-1}$ engendré par la famille libre des $v_{(j)}$, $|j| \in \{0, ..., d-1\}$, mais pas sur son orthogonal. Pour avoir des matrices définies partout, écrivons
   $$\chi_t = \begin{pmatrix} \chi_{11} & \chi_{12} \\ \chi_{21} & \chi_{22} \end{pmatrix} \qquad \hat{\chi}_{-t} = \begin{pmatrix} \hat{\chi}_{11} & \hat{\chi}_{12} \\ \hat{\chi}_{21} & \hat{\chi}_{22} \end{pmatrix}$$
   où les blocs de la première colonne, correspondant à $\mathcal{S}^{d-1}$, sont connus. Il reste à déterminer ceux de la deuxième colonne. On souhaite avoir ${}^t\chi_t = \hat{\chi}_{-t}$. La relation $\mathcal{R}\cdot$ assure que les conditions de compatibilité données par les blocs de la première colonne sont vérifiées ; on prend alors des blocs convenables pour la deuxième colonne.

   Montrons par récurrence sur $|j|$ qu'avec χ défini de la sorte, $\forall j$, $|j| \in \{0, ..., d\}$,
   $$v_{(j)} = \chi^{(j)} v_0. \tag{3}$$

Pour $|j| = 0$, on a $v_0 = \chi^j v_0 = Id\, v_0$
Supposons le résultat vrai pour $|j| < d_1 \leq d$.
Soit $s = \{t\} * j$ avec $t \neq 0, -n \leq t \leq n$ et $|j| = d_1 - 1$.

$$\chi^{(s)} v_0 = \chi_t \chi^{(j)} v_0 = \chi_t v_{(j)} = v_{(\{t\}*j)} = v_{(s)}$$

d'où (3) pour $s = d_1$.

2. Si $v_0 = 0$ ou si les $v_{(j)}$, $|j| \in \{0, ..., d-1\}$ sont liés, on « perturbe » les $v_{(j)}$, tout en conservant la relation $\mathcal{R}\cdot$, afin d'obtenir un ensemble de vecteurs linéairement indépendants.

Lemme 6 (Perturbation assurant l'indépendance linéaire)**.** *Soient $v_{(j)}, |j| \in \{0, ..., d\}$ des vecteurs de $\mathbb{R}^r$, qui vérifient la relation $\mathcal{R}\cdot$.*

(a) Si les $\phi_{(j)} \in \mathbb{R}^r, |j| \in \{0, ..., d\}$, sont linéairement indépendants et satisfont $\mathcal{R}\cdot$, et si pour tous $(i), (j)$, $v_{(i)}$ est orthogonal à $\phi_{(j)}$, alors les vecteurs :

$$\tilde{v}_{(j)} = v_{(j)} + \phi_{(j)}$$

sont linéairement indépendants et vérifient $\mathcal{R}\cdot$.

(b) S'il existe des vecteurs linéairement indépendants $\psi_{(j)} \in \mathbb{R}^q, |j| \in \{0, ..., d\}$, qui vérifient $\mathcal{R}\cdot$ et si $r \geq \nu(d)+q$, alors il existe des perturbations arbitrairement petites des $v_{(j)}$, i.e. $\forall (j)\ \exists \phi_{(j)}, \tilde{v}_{(j)} = v_{(j)} + \phi_{(j)}$ sont linéairement indépendants et satisfont $\mathcal{R}\cdot$

Démonstration. (a) La relation $\mathcal{R}\cdot$ découle de l'orthogonalité des $v_{(i)}$ et des $\phi_{(j)}$, qui entraîne $\tilde{v}_{(i)} \cdot \tilde{v}_{(j)} = v_{(i)} \cdot v_{(j)} + \phi_{(i)} \cdot \phi_{(j)}$ et du fait que les $v_{(j)}$ et les $\phi_{(j)}$ vérifient $\mathcal{R}\cdot$.

Montrons que les $\tilde{v}_{(j)}$ sont linéairement indépendants. Supposons qu'il existe des scalaires α_j tels que :

$$0 = \sum_j \alpha_j \tilde{v}_{(j)} = \sum_j \alpha_j v_{(j)} + \sum_j \alpha_j \phi_{(j)}$$

Grâce à la condition d'orthogonalité, en calculant la norme de

$$\sum_j \alpha_j \phi_{(j)}$$

on remarque que cette combinaison linéaire est nulle. Or les $\phi_{(j)}$ sont linéairement indépendants, donc on en déduit que les α_j sont tous nuls, d'où l'indépendance linéaire des $\tilde{v}_{(j)}$.

(b) Le supplémentaire orthogonal $\mathcal{V}^\perp$ de vect($\{v_{(j)}\}$) est de dimension $\geq q$, donc on a un plongement isométrique de $\mathbb{R}^q$, qui contient les $\psi_{(j)}$, dans $\mathcal{V}^\perp$. $\forall j$, notons $\tilde{\psi}_{(j)}$ l'image de $\psi_{(j)}$. Soit $\epsilon > 0$. On pose :

$$\tilde{v}_{(j)} = v_{(j)} + \epsilon\tilde{\psi}_{(j)} = v_{(j)} + \phi_{(j)}$$

Les $v_{(j)}$ sont orthogonaux aux $\phi_{(j)}$ par construction de ces derniers. Comme les $\psi_{(j)}$ vérifient $\mathcal{R}\cdot$, il en est de même des $\phi_{(j)}$. De plus, les $\phi_{(j)}$ sont linéairement indépendants en tant qu'images des $\psi(j)$ par une injection. Donc, d'après (a), les $\tilde{v}_{(j)} = v_{(j)} + \phi_{(j)}$ sont linéairement indépendants et vérifient $\mathcal{R}\cdot$.

□

Lemme 7 (Existence d'une famille libre vérifiant $\mathcal{R}\cdot$)**.** *Pour q assez grand, il existe un ensemble de vecteurs $\psi_{(j)} \in \mathbb{R}^q$ qui vérifient $\mathcal{R}\cdot$.*

Démonstration. Montrons qu'il existe un vecteur de la forme $V^d(\chi)v_0$ dont les composantes soient linéairement indépendantes. En effet, on sait déjà qu'elles vérifient $\mathcal{R}\cdot$. Soit un vecteur $v_0 \in \mathbb{R}^q$. Supposons que, $\forall v$ de la forme $V^d(\chi)v_0$, ses composantes sont liées, i.e. $\forall\chi = \{\chi_1, ..., \chi_n\}$, il existe des réels $\lambda_j(\chi, v_0)$ tels que

$$\sum_j \lambda_j(\chi, v_0)V^d(\chi)_j v_0 = 0 \tag{4}$$

Dans [3] est démontré que si (4) est vraie pour tout χ assez grand et pour tout v_0, il existe des réels α_j tels que le polynôme non commutatif

$$\sum_j \alpha_j V^d(X)_j$$

soit nul. Mais les $V^d(X)j$ sont des monômes distincts, donc ils sont linéairement indépendants, ce qui contredit ce qui précède. D'où l'existence d'un vecteur de la forme $V^d(\chi)v_0$ ayant ses composantes linéairement indépendantes. □

Il suffit maintenant d'associer ces deux lemmes pour terminer la démonstration du 2^e cas du théorème.

□

Lemme 8. *On a :*

$$\overline{\mathcal{A}_{V^d,q}} = (\mathcal{B}_{V^d})^{\perp+}$$

Démonstration. Si q est assez grand,

$$\begin{aligned}\overline{\mathcal{A}_{V^d,q}} &= \{A_v\colon v \text{ vérifie } \mathcal{R}\cdot\} \\ &= \left\{A_v\colon v \text{ vérifie } v_i\cdot v_j = v_k\cdot v_l \text{ pour } \{(i,j),(k,l)\in\mathcal{P}\}\right\}\end{aligned}$$

où $\mathcal{P}$ est un certaine collection de paires de couples.

Donc $\overline{\mathcal{A}_{V^d,q}} = \mathcal{A}^{\mathcal{P}} = (\mathcal{B}^{\mathcal{P}})^{\perp+} = (\mathcal{B}_{V^d})^{\perp+}$ d'après le lemme 4. □

Lemme 9. *L'ensemble $(\mathcal{B}_{V^d})^{\perp+}$ contient une matrice inversible.*

Démonstration. En écrivant $\mathcal{B}_{V^d} = \mathcal{B}^{\mathcal{P}}$, on sait, d'après le lemme 4, que la seule façon d'avoir $(\mathcal{B}_{V^d})^{\perp+}$ ne contenant pas de matrice inversible serait que les vecteurs de chaque ensemble $\{v_0,...,v_{\nu(d)-1}\}$ de $\mathbb{R}^q$ vérifiant

$$v_i\cdot v_j = v_k\cdot v_l \text{ pour tout } \{(i,j),(k,l)\}\in\mathcal{P} \tag{5}$$

soient liés. Mais le lemme 7 assure l'existence, pour q assez grand, d'un ensemble de vecteurs linéairement indépendants de $\mathbb{R}^q$ vérifiant (5). □

3.6 Fin de la démonstration

Théorème 13 (Q est somme de carrés)**.** *S'il existe q tel que $\overline{\mathcal{A}_{V^d,q}} = (\mathcal{B}_{V^d})^{\perp+} \subset \mathfrak{S}_p(\mathbb{R})$ et si $\mathcal{B}_{V^d}$ contient une matrice inversible, le fait que Q soit positif au sens matriciel implique que Q est somme de carrés .*

Démonstration. En effet,

$$\ell_{M_Q} \geq 0 \text{ sur } \mathcal{A}_{V^d,q}$$

de sorte que si

$$\overline{\mathcal{A}_{V^d,q}} = (\mathcal{B}_{V^d})^{\perp+}$$

$$\ell_{M_Q} \geq 0 \text{ sur } (\mathcal{B}_{V^d})^{\perp+}$$

Donc il existe une matrice symétrique positive M telle que $M = M_Q + B$, avec $B\in\mathcal{B}_{V^d}$ c'est-à-dire :

$$Q(X) =^t V^d(X)M_QV^d(X) =^t V^d(X)MV^d(X)$$

On utilise alors la décomposition de Cholesky : on peut écrire $M =^t LDL$ avec D diagonale positive. Ainsi le polynôme Q est décomposé en somme de carrés. □

4 Conclusion

4.1 Prolongements

En réalité, le résultat obtenu est plus fort que celui annoncé. Pour montrer qu'un polynôme symétrique Q est somme de carrés, il n'est pas nécessaire de tester la condition de positivité pour toutes les matrices de toutes les tailles : il suffit de vérifier que Q prend des valeurs positives pour toutes les matrices d'une taille $q \geq p$, ou encore pour toutes les matrices de taille $p = \nu(d)$.

Soit Q un polynôme hermitien en X ($2n$ indéterminées) à coefficients complexes.

On remarque que substituer les indéterminées X par des matrices χ à coefficients complexes revient à le faire avec des matrices réelles dans le sens suivant : à X_k, on fait correspondre $R_k + iI_k$ et à ${}^tX_k$, ${}^tR_k - i{}^tI_k$, de sorte que Q devient un polynôme hermitien à coefficients complexes en les « $4n$ indéterminées réelles » R_k et I_k. Cette caractérisation permet d'utiliser le lemme 7, qui s'applique dans le cas de matrices χ réelles.

En étendant les définitions « positif » et « somme de carrés » aux complexes, on a : si Q est positif, il est somme de carrés. En effet, il existe une représentation de Gram de Q avec M_Q hermitienne, puis tout le reste de la démonstration étant valide en remplaçant les réels par les complexes, on obtient un résultat similaire à celui du cas réel.

4.2 Un algorithme pour tester la positivité

Les auteurs du deuxième article que nous avons étudié se sont intéressés à la positivité des polynômes à variables non commutatives parce qu'ils souhaitaient développer un package NCalgebra d'algèbre linéaire non commutative pour Mathematica. Ce package doit permettre de résoudre des systèmes linéaires, des problèmes technologiques, dans lesquels interviennent des inégalités matricielles.

En fait, tester la condition de positivité sur un polynôme demande un temps démesuré : pour un polynôme à deux variables et des matrices de taille 5×5, il faudrait de l'ordre de 10^{60} années pour faire le test !

En revanche, d'autres chercheurs (Reznik, Powers-Wörmann, Parrilo) ont mis au point des techniques permettant de tester si un polynôme de taille raisonnable est somme de carrés. On en déduit que les résultats de Helton et Mc Cullough prouvent qu'il est possible de vérifier le positivité d'un polynôme en pratique, puisque la positivité est équivalente au fait que le polynôme soit somme de carrés.

L'algorithme de Powers-Wörmann, décrit dans [8], repose sur l'équivalence entre être une somme de carrés et avoir une représentation de Gram. Le but de l'algorithme est de trouver une matrice M positive telle que le polynôme f soit égal à ${}^tXMX$. Pour cela, l'algorithme est divisé en plusieurs parties.

La première consiste à déterminer les matrices (non nécessairement positives) qui conviennent dans la représentation de Gram. Si on part d'un polynôme $Q = \sum_\alpha q_\alpha X^\alpha$, cela revient à résoudre un système $\sum_{V_i+V_j=\alpha} m_{i,j} = q_\alpha$ en les $m_{i,j}$. Or chaque inconnue n'intervient que dans une seule équation, donc on peut poser dans chaque équation toutes les inconnues sauf une en paramètres λ_i et résoudre en la dernière inconnue. La solution est alors donnée par $\sum_i \lambda_i M_i$.

On cherche ensuite les valeurs des paramètres qui rendent la matrice positive, donc toutes ses valeurs propres positives. Pour cela on utilise la règle des signes de Descartes sur le polynôme caractéristique, et on cherche si l'ensemble des solutions en λ est non vide (ce qui est assez lourd en complexité).

Une fois obtenue une représentation de Gram du polynôme, on peut en déduire une écriture sous la forme d'une somme de carrés. La complexité est polynômiale en le nombre de variables, tandis que les méthodes de points critiques sont exponentielles. Différentes questions se posent alors, en particulier la minimisation du nombre de carrés dans l'écriture. Par exemple le polynôme $p(x,y) = x^2 - xy^2 + y^4 + 1$ s'écrit aussi $\frac{3}{4}(x-y^2)^2 + \frac{1}{4}(x+y^2)^2 + 1$. Ce problème est à notre connaissance toujours ouvert.

5 Références

[1] S. McCullough, Factorization of operator-valued polynomials in several noncommuting variables, Elsevier, Linear algebra and its applications, 2000.

[2] J. W. Helton, « Positive» noncommutative polynomials are sums of squares, Ann. of Math., **156** (2002), 675-694.

[3] J. F. Camino, J. W. Helton, R. E. Skelton, J. Ye, Matrix inequalities : a symbolic procedure to determine convexity automatically, www.math.ucsd.edu/∼helton, prépublication.

[4] J. W. Helton et M. Putinar, Positive polynomials in scalar and matrix variables, the spectral theorem and optimization, preprint UC Santa Barbara Mathematics Department, 2006-42, www.math.ucsb.edu/∼drm/preprintseries

[5] H. Royden, Real Analysis, The Macmillan Co., New York, 1964

[6] M. Rosenblum et J. Rovnyak, Hardy classes and operator theory, Oxford Science Publications, 1985.

[7] M. Takesaki, Theory of Operator Algebra, tomes I et III, Encyclopaedia of Mathematical Sciences, Springer, 1979.

[8] V. Powers et T. Wörmann, An algorithm for sums of squares of real polynomials, www.mathcs.emory.edu/∼vicki/pub/sos.pdf

Nous tenons à remercier Philippe Biane qui a encadré notre travail.