

Introduction à la géométrie algébrique réelle et application à l'optimisation polynomiale

Fabien Priziac

Aix-Marseille Université/Institut de Mathématiques de Marseille

13 novembre 2019

Polynômes à coefficients réels en plusieurs variables

$$\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \dots, X_n] := \{\text{polynômes en } n \text{ variables à coefficients réels}\}.$$

$\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \dots, X_n] := \{\text{polynômes en } n \text{ variables à coefficients réels}\}.$

Exemples

- $p = X^2 + 1 \in \mathbb{R}[X]$
- $p = Y^2 - X^3 \in \mathbb{R}[X, Y]$
- $p = X^2 - Y^2Z \in \mathbb{R}[X, Y, Z]$

$\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \dots, X_n] := \{\text{polynômes en } n \text{ variables à coefficients réels}\}.$

Exemples

- $p = X^2 + 1 \in \mathbb{R}[X]$
- $p = Y^2 - X^3 \in \mathbb{R}[X, Y]$
- $p = X^2 - Y^2Z \in \mathbb{R}[X, Y, Z]$

Si $p \in \mathbb{R}[\underline{X}]$,

Polynômes à coefficients réels en plusieurs variables

$\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \dots, X_n] := \{\text{polynômes en } n \text{ variables à coefficients réels}\}.$

Exemples

- $p = X^2 + 1 \in \mathbb{R}[X]$
- $p = Y^2 - X^3 \in \mathbb{R}[X, Y]$
- $p = X^2 - Y^2Z \in \mathbb{R}[X, Y, Z]$

Si $p \in \mathbb{R}[\underline{X}]$, p s'écrit

$$p = \sum_{\text{finie}} a_{\alpha} X^{\alpha},$$

où $X^{\alpha} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ si $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$,

$\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \dots, X_n] := \{\text{polynômes en } n \text{ variables à coefficients réels}\}.$

Exemples

- $p = X^2 + 1 \in \mathbb{R}[X]$
- $p = Y^2 - X^3 \in \mathbb{R}[X, Y]$
- $p = X^2 - Y^2Z \in \mathbb{R}[X, Y, Z]$

Si $p \in \mathbb{R}[\underline{X}]$, p s'écrit

$$p = \sum_{\text{finie}} a_{\alpha} X^{\alpha},$$

où $X^{\alpha} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ si $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, et on note

$$\deg(p) := \max_{\alpha} (\alpha_1 + \dots + \alpha_n).$$

Polynômes à coefficients réels en plusieurs variables

$\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \dots, X_n] := \{\text{polynômes en } n \text{ variables à coefficients réels}\}.$

Exemples

- $p = X^2 + 1 \in \mathbb{R}[X]$
- $p = Y^2 - X^3 \in \mathbb{R}[X, Y]$
- $p = X^2 - Y^2Z \in \mathbb{R}[X, Y, Z]$

Si $p \in \mathbb{R}[\underline{X}]$, p s'écrit

$$p = \sum_{\text{finie}} a_{\alpha} X^{\alpha},$$

où $X^{\alpha} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ si $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, et on note

$$\deg(p) := \max_{\alpha} (\alpha_1 + \dots + \alpha_n).$$

Remarque

$(\mathbb{R}[\underline{X}], \cdot, +, \times)$ est une $\mathbb{R}$ -algèbre de type fini.

Soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$.

Systèmes d'équations polynomiales

Soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note $V(p_1, \dots, p_m)$ l'ensemble des solutions $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ du système

$$\begin{cases} p_1(x) = 0 \\ \vdots \\ p_m(x) = 0 \end{cases}$$

Systèmes d'équations polynomiales

Soient $p_1, \dots, p_m \in \mathbb{R}[X]$. On note $V(p_1, \dots, p_m)$ l'ensemble des solutions $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ du système

$$\begin{cases} p_1(x) = 0 \\ \vdots \\ p_m(x) = 0 \end{cases}$$

Définition

$V(p_1, \dots, p_m)$ est appelé un *ensemble algébrique réel*.

Soient $p_1, \dots, p_m \in \mathbb{R}[X]$. On note $V(p_1, \dots, p_m)$ l'ensemble des solutions $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ du système

$$\begin{cases} p_1(x) = 0 \\ \vdots \\ p_m(x) = 0 \end{cases}$$

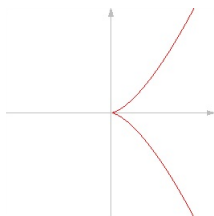
Définition

$V(p_1, \dots, p_m)$ est appelé un *ensemble algébrique réel*.

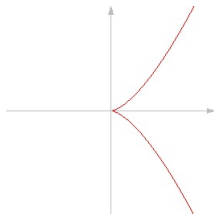
Remarque : $V(p_1, \dots, p_m) = V(p_1^2 + \dots + p_m^2)$.

Exemples

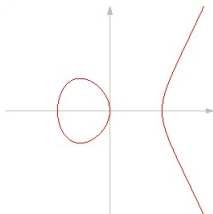
- $V(Y^2 - X^3)$:



Exemples



- $V(Y^2 - X^3)$:



- $V(X + Y^2 - X^3)$:

- $V(X^2 + Y^2 + Z^2 - 1)$:



- $V(X^2 + Y^2 + Z^2 - 1)$:



- $V(16(X^2 + Y^2) - (X^2 + Y^2 + Z^2 + 3)^2)$:



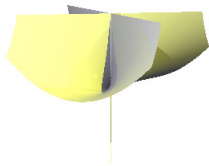
- $V(X^2 + Y^2 - Z^2) :$



- $V(X^2 + Y^2 - Z^2) :$



- $V(X^2 - Y^2Z) :$



Systèmes d'inégalités polynomiales

Soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$.

Systèmes d'inégalités polynomiales

Soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note $S(p_1, \dots, p_m)$ l'ensemble des solutions $x \in \mathbb{R}^n$ du système

$$\begin{cases} p_1(x) \geq 0 \\ \vdots \\ p_m(x) \geq 0 \end{cases}$$

Soient $p_1, \dots, p_m \in \mathbb{R}[X]$. On note $S(p_1, \dots, p_m)$ l'ensemble des solutions $x \in \mathbb{R}^n$ du système

$$\begin{cases} p_1(x) \geq 0 \\ \vdots \\ p_m(x) \geq 0 \end{cases}$$

Définition

$S(p_1, \dots, p_m)$ est appelé un *ensemble semi-algébrique fermé basique*.

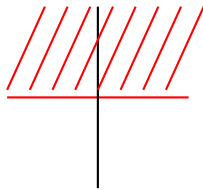
Soient $p_1, \dots, p_m \in \mathbb{R}[X]$. On note $S(p_1, \dots, p_m)$ l'ensemble des solutions $x \in \mathbb{R}^n$ du système

$$\begin{cases} p_1(x) \geq 0 \\ \vdots \\ p_m(x) \geq 0 \end{cases}$$

Définition

$S(p_1, \dots, p_m)$ est appelé un *ensemble semi-algébrique fermé basique*.

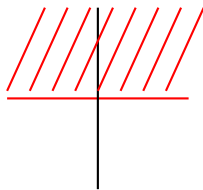
Remarque : $V(p) = S(p, -p)$.



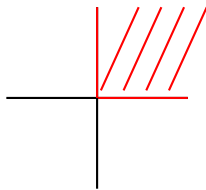
- $S(Y)$:

Exemples

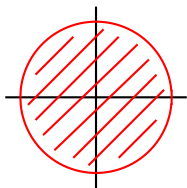
- $S(Y)$:



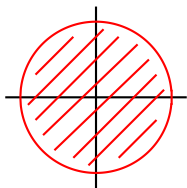
- $S(X, Y)$:



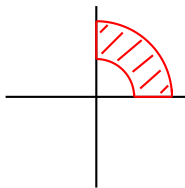
- $S(1 - X^2 - Y^2) :$



- $S(1 - X^2 - Y^2) :$



- $S(1 - X^2 - Y^2, X^2 + Y^2 - \frac{1}{4}, X, Y) :$



Ensembles semi-algébriques

Définition

Un *ensemble semi-algébrique* de $\mathbb{R}^n$ est une union finie d'ensembles de la forme

$$\{x \in \mathbb{R}^n \mid p(x) = 0, q_1(x) > 0, \dots, q_l(x) > 0\}$$

avec $p, q_1, \dots, q_l \in \mathbb{R}[\underline{X}]$.

Définition

Un *ensemble semi-algébrique* de $\mathbb{R}^n$ est une union finie d'ensembles de la forme

$$\{x \in \mathbb{R}^n \mid p(x) = 0, q_1(x) > 0, \dots, q_l(x) > 0\}$$

avec $p, q_1, \dots, q_l \in \mathbb{R}[\underline{X}]$.

Remarques :

Définition

Un *ensemble semi-algébrique* de $\mathbb{R}^n$ est une union finie d'ensembles de la forme

$$\{x \in \mathbb{R}^n \mid p(x) = 0, q_1(x) > 0, \dots, q_l(x) > 0\}$$

avec $p, q_1, \dots, q_l \in \mathbb{R}[\underline{X}]$.

Remarques :

- $S(p) = V(p) \cup \{p > 0\}$,

Définition

Un *ensemble semi-algébrique* de $\mathbb{R}^n$ est une union finie d'ensembles de la forme

$$\{x \in \mathbb{R}^n \mid p(x) = 0, q_1(x) > 0, \dots, q_l(x) > 0\}$$

avec $p, q_1, \dots, q_l \in \mathbb{R}[\underline{X}]$.

Remarques :

- $S(p) = V(p) \cup \{p > 0\}$,
- $\{p > 0\} = \mathbb{R}^n \setminus S(-p)$,

Définition

Un *ensemble semi-algébrique* de $\mathbb{R}^n$ est une union finie d'ensembles de la forme

$$\{x \in \mathbb{R}^n \mid p(x) = 0, q_1(x) > 0, \dots, q_l(x) > 0\}$$

avec $p, q_1, \dots, q_l \in \mathbb{R}[X]$.

Remarques :

- $S(p) = V(p) \cup \{p > 0\}$,
- $\{p > 0\} = \mathbb{R}^n \setminus S(-p)$,
- $\{p \neq 0\} = \{p > 0\} \cup \{-p > 0\}$.

Définition

Un *ensemble semi-algébrique* de $\mathbb{R}^n$ est une union finie d'ensembles de la forme

$$\{x \in \mathbb{R}^n \mid p(x) = 0, q_1(x) > 0, \dots, q_l(x) > 0\}$$

avec $p, q_1, \dots, q_l \in \mathbb{R}[X]$.

Remarques :

- $S(p) = V(p) \cup \{p > 0\}$,
- $\{p > 0\} = \mathbb{R}^n \setminus S(-p)$,
- $\{p \neq 0\} = \{p > 0\} \cup \{-p > 0\}$.

Proposition

Stabilité des s.a. de $\mathbb{R}^n$ sous union, intersection, complémentaire.

Exemple



Soit A un s.a. de $\mathbb{R}^n$.

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$ et

$$\mathcal{P}(A) := \mathbb{R}[\underline{X}] / I(A)$$

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$ et

$$\mathcal{P}(A) := \mathbb{R}[\underline{X}] / I(A)$$

($\mathbb{R}$ -algèbre de type fini des *fonctions polynomiales* sur A).

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$ et

$$\mathcal{P}(A) := \mathbb{R}[\underline{X}] / I(A)$$

($\mathbb{R}$ -algèbre de type fini des *fonctions polynomiales* sur A).

Définition

Soit B un s.a. de $\mathbb{R}^m$. Une application $\varphi = (\varphi_1, \dots, \varphi_m) : A \rightarrow B$ est

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$ et

$$\mathcal{P}(A) := \mathbb{R}[\underline{X}]/I(A)$$

($\mathbb{R}$ -algèbre de type fini des *fonctions polynomiales* sur A).

Définition

Soit B un s.a. de $\mathbb{R}^m$. Une application $\varphi = (\varphi_1, \dots, \varphi_m) : A \rightarrow B$ est

- *polynomiale* si $\forall i \in \{1, \dots, m\}, \varphi_i \in \mathcal{P}(A)$,

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$ et

$$\mathcal{P}(A) := \mathbb{R}[\underline{X}]/I(A)$$

($\mathbb{R}$ -algèbre de type fini des *fonctions polynomiales* sur A).

Définition

Soit B un s.a. de $\mathbb{R}^m$. Une application $\varphi = (\varphi_1, \dots, \varphi_m) : A \rightarrow B$ est

- *polynomiale* si $\forall i \in \{1, \dots, m\}, \varphi_i \in \mathcal{P}(A)$,
- *un isomorphisme polynomial* si φ est poly., bij. et φ^{-1} poly.

Soit A un s.a. de $\mathbb{R}^n$.

On note $I(A) := \{p \in \mathbb{R}[\underline{X}] \mid \forall x \in A, p(x) = 0\}$ et

$$\mathcal{P}(A) := \mathbb{R}[\underline{X}] / I(A)$$

($\mathbb{R}$ -algèbre de type fini des *fonctions polynomiales* sur A).

Définition

Soit B un s.a. de $\mathbb{R}^m$. Une application $\varphi = (\varphi_1, \dots, \varphi_m) : A \rightarrow B$ est

- *polynomiale* si $\forall i \in \{1, \dots, m\}, \varphi_i \in \mathcal{P}(A)$,
- *un isomorphisme polynomial* si φ est poly., bij. et φ^{-1} poly.

Remarque : Toute application polynomiale $\varphi : A \rightarrow B$ induit un morphisme de $\mathbb{R}$ -algèbres $\varphi^* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$; $f \mapsto f \circ \varphi$.

Théorème (Tarski-Seidenberg)

Soit $\varphi : A \rightarrow B$ une application polynomiale entre s.a., alors $\varphi(A)$ est un ensemble semi-algébrique.

Théorème (Tarski-Seidenberg)

Soit $\varphi : A \rightarrow B$ une application polynomiale entre s.a., alors $\varphi(A)$ est un ensemble semi-algébrique.

Remarque : L'image d'un ens. alg. par une application polynomiale n'est *pas algébrique* en général : pour $\varphi : \mathbb{R} \rightarrow \mathbb{R} ; x \mapsto x^2$, on a $\varphi(\mathbb{R}) = \{x \geq 0\}$.

Soit V un ensemble algébrique réel.

Soit V un ensemble algébrique réel. Alors $\mathcal{P}(V)$ est un *anneau réel* :

$$\forall f_1, \dots, f_m \in \mathcal{P}(V), f_1^2 + \dots + f_k^2 = 0 \Rightarrow f_1 = \dots = f_k = 0.$$

Soit V un ensemble algébrique réel. Alors $\mathcal{P}(V)$ est un *anneau réel* :

$$\forall f_1, \dots, f_m \in \mathcal{P}(V), f_1^2 + \dots + f_m^2 = 0 \Rightarrow f_1 = \dots = f_m = 0.$$

Théorème (Nullstellensatz réel)

A toute application polynomiale entre ens. alg. réels *correspond* un morphisme de $\mathbb{R}$ -algèbres entre $\mathbb{R}$ -algèbres de type fini réelles.

Soit G un groupe de Lie compact

Soit G un groupe de Lie compact agissant sur V par iso. polynomiaux.

Soit G un groupe de Lie compact agissant sur V par iso. polynomiaux.

Exemple

$V = \mathbb{R}^2$, $G = \{id, s\}$, $s : (x, y) \mapsto (-x, y)$.

Soit G un groupe de Lie compact agissant sur V par iso. polynomiaux.

Exemple

$V = \mathbb{R}^2$, $G = \{id, s\}$, $s : (x, y) \mapsto (-x, y)$.

- L'action de G sur V induit une action de G sur $\mathcal{P}(V)$:

$$g \cdot f := f \circ g^{-1}.$$

Soit G un groupe de Lie compact agissant sur V par iso. polynomiaux.

Exemple

$V = \mathbb{R}^2$, $G = \{id, s\}$, $s : (x, y) \mapsto (-x, y)$.

- L'action de G sur V induit une action de G sur $\mathcal{P}(V)$:

$$g \cdot f := f \circ g^{-1}.$$

- $\mathcal{P}(V)^G \subset \mathcal{P}(V)$ est une $\mathbb{R}$ -algèbre réelle.

Théorème de finitude de Hilbert

$\mathcal{P}(V)^G$ est de type fini.

Théorème de finitude de Hilbert

$\mathcal{P}(V)^G$ est de type fini.

Conséquences :

Théorème de finitude de Hilbert

$\mathcal{P}(V)^G$ est de type fini.

Conséquences :

- $\mathcal{P}(V)^G$ correspond à un ens. alg. réel Z ,

Théorème de finitude de Hilbert

$\mathcal{P}(V)^G$ est de type fini.

Conséquences :

- $\mathcal{P}(V)^G$ correspond à un ens. alg. réel Z ,
- l'inclusion $\mathcal{P}(V)^G \hookrightarrow \mathcal{P}(V)$ correspond à une application poly.
 $\pi : V \rightarrow Z$.

Théorème de finitude de Hilbert

$\mathcal{P}(V)^G$ est de type fini.

Conséquences :

- $\mathcal{P}(V)^G$ correspond à un ens. alg. réel Z ,
- l'inclusion $\mathcal{P}(V)^G \hookrightarrow \mathcal{P}(V)$ correspond à une application poly.
 $\pi : V \rightarrow Z$.

Mais π n'est pas surjective en général !

Théorème de finitude de Hilbert

$\mathcal{P}(V)^G$ est de type fini.

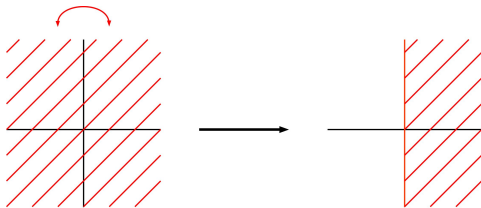
Conséquences :

- $\mathcal{P}(V)^G$ correspond à un ens. alg. réel Z ,
- l'inclusion $\mathcal{P}(V)^G \hookrightarrow \mathcal{P}(V)$ correspond à une application poly.
 $\pi : V \rightarrow Z$.

Mais π n'est pas surjective en général !

On note $V//G := \pi(V)$: c'est un ens. semi-algébrique.

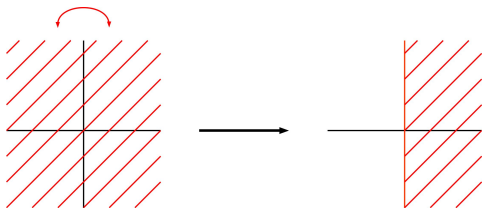
Exemples



• $\mathbb{R}^2 \quad (x, y) \mapsto (-x, y)$

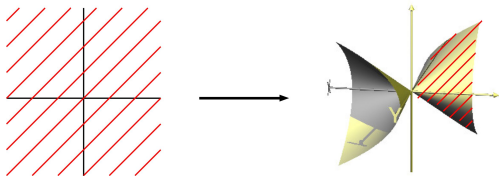
$\{x \geq 0\}$

Exemples



• $\mathbb{R}^2 \quad (x, y) \mapsto (-x, y)$

$\{x \geq 0\}$



• $\mathbb{R}^2 \quad (x, y) \mapsto (-x, -y)$

$\{z^2 = xy, x \geq 0, y \geq 0\}$

Le 17^{ème} problème de Hilbert

Soit $p \in \mathbb{R}[\underline{X}]$.

Le 17^{ème} problème de Hilbert

Soit $p \in \mathbb{R}[\underline{X}]$.

Théorème (Artin)

Si $p \geq 0$ sur $\mathbb{R}^n$, alors $\exists h_1, \dots, h_m$ fractions rationnelles t.q.

$$p = h_1^2 + \dots + h_m^2.$$

Soit $p \in \mathbb{R}[\underline{X}]$.

Théorème (Artin)

Si $p \geq 0$ sur $\mathbb{R}^n$, alors $\exists h_1, \dots, h_m$ fractions rationnelles t.q.

$$p = h_1^2 + \dots + h_m^2.$$

Remarque : L'écriture précédente constitue un *certificat de positivité* pour p .

Sommes de carrés et certificats

On note

$$\Sigma := \left\{ \sum_{finie} q_j^2 \mid q_j \in \mathbb{R}[\underline{X}] \right\}.$$

On note

$$\Sigma := \left\{ \sum_{finie} q_j^2 \mid q_j \in \mathbb{R}[\underline{X}] \right\}.$$

Théorème

- (Nullstellensatz réel) $V(p) = \emptyset$ ssi $\exists q \in \mathbb{R}[\underline{X}], \exists \sigma \in \Sigma$ tels que

$$-1 = \sigma + qp.$$

On note

$$\Sigma := \left\{ \sum_{finie} q_j^2 \mid q_j \in \mathbb{R}[\underline{X}] \right\}.$$

Théorème

- (Nullstellensatz réel) $V(p) = \emptyset$ ssi $\exists q \in \mathbb{R}[\underline{X}], \exists \sigma \in \Sigma$ tels que

$$-1 = \sigma + qp.$$

- $S(p_1, \dots, p_m) = \emptyset$ ssi $\exists \sigma_J \in \Sigma$ tels que

$$-1 = \sum_J \sigma_J p_J.$$

On note

$$\Sigma := \left\{ \sum_{finie} q_j^2 \mid q_j \in \mathbb{R}[\underline{X}] \right\}.$$

et, pour $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$, $J \subset \{1, \dots, m\}$, $p_J := \prod_{j \in J} p_j$.

Théorème

- (Nullstellensatz réel) $V(p) = \emptyset$ ssi $\exists q \in \mathbb{R}[\underline{X}]$, $\exists \sigma \in \Sigma$ tels que

$$-1 = \sigma + qp.$$

- $S(p_1, \dots, p_m) = \emptyset$ ssi $\exists \sigma_J \in \Sigma$ tels que

$$-1 = \sum_J \sigma_J p_J.$$

On note

$$\Sigma := \left\{ \sum_{finie} q_j^2 \mid q_j \in \mathbb{R}[\underline{X}] \right\}.$$

et, pour $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$, $J \subset \{1, \dots, m\}$, $p_J := \prod_{j \in J} p_j$.

Théorème

- (Nullstellensatz réel) $V(p) = \emptyset$ ssi $\exists q \in \mathbb{R}[\underline{X}], \exists \sigma \in \Sigma$ tels que

$$-1 = \sigma + qp.$$

- $S(p_1, \dots, p_m) = \emptyset$ ssi $\exists \sigma_J \in \Sigma$ tels que

$$-1 = \sum_J \sigma_J p_J.$$

Remarque : Bornes sur les degrés de σ , q , σ_J .

On note $C(p_1, \dots, p_m) := \left\{ \sum_J \sigma_J p_J \mid \sigma_J \in \Sigma \right\}$.

On note $C(p_1, \dots, p_m) := \left\{ \sum_J \sigma_J p_J \mid \sigma_J \in \Sigma \right\}$.

Théorème (Positivstellensatz)

$p \geq 0$ sur $S(p_1, \dots, p_m)$ ssi $\exists k \in \mathbb{N}, \exists h, g \in C(p_1, \dots, p_m)$ tels que

$$ph = p^{2k} + g.$$

On note $C(p_1, \dots, p_m) := \left\{ \sum_J \sigma_J p_J \mid \sigma_J \in \Sigma \right\}$.

Théorème (Positivstellensatz)

$p \geq 0$ sur $S(p_1, \dots, p_m)$ ssi $\exists k \in \mathbb{N}, \exists h, g \in C(p_1, \dots, p_m)$ tels que

$$ph = p^{2k} + g.$$

Remarque : Bornes sur les degrés et sur k .

Soit $p = \sum_{\alpha} p_{\alpha} X^{\alpha} \in \mathbb{R}[\underline{X}]$, $\deg(p) \leq d$.

Somme de carrés et matrices semi-définies positives

Soit $p = \sum_{\alpha} p_{\alpha} X^{\alpha} \in \mathbb{R}[\underline{X}]$, $\deg(p) \leq d$. On note

$$p = \sum_{\alpha} p_{\alpha} X^{\alpha} = {}^t \mathbf{p} \mathbf{x} = {}^t \mathbf{x} \mathbf{p}.$$

Somme de carrés et matrices semi-définies positives

Soit $p = \sum_{\alpha} p_{\alpha} X^{\alpha} \in \mathbb{R}[\underline{X}]$, $\deg(p) \leq d$. On note

$$p = \sum_{\alpha} p_{\alpha} X^{\alpha} = {}^t \mathbf{p} \mathbf{x} = {}^t \mathbf{x} \mathbf{p}.$$

où

$$\mathbf{x} := {}^t(X^{\alpha}) = {}^t(1, X_1, \dots, X_n, X_1^2, X_1 X_2, \dots, X_n^d) \in \mathbb{R}^N$$

$$\mathbf{p} := {}^t(p_{\alpha}) \in \mathbb{R}^N,$$

Somme de carrés et matrices semi-définies positives

Soit $p = \sum_{\alpha} p_{\alpha} X^{\alpha} \in \mathbb{R}[\underline{X}]$, $\deg(p) \leq d$. On note

$$p = \sum_{\alpha} p_{\alpha} X^{\alpha} = {}^t \mathbf{p} \mathbf{x} = {}^t \mathbf{x} \mathbf{p}.$$

où

$$\mathbf{x} := {}^t(X^{\alpha}) = {}^t(1, X_1, \dots, X_n, X_1^2, X_1 X_2, \dots, X_n^d) \in \mathbb{R}^N$$

$$\mathbf{p} := {}^t(p_{\alpha}) \in \mathbb{R}^N,$$

avec $N := \binom{n+d}{d}$.

Soit $q_j \in \mathbb{R}[\underline{X}]$, $\deg(q_j) \leq d$.

Somme de carrés et matrices semi-définies positives

Soit $q_j \in \mathbb{R}[\underline{X}]$, $\deg(q_j) \leq d$. Alors

$$\Sigma \ni \sum_j q_j^2$$

Soit $q_j \in \mathbb{R}[\underline{X}]$, $\deg(q_j) \leq d$. Alors

$$\Sigma \ni \sum_j q_j^2 = \sum_j {}^t \mathbf{x} \mathbf{q}_j {}^t \mathbf{q}_j \mathbf{x}$$

Soit $q_j \in \mathbb{R}[\underline{X}]$, $\deg(q_j) \leq d$. Alors

$$\Sigma \ni \sum_j q_j^2 = \sum_j {}^t \mathbf{x} \mathbf{q}_j {}^t \mathbf{q}_j \mathbf{x} = {}^t \mathbf{x} \left(\sum_j \mathbf{q}_j {}^t \mathbf{q}_j \right) \mathbf{x}$$

Somme de carrés et matrices semi-définies positives

Soit $q_j \in \mathbb{R}[\underline{X}]$, $\deg(q_j) \leq d$. Alors

$$\Sigma \ni \sum_j q_j^2 = \sum_j {}^t \mathbf{x} \mathbf{q}_j {}^t \mathbf{q}_j \mathbf{x} = {}^t \mathbf{x} \left(\sum_j \mathbf{q}_j {}^t \mathbf{q}_j \right) \mathbf{x} =: {}^t \mathbf{x} Q \mathbf{x}$$

où $Q \in M_N(\mathbb{R})$ est symétrique et semi-définie positive i.e.
 $\forall \mathbf{v} \in \mathbb{R}^N, {}^t \mathbf{v} Q \mathbf{v} \geq 0$.

Soit $p \in \mathbb{R}[\underline{X}]$ de degré $2d$.

Somme de carrés et matrices semi-définies positives

Soit $p \in \mathbb{R}[\underline{X}]$ de degré $2d$.

Proposition

$p \in \Sigma$ ssi $\exists Q \in M_N(\mathbb{R})$ semi-définie positive telle que ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$.

Soit $p \in \mathbb{R}[\underline{X}]$ de degré $2d$.

Proposition

$p \in \Sigma$ ssi $\exists Q \in M_N(\mathbb{R})$ semi-définie positive telle que ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$.

Remarque : ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$ ssi

$$\forall \alpha, \quad p_\alpha = \sum_{\mu+\nu=\alpha} Q_{\mu,\nu}$$

Soit $p \in \mathbb{R}[X]$ de degré $2d$.

Proposition

$p \in \Sigma$ ssi $\exists Q \in M_N(\mathbb{R})$ semi-définie positive telle que ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$.

Remarque : ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$ ssi

$$\forall \alpha, \quad p_\alpha = \sum_{\mu+\nu=\alpha} Q_{\mu,\nu} = \text{tr}(QH_\alpha)$$

$$\text{avec } H_\alpha = (h_{\mu,\nu}) \text{ avec } h_{\mu,\nu} = \begin{cases} 1 & \text{si } \mu + \nu = \alpha, \\ 0 & \text{sinon.} \end{cases}$$

Soit $p \in \mathbb{R}[X]$ de degré $2d$.

Proposition

$p \in \Sigma$ ssi $\exists Q \in M_N(\mathbb{R})$ semi-définie positive telle que ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$.

Remarque : ${}^t\mathbf{p}\mathbf{x} = {}^t\mathbf{x}Q\mathbf{x}$ ssi

$$\forall \alpha, \quad p_\alpha = \sum_{\mu+\nu=\alpha} Q_{\mu,\nu} = \text{tr}(QH_\alpha) =: \langle Q, H_\alpha \rangle$$

$$\text{avec } H_\alpha = (h_{\mu,\nu}) \text{ avec } h_{\mu,\nu} = \begin{cases} 1 & \text{si } \mu + \nu = \alpha, \\ 0 & \text{sinon.} \end{cases}$$

Somme de carrés, matrices semi-définies positives et optimisation semi-définie

Déterminer si $p \in \Sigma$ revient à résoudre le problème

Trouver $Q \in M_N(\mathbb{R})$ telle que

- Q est symétrique semi-définie positive,
- $\forall \alpha, \langle Q, H_\alpha \rangle = p_\alpha$.

Somme de carrés, matrices semi-définies positives et optimisation semi-définie

Déterminer si $p \in \Sigma$ revient à résoudre le problème d'*optimisation semi-définie*

Trouver $Q \in M_N(\mathbb{R})$ telle que

- Q est symétrique semi-définie positive,
- $\forall \alpha, \quad \langle Q, H_\alpha \rangle = p_\alpha.$

Soient $A, H_j \in M_N(\mathbb{R})$ des matrices symétriques et $b = (b_j) \in \mathbb{R}^m$.

Soient $A, H_j \in M_N(\mathbb{R})$ des matrices symétriques et $b = (b_j) \in \mathbb{R}^m$.

Le problème

Déterminer le supremum de la quantité $\langle Q, A \rangle$ avec

- $Q \in M_N(\mathbb{R})$ symétrique semi-définie positive,
- $\forall j, \langle Q, H_j \rangle = b_j$.

Soient $A, H_j \in M_N(\mathbb{R})$ des matrices symétriques et $b = (b_j) \in \mathbb{R}^m$.

Le problème

Déterminer le supremum de la quantité $\langle Q, A \rangle$ avec

- $Q \in M_N(\mathbb{R})$ symétrique semi-définie positive,
- $\forall j, \langle Q, H_j \rangle = b_j$.

est appelé *problème d'optimisation semi-définie (primal)*.

Soient $A, H_j \in M_N(\mathbb{R})$ des matrices symétriques et $b = (b_j) \in \mathbb{R}^m$.

Le problème

Déterminer le supremum de la quantité $\langle Q, A \rangle$ avec

- $Q \in M_N(\mathbb{R})$ symétrique semi-définie positive,
- $\forall j, \langle Q, H_j \rangle = b_j$.

est appelé *problème d'optimisation semi-définie (primal)*.

Un posd est résoluble numériquement à une précision ϵ près, en temps polynomial en N et $\ln(1/\epsilon)$.

Soit $p \in \mathbb{R}[\underline{X}]$, soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$.

Certificats de positivité (suite)

Soit $p \in \mathbb{R}[\underline{X}]$, soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note

$$K := S(p_1, \dots, p_m),$$

$$C := C(p_1, \dots, p_m) = \{\sum_J \sigma_J p_J \mid \sigma_J \in \Sigma\}.$$

Certificats de positivité (suite)

Soit $p \in \mathbb{R}[\underline{X}]$, soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note

$$K := S(p_1, \dots, p_m),$$

$$C := C(p_1, \dots, p_m) = \{\sum_J \sigma_J p_J \mid \sigma_J \in \Sigma\}.$$

Théorème (Positivstellensatz, certificat de positivité stricte)

$p > 0$ sur K ssi

Certificats de positivité (suite)

Soit $p \in \mathbb{R}[\underline{X}]$, soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note

$$K := S(p_1, \dots, p_m),$$

$$C := C(p_1, \dots, p_m) = \{\sum_J \sigma_J p_J \mid \sigma_J \in \Sigma\}.$$

Théorème (Positivstellensatz, certificat de positivité stricte)

$p > 0$ sur K ssi $\exists h, g \in C$ tels que

$$ph = 1 + g.$$

Certificats de positivité (suite)

Soit $p \in \mathbb{R}[\underline{X}]$, soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note

$$K := S(p_1, \dots, p_m),$$

$$C := C(p_1, \dots, p_m) = \{\sum_J \sigma_J p_J \mid \sigma_J \in \Sigma\}.$$

Théorème (Positivstellensatz, certificat de positivité stricte)

$p > 0$ sur K ssi $\exists h, g \in C$ tels que

$$ph = 1 + g.$$

Remarques :

- Bornes sur les degrés.

Soit $p \in \mathbb{R}[\underline{X}]$, soient $p_1, \dots, p_m \in \mathbb{R}[\underline{X}]$. On note

$$K := S(p_1, \dots, p_m),$$

$$C := C(p_1, \dots, p_m) = \{ \sum_J \sigma_J p_J \mid \sigma_J \in \Sigma \}.$$

Théorème (Positivstellensatz, certificat de positivité stricte)

$p > 0$ sur K ssi $\exists h, g \in C$ tels que

$$ph = 1 + g.$$

Remarques :

- Bornes sur les degrés.
- Décidable par un problème d'optimisation semi-définie, de grande taille (nombre de sommes de carrés $= 2^{m+1}$).

On suppose

Le Positivstellensatz de Putinar

On suppose K compact

Le Positivstellensatz de Putinar

On suppose K compact et

Hypothèse (H)

Il existe $q \in \mathcal{C}$ tel que $\{q \geq 0\}$ est compact.

Le Positivstellensatz de Putinar

On suppose K compact et

Hypothèse (H)

Il existe $q \in C$ tel que $\{q \geq 0\}$ est compact.

Alors

Théorème (Positivstellensatz de Putinar)

$$p > 0 \text{ sur } K$$

Le Positivstellensatz de Putinar

On suppose K compact et

Hypothèse (H)

Il existe $q \in \mathcal{C}$ tel que $\{q \geq 0\}$ est compact.

Alors

Théorème (Positivstellensatz de Putinar)

$$p > 0 \text{ sur } K \Rightarrow \exists \sigma_0, \sigma_j \in \Sigma \text{ t.q. } p = \sigma_0 + \sum_{i=1}^m \sigma_j p_j.$$

Le Positivstellensatz de Putinar

On suppose K compact et

Hypothèse (H)

Il existe $q \in \mathcal{C}$ tel que $\{q \geq 0\}$ est compact.

Alors

Théorème (Positivstellensatz de Putinar)

$$p > 0 \text{ sur } K \Rightarrow \exists \sigma_0, \sigma_j \in \Sigma \text{ t.q. } p = \sigma_0 + \sum_{i=1}^m \sigma_j p_j.$$

Remarques :

- Bornes sur les degrés.
- Nombre de sommes de carrés = $m + 1$.

Application à l'optimisation polynomiale

But : calculer $p^{\min} := \inf \{p(x) \mid x \in K\}$

Application à l'optimisation polynomiale

But : calculer $p^{\min} := \inf \{p(x) \mid x \in K\}$

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{\min} = d(x_0, K)^2$.

Application à l'optimisation polynomiale

But : calculer $p^{min} := \inf \{p(x) \mid x \in K\}$

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{min} = d(x_0, K)^2$.

Idée :

$$p^{min} = \sup \{ \lambda \mid p - \lambda \geq 0 \}$$

But : calculer $p^{min} := \inf \{p(x) \mid x \in K\}$

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{min} = d(x_0, K)^2$.

Idée :

$$\begin{aligned} p^{min} &= \sup \{ \lambda \mid p - \lambda \geq 0 \} \\ &= \sup \{ \lambda \mid p - \lambda > 0 \} \end{aligned}$$

Application à l'optimisation polynomiale

On suppose K compact et (H).

But : calculer $p^{min} := \inf \{p(x) \mid x \in K\}$

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{min} = d(x_0, K)^2$.

Idée :

$$\begin{aligned} p^{min} &= \sup \{ \lambda \mid p - \lambda \geq 0 \} \\ &= \sup \{ \lambda \mid p - \lambda > 0 \} \end{aligned}$$

Application à l'optimisation polynomiale

On suppose K compact et (H). On pose $p_0 := 1$.

But : calculer $p^{\min} := \inf \{p(x) \mid x \in K\} = \min \{p(x) \mid x \in K\}$.

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{\min} = d(x_0, K)^2$.

Idée :

$$\begin{aligned} p^{\min} &= \sup \{ \lambda \mid p - \lambda \geq 0 \} \\ &= \sup \{ \lambda \mid p - \lambda > 0 \} \\ &= \sup \{ \lambda \mid p - \lambda = \sum_{j=0}^m \sigma_j p_j, \quad \sigma_j \in \Sigma \} \end{aligned}$$

Application à l'optimisation polynomiale

On suppose K compact et (H). On pose $p_0 := 1$.

But : calculer $p^{min} := \inf \{p(x) \mid x \in K\} = \min \{p(x) \mid x \in K\}$.

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{min} = d(x_0, K)^2$.

Idée :

$$\begin{aligned} p^{min} &= \sup \{ \lambda \mid p - \lambda \geq 0 \} \\ &= \sup \{ \lambda \mid p - \lambda > 0 \} \\ &= \sup \{ \lambda \mid p - \lambda = \sum_{i=0}^m \sigma_i p_i, \quad \sigma_i \in \Sigma \} \end{aligned}$$

Problème : Bornes sur les degrés ?

Application à l'optimisation polynomiale

On suppose K compact et (H). On pose $p_0 := 1$.

But : calculer $p^{min} := \inf \{p(x) \mid x \in K\} = \min \{p(x) \mid x \in K\}$.

Exemple

Soit $x_0 \in \mathbb{R}^n$, $p(x) := \|x - x_0\|^2$, alors $p^{min} = d(x_0, K)^2$.

Idée :

$$\begin{aligned} p^{min} &= \sup \{ \lambda \mid p - \lambda \geq 0 \} \\ &= \sup \{ \lambda \mid p - \lambda > 0 \} \\ &= \sup \{ \lambda \mid p - \lambda = \sum_{j=0}^m \sigma_j p_j, \quad \sigma_j \in \Sigma \} \end{aligned}$$

Problème : Bornes sur les degrés ?

Solution : Constituer une suite de problèmes d'optimisation semi-définie bornés (méthode de Lasserre).

On note

$$p_k^{min} := \sup \left\{ \lambda \mid p - \lambda = \sum_{i=0}^m \sigma_i p_i, \quad \sigma_i \in \Sigma, \quad \deg(\sigma_i p_i) \leq k \right\}$$

On note

$$p_k^{min} := \sup \left\{ \lambda \mid p - \lambda = \sum_{i=0}^m \sigma_i p_i, \quad \sigma_i \in \Sigma, \quad \deg(\sigma_i p_i) \leq k \right\}$$

Calculer p_k^{min} revient à résoudre le problème d'optimisation semi-définie suivant :

On note

$$p_k^{\min} := \sup \left\{ \lambda \mid p - \lambda = \sum_{i=0}^m \sigma_i p_i, \quad \sigma_i \in \Sigma, \quad \deg(\sigma_i p_i) \leq k \right\}$$

Calculer $p_k^{\min}$ revient à résoudre le problème d'optimisation semi-définie suivant :

Trouver le supremum de la quantité $\sum_{j=0}^m \langle Q_j, G_0^j \rangle$ avec

- $Q_j \in M_{N_j}(\mathbb{R})$ symétriques semi-définies positives,
- $\forall \alpha \neq 0, \sum_{j=0}^m \langle Q_j, G_\alpha^j \rangle = p_\alpha$.

où N_j dépend de k .

Théorème (Lasserre)

La suite $(p_k^{min})_k$ converge vers p^{min} .

Théorème (Lasserre)

La suite $(p_k^{min})_k$ converge vers p^{min} .

Remarques :

Théorème (Lasserre)

La suite $(p_k^{min})_k$ converge vers p^{min} .

Remarques :

- Génériquement, la convergence est finie.

Théorème (Lasserre)

La suite $(p_k^{min})_k$ converge vers p^{min} .

Remarques :

- Génériquement, la convergence est finie.
- Algorithme (GloptiPoly), avec condition (suffisante) d'arrêt et extraction de vecteurs minimisants.

Théorème (Lasserre)

La suite $(p_k^{min})_k$ converge vers p^{min} .

Remarques :

- Génériquement, la convergence est finie.
- Algorithme (GloptiPoly), avec condition (suffisante) d'arrêt et extraction de vecteurs minimisants.
- Méthode pour le cas non-compact sous une autre hypothèse (H).

-  J. Bochnak, M. Coste, M.-F. Roy, *Real Algebraic Geometry*, 1998.
-  J. B. Lasserre, *An Introduction to Polynomial and Semi-Algebraic Optimization*, 2015.
-  V. Jeyakumar, J. B. Lasserre, G. Li, *On Polynomial Optimization Over Non-compact Semi-algebraic Sets*, 2014.
-  M. Laurent, *Sums of Squares, Moment Matrices and Optimization Over Polynomials*, 2008.
-  M. Schweighofer, *Optimization of Polynomials on Compact Semialgebraic Sets*, 2005.